Introducción al álgebra conmutativa

Alexey Beshenov (cadadr@gmail.com)

Universidad de El Salvador. 2018

Estos apuntes acompañan un curso de álgebra conmutativa en el programa de maestría de la Universidad de El Salvador. Vamos a seguir el libro de David Eisenbud "Commutative Algebra with a View Toward Algebraic Geometry" (Springer GTM 150) y trataremos de cubrir los capítulos 2, 4–7. Los temas principales son localización, dependencia integral, planitud y completación.

El texto de abajo esencialmente sigue el libro de Eisenbud. Otras fuentes recomendadas son

- El libro de texto "Introduction to Commutative Algebra" de Atiyah y Macdonald.
- A. Altman, S. Kleiman, "A Term of Commutative Algebra".
- Los apuntes "A Primer of Commutative Algebra" de James S. Milne disponibles en su página `http://www.jmilne.org/math/`
- Los apuntes de Pete L. Clark `http://math.uga.edu/~pete/integral.pdf`

Álgebra conmutativa tiene el siguiente propósito. Los objetos que se estudian en geometría algebraica se conocen como **esquemas** y pueden ser interpretados como el resultado de pegamento de anillos conmutativos. Esto es similar a la situación con variedades topológicas, diferenciables, complejas, etcétera, donde una variedad se ve localmente como $\mathbb{R}^n$ o $\mathbb{C}^n$. Ya que en geometría algebraica, un objeto geométrico se ve localmente como un anillo conmutativo, para estudiar los objetos geométricos, primero hay que conocer bien las propiedades de anillos conmutativos. Los detalles técnicos de esta historia se estudian en el presente curso y luego en el curso de geometría algebraica. Esta fusión de álgebra y geometría proporcionó fundamentos rigurosos a la geometría algebraica clásica y además ha dado muchos frutos en la teoría de números moderna.

Los ejercicios que aparecen en el texto son obligatorios. La nota final del curso corresponderá al porcentaje de los ejercicios entregados.

Índice

0 Algunas nociones preliminares

Antes de llegar a los resultados nuevos e interesantes, necesitamos revisar ciertas nociones básicas de álgebra, más que todo para fijar la terminología y notación. Para más detalles el lector puede consultar cualquier libro de texto de álgebra. También usaré el lenguaje categórico, para el cual se pueden revisar mis apuntes http://cadadr.org/san-salvador/2018-06-categorias/categorias.pdf

0.1 Anillos e ideales

En este curso todos los **anillos** serán conmutativos con identidad. Por la definición, se supone que un **homomorfismo** de anillos $f\colon R \to S$ preserva la identidad: $f(1_R) = 1_S$.

0.1. Definición. Para dos anillos R y S su **producto directo** es el producto cartesiano

$$R \times S := \{(r, s) \mid r \in R, s \in S\}$$

respecto a las operaciones

$$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2), \quad (r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2, s_1 s_2).$$

Se ve que $R \times S$ junto con las proyecciones a R y S es efectivamente *el producto* de R y S en la categoría de anillos conmutativos.

0.2. Definición. Se dice que $u \in R$ es una **unidad** (o un elemento **invertible**) si existe $u^{-1} \in R^\times$ tal que $uu^{-1} = 1$ (note que en este caso u^{-1} es necesariamente único). Las unidades forman un grupo respecto a la multiplicación que se denota por $R^\times$.

0.3. Definición. Un **cuerpo** es un anillo donde $1 \neq 0$ y todo elemento no nulo es invertible.

0.4. Definición. Si $xy = 0$ en R para algunos elementos x e y, entonces se dice que x e y son **divisores de cero**. En particular, si $x^n = 0$ para algún $n = 1, 2, 3, 4, \ldots$, se dice que x es un **nilpotente**.

Un anillo no nulo sin divisores de cero no nulos se llama un **dominio de integridad**, o simplemente un **dominio**.

Si $1 = 0$, entonces los axiomas de anillos implican que $R = \{0\}$. Es un anillo legítimo, llamado el **anillo nulo**, pero este no se considera como un dominio ni como un cuerpo.

0.5. Definición. Un **ideal** $\mathfrak{a} \subseteq R$ es un subgrupo abeliano que además está cerrado respecto a la multiplicación por los elementos de R: si $x \in \mathfrak{a}$ y $r \in R$, entonces $rx \in \mathfrak{a}$.

Si $\mathfrak{a} \neq R$, se dice que $\mathfrak{a}$ es un ideal **propio**.

Note que si $\mathfrak{a}_i \subseteq R$ son ideales, entonces $\bigcap_i \mathfrak{a}_i$ es también un ideal.

Para un ideal $\mathfrak{a} \subseteq R$ se ve que sobre las clases laterales $R/\mathfrak{a}$ se puede definir el producto

$$(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) := (xy + \mathfrak{a}).$$

De esta manera $R/\mathfrak{a}$ se vuelve un anillo, llamado el **anillo cociente** de R por $\mathfrak{a}$. La proyección canónica $R \to R/\mathfrak{a}$ es un homomorfismo de anillos. Para un homomorfismo $f\colon R \to S$ el **núcleo**

$$\ker f := \{r \in R \mid f(r) = 0\}$$

es un ideal en R y hay un isomorfismo canónico

$$R/\ker f \cong \operatorname{im} f := \{f(r) \mid r \in R\}$$

que se conoce como el **primer teorema de isomorfía**.

0.6. Definición. Para un subconjunto $S \subseteq R$ el ideal **generado** por S es el mínimo entre los ideales $\mathfrak{a} \subseteq R$ tales que $\mathfrak{a} \supseteq S$. Este ideal se denota por (S).

Se ve que los elementos de (S) son precisamente las combinaciones R-lineales de los elementos de S:

$$(S) = \left\{ \sum_i r_i s_i \;\middle|\; r_i \in R,\ s_i \in S \right\}.$$

0.7. Definición. Si un ideal $\mathfrak{a} \subseteq R$ puede ser generado por un elemento (se tiene $\mathfrak{a} = (x)$ para algún $x \in R$), entonces se dice que $\mathfrak{a}$ es un **ideal principal**. Un dominio donde todos los ideales son principales se llama un **dominio de ideales principales**.

0.8. Ejemplo. $\mathbb{Z}$ y $k[X]$ son dominios de ideales principales. La razón detrás de esto es el algoritmo de Euclides. Para un ideal no nulo $\mathfrak{a} \subseteq \mathbb{Z}$, sea x el mínimo entero positivo tal que $x \in \mathfrak{a}$. Luego, para $y \in \mathfrak{a}$ la división con resto nos da $y = qx + r$, donde $q, r \in \mathbb{Z}$ y $0 \le |r| < x$. Pero $r = y - qx \in \mathfrak{a}$, y por lo tanto $r = 0$ por nuestra elección de x. Esto significa que todo elemento de $\mathfrak{a}$ es divisible por x, y luego $\mathfrak{a} = (x)$. En el caso del anillo de polinomios, la prueba es idéntica: para un ideal $\mathfrak{a} \subseteq k[X]$ hay que considerar un polinomio no nulo f de mínimo grado posible tal que $f \in k[X]$. Luego, $\mathfrak{a} = (f)$. ▲

0.9. Definición. Un ideal $\mathfrak{p} \subset R$ es **primo** si se cumplen las siguientes condiciones:

1) $\mathfrak{p} \neq R$,
2) si $xy \in \mathfrak{p}$ para algunos $x, y \in R$, entonces $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$.

0.10. Definición. Para dos ideales $\mathfrak{a}, \mathfrak{b} \subseteq R$ por $\mathfrak{ab}$ se denota el ideal generado por los productos ab donde $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$. Para $n = 1, 2, 3, 4, \ldots$ el ideal $\mathfrak{a}^n$ se define como el producto $\underbrace{\mathfrak{a} \cdots \mathfrak{a}}_{n}$; es decir, es el ideal generado por $a_1 \cdots a_n$ donde $a_i \in \mathfrak{a}$.

Ejercicio 1. Demuestre que R es un cuerpo si y solamente si el único ideal propio de R es (0).

Ejercicio 2. Sea $\mathfrak{p} \subset R$ un ideal primo.

1) Demuestre que si $\mathfrak{ab} \subseteq \mathfrak{p}$, entonces $\mathfrak{a} \subseteq \mathfrak{p}$ o $\mathfrak{b} \subseteq \mathfrak{p}$.
2) Demuestre que si $\mathfrak{a}^n \subseteq \mathfrak{p}$, entonces $\mathfrak{a} \subseteq \mathfrak{p}$.

0.11. Definición. Un ideal $\mathfrak{m} \subset R$ es **maximal** si se cumplen las siguientes condiciones:

1) $\mathfrak{m} \neq R$,
2) si $\mathfrak{m} \subseteq \mathfrak{a}$ para algún ideal propio $\mathfrak{a} \subsetneq R$, entonces $\mathfrak{a} = \mathfrak{m}$.

Ejercicio 3. Sea $f\colon R \to S$ un homomorfismo de anillos.

1) Demuestre que para todo ideal $\mathfrak{a} \subseteq S$ su preimagen $f^{-1}(\mathfrak{a}) \subseteq R$ es también un ideal.
2) Demuestre que para todo ideal primo $\mathfrak{p} \subset S$ su preimagen $f^{-1}(\mathfrak{p}) \subset R$ es un ideal primo.
3) Demuestre que para un ideal maximal $\mathfrak{m} \subset S$ su preimagen $f^{-1}(\mathfrak{m}) \subset R$ no tiene por qué ser es un ideal maximal (encuentre un contraejemplo).

Ejercicio 4. Deduzca del **lema de Zorn**[*] que todo ideal propio $\mathfrak{a} \subsetneq R$ está contenido en algún ideal maximal. En particular, todo anillo no nulo posee un ideal maximal.
(No me gustaría revisar la teoría de conjuntos; véase por ejemplo el primer capítulo de Atiyah–Macdonald.)

[*] Max Zorn (1906–1993), matemático y lógico alemán.

0.12. Definición. Si R es un anillo que posee solo un ideal maximal, se dice que R es un **anillo local**.

Todo cuerpo es un anillo local: el único ideal propio en este caso es (0). Hay muchos ejemplos más interesantes y no tan triviales, pero los veremos más adelante. Un ejemplo conocido: el anillo de enteros p-ádicos $\mathbb{Z}_p$ es un anillo local: su único ideal maximal es el ideal generado por p.

Ejercicio 5. A partir de nuestras definiciones, deduzca la siguiente caracterización de ideales primos y maximales.

1) Un ideal $\mathfrak{p} \subset R$ es primo si y solamente si $R/\mathfrak{p}$ es un dominio.
2) Un ideal $\mathfrak{m} \subset R$ es maximal si y solamente si $R/\mathfrak{m}$ es un cuerpo.

En particular, todo ideal maximal es primo.

0.13. Definición. El conjunto de los ideales primos de R se llama el **espectro** de R y se denota por

$$\operatorname{Spec} R := \{\mathfrak{p} \subset R \mid \mathfrak{p} \text{ primo}\}.$$

El conjunto de los ideales maximales se llama el **espectro maximal**:

$$\operatorname{Specm} R := \{\mathfrak{m} \subset R \mid \mathfrak{m} \text{ maximal}\}.$$

Ejercicio 6. Sea R un anillo y $\mathfrak{a}$ un ideal.

1) Demuestre que hay una biyección natural entre los ideales $\mathfrak{b} \subset R$ tales que $\mathfrak{a} \subseteq \mathfrak{b}$ y los ideales $\overline{\mathfrak{b}} \subseteq R/\mathfrak{a}$, dada por $\overline{\mathfrak{b}} := \mathfrak{b}/\mathfrak{a}$.
2) Demuestre que esta biyección preserva inclusiones, intersecciones, sumas de ideales.
   (Basta probar la preservación de inclusiones; luego, note que $\bigcap_i \mathfrak{b}_i$ es el ideal maximal contenido en los $\mathfrak{b}_i$ y $\sum_i \mathfrak{b}_i$ es el ideal mínimo que contiene a todos los $\mathfrak{b}_i$.)
3) Demuestre que esta biyección se restringe a una biyección entre los ideales primos

   $$\operatorname{Spec} R/\mathfrak{a} \cong \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq \mathfrak{a}\}$$

   y entre los ideales maximales

   $$\operatorname{Specm} R/\mathfrak{a} \cong \{\mathfrak{m} \in \operatorname{Specm} R \mid \mathfrak{m} \supseteq \mathfrak{a}\}.$$

Ejercicio 7 (Topología de Zariski[*])**.** Sea R un anillo. Para un subconjunto $S \subset R$ definamos

$$V(S) := \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq S\}.$$

1) Demuestre que $V(S) = V(\mathfrak{a})$ donde $\mathfrak{a} = (S)$.
2) Demuestre que los conjuntos $V(S)$ satisfacen los axiomas de conjuntos *cerrados* de una topología. Específicamente,

   $$V(0) = \operatorname{Spec} R, \quad V(1) = \emptyset;$$

   para las uniones *finitas* se tiene

   $$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}),$$

   mientras que para las intersecciones *arbitrarias*

   $$\bigcap_i V(\mathfrak{a}_i) = V(\sum_i \mathfrak{a}_i).$$

[*] Oscar Zariski (1899–1986), geómetra algebraico de origen polaco.

La topología sobre $\operatorname{Spec} R$ definida por los conjuntos cerrados $V(S)$ se llama la **topología de Zariski**.

3) Demuestre que la topología de Zariski no suele ser Hausdorff. Considere, por ejemplo, el caso de $R = k[X]$ donde k es un cuerpo algebraicamente cerrado.

4) Para $f \in R$ definamos
$$U(f) := \{\mathfrak{p} \in \operatorname{Spec} R \mid f \notin \mathfrak{p}\}.$$
Demuestre que estos conjuntos forman una base de la topología de Zariski.

5) Demuestre que $\operatorname{Spec} R = \bigcup_i U(f_i)$ para una familia finita de elementos $f_i \in R$ si y solamente si $(f_i) = R$.

6) Demuestre que $\operatorname{Spec} R$ es **casi-compacto** (todo recubrimiento abierto posee un subrecubrimiento finito).

7) Demuestre que todo homomorfismo de anillos $\phi\colon R \to S$ induce una aplicación *continua*
$$\operatorname{Spec} S \to \operatorname{Spec} R,$$
$$\mathfrak{p} \to \phi^{-1}(\mathfrak{p}).$$

8) Describa los puntos del espacio $\operatorname{Spec} \mathbb{Z}$. ¿Cuáles puntos son cerrados (satisfacen $\overline{\{\mathfrak{p}\}} = \{\mathfrak{p}\}$)? Calcule la cerradura de los puntos abiertos.

Para más resultados sobre el espectro, también se pueden hacer los ejercicios 1.15–1.26 de Atiyah–Macdonald.

0.14. Definición. Se dice que un elemento $p \in R$ es **primo** si el ideal generado por p es primo. Esto es equivalente a pedir que

1) $p \notin R^\times$,

2) si $p \mid xy$, entonces $p \mid x$ o $p \mid y$.

Se dice que $r \in R$ es **irreducible** si

1) $r \notin R^\times$,

2) si $r \mid st$, entonces $s \in R^\times$ o $t \in R^\times$.

0.15. Definición. Se dice que un R es **anillo factorial** (o un **dominio de factorización única**) si R es un dominio y todo elemento no nulo de R se factoriza de modo único en un producto de elementos irreducibles, salvo permutación de los múltiplos y multiplicación por las unidades.

0.16. Ejemplo. El anillo de los enteros $\mathbb{Z}$ es factorial: para todo entero no nulo se tiene
$$n = \pm \prod_p p^{v_p(n)}.$$

En general, todo dominio de ideales principales es factorial.

Si R es un anillo factorial, entonces el anillo de polinomios $R[X_1, \ldots, X_n]$ es también factorial. Este resultado es esencialmente lo que se conoce como el **lema de Gauss**. ▲

0.17. Definición. Para dos ideales $\mathfrak{a}, \mathfrak{b} \subseteq R$ el **ideal cociente** correspondiente viene dado por
$$(\mathfrak{a} : \mathfrak{b}) := \{x \in R \mid x\mathfrak{b} \subseteq \mathfrak{a}\}.$$
Este es un ideal. En particular, para $\mathfrak{a} = 0$ el ideal
$$\operatorname{Ann} \mathfrak{b} := (0 : \mathfrak{b}) := \{x \in R \mid x\mathfrak{b} = 0\}$$
se llama el **aniquilador** de $\mathfrak{b}$.

0.2 Módulos

0.18. Definición. Un R-módulo M es un grupo abeliano dotado de una acción de R

$$R \times M \to M,$$
$$(r, m) \mapsto r \cdot m$$

que satisface los siguientes axiomas:

$$r \cdot (s \cdot m) = (rs) \cdot m,$$
$$r \cdot (m + n) = r \cdot m + r \cdot n,$$
$$(r + s) \cdot m = r \cdot m + s \cdot m,$$
$$1 \cdot m = m$$

para cualesquiera $r, s \in R$, $m, n \in M$.

Un **submódulo** $N \subseteq M$ es un subgrupo abeliano tal que la acción de R sobre M se restringe a N.

Una **aplicación R-lineal** (o un homomorfismo de R-módulos) $f\colon M \to N$ es un homomorfismo de grupos abelianos que es compatible con las acciones de R; es decir, satisface $f(r \cdot m) = r \cdot f(m)$ para cualesquiera $r \in R$, $m \in M$.

Si $N \subseteq M$ es un submódulo, entonces el cociente de grupos abelianos M/N es también un R-módulo respecto a la acción

$$r \cdot (m + N) := (r \cdot m) + N.$$

La proyección canónica $M \twoheadrightarrow M/N$ es evidentemente R-lineal. Para toda aplicación R-lineal $f\colon M \to N$ tenemos un isomorfismo canónico

$$M/\ker f \cong \operatorname{im} f$$

(esto es el **primer teorema de isomorfía** para R-módulos). Aquí $\ker f$ es el **núcleo** de f que es el submódulo de M dado por

$$\ker f := \{m \in M \mid f(m) = 0\}.$$

El papel dual juega el **conúcleo** que se define por

$$\operatorname{coker} f := N/\operatorname{im} f.$$

0.19. Ejemplo. Notamos que un R-submódulo de R es la misma cosa que un ideal $\mathfrak{a} \subseteq R$. El anillo cociente $R/\mathfrak{a}$ es también un R-módulo. La proyección canónica $R \to R/\mathfrak{a}$ es una aplicación R-lineal. ▲

0.20. Definición. Para un R-módulo M el **aniquilador** es el ideal

$$\operatorname{Ann} M := \{r \in R \mid r \cdot M = 0\}.$$

Por ejemplo, $\operatorname{Ann}(R/\mathfrak{a}) = \mathfrak{a}$. De la misma manera, para un elemento $m \in M$ se define

$$\operatorname{Ann} m := \{r \in R \mid r \cdot m = 0\}.$$

0.21. Definición. Para dos R-módulos M y N su **suma directa** es su suma directa como grupos abelianos

$$M \oplus N := \{(m, n) \mid m \in M, n \in N\}$$

con la acción de R definida por

$$r \cdot (m, n) := (r \cdot m, r \cdot n).$$

La suma directa $M \oplus N$ es a la vez el producto y el coproducto de M y N en la categoría de R-módulos. Para una familia infinita de R-módulos la **suma directa** se define como

$$\bigoplus_i M_i := \{(m_i) \mid m_i \in M_i, m_i = 0, \text{ salvo un número finito de los } i\}$$
$$= \{\text{sumas formales finitas } \sum_i m_i \mid m_i \in M_i\},$$

mientras que el **producto directo** viene dado por

$$\prod_i M_i := \{(m_i) \mid m_i \in M_i\}.$$

El producto directo $\prod_i M_i$ es el producto de los M_i en la categoría de R-módulos, y la suma directa $\bigoplus_i M_i$ es el coproducto. Notamos que $\bigoplus_i M_i$ es un submódulo de $\prod_i M_i$.

0.22. Definición. Se dice que una sucesión de aplicaciones R-lineales

$$\cdots \to M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \to \cdots$$

es **exacta en** M_i si $\operatorname{im} f_{i+1} = \ker f_i$. Se dice que es **exacta** si es exacta en M_i para todo i. En particular, una sucesión exacta de la forma

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

se llama una **sucesión exacta corta**. Su exactitud significa que

1) i es un monomorfismo,
2) p es un epimorfismo,
3) $\operatorname{im} i = \ker p$.

0.23. Ejemplo. Para toda aplicación R-lineal $f\colon M \to N$ se tiene una sucesión exacta

$$0 \to \ker f \to M \xrightarrow{f} N \to \operatorname{coker} f \to 0$$

▲

0.24. Ejemplo. Sea M un R-módulo y M_1, M_2 sus submódulos. Entonces, la sucesión

$$0 \to M_1 \cap M_2 \xrightarrow{m \mapsto (m,m)} M_1 \oplus M_2 \xrightarrow{(m_1,m_2) \mapsto m_1 - m_2} M_1 + M_2 \to 0$$

es exacta. Aquí $M_1 + M_2$ es el submódulo generado por M_1 y M_2 (el mínimo submódulo que contiene a M_1 y M_2). ▲

0.25. Ejemplo. Sea $\mathfrak{a} \subset R$ un ideal y sea $x \in R$ un elemento. Entonces, la sucesión

$$0 \to R/(\mathfrak{a} : x) \xrightarrow{\times x} R/\mathfrak{a} \to R/(\mathfrak{a} + (x)) \to 0$$

es exacta. Aquí

$$(\mathfrak{a} : x) := \{r \in R \mid r \cdot (x) \subseteq \mathfrak{a}\} \supseteq \mathfrak{a}.$$

▲

Ejercicio 8. Para una sucesión exacta corta

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

las siguientes condiciones son equivalentes.

1) Existe una aplicación R-lineal $r\colon M \to M'$ tal que $r \circ i = \mathrm{id}_{M'}$.

2) Existe una aplicación R-lineal $s\colon M'' \to M$ tal que $p \circ s = \mathrm{id}_{M''}$.

3) Existe una aplicación R-lineal $f\colon M' \oplus M'' \to M$ que hace parte del diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{m' \mapsto (m',0)} & M' \oplus M'' & \xrightarrow{(m',m'') \mapsto m''} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \end{array}$$

Además, todo f que hace parte de un diagrama conmutativo con filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & N & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

es automáticamente un isomorfismo (véase el ejercicio 10).

Cuando se cumple una de las condiciones equivalentes 1)–3), se dice que la sucesión exacta corta **se escinde**, o que es **escindida**[*].

0.26. Definición. Para un conjunto I el R-módulo libre **generado** por los elementos de I es un módulo R^I junto con una inclusión $I \hookrightarrow R^I$ caracterizado por la siguiente propiedad universal: si M es un R-módulo, entonces toda aplicación de conjuntos $I \to M$ se extiende de modo único a una aplicación R-lineal $R^I \to M$.

$$\begin{array}{ccc} I & \longrightarrow & M \\ \downarrow & \overset{\exists!}{\nearrow} & \\ R^I & & \end{array}$$

Si $M \cong R^I$ para algún I, se dice que M es un **módulo libre de rango** $|I|$.

La construcción de R^I es la siguiente: hay que tomar la suma directa de copias de R indexada por los elementos de I:

$$R^I = \bigoplus_{i \in I} R.$$

En este caso la aplicación $I \hookrightarrow R^I$ asocia a $i \in I$ el elemento $e_i := (0,\dots,1,\dots,0)$ donde 1 está en la i-ésima posición.

El rango de un módulo libre sobre cualquier anillo conmutativo está bien definido: $R^I \cong R^J$ implica $|I| = |J|$. Si $R = k$ es un cuerpo, entonces todo R-módulo V es un espacio vectorial sobre k y en los cursos de álgebra lineal se demuestra que V posee una base[**]; es decir, que es siempre libre. El rango en este caso es la dimensión. Sobre un anillo que no es un cuerpo, hay módulos que no son libres (no poseen una base). Sin embargo, hay la siguiente noción de finitud muy útil.

0.27. Definición. Para un R-módulo M se dice que algunos elementos $m_i \in M$ **generan** a M si todo elemento de M puede ser expresado como una combinación R-lineal $\sum_{i \in I} r_i\, m_i$; en otras palabras, si la aplicación

$$\begin{aligned} f\colon R^I &\to M, \\ e_i &\mapsto m_i \end{aligned}$$

[*] *split* en inglés.

[**] Por cierto, esto también se demuestra mediante el lema de Zorn, así que haga el ejercicio 4.

es sobreyectiva. Si M posee un número finito de generadores, entonces se dice que M es **finitamente generado**. Si $\ker f$ es también finitamente generado; es decir, si existe un número finito de elementos $n_j \in \ker f$ y hay un epimorfismo

$$\begin{aligned} g\colon R^J &\to \ker f, \\ e_j &\mapsto n_j, \end{aligned}$$

entonces se dice que M es un módulo **finitamente presentado**. Esto significa que existe una sucesión exacta

$$R^J \xrightarrow{g} R^I \xrightarrow{f} M \to 0$$

donde I y J son finitos.

0.3 El lema de la serpiente y sus consecuencias

Vamos a necesitar los siguientes resultados básicos del álgebra homológica. Recomiendo que el lector haga estos ejercicios porque estos serán útiles en la clase de topología algebraica.

Ejercicio 9 (El lema de la serpiente)**.** Supongamos que hay un diagrama conmutativo de aplicaciones R-lineales con filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{p'} & C' & \longrightarrow & 0 \end{array}$$

Demuestre que hay una aplicación natural R-lineal $\delta\colon \ker h \to \operatorname{coker} f$ que hace parte de una sucesión exacta

$$0 \to \ker f \to \ker g \to \ker h \xrightarrow{\delta} \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h \to 0$$

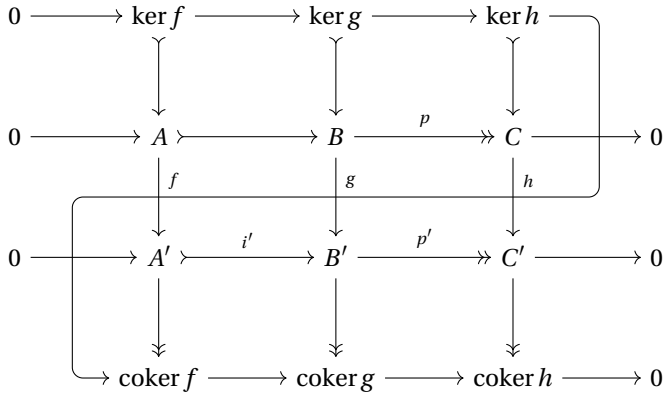
Aquí las aplicaciones $\ker f \to \ker g \to \ker h$ están inducidas por las aplicaciones $A \to B \to C$ y las aplicaciones $\operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h$ están inducidas por $A' \to B' \to C'$. Lo más interesante es construir δ. Para $c \in \ker h$, ya que $p\colon B \to C$ es una aplicación sobreyectiva, existe $b \in B$ tal que $p(b) = c$. Luego, tenemos $g(b) \in \ker p' = \operatorname{im} i'$, así que existe un elemento único $a' \in A'$ tal que $i'(a') = g(b)$. Sea $\delta(c)$ la imagen de a' en $\operatorname{coker} f$.

1) Demuestre que $\delta(c) \in \operatorname{coker} f$ está definido de modo único por la descripción de arriba.

2) Demuestre que δ es una aplicación R-lineal.

3) Demuestre que la sucesión con ker y coker de arriba es exacta.

Este resultado se conoce como el **lema de la serpiente** porque la aplicación δ puede ser dibujada de la siguiente manera:



Ejercicio 10 (El lema del tres)**.** Consideremos un diagrama conmutativo de aplicaciones R-lineales con filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

Demuestre que

1) si f y h son mono, entonces g es también mono,
2) si f y h son epi, entonces g es también epi,
3) si f y h son iso, entonces g es también iso,

(use el lema de la serpiente).

Ejercicio 11 (El lema del cinco)**.** Consideremos un diagrama conmutativo de aplicaciones R-lineales con filas exactas

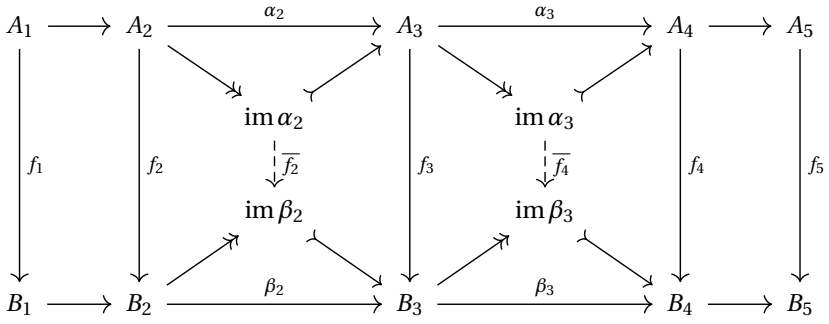
$$\begin{array}{ccccccccc} A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & A_4 & \longrightarrow & A_5 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & B_4 & \longrightarrow & B_5 \end{array}$$

Demuestre que

1) Si f_2 y f_4 son mono y f_1 es epi, entonces f_3 es mono,
2) Si f_2 y f_4 son epi y f_5 es mono, entonces f_3 es epi,
3) Si f_1 es epi, f_5 es mono y f_2, f_4 son iso, entonces f_3 es iso.

Sugerencia: se pueden factorizar las "factorizaciones epi-mono" de las aplicaciones

$$\alpha_2 \colon A_2 \to A_3,\ \alpha_3 \colon A_3 \to A_4,\ \beta_2 \colon B_2 \to B_3,\ \beta_3 \colon B_3 \to B_4$$



Luego, demuestre que

a) si f_4 es mono, entonces $\overline{f_4}$ es mono,
b) si f_2 es epi, entonces $\overline{f_2}$ es epi,
c) si f_2 es mono y f_1 es epi, entonces $\overline{f_2}$ es mono,
d) si f_4 es epi y f_5 es mono, entonces $\overline{f_4}$ es epi

y usando a)–d) aplique el lema del tres al diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{im}\alpha_2 & \longrightarrow & A_3 & \longrightarrow & \operatorname{im}\alpha_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \overline{f_2}} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle \overline{f_4}} & & \\ 0 & \longrightarrow & \operatorname{im}\beta_2 & \longrightarrow & B_3 & \longrightarrow & \operatorname{im}\beta_3 & \longrightarrow & 0 \end{array}$$

0.4 Álgebras

0.28. Definición. Si R y A son anillos, se dice que A está dotado de una estructura de R-**álgebra** si está especificado un homomorfismo $\alpha\colon R \to A$.

En este caso normalmente R se identifica con su imagen en A y en lugar de $f(r)\cdot a$ se escribe $r\cdot a$. También para un ideal $\mathfrak{a} \subseteq A$ es común escribir $R \cap \mathfrak{a}$ en lugar de $\alpha^{-1}(\mathfrak{a})$.

Un **homomorfismo** de R-álgebras es un homomorfismo de anillos $f\colon A \to B$ que respecta las estructuras de R-álgebras: $f(r\cdot a) = r\cdot f(a)$.

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ & {\scriptstyle\alpha}\nwarrow \quad \nearrow{\scriptstyle\beta} & \\ & R & \end{array}$$

0.29. Ejemplo. Todo anillo R tiene una estructura única de $\mathbb{Z}$-álgebra: existe un homomorfismo único[*] $\mathbb{Z} \to R$. En otras palabras, $\mathbb{Z}$ es un objeto inicial en la categoría de anillos. ▲

0.30. Ejemplo. El anillo de polinomios $R[X_1,\dots,X_n]$ es una R-álgebra: la inclusión de R como los polinomios constantes es un homomorfismo $R \to R[X_1,\dots,X_n]$. ▲

0.31. Definición. Se dice que una R-álgebra A es **finitamente generada** si existe un número finito de elementos $x_1,\dots,x_n \in A$ tales que todo elemento de A se obtiene como un polinomio en x_i con coeficientes en R; es decir, si existe un homomorfismo sobreyectivo

$$\begin{aligned} R[X_1,\dots,X_n] &\to A, \\ X_i &\mapsto x_i. \end{aligned}$$

En este caso también se escribe $A = R[x_1,\dots,x_n]$.

Cuidado con la terminología: $R[X_1,\dots,X_n]$ es una *R-álgebra finitamente generada*, pero no es un *R-módulo finitamente generado*.

0.5 Anillos y módulos noetherianos

0.32. Definición. Un anillo R es **noetheriano**[**] si se cumple una de las siguientes condiciones equivalentes.

1) Todo ideal $\mathfrak{a} \subseteq R$ es finitamente generado.

2) Toda cadena ascendente de ideales en R

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq R$$

se estabiliza; es decir, $\mathfrak{a}_i = \mathfrak{a}_{i+1}$ para $i \gg 0$.

[*] Recuerde que por nuestra convención un homomorfismo de anillos aplica 1 en 1.

[**] Emmy Noether (1882–1935), matemática alemana.

En efecto, dado un ideal $\mathfrak{a}$ que no es finitamente generado, se puede encontrar una cadena creciente de ideales

$$(x_0) \subsetneq (x_0, x_1) \subsetneq (x_0, x_1, x_2) \subsetneq \cdots$$

que no se estabiliza (sea $x_0 := 0$, y luego por inducción, ya que $(x_0, x_1, \ldots, x_n) \subsetneq \mathfrak{a}$, podemos escoger $x_{n+1} \in \mathfrak{a} \setminus (x_1, \ldots, x_n)$). En la otra dirección, supongamos que todo ideal en R es finitamente generado. Sea

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq R$$

una cadena ascendente de ideales. Entonces, la unión

$$\mathfrak{a} := \bigcup_{i \geq 0} \mathfrak{a}_i$$

es también un ideal y $\mathfrak{a} = (x_0, x_1, \ldots, x_n)$ para algunos $x_0, x_1, \ldots, x_n \in R$. Pero cada uno de estos elementos pertenece a algún ideal de la cadena, así que $\{x_0, x_1, \ldots, x_n\} \subset \mathfrak{a}_i$ para algún índice i suficientemente grande. Luego, $\mathfrak{a}_i = (x_0, x_1, \ldots, x_n)$ y

$$\mathfrak{a}_i = \mathfrak{a}_{i+1} = \mathfrak{a}_{i+2} = \cdots$$

0.33. Ejemplo. Todo cuerpo es un anillo noetheriano: en este caso el único ideal propio es (0). Todo dominio de ideales principales, por ejemplo $\mathbb{Z}$, es noetheriano: en este caso los ideales no son solamente finitamente generados, sino siempre tienen un generador. ▲

Muchos ejemplos importantes de anillos noetherianos surgen del siguiente resultado.

0.34. Proposición (Teorema de la base de Hilbert). *Si R es un anillo noetheriano, entonces el anillo de polinomios $R[X]$ es también noetheriano.*

Demostración. Consideremos una cadena ascendente de ideales

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq R[X].$$

Necesitamos ver que esta se estabiliza.

Sea $\mathfrak{a}_{i,d}$ el ideal de los elementos de R que aparecen como los coeficientes mayores de los polinomios de grado d en $\mathfrak{a}_i$. Tenemos

$$\mathfrak{a}_{i,d} \subseteq \mathfrak{a}_{i',d'} \quad \text{si } i \leq i' \text{ y } d \leq d'.$$

Entre los $\mathfrak{a}_{i,d}$ hay un número finito de ideales distintos. Supongamos lo contrario. En este caso una familia infinita de ideales distintos corresponde a un subconjunto infinito de los índices dobles $(i, d) \in \mathbb{N} \times \mathbb{N}$ y entre ellos se puede escoger una cadena infinita (i_k, d_k) con

$$i_0 \leq i_1 \leq i_2 \leq \cdots, \quad d_0 \leq d_1 \leq d_2 \leq \cdots$$

De aquí se obtiene una cadena ascendente

$$\mathfrak{a}_{i_0,d_0} \subsetneq \mathfrak{a}_{i_1,d_1} \subsetneq \mathfrak{a}_{i_2,d_2} \subsetneq \cdots \subsetneq R$$

pero esto contradice nuestra hipótesis que R es noetheriano.

Entonces, existe un índice i tal que

$$\mathfrak{a}_{i,d} = \mathfrak{a}_{i+1,d} = \mathfrak{a}_{i+2,d} = \cdots$$

para todo d.

Supongamos que $f \in \mathfrak{a}_{i'}$ para $i' \geq i$. Veamos por inducción sobre $d = \deg f$ que $f \in \mathfrak{a}_i$. Como la base de inducción se puede considerar el caso de $d = -\infty$; es decir, $f = 0$. Para el paso inductivo, por lo que hemos demostrado, existe un polinomio $g \in \mathfrak{a}_i$ que tiene el mismo coeficiente mayor que f y el mismo grado d. Luego, $\deg(f - g) < d$ y por la hipótesis de inducción $f - g \in \mathfrak{a}_i$, así que $f \in \mathfrak{a}_i$. ■

0.35. Corolario. *Si R es un anillo noetheriano, entonces para todo n el anillo de polinomios $R[X_1,\dots,X_n]$ es también noetheriano.*

Demostración. Inducción sobre n: el caso base es $n=0$ y el paso inductivo es 0.34 junto con el isomorfismo $R[X_1,\dots,X_n] \cong R[X_1,\dots,X_{n-1}][X_n]$. ■

0.36. Proposición. *Supongamos que R es un anillo noetheriano.*

1) *Para todo ideal $\mathfrak{a} \subseteq R$ el anillo cociente $R/\mathfrak{a}$ es también noetheriano.*
2) *Para todo homomorfismo $f\colon R \to S$ el anillo $\operatorname{im} f$ es noetheriano*[*].

Demostración. Las propiedades 1) y 2) son equivalentes: para un homomorfismo $f\colon R \to S$ se tiene el teorema de isomorfía $\operatorname{im} f \cong R/\ker f$.

Consideremos la proyección canónica al anillo cociente $f\colon R \to R/\mathfrak{a}$. Si $\mathfrak{b}$ es un ideal en $R/\mathfrak{a}$, entonces el ideal $f^{-1}(\mathfrak{b}) \subseteq R$ es finitamente generado, ya que R es noetheriano. Tenemos $f^{-1}(\mathfrak{b}) = (x_1,\dots,x_n)$ para algunos $x_1,\dots,x_n \in R$. Luego, $\mathfrak{b} = (f(x_1),\dots,f(x_n))$. ■

0.37. Corolario. *Si R es un anillo noetheriano y A es una R-álgebra finitamente generada, entonces A es también un anillo noetheriano.*

Demostración. Por la definición, A es una R-álgebra finitamente generada si hay un homomorfismo sobreyectivo $R[X_1,\dots,X_n] \to A$. Podemos aplicar 0.35 y 0.36 ■

Ejercicio 12. Un subanillo de un anillo noetheriano no tiene por qué ser noetheriano. Encuentre algún contraejemplo.

También tenemos una noción más general de *módulo* noetheriano.

0.38. Definición. Un R-módulo M es **noetheriano** si se cumple una de las siguientes condiciones equivalentes.

1) Todo submódulo $N \subseteq M$ es finitamente generado.
2) Toda cadena ascendente de submódulos de M

$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq M$$

se estabiliza; es decir, $N_i = N_{i+1}$ para $i \gg 0$.

Notamos que esto generaliza la noción del anillo noetheriano: R es noetheriano si es noetheriano como R-módulo.

0.39. Proposición. *Si R es un anillo noetheriano y M es un R-módulo finitamente generado, entonces M es noetheriano.*

Demostración. Sean $m_1\dots,m_r$ generadores de M y sea N un submódulo de M. Necesitamos probar que N es finitamente generado. Procedamos por inducción sobre r. Si $r=1$, tenemos una aplicación R-lineal sobreyectiva

$$\begin{aligned} p\colon R &\twoheadrightarrow M, \\ 1 &\mapsto m_1. \end{aligned}$$

Luego, $p^{-1}(N) \subseteq R$ es un ideal finitamente generado, ya que R es noetheriano. Tenemos $p^{-1}(N) = (x_1,\dots,x_n)$ para algunos $x_1,\dots,x_n \in R$ y luego $p(x_1),\dots,p(x_n)$ son generadores de N.

[*] En palabras: *toda imagen homomorfa de un anillo noetheriano es también noetheriana*.

Supongamos ahora que $r > 1$. Pasemos al cociente de M por el submódulo generado por m_1:

$$p\colon M \twoheadrightarrow M/Rm_1.$$

El módulo Rm_1 es noetheriano por el argumento de arriba. Luego, $N \cap Rm_1$, siendo un submódulo de Rm_1, es finitamente generado. Sean $n_1, \ldots, n_s \in N \cap Rm_1$ sus generadores.

El módulo M/Rm_1 tiene $p(m_2), \ldots, p(m_n)$ como sus generadores, y entonces es también noetheriano por la hipótesis de inducción. Se sigue que $\overline{N} := p(N) \subseteq M/Rm_1$ es finitamente generado. Sean $n_1', \ldots, n_t'$ elementos de N cuyas imágenes generan a $\overline{N}$. Esto significa que para todo elemento $n \in N$ se tiene

$$n - \sum_{1 \le i \le t} r_i' n_i' \in N \cap Rm_1$$

para algunos $r_i' \in R$. Luego,

$$n - \sum_{1 \le i \le t} r_i' n_i' = \sum_{1 \le j \le s} r_j n_j$$

para algunos $r_j \in R$. Se sigue que todo elemento de N es una combinación R-lineal de $n_1, \ldots, n_s, n_1', \ldots, n_t'$. ■

0.6 El Hom

0.40. Definición. Si M y N son dos R-módulos, entonces las aplicaciones R-lineales $M \to N$ forman un R-módulo $\mathrm{Hom}_R(M, N)$, donde la suma y la acción de R están definidas por

$$(f+g)(m) := f(m) + g(m), \quad (r \cdot f)(m) := r \cdot f(m) = f(r \cdot m).$$

Ejercicio 13. Calcule los siguientes grupos abelianos $\mathrm{Hom}_{\mathbb{Z}}(-,-)$.

1) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(m,n)\mathbb{Z}$, donde (m,n) denota el máximo común divisor de m y n.

2) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.

3) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}) \cong \mathbb{Q}$.

4) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$.

5) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Z}) = 0$.

$\mathrm{Hom}_R(-,-)$ es un funtor R-**Mód** $\to$ R-**Mód** en ambos argumentos. A saber, para M fijo, $\mathrm{Hom}_R(M,-)$ es un funtor covariante, y para N fijo $\mathrm{Hom}_R(-,N)$ es un funtor contravariante.

0.41. Observación. *Hay un isomorfismo natural de R-módulos*

$$\begin{aligned} \mathrm{Hom}_R(R, N) &\xrightarrow{\cong} N, \\ f &\mapsto f(1). \end{aligned}$$

0.42. Observación. *Hay isomorfismos naturales de R-módulos*

$$\mathrm{Hom}_R(M, \prod_i N_i) \cong \prod_i \mathrm{Hom}_R(M, N_i),$$
$$\mathrm{Hom}_R(\bigoplus_i M_i, N) \cong \prod_i \mathrm{Hom}_R(M_i, N).$$

Demostración. Esencialmente, esto es la propiedad universal del producto y coproducto. ■

Ejercicio 14. Sea

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

una sucesión exacta corta de R-módulos.

1) Demuestre que para un R-módulo fijo M la sucesión correspondiente

$$0 \to \mathrm{Hom}_R(M, A) \xrightarrow{i_*} \mathrm{Hom}_R(M, B) \xrightarrow{p_*} \mathrm{Hom}_R(M, C)$$

es exacta (sin "$\to 0$" a la derecha: la aplicación p_* no es necesariamente sobreyectiva).

2) Demuestre que para un R-módulo fijo N la sucesión correspondiente

$$0 \to \mathrm{Hom}_R(C, N) \xrightarrow{p^*} \mathrm{Hom}_R(B, N) \xrightarrow{i^*} \mathrm{Hom}_R(A, N)$$

es exacta (sin "$\to 0$" a la derecha).

Se dice que los funtores $\mathrm{Hom}_R(M, -)$ y $\mathrm{Hom}_R(-, N)$ son **exactos por la izquierda**.

Ejercicio 15. Consideremos la sucesión exacta corta de $\mathbb{Z}$-módulos (grupos abelianos)

$$0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

1) Demuestre que al aplicar el funtor covariante $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, -)$ se obtiene una sucesión

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$$

donde

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0 \quad \text{y} \quad \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$$

y entonces la aplicación $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ no es sobreyectiva.

2) Demuestre que al aplicar el funtor contravariante $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ se obtiene

$$0 \to \underbrace{\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})}_{=0} \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z}$$

donde la última aplicación no es sobreyectiva.

0.7 El producto tensorial

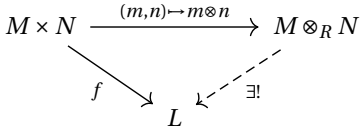
0.43. Definición. Sean M y N dos R-módulos. Entonces, el **producto tensorial** $M \otimes_R N$ es el R-módulo generado por los elementos $m \otimes n$ con $m \in M$ y $n \in N$ respecto a las relaciones[*]

$$\begin{aligned}(rm) \otimes n &= r\,(m \otimes n) = m \otimes (rn),\\ (m_1 + m_2) \otimes n &= m_1 \otimes n + m_2 \otimes n,\\ m \otimes (n_1 + n_2) &= m \otimes n_1 + m \otimes n_2.\end{aligned}$$

El significado de esta construcción es la siguiente propiedad universal.

[*] Es decir, se considera el R-módulo libre enorme generado por $m \otimes n$ y luego se toma su cociente por el submódulo generado por las relaciones.

0.44. Proposición. *Sean M, N, L tres R-módulos. Toda aplicación R-bilineal $f\colon M \times N \to L$ corresponde a una aplicación R-lineal única $M \otimes_R N \to L$ que hace conmutar el diagrama*



Ejercicio 16. Calcule los siguientes productos tensoriales de grupos abelianos.

1) $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/(m,n)\mathbb{Z}$, donde (m,n) denota el máximo común divisor de m y n.

2) $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

3) $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

4) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$.

5) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

6) $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

El producto tensorial es funtorial en ambos argumentos. Para un R-módulo fijo N una aplicación R-lineal $f\colon M \to M'$ induce una aplicación R-lineal

$$\begin{aligned} f \otimes \mathrm{id}\colon M \otimes_R N &\to M' \otimes_R N, \\ m \otimes n &\mapsto f(m) \otimes n. \end{aligned}$$

De la misma manera, para M fijo, una aplicación $g\colon N \to N'$ induce

$$\begin{aligned} \mathrm{id} \otimes g\colon M \otimes_R N &\to M \otimes_R N', \\ m \otimes n &\mapsto m \otimes g(n). \end{aligned}$$

Entonces, $M \otimes_R -$ y $- \otimes_R N$ son funtores covariantes R-**Mód** $\to$ R-**Mód**.

0.45. Comentario. Si M es un R-módulo y S es una R-álgebra, entonces $S \otimes_R M$ es un S-módulo: la acción de S se define por

$$s' \cdot (s \otimes m) := s's \otimes m.$$

En este caso el producto tensorial $S \otimes_R -$ es un funtor R-**Mód** $\to$ S-**Mód**.

0.46. Observación. *Hay isomorfismos naturales de R-módulos*

$$M \otimes_R N \cong N \otimes_R M, \quad (L \otimes_R M) \otimes_R N \cong L \otimes_R (M \otimes_R N).$$

Demostración. Use la propiedad universal del producto tensorial. ■

0.47. Observación. *Hay un isomorfismo natural*

$$\begin{aligned} R \otimes_R M &\xrightarrow{\cong} M, \\ r \otimes m &\mapsto r \cdot m. \end{aligned}$$

Ejercicio 17. Sea

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

una sucesión exacta corta de R-módulos. Demuestre que para un R-módulo fijo N la sucesión correspondiente

$$N \otimes_R M' \xrightarrow{\mathrm{id}\otimes i} N \otimes_R M \xrightarrow{\mathrm{id}\otimes p} N \otimes_R M'' \to 0$$

es exacta (sin "$0 \to$" a la izquierda: la aplicación $i \otimes \mathrm{id}$ no es necesariamente inyectiva).

Se dice que el funtor $N \otimes_R -$ es **exacto por la derecha**.

Ejercicio 18. Consideremos la sucesión exacta corta de $\mathbb{Z}$-módulos (grupos abelianos)

$$0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

Demuestre que al aplicar $- \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ se obtiene una sucesión

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/n\mathbb{Z} \to 0$$

donde el primer homomorfismo claramente no es inyectivo.

El producto tensorial y el Hom son funtores adjuntos.

0.48. Proposición. *Hay un isomorfismo natural de R-módulos*

$$\mathrm{Hom}_R(M \otimes_R N, L) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, L)).$$

Dejo los detalles al lector. La idea detrás de este isomorfismo es muy sencilla: dada una aplicación lineal $f\colon m\otimes n \mapsto f(m\otimes n)$, se puede considerar la aplicación $m \mapsto (n \mapsto f(m\otimes n))$. Viceversa, a partir de una aplicación $m \mapsto (f_m\colon N \to L)$ se define $m \otimes n \mapsto f_m(n)$.

0.49. Corolario. *El producto tensorial preserva sumas directas:*

$$\Big(\bigoplus_i M_i\Big) \otimes_R N \cong \bigoplus_i \Big(M_i \otimes_R N\Big).$$

Demostración. Todo adjunto por la izquierda preserva coproductos. ∎

0.50. Comentario. De hecho, la exactitud de Hom por la izquierda (ejercicio 14) y la exactitud de $\otimes$ por la derecha (ejercicio 17) son también consecuencias de la adjunción: todo funtor adjunto por la izquierda es exacto por la derecha y todo funtor adjunto por la derecha es exacto por la izquierda.

0.51. Proposición. *Si A y B son R-álgebras, entonces el producto tensorial $A \otimes_R B$ es una R-álgebra con la multiplicación definida por*

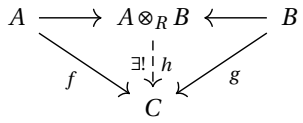
$$(a \otimes b) \cdot (a' \otimes b') := (aa') \otimes (bb').$$

Junto con los homomorfismos canónicos

$$\begin{array}{ccccc} A & \longrightarrow & A \otimes_R B & \longleftarrow & B \\ a & \longmapsto & a \otimes 1 & & \\ & & 1 \otimes b & \longmapsfrom & b \end{array}$$

esto es el coproducto de A y B en la categoría de R-álgebras.

Demostración. Los axiomas de álgebras conmutativas para $A \otimes_R B$ se verifican directamente. La propiedad universal del coproducto nos dice que para toda R-álgebra C y dos homomorfismos de R-álgebras $f\colon A \to C$ y $g\colon B \to C$ existe un homomorfismo único $h\colon A \otimes_R B \to C$ que hace conmutar el diagrama



En efecto, para que los dos triángulos conmuten, hay que poner

$$h(a \otimes 1) = f(a), \quad h(1 \otimes b) = g(b).$$

Luego, necesariamente

$$h(a \otimes b) = h((a \otimes 1) \cdot (1 \otimes b)) = h(a \otimes 1)\, h(1 \otimes b) = f(a)\, g(b).$$

■

No olvidemos que todo anillo conmutativo es una $\mathbb{Z}$-álgebra. Entonces, $R \otimes_{\mathbb{Z}} S$ es el coproducto de R y S en la categoría de anillos conmutativos.

1 Localización

La idea de la localización es bastante sencilla y natural: dado un anillo R y algunos elementos $u \in R$, queremos "añadir" los inversos u^{-1} de manera formal. Esto generaliza la construcción de los números racionales $\mathbb{Q}$ a partir de los números enteros $\mathbb{Z}$. La idea es la misma: hay que considerar las "fracciones" $\frac{r}{u}$ donde en el denominador están los elementos que queremos invertir. El lector probablemente conoce la construcción del cuerpo cociente de un dominio. Nuestro caso será más general: R es cualquier anillo (conmutativo) y se invierten solo ciertos elementos.

1.1 Construcciones y propiedades básicas

1.1. Construcción. Para un anillo R se dice que $U \subseteq R$ es un **subconjunto multiplicativo** si

1) $1 \in U$,

2) $uv \in U$ para cualesquiera $u, v \in U$.

Para un R-módulo M consideremos la relación de equivalencia sobre el conjunto $M \times U$ dada por

$$(m,u) \sim (m',u') \iff v\cdot(u'\cdot m - u\cdot m') = 0 \text{ para algún } v \in U.$$

Denotemos por $\frac{m}{u}$ la clase de equivalencia de (m,u) respecto a esta relación. La **localización en** U de M es el R-módulo

$$M[U^{-1}] := M \times U/\sim$$

donde la adición y acción de R están definidos por

$$\frac{m}{u} + \frac{m'}{u'} := \frac{u'\cdot m + u\cdot m'}{uu'}, \qquad r\cdot\frac{m}{u} := \frac{r\cdot m}{u}.$$

Tenemos una aplicación canónica R-lineal

$$\begin{aligned}\phi\colon M &\to M[U^{-1}],\\ m &\mapsto \frac{m}{1}.\end{aligned}$$

Además, si $M = R$, entonces $R[U^{-1}]$ es un anillo respecto a la multiplicación

$$\frac{r}{u}\cdot\frac{r'}{u'} := \frac{rr'}{uu'}.$$

En este caso la aplicación $\phi\colon r \mapsto \frac{r}{1}$ es un homomorfismo de anillos. La localización $M[U^{-1}]$ tiene una estructura de $R[U^{-1}]$-módulo dada por

$$\frac{r}{u}\cdot\frac{m}{u'} := \frac{r\cdot m}{uu'}.$$

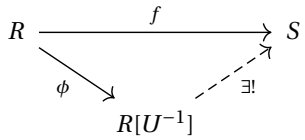
Ejercicio 19. Verifique que

$$(m,u) \sim (m',u') \iff v\cdot(u'\cdot m - u\cdot m') = 0 \text{ para algún } v \in U$$

es una relación de equivalencia.

La localización $R[U^{-1}]$ se caracteriza por la siguiente propiedad universal.

1.2. Proposición. *Sea $f\colon R \to S$ un homomorfismo de anillos que envía todo elemento de U en un elemento invertible en S (es decir, $f(U) \subseteq S^\times$). Entonces, f se factoriza de modo único por $\phi\colon R \to R[U^{-1}]$:*



Idea de la demostración. Si para todo $u \in U$ se tiene $f(u) \in S^\times$, entonces los elementos $f(r)\,f(u)^{-1}$ en S satisfacen las mismas relaciones que las fracciones $\frac{r}{u}$ en $R[U^{-1}]$. ■

1.3. Comentario. Para construir la localización, necesitamos suponer que $U \subseteq R$ es un subconjunto multiplicativo; en el caso contrario $\sim$ no es una relación de equivalencia. La propiedad universal de arriba puede ser formulada para cualquier subconjunto $U \subseteq R$, pero se ve que esta propiedad será satisfecha precisamente por la localización $R[\overline{U}^{-1}]$, donde $\overline{U}$ es la "cerradura multiplicativa" de U. En efecto, si u, v se vuelven invertibles, entonces su producto es también invertible: $(uv)^{-1} = u^{-1}\,v^{-1}$.

1.4. Observación. *Cada aplicación R-lineal $f\colon M \to N$ induce una aplicación $R[U^{-1}]$-lineal*

$$f[U^{-1}]\colon M[U^{-1}] \to N[U^{-1}],$$
$$\frac{m}{u} \mapsto \frac{f(m)}{u}.$$

*La localización es un funtor R-**Mód** $\to R[U^{-1}]$-**Mód**.*

Demostración. No olvidemos que antes de todo, hay que verificar que la aplicación $f[U^{-1}]$ está bien definida: si $\frac{m}{u} = \frac{m'}{u'}$, entonces

$$v \cdot (u' \cdot m - u \cdot m') = 0 \text{ para algún } v \in U.$$

Luego, usando que f es R-lineal,

$$0 = f(v \cdot (u' \cdot m - u \cdot m')) = v \cdot f((u' \cdot m - u \cdot m')) = v \cdot (f(u' \cdot m) - f(u \cdot m')) = v \cdot (u' \cdot f(m) - u \cdot f(m')),$$

lo que significa que $\frac{f(m)}{u} = \frac{f(m')}{u'}$. El resto está claro. ■

1.5. Observación. *Para $m \in M$ se tiene $\phi(m) = \frac{m}{1} = 0$ en $M[U^{-1}]$ si y solamente si m se aniquila por algún elemento de U.*

Demostración. Por la definición de la relación de equivalencia $\sim$, se tiene $\frac{m}{1} = \frac{0}{1}$ si y solamente si $v \cdot m = 0$ para algún $v \in U$. ■

1.6. Observación. *Si M es un R-módulo finitamente generado, entonces $M[U^{-1}] = 0$ si y solamente si M se aniquila por algún elemento de U.*

Demostración. Si hay un elemento $v \in U$ tal que $v \cdot M = 0$, entonces de la observación precedente tenemos $M[U^{-1}] = 0$.

Viceversa, si $M[U^{-1}] = 0$, entonces para cada elemento $m \in M$ existe $v \in U$ tal que $v \cdot m = 0$. Sean $m_1, \ldots, m_s$ generadores de M y sean $v_1, \ldots, v_s \in U$ elementos tales que

$$v_1 \cdot m_1 = \cdots = v_s \cdot m_s = 0.$$

Luego, todo elemento de M es una combinación R-lineal de los m_i y se tiene

$$(v_1 \cdots v_s) \cdot \sum_{1 \le i \le s} r_i \cdot m_i = 0.$$

■

1.7. Ejemplo. Sea R un dominio y sea $U := R \setminus \{0\}$. En este caso la localización $R[U^{-1}]$ se denota por $K(R)$ y es un cuerpo que se conoce como el **cuerpo cociente** o **cuerpo de fracciones** asociado a R. El homomorfismo canónico $\phi\colon R \to K(R)$ es inyectivo.

En general, si R es cualquier anillo y U es el subconjunto de los elementos que no son divisores de cero, entonces $\phi\colon R \to K(R) := R[U^{-1}]$ es un homomorfismo inyectivo. ▲

1.8. Ejemplo. Para un ideal $\mathfrak{p} \subset R$ el subconjunto $U := R \setminus \mathfrak{p}$ es multiplicativo si y solamente si $\mathfrak{p}$ es primo. En este caso se usa la notación

$$R_{\mathfrak{p}} := R[U^{-1}], \quad M_{\mathfrak{p}} := M[U^{-1}].$$

En particular, si R es un dominio, podemos tomar $\mathfrak{p} = (0)$, y luego $R_{(0)} = K(R)$. ▲

1.9. Ejemplo. Para un elemento fijo $x \in R$ consideremos el subconjunto multiplicativo $U := \{1, x, x^2, x^3, \ldots\}$. La localización de R en x se denota por R_x, o también por $R[x^{-1}]$ o $R\left[\frac{1}{x}\right]$. ▲

Ejercicio 20. Sea R un anillo y $x, y \in R$ algunos elementos. Demuestre que $R[x^{-1}][y^{-1}] \cong R[(xy)^{-1}]$.
Sugerencia: demuestre que la composición de los homomorfismos canónicos de localización

$$R \to R[x^{-1}] \to R[x^{-1}][y^{-1}]$$

satisface la propiedad universal del homomorfismo canónico $R \to R[(xy)^{-1}]$.

1.10. Ejemplo. Para $R = \mathbb{Z}$ y un ideal primo $(p) \subset \mathbb{Z}$ tenemos

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, p \nmid b \right\} \subset \mathbb{Q}.$$

Esto es un caso particular de 1.8. Para $n = 1, 2, 3, 4, \ldots$ tenemos

$$\mathbb{Z}\left[\frac{1}{n}\right] = \left\{ \frac{a}{p_1^{e_1} \cdots p_s^{e_s}} \;\middle|\; a \in \mathbb{Z}, e_i \in \mathbb{N} \right\} \subset \mathbb{Q}$$

donde $p_1, \ldots, p_s$ son los primos que aparecen en la factorización de n. Esto es un caso particular de 1.9. ▲

1.2 Ideales en la localización

Una pregunta muy natural es qué sucede con los ideales de un anillo R después de pasar a una localización $R[U^{-1}]$. Resulta que todos los ideales de $R[U^{-1}]$ vienen de los ideales de R. Para aclarar qué está pasando, empecemos por la siguiente situación más general.

1.11. Definición. Sea $f\colon R \to S$ un homomorfismo de anillos. Para un ideal $\mathfrak{b} \subseteq S$ el ideal

$$\mathfrak{b}^c := f^{-1}(\mathfrak{b}) \subseteq R$$

se llama la **contracción** de $\mathfrak{b}$ respecto a f. Para un ideal $\mathfrak{a} \subseteq R$ el ideal

$$\mathfrak{a}^e := f(\mathfrak{a})\, S \subseteq S$$

(es decir, el ideal en S generado* por el subconjunto $f(\mathfrak{a}) \subseteq S$) se llama la **extensión** de $\mathfrak{a}$ respecto a f.

1.12. Proposición. *Sea $f\colon R \to S$ un homomorfismo de anillos.*

1) *Si $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$, entonces $\mathfrak{a}_1^e \subseteq \mathfrak{a}_2^e$.*
2) *Si $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$, entonces $\mathfrak{b}_1^c \subseteq \mathfrak{b}_2^c$.*

*En general, $f(\mathfrak{a})$ no tiene por qué ser un ideal en S. Considere por ejemplo la inclusión $f\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$ y cualquier ideal no nulo $(n) \subseteq \mathbb{Z}$.

3) $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$, $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$.

4) $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.

5) $\mathfrak{b}^c = \mathfrak{b}^{cec}$, $\mathfrak{a}^e = \mathfrak{a}^{ece}$.

6) Sea

$$C := \{\mathfrak{a} \subseteq R \mid \mathfrak{a} = \mathfrak{b}^c \text{ para algún } \mathfrak{b} \subseteq S\}$$

el conjunto de las contracciones de los ideales en S y sea

$$E := \{\mathfrak{b} \subseteq S \mid \mathfrak{b} = \mathfrak{a}^e \text{ para algún } \mathfrak{a} \subseteq R\}$$

el conjunto de las extensiones de los ideales en R. Luego,

$$C = \{\mathfrak{a} \subseteq R \mid \mathfrak{a}^{ec} = \mathfrak{a}\} \quad \text{y} \quad E = \{\mathfrak{b} \subseteq R \mid \mathfrak{b}^{ce} = \mathfrak{b}\}.$$

La aplicación $\mathfrak{a} \mapsto \mathfrak{a}^e$ es una biyección entre C y E, su inversa siendo $\mathfrak{b} \mapsto \mathfrak{b}^c$.

7) Si $\mathfrak{p} \subset S$ es un ideal primo, entonces $\mathfrak{p}^c \subset R$ es también primo.

Demostración. 1) es evidente.

2) y 4) vienen del hecho de que para cualquier aplicación entre conjuntos $f\colon X \to Y$ se tiene $f^{-1}(A) \subseteq f^{-1}(B)$ si $A \subseteq B \subseteq Y$ y $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$ para cualesquiera $A, B \subseteq Y$.

La parte 3) está clara y 5) es una consecuencia de 1), 2) y 3): tenemos $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$ y luego $\mathfrak{b}^c \supseteq \mathfrak{b}^{cec}$. Por otro lado, $\mathfrak{b}^c \subseteq (\mathfrak{b}^c)^{ec}$. De la misma manera, $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ implica que $\mathfrak{a}^e \subseteq \mathfrak{a}^{ece}$, pero también $\mathfrak{a}^e \supseteq (\mathfrak{a}^e)^{ce}$.

En la parte 6), si $\mathfrak{a} \in C$, entonces $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b}^{cec} = \mathfrak{a}^{ec}$. Viceversa, si $\mathfrak{a} = \mathfrak{a}^{ec}$, entonces $\mathfrak{a}$ es la contracción de $\mathfrak{a}^e$. De la misma manera se verifica la descripción para E.

En fin, 7) hace parte del ejercicio 3 (¡hágalo!). ■

1.13. Proposición. *Consideremos el homomorfismo canónico de localización*

$$\begin{aligned} \phi\colon R &\to R[U^{-1}], \\ r &\mapsto \frac{r}{1}. \end{aligned}$$

1) Todo ideal $\mathfrak{b} \subseteq R[U^{-1}]$ es una extensión de algún ideal en R respecto a ϕ; específicamente,

$$\mathfrak{b} = \mathfrak{b}^{ce} = \phi^{-1}(\mathfrak{b})\, R[U^{-1}].$$

En particular, $\mathfrak{b} \mapsto \phi^{-1}(\mathfrak{b})$ es una aplicación inyectiva.

2) Un ideal $\mathfrak{a} \subseteq R$ es de la forma $\mathfrak{b}^c = \phi^{-1}(\mathfrak{b})$ para algún $\mathfrak{b} \subseteq R[U^{-1}]$ si y solamente si los elementos de U no son divisores de cero en $R/\mathfrak{a}$.

3) Hay una biyección

$$\begin{aligned} \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap U = \emptyset\} &\cong \operatorname{Spec} R[U^{-1}], \\ \mathfrak{p} &\mapsto \mathfrak{p}^e, \\ \mathfrak{q}^c &\mapsfrom \mathfrak{q}, \end{aligned}$$

que es la restricción de la biyección entre C y E en la proposición anterior.

Demostración. Para un ideal $\mathfrak{b} \subseteq R[U^{-1}]$ y $\frac{r}{u} \in \mathfrak{b}$ tenemos $\frac{r}{1} = \frac{u}{1} \cdot \frac{r}{u} \in \mathfrak{b}$, así que $r \in \mathfrak{b}^c$ y $\frac{r}{u} \in \mathfrak{b}^{ce}$. Esto demuestra que $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$, y la otra inclusión $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$ se cumple en cualquier caso (véase la proposición anterior). Entonces, $\mathfrak{b} = \mathfrak{b}^{ce}$. Esto establece la parte 1).

En la parte 2), primero notemos que los elementos de $\mathfrak{a}^e = \mathfrak{a}R[U^{-1}]$ son de la forma $\sum_i \frac{r_i}{u_i}\frac{a_i}{1} = \sum_i \frac{r_i a_i}{u_i}$ para $a_i \in \mathfrak{a}$ y $\frac{r_i}{u_i} \in R[U^{-1}]$. Al pasar al común denominador, se ve que son nada más las fracciones $\frac{a}{u}$ donde $a \in \mathfrak{a}$ y $u \in U$. Luego,

$$\mathfrak{a}^{ec} = \left\{ r \in R \;\middle|\; \frac{a}{u} = \frac{r}{1} \text{ para algunos } a \in \mathfrak{a}, u \in U \right\}.$$

Tenemos

$$\frac{a}{u} = \frac{r}{1} \iff v \cdot (a - ur) = 0 \text{ para algún } v \in U.$$

Ahora si $va = vur$, entonces $vur \in \mathfrak{a}$. Viceversa, si para $r \in R$ existe $u \in U$ tal que $ur \in \mathfrak{a}$, entonces $\frac{ur}{u} = \frac{r}{1}$. Podemos concluir que

$$\mathfrak{a}^{ec} = \{ r \in R \mid ur \in \mathfrak{a} \text{ para algún } u \in U \}.$$

Luego,

$$\mathfrak{a} \in C \iff \mathfrak{a}^{ec} \subseteq \mathfrak{a} \iff \boxed{ur \in \mathfrak{a} \text{ para algún } u \in U \Rightarrow r \in \mathfrak{a}},$$

y la última condición quiere decir precisamente que los elementos de U no son divisores de cero en $R/\mathfrak{a}$.

En la parte 3), si $\mathfrak{q} \in \operatorname{Spec} R[U^{-1}]$, entonces $\mathfrak{p} = \mathfrak{q}^c \in \operatorname{Spec} R$, donde los elementos de U no son divisores de cero en $R/\mathfrak{p}$ según 2). El cociente $R/\mathfrak{p}$ es un dominio, así que la última condición significa que $\mathfrak{p} \cap U = \emptyset$.

Para $\mathfrak{p} \in \operatorname{Spec} R$ y su extensión $\mathfrak{p}^e \subseteq R[U^{-1}]$ tenemos

$$R[U^{-1}]/\mathfrak{p}^e \cong (R/\mathfrak{p})[\overline{U}^{-1}],$$

donde $\overline{U}$ denota la imagen de U en el cociente $R/\mathfrak{p}$. Luego, $R/\mathfrak{p}$ es un dominio y para $(R/\mathfrak{p})[\overline{U}^{-1}]$ hay dos posibilidades:

a) $0 \notin \overline{U}$, y entonces $(R/\mathfrak{p})[\overline{U}^{-1}]$ es un dominio, y por ende $\mathfrak{p}^e$ es un ideal primo en $R[U^{-1}]$;

b) $0 \in \overline{U}$, y entonces $(R/\mathfrak{p})[\overline{U}^{-1}] = 0$, y por ende $\mathfrak{p}^e = R[U^{-1}]$.

La condición $0 \notin \overline{U}$ es equivalente a $\mathfrak{p} \cap U = \emptyset$. ■

1.14. Corolario. *Si R es un anillo noetheriano, entonces toda localización $R[U^{-1}]$ es un anillo noetheriano.*

Demostración. Para un ideal $\mathfrak{b} \subseteq R[U^{-1}]$ tenemos $\mathfrak{b} = \phi^{-1}(\mathfrak{b})\,R[U^{-1}]$ donde $\phi^{-1}(\mathfrak{b})$ es un ideal en R. Si R es noetheriano, tenemos $\phi^{-1}(\mathfrak{b}) = (x_1, \ldots, x_n)$ para algunos $x_1, \ldots, x_n \in R$. Luego, $\mathfrak{b} = (\phi(x_1), \ldots, \phi(x_n))$. ■

1.15. Corolario. *Hay una biyección natural*

$$\operatorname{Spec} R_{\mathfrak{p}} \cong \{ \mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \subseteq \mathfrak{p} \}.$$

En particular, $R_{\mathfrak{p}}$ es un anillo local: su único ideal maximal es $\mathfrak{p}R_{\mathfrak{p}}$.

Demostración. Por la definición, $R_{\mathfrak{p}} = R[U^{-1}]$ donde $U := R \setminus \mathfrak{p}$. Entonces, la condición $\mathfrak{q} \cap U = \emptyset$ es equivalente a $\mathfrak{q} \subseteq \mathfrak{p}$. ■

1.3 Localización y el producto tensorial

Hemos construido de modo explícito la localización $M[U^{-1}]$ para un R-módulo M, pero resulta que esta construcción corresponde al producto tensorial con $R[U^{-1}]$.

1.16. Proposición.

1) Hay un isomorfismo natural de $R[U^{-1}]$-módulos

$$\begin{aligned} \alpha\colon R[U^{-1}] \otimes_R M &\xrightarrow{\cong} M[U^{-1}], \\ \frac{r}{u} \otimes m &\mapsto \frac{r \cdot m}{u}. \end{aligned}$$

2) La naturalidad significa que la funtorialidad de la localización corresponde a la funtorialidad de $R[U^{-1}] \otimes_R -$.

Demostración. La aplicación $\left(\frac{r}{u}, m\right) \mapsto \frac{r \cdot m}{u}$ es visiblemente R-bilineal y por esto induce la apliación R-lineal $\frac{r}{u} \otimes m \mapsto \frac{r \cdot m}{u}$. De hecho, es $R[U^{-1}]$-lineal:

$$\frac{r'}{u'} \cdot \left(\frac{r}{u} \otimes m\right) := \frac{r'r}{u'u} \otimes m.$$

Bastaría encontrar la aplicación inversa a α (que será automáticamente $R[U^{-1}]$-lineal). Definamos

$$\begin{aligned} \beta'\colon M \times U &\to R[U^{-1}] \otimes_R M, \\ (m, u) &\mapsto \frac{1}{u} \otimes m. \end{aligned}$$

Si tenemos $\frac{m}{u} = \frac{m'}{u'}$, entonces existe algún $v \in U$ tal que

$$vu' \cdot m = vu \cdot m'.$$

Luego,

$$\begin{aligned} \frac{1}{vuu'} \otimes vu' \cdot m &= \frac{1}{vuu'} \otimes vu \cdot m', \\ \frac{\cancel{vu'}}{\cancel{v}uu'} \otimes m &= \frac{\cancel{vu}}{\cancel{vu}u'} \otimes m', \\ \frac{1}{u} \otimes m &= \frac{1}{u'} \otimes m', \end{aligned}$$

así que $\beta'(m, u) = \beta'(m', u')$. Podemos concluir que β' induce una aplicación

$$\begin{aligned} \beta\colon M[U^{-1}] &\to R[U^{-1}] \otimes_R M, \\ \frac{m}{u} &\mapsto \frac{1}{u} \otimes m, \end{aligned}$$

y se ve que β y α son mutuamente inversas.

En la parte 2), notamos que para toda aplicación R-lineal $f\colon M \to N$ el diagrama

$$\begin{array}{ccc} R[U^{-1}] \otimes_R M & \xrightarrow{\mathrm{id} \otimes f} & R[U^{-1}] \otimes_R N \\ {\scriptstyle \alpha_M}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \alpha_N} \\ M[U^{-1}] & \xrightarrow[f[U^{-1}]]{} & N[U^{-1}] \end{array}$$

conmuta:

$$\begin{array}{ccc} \frac{r}{u}\otimes m & \longmapsto & \frac{r}{u}\otimes f(m) \\ \downarrow & & \downarrow \\ \frac{r\cdot m}{u} & \longmapsto & \frac{f(r\cdot m)}{u} = \frac{r\cdot f(m)}{u} \end{array}$$

■

1.17. Corolario. *Localización preserva sumas directas: se tiene*

$$\left(\bigoplus_i M_i\right)[U^{-1}] \cong \bigoplus_i M_i[U^{-1}].$$

Demostración. Se sigue del resultado anterior y el hecho de que todos productos tensoriales conmuten con sumas directas (véase 0.49). ■

1.4 Planitud de la localización

Recordemos el ejercicio 17 donde hemos notado que para toda sucesión exacta corta

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

la sucesión correspondiente

$$N\otimes_R M' \xrightarrow{\mathrm{id}\otimes i} N\otimes_R M \xrightarrow{\mathrm{id}\otimes p} N\otimes_R M'' \to 0$$

es exacta. En general, la aplicación $\mathrm{id}\otimes i$ no es necesariamente inyectiva.

1.18. Definición. Si N es un R-módulo tal que toda sucesión exacta corta de R-módulos

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

induce una sucesión exacta corta

$$0 \to N\otimes_R M' \xrightarrow{\mathrm{id}\otimes i} N\otimes_R M \xrightarrow{\mathrm{id}\otimes p} N\otimes_R M'' \to 0$$

entonces se dice que N es **plano**.

Ejercicio 21. Demuestre que todo R-módulo libre es plano.

1.19. Proposición. *Toda localización $R[U^{-1}]$ es un R-módulo plano. En otras palabras, usando la identificación de 1.16, una sucesión exacta de R-módulos*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

induce una sucesión exacta de $R[U^{-1}]$-módulos

$$0 \to M'[U^{-1}] \xrightarrow{i[U^{-1}]} M[U^{-1}] \xrightarrow{p[U^{-1}]} M''[U^{-1}] \to 0$$

Demostración. La exactitud en $M[U^{-1}]$ y $M''[U^{-1}]$ se cumple para cualquier producto tensorial (¡haga el ejercicio 17!), hay que comprobar la exactitud en $M'[U^{-1}]$; es decir, que toda aplicación R-lineal inyectiva $i\colon M' \to M$ induce una aplicación inyectiva $i[U^{-1}]\colon M'[U^{-1}] \to M[U^{-1}]$.

Para $\frac{m'}{u} \in M'[U^{-1}]$ tenemos $\frac{i(m')}{u} = 0$ en $M[U^{-1}]$ si y solamente si existe $v \in U$ tal que $v\cdot i(m') = 0$. Luego, $v\cdot i(m') = i(v\cdot m') = 0$, y puesto que i es inyectiva, podemos concluir que $v\cdot m = 0$. Esto implica que $\frac{m'}{u} = 0$ en $M'[U^{-1}]$. ■

1.20. Corolario. *La localización preserva intersecciones finitas: para submódulos $M_1, \dots, M_s \subseteq M$ se tiene*

$$\left(\bigcap_i M_i\right)[U^{-1}] \cong \bigcap_i M[U^{-1}].$$

Demostración. Tenemos una sucesión exacta corta

$$0 \to \bigcap_i M_i \xrightarrow{i} M \xrightarrow{p} \bigoplus_i M/M_i \to 0$$

donde la aplicación p está inducida por las proyecciones canónicas $M \twoheadrightarrow M/M_i$. Al tomar la localización, se obtiene una sucesión exacta corta

$$0 \to \left(\bigcap_i M_i\right)[U^{-1}] \xrightarrow{i[U^{-1}]} M[U^{-1}] \xrightarrow{p[U^{-1}]} \left(\bigoplus_i M/M_i\right)[U^{-1}] \to 0$$

Luego,

$$\left(\bigoplus_i M/M_i\right)[U^{-1}] \cong \bigoplus_i M/M_i[U^{-1}] \cong \bigoplus_i M[U^{-1}]/M_i[U^{-1}]$$

(usando que la localización, como todo producto tensorial, conmuta con sumas directas y cocientes). Entonces,

$$\left(\bigcap_i M_i\right)[U^{-1}] \cong \ker p[U^{-1}] \cong \ker\left(M[U^{-1}] \twoheadrightarrow \bigoplus_i M[U^{-1}]/M_i[U^{-1}]\right) \cong \left(\bigcap_i M_i[U^{-1}]\right).$$

■

He aquí otra consecuencia importante de 1.19.

1.21. Corolario. *Sea M un R-módulo.*

1) *Para $m \in M$ tenemos $m = 0$ si y solamente si m se anula en la localización $M_{\mathfrak{m}}$ para todo $\mathfrak{m} \in \operatorname{Specm} R$.*

2) *Tenemos $M = 0$ si y solamente si $M_{\mathfrak{m}} = 0$ para todo $\mathfrak{m} \in \operatorname{Specm} R$.*

Aquí $M_{\mathfrak{m}}$ denota la localización de M en $U := R \setminus \mathfrak{m}$ (véase 1.8). Notamos que m se anula en $M_{\mathfrak{m}}$ si y solamente si existe un elemento $v \in R \setminus \mathfrak{m}$ tal que $v \cdot m = 0$. En términos del aniquilador de m

$$\operatorname{Ann} m := \{r \in R \mid r \cdot m = 0\},$$

tenemos

$$m \text{ se anula en } M_{\mathfrak{m}} \iff (R \setminus \mathfrak{m}) \cap \operatorname{Ann} m \neq \emptyset \iff \operatorname{Ann} m \not\subseteq \mathfrak{m}.$$

Demostración. La parte 2) es una consecuencia inmediata de 1). Para probar 1), notamos que si m se anula en toda localización $M_{\mathfrak{m}}$, entonces $\operatorname{Ann} m \not\subseteq \mathfrak{m}$ para todo $\mathfrak{m}$. Pero todo ideal propio está contenido en algún ideal maximal (¡haga el ejercicio 4!), así que esto significa que $\operatorname{Ann} m = R$. En particular, $m = 1 \cdot m = 0$. ■

1.22. Corolario. *Una aplicación R-lineal $f\colon M \to N$ es mono (resp. epi, iso) si y solamente si la aplicación $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ es mono (resp. epi, iso) para todo $\mathfrak{m} \in \operatorname{Specm} R$.*

Demostración. Consideremos la sucesión exacta

$$0 \to \ker f \to M \xrightarrow{f} N \to \operatorname{coker} f \to 0$$

La localización preserva sucesiones exactas cortas, y por ende todas las sucesiones exactas[*], así que para todo $\mathfrak{m}$ se tiene una sucesión exacta

$$0 \to (\ker f)_{\mathfrak{m}} \to M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \to (\operatorname{coker} f)_{\mathfrak{m}} \to 0$$

Luego,

$$(\ker f)_{\mathfrak{m}} \cong \ker f_{\mathfrak{m}}, \quad (\operatorname{coker} f)_{\mathfrak{m}} \cong \operatorname{coker} f_{\mathfrak{m}}.$$

Tenemos

$$f \text{ es mono} \iff \ker f = 0 \iff (\ker f)_{\mathfrak{m}} = 0 \text{ para todo } \mathfrak{m} \iff \ker f_{\mathfrak{m}} = 0 \text{ para todo } \mathfrak{m}$$
$$\iff f_{\mathfrak{m}} \text{ es mono para todo } \mathfrak{m}.$$

De la misma manera,

$$f \text{ es epi} \iff \operatorname{coker} f = 0 \iff (\operatorname{coker} f)_{\mathfrak{m}} = 0 \text{ para todo } \mathfrak{m} \iff \operatorname{coker} f_{\mathfrak{m}} = 0 \text{ para todo } \mathfrak{m}$$
$$\iff f_{\mathfrak{m}} \text{ es epi para todo } \mathfrak{m}.$$

En fin,

$$f \text{ es iso} \iff f \text{ es mono y epi} \iff f_{\mathfrak{m}} \text{ es mono y epi para todo } \mathfrak{m} \iff f_{\mathfrak{m}} \text{ es iso para todo } \mathfrak{m}.$$

■

1.5 Localización e ideales primos

1.23. Proposición. *Sea $U \subset R$ un subconjunto multiplicativo y sea $\mathfrak{a} \subset R$ un ideal que es maximal entre los ideales tales que $\mathfrak{a} \cap U = \emptyset$. Entonces, $\mathfrak{a}$ es un ideal primo.*

En otras palabras, $\mathfrak{a}$ es un ideal tal que $\mathfrak{a} \cap U = \emptyset$. Además, si $\mathfrak{a}' \subset R$ es otro ideal tal que $\mathfrak{a}' \cap U = \emptyset$ y $\mathfrak{a} \subseteq \mathfrak{a}'$, entonces $\mathfrak{a}' = \mathfrak{a}$. La existencia de $\mathfrak{a}$ con esta propiedad se deduce del lema de Zorn (¡ejercicio para el lector!).

Demostración. Primero, notamos que $\mathfrak{a}R[U^{-1}]$ es un ideal maximal en $R[U^{-1}]$. Consideremos el homomorfismo canónico de la localización $\phi\colon R \to R[U^{-1}]$. Para un ideal $\mathfrak{b} \subseteq R[U^{-1}]$ la preimagen $\phi^{-1}(\mathfrak{b})$ es un ideal en R, y además $\mathfrak{b} \mapsto \phi^{-1}(\mathfrak{b})$ es una aplicación inyectiva entre los ideales en $R[U^{-1}]$ y los ideales en R (véase 1.13). Ahora si

$$\mathfrak{a}R[U^{-1}] \subseteq \mathfrak{b} \subsetneq R[U^{-1}],$$

entonces

$$\mathfrak{a} \subseteq \phi^{-1}(\mathfrak{a}R[U^{-1}]) \subseteq \phi^{-1}(\mathfrak{b}),$$

donde $\phi^{-1}(\mathfrak{b}) \cap U = \emptyset$, puesto que $\mathfrak{b} \neq R[U^{-1}]$. Pero por la elección de $\mathfrak{a}$, esto implica que

$$\mathfrak{a} = \phi^{-1}(\mathfrak{a}R[U^{-1}]) = \phi^{-1}(\mathfrak{b}),$$

y por la inyectividad de ϕ^{-1}, tenemos $\mathfrak{a}R[U^{-1}] = \mathfrak{b}$. Esto demuestra que $\mathfrak{a}R[U^{-1}]$ es un ideal maximal en $R[U^{-1}]$. En particular, su preimagen $\mathfrak{p} := \phi^{-1}(\mathfrak{a}R[U^{-1}])$ es un ideal primo en R. Pero $\mathfrak{a} \subseteq \mathfrak{p}$ y $\mathfrak{p} \cap U = \emptyset$, así que de nuevo, por la elección de $\mathfrak{a}$, tenemos $\mathfrak{a} = \mathfrak{p}$. ■

Recordemos la siguiente definición.

[*] Ejercicio para el lector: "descomponer" una sucesión exacta en sucesiones exactas cortas.

1.24. Definición. Para un ideal $\mathfrak{a} \subseteq R$ su **radical** es el ideal definido por

$$\sqrt{\mathfrak{a}} := \{x \in R \mid x^n \in \mathfrak{a} \text{ para algún } n = 1,2,3,4,\ldots\}.$$

En particular, el radical del ideal nulo $\mathfrak{a} = (0)$ se llama el **nilradical** y es el ideal compuesto por los nilpotentes de R:

$$N(R) := \sqrt{(0)} := \{x \in R \mid x^n = 0 \text{ para algún } n = 1,2,3,4,\ldots\}.$$

Como una apliación de 1.23, vamos a probar la siguiente caracterización del radical.

1.25. Corolario. *Para todo ideal $\mathfrak{a} \subseteq R$ se tiene*

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} R \\ \mathfrak{p} \supseteq \mathfrak{a}}} \mathfrak{p} \quad \textit{y en particular} \quad N(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}.$$

Demostración. La inclusión del radical $\sqrt{\mathfrak{a}}$ en la intersección de los $\mathfrak{p}$ es fácil. Si tenemos $x \in \sqrt{\mathfrak{a}}$, entonces $x^n \in \mathfrak{a}$ para algún n. Luego, para todo ideal primo $\mathfrak{p}$ tal que $\mathfrak{p} \supseteq \mathfrak{a}$, esto implica que $x \in \mathfrak{p}$[*].

La otra inclusión es más interesante. Supongamos que $x \notin \sqrt{\mathfrak{a}}$. Consideremos el conjunto multiplicativo $U := \{1, x, x^2, x^3, \ldots\}$. Tenemos $\mathfrak{a} \cap U = \emptyset$. Sea $\mathfrak{p}$ un ideal maximal respecto a la propiedad que $\mathfrak{p} \cap U = \emptyset$ y $\mathfrak{p} \supseteq \mathfrak{a}$. Este ideal $\mathfrak{p}$ existe gracias al lema de Zorn y es primo según 1.23. Entonces, podemos concluir que $x \notin \mathfrak{p}$ para algún ideal primo $\mathfrak{p}$ tal que $\mathfrak{p} \supseteq \mathfrak{a}$. Entonces,

$$x \notin \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} R \\ \mathfrak{p} \supseteq \mathfrak{a}}} \mathfrak{p}.$$

■

1.6 Localización y el Hom

Una pregunta natural es cuál es la relación entre las aplicaciones R-lineales $M \to N$ y las aplicaciones $R[U^{-1}]$-lineales $M[U^{-1}] \to N[U^{-1}]$. Cuando M es un módulo finitamente presentado, el siguiente resultado nos da la respuesta.

1.26. Teorema. *Sean R un anillo, S una R-álgebra y M y N dos R-módulos. Supongamos M es finitamente presentado y S es plano sobre R. Entonces, la aplicación S-lineal natural*

$$\alpha_M \colon S \otimes_R \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N),$$
$$1 \otimes f \mapsto \mathrm{id}_S \otimes f$$

es un isomorfismo.

Como vimos en 1.19, la localización $R[U^{-1}]$ es plana sobre R. Entonces, como un caso particular del teorema se obtiene el siguiente resultado.

1.27. Corolario. *Sea R un anillo y sean M y N dos R-módulos donde M es finitamente presentado. Entonces, hay un isomorfismo natural*

$$\operatorname{Hom}_R(M,N)[U^{-1}] \cong \operatorname{Hom}_{R[U^{-1}]}(M[U^{-1}], N[U^{-1}]).$$

Demostración de 1.26. Primero, notamos que la aplicación

$$\operatorname{Hom}_R(M,N) \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N),$$
$$f \mapsto \mathrm{id}_S \otimes f$$

[*] Por la definición del ideal primo, si $xy \in \mathfrak{p}$, entonces $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$. De aquí por inducción se sigue que $x^n \in \mathfrak{p}$ implica $x \in \mathfrak{p}$

es R-lineal, con valores en un S-módulo y se extiende de modo único a la aplicación S-lineal α_M. Queremos probar que α_M es un isomorfismo si M es finitamente presentado.

Primero, analicemos el caso cuando $M = R$. Hay un isomorfismo natural de R-módulos

$$\begin{aligned} \beta\colon \operatorname{Hom}_R(R,N) &\xrightarrow{\cong} N, \\ f &\mapsto f(1); \end{aligned}$$

y por otro lado,

$$\begin{aligned} \gamma\colon \operatorname{Hom}_S(S\otimes_R R, S\otimes_R N) &\xrightarrow{\cong} S\otimes_R N, \\ f &\mapsto f(1\otimes 1) \end{aligned}$$

(este viene del isomorfismo canónico $S\otimes_R R\cong S$ dado por $s\otimes r\mapsto s\cdot r$, su aplicación inversa siendo $s\mapsto s\otimes 1$). Gracias a los isomorfismos β y γ, la aplicación α_R se identifica con la aplicación identidad sobre $S\otimes_R N$:

$$\begin{array}{ccc} S\otimes_R \operatorname{Hom}_R(R,N) & \xrightarrow{\alpha_R} & \operatorname{Hom}_S(S\otimes_R R, S\otimes_R N) \\ {\scriptstyle \mathrm{id}_S\otimes\beta}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \gamma} \\ S\otimes_S N & \xrightarrow[\mathrm{id}]{} & S\otimes_R N \end{array} \qquad \begin{array}{ccc} 1\otimes f & \longmapsto & \mathrm{id}_S\otimes f \\ \downarrow & & \downarrow \\ 1\otimes f(1) & = & 1\otimes f(1) \end{array}$$

Entonces, α_R es un isomorfismo.

Ahora supongamos que $M = R^{\oplus n}$ **es una suma directa de un número finito de copias de** R. Tenemos

$$S\otimes_R \operatorname{Hom}_R(R^{\oplus n}, N) \cong S\otimes_R \operatorname{Hom}_R(R,N)^{\oplus n} \cong (S\otimes_R \operatorname{Hom}_R(R,N))^{\oplus n}$$

—aquí hemos usado el hecho de que $\operatorname{Hom}_R(-,N)$ preserve sumas directas *finitas* y $S\otimes_R -$ conmute con sumas directas. De la misma manera,

$$\operatorname{Hom}_S(S\otimes_R R^{\oplus n}, N) \cong \operatorname{Hom}_S((S\otimes_R R)^{\oplus n}, N) \cong \operatorname{Hom}_S(S\otimes_R R, N)^{\oplus n}.$$

El lector puede comprobar que bajo estos isomorfismos, se puede identificar la aplicación $\alpha_{R^{\oplus n}}$ con la aplicación

$$(\alpha_R)^{\oplus n}\colon (S\otimes_R \operatorname{Hom}_R(R,N))^{\oplus n} \to \operatorname{Hom}_S(S\otimes_R R, N)^{\oplus n}.$$

Acabamos de ver que α_R es un isomorfismo, y por lo tanto la aplicación de arriba es un isomorfismo.

Estamos listos para considerar el caso general cuando M **es finitamente presentado**. Recordemos que esto quiere decir que hay una sucesión exacta

$$R^{\oplus n} \to R^{\oplus m} \to M \to 0 \tag{1.1}$$

El funtor contravariante $\operatorname{Hom}_R(-,N)$ es exacto por la izquierda, así que al aplicarlo a (1.1) se obtiene una sucesión exacta

$$0 \to \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(R^{\oplus m}, N) \to \operatorname{Hom}_R(R^{\oplus n}, N)$$

Luego, tomando el producto tensorial con S se obtiene una sucesión exacta

$$0 \to S\otimes_R \operatorname{Hom}_R(M,N) \to S\otimes_R \operatorname{Hom}_R(R^{\oplus m}, N) \to S\otimes_R \operatorname{Hom}_R(R^{\oplus n}, N) \tag{1.2}$$

—aquí la exactitud por la izquierda viene de la hipótesis de que S sea plano sobre R. También podríamos primero tensorizar (1.1) con S;

$$S\otimes_R R^{\oplus n} \to S\otimes_R R^{\oplus m} \to S\otimes_R M \to 0$$

y luego aplicar $\mathrm{Hom}_S(-, S\otimes_R N)$:

$$0 \to \mathrm{Hom}_S(S\otimes_R M, S\otimes_R N) \to \mathrm{Hom}_S(S\otimes_R R^{\oplus m}, S\otimes_R N) \to \mathrm{Hom}_S(S\otimes_R R^{\oplus n}, S\otimes_R N) \tag{1.3}$$

Ahora las sucesiones exactas (1.2) y (1.3) forman parte del diagrama conmutativo

$$\begin{array}{ccccccc}
0 & \longrightarrow & S\otimes_R \mathrm{Hom}_R(M,N) & \longrightarrow & S\otimes_R \mathrm{Hom}_R(R^{\oplus m},N) & \longrightarrow & S\otimes_R \mathrm{Hom}_R(R^{\oplus n},N) \\
 & & \downarrow{\scriptstyle \alpha_M} & & \downarrow{\scriptstyle \alpha_{R^{\oplus m}}} & & \downarrow{\scriptstyle \alpha_{R^{\oplus n}}} \\
0 & \longrightarrow & \mathrm{Hom}_S(S\otimes_R M, S\otimes_R N) & \longrightarrow & \mathrm{Hom}_S(S\otimes_R R^{\oplus m}, S\otimes_R N) & \longrightarrow & \mathrm{Hom}_S(S\otimes_R R^{\oplus n}, S\otimes_R N)
\end{array}$$

Aquí las últimas dos flechas verticales son isomorfismos, y entonces por el lema del cinco (ejercicio 11) podemos concluir que α_M es también un isomorfismo. ■

1.28. Comentario. La prueba que acabamos de ver usa ideas rudimentarias de álgebra homológica.

2 Longitud

2.1. Definición. Se dice que un R-módulo es **artiniano**[*] si toda cadena decreciente de submódulos

$$M \supseteq M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

se estabiliza: $M_i = M_{i+1}$ para todo i suficientemente grande. Se dice que un anillo R es **artiniano** si es artiniano como un R-módulo (toda cadena decreciente de ideales se estabiliza).

2.2. Ejemplo. El anillo $\mathbb{Z}$ es noetheriano pero no es artiniano: tenemos por ejemplo una cadena decreciente infinita de subgrupos

$$\mathbb{Z} \supsetneq (p) \supsetneq (p^2) \supsetneq (p^3) \supsetneq \cdots$$

▲

Ejercicio 22. El grupo abeliano $\mathbb{Z}[1/p]/\mathbb{Z}$ es isomorfo al grupo multiplicativo de las raíces de la unidad de orden p^n:

$$\mu_{p^\infty}(\mathbb{C}) := \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ para algún } n = 0, 1, 2, 3, \ldots\} = \bigcup_{n \geq 0} \mu_{p^n}(\mathbb{C}).$$

1) Encuentre una cadena creciente infinita de subgrupos de $\mu_{p^\infty}(\mathbb{C})$.

2) Demuestre que todo subgrupo propio $G \subsetneq \mu_{p^\infty}(\mathbb{C})$ es finito.

3) Concluya que $\mathbb{Z}[1/p]/\mathbb{Z}$ es un $\mathbb{Z}$-módulo artiniano que no es noetheriano.

Un ejemplo obvio de módulos artinianos nos dan módulos finitos. Uno de los objetivos de esta sección es entender la estructura de módulos y anillos artinianos.

2.1 Series de composición

2.3. Definición. Para un R-módulo M Una cadena de sumbmódulos propios

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0$$

es una **serie de composición** si todo cociente M_i/M_{i+1} para $i = 0, 1, \ldots, n$ es un R-módulo no nulo **simple** (es decir, no tiene submódulos propios no nulos). El número n se llama la **longitud** de la serie de composición.

2.4. Observación. *En una serie de composición se tiene $M_i/M_{i+1} \cong R/\mathfrak{m}$ donde $\mathfrak{m} \cong \operatorname{Ann}(M_i/M_{i+1})$ es un ideal maximal.*

Demostración. Si M_i/M_{i+1} es simple, entonces todo elemento no nulo de M_i/M_{i+1} genera a todo M_i/M_{i+1}. Esto significa que hay un epimorfismo R-lineal $R \twoheadrightarrow M_i/M_{i+1}$. Luego, $M_i/M_{i+1} \cong R/\mathfrak{m}$ donde $\mathfrak{m}$ es el núcleo. El cociente $R/\mathfrak{m}$ tiene que ser un R-módulo simple, así que es un cuerpo y $\mathfrak{m}$ es un ideal maximal. Este es el aniquilador del cociente $R/\mathfrak{m}$. ■

2.5. Lema. *Supongamos que M es un R-módulo noetheriano y artiniano. Entonces, M admite una serie de composición de longitud finita.*

Demostración. Gracias a la condición noetheriana, podemos tomar en M un submódulo propio maximal M_1. Luego, tomar en M_1 un submódulo propio maximal M_2, etcétera. Gracias a la condición artiniana, en algún momento este proceso termina por $M_n = 0$. ■

[*] Emil Artin (1898–1962), matemático austriaco.

2.6. Definición. Para un R-módulo M la **longitud** es la mínima longitud de las series de composición:

$$\ell(M) := \{n \mid \text{existe una serie de composición } M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0\}.$$

Si M no admite una serie de composición de longitud finita, entonces se pone $\ell(M) = \infty$.

Notamos que $\ell(M) = 0$ significa que $M = 0$, mientras que $\ell(M) = 1$ significa que M es un módulo simple. En realidad, si M admite series de composición finitas, todas tienen la misma longitud, pero necesitamos trabajar un poco para probarlo.

2.7. Lema. *Si $M' \subsetneq M$ es un submódulo propio y $\ell(M) < \infty$, entonces $\ell(M') < \ell(M)$.*

Demostración. Sea

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0$$

una serie de composición para M. Consideremos los submódulos $M'_i := M_i \cap M'$. Tenemos una cadena

$$M' = M'_0 \supseteq M'_1 \supseteq M'_2 \supseteq \cdots \supseteq M'_n = 0 \tag{*}$$

donde

$$M'_i / M'_i \cong \frac{M'_i + M_{i+1}}{M_{i+1}} \subseteq M_i / M_{i+1}.$$

Ya que M_i / M_{i+1} son módulos simples, para M'_i / M'_{i+1} hay dos posibilidades:

1) $M'_i = M'_{i+1}$;

2) $M'_i / M'_i \cong M_i / M_{i+1}$, y en este caso $M'_i + M_{i+1} = M_i$.

Esto significa que a partir de (*) se obtiene una serie de composición para M', hay que solo quitar las repeticiones $M'_i = M'_{i+1}$. Si logramos probar que estas repeticiones existen; es decir, que por lo menos una vez se cumple 1), entonces la serie de composición será más corta que (*).

Supongamos que para todo i se cumple 2). En este caso por inducción descendiente sobre i se puede probar que $M_i \subseteq M'$. Es cierto para $i = n$, dado que $M_n = 0$. Luego, si $M_{i+1} \subseteq M'$, entonces $M'_i = M'_i + M_{i+1}$, y 2) nos da $M_i = M'_i \subseteq M$.

Sin embargo, para $i = 0$ se obtiene $M = M_0 \subseteq M'$, lo que contradice nuestra hipótesis sobre M'. Podemos concluir que 2) no siempre se cumple. ■

2.8. Proposición. *Si M es un R-módulo de longitud finita y*

$$M = N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_k$$

es cualquier cadena de submódulos propios, entonces $k \leq \ell(M)$.

Demostración. Inducción sobre $\ell(M)$. Si $\ell(M) = 0$, entonces $M = 0$ y no hay que probar nada. Para el paso inductivo, notamos que $\ell(N_1) < \ell(M)$ por el lema anterior, y luego $k - 1 \leq \ell(N_1)$ por la hipótesis de inducción. ■

2.9. Corolario. *Si $\ell(M) < \infty$, entonces toda serie de composición para M tiene longitud $\ell(M)$.*

2.10. Corolario. *Si $\ell(M) < \infty$, entonces M es noetheriano y artiniano.*

Demostración. La longitud $\ell(M)$ es una cota superior sobre la longitud de cualquier cadena de submódulos, creciente o decreciente. ■

Junto con 2.5 el último resultado nos dice que los módulos de longitud finita son precisamente los módulos noetherianos y artinianos al mismo tiempo.

Ejercicio 23. Sea V un espacio vectorial sobre un cuerpo k. Las siguientes condiciones son equivalentes:

1) $\dim_k V < \infty$,
2) $\ell(V) < \infty$,
3) V es noetheriano,
4) V es artiniano.

En este caso $\ell(V) = \dim_k V$.

Ejercicio 24. Demuestre que la longitud es **aditiva** en el siguiente sentido.

1) Sea
$$0 \to M' \to M \to M'' \to 0$$
una sucesión exacta corta de R-módulos. Demuestre que se tiene $\ell(M) < \infty$ si y solamente si $\ell(M'), \ell(M'') < \infty$, y que en este caso
$$\ell(M) = \ell(M') + \ell(M'').$$
2) En particular, si $N \subseteq M$ es un submódulo, entonces $\ell(M) < \infty$ si y solamente si $\ell(N), \ell(M/N) < \infty$, y en este caso
$$\ell(M) = \ell(N) + \ell(M/N).$$
3) Si $\ell(M), \ell(N) < \infty$, entonces
$$\ell(M \oplus N) = \ell(M) + \ell(N)$$
y para $n = 1, 2, 3, \ldots$
$$\ell(M^{\oplus n}) = n \cdot \ell(M).$$

2.2 Módulos de longitud finita

2.11. Teorema. *Sea M un R-módulo de longitud finita. Entonces, hay un isomorfismo canónico*
$$\phi\colon M \xrightarrow{\cong} \bigoplus_{\mathfrak{m}} M_{\mathfrak{m}}$$
inducido por las aplicaciones canónicas de localización $M \to M_{\mathfrak{m}}$ y la suma es sobre los ideales maximales $\mathfrak{m}$ tales que en una serie de descomposición
$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0$$
se tiene $M_i/M_{i+1} \cong R/\mathfrak{m}$ para algún i.

El número de los cocientes M_i/M_{i+1} isomorfos a $R/\mathfrak{m}$ es igual a la longitud $\ell(M_{\mathfrak{m}})$ y por lo tanto no depende de una serie de composición particular.

En particular, el teorema quiere decir que para un R-módulo fijo M de longitud finita todas las series de composición coinciden en el sentido de que la longitud es siempre la misma (como ya probamos arriba) y además los cocientes asociados M_i/M_{i+1} son los mismos salvo isomorfismo y permutación. Este resultado se conoce como el **teorema de Jordan–Hölder**[*] y es válido para las series de composición de grupos y series de composición de módulos sobre anillos no conmutativos.

[*] Camille Jordan (1838–1922), matemático francés; Otto Hölder (1859–1937), matemático alemán.

Demostración. Gracias a 1.22, será suficiente probar que

$$\phi_{\mathfrak{m}'}\colon M_{\mathfrak{m}'} \to \left(\bigoplus_{\mathfrak{m}} M_{\mathfrak{m}}\right)_{\mathfrak{m}'} \cong \bigoplus_{\mathfrak{m}} (M_{\mathfrak{m}})_{\mathfrak{m}'}$$

es un isomorfismo para todo $\mathfrak{m}' \in \operatorname{Specm} R$.

Supongamos primero que $\ell(M) = 1$. Esto quiere decir que M es un R-módulo simple y $M \cong R/\mathfrak{m}$ donde $\mathfrak{m} = \operatorname{Ann} M$. La serie de composición es

$$M = M_0 \subsetneq M_1 = 0$$

Los elementos de $U = R \setminus \mathfrak{m}$ ya son invertibles en $R/\mathfrak{m}$ y la aplicación canónica de localización $\phi\colon M \to M_{\mathfrak{m}}$ es un isomorfismo. Notamos que cuando $\mathfrak{m}' \neq \mathfrak{m}$, se tiene $\mathfrak{m} \not\subseteq \mathfrak{m}'$, así que $\mathfrak{m}$ contiene un elemento de $U' = R \setminus \mathfrak{m}'$ y

$$M_{\mathfrak{m}'} \cong (R/\mathfrak{m})_{\mathfrak{m}'} \cong R_{\mathfrak{m}'}/\mathfrak{m}R_{\mathfrak{m}'} = 0.$$

Ahora en el caso general, podemos escoger una serie de composición

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_n = 0$$

Localizándola en $\mathfrak{m}$, se obtiene una cadena de submódulos

$$(*) \qquad M_{\mathfrak{m}} = (M_0)_{\mathfrak{m}} \supsetneq (M_1)_{\mathfrak{m}} \supsetneq (M_2)_{\mathfrak{m}} \supsetneq \cdots \supsetneq (M_n)_{\mathfrak{m}} = 0$$

Puesto que $\ell(M_i/M_{i+1}) = 1$, la discusión anterior demuestra que

$$(M_i)_{\mathfrak{m}}/(M_{i+1})_{\mathfrak{m}} \cong (M_i/M_{i+1})_{\mathfrak{m}} \cong \begin{cases} M_i/M_{i+1}, & \text{si } M_i/M_{i+1} \cong R/\mathfrak{m}, \\ 0, & \text{en el caso contrario.} \end{cases}$$

Quitando de (*) los submódulos iguales, se obtiene una serie de descomposición para $M_{\mathfrak{m}}$. En particular, si M_i/M_{i+1} no es isomorfo a $R/\mathfrak{m}$ para ningún i, entonces $M_{\mathfrak{m}} = 0$. De nuevo, por la discusión anterior, la aplicación canónica $M_{\mathfrak{m}'} \to (M_{\mathfrak{m}})_{\mathfrak{m}'}$ es un isomorfismo si $\mathfrak{m}' = \mathfrak{m}$ y es la aplicación nula $0 \to 0$ en el caso contrario. ■

2.12. Ejemplo. Consideremos el $\mathbb{Z}$-módulo $\mathbb{Z}/12\mathbb{Z}$ (los restos módulo n). Es finito, así que es obviamente noetheriano y artiniano. Podemos tomar una serie de composición

$$\mathbb{Z}/12\mathbb{Z} \supsetneq (3) \supsetneq (6) \supsetneq (0)$$

Los cocientes correspondientes son

$$(\mathbb{Z}/12\mathbb{Z})/(3) \cong \mathbb{Z}/3\mathbb{Z}, \quad (3)/(6) \cong \mathbb{Z}/2\mathbb{Z}, \quad (6) \cong \mathbb{Z}/2\mathbb{Z}.$$

Ahora

$$(\mathbb{Z}/12\mathbb{Z})_{(2)} \cong (\mathbb{Z}_{(2)}/4\mathbb{Z}_{(2)}) \cong \mathbb{Z}/4\mathbb{Z}, \quad (\mathbb{Z}/12\mathbb{Z})_{(3)} \cong (\mathbb{Z}_{(3)}/3\mathbb{Z}_{(3)}) \cong \mathbb{Z}/3\mathbb{Z}.$$

El resultado que acabamos de probar nos dice que

$$\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Esto es nada más el teorema chino del resto. ▲

2.13. Proposición. *Sea M un R-módulo de longitud finita y sea $\mathfrak{m}$ un ideal maximal en R. Entonces, las siguientes condiciones son equivalentes:*

1) $M \cong M_{\mathfrak{m}}$,

2) $\mathfrak{m}^n \cdot M = 0$ *para algún* $n = 0, 1, 2, 3, \ldots$

Recordemos que $\mathfrak{m}^n$ denota el ideal generado por los productos $x_1 \cdots x_n$ donde $x_i \in \mathfrak{m}$ (véase 0.10).

Demostración. Supongamos que $M \cong M_{\mathfrak{m}}$. En este caso las series de composición para M son de la forma

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_0 = 0$$

donde $M_i / M_{i+1} \cong R/\mathfrak{m}$ y $\mathfrak{m} = \operatorname{Ann}(M_i / M_{i+1})$; es decir, $\mathfrak{m} \cdot M_i \subseteq M_{i+1}$. Demostremos por inducción que $\mathfrak{m}^i \cdot M \subseteq M_i$ para todo i. La base es el caso de $i = 0$ cuando $M_0 = M$. Supongamos que $\mathfrak{m}^i \cdot M \subseteq M_i$. Luego,

$$\mathfrak{m}^{i+1} \cdot M = \mathfrak{m} \cdot (\mathfrak{m}^i \cdot M) \subseteq \mathfrak{m} \cdot M_i \subseteq M_{i+1}.$$

En particular, para $i = n$ se tiene $\mathfrak{m}^n \cdot M \subseteq M_n = 0$.

Viceversa, supongamos que $\mathfrak{m}^n \cdot M = 0$. En este caso para otro ideal maximal $\mathfrak{m}'$ se tiene $\mathfrak{m} \not\subseteq \mathfrak{m}'$, así que $\mathfrak{m}$ contiene un elemento $v \in R \setminus \mathfrak{m}'$. Luego, $v^n \cdot M = 0$, así que $M_{\mathfrak{m}'} = 0$. Gracias al teorema 2.11 podemos concluir que $M \cong M_{\mathfrak{m}}$. ■

2.3 Anillos artinianos

Resulta que para los *anillos* la condición artiniana automáticamente implica la condición noetheriana. Específicamente, tenemos la siguiente caracterización de anillos artinianos.

2.14. Teorema. *Sea R un anillo conmutativo. Las siguientes condiciones son equivalentes.*

1) R es noetheriano y todos los ideales primos en R son maximales.

2) R tiene longitud finita como un R-módulo.

3) R es artiniano.

En este caso R tiene un número finito de ideales maximales.

Demostración. 1) ⇒ 2). Supongamos que R es noetheriano y todos los ideales primos en R son maximales. Vamos a ver que R necesariamente tiene longitud finita. En efecto, si R no es de longitud finita, sea $\mathfrak{a}$ un ideal que es maximal respecto a la propiedad que $R/\mathfrak{a}$ tiene longitud infinita (tal ideal $\mathfrak{a}$ existe gracias a la condición noetheriana).

En este caso $\mathfrak{a}$ es un ideal primo. En efecto, supongamos que $xy \in \mathfrak{a}$ para algunos $x, y \in R$ y $x \notin \mathfrak{a}$. Tenemos una sucesión exacta corta

$$0 \to R/(\mathfrak{a} : x) \xrightarrow{\times x} R/\mathfrak{a} \to R/(\mathfrak{a} + (x)) \to 0$$

donde

$$(\mathfrak{a} : x) := \{r \in R \mid r \cdot (x) \subseteq \mathfrak{a}\} \supseteq \mathfrak{a}.$$

Notamos que $y \in (\mathfrak{a} : x)$. Por nuestra hipótesis que $x \notin \mathfrak{a}$, tenemos $\mathfrak{a} \subsetneq \mathfrak{a} + (x)$. Si además $y \notin \mathfrak{a}$, entonces por la elección de $\mathfrak{a}$ se tiene $\ell(R/(\mathfrak{a} : x)) < \infty$ y $\ell(R/(\mathfrak{a} + (x))) < \infty$. Por el ejercicio 24, esto implicaría que $\ell(R/\mathfrak{a})$, pero no es el caso. Entonces, $y \in \mathfrak{a}$.

Ahora si todos los ideales primos son maximales, entonces $R/\mathfrak{a}$ es un cuerpo y tiene longitud 1. Contradicción.

2) ⇒ 3). Ya probamos en 2.10 que todo módulo de longitud finita es necesariamente noetheriano y artiniano.

3) ⇒ 1). Supongamos que R es artiniano. Primero, vamos a ver que

$$0 = \mathfrak{m}_1 \cdots \mathfrak{m}_s$$

para algunos ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_s \subset R$. En efecto, ya que R es artiniano, entre todos los ideales que son productos de ideales maximales existe un ideal mínimo $\mathfrak{a} = \mathfrak{m}_1 \cdots \mathfrak{m}_s$.

Vamos a ver que en efecto $\mathfrak{a} = 0$. Por la minimalidad de $\mathfrak{a}$, para cualquier ideal maximal $\mathfrak{m} \subset R$ se tiene $\mathfrak{a} = \mathfrak{m} \cdot \mathfrak{a} \subseteq \mathfrak{m}$. El ideal $\mathfrak{a}^2 \subseteq \mathfrak{a}$ es también un producto de ideales maximales, y por lo tanto $\mathfrak{a}^2 = \mathfrak{a}$. Ahora si $\mathfrak{a} \neq 0$, sea $\mathfrak{b}$ un ideal mínimo entre los ideales tales que $\mathfrak{b}\mathfrak{a} \neq 0$ (de nuevo, su existencia se sigue de la condición artiniana). Tenemos

$$(\mathfrak{b}\mathfrak{a}) \cdot \mathfrak{a} = \mathfrak{b} \cdot \mathfrak{a}^2 = \mathfrak{b}\mathfrak{a} \neq 0$$

Por otro lado, $\mathfrak{b}\mathfrak{a} \subseteq \mathfrak{b}$, así que por la minimalidad de $\mathfrak{b}$ se tiene $\mathfrak{b}\mathfrak{a} = \mathfrak{b}$. Ya que $\mathfrak{b}\mathfrak{a} \neq 0$, existe $x \in \mathfrak{b}$ tal que $x \cdot \mathfrak{a} \neq 0$. Por la minimalidad de $\mathfrak{b}$, se tiene $\mathfrak{b} = (x)$. Ahora la ecuación

$$\mathfrak{b}\mathfrak{a} = \mathfrak{b} \iff (x) \cdot \mathfrak{a} = (x)$$

significa que existe $y \in \mathfrak{a}$ tal que $xy = x$; es decir, $(1 - y)\, x = 0$. Pero y, siendo un elemento de $\mathfrak{a}$, pertenece a todos los ideales maximales, así que[*] $1 - y \in R^\times$. Podemos deducir que $x = 0$, pero en este caso $\mathfrak{b}\mathfrak{a} = \mathfrak{b} = (x) = 0$. Contradicción. Entonces, $\mathfrak{a} = 0$.

Esto demuestra que se cumple $0 = \mathfrak{m}_1 \cdots \mathfrak{m}_s$ para algunos ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_s \subset R$. Ahora para cualquier ideal primo $\mathfrak{p} \subset R$ se tiene $\mathfrak{m}_1 \cdots \mathfrak{m}_s = (0) \subseteq \mathfrak{p}$, y por lo tanto $\mathfrak{m}_i \subseteq \mathfrak{p}$ (véase el ejercicio 2) y luego $\mathfrak{p} = \mathfrak{m}_i$ por la maximalidad de $\mathfrak{m}_i$. Esto demuestra que todo ideal primo es maximal y que hay un número finito de ellos.

Nos falta ver que R es un anillo noetheriano. Vamos a probar que es de longitud finita. Para $i = 1, 2, \ldots, s$ denotemos

$$\mathfrak{a}_i := \mathfrak{m}_1 \cdots \mathfrak{m}_i$$

y consideremos la cadena decreciente

$$R \supseteq \mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \mathfrak{a}_3 \supseteq \cdots \supseteq \mathfrak{a}_s = 0$$

Para todo i el cociente

$$V_i := \mathfrak{a}_{i-1}/\mathfrak{a}_i$$

es un espacio vectorial sobre el cuerpo $R/\mathfrak{m}_i$. Para una colección de elementos linealmente independientes $v_1, v_2, v_3, v_4, \ldots \in V_i$ consideremos la cadena decreciente

$$V_i \supseteq \langle v_1, v_2, v_3, v_4, \ldots \rangle \supseteq \langle v_2, v_3, v_4, \ldots \rangle \supseteq \langle v_3, v_4, \ldots \rangle \supseteq \langle v_4, \ldots \rangle \supseteq \cdots$$

Esta cadena siempre se estabiliza puesto que R es artiniano (la cadena de arriba corresponde a una cadena de ideales en R que contienen a $\mathfrak{m}_i$). Entonces, $\dim_{k_i} V_i < \infty$ para todo i; es decir, $\ell(V_i) < \infty$. Luego, tenemos

$$\begin{aligned}
\ell(R) &= \ell(\mathfrak{a}_1) + \underbrace{\ell(R/\mathfrak{a}_1)}_{=1}, \\
\ell(\mathfrak{a}_1) &= \ell(\mathfrak{a}_2) + \ell(V_2), \\
\ell(\mathfrak{a}_2) &= \ell(\mathfrak{a}_3) + \ell(V_3), \\
&\cdots \\
\ell(\mathfrak{a}_s) &= 0.
\end{aligned}$$

Empezando por la última relación, por inducción decreciente sobre i se deduce que $\ell(\mathfrak{a}_i) < \infty$ para todo $i = 1, \ldots, s$ y $\ell(R) < \infty$. ■

2.15. Corolario. *Todo anillo artiniano es un producto directo finito de anillos locales artinianos.*

[*] Si $1 - y$ no es invertible, entonces este elemento pertenece a algún ideal maximal $\mathfrak{m}$. Pero $y \in \mathfrak{m}$, así que $1 \in \mathfrak{m}$. Contradicción.

Demostración. Si R es artiniano, entonces es de longitud finita por el teorema anterior. Luego, 2.11 nos dice que hay un isomorfismo de R-módulos

$$R \xrightarrow{\cong} \bigoplus_{\mathfrak{m}} R_{\mathfrak{m}}$$

inducido por las aplicaciones canónicas de localización. La suma es finita (como se sigue de 2.11, y además en el teorema anterior notamos que en general en R hay un número finito de ideales maximales). Como R-módulo, el producto de R-álgebras $\prod_{\mathfrak{m}} R_{\mathfrak{m}}$ coincide con $\bigoplus_{\mathfrak{m}} R_{\mathfrak{m}}$. Las aplicaciones canónicas de localización son homomorfismos de R-álgebras, así que en realidad se tiene un isomorfismo de R-álgebras

$$R \xrightarrow{\cong} \prod_{\mathfrak{m}} R_{\mathfrak{m}}.$$

■

2.16. Corolario. *Sea $\mathfrak{a}$ un ideal en un anillo noetheriano R. Sea $\mathfrak{p} \subset R$ un ideal primo tal que $\mathfrak{a} \subset \mathfrak{p}$. Las siguientes condiciones son equivalentes.*

1) *$\mathfrak{p}$ es mínimo entre los ideales primos que contienen $\mathfrak{a}$.*
2) *$R_{\mathfrak{p}}/\mathfrak{a}R_{\mathfrak{p}}$ es un anillo artiniano.*
3) *Se tiene $(\mathfrak{p}R_{\mathfrak{p}})^n \subseteq \mathfrak{a}R_{\mathfrak{p}}$ para n suficientemente grande.*

Demostración. 1) $\Rightarrow$ 2). Los ideales primos en el cociente $R_{\mathfrak{p}}/\mathfrak{a}R_{\mathfrak{p}}$ corresponden a los ideales primos $\mathfrak{q} \subset R_{\mathfrak{p}}$ tales que

$$\mathfrak{a}R_{\mathfrak{p}} \subseteq \mathfrak{q} \subseteq \mathfrak{p}R_{\mathfrak{p}}.$$

Luego, tenemos

$$\mathfrak{a} \subseteq \phi^{-1}(\mathfrak{a}R_{\mathfrak{p}}) \subseteq \phi^{-1}(\mathfrak{q}) \subseteq \mathfrak{p}$$

donde $\phi\colon R \to R_{\mathfrak{p}}$ es la aplicación canónica de localización. Por la minimalidad de $\mathfrak{p}$, tenemos $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$; es decir, $\mathfrak{q} = \mathfrak{p}R_{\mathfrak{p}}$. En particular, todos los ideales primos en $R_{\mathfrak{p}}/\mathfrak{a}R_{\mathfrak{p}}$ son maximales y por lo tanto $R_{\mathfrak{p}}/\mathfrak{a}R_{\mathfrak{p}}$ es artiniano por 2.14.

2) $\Rightarrow$ 3). Si $R_{\mathfrak{p}}/\mathfrak{a}R_{\mathfrak{p}}$ es artiniano, entonces es de longitud finita como un módulo sobre sí mismo según 2.14. Gracias a 2.13 podemos concluir que $(\mathfrak{p}R_{\mathfrak{p}})^n \subseteq \mathfrak{a}R_{\mathfrak{p}}$ para algún n.

3) $\Rightarrow$ 1). Supongamos que $(\mathfrak{p}R_{\mathfrak{p}})^n \subseteq \mathfrak{a}R_{\mathfrak{p}}$. Sea $\mathfrak{q}$ un ideal primo en R tal que $\mathfrak{a} \subseteq \mathfrak{q} \subseteq p$. Luego, en $R_{\mathfrak{p}}$ hay una cadena de ideales

$$(\mathfrak{p}R_{\mathfrak{p}})^n \subseteq \mathfrak{a}R_{\mathfrak{p}} \subseteq \mathfrak{q}R_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}.$$

La primalidad de $\mathfrak{q}R_{\mathfrak{p}}$ implica que $\mathfrak{p}R_{\mathfrak{p}} \subseteq \mathfrak{q}R_{\mathfrak{q}}$, luego $\mathfrak{q}R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ y por esto $\mathfrak{q} = \mathfrak{p}$. ■

2.17. Corolario. *Sea R un anillo noetheriano y sea M un R-módulo finitamente generado. Las siguientes condiciones son equivalentes.*

1) *M es de longitud finita.*
2) *Para un producto finito de ideales maximales $\mathfrak{m}_1 \cdots \mathfrak{m}_n$ se tiene $(\mathfrak{m}_1 \cdots \mathfrak{m}_n) \cdot M$.*
3) *Todos los ideales primos que contienen a $\operatorname{Ann} M$ son maximales.*
4) *El anillo $R/\operatorname{Ann} M$ es artiniano.*

Demostración. 1) ⇒ 2). Si M es de longitud finita, entonces

$$M \cong M_{\mathfrak{m}_1} \oplus \cdots \oplus M_{\mathfrak{m}_s}$$

según 2.11. Luego, según 2.13, para cada $M_{\mathfrak{m}_i}$ se tiene $\mathfrak{m}_i^{n_i} \cdot M_{\mathfrak{m}_i} = 0$ para algún n_i. Podemos concluir que

$$\mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_s^{n_s} \cdot M = 0.$$

2) ⇒ 3). Si tenemos $\mathfrak{m}_1 \cdots \mathfrak{m}_n \cdot M = 0$ y $\mathfrak{p} \supseteq \operatorname{Ann} M$, entonces $\mathfrak{p} \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n$ y luego $\mathfrak{p} \supseteq \mathfrak{m}_i$ para algún i por la primalidad de $\mathfrak{p}$ y luego $\mathfrak{p} = \mathfrak{m}_i$ por la maximalidad de i.

3) ⇒ 4). Según 2.14, un anillo es artiniano si y solamente si es noetheriano y todo ideal primo es maximal. Los ideales primos en el cociente $R/\operatorname{Ann} M$ corresponden a los ideales primos en R que contienen a $\operatorname{Ann} M$.

4) ⇒ 1). Supongamos que el anillo cociente $R/\operatorname{Ann} M$ es artiniano. Entonces, es de longitud finita como un $R/\operatorname{Ann} M$-módulo o como un R-módulo. Si M es finitamente generado como un R-módulo, entonces es finitamente generado como un $R/\operatorname{Ann} M$-módulo. Tenemos una sobreyección $(R/\operatorname{Ann} M)^{\oplus n} \twoheadrightarrow M$. La longitud de $(R/\operatorname{Ann} M)^{\oplus n}$ es finita, así que la longitud de M es finita (véase el ejercicio 24). ■

2.18. Corolario. *Sea R un anillo noetheriano y sea $M \neq 0$ un R-módulo finitamente generado. Sea $\mathfrak{p} \subset R$ un ideal primo tal que $\mathfrak{p} \supseteq \operatorname{Ann} M$. Las siguientes condiciones son equivalentes.*

1) *$\mathfrak{p}$ es mínimo entre los ideales primos tales que $\mathfrak{p} \supseteq \operatorname{Ann} M$.*

2) *$M_{\mathfrak{p}}$ es un $R_{\mathfrak{p}}$-módulo no nulo de longitud finita.*

Demostración. Hagamos primero un par de observaciones.

- Se tiene $M_{\mathfrak{p}} = 0$ si y solamente si $v \cdot M = 0$ para algún $v \in R \setminus \mathfrak{p}$ (véase 1.6). Esto no sucede cuando $\operatorname{Ann} M \subseteq \mathfrak{p}$.
- Para el aniquilador de $M_{\mathfrak{p}}$ se cumple

$$\operatorname{Ann}(M_{\mathfrak{p}}) := \left\{ \frac{r}{u} \in R_{\mathfrak{p}} \;\middle|\; \frac{r}{u} \cdot M_{\mathfrak{p}} = 0 \right\} = \{ r \in R \mid r \cdot M = 0 \} R_{\mathfrak{p}} = \operatorname{Ann}(M) R_{\mathfrak{p}}.$$

Para probar 1) ⇒ 2), notamos que si hay un ideal primo $\mathfrak{q} \subset R_{\mathfrak{p}}$ tal que $\operatorname{Ann}(M_{\mathfrak{p}}) \subseteq \mathfrak{q}$, entonces

$$\operatorname{Ann}(M) \subseteq \phi^{-1}(\operatorname{Ann}(M) R_{\mathfrak{p}}) = \phi^{-1}(M_{\mathfrak{p}}) \subseteq \phi^{-1}(\mathfrak{q}) \subseteq \mathfrak{p}.$$

Luego, por la minimalidad de $\mathfrak{p}$, se tiene $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$ y por lo tanto $\mathfrak{q} = \mathfrak{p} R_{\mathfrak{p}}$ que es el único ideal maximal en $R_{\mathfrak{p}}$. Entonces, se cumple la condición 3) de 2.17 que implica que $M_{\mathfrak{p}}$ es de longitud finita como un $R_{\mathfrak{p}}$-módulo.

En la dirección 2) ⇒ 1), si $M_{\mathfrak{p}}$ es de longitud finita sobre $R_{\mathfrak{p}}$, entonces por 2.17 todo ideal primo en $R_{\mathfrak{p}}$ que contiene a $\operatorname{Ann}(M_{\mathfrak{p}})$ es maximal; es decir, coincide con $\mathfrak{p} R_{\mathfrak{p}}$. Ahora si

$$\operatorname{Ann}(M) \subseteq \mathfrak{q} \subseteq \mathfrak{p} \subset R,$$

entonces tenemos

$$\operatorname{Ann}(M_{\mathfrak{p}}) = \operatorname{Ann}(M) R_{\mathfrak{p}} \subseteq \mathfrak{q} R_{\mathfrak{p}} \subseteq \mathfrak{p} R_{\mathfrak{p}} \subset R_{\mathfrak{p}},$$

así que $\mathfrak{q} R_{\mathfrak{p}} = \mathfrak{p} R_{\mathfrak{p}}$ y por lo tanto $\mathfrak{q} = \mathfrak{p}$. Esto demuestra la minimalidad de $\mathfrak{p}$. ■

3 El teorema de Cayley–Hamilton y el lema de Nakayama

El teorema de Cayley–Hamilton[*] clásico dice que si $\phi\colon V \to V$ es un endomorfismo de un espacio vectorial de dimensión finita y

$$p = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in k[X]$$

es su polinomio característico, entonces

$$p(\phi) = \phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0 \,\mathrm{id} = 0.$$

En esta sección vamos a ver una generalización de este resultado y sus aplicaciones.

3.1 El teorema de Cayley–Hamilton

3.1. Proposición (El teorema de Cayley–Hamilton). *Sea R un anillo, $\mathfrak{a} \subseteq R$ un ideal y M un R-módulo finitamente generado. Sea $\phi\colon M \to M$ un endomorfismo R-lineal que satisface $\phi(M) \subseteq \mathfrak{a}\cdot M$. Entonces, ϕ satisface una relación*

$$\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_1\phi + a_0 \,\mathrm{id} = 0$$

en el anillo $\mathrm{End}_R(M)$ *donde* $a_i \in \mathfrak{a}$.

Demostración. Sean $m_1, \ldots, m_n$ generadores de M como un R-módulo. Puesto que $\phi(m_i) \in \mathfrak{a}\cdot M$, tenemos ecuaciones

$$\phi(m_i) = \sum_{1 \le j \le n} a_{ij}\, m_j$$

para algunos $a_{ij} \in \mathfrak{a}$. Consideremos M como un $R[X]$-módulo donde X actúa sobre M como ϕ (es decir, $X \cdot m := \phi(m)$). Las ecuaciones de arriba corresponden a la identidad en el anillo de matrices $M_n(R[X])$

$$X\,m = A\,m \iff (XI - A)\,m = 0,$$

donde I es la matriz identidad de $n \times n$, la matriz A tiene a_{ij} como sus coeficientes y $m := (m_1, \ldots, m_n)^t$. Multiplicando esta ecuación por la matriz de cofactores de $XI - A$, se obtiene

$$\det(XI - A)\cdot m = 0.$$

Es decir, $\det(XI - A) \in R[X]$ aniquila a todo generador de M, y por lo tanto

$$\det(XI - A)\cdot M = 0.$$

Es fácil ver que

$$\det(XI - A) = \det\begin{pmatrix} X - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & X - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & X - a_{nn} \end{pmatrix}$$

es un polinomio mónico de grado n y sus coeficientes $a_0, a_1, \ldots, a_{n-1}$ pertenecen al ideal $\mathfrak{a}$. ∎

[*] Arthur Cayley (1821–1895), matemático británico; William Rowan Hamilton (1805–1865), matemático irlandés.

3.2 El lema de Nakayama

Ahora vamos a deducir del teorema de Cayley–Hamilton un resultado muy importante, conocido como el lema de Nakayama. Primero, necesitamos un pequeño lema.

3.2. Lema. *Sea M un R-módulo finitamente generado. Sea $\mathfrak{a} \subseteq R$ un ideal tal que $\mathfrak{a} \cdot M = M$. Entonces, existe $x \in \mathfrak{a}$ tal que x actúa sobre M como la identidad; es decir,* $(1-x) \cdot M = 0$.

Demostración. Aplicando el teorema de Cayley–Hamilton al endomorfismo identidad $\mathrm{id}\colon M \to M$, se deduce que existen $a_0, a_1, \ldots, a_{n-1} \in \mathfrak{a}$ tales que para todo $m \in M$ se tiene

$$m + a_{n-1}\, m + \cdots + a_1\, m + a_0\, m = (1 + a_{n-1} + \cdots + a_1 + a_0)\, m = 0.$$

Entonces, podemos tomar $x = -(a_{n-1} + \cdots + a_1 + a_0)$. ■

3.3. Teorema (El lema de Nakayama[*]). *Sea R un anillo y sea $\mathfrak{a}$ un ideal que está contenido en todos los ideales maximales de R. Sea M un R-módulo finitamente generado.*

1) *Si $\mathfrak{a} \cdot M = M$, entonces $M = 0$.*
2) *Si las imágenes de algunos elementos $m_1, \ldots, m_n \in M$ en $M/\mathfrak{a}M$ generan a $M/\mathfrak{a}M$ como un R-módulo, entonces $m_1, \ldots, m_n$ generan a M como un R-módulo.*

Este resultado normalmente se aplica cuando R es un anillo local y $\mathfrak{a} = \mathfrak{m}$ es su único ideal maximal.

Demostración. En 1), por el lema anterior existe $x \in \mathfrak{a}$ tal que $(1-x) \cdot M = 0$. Dado que x pertenece a todos los ideales maximales, $1 - x$ es invertible y luego $M = 0$.

En 2), consideremos el módulo $N := M/\langle m_1, \ldots, m_n \rangle$. Tenemos

$$N/\mathfrak{a}N = M/(\mathfrak{a} + \langle m_1, \ldots, m_n \rangle) = M/M = 0.$$

Entonces, $\mathfrak{a} \cdot N = N$ y la parte 1) implica que $N = 0$. ■

3.4. Comentario. Note que la prueba usa la hipótesis que M es finitamente generado. La parte 2) no significa que si $M/\mathfrak{a}M$ es finitamente generado, entonces M es finitamente generado.

3.5. Corolario. *Sea R un anillo local y sean M y N dos R-módulos finitamente generados tales que $M \otimes_R N = 0$. Entonces, $M = 0$ o $N = 0$.*

Demostración. Sea $\mathfrak{m}$ el ideal maximal de R. Si $M \neq 0$, entonces $\mathfrak{m} \cdot M \neq M$ por el lema de Nakayama, así que $M/\mathfrak{m}M$ es un espacio vectorial no nulo de dimensión finita sobre $R/\mathfrak{m}$. Tenemos entonces una sobreyección

$$M \twoheadrightarrow M/\mathfrak{m}M \twoheadrightarrow R/\mathfrak{m}.$$

La exactitud de $- \otimes_R N$ por la derecha implica que hay una sobreyección de $M \otimes_R N$ a $R/\mathfrak{m} \otimes_R N \cong N/\mathfrak{m}N$. Si $M \otimes_R N = 0$, esto significa que $N/\mathfrak{m}N = 0$. El lema de Nakayama implica que $N = 0$. ■

3.6. Corolario. *Sea R cualquier anillo y sean M y N dos R-módulos finitamente generados tales que $M \otimes_R N = 0$. Entonces,* $\operatorname{Ann} M + \operatorname{Ann} N = R$.

Demostración. Si $\operatorname{Ann} M + \operatorname{Ann} N \neq R$, entonces existe un ideal maximal $\mathfrak{m}$ tal que $\operatorname{Ann} M, \operatorname{Ann} N \subseteq \mathfrak{m}$. En este caso $M_\mathfrak{m} \neq 0$ y $N_\mathfrak{m} \neq 0$ (véase 1.6). Sin embargo,

$$M_\mathfrak{m} \otimes_{R_\mathfrak{m}} N_\mathfrak{m} \cong (M \otimes_R N)_\mathfrak{m} = 0,$$

lo que contradice el resultado anterior. ■

[*] Tadashi Nakayama (1912–1964), matemático japonés.

3.7. Ejemplo. Tenemos $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(m,n)\mathbb{Z}$. Luego, $\operatorname{Ann}\mathbb{Z}/m\mathbb{Z} = (m)$ y $\operatorname{Ann}\mathbb{Z}/n\mathbb{Z} = (n)$. El producto tensorial es nulo cuando m y n son coprimos; es decir, cuando $(m) + (n) = (m,n) = (1)$. ▲

Ejercicio 25. Sea P un R-módulo proyectivo finitamente generado. Esto es equivalente a decir que existe otro R-módulo Q tal que $P \oplus Q \cong R^n$ es un R-módulo libre. En este ejercicio vamos a probar que si R es un anillo local, entonces P es libre. Sea $\mathfrak{m}$ el ideal maximal de R y sea $k := R/\mathfrak{m}$.

Identifiquemos P y Q con submódulos de R^n.

1) Sean $\overline{p}_1, \ldots, \overline{p}_s$ y $\overline{q}_1, \ldots, \overline{q}_t$ algunas bases de los subespacios vectoriales $P/\mathfrak{m}P \subset k^n$ y $Q/\mathfrak{m}Q \subset k^n$ respectivamente (aquí $s + t = n$).

2) Deduzca del lema de Nakayama que $\{\overline{p}_i\}$ y $\{\overline{q}_j\}$ se levantan a generadores $\{p_i\}$ y $\{q_j\}$ de P y Q respectivamente.

3) Demuestre que si $\{\overline{p}_i\} \cup \{\overline{q}_j\}$ son linealmente independientes sobre k, entonces $\{p_i\} \cup \{q_j\}$ son linealmente independientes sobre R y por ende forman bases libres.

   Sugerencia: considere la matriz en $M_n(k)$ formada por los vectores $\overline{p}_i$ y $\overline{q}_j$. Demuestre que si su determinante no es nulo, entonces el determinante de la matriz correspondiente en $M_n(R)$ formada por p_i y q_j es invertible en R.

(En general, un famoso teorema de Kaplansky nos dice que sobre un anillo local, *todos* los módulos proyectivos son libres, sin asumir que son finitamente generados.)

3.3 Módulos libres y finitamente generados

He aquí otra aplicación del teorema de Cayley–Hamilton.

3.8. Lema. *Sea M un R-módulo finitamente generado y sea $\alpha\colon M \to M$ un epimorfismo. Entonces, α es un isomorfismo.*

(Note que si R es un cuerpo, esto es un resultado bien conocido de álgebra lineal.)

Demostración. Podemos considerar M como un $R[T]$-módulo donde T actúa como α y el ideal (T) en $R[T]$. Tenemos $(T) \cdot M = M$, puesto que α es un epimorfismo. El teorema de Cayley–Hamilton aplicado al endomorfismo $\mathrm{id}\colon M \to M$ nos dice que existen $a_0, a_1, \ldots, a_{n-1} \in (T)$ tales que

$$\mathrm{id} + a_{n-1}\,\mathrm{id} + \cdots + a_1\,\mathrm{id} + a_0\,\mathrm{id} = 0.$$

Puesto que todos los a_i son divisibles por T, esto significa que existe un polinomio $p \in R[T]$ tal que para todo $m \in M$ se cumple

$$m = p(T)\,T \cdot m;$$

en otras palabras,

$$\mathrm{id}_M = p(\alpha) \circ \alpha = \alpha \circ p(\alpha).$$

Entonces, $p(\alpha) = \alpha^{-1}$. ■

3.9. Proposición. *Sea $M \cong R^{\oplus n}$ es un R-módulo libre.*

1) Toda colección de n elementos que genera a M forma una base libre de M.

*2) El número n está bien definido y se llama el **rango** de M.*

Demostración. Una elección de n generadores de M corresponde a un epimorfismo $\beta\colon R^{\oplus n} \twoheadrightarrow M$. Para probar que los generadores forman una base libre, necesitamos ver que β es un isomorfismo. La composición de un isomorfismo $\gamma\colon M \xrightarrow{\cong} R^{\oplus n}$ con β nos da un epimorfismo $\beta\circ\gamma\colon M \to M$. Por el resultado anterior, es un isomorfismo. Se sigue que $\beta = (\beta\circ\gamma)\circ\gamma^{-1}$ es también un isomorfismo, siendo la composición de dos isomorfismos. Esto demuestra 1).

Para la parte 2), supongamos que $R^{\oplus m} \cong R^{\oplus n}$ donde $m < n$. La base canónica de $R^{\oplus m}$ puede ser extendida a una colección de n elementos que generan a $R^{\oplus m}$, por ejemplo, añadiendo elementos nulos. Pero estos generadores no son linealmente independientes, lo que contradice a 1). ■

3.10. Comentario. Para anillos *no conmutativos* el rango de un módulo libre en general no está bien definido. Sea M un R-módulo no nulo tal que $M \oplus M \cong M$ (se puede tomar $R = k$ un cuerpo y $M = V$ un espacio vectorial de dimensión infinita). Entonces, para el anillo no conmutativo $A := \mathrm{End}_R(M)$ se tiene

$$A \oplus A = \mathrm{Hom}_R(M,M) \oplus \mathrm{Hom}_R(M,M) \cong \mathrm{Hom}_R(M, M\oplus M) \cong \mathrm{Hom}_R(M,M) \cong A.$$

4 Dependencia integral y normalización

Un elemento de una R-álgebra es **integral** sobre R si este satisface algún polinomio *mónico* con coeficientes en R. Es algo más restrictivo que dependencia integral (en la teoría de las extensiones algebraicas de cuerpos), cuando no se pide que el polinomio sea mónico. En esta sección vamos a investigar este concepto.

4.1. Proposición. *Sea R un anillo y sea $\mathfrak{a}$ un ideal en el anillo de polinomios $R[X]$. Denotemos por S la R-álgebra $R[X]/\mathfrak{a}$ y por s la imagen de X en el cociente.*

1) *S está generado por $\leq n$ elementos como un R-módulo si y solamente si $\mathfrak{a}$ contiene un polinomio mónico de grado $\leq n$. En este caso $1, s, \ldots, s^{n-1}$ son generadores de S.*

   En particular, S es un R-módulo finitamente generado si y solamente si $\mathfrak{a}$ contiene un polinomio mónico.

2) *S es un R-módulo libre de rango n si y solamente si $\mathfrak{a}$ puede ser generado por un polinomio mónico de grado n. En este caso $1, s, \ldots, s^{n-1}$ forman una base libre de S sobre R.*

Demostración. El R-módulo $R[X]$ está generado por $1, X, X^2, X^3, \ldots$, así que S está generado por $1, s, s^2, s^3, \ldots$ Ahora si $\mathfrak{a}$ contiene un polinomio mónico

$$p = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

entonces

$$s^n = -(a_{n-1} s^{n-1} + \cdots + a_1 s + a_0),$$

así que las potencias superiores de s se expresan en términos de combinaciones R-lineales de $1, s, \ldots, s^{n-1}$.

Viceversa, supongamos que S está generado por n elementos. Consideremos la multiplicación por s como un endomorfismo R-lineal $\phi\colon S \to S$. Tenemos $\phi(S) \subseteq R \cdot S$, así que el teorema de Cayley–Hamilton aplicado a ϕ nos dice que para algunos $a_0, a_1, \ldots, a_{n-1} \in R$ se cumple

$$(s^n + a_{n-1} s^{n-1} + \cdots + a_1 s + a_0) \cdot S = 0.$$

En particular, $s^n + a_{n-1} s^{n-1} + \cdots + a_1 s + a_0$ aniquila a $1 \in S$ y por lo tanto

$$s^n + a_{n-1} s^{n-1} + \cdots + a_1 s + a_0 = 0;$$

es decir, el polinomio mónico

$$p = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

pertenece a $\mathfrak{a}$. Esto demuestra la parte 1).

En la parte 2), si $\mathfrak{a} = (p)$ donde p es mónico de grado n, entonces, como acabamos de ver en 1), los elementos $1, s, \ldots, s^{n-1}$ generan a S como un R-módulo. Para ver que entre $1, s, \ldots, s^{n-1}$ no puede haber una relación R-lineal no trivial, notamos que si

$$c_{n-1} s^{n-1} + \cdots + c_1 s + c_0 = 0,$$

entonces

$$c_{n-1} X^{n-1} + \cdots + c_1 X + c_0 \in (p),$$

pero dado que p es mónico, los múltiplos no nulos de p son de grado $\geq n$: tenemos

$$(X^n + \cdots)\,(b_m X^m + \cdots) = b_m X^{n+m} + \cdots$$

Esto significa que $c_0 = c_1 = \cdots = c_{n-1} = 0$.

Viceversa, supongamos que S es un R-módulo libre de rango n. En particular, S tiene n generadores y por la parte 1) existe un polinomio mónico $p \in R[X]$ de grado n tal que $p \in \mathfrak{a}$. También por la parte 1), los elementos $1, s, \ldots, s^{n-1}$ generan a S como un R-módulo. Luego, como probamos en 3.9, estos elementos forman una base libre de S.

Vamos a probar que p genera al ideal $\mathfrak{a}$. Si $f \in \mathfrak{a}$ es otro polinomio, podemos escribir* $f = g\,p + q$, donde $\deg q < \deg p = n$. En particular, $q \in \mathfrak{a}$. Como arriba, q puede ser interpretado como una relación lineal entre $1, s, \ldots, s^{n-1}$. Pero estos elementos forman una base libre de S, y por ende $q = 0$. ■

4.2. Definición. Sea S una R-álgebra.

1) Si para $s \in S$ se tiene $p(s) = 0$ para algún polinomio mónico $p \in R[X]$, entonces se dice que s es un elemento **integral** sobre R. Si todos los elementos de S son integrales sobre R, se dice que S es un anillo **integral** sobre R.

2) El conjunto de los elementos de S que son integrales sobre R se llama la **cerradura integral** o la **normalización de R en S**.

3) En el caso particular cuando R es un dominio y $S = K(R)$ es su cuerpo cociente, la normalización de R en S se llama simplemente la **normalización** de R. Si R coincide con su normalización, se dice que R es un **dominio normal**.

El objetivo de esta sección es el siguiente resultado.

4.3. Teorema. *Sea S una R-álgebra. Entonces, la cerradura integral de R en S es una subálgebra de S. En particular, si S está generada como una R-álgebra por elementos integrales sobre R, entonces S es integral sobre R.*

Antes de probar el teorema, vamos a establecer un par de resultados auxiliares y ver un par de ejemplos.

4.4. Observación. *Todo anillo factorial es un dominio normal.*

Demostración. Sea R un anillo factorial. Hay que probar que todos los elementos del cuerpo de fracciones $K(R)$ que son integrales sobre R de hecho pertenecen a R. Para una fracción $\frac{r}{s}$ podemos suponer que r y s son coprimos. Si $\frac{r}{s}$ es integral sobre R, entonces hay una relación

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\frac{r}{s} + a_0 = 0.$$

Multiplicando esta ecuación por s^n, se obtiene

$$r^n + s\,a_{n-1}\,r^{n-1} + \cdots + s^{n-1}\,a_1\,r + s^n\,a_0 = 0.$$

Pero esto implica que $s \mid r$. Dado que r y s son coprimos, esto significa que necesariamente $s \in R^\times$ y $\frac{r}{s} \in R$. ■

4.5. Ejemplo. $\mathbb{Z}$ es un dominio normal. Los anillos de polinomios $k[X_1, \ldots, X_n]$ y $\mathbb{Z}[X_1, \ldots, X_n]$ son dominios normales. ▲

Como muchos otros conceptos en álgebra conmutativa, la noción de elementos integrales y normalización está motivada por la teoría de números algebraica.

---

* ¡Esto es posible puesto que p es mónico! Procedamos por inducción sobre $d := \deg f$. Si $d < n$, podemos tomar $g = 0$ y $q = f$. Para el paso inductivo, si $f = a_d\,X^d + a_{d-1}\,X^{d-1} + \cdots$, entonces $\deg(f - a_d\,X^{d-n}\,p) < d$ y por la hipótesis de inducción,

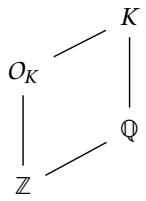
$$f - a_d\,X^{d-n}\,p = g\,p + q,$$

donde $\deg q < n$. Podemos escribir

$$f = (g + a_d\,X^{d-n})\,p + q.$$

Esta es la división larga habitual.

4.6. Definición. Si $K/\mathbb{Q}$ es una extensión finita, se dice que K es un **cuerpo de números**. La cerradura integral de $\mathbb{Z}$ en K se llama el **anillo de los enteros de** K y se denota por O_K.



En general, los elementos de la cerradura integral de $\mathbb{Z}$ en $\overline{\mathbb{Q}}$ se llaman los **enteros algebraicos**.

Ejercicio 26. Sea d un entero libre de cuadrados (positivo o negativo). Demuestre que

$$O_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{si } d \equiv 2,3 \mod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{si } d \equiv 1 \mod 4. \end{cases}$$

4.7. Definición. Si S es una R-álgebra que es finitamente generada como un R-módulo, entonces se dice que S es **finita** sobre S.

Ejercicio 27. Si S es una R-álgebra finita y M un S-módulo finitamente generado. Demuestre que M es finitamente generado como R-módulo.

4.8. Lema. *Una R-álgebra es finita sobre R si y solamente si S es generada como una R-álgebra por un número finito de elementos integrales sobre R.*

Demostración. Si S es finita sobre R, entonces para todo $s \in S$ la multiplicación por s es un endomorfismo R-lineal $\phi\colon S \to S$ y el teorema de Cayley–Hamilton aplicado a ϕ nos dice que s satisface un polinomio mónico en $R[X]$. (Ya vimos este argumento en 4.1.)

Viceversa, supongamos que S está generada como R-álgebra por elementos $x_1, \ldots, x_n \in S$ que son integrales sobre R. Procedamos por inducción sobre n. El caso de $n = 1$ ya lo analizamos en 4.1: si tenemos $S = R[x_1]$ donde x_1 es integral sobre R, entonces S es finitamente generado como un R-módulo. Para el paso inductivo, sea $S' := R[x_1, \ldots, x_{n-1}]$ la subálgebra de S generada por $x_1, \ldots, x_{n-1}$. Por la hipótesis de inducción, S' es un R-módulo finitamente generado. Luego, $S = S'[x_n]$, donde x_n es integral sobre R y por lo tanto es integral sobre S'. Esto significa que S es finitamente generado como un S'-módulo. Podemos deducir que S es finitamente generado como un R-módulo[*]. ■

El último resultado es suficiente para probar el teorema 4.3 cuando el anillo R es noetheriano.

Demostración de 4.3 bajo la hipótesis que R es noetheriano. Sea S una R-álgebra y sean $s, s' \in S$ dos elementos integrales sobre R. Está claro que $r \cdot s$ es también integral para cualesquiera $r \in R$: dada una relación mónica

$$s^n + a_{n-1}\, s^{n-1} + \cdots + a_1\, s + a_0 = 0$$

con $a_0, a_1, \ldots, a_{n-1} \in R$, tenemos

$$r^n\,(s^n + a_{n-1}\, s^{n-1} + \cdots + a_1\, s + a_0) = (rs)^n + r a_{n-1}\,(rs)^{n-1} + \cdots + r^{n-1} a_1\,(rs) + r^n a_0 = 0.$$

Lo que no está evidente es cómo a partir de relaciones mónicas para s y s' encontrar tales relaciones para $s \pm s'$ y ss'. Sin embargo, podemos usar el siguiente argumento implícito.

La subálgebra $R[s, s'] \subseteq S$ es finita según 4.8. Si R es noetheriano, entonces $R[s, s']$ es un R-módulo noetheriano (véase 0.39) y las subálgebras $R[s \pm s'], R[ss'] \subseteq R[s, s']$ son también finitas sobre R y por lo tanto $s \pm s'$ y ss' son integrales sobre R (usando 4.8 en la otra dirección). ■

[*] Si $\{s'_i\}$ son los generadores de S' como un R-módulo y $\{s_j\}$ son los generadores de S como un S'-módulo, entonces se ve que los productos $\{s'_i\, s_j\}$ generan a S como un R-módulo.

4.9. Ejemplo. Esto es el argumento que se usa normalmente para probar que los enteros algebraicos forman un anillo. Primero se demuestra que $\alpha \in \overline{\mathbb{Q}}$ es un entero algebraico si y solamente si $\mathbb{Z}[\alpha]$ es un grupo abeliano finitamente generado. Luego, para dos enteros algebraicos α y β el grupo $\mathbb{Z}[\alpha, \beta]$ es finitamente generado, y luego $\mathbb{Z}[\alpha \pm \beta]$ y $\mathbb{Z}[\alpha\beta]$ son finitamente generados, siendo sus subgrupos. ▲

Como suele pasar, aunque la hipótesis noetheriana simplifica las cosas, no es necesaria. Pero primero, necesitamos otro lema.

4.10. Lema. *Sea S una R-álgebra y $s \in S$. Las siguientes condiciones son equivalentes.*

1) *s es integral sobre R;*
2) *existe un S-módulo N y un R-submódulo finitamente generado $M \subseteq N$ que no se aniquila por ningún elemento no nulo de S tal que $sM \subseteq M$.*

Demostración. Si s es integral sobre R, entonces podemos tomar $N = S$ y $M = R[s] \subseteq S$. El último es un R-módulo finitamente generado según 4.1. Notamos que $1 \in R[s]$ no se aniquila por ningún elemento de S. Esto establece la implicación 1) ⇒ 2).

Para probar que 2) ⇒ 1), notamos que gracias a la hipótesis que $sM \subseteq M$, la multiplicación por s es un endomorfismo R-lineal $\phi\colon M \to M$. Podemos aplicar el teorema de Cayley–Hamilton para deducir que existe un polinomio mónico $p \in R[X]$ tal que $p(s) \cdot M = 0$. La hipótesis sobre M implica que $p(s) = 0$, así que s es integral sobre R. ■

Demostración de 4.3. Sea S una R-álgebra y sean $s, s' \in S$ dos elementos integrales sobre R. Queremos probar que $s \pm s'$ y ss' son también integrales sobre R. Consideremos los R-módulos $M := R[s]$ y $M' := R[s']$. Son finitamente generados por 4.1. Sea MM' el módulo generado por los productos mm' donde $m \in M$ y $m' \in M'$. Es también finitamente generado: basta tomar los productos de los generadores de M y M'. Luego,

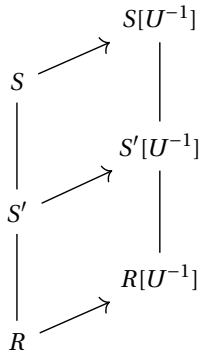
$$(s \pm s')MM' \subseteq sMM' + Ms'M' \subseteq MM' + MM' = MM'$$

y

$$ss'MM' = sMs'M' \subseteq MM'.$$

De 4.10 podemos concluir que $s \pm s'$ y ss' son integrales sobre R. ■

4.11. Proposición (Cerradura integral conmuta con la localización). *Sean $R \subseteq S$ anillos y sea $U \subseteq R$ un subconjunto multiplicativo. Si S' es la cerradura integral de R en S, entonces $S'[U^{-1}]$ es la cerradura integral de $R[U^{-1}]$ en $S[U^{-1}]$.*



Demostración. Los elementos de $S'[U^{-1}]$ son de la forma $\frac{s}{u}$ donde $s \in S$ es integral sobre R y $u \in U$. Una relación

$$s^n + a_{n-1}\, s^{n-1} + \cdots + a_1\, s + a_0 = 0$$

con $a_i \in R$ nos da una relación

$$\left(\frac{s}{u}\right)^n + \frac{a_{n-1}}{u}\left(\frac{s}{u}\right)^{n-1} + \cdots + \frac{a_1}{u^{n-1}}\,\frac{s}{u} + \frac{a_0}{u^n} = 0,$$

donde $\frac{a_i}{u^{n-i}} \in R[U^{-1}]$, así que todos los elementos de $S'[U^{-1}]$ son integrales sobre $R[U^{-1}]$. Viceversa, si un elemento $\frac{s}{u} \in S[U^{-1}]$ es integral sobre $R[U^{-1}]$, esto significa que hay una relación

$$\left(\frac{s}{u}\right)^n + \frac{a_{n-1}}{u_{n-1}}\left(\frac{s}{u}\right)^{n-1} + \cdots + \frac{a_1}{u_1}\,\frac{s}{u} + \frac{a_0}{u_0} = 0,$$

donde $a_i \in R$, $u_i \in U$. Multiplicando la ecuación de arriba por $(u\, u_0\, u_1 \cdots u_{n-1})^n$, se obtiene

$$\begin{aligned}(u_0\, u_1 \cdots u_{n-1}\, s)^n + a_{n-1}\, u\, u_0\, u_1 \cdots u_{n-2}\,(u_0\, u_1 \cdots u_{n-1}\, s)^{n-1} + \cdots \\ + a_1\, u^{n-1}\, u_0^{n-1}\, u_1^{n-2} \cdots u_{n-1}^{n-1}\,(u_0\, u_1 \cdots u_{n-1}\, s) + a_0\, u^n\, u_0^{n-1}\, u_1^n \cdots u_{n-1}^n = 0,\end{aligned}$$

lo que nos dice que $u_0\, u_1 \cdots u_{n-1}\, s$ es integral sobre R. Luego,

$$\frac{s}{u} = \frac{u_0\, u_1 \cdots u_{n-1}\, s}{u\, u_0\, u_1 \cdots u_{n-1}} \in S'[U^{-1}].$$

■

Ejercicio 28. Sea R un dominio. Demuestre que R es normal si y solamente si $R_{\mathfrak{m}}$ es normal para todo $\mathfrak{m} \in \operatorname{Specm} R$. (Indicación: use 1.22.)

4.1 Factorización de polinomios

El siguiente resultado fue conocido a Gauss: *si un polinomio mónico $f \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Z}[X]$, entonces es irreducible en $\mathbb{Q}[X]$*. Ahora vamos a ver una generalización.

4.12. Proposición. *Sean $R \subseteq S$ anillos y sea $f \in R[X]$ un polinomio mónico. Si f se factoriza en $S[X]$ como $g \cdot h$ donde g y h son polinomios mónicos, entonces los coeficientes de g y h son integrales sobre R.*

Demostración. Los polinomios g y h se factorizan en productos de polinomios lineales $X - \alpha$ en alguna extensión de anillos $T \supseteq S$. A saber, consideremos el anillo cociente $S[\alpha_1] := S[X]/(g)$. Denotemos por α_1 la imagen de X en el cociente. Luego, se tiene

$$g = (X - \alpha_1)\, g_1$$

donde $g_1 \in S[\alpha_1][X]$ y $\deg g_1 < \deg g$. En efecto, puesto que g es mónico, podemos dividirlo con resto por $X - \alpha$:

$$g = (X - \alpha)\, g_1 + q,$$

donde $q \in S[\alpha_1]$ es una constante. Pero $g = X - \alpha = 0$ en $S[\alpha_1][X]$, así que $q = 0$. Repitiendo este proceso, podemos concluir que

$$g = (X - \alpha_1) \cdots (X - \alpha_m)$$

y de la misma manera

$$h = (X - \beta_1) \cdots (X - \beta_n)$$

en $T[X]$ para alguna extensión apropiada $T \supseteq S$.

Puesto que

$$f = g \cdot h = (X - \alpha_1) \cdots (X - \alpha_m)\,(X - \beta_1) \cdots (X - \beta_n).$$

es un polinomio mónico con coeficientes en R y α_i, β_j son sus raíces, los elementos α_i, β_j son integrales sobre R. Los coeficientes de g y h se expresan como polinomios simétricos elementales en α_i y β_j, así que son también integrales sobre R. Por ejemplo, si

$$g = X^m + a_{m-1}\,X^{m-1} + \cdots + a_1\,X + a_0 = (X - \alpha_1) \cdots (X - \alpha_m),$$

entonces las **fórmulas de Vieta** nos dan

$$a_{m-k} = (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le m} \alpha_{i_1} \cdots \alpha_{i_k}.$$

■

4.13. Corolario. *Sea R un dominio normal y sea Q el cuerpo de fracciones de R. Entonces, todo polinomio mónico $f \in R[X]$ irreducible en $R[X]$ es también irreducible en $Q[X]$.*

Demostración. Supongamos que en $Q[X]$ se cumple $f = g \cdot h$. Si

$$g = a_m\,X^m + a_{m-1}\,X^{m-1} + \cdots, \quad h = b_n\,X^n + b_{n-1}\,X^{n-1} + \cdots,$$

entonces el grado de f es $m + n$ y su coeficiente mayor es $a_m\,b_n = 1$. Luego,

$$f = (b_n\,g) \cdot (a_m\,h),$$

donde $b_n\,g$ y $a_m\,h$ son polinomios mónicos en $Q[X]$. Por el resultado anterior, sus coeficientes son integrales sobre R, y por la hipótesis que R es un dominio normal, esto significa que $b_n\,g, a_m\,h \in R[X]$. Pero f es irreducible en $R[X]$, así que $b_n\,g$ o $a_m\,h$ es un polinomio constante en $R[X]$, y luego g o h es un polinomio constante en $Q[X]$. ■

4.14. Corolario. *Sea R un dominio normal. Entonces, todo polinomio mónico irreducible $f \in R[X]$ es primo.*

Demostración. Denotemos por Q el cuerpo de fracciones de R. Por el corolario de arriba, f es irreducible en $Q[X]$. Puesto que $Q[X]$ es un anillo factorial, esto implica que el ideal $fQ[X]$ es primo. El cociente $R[X]/(f)$ es un R-módulo libre (véase 4.1), así que la aplicación

$$R[X]/(f) \to Q \otimes_R (R[X]/(f)) \cong Q[X]/fQ[X]$$

es inyectiva. Ahora $Q[X]/fQ[X]$ es un dominio de integridad, puesto que $fQ[X]$ es un ideal primo, así que $R[X]/(f)$ es también un dominio de integridad y (f) es un ideal primo en $R[X]$. ■

4.2 Ideales primos en extensiones integrales

4.15. Lema. *Sea $R \subseteq S$ es una extensión integral de anillos (es decir, todo elemento de S es integral sobre R).*

1) *Para todo ideal $\mathfrak{a} \subset S$ el anillo cociente $S/\mathfrak{a}$ es integral sobre $R/(R \cap \mathfrak{a})$.*
2) *Para todo conjunto multiplicativo $U \subset R$ la localización $S[U^{-1}]$ es integral sobre $R[U^{-1}]$.*
3) *Si R y S son dominios, entonces el cuerpo de fracciones $K(S)$ es integral sobre $K(R)$, y en particular $K(S)/K(R)$ es una extensión algebraica.*

Demostración. En la parte 1), el anillo cociente $R/(R\cap\mathfrak{a})$ se identifica con un subanillo de $S/\mathfrak{a}$ de la siguiente manera. La proyección canónica $S \twoheadrightarrow S/\mathfrak{a}$ restringida a R nos da un homomorfismo $p\colon R \to S/\mathfrak{a}$. Luego, $p(R) \cong R/\ker p = R/(R\cap\mathfrak{a})$.

Para probar que $S/\mathfrak{a}$ es integral sobre $R/(R\cap\mathfrak{a})$, basta notar que todo elemento $\overline{s} \in S/\mathfrak{a}$ está representado por un elemento $s \in S$ tal que

$$s^n + a_{n-1}\, s^{n-1} + \cdots + a_1\, s + a_0 = 0$$

para algunos $a_0, a_1, \ldots, a_{n-1} \in R$. Al reducir la relación de arriba módulo $\mathfrak{a}$ se obtiene

$$\overline{s}^n + \overline{a_{n-1}}\,\overline{s}^{n-1} + \cdots + \overline{a_1}\,\overline{s} + \overline{a_0} = 0$$

donde $\overline{a_0}, \overline{a_1}, \ldots, \overline{a_{n-1}} \in R/(R\cap\mathfrak{a})$.

La parte 2) es un caso particular de 4.11 (se tiene $S' = S$).

En la parte 3), consideremos una fracción $\frac{s}{t} \in K(S)$. Por la hipótesis, s y t son integrales sobre R; en particular, se tiene

$$t^n + a_{n-1}\, t^{n-1} + \cdots + a_1\, t + a_0 = 0$$

para algunos $a_0, a_1, \ldots, a_{n-1} \in R$. Dividiendo esta ecuación por una potencia de t, se puede asumir que $a_0 \neq 0$. Luego, multiplicándola por $\frac{1}{a_0\, t^n}$, se obtiene

$$\frac{1}{a_0} + \frac{a_{n-1}}{a_0}\,\frac{1}{t} + \cdots + \frac{a_1}{a_0}\left(\frac{1}{t}\right)^{n-1} + \left(\frac{1}{t}\right)^n = 0$$

donde los coeficientes de $\left(\frac{1}{t}\right)^i$ están en $K(R)$. Entonces, $\frac{1}{t}$ es integral sobre $K(R)$, y $\frac{s}{t} = \frac{s}{1}\cdot\frac{1}{t}$ también lo es, siendo el producto de dos elementos integrales. ■

4.16. Comentario. Hay un momento sutil en la parte 1): una relación polinomial cualquiera

$$a_n\, s^n + a_{n-1}\, s^{n-1} + \cdots + a_1\, s + a_0 = 0$$

puede volverse trivial al reducirla módulo $\mathfrak{a}$ si $a_0, a_1, \ldots, a_n \in \mathfrak{a}$. Es importante que las relaciones sean *mónicas* con $a_n = 1$. Estas no se trivializan al pasar al cociente, salvo cuando $1 \in \mathfrak{a}$, pero en este caso $S/\mathfrak{a} = R/(R\cap\mathfrak{a}) = 0$ y todo se vuelve trivial.

4.17. Proposición ("Going up", Cohen–Seidenberg). *Sea $R \subseteq S$ una extensión integral de anillos.*

1) *Para un ideal primo $\mathfrak{p} \subset R$ existe un ideal primo $\mathfrak{q} \subset S$ tal que $R \cap \mathfrak{q} = \mathfrak{p}$.*
2) *Tal ideal $\mathfrak{q}$ puede ser escogido tal que $\mathfrak{q} \supseteq \mathfrak{a}$ para cualquier ideal fijo $\mathfrak{a} \subset S$ que satisface $R \cap \mathfrak{a} \subseteq \mathfrak{p}$.*

En este caso se dice que el ideal $\mathfrak{q}$ **está arriba de** $\mathfrak{p}$.

$$\begin{array}{ccccc} \mathfrak{a} & \subseteq & \mathfrak{q} & \subset & S \\ | & & | & & | \\ R\cap\mathfrak{a} & \subseteq & \mathfrak{p} & \subset & R \end{array}$$

4.18. Ejemplo. En la teoría de números algebraica se estudian las extensiones integrales $\mathbb{Z} \subseteq O_K$ (véase 4.6) y los ideales primos $\mathfrak{p} \subset O_K$ que están arriba de los primos $(p) \subset \mathbb{Z}$.

Por ejemplo, para $K = \mathbb{Q}(\sqrt{-1})$ tenemos $O_K = \mathbb{Z}[\sqrt{-1}]$. El ideal $\mathfrak{p} := (1+\sqrt{-1}) \subset \mathbb{Z}[\sqrt{-1}]$ es primo y está arriba de $(2) \subset \mathbb{Z}$ (note que $(1+\sqrt{-1})^2 = 2\sqrt{-1}$ donde $\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]^\times$, así que $\mathfrak{p}^2 = 2\mathbb{Z}[\sqrt{-1}]$). ▲

Demostración de 4.17. En la parte 2), si $\mathfrak{a} \subset S$, entonces tenemos

$$\operatorname{Spec} S/\mathfrak{a} \cong \{\mathfrak{q} \in \operatorname{Spec} S \mid \mathfrak{a} \subseteq \mathfrak{q}\}, \quad \operatorname{Spec} R/(R \cap \mathfrak{a}) \cong \{\mathfrak{p} \in \operatorname{Spec} R \mid R \cap \mathfrak{a} \subseteq \mathfrak{p}\},$$

así que pasando a los cocientes $S/\mathfrak{a}$ y $R/(R\cap\mathfrak{a})$ (donde $S/\mathfrak{a}$ es integral sobre $R/(R\cap\mathfrak{a})$, como notamos en 4.17), se puede asumir que $\mathfrak{a} = 0$ y la parte 2) se seguiría de la parte 1).

Para probar 1) podemos primero localizar R en $\mathfrak{p}$. A saber, consideremos el conjunto multiplicativo $U := R \setminus \mathfrak{p}$ y pasemos a las localizaciones $R_\mathfrak{p} := R[U^{-1}]$ y $S[U^{-1}]$. Según 4.17, la localización $S[U^{-1}]$ es integral sobre $R_\mathfrak{p}$. Recordemos que

$$\operatorname{Spec} S[U^{-1}] \cong \{\mathfrak{q} \in \operatorname{Spec} S \mid \mathfrak{q} \cap U = \emptyset\} = \{\mathfrak{q} \in \operatorname{Spec} S \mid R \cap \mathfrak{q} \subseteq \mathfrak{p}\}$$

y

$$\operatorname{Spec} R_\mathfrak{p} \cong \{\mathfrak{p}' \in \operatorname{Spec} R \mid \mathfrak{p}' \subseteq \mathfrak{p}\}.$$

De esta manera el resultado se reduce al caso cuando R es un anillo local y $\mathfrak{p}$ es su único ideal maximal. En este caso $\mathfrak{p}S \neq S$. En efecto, si $\mathfrak{p}S = S$, entonces

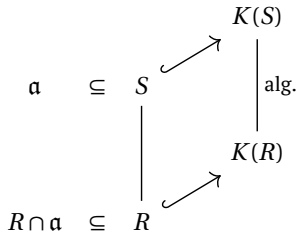
$$1 = s_1 x_1 + \cdots + s_n x_n$$

para algunos $s_1, \ldots, s_n \in S$ y $x_1, \ldots, x_n$. Los elementos $s_1, \ldots, s_n$ son integrales sobre R por la hipótesis, así que el álgebra $S' := R[s_1, \ldots, s_n]$ es un R-módulo finitamente generado según 4.8. Ahora $\mathfrak{p}S' = S'$, puesto que $1 \in S'$. Pero el lema de Nakayama (véase 3.3) implica que $S' = 0$. Contradicción.

Entonces, $\mathfrak{p}S \neq S$. Sea $\mathfrak{q}$ un ideal maximal en S que contiene a $\mathfrak{p}S$. En este caso $R \cap \mathfrak{q} \supseteq \mathfrak{p}$, y por la maximalidad $R \cap \mathfrak{q} = \mathfrak{p}$. ■

Si $R \subseteq S$ es una extensión integral, entonces, como notamos en 4.15, la extensión $K(S)/K(R)$ es algebraica. La última condición es menos restrictiva que pedir que S sea integral sobre R. En esta situación tenemos el siguiente resultado sobre los ideales en S y R.

4.19. Lema. *Sean $R \subseteq S$ dominios. Si el cuerpo de fracciones $K(S)$ es una extensión algebraica de $K(R)$, entonces todo ideal no nulo en S tiene intersección no nula con R.*



Demostración. Sea $x \in \mathfrak{a}$ un elemento no nulo. Por la hipótesis, se tiene

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

para algunos $a_0, a_1, \ldots, a_n \in K(R)$. Multiplicando esta ecuación por el común denominador de los coeficientes y dividiéndola por una potencia de x, se puede asumir que $a_0, a_1, \ldots, a_n \in R$ y $a_0 \neq 0$. Luego, $a_0 \in \mathfrak{a}$. ■

Usando este resultado, podemos probar que para una extensión integral $R \subseteq S$ y un ideal primo $\mathfrak{p} \subset R$ dos ideales primos en S que están arriba de $\mathfrak{p}$ son incomparables.

4.20. Corolario. *Sea $R \subseteq S$ una extensión integral de anillos. Sean $\mathfrak{q}, \mathfrak{q}' \subset S$ dos ideales primos diferentes tales que $R \cap \mathfrak{q} = R \cap \mathfrak{q}'$. Entonces, $\mathfrak{q}$ y $\mathfrak{q}'$ son **incomparables** (es decir, se tiene $\mathfrak{q} \not\subseteq \mathfrak{q}'$ y $\mathfrak{q}' \not\subseteq \mathfrak{q}$).*

Demostración. Vamos a probar que si $\mathfrak{q} \subseteq \mathfrak{q}' \subset S$ son ideales primos tales que $R \cap \mathfrak{q} = R \cap \mathfrak{q}'$, entonces $\mathfrak{q} = \mathfrak{q}'$. Pasando a los cocientes $R/(R \cap \mathfrak{q})$ y $S/\mathfrak{q}$, la situación se reduce al caso cuando S es un dominio, $\mathfrak{q} = 0$ y $\mathfrak{q}' \cap R = 0$. Aquí para justificar la reducción a los cocientes, otra vez usamos la parte 1) del lema 4.15. Por la parte 3) del mismo lema, el cuerpo de fracciones $K(S)$ es una extensión algebraica de $K(R)$. Por el lema 4.19, tenemos $\mathfrak{q}' = 0 = \mathfrak{q}$. ■

4.21. Corolario. *Si $R \subseteq S$ es una extensión integral de dominios, entonces S es un cuerpo si y solamente si R lo es.*

Demostración. Si R es un cuerpo y S es integral sobre S, entonces $K(S)/R$ es una extensión algebraica. Por el lema 4.19, todo ideal no nulo de S contiene un elemento no nulo de R. Pero los elementos no nulos de R son unidades.

Viceversa, supongamos que S es un cuerpo. Sea $\mathfrak{m}$ un ideal maximal de R. Según 4.17, existe un ideal primo $\mathfrak{q} \subset S$ tal que $R \cap \mathfrak{q} = \mathfrak{m}$. Pero siendo un cuerpo, S no tiene ideales propios no nulos, así que $\mathfrak{m} = (0)$ ■

Ejercicio 29. Sea S un anillo. Supongamos que un elemento $s \in S$ satisface una ecuación

$$a_n s^n + a_{n-1} s^{n-1} + \cdots + a_1 s + a_0 = 0.$$

Demuestre que si $a_0 \in S^\times$, entonces $s \in S^\times$. Use esta observación para obtener una prueba directa de 4.21.

4.22. Corolario. *Sea S una R-álgebra integral y sea $\mathfrak{p} \subset S$ un ideal primo. Entonces, $\mathfrak{p}$ es maximal si y solamente si el ideal $R \cap \mathfrak{p}$ es maximal en R.*

Demostración. Se sigue del resultado anterior al pasar a los cocientes $S/\mathfrak{p}$ y $R/(R \cap \mathfrak{p})$. ■

5 Anillos de Jacobson y el teorema de los ceros

En esta sección vamos a establecer una generalización del teorema de los ceros de Hilbert. Todo se basa en la siguiente noción.

5.1. Definición. Se dice que R es un **anillo de Jacobson**[*] si todo ideal primo de R es una intersección de ideales maximales. En otras palabras, se pide que para todo ideal primo $\mathfrak{p} \subset R$ se cumpla

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \in \operatorname{Specm} R \\ \mathfrak{m} \supseteq \mathfrak{p}}} \mathfrak{m}. \tag{5.1}$$

5.2. Ejemplo. Todo cuerpo es un anillo de Jacobson: en este caso el único ideal primo es (0). Un anillo local es de Jacobson si su ideal maximal es el único ideal primo. ▲

5.3. Ejemplo. El anillo de los enteros $\mathbb{Z}$ es de Jacobson: sus ideales primos no nulos (p) son maximales y el ideal nulo (0) es la intersección de todos los ideales maximales: 0 es el único número que es divisible por un número infinito de primos.

El anillo de polinomios en una variable $k[T]$ es de Jacobson por las mismas razones. Es un dominio de ideales principales y los ideales primos no nulos de $k[T]$ son de la forma (p) donde $p \in k[T]$ es un polinomio mónico irreducible. Puesto que $(p) \subseteq (q)$ equivale a $q \mid p$, todos estos ideales son maximales. El ideal primo (0) es la intersección de los ideales (p)[**]. ▲

5.4. Observación. *Si R es de Jacobson, entonces todo cociente $R/\mathfrak{a}$ es también de Jacobson.*

Demostración. Recordemos del ejercicio 6 que hay una biyección entre los ideales $\overline{\mathfrak{b}} \subseteq R/\mathfrak{a}$ y los ideales $\mathfrak{b} \subseteq R$ tales que $\mathfrak{b} \supseteq \mathfrak{a}$, dada por $\overline{\mathfrak{b}} := \mathfrak{b}/\mathfrak{a}$. Esta biyección preserva ideales primos, ideales maximales e intersecciones. Luego, si para todo ideal primo en R se cumple (5.1), entonces para todo ideal primo en $R/\mathfrak{a}$ se cumple (5.1). ■

Nos va a servir la siguiente caracterización.

5.5. Lema. *Sea R un anillo. Las siguientes condiciones son equivalentes.*

1) *R es de Jacobson;*
2) *Si $\mathfrak{p} \subset R$ es un ideal primo y el dominio $R/\mathfrak{p}$ contiene un elemento $x \neq 0$ tal que $(R/\mathfrak{p})[x^{-1}]$ es un cuerpo, entonces $R/\mathfrak{p}$ es un cuerpo.*

Demostración. 1) $\Rightarrow$ 2). Supongamos que R es de Jacobson. Sea $\mathfrak{p} \subset R$ un ideal primo. Entonces, el dominio $R/\mathfrak{p}$ es también de Jacobson. En particular, el ideal primo $(0) \subset R/\mathfrak{p}$ es una intersección de ideales maximales en $R/\mathfrak{p}$, y luego

$$\bigcap_{\mathfrak{m} \in \operatorname{Specm} R/\mathfrak{p}} \mathfrak{m} = (0). \tag{5.2}$$

Sea $x \in R/\mathfrak{p}$ un elemento tal que $(R/\mathfrak{p})[x^{-1}]$ es un cuerpo. Tenemos entonces

$$\{(0)\} = \operatorname{Spec}(R/\mathfrak{p})[x^{-1}] \cong \{\mathfrak{q} \in \operatorname{Spec} R/\mathfrak{p} \mid x \notin \mathfrak{q}\}.$$

Esto significa que si $\mathfrak{q} \subset R/\mathfrak{p}$ es un ideal primo no nulo, entonces $x \in \mathfrak{q}$. Pero (5.2) implica que (0) es un ideal maximal en $R/\mathfrak{p}$ y es un cuerpo.

[*] Nathan Jacobson (1910–1999), algebrista estadounidense.

[**] En $k[T]$ hay un número infinito de polinomios mónicos irreducibles por la misma razón que en $\mathbb{Z}$ hay un número infinito de primos: si $p_1, \ldots, p_n$ son polinomios mónicos irreducibles, entonces $p_1 \cdots p_n + 1$ es mónico y no es divisible por $p_1, \ldots, p_n$. Este argumento pertenece a Euclides.

2) $\Rightarrow$ 1). Sea R un anillo que satisface la propiedad 2). Para un ideal primo $\mathfrak{q} \subset R$ consideremos

$$\mathfrak{a} := \bigcap_{\substack{\mathfrak{m} \in \operatorname{Specm} R \\ \mathfrak{m} \supseteq \mathfrak{q}}} \mathfrak{m}.$$

Vamos a probar que $\mathfrak{a} = \mathfrak{q}$. Supongamos que $\mathfrak{q} \subsetneq \mathfrak{a}$. Sea $x \in \mathfrak{a} \setminus \mathfrak{q}$. Por el lema de Zorn, existe un ideal primo $\mathfrak{p} \subset R$ que es maximal entre los ideales primos tales que $\mathfrak{p} \supseteq \mathfrak{q}$ y $x \notin \mathfrak{p}$. Notamos que puesto que $x \in \mathfrak{a}$, para todo ideal maximal $\mathfrak{m}$ tal que $\mathfrak{m} \supseteq \mathfrak{p} \supseteq \mathfrak{q}$ se tiene $x \in \mathfrak{m}$, así que $\mathfrak{p}$ no es un ideal maximal en R y el cociente $R/\mathfrak{p}$ no es un cuerpo. Sin embargo, el ideal $\mathfrak{p}R[x^{-1}]$ es maximal en la localización $R[x^{-1}]$ por la elección de $\mathfrak{p}$:

$$\operatorname{Spec} R[x^{-1}] \cong \{\mathfrak{p}' \in \operatorname{Spec} R \mid x \notin \mathfrak{p}'\}.$$

Luego,

$$R[x^{-1}]/\mathfrak{p}R[x^{-1}] \cong (R/\mathfrak{p})[x^{-1}]$$

es un cuerpo. Pero la propiedad 2) implica que $R/\mathfrak{p}$ es un cuerpo. Contradicción. ■

En particular, si en el lema de arriba R es un dominio y $\mathfrak{p} = (0)$, se obtiene lo siguiente.

5.6. Corolario. *Sea R un dominio de Jacobson. Si $R[x^{-1}]$ es un cuerpo para algún $x \in R$, entonces R es un cuerpo.*

Ejercicio 30. Hemos visto en 1.25 que

$$N(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$$

es el **nilradical** de R. De modo similar, definamos el **radical de Jacobson** por

$$J(R) := \bigcap_{\mathfrak{m} \in \operatorname{Specm} R} \mathfrak{m}.$$

Demuestre que las siguientes condiciones son equivalentes.

1) R es un anillo de Jacobson.
2) Para todo ideal $\mathfrak{a} \subseteq R$ se cumple $N(R/\mathfrak{a}) = J(R/\mathfrak{a})$.
3) Para todo ideal primo $\mathfrak{p} \subset R$ se cumple $N(R/\mathfrak{p}) = J(R/\mathfrak{p})$.

Estamos listos para probar el resultado principal de esta sección.

5.7. Teorema (Teorema de los ceros, versión general). *Sea R un anillo de Jacobson y sea S una R-álgebra finitamente generada. Entonces,*

1) S es también un anillo de Jacobson;

2) si $\mathfrak{m} \subset S$ es un ideal maximal, entonces $R \cap \mathfrak{m}$[*] es un ideal maximal en R y el cuerpo $S/\mathfrak{m}$ es una extensión finita de $R/(R \cap \mathfrak{m})$.

Demostración. Empecemos por el caso muy particular cuando $R = k$ es un cuerpo y $S = k[T]$ es el anillo de polinomios en una variable. Ya notamos en 5.3 que $k[T]$ es de Jacobson. Para la segunda parte, basta notar que si $\mathfrak{m} = (f) \subset k[T]$ es un ideal maximal, entonces $k \cap (f) = (0)$ y $k[T]/(f)$ es una extensión finita de k.

Ahora supongamos que S está generada como una R-álgebra por un elemento $s \in S$. Según el lema 5.5, para probar que S es de Jacobson, basta probar que si $\mathfrak{p} \subset S$ es primo y $(S/\mathfrak{p})[x^{-1}]$ es un cuerpo para algún $x \in S/\mathfrak{p}$, entonces $S/\mathfrak{p}$ es un cuerpo.

[*] Recordemos que una R-álgebra S es un homomorfismo de anillos $\alpha\colon R \to S$ y "$R \cap \mathfrak{m}$" denota el ideal $\alpha^{-1}(\mathfrak{m}) \subseteq R$.

Pasemos de S y R a los cocientes $S/\mathfrak{p}$ y $R/(R\cap\mathfrak{p})$. Notamos que $R\cap\mathfrak{p} := \alpha^{-1}(\mathfrak{p})$ es un ideal primo, siendo la preimagen de un ideal primo[*]. De esta manera el problema se reduce al caso cuando $R \subseteq S$ son dominios y hay que probar que si $S[x^{-1}]$ es un cuerpo, entonces S es un cuerpo. De hecho, vamos a probar que en este caso R es también un cuerpo y S es una extensión finita de R, lo que establece la parte 2) a la vez.

Tenemos $S \cong R[T]/\mathfrak{q}$ donde $\mathfrak{q} \subset R[T]$ es algún ideal primo; el generador $s \in S$ es la imagen de T en el cociente. Denotemos por k el cuerpo de fracciones de R. Si $S[x^{-1}]$ es un cuerpo, entonces

$$S[x^{-1}] = (R[T]/\mathfrak{q})[x^{-1}] = (k[T]/\mathfrak{q}k[T])[x^{-1}] = k[T]/\mathfrak{q}k[T].$$

Notamos que necesariamente $\mathfrak{q} \neq 0$, puesto que $k[T]$ no es un cuerpo. En este caso $k[T]/\mathfrak{q}k[T]$ es una extensión finita de k.

Para un polinomio no nulo

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathfrak{q}$$

donde $a_n \neq 0$ se tiene

$$a_n s^n + a_{n-1} s^{n-1} + \cdots + a_1 s + a_0 = 0.$$

Podemos dividir esta ecuación por a_n y concluir que $S[a_n^{-1}]$ es integral sobre $R[a_n^{-1}]$. En particular, $x \in S$ satisface alguna relación

$$x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 = 0$$

donde $b_0, b_1, \ldots, b_{m-1} \in R[a_n^{-1}]$. Podemos asumir que $b_0 \neq 0$ (en el caso contrario basta dividir la ecuación por una potencia de x: esto tiene sentido, puesto que $x \neq 0$ y $S[a_n^{-1}]$ es un dominio de integridad). Dividiendo esta ecuación por $\frac{1}{b_0 x^m}$, podemos concluir que el cuerpo $S[x^{-1}]$ es una extensión integral de $R[(a_n b_0)^{-1}] = R[a_n^{-1}][b_0^{-1}]$:

$$\frac{1}{b_0} + \frac{b_{m-1}}{b_0}\frac{1}{x} + \cdots + \frac{b_1}{b_0}\left(\frac{1}{x}\right)^{m-1} + \left(\frac{1}{x}\right)^m = 0.$$

Pero 4.21 implica que $R[(a_n b_0)^{-1}]$ es también un cuerpo. Puesto que R es de Jacobson, podemos concluir que R es un cuerpo. De nuevo, gracias a 4.21, el hecho de que $S[a_n^{-1}] = S$ sea integral sobre el cuerpo $R[a_n^{-1}] = R$ implica que S es un cuerpo.

Acabamos de probar el teorema bajo la hipótesis que S está generada por un elemento como R-álgebra. Para el caso general, se puede proceder por inducción. Supongamos que $S = R[s_1, \ldots, s_n]$. La base de inducción es $n = 1$. Supongamos que el teorema se cumple para $n-1$ generadores. Entonces,

$$R[s_1, \ldots, s_n] \cong R[s_1, \ldots, s_{n-1}][s_n]$$

es una álgebra generada por un elemento s_n sobre el anillo de Jacobson $R[s_1, \ldots, s_{n-1}]$, y por ende es de Jacobson.

La parte 2) se demuestra de la misma manera. Si $\mathfrak{m} \subset R[s_1, \ldots, s_n] \cong R[s_1, \ldots, s_{n-1}][s_n]$ es un ideal maximal, entonces podemos escribir

$$R \cap \mathfrak{m} = R \cap (R[s_1, \ldots, s_{n-1}] \cap \mathfrak{m}).$$

Aquí el ideal $R[s_1, \ldots, s_{n-1}] \cap \mathfrak{m}$ es maximal en $R[s_1, \ldots, s_{n-1}]$ por el caso de $n = 1$. Luego, por la hipótesis de inducción, $R \cap \mathfrak{m}$ es maximal en R. ■

Ahora vamos a explicar la relación del último teorema con el teorema de los ceros clásico. Nos bastará el siguiente caso particular.

5.8. Corolario. *Sea k un cuerpo. Si $\mathfrak{m}$ es un ideal maximal en $k[X_1, \ldots, X_n]$, entonces $k[X_1, \ldots, X_n]/\mathfrak{m}$ es una extensión finita de k. En particular, si k es un cuerpo algebraicamente cerrado, entonces $k[X_1, \ldots, X_n]/\mathfrak{m} \cong k$.*

[*] Esto siempre se cumple para cualquier homomorfismo de anillos. Estamos tratando de probar que bajo las hipótesis del teorema, el ideal $\alpha^{-1}(\mathfrak{m}) \subset R$ es maximal para todo ideal maximal $\mathfrak{m} \subset S$.

Demostración. k es un anillo de Jacobson y $k[X_1,\dots,X_n]$ es una k-álgebra finitamente generada. Tenemos $k\cap\mathfrak{m}=(0)$, y podemos aplicar la parte 2) de 5.7. ■

Recordemos alguna notación de geometría algebraica elemental. Sea k un cuerpo. Por $\mathbb{A}^n(k) := k^n$ se denota el espacio afín de dimensión n sobre k. Para un ideal $\mathfrak{a}\subseteq k[X_1,\dots,X_n]$ el **conjunto algebraico** correspondiente es el conjunto de los ceros comunes de los polinomios de $\mathfrak{a}$:

$$V(\mathfrak{a}) := \{x\in\mathbb{A}^n(k) \mid f(x)=0 \text{ para todo } f\in\mathfrak{a}\}\subseteq\mathbb{A}^n(k).$$

Para un subconjunto $X\subset\mathbb{A}^n(k)$ se puede considerar el ideal formado por los polinomios que se anulan en X:

$$I(X) := \{f\in k[X_1,\dots,X_n] \mid f(x)=0 \text{ para todo } x\in X\}.$$

5.9. Observación. *Para todo punto $x=(x_1,\dots,x_n)\in\mathbb{A}^n(k)$ el ideal*

$$\mathfrak{m}_x := (X_1-x_1,\dots,X_n-x_n)$$

es maximal en $k[X_1,\dots,X_n]$.

Demostración. Consideremos el homomorfismo de evaluación en x

$$\begin{aligned} ev_x\colon k[X_1,\dots,X_n] &\twoheadrightarrow k,\\ f &\mapsto f(x).\end{aligned}$$

El núcleo de este homomorfismo es $\mathfrak{m}_x$, y luego

$$k[X_1,\dots,X_n]/\mathfrak{m}_x\cong k.$$

■

En general, no todos los ideales maximales de $k[X_1,\dots,X_n]$ son de la forma $\mathfrak{m}_x$. Por ejemplo, el ideal (X^2+1) es maximal en $\mathbb{R}[X]$, dado que $\mathbb{R}[X]/(X^2+1)\cong\mathbb{C}$. Sin embargo, si trabajamos sobre un cuerpo algebraicamente cerrado, esto es cierto.

5.10. Proposición. *Sea k un cuerpo algebraicamente cerrado. Entonces, hay una biyección natural*

$$\mathbb{A}^n(k)\cong \operatorname{Specm} k[X_1,\dots,X_n]$$

dada por $x\mapsto\mathfrak{m}_x$.

Demostración. Sea $\mathfrak{m}\subset k[X_1,\dots,X_n]$ un ideal maximal. Luego, según 5.8 hay un isomorfismo

$$k[X_1,\dots,X_n]/\mathfrak{m}\cong k.$$

Consideremos la composición

$$\phi\colon k[X_1,\dots,X_n]\twoheadrightarrow k[X_1,\dots,X_n]/\mathfrak{m}\xrightarrow{\cong} k.$$

Para $x := (\phi(X_1),\dots,\phi(X_n))$ se tiene

$$\mathfrak{m}_x\subseteq\ker\phi=\mathfrak{m},$$

y luego $\mathfrak{m}_x=\mathfrak{m}$ por la maximalidad de $\mathfrak{m}_x$. ■

5.11. Corolario. *Sea k un cuerpo algebraicamente cerrado y sea $X\subseteq\mathbb{A}^n(k)$ un conjunto algebraico. Entonces, hay una biyección natural*

$$X\cong \operatorname{Specm} k[X_1,\dots,X_n]/I(X)$$

dada por $x\mapsto\overline{\mathfrak{m}_x}$.

Demostración. Para $x \in \mathbb{A}^n(k)$ consideremos el homomorfismo de evaluación

$$\phi\colon k[X_1,\dots,X_n] \twoheadrightarrow k[X_1,\dots,X_n]/\mathfrak{m}_x \xrightarrow{\cong} k.$$

Notamos que $x \in X$ si y solamente si $\phi(f) = 0$ para todo $f \in I(X)$; es decir, si y solamente si $\mathfrak{m}_x \supseteq I(X)$. Como acabamos de ver, todos los ideales maximales de $k[X_1,\dots,X_n]$ son de la forma $\mathfrak{m}_x$ para algún $x \in \mathbb{A}^n(k)$. Entonces,

$$X \cong \{\mathfrak{m} \in \operatorname{Specm} k[X_1,\dots,X_n] \mid \mathfrak{m} \supseteq I(X)\} \cong \operatorname{Specm} k[X_1,\dots,X_n]/I(X).$$

■

5.12. Corolario. *Sea k es un cuerpo algebraicamente cerrado. Entonces, para todo ideal $\mathfrak{a} \subseteq k[X_1,\dots,X_n]$ se tiene*

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}},$$

donde $\sqrt{\mathfrak{a}}$ es el radical de $\mathfrak{a}$ (véase 1.24).

Demostración. Tenemos

$$V(\mathfrak{a}) \cong \{\mathfrak{m} \in \operatorname{Specm} k[X_1,\dots,X_n] \mid \mathfrak{m} \supseteq \mathfrak{a}\},$$

y luego

$$I(V(\mathfrak{a})) = \bigcap_{\substack{\mathfrak{m}\in\operatorname{Specm} k[X_1,\dots,X_n] \\ \mathfrak{m}\supseteq\mathfrak{a}}} \mathfrak{m}.$$

Pero $k[X_1,\dots,X_n]$ es un anillo de Jacobson, entonces todo ideal primo $\mathfrak{p} \subset k[X_1,\dots,X_n]$ es una intersección de ideales maximales, y por ende

$$\bigcap_{\substack{\mathfrak{m}\in\operatorname{Specm} k[X_1,\dots,X_n] \\ \mathfrak{m}\supseteq\mathfrak{a}}} \mathfrak{m} = \bigcap_{\substack{\mathfrak{p}\in\operatorname{Spec} k[X_1,\dots,X_n] \\ \mathfrak{p}\supseteq\mathfrak{a}}} \mathfrak{p} = \sqrt{\mathfrak{a}}.$$

El último paso usa la caracterización del radical que establecimos 1.25. ■

Los resultados 5.10, 5.11, 5.12 son diverentes versiones del **teorema de los ceros de Hilbert**. El punto clave de las pruebas es el corolario 5.8 de 5.7. En este sentido 5.7 es una versión generalizada del teorema de los ceros.

6 Lema de Artin–Rees

6.1. Definición. Sean R un anillo, $\mathfrak{a} \subseteq R$ un ideal y M un R-módulo. Una $\mathfrak{a}$**-filtración** de M es una cadena de submódulos

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

donde $\mathfrak{a}M_n \subseteq M_{n+1}$ para todo $n \geq 0$.

Para un submódulo $M' \subseteq M$ la $\mathfrak{a}$-filtración **inducida** sobre M' viene dada por

$$M' = M'_0 \supseteq M'_1 \supseteq M'_2 \supseteq \cdots$$

donde $M'_n := M' \cap M_n$. Notamos que

$$\mathfrak{a}M'_n = \mathfrak{a}(M' \cap M_n) \subseteq M' \cap \mathfrak{a}M_n \subseteq M' \cap M_{n+1} =: M'_{n+1},$$

así que esto es también una $\mathfrak{a}$-filtración.

Un caso particular de interés es la **filtración** $\mathfrak{a}$**-ádica** donde $M_n := \mathfrak{a}^n M$ y se cumple $\mathfrak{a}M_n = M_{n+1}$. Para un submódulo $M' \subseteq M$ la filtración inducida sobre M' no tiene por qué ser la filtración $\mathfrak{a}$-ádica: es posible que $\mathfrak{a}M'_n \subsetneq M'_{n+1}$. Sin embargo, bajo ciertas condiciones de finitud, esto no está lejos de realidad: lo que se preserva es la *estabilidad*: las igualdades $\mathfrak{a}M'_n = M'_{n+1}$ se van a cumplir para n suficientemente grande.

6.2. Definición. Se dice que una $\mathfrak{a}$-filtración

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

es **estable** si $\mathfrak{a}M_n = M_{n+1}$ para todo n suficientemente grande.

6.3. Teorema (El lema de Artin–Rees). *Sean R un anillo noetheriano, $\mathfrak{a} \subseteq R$ un ideal, M un R-módulo finitamente generado y*

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

una $\mathfrak{a}$-filtración estable. Luego, para todo submódulo $M' \subseteq M$ la filtración inducida

$$M' = M'_0 \supseteq M'_1 \supseteq M'_2 \supseteq \cdots, \quad M'_n := M' \cap M_n$$

es también estable.

Para probarlo, vamos a usar una construcción auxiliar. Recordemos que R es un **anillo graduado** si se tiene una descomposición en una suma directa de grupos abelianos

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$$

que satisface $R_m R_n \subseteq R_{m+n}$ para todo $m, n \geq 0$. Un ejemplo típico es el anillo de polinomios $R[t]$ donde la graduación viene dada por

$$R[t]_n := R\langle t^n \rangle.$$

Un R**-módulo graduado** es un R-módulo M junto con una descomposición en una suma directa de grupos abelianos

$$M = M_0 \oplus M_1 \oplus M_2 \oplus \cdots$$

tal que $R_m M_n \subseteq M_{m+n}$ para todo $m, n \geq 0$.

En particular, todo elemento $x \in M$ puede ser expresado de modo único como una suma finita de elementos $x_n \in M_n$, llamados las **componentes homogéneas** de x.

6.4. Definición. Sean R un anillo, $\mathfrak{a} \subseteq R$ un ideal, M un R-módulo y

$$\mathcal{J}\colon M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

una $\mathfrak{a}$-filtración. Consideremos el anillo graduado

$$B_{\mathfrak{a}}R := R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \cdots$$

y pongamos

$$B_{\mathcal{J}}M := M \oplus M_1 \oplus M_2 \oplus \cdots$$

Este es un $B_{\mathfrak{a}}R$-módulo graduado: dado que $\mathcal{J}$ es una $\mathfrak{a}$-filtración, se cumple $\mathfrak{a}^m M_n \subseteq M_{m+n}$.

El módulo graduado $B_{\mathcal{J}}M$ detecta estabilidad de la filtración en el siguiente sentido.

6.5. Lema. *Sean R un anillo, $\mathfrak{a} \subseteq R$ un ideal, M un R-módulo finitamente generado y*

$$\mathcal{J}\colon M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

una $\mathfrak{a}$-filtración donde M_n son submódulos finitamente generados. Luego, la filtración es estable si y solo si $B_{\mathcal{J}}M$ es un $B_{\mathfrak{a}}R$-módulo finitamente generado.

Demostración. Supongamos que $B_{\mathcal{J}}M$ es finitamente generado. Entonces, los generadores pertenecen a los primeros n términos de la suma directa para n suficientemente grande:

$$M \oplus M_1 \oplus M_2 \oplus \cdots \oplus M_n.$$

Tomando las componentes homogéneas de los generadores, podemos concluir que $B_{\mathcal{J}}M$ está generado por un número finito de los elementos de M_i para $i \leq n$. Luego, por la hipótesis, el resto de la suma directa

$$M_n \oplus M_{n+1} \oplus M_{n+2} \oplus M_{n+3} \oplus \cdots$$

está generado como $B_{\mathfrak{a}}R$-módulo por los elementos de M_n, lo que significa que

$$M_{n+i} = \mathfrak{a}^i M_n \quad \text{para todo } i \geq 0. \tag{6.1}$$

Esto precisamente quiere decir que la filtración es estable.

Viceversa, si la filtración es estable, entonces existe n tal que se cumple (6.1). Luego, la unión de los generadores de $M_0, M_1, \ldots, M_n$ genera a $B_{\mathcal{J}}M$ como un $R_{\mathfrak{a}}$-módulo. ■

Demostración del lema de Artin–Rees 6.3. Denotemos por $\mathcal{J}$ la filtración sobre M y por $\mathcal{J}'$ la filtración inducida sobre M'. Notamos que $B_{\mathfrak{a}}R$ es una R-álgebra finitamente generada, y puesto que R es un anillo noetheriano por nuestra hipótesis, $B_{\mathfrak{a}}R$ es también un anillo noetheriano.

Ahora, si $\mathcal{J}$ es una filtración estable, entonces $B_{\mathcal{J}}M$ es un $B_{\mathfrak{a}}R$-módulo finitamente generado, y luego $B_{\mathcal{J}'}M'$ es también un $B_{\mathfrak{a}}R$-módulo finitamente generado, siendo un submódulo de $B_{\mathcal{J}}M$. Lo último significa que la filtración $\mathcal{J}'$ es estable. ■

Más adelante nos va a servir el siguiente caso particular.

6.6. Corolario. *Sean R un anillo noetheriano, $\mathfrak{a} \subseteq R$ un ideal, M un R-módulo finitamente generado y $M' \subseteq M$ un submódulo. Entonces, para todo $n \geq 0$ existe $t \geq 0$ tal que*

$$M' \cap \mathfrak{a}^t M \subseteq \mathfrak{a}^n M'.$$

Demostración. Consideremos la filtración $\mathfrak{a}$-ádica sobre M:

$$M \supseteq \mathfrak{a}M \supseteq \mathfrak{a}^2 M \supseteq \mathfrak{a}^3 M \supseteq \cdots$$

El lema de Artin–Rees nos dice que la filtración inducida sobre M' es estable; es decir,

$$\mathfrak{a}(M' \cap \mathfrak{a}^m M) = M' \cap \mathfrak{a}^{m+1} M$$

para m suficientemente grande. Luego, para todo $n \geq 0$

$$M' \cap \mathfrak{a}^{m+n} M = \mathfrak{a}^n (M' \cap \mathfrak{a}^m M) \subseteq \mathfrak{a}^n M'.$$

■

6.1 El teorema de intersección de Krull

He aquí un corolario importante del lema de Artin–Rees.

6.7. Teorema (El teorema de intersección de Krull). *Sean R un anillo noetheriano y $\mathfrak{a} \subseteq R$ un ideal.*

1) *Si M es un R-módulo finitamente generado, entonces existe $x \in \mathfrak{a}$ tal que*

$$(1-x) \cdot \left(\bigcap_{j \geq 1} \mathfrak{a}^j M \right) = 0.$$

2) *Si R es un dominio o un anillo local y $\mathfrak{a} \neq R$ es un ideal propio, entonces*

$$\bigcap_{j \geq 1} \mathfrak{a}^j = 0.$$

Demostración. Consideremos la filtración $\mathfrak{a}$-ádica sobre M:

$$M \supseteq \mathfrak{a}M \supseteq \mathfrak{a}^2 M \supseteq \mathfrak{a}^3 M \supseteq \cdots.$$

La filtración inducida sobre el submódulo $M' := \bigcap_{j \geq 1} \mathfrak{a}^j M$ viene dada por

$$M'_n := \left(\bigcap_{j \geq 1} \mathfrak{a}^j M \right) \cap \mathfrak{a}^n M = M' \text{ para todo } n \geq 0.$$

El lema de Artin–Rees nos dice que esta filtración es estable, lo que significa simplemente que $\mathfrak{a}M' = M'$. Dado que M' es un R-módulo finitamente generado (usando la hipótesis que R es noetheriano y M es finitamente generado), esto nos permite concluir que existe $x \in \mathfrak{a}$ tal que $(1-x) \cdot M' = 0$ (lo probamos en 3.2 usando el teorema de Cayley–Hamilton). Esto establece la parte 1).

Ahora en la parte 2), basta tomar $M = R$. Sabemos que existe $x \in \mathfrak{a}$ tal que

$$(1-x) \cdot \left(\bigcap_{j \geq 1} \mathfrak{a}^j \right) = 0.$$

Dado que $\mathfrak{a}$ es un ideal propio, $x \neq 1$. Si R es un dominio, esto es suficiente para concluir que $\bigcap_{j \geq 1} \mathfrak{a}^j = 0$. Si R es un anillo local, entonces $x \in \mathfrak{a} \subsetneq R$ debe pertenecer al ideal maximal $\mathfrak{m}$ y luego $1 - x \in R^\times$ y también podemos concluir que $\bigcap_{j \geq 1} \mathfrak{a}^j = 0$. ■

Ejercicio 31. Sea R el **anillo de los gérmenes** en 0 de las $\mathcal{C}^\infty$-funciones $f : \mathbb{R} \to \mathbb{R}$. Específicamente, R es el cociente del anillo $\mathcal{C}^\infty(\mathbb{R})$ por la relación de equivalencia

$$f \sim g \iff f|_U = g|_U \text{ para algún entorno abierto } U \ni 0.$$

1) Demuestre que R es un anillo local y su ideal maximal $\mathfrak{m}$ está generado por la función x.

2) Demuestre que para la función $f(x) := e^{-1/x^2}$ se tiene $f \in \bigcap_{j\geq 0} \mathfrak{m}^j$, aunque $f \neq 0$ en R.

Este es un contraejemplo para el teorema de intersección de Krull en el caso de anillos que no son noetherianos.

7 Criterios de planitud

En esta sección vamos a ver algunos criterios de planitud de módulos. Recordemos que se dice que un R-módulo N es **plano** si para toda sucesión exacta corta de R-módulos

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

el producto tensorial con N induce una sucesión exacta corta

$$0 \to M' \otimes_R N \xrightarrow{i\otimes \mathrm{id}} M \otimes_R N \xrightarrow{p\otimes \mathrm{id}} M'' \otimes_R N \to 0$$

En general, si N no es plano, $i \otimes \mathrm{id}$ no siempre será una aplicación inyectiva; lo que se tiene es una sucesión exacta *larga*

$$\cdots \longrightarrow \mathrm{Tor}_n^R(M', N) \longrightarrow \mathrm{Tor}_n^R(M, N) \longrightarrow \mathrm{Tor}_n^R(M'', N) \longrightarrow$$
$$\mathrm{Tor}_{n-1}^R(M', N) \longrightarrow \mathrm{Tor}_{n-1}^R(M, N) \longrightarrow \mathrm{Tor}_{n-1}^R(M'', N) \longrightarrow \cdots$$

$$\cdots \longrightarrow \mathrm{Tor}_1^R(M', N) \longrightarrow \mathrm{Tor}_1^R(M, N) \longrightarrow \mathrm{Tor}_1^R(M'', N) \longrightarrow$$
$$M' \otimes_R N \longrightarrow M \otimes_R N \longrightarrow M'' \otimes_R N \longrightarrow 0$$

Para la construcción de $\mathrm{Tor}_n^R(-,-)$ y sus propiedades, véanse por ejemplo mis apuntes

cadadr.org/san-salvador/2018-08-algebra-conmutativa/resoluciones-y-tor.pdf

7.1 Planitud y $\mathrm{Tor}_1^R(R/\mathfrak{a}, M)$

7.1. Teorema. *Sea R un anillo y M un R-módulo. Las siguientes condiciones son equivalentes.*

1) *M es plano.*
2) *Para todo ideal $\mathfrak{a} \subseteq R$ la aplicación*

$$\mathfrak{a} \otimes_R M \to R \otimes_R M \xrightarrow{\cong} M, \quad r \otimes m \mapsto rm$$

inducida por la inclusión $\mathfrak{a} \subseteq R$ es inyectiva.

2') *Para todo ideal finitamente generado $\mathfrak{a} \subseteq R$ la aplicación $\mathfrak{a} \otimes_R M \to M$ es inyectiva.*

3) $\mathrm{Tor}_1^R(R/\mathfrak{a}, M) = 0$ *para todo ideal $\mathfrak{a} \subseteq R$.*

3') $\mathrm{Tor}_1^R(R/\mathfrak{a}, M) = 0$ *para todo ideal finitamente generado $\mathfrak{a} \subseteq R$.*

Demostración. Si M es plano, entonces la sucesión exacta corta

$$0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$$

induce una sucesión exacta corta

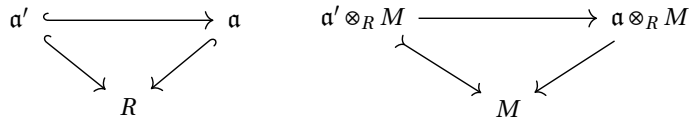
$$0 \to \mathfrak{a} \otimes_R M \to M \to R/\mathfrak{a} \otimes_R M \to 0$$

así que 1) $\Rightarrow$ 2). Además, 2) $\Leftrightarrow$ 3), puesto que en general lo que se obtiene es una sucesión

$$\cdots \to \underbrace{\operatorname{Tor}_1^R(R, M)}_{=0} \to \operatorname{Tor}_1^R(R/\mathfrak{a}, M) \to \mathfrak{a} \otimes_R M \to M \to R/\mathfrak{a} \otimes_R M \to 0$$

cuya exactitud nos dice que la aplicación $\mathfrak{a} \otimes_R M \to M$ es inyectiva si y solamente si $\operatorname{Tor}_1^R(R/\mathfrak{a}, M) = 0$. De la misma manera, tenemos equivalencia 2′) $\Leftrightarrow$ 3′), y por supuesto, 2) $\Rightarrow$ 2′) y 3) $\Rightarrow$ 3′).

Notamos que 2′) $\Rightarrow$ 2). En efecto, asumamos que se cumple 2). Para probar que la aplicación $\mathfrak{a} \otimes_R M \to M$ es inyectiva, hay que ver que todo elemento no nulo $x = \sum_i r_i \otimes m_i \in \mathfrak{a} \otimes_R M$ va a un elemento no nulo en M. Sea $\mathfrak{a}' \subset \mathfrak{a}$ el ideal generado por los r_i. Ahora x está en la imagen de $\mathfrak{a}' \otimes_R M \to \mathfrak{a} \otimes_R M$ y la aplicación $\mathfrak{a}' \otimes_R M \to M$ es inyectiva, puesto que el ideal $\mathfrak{a}'$ es finitamente generado. Entonces, x va a un elemento no nulo en M.



Ahora probemos la implicación 3) $\Rightarrow$ 1). Para deducir de 3) que M es plano, hay que ver que toda inclusión $N' \subset N$ induce una aplicación intectiva $N' \otimes_R M \to N \otimes_R M$. El módulo $N \otimes_R M$ está generado por los elementos $n \otimes m$ donde $n \in N$ y $m \in M$, respecto a las relaciones de bilinelidad. Para un elemento $x \in N' \otimes_R M$ en la condición que x va a cero en $N \otimes_R M$ aparece solo un número finito de elementos de N, así que sería suficiente probar que la propiedad deseada se cumple para N finitamente generado. En este caso podemos escoger una cadena de submódulos

$$N' = N_0 \subset N_1 \subset \cdots \subset N_p = N$$

donde cada uno de los cocientes N_{i+1}/N_i está generado por un elemento; es decir, $N_{i+1}/N_i \cong R/\mathfrak{a}_i$ para algún ideal $\mathfrak{a}_i \subset R$. El producto tensorial con M nos da una cadena de aplicaciones

$$N' \otimes_R M = N_0 \otimes_R M \to N_1 \otimes_R M \to \cdots \to N_p \otimes_R M = N \otimes_R M$$

y bastaría comprobar que $N_i \otimes_R M \to N_{i+1} \otimes_R M$ es inyectiva para todo i. En efecto, la sucesión exacta corta

$$0 \to N_i \to N_{i+1} \to R/\mathfrak{a}_i \to 0$$

nos da

$$\cdots \to \operatorname{Tor}_1^R(R/\mathfrak{a}_i, M) \to N_i \otimes_R M \to N_{i+1} \otimes_R M \to R/\mathfrak{a}_i \otimes_R M \to 0$$

donde $\operatorname{Tor}_1^R(R/\mathfrak{a}_i, M) = 0$ por la hipótesis de 3). ■

7.2. Corolario. *Sea R un dominio de ideales principales y M un R-módulo. Entonces, M es plano si y solamente si M es libre de torsión:*

$$M_{tors} := \{m \in M \mid x \cdot m = 0 \text{ para algún } x \neq 0\} = 0.$$

Demostración. Por el resultado anterior, M es plano si y solamente si para todo ideal $(x) \subset R$ se cumple $\operatorname{Tor}_1^R(R/(x), M) = 0$. Esto es cierto para $x = 0$ (se tiene $\operatorname{Tor}_1^R(R, -) = 0$), así que podemos asumir que $x \neq 0$. En este caso hay una sucesión exacta corta

$$0 \to R \xrightarrow{\times x} R \to R/(x) \to 0$$

que induce una sucesión exacta

$$0 \to \operatorname{Tor}_1^R(R/(x), M) \to M \xrightarrow{\times x} M \to M/xM \to 0$$

Entonces,

$$\operatorname{Tor}_1^R(R/(x), M) \cong \ker(M \xrightarrow{\times x} M) = \{m \in M \mid x \cdot m = 0\}.$$

Así que tenemos $\operatorname{Tor}_1^R(R/(x), M) = 0$ para todo $x \neq 0$ si y solamente si $M_{\text{tors}} = 0$. ■

7.3. Ejemplo. El grupo abeliano $\mathbb{Q}$ es un $\mathbb{Z}$-módulo plano, siendo una localización de $\mathbb{Z}$. Es un $\mathbb{Z}$-módulo libre de torsión, pero no es libre. En efecto, para dos subgrupos no triviales $A, B \subset \mathbb{Q}$, para cualesquiera $\frac{a}{b} \in A$, $\frac{c}{d} \in B$ se tiene $bc \cdot \frac{a}{b} = ad \cdot \frac{c}{d} = ac \in A \cap B$. Esto demuestra que $A, B \neq 0$ implica $A \cap B \neq 0$. En particular, si $\mathbb{Q} = A \oplus B$, entonces necesariamente $A = 0$ o $B = 0$. ▲

7.2 El criterio local de planitud

Cuando R es un anillo local, el criterio de planitud 7.4 puede ser simplificado, bajo ciertas hipótesis adicionales.

7.4. Teorema. *Sean $(R, \mathfrak{m})$ un anillo local noetheriano, $(S, \mathfrak{n})$ una R-álgebra local noetheriana tal que $\mathfrak{m}S \subseteq \mathfrak{n}$ y M un S-módulo finitamente generado. Luego, M es plano sobre R si y solamente si $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$.*

(Muy a menudo este resultado se usa cuando $S = R$ o $M = S$.)

Demostración. Si M es plano sobre R, entonces $\operatorname{Tor}_1^R(-, M) = 0$. Viceversa, supongamos que $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$. Tenemos que deducir que M es plano.

Primero notamos que si $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$, entonces $\operatorname{Tor}_1^R(N, M) = 0$ para todo R-módulo de longitud finita N. En efecto, si $\ell(N) = 1$, entonces $N = R/\mathfrak{m}$ y el resultado se cumple por la hipótesis. Si $\ell(N) > 1$, podemos tomar un submódulo propio no nulo $N' \subset N$ y considerar la sucesión exacta corta

$$0 \to N' \to N \to N/N' \to 0$$

Esta induce una sucesión exacta

$$\cdots \to \operatorname{Tor}_1^R(N', M) \to \operatorname{Tor}_1^R(N, M) \to \operatorname{Tor}_1^R(N/N', M) \to \cdots$$

Tenemos $\ell(N) = \ell(N') + \ell(N/N')$ y en particular $\ell(N), \ell(N/N') < \ell(N)$, así que por la hipótesis de inducción

$$\operatorname{Tor}_1^R(N', M) = \operatorname{Tor}_1^R(N/N', M) = 0.$$

La exactitud de la sucesión de arriba implica entonces que $\operatorname{Tor}_1^R(N, M) = 0$.

Para probar que M es plano, según 7.4 sería suficiente probar que para todo ideal $\mathfrak{a} \subset R$ la aplicación $\mathfrak{a} \otimes_R M \to M$ es inyectiva. Supongamos que $x \in \mathfrak{a} \otimes_R M$ es un elemento que va a cero. Hay que probar que $x = 0$.

Notamos que $\mathfrak{a} \otimes_R M$ es un S-módulo finitamente generado. Además, por la hipótesis $\mathfrak{m}S \subseteq \mathfrak{m}$ se cumple

$$\mathfrak{m}^n (\mathfrak{a} \otimes_R M) \subseteq \mathfrak{n}^n (\mathfrak{a} \otimes_R M).$$

El teorema de intersección de Krull (véase 6.7) nos dice que

$$\bigcap_{n \geq 0} \mathfrak{m}^n (\mathfrak{a} \otimes_R M) \subseteq \bigcap_{n \geq 0} \mathfrak{n}^n (\mathfrak{a} \otimes_R M) = 0,$$

así que para concluir que $x = 0$ bastaría probar que x está en $\mathfrak{m}^n (\mathfrak{a} \otimes_R M)$ para todo $n \geq 0$; es decir, que x está en la imagen de $(\mathfrak{m}^n \mathfrak{a}) \otimes_R M \to \mathfrak{a} \otimes_R M$ para todo $n \geq 0$.

El lema de Artin–Rees implica que para todo $n \geq 0$ existe $t \geq 0$ tal que $\mathfrak{m}^t \cap \mathfrak{a} \subseteq \mathfrak{m}^n \mathfrak{a}$ (véase 6.6), y por ende sería suficiente probar que x está en la imagen de $(\mathfrak{m}^t \cap \mathfrak{a}) \otimes_R M \to \mathfrak{a} \otimes_R M$ para todo $t \geq 0$. Gracias a la sucesión exacta

$$(\mathfrak{m}^t \cap \mathfrak{a}) \otimes_R M \xrightarrow{i \otimes \mathrm{id}} \mathfrak{a} \otimes_R M \xrightarrow{p \otimes \mathrm{id}} \mathfrak{a}/(\mathfrak{m}^t \cap \mathfrak{a}) \otimes_R M \to 0$$

esto es equivalente a probar que $x \in \ker(p \otimes \mathrm{id})$.

Consideremos el diagrama conmutativo

$$\begin{array}{ccc} \mathfrak{a} & \xrightarrow{p} & \mathfrak{a}/(\mathfrak{m}^t \cap \mathfrak{a}) \\ \downarrow & & \downarrow \phi \\ R & \twoheadrightarrow & R/\mathfrak{m}^t \end{array}$$

donde la aplicación ϕ viene dada por

$$\mathfrak{a}/(\mathfrak{m}^t \cap \mathfrak{a}) \xrightarrow{\cong} (\mathfrak{a}+\mathfrak{m}^t)/\mathfrak{m}^t \rightarrowtail R/\mathfrak{m}^t.$$

Al tensorizar el diagrama de arriba con M, se obtiene el diagrama conmutativo

$$\begin{array}{ccc} \mathfrak{a} \otimes_R M & \xrightarrow{p\otimes \mathrm{id}} & \mathfrak{a}/(\mathfrak{m}^t \cap \mathfrak{a}) \otimes_R M \\ \downarrow & & \downarrow \phi\otimes \mathrm{id} \\ M & \twoheadrightarrow & R/\mathfrak{m}^t \otimes_R M \end{array}$$

Por la hipótesis, $x \in \mathfrak{a} \otimes_R M$ va a cero en M, entonces para concluir que $(p \otimes \mathrm{id})(x) = 0$ sería suficiente probar que la aplicación $\phi \otimes \mathrm{id}$ es inyectiva; es decir, que $(\mathfrak{a}+\mathfrak{m}^t)/\mathfrak{m}^t \rightarrowtail R/\mathfrak{m}^t$ induce una aplicación intectiva $(\mathfrak{a}+\mathfrak{m}^t)/\mathfrak{m}^t \otimes_R M \rightarrowtail R/\mathfrak{m}^t \otimes_R M$. Consideremos la sucesión exacta

$$\cdots \to \mathrm{Tor}_1^R(R/(\mathfrak{a}+\mathfrak{m}^t), M) \to (\mathfrak{a}+\mathfrak{m}^t)/\mathfrak{m}^t \otimes_R M \to R/\mathfrak{m}^t \otimes_R M \to R/(\mathfrak{a}+\mathfrak{m}^t) \otimes_R M \to 0$$

Tenemos $\mathfrak{m}^t \cdot (R/(\mathfrak{a}+\mathfrak{m}^t)) = 0$, lo que implica que $\ell(R/(\mathfrak{a}+\mathfrak{m}^t)) = 0$ (véase 2.17) y por la primera parte de la prueba podemos concluir que $\mathrm{Tor}_1^R(R/(\mathfrak{a}+\mathfrak{m}^t), M) = 0$. ■

7.5. Lema. *Sean R un anillo, M un R-módulo y $x \in R$ un elemento que no es un divisor de cero en R, ni sobre M. Luego, para todo $R/(x)$-módulo N se tiene*

$$\mathrm{Tor}_n^{R/(x)}(N, M/xM) \cong \mathrm{Tor}_n^R(N, M).$$

Demostración. Tenemos una sucesión exacta corta

$$0 \to R \xrightarrow{\times x} R \to R/(x) \to 0$$

que induce una sucesión exacta larga

$$\cdots \to \underbrace{\mathrm{Tor}_n^R(R, M)}_{=0} \to \mathrm{Tor}_n^R(R/(x), M) \to \underbrace{\mathrm{Tor}_{n-1}^R(R, M)}_{=0} \to \cdots$$
$$\to \underbrace{\mathrm{Tor}_1^R(R, M)}_{=0} \to \mathrm{Tor}_1^R(R/(x), M) \to M \xrightarrow{\times x} M \to R/(x) \otimes_R M \to 0$$

Se sigue que

$$\mathrm{Tor}_n^R(R/(x), M) \cong \begin{cases} M \to R/(x) \otimes_R M \cong M/xM, & n = 0, \\ \{m \in M \mid x \cdot m = 0\}, & n = 1, \\ 0, & n > 1. \end{cases}$$

Bajo la hipótesis que x no es un divisor de cero sobre M, tenemos $\mathrm{Tor}_n(R/(x), M) = 0$ para todo $n \neq 0$.

Para calcular $\mathrm{Tor}_n^R(N, M)$, escojamos una resolución libre de M

$$\cdots \to F_2 \to F_1 \to F_0 \to M \to 0$$

Luego,

$$\operatorname{Tor}_n^R(N,M) = H_n(F_\bullet \otimes_R N).$$

Tenemos

$$H_n(R/(x) \otimes_R F_\bullet) = \operatorname{Tor}_n(R/(x), M) = 0 \text{ para } n \neq 0,$$

lo que significa que al tensorizarlo con $R/(x)$, el complejo $F_\bullet$ no pierde la exactitud en $n > 0$ y

$$\cdots \to R/(x) \otimes_R F_2 \to R/(x) \otimes_R F_1 \to R/(x) \otimes_R F_0 \to M/xM \to 0$$

es una resolución de M/xM por $R/(x)$-módulos libres $R/(x) \otimes_R F_n$. Tenemos

$$\operatorname{Tor}_n^{R/(x)}(N, M/xM) = H_n(N \otimes_{R/(x)} (R/(x) \otimes_R F_\bullet)) \cong H_n(N \otimes_R F_\bullet) \cong \operatorname{Tor}_n^R(N,M).$$

■

7.6. Proposición. *Sean $(R,\mathfrak{m})$ un anillo local noetheriano, $(S,\mathfrak{n})$ una R-álgebra local noetheriana tal que $\mathfrak{m}S \subseteq \mathfrak{n}$ y M un S-módulo finitamente generado. Sea $x \in R$ un elemento que no es un divisor de cero en R, ni sobre M. Entonces, M es plano sobre R si y solamente si M/xM es plano sobre $R/(x)$.*

Notamos que en general, si R' es una R-álgebra y M es un R-módulo plano, entonces $R' \otimes_R M$ es un R'-módulo plano, puesto que para cualquier R'-módulo N se tiene

$$(R' \otimes_R M) \otimes_{R'} N \cong M \otimes_R N.$$

Entonces, si M es plano sobre R, el módulo $R/(x) \otimes_R M \cong M/xM$ es plano sobre $R/(x)$. Lo que nos interesa es la otra implicación.

Demostración. Bajo las hipótesis de la proposición, el criterio local de planitud 7.4 nos dice que M/xM es plano sobre $R/(x)$ si y solamente si $\operatorname{Tor}_1^{R/(x)}(R/\mathfrak{m}, M/xM) = 0$. Según el lema de arriba, esto es equivalente a $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$; es decir, a la planitud de M sobre R. ■

7.3 Ejercicios sobre planitud y Tor

Ejercicio 32. Consideremos el anillo $R = k[X, Y]$ y el ideal $\mathfrak{a} := (X, Y) \subset R$. Demuestre que la inclusión $\mathfrak{a} \rightarrowtail R$ induce una aplicación $\mathfrak{a} \otimes_R \mathfrak{a} \to \mathfrak{a}$ que ya no es inyectiva. Este es un ejemplo de un R-módulo libre de torsión que no es plano.

Ejercicio 33. Supongamos que R es un anillo noetheriano y M, N son R-módulos finitamente generados. Demuestre que los módulos $\operatorname{Tor}_n^R(M, N)$ son también finitamente generados.

Ejercicio 34. Sean $\mathfrak{a}, \mathfrak{b}$ ideales en un anillo conmutativo R. Demuestre que

$$\operatorname{Tor}_1^R(R/\mathfrak{a}, R/\mathfrak{b}) \cong \frac{\mathfrak{a} \cap \mathfrak{b}}{\mathfrak{a}\mathfrak{b}}, \quad \operatorname{Tor}_2^R(R/\mathfrak{a}, R/\mathfrak{b}) \cong \ker(\mathfrak{a} \otimes_R \mathfrak{b} \to \mathfrak{a}\mathfrak{b}).$$

Ejercicio 35. Sean R un anillo y M un R-módulo finitamente presentado.

1) Supongamos que $(R, \mathfrak{m})$ es un anillo local. Usando el lema de Nakayama, demuestre que M es plano si y solo si $\operatorname{Tor}_1^R(M, R/\mathfrak{m}) = 0$.

2) Demuestre que en general, M es plano sobre R si y solo si $M_\mathfrak{m}$ es plano sobre $R_\mathfrak{m}$ para todos los ideales maximales $\mathfrak{m} \subset R$.

   (Si N es un $R_\mathfrak{m}$-módulo, note que $M \otimes_R N \cong M \otimes_{R_\mathfrak{m}} N$ y use 1.22.)

Ejercicio 36. Demuestre que $\operatorname{Tor}_n^R(M, N)$ puede ser calculado usando **resoluciones planas**. Es decir, se puede tomar una sucesión exacta

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

donde P_n son R-módulos planos, y luego

$$H_n(P_\bullet \otimes_R N) \cong \operatorname{Tor}_n^R(M, N).$$

Ejercicio 37. Deduzca del ejercicio anterior que Tor conmuta con la localización:

$$\operatorname{Tor}_n^R(M, N)[U^{-1}] \cong \operatorname{Tor}_n^{R[U^{-1}]}(M[U^{-1}], N[U^{-1}]).$$

Ejercicio 38. Sea R un dominio de integridad y sea $K(R)$ su cuerpo de fracciones. Demuestre que

$$\operatorname{Tor}_1^R(K(R)/R, M) \cong M_{\text{tors}} := \{m \in M \mid x \cdot m = 0 \text{ para algún } x \neq 0\}.$$

Ejercicio 39. Sea

$$\cdots \to M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \to \cdots$$

un complejo de R-módulos y sea P un R-módulo plano. Demuestre que

$$H_n(M_\bullet \otimes_R P) \cong H_n(M_\bullet) \otimes_R P.$$

Ejercicio 40 (Fórmula de Künneth)**.** Sea

$$\cdots \to P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \cdots$$

un complejo de R-módulos planos. Supongamos que para todo n el submódulo $\operatorname{im} d_n \subseteq P_{n-1}$ es también plano.

1) Deduzca que para todo n la sucesión exacta corta

$$0 \to \ker d_n \to P_n \xrightarrow{d_n} \operatorname{im} d_n \to 0$$

induce una sucesión exacta corta

$$0 \to \ker d_n \otimes_R M \to P_n \otimes_R M \xrightarrow{d_n} \operatorname{im} d_n \otimes_R M \to 0$$

y estas sucesiones forman una sucesión exacta corta de complejos

$$0 \to \ker d_\bullet \otimes_R M \to P_\bullet \otimes_R M \xrightarrow{d_\bullet \otimes \mathrm{id}} \operatorname{im} d_\bullet \otimes_R M \to 0$$

donde los complejos $\ker d_\bullet$ e $\operatorname{im} d_\bullet$ tienen diferenciales nulos.

2) Analice la sucesión exacta larga correspondiente

$$\cdots \to H_n(\ker d_\bullet \otimes_R M) \to H_n(P_\bullet \otimes_R M) \to H_n(\operatorname{im} d_\bullet \otimes_R M) \xrightarrow{\delta_n} H_{n-1}(\ker d_\bullet \otimes_R M) \to \cdots$$

identifíquela con la sucesión exacta

$$\cdots \to \ker d_n \otimes_R M \to H_n(P_\bullet \otimes_R M) \to \operatorname{im} d_n \otimes_R M \to \ker d_{n-1} \otimes_R M \to \cdots$$

donde la última aplicación está inducida por la inclusión $\operatorname{im} d_n \rightarrowtail \ker d_{n-1}$.

3) De la sucesión exacta corta

$$0 \to \operatorname{im} d_n \to \ker d_{n-1} \to H_{n-1}(P_\bullet) \to 0$$

deduzca que

$$\operatorname{Tor}_1^R(H_{n-1}(P_\bullet), M) \cong \operatorname{im}(H_n(P_\bullet \otimes_R M) \to \operatorname{im} d_n \otimes_R M)$$

y también note que

$$\ker(H_n(P_\bullet \otimes_R M) \to \operatorname{im} d_n \otimes_R M) \cong H_n(P_\bullet) \otimes_R M.$$

4) Concluya que para todo n se tiene una sucesión exacta corta

$$0 \to H_n(P_\bullet) \otimes_R M \to H_n(P_\bullet \otimes_R M) \to \operatorname{Tor}_1^R(H_{n-1}(P_\bullet), M) \to 0$$

Estas sucesiones exactas cortas explica qué sucede con la homología de un complejo al tensorizarlo con M.

7.4 Ejercicios sobre los funtores Ext

En clase hemos visto solamente los funtores Tor, pero la construcción general de funtores derivados puede ser usada para definir los funtores Ext.

Ejercicio 41. Sean M y N dos R-módulos.

1) Escojamos una resolución proyectiva

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \to 0$$

demuestre que al aplicar el funtor contravariante $\operatorname{Hom}_R(-, M)$, se obtiene un complejo

$$\operatorname{Hom}_R(P_\bullet, N): \quad 0 \to \underbrace{\operatorname{Hom}_R(P_0, N)}_{\deg 0} \xrightarrow{d_0 := d_1^*} \underbrace{\operatorname{Hom}_R(P_1, N)}_{\deg -1} \xrightarrow{d_{-1} := d_2^*} \underbrace{\operatorname{Hom}_R(P_2, N)}_{\deg -2} \to \cdots$$

donde

$$d_{-n} := d_{n+1}^* \colon \underbrace{\operatorname{Hom}_R(P_n, N)}_{\deg -n} \to \underbrace{\operatorname{Hom}_R(P_{n+1}, N)}_{\deg -n-1}$$

2) Pongamos

$$\mathrm{Ext}^n_R(M,N) := H_{-n}(\mathrm{Hom}_R(P_\bullet, N)) := \frac{\ker d_{-n}}{\mathrm{im}\, d_{-n+1}}.$$

Demuestre que el resultado no depende de la elección de resolución proyectiva y esto define un funtor contravariante $\mathrm{Ext}^n_R(-,N)$.

Ejercicio 42.

1) Demuestre que $\mathrm{Ext}^0_R(-,N) \cong \mathrm{Hom}_R(-,N)$.

2) Demuestre que una sucesión exacta corta

$$0 \to M' \to M \to M'' \to 0$$

induce una sucesión exacta larga

$$0 \to \mathrm{Hom}_R(M'',N) \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M',N) \to \\ \mathrm{Ext}^1_R(M'',N) \to \mathrm{Ext}^1_R(M,N) \to \mathrm{Ext}^1_R(M',N) \to \cdots$$

3) Demuestre que $\mathrm{Ext}^n_R(P,N) = 0$ para $n \geq 1$ si P es un R-módulo proyectivo.

4) Demuestre que las siguientes condiciones son equivalentes:

   a) el funtor $\mathrm{Hom}_R(-,N)$ es exacto;
   b) $\mathrm{Ext}^1_R(-,N) = 0$;
   c) $\mathrm{Ext}^n_R(-,N) = 0$ para todo $n \geq 1$.

Ejercicio 43. Calcule los grupos $\mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$.

Ejercicio 44. Sea R un anillo y sea $x \in R$ un elemento que no es un divisor de cero. Para un R-módulo M calcule $\mathrm{Ext}^n_R(R/(x), M)$.

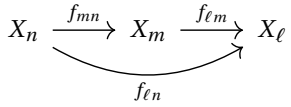
8 Completación

Revisemos el siguiente concepto categórico.

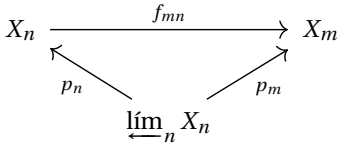
8.1. Definición. En una categoría, sea X_n una familia de objetos indexada por $n = 1, 2, 3, \ldots$ Supongamos que para cualesquiera $m \leq n$ está especificado un morfismo $f_{mn} \colon X_n \to X_m$ de tal manera que

1) $f_{nn} = \mathrm{id}_{X_n}$ para todo n,

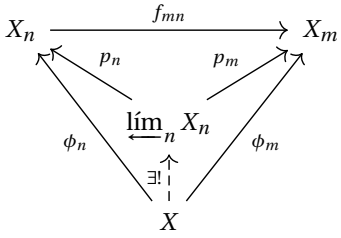
2) $f_{\ell n} = f_{\ell m} \circ f_{mn}$ para cualesquiera $\ell \leq m \leq n$:



Se dice que X_i con los morfismos $f_{mn} \colon X_n \to X_m$ forman un **sistema inverso**. El **límite inverso** correspondiente es un objeto $\varprojlim_n X_n$ junto con morfismos $p_n \colon \varprojlim_n X_n \to X_n$ tales que $p_m = f_{mn} \circ p_n$ para cualesquiera $m \leq n$:



Además, se pide la siguiente propiedad universal: si X es otro objeto con morfismos $\phi_n \colon X \to X_n$ tales que $\phi_m = f_{mn} \circ \phi_n$ para cualesquiera $m \leq n$, entonces existe un único morfismo $X \to \varprojlim_n X_n$ que conmuta con los morfismos p_n y ϕ_n:



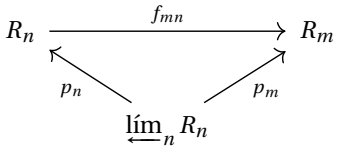
Los límites inversos son casos particulares de **límites**. Como siempre, la propiedad universal implica que si el límite inverso $\varprojlim_n X_n$ existe, este es único salvo isomorfismo único.

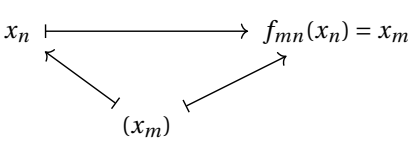
8.2. Observación. *El límite inverso de anillos siempre existe. Este viene dado por*

$$\varprojlim_n R_n = \{x = (x_1, x_2, x_3, \ldots) \in \prod_n R_n \mid f_{mn}(x_n) = x_m \text{ para cualesquiera } m \leq n\}$$

respecto a las operaciones naturales término por término y los homomorfismos $p_n \colon \varprojlim_n R_n \to R_n$ *inducidos por los homomorfismos de proyección* $\prod_n R_n \to R_n$.

Demostración. Por la definición de $\varprojlim_n R_n$, se tienen diagramas conmutativos

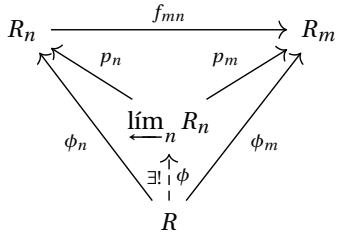




Ahora para otro anillo R y una familia de homomorfismos $\phi_n\colon R \to R_n$ que satisfacen $\phi_m = f_{mn}\circ\phi_n$ para cualesquiera $m \le n$, existe un homomorfismo único $\phi\colon R \to \varprojlim_n R_n$ tal que $p_n\circ\phi = \phi_n$ para todo n. En efecto, se ve que la única posible opción es de poner

$$\phi(x) := (\phi_n(x)).$$

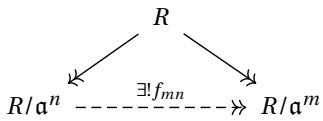
Este elemento pertenece a $\varprojlim_n R_n$: si $m \le n$, entonces $f_{mn}\circ\phi_n(x) = \phi_m(x)$.



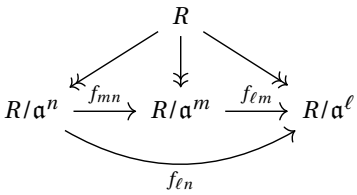
■

Nos va a interesar el siguiente caso muy particular de límites inversos de anillos.

8.3. Definición. Sea R un anillo conmutativo y $\mathfrak{a} \subseteq R$ un ideal. Consideremos los homomorfismos canónicos de proyección sobre el anillo cociente $R \twoheadrightarrow R/\mathfrak{a}^n$. Si $m \le n$, entonces $\mathfrak{a}^n \subseteq \mathfrak{a}^m$, así que por la propiedad universal del núcleo existe un homomorfismo único $f_{mn}\colon R/\mathfrak{a}^n \twoheadrightarrow R/\mathfrak{a}^m$ que hace conmutar el diagrama



Estos homomorfismos forman un sistema inverso de anillos:



El límite inverso correspondiente se llama la **completación** de R respecto al ideal $\mathfrak{a}$ (o la **completación $\mathfrak{a}$-ádica**) y se denota por

$$\widehat{R}_{\mathfrak{a}} := \varprojlim_n R/\mathfrak{a}^n,$$

o simplemente por $\widehat{R}$ cuando se conoce el ideal en cuestión.

Se dice que un anillo R es **completo** respecto a un ideal $\mathfrak{a} \subseteq R$ si R junto con los homomorfismos canónicos $R \twoheadrightarrow R/\mathfrak{a}^n$ satisface la propiedad universal de $\varprojlim_n R/\mathfrak{a}^n$.

Nuestra construcción de 8.2 da

$$\widehat{R} = \{x = (x_1, x_2, x_3, \ldots) \in \prod_{n\ge 1} R/\mathfrak{a}^n \mid x_n \equiv x_m \pmod{\mathfrak{a}^m} \text{ para cualesquiera } m \le n\}.$$

8.4. Ejemplo. Consideremos el anillo de polinomios en n variables $S := R[X_1, \ldots, X_n]$ y el ideal maximal $\mathfrak{m} = (X_1, \ldots, X_n)$. La completación de S respecto a $\mathfrak{m}$ es isomorfa al anillo de las series formales $R[\![X_1, \ldots, X_n]\!]$.

En efecto, tenemos

$$\widehat{S} = \{f = (f_1, f_2, f_3, \ldots) \in \prod_{i \geq 1} R[X_1, \ldots, X_n]/\mathfrak{m}^i \mid f_j \equiv f_i \pmod{\mathfrak{a}^i} \text{ para cualesquiera } i \leq j\}.$$

Las aplicaciones canónicas

$$R[[X_1, \ldots, X_n]] \twoheadrightarrow R[[X_1, \ldots, X_n]]/\mathfrak{m}^i \xrightarrow{\cong} R[X_1, \ldots, X_n]/\mathfrak{m}^i$$

inducen un homomorfismo

$$\begin{aligned} R[[X_1, \ldots, X_n]] &\to \widehat{S}, \\ f &\mapsto (f + \mathfrak{m}, f + \mathfrak{m}^2, f + \mathfrak{m}^3 \ldots). \end{aligned}$$

Este homomorfismo tiene inverso dado por

$$\begin{aligned} \widehat{S} &\to R[[X_1, \ldots, X_n]], \\ (f_1 + \mathfrak{m}, f_2 + \mathfrak{m}^2, f_3 + \mathfrak{m}^3 \ldots) &\mapsto f_1 + (f_2 - f_1) + (f_3 - f_2) + \cdots. \end{aligned}$$

La suma $f_1 + (f_2 - f_1) + (f_3 - f_2) + \cdots$ es una serie formal bien definida, dado que $\deg(f_{i+1} - f_i) \geq i + 1$, y se ve que el resultado no depende de la elección de f_i de las clases $f_i + \mathfrak{m}^i$. ▲

8.5. Observación. *Si R es un anillo completo respecto a un ideal $\mathfrak{a} \subset R$, entonces es completo respecto a cualquier potencia $\mathfrak{a}^n \subset R$.*

Demostración. Ejercicio para el lector. ■

Además, nos va a interesar la completación de R-módulos.

8.6. Definición. Sea R un anillo conmutativo y $\mathfrak{a} \subseteq R$ un ideal. Para un R-módulo M su **completación** respecto al ideal $\mathfrak{a}$ es el límite inverso de R-módulos

$$\widehat{M}_\mathfrak{a} := \varprojlim_n M/\mathfrak{a}^n M,$$

Como en el caso de anillos, el último límite inverso siempre existe y viene dado por

$$\widehat{M}_\mathfrak{a} = \{x = (x_1, x_2, x_3, \ldots) \in \prod_{n \geq 1} M/\mathfrak{a}^n M \mid x_n \equiv x_m \pmod{\mathfrak{a}^m} \text{ para cualesquiera } m \leq n\}.$$

Notamos que $\widehat{M}_\mathfrak{a}$ tiene estructura natural de $\widehat{R}_\mathfrak{a}$-módulo.

Dejo al lector comprobar la funtorialidad: toda aplicación R-lineal $f\colon M \to N$ induce de modo funtorial una aplicación $\widehat{R}_\mathfrak{a}$-lineal $\widehat{f}\colon \widehat{M}_\mathfrak{a} \to \widehat{N}_\mathfrak{a}$ (esto se sigue de la funtorialidad de límites inversos).

8.1 Propiedades claves de la completación

La completación de R-módulos se comporta bien bajo ciertas hipótesis de finitud: hay que asumir que R es un anillo noetheriano y M es un módilo finitamente generado.

8.7. Teorema. *Sean R un anillo noetheriano y $\mathfrak{a} \subset R$ un ideal.*

1) *La completación es **exacta** para R-módulos finitamente generados: toda sucesión exacta corta de R-módulos finitamente generados*

$$0 \to M' \to M \to M'' \to 0$$

induce una sucesión exacta corta

$$0 \to \widehat{M'}_\mathfrak{a} \to \widehat{M}_\mathfrak{a} \to \widehat{M''}_\mathfrak{a} \to 0$$

2) Si M es un R-módulo finitamente generado, entonces la aplicación natural $\widehat{R}_\mathfrak{a}$-lineal

$$\widehat{R}_\mathfrak{a} \otimes_R M \to \widehat{M}_\mathfrak{a}$$

(inducida por la propiedad universal del producto tensorial) es un isomorfismo.

3) La completación $\widehat{R}_\mathfrak{a}$ es una R-álgebra plana.

Bosquejo de la demostración. En 1), a partir de la sucesión exacta corta

$$0 \to M' \to M \to M'' \to 0$$

tomando el producto tensorial $- \otimes_R R/\mathfrak{a}^n$ se obtiene una sucesión exacta

$$M'/\mathfrak{a}^n M' \to M/\mathfrak{a}^n M \to M''/\mathfrak{a}^n M'' \to 0$$

y luego una sucesión exacta corta

$$0 \to M'/(\mathfrak{a}^n M \cap M') \to M/\mathfrak{a}^n M \to M''/\mathfrak{a}^n M'' \to 0$$

Pasando a los límites inversos, se obtiene

$$0 \to \varprojlim M'/(\mathfrak{a}^n M \cap M') \to \widehat{M}_\mathfrak{a} \to \widehat{M''}_\mathfrak{a} \to 0$$

— en efecto, la aplicación de $\varprojlim$ es siempre exacta por la derecha, y en nuestro caso es también exacta por la izquierda, dado que las aplicaciónes

$$M'/(\mathfrak{a}^{n+1} M \cap M') \to M'/(\mathfrak{a}^n M \cap M')$$

del primer sistema inverso son sobreyectivas (véase Atiyah–Macdonald, Proposition 10.2). Ahora el punto clave es notar usando el lema de Artin–Rees (véase §6) que

$$\varprojlim M'/(\mathfrak{a}^n M \cap M') \cong \widehat{M'}_\mathfrak{a}.$$

En 2), primero notamos que si M es un R-módulo libre de rango finito, entonces se tiene un isomorfismo

$$\widehat{R}_\mathfrak{a} \otimes_R M \cong \widehat{M}_\mathfrak{a}.$$

Dado que R es un anillo noetheriano, la hipótesis que M es finitamente generado implica que es finitamente presentado; es decir, existe una sucesión exacta

$$F' \to F \to M \to 0$$

donde F' y F son R-módulos libres de rango finito. A partir de esta sucesión exacta, podemos considerar el diagrama con filas exactas

$$\begin{array}{ccccccccc}
 & & \widehat{R}_\mathfrak{a} \otimes_R F' & \longrightarrow & \widehat{R}_\mathfrak{a} \otimes_R F & \longrightarrow & \widehat{R}_\mathfrak{a} \otimes_R M & \longrightarrow & 0 \\
 & & \downarrow \cong & & \downarrow \cong & & \downarrow & & \\
0 & \longrightarrow & \widehat{F'}_\mathfrak{a} & \longrightarrow & \widehat{F}_\mathfrak{a} & \longrightarrow & \widehat{M}_\mathfrak{a} & \longrightarrow & 0
\end{array}$$

Aquí la primera fila se obtiene aplicando $\widehat{R}_\mathfrak{a} \otimes_R -$ y la segunda fila se obtiene pasando a la completación. Las primeras dos flechas verticales son isomorfismos, puesto que F' y F son libres de rango finito. Entonces, el lema de la serpiente (o el lema del cinco) implica que la tercera flecha es también un isomorfismo.

En la parte 3), es suficiente probar que para toda aplicación inyectiva de *módulos finitamente generados* $M' \to M$ el producto tensorial da una aplicación inyectiva $\widehat{R}_\mathfrak{a} \otimes_R \to \widehat{R}_\mathfrak{a} \otimes_R M$ (véase 7.1), y esto se sigue directamente de 2). ■

8.2 Ejemplo aritmético: el anillo de enteros de un cuerpo local no arquimediano

En esta sección voy a revisar brevemente las propiedades de cuerpos completos respecto a una norma no arquimediana discreta $\|\cdot\|$. El lector también puede consultar mis apuntes sobre los números p-ádicos

san-salvador/2018-04-topologia-p-adica/topologia-p-adica.pdf

Lo que sigue es una pequeña generalización.

Sea K un cuerpo dotado de una **norma no arquimediana**; es decir, una aplicación $\|\cdot\|\colon K \to \mathbb{R}_{\geq 0}$ que satisface las siguientes propiedades:

1) $\|x\| = 0$ si y solamente si $x = 0$;

2) $\|xy\| = \|x\| \cdot \|y\|$ para cualesquiera $x, y \in K$;

3) la **desigualdad ultramétrica** $\|x + y\| \leq \max\{\|x\|, \|y\|\}$.

8.8. Observación. *Sea K un cuerpo con una norma no-arquimediana $\|\cdot\|$. Entonces*

1) El conjunto

$$O_K := \{x \in K \mid \|x\| \leq 1\}$$

*es un subanillo de K, llamado el **anillo de enteros** de K.*

2) Los elementos invertibles de O_K son

$$O_K^\times = \{x \in O_K \mid \|x\| = 1\}.$$

3) O_K es un anillo local y su único ideal maximal es

$$\mathfrak{m}_K = \{x \in O_K \mid \|x\| < 1\}.$$

*El cuerpo correspondiente $\kappa := O_K/\mathfrak{m}_K$ se llama el **cuerpo residual** de K.*

Demostración. Para 1) basta notar que $\|0\| = 0 \leq 1$ y $\|1\| = 1$, y si tenemos $\|x\| \leq 1$ y $\|y\| \leq 1$, entonces

$$\|x + y\| \leq \max\{\|x\|, \|y\|\} \leq 1 \quad \text{y} \quad \|xy\| = \|x\| \cdot \|y\| \leq 1.$$

Para 2), si $x \in O_K$ es invertible en O_K, entonces $x^{-1} \in O_K$. Luego, $\|x^{-1}\| = \|x\|^{-1} \leq 1$. Entonces $\|x\| \leq 1$ y $\|x\| \geq 1$. En otra dirección, si $\|x\| = 1$, entonces $x \neq 0$ y x es invertible en K. Pero $\|x^{-1}\| = \|x\|^{-1} = 1$ y $x^{-1} \in O_K$.

Para 3), está claro que $\mathfrak{m}_K$ es un ideal. Como acabamos de ver en 2), todo elemento no invertible de O_K pertenece a $\mathfrak{m}_K$. Esto implica que $\mathfrak{m}_K$ es el único ideal maximal. ■

8.9. Definición. Sea K un cuerpo con una norma no-arquimediana $\|\cdot\|$. El **grupo de valores** de $\|\cdot\|$ es dado por

$$\Gamma_K := \{\|x\| \mid x \in K^\times\}.$$

Se dice que $\|\cdot\|$ es una **norma discreta** si

1) $\|\cdot\|$ no es trivial,

2) Γ_K es un subgrupo **discreto** del grupo $\mathbb{R}_{>0} \subset \mathbb{R}^\times$ respecto a la topología habitual; es decir, para todo $v \in \Gamma_K$ existe un conjunto abierto $U \subset \mathbb{R}_{>0}$ tal que $U \cap \Gamma_K = \{v\}$.

8.10. Observación. *Si $\|\cdot\|$ es una norma no-arquimediana discreta sobre un cuerpo F, la extensión de $\|\cdot\|$ a la compleción $\widehat{F}$ es también discreta.*

Demostración. Usando la desigualdad ultramétrica, se puede notar que si $x = \lim_{n\to\infty} a_n \in \widehat{F}$ para alguna sucesión de Cauchy $(a_n)_{n\in\mathbb{N}}$ en F, entonces $\|x\| := \lim_{n\to\infty} \|a_n\|$ coincide con $\|a_n\|$ para todo $n \gg 0$. ■

8.11. Proposición. *Sea K un cuerpo con una norma no arquimediana discreta $\|\cdot\|$.*

1) *El grupo $\Gamma_K \subset \mathbb{R}^\times$ es cíclico. Específicamente, existe algún $\pi \in \mathfrak{m}_K$, llamado un **uniformizador**, tal que*

$$\Gamma_K = \{\|\pi\|^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z}.$$

2) *Todo elemento $x \in K^\times$ puede ser escrito como $u\pi^n$ para algunos $u \in O_K^\times$ y $n \in \mathbb{Z}$.*

3) *El ideal maximal $\mathfrak{m}_K$ es principal, generado por π.*

4) *Todo ideal no nulo en O_K es de la forma $\mathfrak{m}_K^n = (\pi^n)$ para algún $n = 0, 1, 2, 3, \ldots$ En particular, O_K es un dominio de ideales principales, y por lo tanto un dominio de factorización única*[*].

5) *K es el cuerpo de fracciones de O_K.*

Demostración. Para ver 1), notamos que dado que Γ_K es un grupo discreto, existe $\pi \in \mathfrak{m}_K$ tale

$$\|\pi\| = \max\{\|x\| \mid x \in K,\ \|x\| < 1\},$$

Luego, para todo $x \in K$ tenemos $\|x\| = \|\pi\|^n$ para algún $n \in \mathbb{Z}$. De hecho, si esto no se cumple, para algún $\|x\| < 1$ y $n = 1, 2, 3, \ldots$ se tiene

$$\|\pi\|^{n+1} < \|x\| < \|\pi\|^n,$$

y entonces

$$\|\pi\| < \|\pi^{-n} x\| < 1,$$

lo que contradice nuestra elección de π.

2) Si $x \in K^\times$, entonces $\|x\| = \|\pi\|^n$ para algún n. Luego, $\|x\pi^{-n}\| = 1$, así que $u := x\pi^{-n} \in O_K^\times$ y $x = u\pi^n$.

3) Ya que $\pi \in \mathfrak{m}_K$, tenemos la inclusión trivial $(\pi) \subseteq \mathfrak{m}_K$. Luego, si $x \in \mathfrak{m}_K$, podemos escribir $x = u\pi^n$ para $u \in O_K^\times$ y $n \in \mathbb{Z}$. Ya que $\|x\| < 1$ y $\|u\| = 1$, tenemos necesariamente $n = 1, 2, 3, \ldots$ Esto demuestra la inclusión $\mathfrak{m}_K \subseteq (\pi)$.

4) Para un ideal no nulo $\mathfrak{a} \subset O_K$, todo elemento no nulo puede ser escrito como $x = u\pi^n$ para $u \in O_K^\times$ y $n \in \mathbb{N}$. Sea x tal elemento con n mínimo posible. Tenemos $\pi^n = u^{-1} x \in (\pi^n)$, así que $(\pi^n) \subseteq \mathfrak{a}$. Luego, para cualquier otro $y \in \mathfrak{a}$, tenemos $y = v\pi^m$, donde $m \geq n$, y $y = v\pi^{m-n}\pi^n \in (\pi^n)$. Esto demuestra la otra inclusión $\mathfrak{a} \subseteq (\pi^n)$.

5) Todo elemento de O_K puede ser escrito como $u\pi^n$ para $u \in O_K^\times$ y $n \in \mathbb{N}$, y todo elemento de K tiene la misma forma con $n \in \mathbb{Z}$. Entonces, está claro que K es el cuerpo mínimo que contiene a O_K. ■

8.12. Proposición. *Sea F un cuerpo con una norma no-arquimediana discreta $\|\cdot\|$ y sea $\widehat{F}$ la compleción correspondiente. La inclusión $O_F \hookrightarrow O_{\widehat{F}}$ induce isomorfismos*

$$O_F/\mathfrak{m}_F^n \cong O_{\widehat{F}}/\mathfrak{m}_{\widehat{F}}^n \text{ para todo } n = 1, 2, 3, \ldots$$

Demostración. Consideremos el homomorfismo canónico

$$f\colon O_F \hookrightarrow O_{\widehat{F}} \twoheadrightarrow O_{\widehat{F}}/\mathfrak{m}_{\widehat{F}}^n.$$

Tenemos

$$\mathfrak{m}_F^n = (\mathfrak{m}_{\widehat{F}} \cap O_F)^n = \mathfrak{m}_{\widehat{F}}^n \cap O_F,$$

[*] Recuerde que la definición de dominios de factorización única exige factorizaciones únicas, salvo unidades. En este caso, según la parte 2) tenemos muchas unidades, y el resto son potencias de π. Entonces, O_K es un dominio de factorización única por razones bastante banales.

así que está claro que $\ker f = \mathfrak{m}_F^n$. El punto clave es probar que f es sobreyectivo.

Por nuestra hipótesis, la norma es discreta, así que $\mathfrak{m}_K = (\pi)$ para un uniformizador π, y luego $x \in \mathfrak{m}_K^n$ si y solamente si $\|x\| \leq \|\pi\|^n$. Sea $x \in O_{\widehat{F}}$. Ya que F es denso en $\widehat{F}$, existe algún $a \in F$ tal que $\|a - x\| < \|\pi\|^n$ y entonces $x \equiv a \pmod{\mathfrak{m}_{\widehat{F}}^n}$. Además,

$$\|a\| = \|a - x + x\| \leq \max\{\|a - x\|, \|x\|\} \leq 1,$$

y por lo tanto $a \in F \cap O_{\widehat{F}} = O_F$. Tenemos $f(a) = x$. ■

8.13. Definición. Un cuerpo completo respecto a una norma no-arquimediana discreta $\|\cdot\|$ se llama un **cuerpo local no arquimediano**[*].

8.14. Teorema (Expansiones en un uniformizador). *Sea K un cuerpo local no arquimediano. Sea π un uniformizador. Denotamos por $\mathcal{A} \subset O_K$ un conjunto de representantes del cuerpo residual $\kappa := O_K/\mathfrak{m}_K$. Entonces*

1) *Todo elemento $x \in O_K$ puede ser escrito de modo único como una serie*

$$x = a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + \cdots$$

donde $a_i \in \mathcal{A}$. Es decir,

$$x = \lim_{n\to\infty} x_n,$$

donde

$$x_n := a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n.$$

2) *En general, todo elemento de K puede ser escrito de modo único como una serie*

$$x = a_{-m}\pi^{-m} + a_{-m+1}\pi^{-m+1} + \cdots + a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + a_4\pi^4 + \cdots$$

para algún m.

Demostración. Según 8.11, todo $x \in K^\times$ puede ser escrito como $x = u\pi^n$ para algunos $u \in O_K^\times$ y $n \in \mathbb{Z}$, así que 1) implica 2).

Para demostrar 1), notamos primero que el límite $\lim_{n\to\infty} x_n$ existe. En efecto, (x_n) es una sucesión de Cauchy, ya que para todo $m \geq n$

$$\|x_m - x_n\| = \|a_{n+1}\pi^{n+1} + a_{n+2}\pi^{n+2} + \cdots + a_{m-1}\pi^{m-1} + a_m\pi^m\| \leq \|\pi\|^{n+1},$$

puesto que $\|a_i\| \leq 1$ y $\|\pi\| < 1$. Para el valor absoluto tenemos

$$\|x\| = \lim_{n\to\infty} \|x_n\| \leq 1,$$

así que $x \in O_K$. Ahora veamos cómo a partir de x se pueden encontrar los coeficientes $a_i \in \mathcal{A}$. Sea $x \in O_K$. Existe único $a_0 \in \mathcal{A}$ tal que $x = a_0 + y_1\pi$ para algún $y_1 \in O_K$. Luego,

$$\|x - a_0\| = \|y_0\| \cdot \|\pi\| \leq \|\pi\|.$$

Sea $a_1 \in \mathcal{A}$ el único elemento tal que $y_1 = a_1 + y_2\pi$ para algún $y_2 \in O_K$. Tenemos

$$x = a_0 + a_1\pi + y_2\pi^2$$

y

$$\|x - (a_0 + a_1\pi)\| = \|y_2\| \cdot \|\pi\|^2 \leq \|\pi\|^2.$$

[*] Algunos autores incluyen la condición que el cuerpo residual $O_K/\mathfrak{m}_K$ es finito. Esto es importante para probar que O_K es complacto.

Continuando de esta manera, por inducción se encuentran $a_i \in \mathcal{A}$ tales que

$$\|x - (a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n)\| \leq \|\pi\|^{n+1}.$$

Entonces,

$$x_n := a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n$$

es una sucesión que tiene como su límite x. Si tenemos otra expansión diferente

$$x = a_0' + a_1'\pi + a_2'\pi^2 + a_3'\pi^3 + \cdots$$

con $a_i' \in \mathcal{A}$, sea n el primer índice donde $a_n' \neq a_n$. Ya que son diferentes representantes de $O_K/\mathfrak{m}_K$, tenemos $a_n' \not\equiv a_n \pmod{\pi}$, así que $\|a_n' - a_n\| = 1$. Denotemos

$$x_n' := a_0' + a_1'\pi + \cdots + a_{n-1}'\pi^{n-1} + a_n'\pi^n.$$

Tenemos

$$\|x_n' - x_n\| = \|(a_n' - a_n)\pi^n\| = \|a_n' - a_n\| \cdot \|\pi^n\| = \|\pi\|^n.$$

Sin embargo,

$$\|x_n' - x_n\| = \|(x_n' - x) + (x - x_n)\| \leq \max\{\|x_n' - x\|, \|x - x_n\|\} \leq \|\pi\|^{n+1},$$

y hemos obtenido una contradicción. ■

8.15. Ejemplo. Consideremos la norma p-ádica $|\cdot|_p$ sobre $\mathbb{Q}$. Esta norma es discreta: sus posibles valores son $1/p^n$ para $n \in \mathbb{Z}$. La completación correspondiente es el cuerpo de los números p-ádicos $\mathbb{Q}_p$. El anillo de enteros correspondiente es $\mathbb{Z}_p$. Como un uniformizador normalmente se toma p. ▲

8.16. Ejemplo. Sea k un cuerpo. Consideremos el cuerpo de funciones racionales

$$k(X) := \left\{ \frac{f}{g} \;\middle|\; f, g \in k[X],\ g \neq 0 \right\}.$$

Para un polinomio $f = \sum_{i \geq 0} a_i X^i \in k[X]$ definamos la **valuación X-ádica** mediante

$$v_X(f) = \min\{i \mid a_i \neq 0\}, \quad v_X(0) := \infty.$$

Luego, para un número fijo $0 < \rho < 1$

$$|f/g|_X := \rho^{v_X(f) - v_X(g)}$$

define una norma no arquimediana discreta sobre $k(X)$. La completación respecto a esta norma es el cuerpo de las series de Laurent $k((X))$ y el anillo de enteros es el anillo de las series formales $k[[X]]$. Las expansiones X-ádicas nos dan

$$k((X)) = \left\{ \sum_{i \geq -n} a_i X^i \;\middle|\; n = 0, 1, 2, 3, \ldots \right\},$$
$$k[[X]] = \left\{ \sum_{i \geq 0} a_i X^i \right\}.$$

▲

8.17. Proposición. *Sea K un cuerpo local no arquimediano. Entonces, su anillo de enteros O_K es completo respecto al ideal maximal $\mathfrak{m}_K$ en el sentido de 8.3.*

Demostración. Sea R un anillo junto con homomorfismos $\phi_n\colon R \to O_K/\mathfrak{m}_K^n$ que satisfacen

$$\phi_m(x) \equiv \phi_n(x) \pmod{\mathfrak{m}_K^m} \text{ para cualesquiera } m \le n.$$

Hay que ver que hay un homomorfismo único $\phi\colon R \to O_K$ que satisface $\phi_n(x) \equiv \phi(x) \pmod{\mathfrak{m}_K^n}$ para todo n.

En términos de expansiones π-ádicas, esto significa que hay una elección única de coeficientes $a_0, a_1, a_2, \ldots$ tales que

$$\phi_n(x) = a_0 + a_1\pi + a_2\pi^2 + \cdots + a_{n-1}\pi^{n-1},$$

y luego necesariamente $\phi(x) = \sum_{n\ge 0} a_n \pi^n$. ■

Los elementos $(x_n) \in \prod_i R/\mathfrak{a}^n$ de la construcción de 8.2 corresponden precisamente a las sumas parciales $x_n = \sum_{0\le i<n} a_i \pi^i$

8.18. Ejemplo. Para construir los números p-ádicos, se puede primero tomar la completación de $\mathbb{Z}$ respecto al ideal (p):

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p,$$

y luego definir $\mathbb{Q}_p$ como el cuerpo de fracciones de este anillo. ▲

8.3 Series de potencias y R-álgebras completas

La propiedad universal de R-álgebra de polinomios $R[X_1, \ldots, X_n]$ nos dice que todo homomorfismo de R-álgebras $f\colon R[X_1, \ldots, X_n] \to S$ se define de modo único por las imágenes $f(X_i)$. El anillo de series formales $R[[X_1, \ldots, X_n]]$ tiene una propiedad parecida, pero respecto a las R-álgebras completas.

8.19. Proposición. *Sea R un anillo y S una R-álgebra completa respecto a un ideal $\mathfrak{a} \subset S$. Dados $f_1, \ldots, f_n \in \mathfrak{a}$, existe un homomorfismo único de R-álgebras*

$$\phi\colon R[[X_1, \ldots, X_n]] \to S$$

tal que $\phi(X_i) = f_i$. Este homomorfismo envía una serie de potencias $g(X_1, \ldots, X_n)$ a $g(f_1, \ldots, f_n) \in S$.

Demostración. Para todo t existe un homomorfismo único de R-álgebras

$$\begin{aligned} R[X_1, \ldots, X_n] &\to S/\mathfrak{a}^t, \\ X_i &\mapsto f_i \pmod{\mathfrak{a}^t}. \end{aligned}$$

Puesto que $f_i \in \mathfrak{a}$, el ideal $(X_1, \ldots, X_n)^t$ está en el núcleo y este homomorfismo se factoriza de modo único por

$$R[[X_1, \ldots, X_n]]/(X_1, \ldots, X_n)^t \cong R[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^t \to S/\mathfrak{a}^t.$$

Esto nos da homomorfismos

$$\begin{aligned} \psi_t\colon R[[X_1, \ldots, X_n]] &\to S/\mathfrak{a}^t, \\ X_i &\mapsto f_i \pmod{\mathfrak{a}^t}. \end{aligned}$$

Luego, la propiedad universal de límites inversos nos produce de estos homomorfismos

$$\begin{aligned} \psi\colon R[[X_1, \ldots, X_n]] &\to \varprojlim_t S/\mathfrak{a}^t \cong S, \\ X_i &\mapsto f_i. \end{aligned}$$

La imagen de $g + (X_1, \ldots, X_n)^t$ en $S/\mathfrak{a}^t$ es $g(f_1, \ldots, f_n) + \mathfrak{a}^t$ para todo t, así que la imagen de g en S es $g(f_1, \ldots, f_n)$ que converge puesto que S es completo respecto a $\mathfrak{a}$. ■

En particular, el último resultado significa que si

$$f = \sum_{i\geq 1} a_i X^i \in XR[[X]]$$

es una serie de potencias con coeficiente constante nulo, entonces $X \mapsto f$ define de modo único un endomorfismo de la R-álgebra $R[[X]]$ que a una serie $g = \sum_{n\geq 0} b_n X^n \in R[[X]]$ asocia la serie

$$g \circ f := \sum_{n\geq 0} b_n f(X)^n.$$

Ya que $a_0 = 0$, toda potencia

$$f(X)^n = \left(\sum_{i\geq 1} a_i X^i\right)^n = \sum_{m\geq 0} \left(\sum_{i_1+\cdots+i_n=m} a_{i_1}\cdots a_{i_n}\right) X^m$$

no tiene términos de grado $m < n$:

$$\begin{aligned} f(X) &= a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 + \cdots, \\ f(X)^2 &= a_1^2 X^2 + 2\, a_1 a_2 X^3 + (2\, a_1 a_3 + a_2^2) X^4 + \cdots, \\ f(X)^3 &= a_1^3 X^3 + 3\, a_1^2 a_2 X^4 + \cdots, \\ f(X)^4 &= a_1^4 X^4 + \cdots \end{aligned}$$

así que la suma infinita $\sum_{n\geq 0} b_n f(X)^n$ tiene sentido. Tenemos

$$g \circ f = \sum_{m\geq 0} c_m X^m,$$

donde $c_0 = b_0$, y para $m > 0$

$$c_m = \sum_{n\geq 1} b_n \left(\sum_{i_1+\cdots+i_n=m} a_{i_1}\cdots a_{i_n}\right). \tag{8.1}$$

8.20. Lema (Teorema de la función inversa para series formales). *Para una serie de potencias $g = \sum_{n\geq 0} b_n X^n \in R[[X]]$ existe otra serie $f \in R[[X]]$ tal que $f(0) = 0$ y $g \circ f = X$ si y solamente si $g(0) = b_0 = 0$ y $g'(0) = b_1 \in R^\times$. En este caso la serie f es única, y además se tiene $f \circ g = X$. Es decir, g y f son mutuamente inversas respecto a la composición.*

Demostración. La condición sobre b_0 y b_1 es necesaria: si existe $f = \sum_{n\geq 0} a_n X^n$ con $a_0 = 0$ tal que

$$g \circ f = \sum_{n\geq 0} b_n f(X)^n = b_0 + b_1 a_1 X + b_2 (a_2 + a_1^2) X^2 + \cdots = X,$$

entonces $b_0 = 0$ y $b_1 a_1 = 1$.

Ahora sea g una serie con $b_0 = 0$ y $b_1 \neq 0$. Tenemos que encontrar una serie $f = \sum_{n\geq 0} a_n X^n$ con $a_0 = 0$ tal que $g \circ f = X$. La última identidad implica que necesitamos poner $a_1 := b_1^{-1}$. Luego, para $n \geq 2$, el coeficiente de X^n en $g \circ f$ es igual al coeficiente de X^n en la suma

$$b_1 f(X) + b_2 f(X)^2 + \cdots + b_n f(X)^n$$

(ya que $f(0) = 0$, en las potencias $f(X)^{n+1}, f(X)^{n+2}, \ldots$ ya no hay términos de grado n). Pero este coeficiente tiene que ser nulo, lo que nos da las ecuaciones

$$b_1 a_n + (\text{algún polinomio en } b_2, b_3, \ldots, b_n, a_1, a_2, \ldots, a_{n-1}) = 0.$$

Puesto que $b_1 \neq 0$, estas ecuaciones por inducción definen *de modo único* todos los coeficientes $a_2, a_3, a_4, \ldots$ Esto demuestra que f existe y es única.

Para ver que se tiene $f \circ g = X$, notamos que en f también $a_0 = 0$ y a_1 es invertible, entonces existe una serie única h tal que $f \circ h = X$. Luego, en la identidad $X = g \circ f$ podemos sustituir h en lugar de X para obtener $h = g \circ (f \circ h)$. Pero $f \circ h = X$, así que $h = g$. ∎

8.21. Corolario. *Sea $f = a_1 X + a_2 X^2 + a_3 X^3 + \cdots \in XR[[X]]$ una serie de potencias. Consideremos el endomorfismo*

$$\begin{aligned} \phi\colon R[[X]] &\to R[[X]], \\ X &\mapsto f \end{aligned}$$

que es constante sobre R y envía X a f. Entonces, ϕ es un isomorfismo si y solo si $f'(0) = a_1 \in R^\times$.

Demostración. Esto es esencialmente el lema anterior formulado de otra manera. Si f cumple la condición $f'(0) \in R^\times$, entonces existe una serie g tal que $f \circ g = g \circ f = X$, y basta definir ϕ^{-1} por $X \mapsto g$.

Viceversa, notamos que ϕ preserva el subconjunto de las series con coeficiente constante no nulo. Si ϕ es un isomorfismo, entonces ϕ preserva el complemento de este conjunto que es el ideal $XR[[X]]$. Luego, X es un generador de $XR[[X]]$, así que $f(X)$ tiene que ser un generador de $XR[[X]]$:

$$f\, R[[X]] = XR[[X]].$$

En particular, debe existir $h = b_0 + b_1 X + b_2 X^2 + \cdots \in R[[X]]$ tal que $fh = X$:

$$(a_1 X + a_2 X^2 + \cdots)(b_0 + b_1 X + b_2 X^2 + \cdots) = a_1 b_0 X + (a_2 b_0 + a_1 b_1) X^2 + \cdots = X$$

lo que implica que $b_0 = a_1^{-1}$. ∎

8.4 Lema de Hensel

Recordemos que el lema de Hensel para un cuerpo completo no arquimediano K afirma lo siguiente.

Si $f(X) \in O_K[X]$ un polinomio con coeficientes en O_K y $x_0 \in O_K$ satisface $\|f(x_0)\| < \|f'(x_0)\|^2$, entonces existe único $x \in O_K$ tal que $f(x) = 0$ y $\|x - x_0\| < \|f'(x_0)\|$.

En particular, si K es un cuerpo local no arquimediano, el anillo O_K es completo respecto al ideal maximal $\mathfrak{m}_K$. Si tenemos

$$f(x_0) \equiv 0 \pmod{f'(x_0)^2\, \mathfrak{m}_K},$$

esto implica que $\|f(x_0)\| < \|f'(x_0)^2\|$, y si

$$x \equiv x_0 \pmod{f'(x_0)\, \mathfrak{m}_K},$$

entonces

$$\|x - x_0\| < \|f'(x_0)\|.$$

Esto motiva el siguiente resultado general para anillos completos.

8.22. Teorema (Lema de Hensel para anillos completos). *Sea R un anillo completo respecto al ideal $\mathfrak{a}$ y sea $f(X) \in R[X]$ un polinomio. Para todo $x_0 \in R$ tal que*

$$f(x_0) \equiv 0 \pmod{f'(x_0)^2\, \mathfrak{a}}$$

existe $x \in R$ que cumple

$$f(x) = 0, \quad x \equiv x_0 \pmod{f'(x_0)\, \mathfrak{a}}.$$

Además, si $f'(x_0)$ no es un divisor de cero en R, entonces este x es único.

(Notamos que gracias a 8.5, el ideal $\mathfrak{a}$ en el enunciado puede ser reemplazado por $\mathfrak{a}^n$ para cualquier $n = 1, 2, 3, \ldots$)

Demostración. Para simplificar la notación, denotemos $z := f'(x_0)$. Si

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d,$$

entonces por la fórmula del binomio

$$f(x_0 + zX) = \sum_{0\le i\le d} a_i (x_0 + zX)^i = \sum_{0\le i\le d} a_i x_0^i + \underbrace{\left(\sum_{1\le i\le d} a_i\, i\, x_0^{i-1}\right)}_{f'(x_0)} zX + \sum_{1\le i\le d} a_i\, g_i(x_0, zX)\,(zX)^2,$$

donde $g_i(x_0, zX)$ es algún polinomio en x_0 y zX con coeficientes enteros (son ciertos coeficientes binomiales, pero no nos sirven las fórmulas explícitas). Esto significa que existe algún polinomio $h \in R[X]$ tal que

$$\begin{aligned} f(x_0 + zX) &= f(x_0) + f'(x_0)\, zX + h(X)\,(zX)^2 \\ &= f(x_0) + z^2\,(X + X^2\, h(X)). \end{aligned}$$

Podemos considerar el homomorfismo de R-álgebras definido por

$$\begin{aligned} \phi\colon R[[X]] &\to R[[X]], \\ X &\mapsto X + X^2\, h(X). \end{aligned}$$

Es un isomorfismo según 8.21, así que existe un homomorfismo inverso $\phi^{-1}\colon R[[X]] \to R[[X]]$. Al aplicarlo a la ecuación de arriba nos queda

$$f(x_0 + z\phi^{-1}(X)) = f(x_0) + z^2\,\phi^{-1}(X + X^2\, h(x)) = f(x_0) + z^2 X.$$

Según nuestra hipótesis, $f(x_0) \equiv 0 \pmod{z^2\mathfrak{a}}$; es decir, $f(x_0) = z^2 c$ para algún $c \in \mathfrak{a}$. Ahora según 8.19 existe un homomorfismo de R-álgebras definido por

$$\begin{aligned} \psi\colon R[[X]] &\to R, \\ X &\mapsto -c \end{aligned}$$

Al aplicarlo tenemos

$$f(x_0 + z\cdot\psi\circ\phi^{-1}(X)) = f(x_0) + z^2\,\psi(X) = f(x_0) - z^2\, c = 0,$$

así que

$$x = x_0 + z\cdot\psi\circ\phi^{-1}(X) \in R$$

es el elemento que estamos buscando. Notamos que $\psi\circ\phi^{-1}(X) \in \mathfrak{a}$. De hecho, siendo un isomorfismo, ϕ^{-1} debe enviar X a una serie en $XR[[X]]$, y luego $\psi(X) \in \mathfrak{a}$. Esto significa que

$$x \equiv x_0 \pmod{z\mathfrak{a}}.$$

Supongamos ahora que z no es un divisor de cero en R. Sea $x' \in R$ otro elemento que satisface

$$f(x') = f(x) = 0, \quad x' \equiv x \equiv x_0 \pmod{z\mathfrak{a}}.$$

Tenemos

$$x = x_0 + za, \quad x' = x_0 + za'$$

para algunos $a, a' \in \mathfrak{a}$. Consideremos los homomorfismos de R-álgebras $\beta, \beta'\colon R[[X]] \to R$ (??? check the errata for p. 201) definidos por

$$\begin{aligned} \beta&\colon X \mapsto a, \\ \beta'&\colon X \mapsto a'. \end{aligned}$$

Al aplicar β y β' a la identidad

$$f(x_0 + zX) = f(x_0) + z^2\,(X + X^2\,h(X))$$

nos queda

$$0 = f(x_0 + za) = f(x_0) + z^2\,(a + a^2\,h(a))$$

y

$$0 = f(x_0 + za') = f(x_0) + z^2\,(a' + a'^2\,h(a')).$$

En particular,

$$z^2\,(a + a^2\,h(a)) = z^2\,(a' + a'^2\,h(a')).$$

Usando que z no es un divisor de cero, tenemos

$$a + a^2\,h(a) = a' + a'^2\,h(a');$$

es decir,

$$\beta \circ \phi(X) = \beta' \circ \phi(X).$$

Pero la imagen de X define a un homomorfismo de R-álgebras $R[[X]] \to R$ de modo único, así que $\beta \circ \phi = \beta' \circ \phi$. Puesto que $\phi\colon R[[X]] \to R[[X]]$ es un isomorfismo, se puede concluir que $\beta = \beta'$. ■

El lector puede consultar mis apuntes

cadadr.org/san-salvador/2018-04-topologia-p-adica/hensel.pdf

para ver algunas aplicaciones típicas del lema de Hensel.