Álgebra conmutativa

José Cuevas Barrientos

3 de abril de 2024

Índice general

Introducción

El álgebra es el estudio de las estructuras matemáticas, esto es, conjuntos dotados de relaciones y/u operaciones que satisfacen una serie de condiciones que lo dotan de una *forma*. Ésto tal vez en principio difiera con la imagen que uno pueda tener del álgebra, pero hay varias consideraciones que tener de esta sentencia, por ejemplo, las estructuras son bastante comunes, los conjuntos numéricos son el ejemplo más importante, de hecho, abren la puerta a una pregunta más fundamental: ¿qué es un número? El lector puede creer que esto es una pregunta trivial ya que conoce números como 1, 0, π o $\sqrt{2}$. ¿Y qué hay de $\varnothing$? No, ésto es un conjunto. Sin embargo, von Neumann propone construir el conjunto de los naturales usando al conjunto vacío $\varnothing$ como sinónimo del 0. En efecto, la teoría de conjuntos nos otorga «materiales» bajo los cuales construimos todo nuestro universo de objetos, en consecuencia los números como tal no han de ser más que conjuntos, luego no es la «composición» del objeto lo que determina su cualidad de número o no.

Veamos otra característica, podríamos decir que el 1 se define como el sucesor del 0 en los naturales. Ésta definición es independiente de cómo definamos 0 o 1, ya sea con conjuntos conocidos o raros, pero sino de cómo se relacionan los elementos de éste conjunto. En este sentido, el conjunto $S := \{1, 0, \pi, \sqrt{2}\}$ no es numérico, ya que carece de propiedades básicas como que $\pi + \pi = 2\pi \notin S$ (a menos claro que redefinamos $+$ para S). Pero ésto conlleva a una apreciación elemental, S puede ser numérico dependiendo de cómo se definen sus operaciones; a ésto es lo que se le dice una *estructura*. Ésto también nos obliga a definir una manera de decir que dos estructuras tienen la misma forma, pero pueden definir en composición, un ejemplo sería encontrar un método para señalar que los conjuntos $\{0, 1, 2, \dots\}$ y {cero,

uno, dos, ...} son, en esencia, la misma estructura. La sentencia empleada para señalar este hecho es «las estructuras son isomorfas». Por supuesto cabe preguntarse ¿la misma estructura en qué sentido? Pues los conjuntos pueden «concordar» en la suma, pero «diferir» en el producto, a lo que se le añade un apellido al término de isomorfismo, por ejemplo: son isomorfas en orden, o isomorfas como espacios vectoriales, etc. Con éste preámbulo, el rol del álgebra se ve más claro, y también se comprende una división del álgebra respecto de las estructuras que estudia.

Para muchos fines, una de las estructuras más básicas (en términos de condiciones) son los *grupos* al que dedicamos un largo capítulo para ver en detalle. Algo de lo que el lector se va a percatar es que mientras más básicas sean las estructuras, más libertades poseen de modo que su estudio suele o verse fragmentado (según añadir más condiciones, como finitud o conmutatividad) o simplemente no puede profundizar demasiado; como es el caso con la teoría nativa de conjuntos, que eventualmente rota entre otros temas más específicos como números ordinales o cardinales para tener más información, pero es aún muy amplia en contextos genéricos, como el axioma de elección demuestra. Al igual que la teoría de conjuntos es vital para comprender o leer otros conceptos en matemáticas, la teoría de grupos es vital para escribir el resto del álgebra. A veces puede sentirse como innecesaria, pero vuelve en contextos inesperados, como en el grupo especial en la teoría de matrices, o el grupo de Galois en la teoría de extensión de cuerpos.

Una de las complicaciones de mi estudio del álgebra es el ¿cómo enseñar eficazmente el álgebra? Es muy común que el primer acercamiento a las «matemáticas abstractas» de varios estudiantes es a través del álgebra lineal, pero la mayoría de textos, inspirados sobretodo en la doctrina de Bourbaki, es comenzar con un tema mucho menos concreto que es la teoría de grupos (si es que yo también tomo ésta decisión fue por seguir los principales libros de álgebra con los que aprendí) y luego ver brevemente el tema de anillos para llegar a módulos. Personalmente, decidí dar un enfoque más cercano al álgebra lineal en el primer capítulo de módulos, para luego retomarlo y enfocarlo hacia la llamada «álgebra conmutativa»; sin embargo, aún incluso después de tanto tiempo de re-editar el texto no me veo del todo convencido, ésto lo menciono para que el lector se sienta con las riendas libres de leer el texto en un orden más o menos libre, pese a que existe una obvia recomendación.

Escritura técnica

Las referencias han sido particularmente un tema móvil dentro de mis apuntes. La bibliografía ha sido planeada en tanto a materiales que empleo directamente y con muy pequeñas excepciones he citado demostraciones en lugar de reproducirlas reorganizadas, de modo que las referencias son textos que he seguido y que considero buenas recomendaciones a seguir también. La escritura del álgebra ha tenido referencias clave que han mutado con el tiempo: durante décadas fueron fundamentales los textos de N. Bourbaki y W. van der Waerden, pero tomo como piedra angular el libro de Lang **[0],** aunque recomiendo mucho más la lectura del Aluffi **[0]** para principiantes. Materiales más completos y extensos lo son los tomos de Rotman **[0]** y, uno de mis preferidos, Jacobson **[0].**

Luego podemos detenernos a materiales más específicos de determinados temas: **[0]** es un libro enfocado en demostraciones del teorema fundamental del álgebra y, por ello, recurre a varios tópicos del álgebra siempre con una motivación y un norte claros; una buena introducción al álgebra, enfocada en cuerpos y anillos conmutativos se puede encontrar en Nagata **[0].** Sobre el álgebra conmutativa, el libro de Atiyah y McDonald **[1]** es la introducción estándar, y el material más sintético de todos; de él se recomienda pasar a Eisenbud **[3]** que es mucho más extenso, pero mantiene una estrecha relación con la geometría algebraica; también el Matsumura **[4]** es una buena continuación, pero el más completo (y por tanto más difícil) es su otro libro **[5].**

1

Compleciones y teoría de la dimensión

1.1 Series de potencias

Definición 1.1 (Notación de multi-índice): Un *multi-índice* α es una tupla de números naturales $\alpha = (\alpha_1, \ldots, \alpha_n)$. Si $\boldsymbol{x} = (x_1, \ldots, x_n)$ es una tupla de indeterminadas, entonces se admiten las siguientes notaciones:

$$\begin{aligned} \alpha + \beta &:= (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n), \\ \boldsymbol{x}^\alpha &:= x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \\ |\alpha| &:= \alpha_1 + \cdots + \alpha_n. \end{aligned}$$

De éste modo, podemos denotar un polinomio de varias indeterminadas $p(\boldsymbol{x}) \in A[\boldsymbol{x}]$ y de grado n como

$$p(\boldsymbol{x}) = \sum_{|\alpha| \leq n} c_\alpha \boldsymbol{x}^\alpha.$$

Ésta notación será útil para la siguiente definición:

Definición 1.2: Sea A un dominio. Una *serie formal de potencias* es un objeto de la forma

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n \geq 0} a_n x^n,$$

donde, al contrario de lo que sucede con los polinomios, pueden haber «infinitos términos». Como los anillos no admiten inicialmente una noción de «suma infinita» por ello enfatizamos que las series son objetos *formales*. Se denota $A[[S]]$ al conjunto de series formales de potencias con coeficientes en A y cuyas indeterminadas están en el conjunto S.

Sea $A[[\boldsymbol{x}]]$ un anillo formal de potencias sobre una tupla de indeterminadas $\boldsymbol{x}$. Se definen la suma y el producto sobre A, así:

$$f(x) := \sum_{\alpha} c_\alpha \boldsymbol{x}^\alpha, \qquad g(x) := \sum_{\alpha} d_\alpha \boldsymbol{x}^\alpha$$

$$f(x) + g(x) := \sum_{\alpha} (c_\alpha + d_\alpha)\boldsymbol{x}^\alpha,$$

$$f(x) \cdot g(x) := \sum_{\alpha} \left(\sum_{\beta+\gamma=\alpha} c_\beta d_\gamma \right) \boldsymbol{x}^\alpha,$$

donde α, β, γ recorren multi-índices. Con ésto es fácil notar que, efectivamente, $A[[\boldsymbol{x}]]$ es un anillo.

En el caso de $A[[x]]$ será útil definir la noción de orden. Sea $f(x) = \sum_{n\geq 0} a_n x^n \in A[[x]]$ no nulo, entonces se define:

$$\operatorname{ord} f := \min\{m : a_m \neq 0\}.$$

En $A[x]$ se daba que todos los inversibles coincidían con los de A. Pero aquí, la historia es un tanto distinta:

Ejemplo. Considere la serie $f(x) := 1 - x = \sum_{n\geq 0} a_n x^n \in \mathbb{Z}[[x]]$ y considere la serie geométrica

$$g(x) := 1 + x + x^2 + x^3 + \cdots = \sum_{n\geq 0} b_n x^n.$$

Ahora, nótese que

$$f(x) \cdot g(x) = 1 + \sum_{n\geq 1} \left(\sum_{i+j=n} a_i b_j \right) x^n = 1 + \sum_{n\geq 1} (a_0 b_n + a_1 b_{n-1}) x^n = 1.$$

Es decir, $f(x) = g(x)^{-1}$.

Una primera pista de como encontrar inversibles es lo siguiente:

Proposición 1.3: Sea A un dominio.

1. Sean $f, g \in A[[x]]$ no nulos, entonces $\operatorname{ord}(f \cdot g) \geq \operatorname{ord} f + \operatorname{ord} g$. En consecuencia, los inversibles de $A[[x]]$ tienen orden cero.
2. Si A es un dominio íntegro, entonces se alcanza la igualdad. En particular, si A es un dominio íntegro, entonces $A[[x]]$ también.

Esto conlleva a la siguiente generalización:

Proposición 1.4: $f(x) \in A[[x]]$ es inversible syss $f(x) = a + xg(x)$ con $g(x) \in A[[x]]$ y $a \in A^\times$. En particular, si A es un cuerpo, entonces los inversibles son exactamente las series de orden cero.

Demostración: Sea $f(x) \equiv a \pmod{\deg 1}$ con a inversible. Entonces $a^{-1}f(x)$ tiene término constante 1, así que nos reduciremos a dicho caso. Sea $f(x) = 1 - h(x) \in A[[x]]$ con h nulo o con $\operatorname{ord} h > 0$. En el primer caso es claro, y en el segundo caso definimos

$$g(x) := 1 + h + h^2 + \cdots \in A[[x]]$$

y notamos, por el mismo razonamiento, que $g(x) = f(x)^{-1}$. Podemos definir bien a $g(x)$, ya que $g(x) \equiv 1 + h + h^2 + \cdots + h^{n-1} \pmod{\deg n}$ para todo n, lo que significa que cada coeficiente se escribe mediante finitas operaciones sobre finitos coeficientes de $h(x)$. □

Proposición 1.5: Sea S un conjunto de indeterminadas, A un dominio y k un cuerpo. Entonces:

1. $(S) \subseteq \mathfrak{J}(A[[S]])$.
2. $\big(k[[S]], (S), k\big)$ es un anillo local.
3. Si $\mathfrak{a} \trianglelefteq A$, entonces $A[[S]]/\mathfrak{a}[[S]] = (A/\mathfrak{a})[[S]]$
4. Si $\mathfrak{a} \trianglelefteq A$ es finitamente generado, entonces $\mathfrak{a}[[S]] = \mathfrak{a} \cdot A[[S]]$.

Trabajar con $A[[x]]$ en lugar de $A[x]$ es un cambio radical. En principio, no es evidente donde los elementos de $A[[x]]$ pueden evaluarse, exceptuando en $\mathfrak{N}(A)$ en donde los objetos eventualmente de anulan. Otra cuestión es que tampoco es fácil estudiar $A[[x]]$ como anillo: ¿por ejemplo, si A es noetheriano, se cumplirá que $A[[x]]$ también? Para la primera pregunta, tenemos una acorazonada: en $\mathbb{R}$ podemos evaluar las series de potencias en

determinados puntos no nulos, pero para ello empleamos la noción de «convergencia» que es perteneciente al reino de la topología. Resulta que ambas dudas serán resueltas empleando herramientas topológicas, lo que nos da, entre otras cosas, una excusa para hablar de compleciones.

1.2 Compleciones

Definición 1.6: Un ***grupo topológico*** es un grupo $(G, \cdot)$ tal que la operación de grupo $- \cdot -\colon G \times G \to G$ y la inversión $()^{-1}\colon G \to G$ son funciones continuas.

Una de las ventajas de una definición aparentemente tan sencilla es que toda la topología está completamente determinada por el comportamiento cerca del 0.

En éste capítulo, trabajaremos con grupos abelianos topológicos, por lo que adoptaremos la notación aditiva, aunque varios teoremas aplican en el caso general. Será útil notar que las traslaciones $\bullet + g$ y la inversión $-\bullet$ son homeomorfismos del grupo topológico.

Lema 1.7: Sea G un grupo abeliano topológico, y sea

$$H := \bigcap \{U : 0 \in U, U \text{ es abierto}\}.$$

Entonces:

1. H es un subgrupo de G.
2. $H = \overline{\{0\}}$.
3. G/H (como grupo y espacio topológico cociente) es de Hausdorff.
4. G es de Hausdorff syss $H = \{0\}$.

Demostración:

1. Sea $x \in H$. Nótese que si U es un entorno del 0, entonces $-U$ también, de modo que $x \in U$ y $x \in -U$, luego $-x \in H$.

   Sea $y \in H$ y U un entorno abierto del 0. Como $y \in U$, luego $0 \in U - y$ y es, por tanto, un entorno del 0, con lo que $x \in U - y$ y luego $x + y \in U$.

2. Nótese que $x \in H$ syss todo entorno del 0 corta a x, es decir, syss x es de acumulación de $\{0\}$. □

Definición 1.8: Si G es un grupo topológico 1AN,[1] entonces una sucesión $(x_n)_{n\in\mathbb{N}} \subseteq G$ se dice ***de Cauchy*** si para todo entorno básico U del 0 existe un $n_0 \in \mathbb{N}$ tal que para todo $n, m \geq n_0$ se satisface que $x_n - x_m \in U$.

Dos sucesiones de Cauchy $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}$ se dicen ***equivalentes*** si $\lim_n x_n - y_n = 0$.

Proposición 1.9: Sea G un grupo topológico 1AN, entonces la relación de «ser equivalentes» en el conjunto de sucesiones de Cauchy de G es una relación de equivalencia. El conjunto cociente dado por dicha relación se denota por $\hat{G}$. Entonces, $\hat{G}$ es un grupo en un sentido canónico, y la aplicación

$$\begin{aligned} \varphi\colon G &\longrightarrow \hat{G} \\ x &\longmapsto [(x, x, x, \dots)] \end{aligned}$$

es un homomorfismo de grupos. Más aún, G es de Hausdorff syss φ es inyectiva.

Una desventaja es que momentaneamente aún carecemos de una topología canónica sobre $\hat{G}$, para ésto necesitamos cambiar un poco la perspectiva.

Para ello tenemos que transitar al concepto categorial de límite inverso. Comencemos con una cadena descendientes de subgrupos de G:

$$G =: G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots,$$

luego tomando cocientes por G se induce el siguiente diagrama (en Ab):

$$G/G_0 \xleftarrow{\pi_1} G/G_1 \xleftarrow{\pi_2} G/G_2 \longleftarrow \cdots$$

Donde $\pi_i\colon G/G_i \to G/G_{i-1}$ es la típica proyección (dada puesto que $\frac{G/G_i}{G_{i-1}/G_i} \cong \frac{G}{G_{i-1}}$ por el tercer teorema de isomorfismos). Intuitivamente los G/G_n's se van haciendo cada vez más grandes y en el límite debería ser $\hat{G}$, pero eso hay que demostrarlo.

Aquí conviene también notar que Ab es una categoría completa (i.e., posee límites inversos, cf. [**45,** Teo. 2.11]), de modo que ésto siempre está bien definido. Más aún, el funtor olvidadizo $U : \mathsf{Ab} \to \mathsf{Set}$ preserva y refleja límites inversos (cf. [**45,** Prop. 2.21]) y es fácil describir los límites inversos de Set (cf. [**45,** Prop. 2.16]).

Éstas observaciones categoriales no son necesarias, pero sí recomendables. En la práctica, en éste capítulo describiremos los límites inversos de necesitarles.

[1] Abreviación de «primer axioma de numerabilidad» (cf. [**48,** Def. 2.30, p. 43]).

Definición 1.10: Se dice que $(A_n)_{n\in\mathbb{N}}$ es un ***sistema inverso*** si corresponde a un diagrama de la forma:

$$A_0 \xleftarrow{\alpha_1} A_1 \xleftarrow{\alpha_2} A_2 \longleftarrow \cdots$$

La manera de calcular el límite inverso de un sistema inverso es la siguiente: primero consideras el producto $A := \prod_{n\in\mathbb{N}} A_n$ y luego consideras el homomorfismo:

$$\begin{aligned} f\colon A &\longrightarrow A \\ \big(a_n\big)_n &\longmapsto \big(a_n - \alpha_{n+1}(a_{n+1})\big)_n \end{aligned}$$

luego $\ker f$ es el conjunto de tuplas $(a_n)_{n\in\mathbb{N}}$ tales que $\alpha_{n+1}(a_{n+1}) = a_n$ para todo $n \in \mathbb{N}$, es decir, $\ker f = \varprojlim_n A_n$. Decimos que el sistema inverso $(A_n)_n$ es un ***sistema suprayectivo*** si el homomorfismo f es suprayectivo. Ésta construcción también nos otorga el límite inverso sobre módulos.

Definición 1.11: Se dice que una cadena $(G_n)_{n\in\mathbb{N}}$ descendiente de subgrupos de un grupo topológico G *induce su topología* si para todo entorno U del 0 se satisface que existe $n \in \mathbb{N}$ tal que $G_n \subseteq U$.

Nótese que una cadena que induce su topología da, indirectamente, una base de entornos del 0, pero como todas las bases de entornos de todos los puntos son las mismas salvo traslación, entonces se concluye que, en cierto modo, una sola cadena decodifica toda la información del espacio.

Proposición 1.12: Sea G un grupo topológico 1AN. Dada una cadena descendiente $(G_n)_{n\in\mathbb{N}}$ de subgrupos de G tal que para todo entorno U del 0 exista un n con $G_n \subseteq U$, entonces $\varprojlim_{n\in\mathbb{N}} G/G_n \cong \hat{G}$ (en Ab).

Demostración: Sea $\boldsymbol{x} := (x_n)_{n\in\mathbb{N}}$ una sucesión de Cauchy en G. Fíjese un n, nótese que, por definición, para m eventualmente grande se satisface que $x_{m+1} - x_m \in G_n$, o lo que es equivalente, la clase lateral $x_m G_n$ es eventualmente constante. Luego podemos definir $\varphi_n\colon \hat{G} \to G/G_n$ como dicho $\varphi_n(\boldsymbol{x}) = x_m$ y queda al lector comprobar que está bien definido y que corresponde a un homomorfismo de grupos.

Finalmente, supongamos que existe otro grupo abeliano L con homomorfismos $\psi_n \in \mathrm{Hom}_{\mathsf{Ab}}(L, G/G_n)$ tales que $\psi_{n+1} \circ \theta_{n+1} = \psi_n$. Luego a cada $g \in L$ podemos asignarle una sucesión de Cauchy eligiendo elementos de la clase de equivalencia de $\psi_n(g) \in G/G_n$ en la n-ésima coordenada. Nótese

que ésta sucesión es efectivamente de Cauchy puesto que se estabiliza trivialmente para todo G_n, y naturalmente, queda al lector ver que ésta aplicación está bien definida y es homomorfismo. □

Proposición 1.13: Sean $(A_n)_n, (B_n)_n, (C_n)_n$ sistemas inversos de Ab, dotados de flechas:

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_{n+1} & \xrightarrow{f_{n+1}} & B_{n+1} & \xrightarrow{g_{n+1}} & C_{n+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \beta_{n+1}} & & \downarrow{\scriptstyle \gamma_{n+1}} & & \\
0 & \longrightarrow & A_n & \xrightarrow[f_n]{} & B_n & \xrightarrow[g_n]{} & C_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

tales que el diagrama entero conmuta y todas las filas son exactas. Entonces se induce una sucesión exacta:

$$0 \longrightarrow \varprojlim_n A_n \xrightarrow{\bar{f}} \varprojlim_n B_n \xrightarrow{\bar{g}} \varprojlim_n C_n$$

Y más aún, si $(A_n)_n$ es un sistema suprayectivo, entonces la sucesión

$$0 \longrightarrow \varprojlim_n A_n \xrightarrow{\bar{f}} \varprojlim_n B_n \xrightarrow{\bar{g}} \varprojlim_n C_n \longrightarrow 0$$

es exacta.

Demostración: Nótese que por la propiedad universal del producto el siguiente diagrama conmuta para todo j:

$$\begin{array}{ccccc}
\prod_{n\in\mathbb{N}} A_n & \overset{\exists!\hat{f}}{\dashrightarrow} & \prod_{n\in\mathbb{N}} B_n & \overset{\exists!\hat{g}}{\dashrightarrow} & \prod_{n\in\mathbb{N}} C_n \\
\downarrow{\scriptstyle \pi_j^A} & & \downarrow{\scriptstyle \pi_j^B} & & \downarrow{\scriptstyle \pi_j^A} \\
A_j & \xrightarrow[f_j]{} & B_j & \xrightarrow[g_j]{} & C_j
\end{array}$$

Definamos $A := \prod_{n\in\mathbb{N}} A_n, B := \prod_{n\in\mathbb{N}} B_n, C := \prod_{n\in\mathbb{N}} C_n$ y sea

$$d^A \colon A \longrightarrow A$$

$$(a_n)_n \longmapsto \big(a_n - \alpha_{n+1}(a_{n+1})\big)_n$$

el cual es un homomorfismo de grupos abelianos, y análogamente para B y C. La particularidad es que $\ker(d^A) = \varprojlim_n A_n$ (¿por qué?), de modo que tenemos el siguiente diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A} & & \downarrow{\scriptstyle d_B} & & \downarrow{\scriptstyle d_C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

el cual conmuta y donde las filas son exactas. Finalmente, por el lema de la serpiente se concluye que

$$0 \longrightarrow \ker(d^A) \longrightarrow \ker(d^B) \longrightarrow \ker(d^C) \longrightarrow \operatorname{coker}(d^A) \longrightarrow \cdots$$

Finalmente, nótese que si $(A_n)_n$ es un sistema suprayectivo, entonces d^A también lo es y $\operatorname{coker}(d^A) = 0$. □

Corolario 1.13.1: Dada una sucesión exacta:

$$0 \longrightarrow G' \longrightarrow G \xrightarrow{p} G'' \longrightarrow 0$$

de grupos abelianos, una cadena descendiente $(G_n)_n$ de subgrupos de G tal que G' posee la topología inducida por la cadena $(G' \cap G_n)_n$ y G'' la inducida por la cadena $\big(p[G_n]\big)_n$. Entonces, al siguiente es una sucesión exacta:

$$0 \longrightarrow \hat{G}' \longrightarrow \hat{G} \longrightarrow \hat{G}'' \longrightarrow 0$$

Corolario 1.13.2: $\hat{G}/\hat{G}_n \cong G/G_n$ y de hecho $\hat{\hat{G}} = G$.

Definición 1.14: Un grupo topológico G se dice ***completo*** si $G \cong \hat{G}$.

Finalmente, ahora podemos pasar a la cuestión acerca de la topología sobre $\hat{G}$. En particular, si volvemos al caso de los módulos, podemos encontrar una descripción conveniente para el problema.

Definición 1.15: Sea M un A-módulo. Una cadena descendiente de submódulos

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

se dice una ***filtración***. Dado un ideal $\mathfrak{a} \trianglelefteq A$, se dice que $(M_n)_{n\in\mathbb{N}}$ es una ***$\mathfrak{a}$-filtración*** si es una filtración y $\mathfrak{a}M_n \subseteq M_{n+1}$ para todo $n \in \mathbb{N}$. Una $\mathfrak{a}$-filtración $(M_n)_{n\in\mathbb{N}}$ se dice ***estable*** si $\mathfrak{a}M_n = M_{n+1}$ para n suficientemente grande.

Lema 1.16: Sean $(M_n)_{n\in\mathbb{N}}$ y $(M'_n)_{n\in\mathbb{N}}$ dos $\mathfrak{a}$-filtraciones estables de M. Entonces poseen diferencia acotada, es decir, existe n_0 tal que $M_{n+n_0} \subseteq M'_n$ y $M'_{n+n_0} \subseteq M_n$. En consecuente $\varprojlim_n M/M_n \cong \varprojlim_n M/M'_n$ (en Top).

Demostración: Basta probarlo para $M'_n = \mathfrak{a}^n M$. Como $(M_n)_n$ es una $\mathfrak{a}$-filtración, entonces $\mathfrak{a}M_n \subseteq M_{n+1}$ y luego, por inducción, $M'_{n+1} = \mathfrak{a}^{n+1}M \subseteq M_{n+1}$. Como $(M_n)_n$ es estable, entonces existe n_0 tal que para todo $n \geq n_0$ se satisface que $\mathfrak{a}M_n = M_{n+1}$, luego $M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subseteq \mathfrak{a}^n M = M'_n$. □

Definición 1.17: La topología sobre $\hat{M}$ tal que $\hat{M} \cong \varprojlim_n M/\mathfrak{a}^n M$ se dice la ***topología $\mathfrak{a}$-ádica***.

1.3 Anillos y módulos graduados

Definición 1.18: Sea A un dominio y sea $\mathfrak{a} \trianglelefteq A$. Se define la ***álgebra de Rees*** de $\mathfrak{a}$ como:[2]

$$A[\mathfrak{a}t] = \mathrm{Bl}_{\mathfrak{a}}(A) := A \oplus \mathfrak{a}t \oplus \mathfrak{a}^2t^2 \oplus \cdots = \bigoplus_{n\in\mathbb{N}} \mathfrak{a}^n t^n.$$

Sea M un A-módulo. Dada una filtración $\mathcal{J} = (M_n)_{n\in\mathbb{N}}$ se define el ***módulo de Rees*** de $\mathcal{J}$ como:

$$\mathrm{Bl}_{\mathcal{J}}(M) := M \oplus M_1 \oplus M_2 \oplus \cdots = \bigoplus_{n\in\mathbb{N}} M_n.$$

La álgebra de Rees $\mathrm{Bl}_{\mathfrak{a}}(A)$ es claramente una A-álgebra graduada. Si $\mathcal{J}$ se elige como una $\mathfrak{a}$-filtración de M, entonces $\mathrm{Bl}_{\mathcal{J}}(M)$ es un $\mathrm{Bl}_{\mathfrak{a}}(A)$-módulo graduado. Además, si A es noetheriano, entonces $\mathfrak{a} = (\alpha_1, \ldots, \alpha_s)$ y por tanto $\mathrm{Bl}_{\mathfrak{a}}(A) = A[\alpha_1, \ldots, \alpha_s]$, luego por bases de Hilbert es noetheriano.

Lema 1.19: Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal de A, M un A-módulo finitamente generado y $\mathcal{J} := (M_n)_{n\in\mathbb{N}}$ una $\mathfrak{a}$-filtración de M. Son

[2] Atiyah y McDonald [**1**] emplea la notación A^*. El texto Bl es una abreviación de *blowup*, ya que ésta álgebra está relacionada a las *explosiones* (eng. *blowups*) en geometría algebraica.

equivalentes:

1. $\mathrm{Bl}_{\mathcal{J}}(M)$ es un $A[\mathfrak{a}t]$-módulo finitamente generado.
2. La filtración $\mathcal{J}$ es $\mathfrak{a}$-estable.

Demostración: Sea $Q_n := \bigoplus_{r=0}^{n} M_r$ y sea

$$M_n^* := M_0 \oplus M_1 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \cdots = Q_n \oplus \mathfrak{a}M_n \oplus \cdots ,$$

el cual es un $A[\mathfrak{a}t]$-módulo graduado finitamente generado. Como $\mathrm{Bl}_{\mathcal{J}}(M) = \bigcup_{n\in\mathbb{N}} Q_n = \bigcup_{n\in\mathbb{N}} M_n^*$, entonces se satisface que $\mathrm{Bl}_{\mathcal{J}}(M)$ es noetheriano syss la cadena M_n^* se estabiliza, es decir, syss $M_n^* = M_{n+1}^* = \cdots = M^*$ desde algún n en adelante. □

Proposición 1.20 (lema de Artin-Rees): Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal de A, M un A-módulo finitamente generado y $(M_n)_{n\in\mathbb{N}}$ una $\mathfrak{a}$-filtración estable de M. Si M' es submódulo de M, entonces $(M' \cap M_n)_n$ es una $\mathfrak{a}$-filtración estable de M'.

Demostración: Basta notar que:

$$\mathfrak{a}(M' \cap M_n) = \mathfrak{a}M' \cap \mathfrak{a}M_n \subseteq M' \cap M_{n+1},$$

por lo que $(M' \cap M_n)_n$ es una $\mathfrak{a}$-filtración. Para comprobar estabilidad emplee el lema anterior. □

En el caso particular de $M_n = \mathfrak{a}^n M$ se obtiene que:

Corolario 1.20.1: Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal de A, M un A-módulo finitamente generado y M' un submódulo de M. Existe un entero r tal que para todo $n \geq r$ se satisface que

$$(\mathfrak{a}^n M) \cap M' = \mathfrak{a}^{n-r}((\mathfrak{a}^r M) \cap M').$$

Algunos textos le llaman a éste corolario el lema de Artin-Rees.
Otra consecuencia es la siguiente:

Teorema 1.21: Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal de A, M un A-módulo finitamente generado y M' un submódulo de M. Entonces las filtraciones $(\mathfrak{a}^n M')_n$ y $((\mathfrak{a}^n M) \cap M')_n$ tienen diferencia acotada. En consecuencia, la $\mathfrak{a}$-topología sobre M' es la topología subespacio de la $\mathfrak{a}$-topología sobre M.

Proposición 1.22: Sean A un dominio noetheriano y M_1, M_2, M_3 un trío de A-módulos finitamente generados. Dada la siguiente sucesión exacta

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

entonces se induce la siguiente sucesión exacta

$$0 \longrightarrow \hat{M_1} \longrightarrow \hat{M_2} \longrightarrow \hat{M_3} \longrightarrow 0.$$

En resumen, $\widehat{(-)} : \mathsf{Mod}_A \to \mathsf{Mod}_{\hat{A}}$ es un funtor exacto.

Proposición 1.23: Sea A un dominio y M un A-módulo finitamente generado. Sea

$$\hat{A} \otimes_A M \hookrightarrow \hat{A} \otimes_A \hat{M} \longrightarrow \hat{A} \otimes_{\hat{A}} \hat{M} = \hat{M}$$

(φ es la composición de las dos flechas)

entonces φ es suprayectiva. Más aún, si A es noetheriano, φ es isomorfismo.

Demostración: Por la proposición anterior se induce:

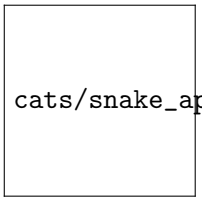
$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & M \otimes N & \longrightarrow & N & \longrightarrow & 0 \\ & & & & \Downarrow & & & & \\ 0 & \longrightarrow & \hat{M} & \longrightarrow & \widehat{M \otimes N} & \longrightarrow & \hat{N} & \longrightarrow & 0 \end{array}$$

Luego, para todo F libre se satisface, por inducción, que $\hat{A} \otimes_A F = \hat{F}$. Si M es finitamente generado, entonces $M \cong F/N$, donde F es libre y F, N son finitamente generados. Luego aplicando tensores se tiene que:

$$\begin{array}{ccccccccc} & & \hat{A} \otimes_A N & \longrightarrow & \hat{A} \otimes_A F = \hat{F} & \xrightarrow{\phi} & \hat{A} \otimes_A M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & \hat{N} & \longrightarrow & \hat{F} & \xrightarrow{\delta} & \hat{M} & \longrightarrow & 0 \end{array}$$

Donde éste diagrama conmuta, la primera fila es exacta en Mod_A y los α, β, γ son homomorfismos de módulos, pero la segunda fila es exacta sólo en Ab. Aún así, empleando que $\phi \circ \alpha = \beta \circ \delta$ es suprayectiva, se concluye que α también lo es.

Si A es noetheriano, entonces ahí la segunda fila sí está en Mod_A y por lema de la serpiente:



de lo que se sigue que $\ker \alpha = 0$ como se quería ver. □

Proposición 1.24: Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal de A, y $\hat{A}$ la compleción $\mathfrak{a}$-ádica de A. Entonces se cumplen:

1. $\hat{A}$ es una A-álgebra plana.
2. $\hat{\mathfrak{a}} = \mathfrak{a}\hat{A} \cong \hat{A} \otimes_A \mathfrak{a}$.
3. $\widehat{(\mathfrak{a}^n)} = (\hat{\mathfrak{a}})^n$.
4. $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$.
5. $\hat{\mathfrak{a}} \subseteq \mathfrak{J}(\hat{A})$.

Demostración: Veamos la 5: Sea $x \in \hat{\mathfrak{a}}$, luego se cumple que

$$(1-x)^{-1} = 1 + x + x^2 + x^3 + \cdots$$

el cual (visto como sucesión de sumas parciales) converge en $\hat{A}$ pues es completo en la topología $\mathfrak{a}$-ádica. Finalmente si $1 - x$ es inversible, entonces $x \in \mathfrak{J}(\hat{A})$. □

Corolario 1.24.1: Sea $(A, \mathfrak{m}, k)$ noetheriano local, y sea $\hat{A}$ su compleción $\mathfrak{m}$-ádica. Entonces $(\hat{A}, \hat{\mathfrak{m}}, k)$ es local.

Proposición 1.25: Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal de A, M un A-módulo finitamente generado y $\hat{M}$ la compleción $\mathfrak{a}$-ádica de M. Entonces:

$$E := \ker(M \to \hat{M}) = \bigcap_{n\in\mathbb{N}} \mathfrak{a}^n M = \{\boldsymbol{m} \in M : \exists x \in \mathfrak{a}\ (1+x)\boldsymbol{m} = \vec{0}\}.$$

Demostración: Veamos que los elementos de E se anulan para algún $1-\alpha$ con $\alpha \in \mathfrak{a}$: Como $E = \overline{\{\vec{0}\}}$, entonces E es el único entorno del $\vec{0}$ en el subespacio E. Como $\mathfrak{a}E \subseteq E$ es abierto y contiene al $\vec{0}$, entonces $\mathfrak{a}E = E$. Como A es noetheriano y M es finitamente generado, entonces E es

finitamente generado y luego por el lema de Nakayama (inciso 1) se cumple que $(1-\alpha)E = 0$ con $\alpha \in \mathfrak{a}$.

Para ver la contención restante, sea $(1-\alpha)\boldsymbol{m} = \vec{0}$, luego

$$\boldsymbol{m} = \alpha\boldsymbol{m} = \alpha^2\boldsymbol{m} = \cdots \in \bigcap_{n\in\mathbb{N}} \mathfrak{a}^n M. \qquad \square$$

Corolario 1.25.1: Sea A es un dominio noetheriano íntegro y $\mathfrak{a} \lhd A$. Entonces

$$\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = 0.$$

Teorema 1.26 (de las intersecciones de Krull): Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal contenido en $\mathfrak{J}(A)$ y M un A-módulo finitamente generado. Entonces:

$$\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n M = 0,$$

es decir, la $\mathfrak{a}$-topología sobre M es de Hausdorff.

Corolario 1.26.1: Sea $(A, \mathfrak{m})$ un dominio noetheriano local y M un A-módulo finitamente generado. Entonces la $\mathfrak{m}$-topología sobre M es de Hausdorff. En particular, la $\mathfrak{m}$-topología sobre A es de Hausdorff.

Corolario 1.26.2: Sea A un dominio noetheriano y $\mathfrak{p}$ un ideal primo. Entonces el $\ker(A \to A_{\mathfrak{p}})$ es la intersección de todos los ideales $\mathfrak{p}$-primarios.

Demostración: Nótese que $(A_{\mathfrak{p}}, \mathfrak{m})$ es local con $\mathfrak{m} := \mathfrak{p}A_{\mathfrak{p}}$, entonces por el corolario anterior, $A_{\mathfrak{p}}$ es de Hausdorff, vale decir,

$$\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = (0) \implies \bigcap_{\mathfrak{q}} \mathfrak{q}^n = \ker(A \to A_{\mathfrak{p}})$$

donde el « $\implies$ » sale del teorema de la correspondencia, y $\mathfrak{q}$ recorre los $\mathfrak{q}^n = \mathfrak{p}$, es decir, recorre los $\mathfrak{p}$-primarios. $\square$

Definición 1.27: Sea $\mathfrak{a}$ un ideal de A, se define:

$$\mathrm{gr}_{\mathfrak{a}}(A) := \frac{\mathrm{Bl}_{\mathfrak{a}}(A)}{\mathfrak{a}\,\mathrm{Bl}_{\mathfrak{a}}(A)} = \bigoplus_{n\in\mathbb{N}} \mathfrak{a}^n/\mathfrak{a}^{n+1},$$

el cual es un anillo graduado. Obviamos el subíndice $\mathfrak{a}$ cuando no haya ambigüedad sobre los signos.

Sea M un A-módulo y $\mathcal{J} := (M_n)_{n\in\mathbb{N}}$ una $\mathfrak{a}$-filtración, se define:

$$\mathrm{gr}_{\mathcal{J}}(M) := \bigoplus_{n\in\mathbb{N}} M_n/M_{n+1},$$

el cual es un $\mathrm{gr}_{\mathfrak{a}}(A)$-módulo graduado. Obviaremos el subíndice cuando la filtración esté implícita.

En lo sucesivo emplearemos la siguiente aplicación:

$$\begin{aligned} \mathrm{in}\colon A &\longrightarrow \mathrm{gr}_{\mathfrak{a}}(A) \\ a &\longmapsto (a \bmod \mathfrak{a}^n)_{n\in\mathbb{N}}. \end{aligned}$$

donde, si $a \notin \mathfrak{a}^n$, entonces rellenamos con ceros hasta el final. Si A es noetheriano y $\mathfrak{a}$ es un ideal propio, entonces se tiene que $\mathrm{in}\, a = 0$ syss $a = 0$, pero como in no es un homomorfismo, entonces ésto no implica inyectividad.

Proposición 1.28: Sea A un dominio noetheriano local y $\mathfrak{a} \lhd A$. Si $\mathrm{gr}_{\mathfrak{a}}(A)$ es un dominio íntegro, entonces A también.

Demostración: Sean $a, b \in A$ tales que $ab = 0$. Luego, claramente $\mathrm{in}(a)\,\mathrm{in}(b) = 0$ y como $\mathrm{gr}(A)$ es un dominio íntegro, necesariamente $a, b \in \bigcap_{n\in\mathbb{N}} \mathfrak{a}^n$, y luego $a = 0 = b$ por el teorema de las intersecciones de Krull. □

Proposición 1.29: Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal propio de A. Entonces:

1. $\mathrm{gr}_{\mathfrak{a}}(A)$ es noetheriano.
2. $\mathrm{gr}_{\mathfrak{a}}(A) \cong \mathrm{gr}_{\hat{\mathfrak{a}}}(\hat{A})$ (como anillos graduados).
3. Si M es un A-módulo finitamente generado, $\mathcal{J} := (M_n)_{n\in\mathbb{N}}$ es una $\mathfrak{a}$-filtración estable. Entonces $\mathrm{gr}_{\mathcal{J}}(M)$ es un $\mathrm{gr}_{\mathfrak{a}}(A)$-módulo finitamente generado.

Demostración:

1. Como A es noetheriano, $\mathfrak{a}$ es finitamente generado, luego $\mathfrak{a} = (\alpha_1, \ldots, \alpha_s)$. Sea $\overline{\alpha}_i$ la proyección de α_i en $\mathfrak{a}/\mathfrak{a}^2$. Luego $\mathrm{gr}_{\mathfrak{a}}(A) = (A/\mathfrak{a})[\overline{\alpha}_1, \ldots, \overline{\alpha}_s]$. $A/\mathfrak{a}$ es noetheriano y $\mathrm{gr}_{\mathfrak{a}}(A)$ es una $(A/\mathfrak{a})$-álgebra de tipo finito, luego es noetheriana.
2. Basta recordar que $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$.

3. Nótese que cada componente homogénea $\mathrm{gr}_n(M)$ es noetheriana, luego es finitamente generada y como $\mathcal{J}$ es estable, entonces $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ para algún $n_0 \geq 0$ y luego $\mathrm{gr}_{n_0+r}(M) = 0$ en $(A/\mathfrak{a})$. Por lo que, $\mathrm{gr}(M) = \bigoplus_{n=0}^{n_0} \mathrm{gr}_n(M)$, el cual es una suma directa finita de módulos finitamente generados, luego es también finitamente generada como $\mathrm{gr}_{\mathfrak{a}}(A)$-módulo. □

Lema 1.30: Sean A, B grupos abelianos con filtraciones $(A_n)_n, (B_n)_n$ resp., que inducen su topología. Sea $\phi\colon A \to B$ un homomorfismo de grupos tal que $\phi[A_n] \subseteq B_n$, y sean $\mathrm{gr}(\phi)\colon \mathrm{gr}(A) \to \mathrm{gr}(B)$ y $\hat{\phi}\colon \hat{A} \to \hat{B}$ los homomorfismos inducidos. Entonces si $\mathrm{gr}(\phi)$ es inyectivo (resp. suprayectivo, isomorfismo), entonces ϕ también lo es.

Demostración: Nótese que se induce el siguiente diagrama conmutativo para todo n:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n/A_{n+1} & \longrightarrow & A/A_{n+1} & \longrightarrow & A/A_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{gr}_n(\phi)} & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \\ 0 & \longrightarrow & B_n/B_{n+1} & \longrightarrow & B/B_{n+1} & \longrightarrow & B/B_n & \longrightarrow & 0 \end{array}$$

con las filas exactas. Luego, por el lema de la serpiente se tiene que se induce la siguiente sucesión exacta:

$$\begin{array}{l} 0 \longrightarrow \ker(\mathrm{gr}_n(\phi)) \longrightarrow \ker(f_{n+1}) \longrightarrow \ker(f_n) \\ \qquad\qquad \curvearrowright \\ \mathrm{coker}(\mathrm{gr}_n(\phi)) \longrightarrow \mathrm{coker}(f_{n+1}) \longrightarrow \mathrm{coker}(f_n) \longrightarrow 0 \end{array}$$

Recordando que $f_0 = 0$, se concluye que por inducción si $\ker(\mathrm{gr}_n(\phi)) = 0$ ($\mathrm{gr}(\phi)$ inyectivo), entonces $\ker(f_n) = 0$ y si $\mathrm{coker}(\mathrm{gr}_n(\phi)) = 0$, entonces $\mathrm{coker}(f_n) = 0$. Finalmente, se concluye por la proposición 1.13. □

Proposición 1.31: Sea A un dominio, $\mathfrak{a}$ un ideal de A, M un A-módulo y $(M_n)_{n\in\mathbb{N}}$ una $\mathfrak{a}$-filtración de M. Si A es completo en la topología $\mathfrak{a}$-ádica, M es Hausdorff en la topología inducida por la filtración y $\mathrm{gr}(M)$ es un $\mathrm{gr}(A)$-módulo finitamente generado, entonces M es finitamente generado.

Demostración: Elija un sistema generador de $\mathrm{gr}(M)$ y sean $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_s$ sus componentes homogéneas de grado $n_1, \ldots, n_s$ resp. Como $\boldsymbol{h}_i \in \mathrm{gr}_{n_i}(M)$,

entonces $\boldsymbol{h}_i = [\boldsymbol{m}_i]$ con $\boldsymbol{m}_i \in M_{n_i}$. Sea $F_i = A$ el módulo con la $\mathfrak{a}$-filtración estable $(\mathfrak{a}^{n_i+r})_{r=0}^{\infty}$, y sea $F := \bigoplus_{i=1}^{s} F_i$, luego, cada F_i es un A-módulo libre generado por 1, por lo que podemos mandar $\boldsymbol{e}_i \mapsto \boldsymbol{m}_i$ para obtener un homomorfismo $\phi\colon F \to M$ de módulos (en particular, de grupos abelianos) filtrados. Luego, ϕ induce un homomorfismo $\mathrm{gr}(\phi)\colon \mathrm{gr}(F) \to \mathrm{gr}(M)$ que es suprayectivo, luego por la proposición anterior, $\hat{\phi}$ es suprayectivo y como el siguiente diagrama conmuta:

$$\begin{array}{ccc} F & \xrightarrow{\phi} & M \\ {\scriptstyle\alpha}\big\downarrow & & \big\downarrow{\scriptstyle\beta} \\ \hat{F} & \xrightarrow{\hat{\phi}} & \hat{M} \end{array}$$

donde α es un isomorfismo puesto que $A = \hat{A}$ y F es libre, de modo que $F = A \otimes_A F = \hat{A} \otimes_A F = \hat{F}$, y β es inyectiva, puesto que M es de Hausdorff; luego β es suprayectiva, y por tanto es isomorfismo, y luego ϕ debe de ser suprayectiva. Luego $\phi(\boldsymbol{e}_i)$ son un sistema generador de M. □

Corolario 1.31.1: Sea A un dominio, $\mathfrak{a}$ un ideal de A, M un A-módulo y $(M_n)_{n\in\mathbb{N}}$ una $\mathfrak{a}$-filtración de M. Si A es completo en la topología $\mathfrak{a}$-ádica, M es Hausdorff en la topología inducida por la filtración y $\mathrm{gr}(M)$ es un $\mathrm{gr}(A)$-módulo noetheriano, entonces M es noetheriano.

Teorema 1.32: Si A es un dominio noetheriano, $\mathfrak{a}$ es un ideal de A, entonces su compleción $\mathfrak{a}$-ádica $\hat{A}$ también es noetheriana.

Demostración: Recordemos que $\mathrm{gr}_{\mathfrak{a}}(A) \cong \mathrm{gr}_{\hat{\mathfrak{a}}}(\hat{A})$ y que $\mathrm{gr}_{\mathfrak{a}}(A)$ es noetheriano. Luego basta aplicar el corolario anterior. □

Teorema 1.33: Sea A un dominio noetheriano, entonces su anillo de potencias $A[[x_1, \ldots, x_n]]$ también es noetheriano.

Demostración: Basta probarlo para $A[[x_1]]$ por inducción, para lo cuál nótese que $A[[x_1]]$ es la compleción (x_1)-ádica de $A[x_1]$ que es noetheriano por bases de Hilbert. □

Teorema 1.34: Sea B un A-álgebra (conmutativa) completa respecto a un ideal $\mathfrak{n} \lhd B$, y sean $f_1, \ldots, f_n \in \mathfrak{n}$. Entonces:

1. Existe un único A-homomorfismo

$$\mathrm{ev}_{(f_1,\ldots,f_n)}\colon A[[x_1,\ldots,x_n]] \to B$$

tal que $x_i \mapsto f_i$.

2. Si el A-homomorfismo inducido $A \to B/\mathfrak{n}$ es un epimorfismo, entonces $\mathrm{ev}_{(f_1,\ldots,f_n)}$ también.

3. Si el homomorfismo de A-álgebras graduadas inducido:

$$\mathrm{gr}(\mathrm{ev}_{(f_1,\ldots,f_n)})\colon A[\boldsymbol{x}] \cong \mathrm{gr}_{(x_1,\ldots,x_n)}(A[[\boldsymbol{x}]]) \to \mathrm{gr}_{\mathfrak{n}}(B)$$

es un monomorfismo, entonces $\mathrm{ev}_{(f_1,\ldots,f_n)}$ también.

Demostración:

1. Para todo exponente $m \in \mathbb{N}$ se cumple que existe un único A-homomorfismo de evaluación

$$\phi_m\colon A[\boldsymbol{x}] \to B/\mathfrak{n}^m$$

que manda $x_i \mapsto f_i$ (mód $\mathfrak{n}^m$). Nótese que ϕ_m se anula en el ideal $(x_1,\ldots,x_n)^m$, de modo que determinan de manera única unos A-homomorfismos:

$$\alpha_m\colon A[[\boldsymbol{x}]]/(x_1,\ldots,x_n)^m \cong A[\boldsymbol{x}]/(x_1,\ldots,x_n)^m \to B/\mathfrak{n}^m.$$

Éstos homomorfismos son tales que el siguiente diagrama siempre conmuta:

$$\begin{array}{ccc} \dfrac{A[[\boldsymbol{x}]]}{(x_1,\ldots,x_n)^m} & \xrightarrow{\alpha_m} & \dfrac{B}{\mathfrak{n}^m} \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow \\ \dfrac{A[[\boldsymbol{x}]]}{(x_1,\ldots,x_n)^{m-1}} & \xrightarrow{\alpha_{m-1}} & \dfrac{B}{\mathfrak{n}^{m-1}} \end{array} \tag{1.1}$$

luego pasando límites inversos tenemos el homomorfismo deseado.

2. Basta notar que en el diagrama (1.1) todos los α_m's son epimorfismos y recordar que los límites inversos preservan exactitud.

3. Sea $0 \neq g \in A[[\boldsymbol{x}]]$. Nótese que $\operatorname{in} g$ es la parte homogénea de menor grado, digamos d, que no es nula en g. Llamando $\varphi := \mathrm{ev}_{(f_1,\ldots,f_n)}$

tenemos que $\ker \operatorname{gr}\varphi = (0)$, luego $\operatorname{gr}\varphi(\operatorname{in} g) \neq 0$ y, en particular, como $\operatorname{gr}\varphi$ es un homomorfismo entre álgebras graduadas, $\operatorname{gr}\varphi(\operatorname{in} g)$ tiene parte homogénea de grado d no nula. Ahora bien, como $g \equiv \operatorname{in} g$ mód $(x_1, \ldots, x_n)^{d+1}$, tenemos que $\varphi(g) \equiv \operatorname{gr}\varphi(\operatorname{in} g)$ (mód $\mathfrak{n}^{d+1}$) por lo que $\varphi(g) \neq 0$ como se quería ver. □

Corolario 1.34.1: Sea $f = a_1x + a_2x^2 + \cdots \in xA[[x]]$ y $\varphi := \operatorname{ev}_f \colon A[[x]] \to A[[x]]$. El endomorfismo φ es un isomorfismo syss $a_1 \in A^\times$.

Demostración: El homomorfismo de evaluación está bien definido por el teorema anterior.

$\Longrightarrow$. Nótese que dado un término de la forma $a + xg(x)$, con $a \in A_{\neq 0}$, éste se manda a $a + f \cdot g(f)$, de modo que $\varphi[A[[x]] \setminus (x)] = A[[x]] \setminus (x)$ y $\varphi[(x)] = (x)$; en particular, f es un generador de (x), luego f mód (x^2) genera $(x)/(x^2)$ y $f \equiv a_1x$ (mód (x^2)), luego necesariamente $a_1 \in A^\times$.

$\Longleftarrow$. Nótese que entonces $\operatorname{gr}\varphi \colon A[x] \to A[x]$ es $\operatorname{gr}\varphi = \operatorname{ev}_{a_1x}$, el cual es un automorfismo dado que a_1 es invertible, luego en particular es monomorfismo y φ también por el teorema anterior. Sea $f =: a_1x + g(x)x^2 = (a_1 + xg(x))x$ para un único $g(x) \in A[[x]]$. Como $a_1 + xg(x) \in A[[x]]^\times$, entonces $(f) = (x)$ y luego φ es un epimorfismo. □

1.4 Teoría de la dimensión

Definición 1.35: Sea C una clase de A-módulos y sea G un grupo abeliano. Una función $\lambda \colon C \to G$ se dice ***aditiva*** si para toda sucesión exacta

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

en C, se satisface que:

$$\lambda(M_1) - \lambda(M_2) + \lambda(M_3) = 0.$$

Ejemplo.

- Sea C la clase de A-módulos finitamente generados libres. Entonces $\operatorname{rang} \colon C \to \mathbb{Z}$ es una función aditiva.

- Sea A un dominio artiniano, entonces por Akizuki es noetheriano, luego todo módulo finitamente generado es noetheriano, y por tanto, también es artiniano. Luego posee longitud finita, finalmente por la proposición **??** se concluye que la longitud $\ell \colon C \to \mathbb{Z}$, donde C son los A-módulos finitamente generados, es una función aditiva.

Éste segundo ejemplo será importante.

Definición 1.36: Sea C la clase de A-módulos finitamente generados y $\lambda\colon C \to \mathbb{Z}$ una función aditiva. Entonces, para todo A-módulo graduado finitamente generado M se define su ***serie de Poincaré-Hilbert*** como

$$\operatorname{Poin}(M,t) := \sum_{n\in\mathbb{N}} \lambda(M_n)t^n \in \mathbb{Z}[[t]].$$

Teorema 1.37 (Hilbert-Serre): Sea A un anillo graduado noetheriano, tal que $A = A_0[\alpha_1,\dots,\alpha_s]$ donde α_i es homogéneo de grado n_i; y sea M un A_0-módulo graduado finitamente generado. Entonces, existe $f(t) \in \mathbb{Z}[t]$ tal que

$$\operatorname{Poin}(M,t) = \frac{f(t)}{\prod_{i=1}^{s}(1-t^{n_i})}.$$

Demostración: Procedemos por inducción sobre s. Si $s = 0$, entonces $A = A_0$ y M es un A_0-módulo finitamente generado, por lo que $M_n = 0$ para n suficientemente grande.

Probaremos que aplica para s: considere el endomorfismo $\boldsymbol{m} \mapsto \alpha_s\boldsymbol{m}$ que manda $M_r \mapsto M_{r+n_s}$, así pues, para todo n, induce la siguiente sucesión exacta:

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{\times\alpha_s} M_{n+n_s} \longrightarrow L_{n+n_s} \longrightarrow 0$$

donde K_n, L_{n+n_s} se definen como el núcleo y conúcleo de la aplicación de modo que la sucesión sea exacta. Luego, por aditividad, y multiplicando todo por t^{n+n_s}:

$$t^{n_s}\lambda(K_n)t^n - t^{n_s}\lambda(M_n)t^n + \lambda(M_{n+n_s})t^{n+n_s} - \lambda(L_{n+n_s})t^{n+n_s} = 0.$$

Sumando sobre n se obtiene que:

$$t^{n_s}\operatorname{Poin}(K,t) + (1-t^{n_s})\operatorname{Poin}(M,t) + g(t) - \operatorname{Poin}(L,t) = 0,$$

donde $g(t)$ son los términos faltantes de los sumandos de $M_\bullet$ y $L_\bullet$. Reordenando se concluye el enunciado. □

Definición 1.38: Sea A un anillo graduado noetheriano y sea M un A_0-módulo finitamente generado. Se denota por $d(M)$ al orden del polo de $\operatorname{Poin}(M,t)$ en 1, es decir, al máximo n tal que

$$\operatorname{Poin}(M,t) = \frac{f(t)}{(1-t)^n g(t)},$$

donde $f, g \in \mathbb{Z}[t]$ y $g(1) \neq 0$.

Corolario 1.38.1: Sea A un anillo graduado noetheriano con $A = A_0[\alpha_1, \ldots, \alpha_s]$ donde cada α_i es homogéneo de grado 1. Sea M un A_0-módulo graduado finitamente generado, entonces $\lambda(M_n) = p(n)$ para n suficientemente grande, con $p(x) \in \mathbb{Q}[x]$ y $\deg(p) = d(M) - 1$.

Demostración: Nótese que $\lambda(M_n)$ es el coeficiente del término t^n en la serie formal $\mathrm{Poin}(M, t)$, la cual por Hilbert-Serre, es el término de $f(t)(1-t)^{-s}$. Reordenando los términos podemos suponer que $d := s = d(M)$ y que $f(1) \neq 0$. Como

$$(1-t)^{-d} = ((1-t)^{-1})^d = (1 + t + t^2 + \cdots)^d = \sum_{i=0}^{\infty} \binom{d+i-1}{d-1} t^i,$$

con el convenio de que $\binom{n}{-1} = \delta_{n,-1}$. Como $f(t) = \sum_{i=0}^{N} a_i t^i$, entonces:

$$\lambda(M_n) = \sum_{i=0}^{N} a_i \binom{d+n-i-1}{d-1},$$

para todo $n \geq N$, que es lo que buscabamos. □

Ejemplo 1.39: Sea $A = A_0[x_1, \ldots, x_s]$ el anillo de polinomios sobre un dominio artiniano A_0. Luego cada componente homogénea A_n es un A_0-módulo libre generado por los monomios de la forma $x_1^{\eta_1} \cdots x_s^{\eta_s}$, donde $\sum_{i=1}^{s} \eta_i = n$, por lo que, por un problema de combinatoria se satisface que

$$\ell(A_n) = \binom{s+n-1}{s-1},$$

con lo que se concluye que $\mathrm{Poin}(A, t) = (1-t)^{-s}$. Luego $d(A) = s$. ⌟

Proposición 1.40: Sea A un anillo graduado noetheriano y M un A_0-módulo graduado finitamente generado. Si $\beta \in A$ es homogéneo y no es divisor de cero en M, entonces $d(M/\beta M) = d(M) - 1$.

Demostración: Sea g tal que $\beta \in A_g$. Basta considerar la siguiente sucesión exacta:

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{\times\beta} M_{n+g} \longrightarrow L_{n+g} \longrightarrow 0$$

y recordar que $K_n = 0$, puesto que β no es divisor de cero, y que $L_{n+g} = M_{n+g}/\beta M_n$. □

Ahora veremos un par de casos particulares para los anillos noetherianos locales:

Proposición 1.41: Sea $(A, \mathfrak{m})$ un dominio noetheriano local, $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario, M un A-módulo finitamente generado y $\mathcal{J} := (M_n)_{n\in\mathbb{N}}$ una $\mathfrak{q}$-filtración estable. Entonces:

1. M/M_n es de longitud finita.

2. Si $\mathfrak{q}$ está generado por al menos s elementos, entonces $\ell(M/M_n) = p(n)$ con $p(x) \in \mathbb{Q}[x]$ y $\deg(p) \leq s$ para n suficientemente grande.

3. El coeficiente lider de p depende exclusivamente de M y de $\mathfrak{q}$, no de la filtración escogida.

Demostración:

1. Sea $\mathrm{gr}_{\mathfrak{q}}(A) := \bigoplus_{n\in\mathbb{N}} \mathfrak{q}^n/\mathfrak{q}^{n+1}$ y $\mathrm{gr}_{\mathcal{J}}(M) := \bigoplus_{n\in\mathbb{N}} M_n/M_{n+1}$. Como A es noetheriano, $\mathrm{gr}(A)$ también y luego $\mathrm{gr}(M)$ es un $\mathrm{gr}(A)$-módulo graduado finitamente generado. Nótese además que en $\mathrm{gr}_0(A) = A/\mathfrak{q}$ el maximal es nilpotente y es noetheriano, por lo tanto, es artiniano. Como $(M_n)_n$ es una $\mathfrak{q}$-filtración, entonces $\mathrm{gr}_n(M)$ es un A-módulo noetheriano y se anula por $\mathfrak{q}$, luego es un $(A/\mathfrak{q})$-módulo noetheriano, por lo tanto, tiene longitud finita. Por inducción se concluye que M/M_n tiene longitud finita y que

$$\ell(M/M_n) = \sum_{r=0}^{n-1} \ell(M_r/M_{r+1}).$$

2. Recordando el ejemplo vemos que ℓ es una función aditiva sobre los $(A/\mathfrak{q})$-módulos finitamente generados. Sea $\mathfrak{q} = (\alpha_1, \ldots, \alpha_s)$, y sea $\overline{\alpha}_i$ la proyección de α_i en $\mathfrak{q}/\mathfrak{q}^2$, luego se sigue que $G(A) = (A/\mathfrak{q})[\overline{\alpha}_1, \ldots, \overline{\alpha}_s]$ con $\overline{\alpha}_i$ homogéneo de grado 1. Luego $\lambda(\mathrm{gr}_n(M)) = \ell(M_n/M_{n+1}) = p(n)$ para n suficientemente grande y $\deg(p) \leq s$ (¿por qué?).

3. Sea $(M'_n)_n$ otra $\mathfrak{q}$-filtración estable. Por el inciso anterior, $\ell(M/M'_n) = q(n)$ para n suficientemente grande. Luego tienen diferencia acotada,

i.e., $M_{n+n_0} \subseteq M'_n$ y $M'_{n+n_0} \subseteq M_n$, por lo que $p(n+n_0) \geq q(n)$ y $q(n+n_0) \geq p(n)$. De ello se concluye que

$$\lim_n \frac{p(n)}{q(n)} = 1,$$

por lo que p, q tienen igual grado y coeficiente lider. □

En el caso particular de $M = A$ se obtiene:

Corolario 1.41.1: Sea $(A, \mathfrak{m})$ un dominio noetheriano local, y $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario generado por s elementos. Entonces $\ell(A/\mathfrak{q}^n) = p(n)$, donde $p(x) \in \mathbb{Q}[x]$ y $\deg(p) \leq s$.

Definición 1.42: Dado un A-módulo M, considerando la filtración $(\mathfrak{q}^n M)_n$ definimos su polinomio de Hilbert-Samuel, denotado $\chi_{\mathfrak{q}}^M(n)$, como el polinomio de $\ell(M/\mathfrak{q}^n M)$ para n suficientemente grande. Si $M = A$, entonces obviamos el superíndice, i.e., $\chi_{\mathfrak{q}}(n) := \chi_{\mathfrak{q}}^A(n)$.

Proposición 1.43: Sea $(A, \mathfrak{m})$ un dominio noetheriano local y $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario. Entonces $\deg(\chi_{\mathfrak{q}}) = \deg(\chi_{\mathfrak{m}})$.

Demostración: Nótese que existe r tal que $\mathfrak{m} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^r$, luego

$$\chi_{\mathfrak{m}}(n) \leq \chi_{\mathfrak{q}}(n) \leq \chi_{\mathfrak{m}}(rn) \qquad \text{para } n \text{ suficientemente grande.}$$

Luego se aplica el mismo truco del límite para concluir que el grado debe ser el mismo. □

Definición 1.44: Sea $(A, \mathfrak{m})$ un dominio noetheriano local. Denotaremos por $d(A) := \deg(\chi_{\mathfrak{q}})$, donde $\mathfrak{q}$ es cualquier ideal $\mathfrak{m}$-primario. En particular, $d(A) = d(\mathrm{gr}_{\mathfrak{m}}(A))$, donde aquí $d(\mathrm{gr}_{\mathfrak{m}}(A))$ representa (en sentido viejo) el orden del polo de $\mathrm{Poin}(\mathrm{gr}_{\mathfrak{m}}(A), t)$ en $t = 1$.

Denotaremos por $\delta(A)$ el mínimo número de generadores de $\mathfrak{q}$, cualquier ideal $\mathfrak{m}$-primario.

Corolario 1.44.1: $\delta(A) \geq d(A)$.

Nuestro objetivo será probar que $d(A) \geq k.\dim(A) \geq \delta(A)$ para concluir que los tres números coinciden.

Proposición 1.45: Sea $(A, \mathfrak{m})$ un dominio noetheriano local, $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario y M un A-módulo finitamente generado. Si $\alpha \in A$ no es divisor de cero en M y $M' := M/\alpha M$, entonces $\deg(\chi_{\mathfrak{q}}^{M'}) \leq \deg(\chi_{\mathfrak{q}}^{M}) - 1$.

Demostración: Definamos $N := \alpha M$, de modo que $M' = M/N$. Consideremos la filtración $N_n := N \cap \mathfrak{q}^n M$ sobre N, luego empleando el tercer y segundo teorema de isomorfismos se construye la siguiente sucesión exacta:

$$0 \longrightarrow \frac{N}{N_n} \longrightarrow \frac{M}{\mathfrak{q}^n M} \longrightarrow \frac{M'}{\mathfrak{q}^n M'} \longrightarrow 0$$

empleando la aditividad de ℓ, entonces para n suficientemente grande se tiene que:

$$g(n) - \chi_{\mathfrak{q}}^{M}(n) + \chi_{\mathfrak{q}}^{M'}(n) = 0.$$

Por el lema de Artin-Rees se concluye que $(N_n)_{n\in\mathbb{N}}$ es una $\mathfrak{q}$-filtración estable de N. Luego como $N \cong M$, se deduce que $g(n)$ y $\chi_{\mathfrak{q}}^{M}(n)$ poseen mismo grado y coeficiente lider, de lo que se concluye el enunciado. □

Corolario 1.45.1: Sea $(A, \mathfrak{m})$ un dominio noetheriano local y $x \in A$ un elemento que no es divisor de cero. Entonces $d(A/(x)) \leq d(A) - 1$.

Proposición 1.46: $d(A) \geq k.\dim(A)$.

Demostración: Procedemos por inducción sobre $d := d(A)$. Si $d = 0$: entonces $\ell(A/\mathfrak{m}^n)$ es constante para n suficientemente grande, luego, por correspondencia, $\ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 0$ y $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, por lo que A es artiniano y $k.\dim A = 0$.

Si $d > 0$: Podemos suponer que $k.\dim(A) > 0$ por lo que sea

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r$$

una cadena de ideales primos en A, y sea $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$, luego $\overline{x} \neq 0$ en $A' := A/\mathfrak{p}_0$, el cual es un dominio íntegro, y por el corolario anterior se cumple que

$$d(A'/(\overline{x})) \leq d(A') - 1.$$

Por correspondencia, $(A', \mathfrak{m}')$ es local, y luego tenemos una proyección $A/\mathfrak{m}^n \to A'/\mathfrak{m}'^n$, de lo que se sigue que $\ell(A/\mathfrak{m}^n) \geq \ell(A'/\mathfrak{m}'^n)$ y en consecuencia $d(A) \geq d(A')$, por lo que $d(A'/(\overline{x})) \leq d - 1$.

Luego por hipótesis inductiva se satisface que $k.\dim(A'/(\overline{x})) \leq d(A'/(\overline{x}))$, pero las imagenes de $\mathfrak{p}_i$ forman una cadena de longitud $r-1$ en $A'/(\overline{x})$, vale decir, $r - 1 \leq d - 1$, de lo que se sigue que $k.\dim(A) \leq d(A)$. □

Corolario 1.46.1: Si A es un dominio noetheriano local, entonces posee dimensión de Krull finita.

Corolario 1.46.2: En un dominio noetheriano local todo ideal primo posee altura finita. Luego toda cadena descendiente de ideales primos posee minimal.

Proposición 1.47: Sea $(A, \mathfrak{m})$ un dominio noetheriano local de dimensión d. Entonces existe un ideal $\mathfrak{m}$-primario generado por d elementos. En consecuencia, $k.\dim(A) \geq \delta(A)$.

Demostración: Construiremos, por inducción, un ideal $(x_1, \ldots, x_d)$ tal que para todo $\mathfrak{p} \supseteq (x_1, \ldots, x_i)$ primo se cumple que $\operatorname{alt}\mathfrak{p} \geq i$. Claramente aplica para $i = 0$. Sea $i > 0$ y sean $\mathfrak{p}_j$, con $1 \leq j \leq s$, los ideales primos minimales que contienen a $(x_1, \ldots, x_{i-1})$ tales que $\operatorname{alt}\mathfrak{p}_j = i - 1$ (nótese que s podría ser 0). Como $i - 1 < d = \operatorname{alt}\mathfrak{m}$, entonces $\mathfrak{p}_j \neq \mathfrak{m}$ para todo j y luego $\mathfrak{m} \neq \bigcup_{j=1}^{s} \mathfrak{p}_j$ por la proposición **??**, luego sea $x_i \in \mathfrak{m} \setminus \bigcup_{i=1}^{s} \mathfrak{p}_j$. Sea $\mathfrak{q}$ un ideal primo que contiene a $(x_1, \ldots, x_i)$, luego contiene a un ideal minimal $\mathfrak{p}$ de $(x_1, \ldots, x_{i-1})$; si $\mathfrak{p} = \mathfrak{p}_j$ para algún j, entonces como $x_i \in \mathfrak{q} \setminus \mathfrak{p}$ se cumple que $\mathfrak{p} \subset \mathfrak{q}$ y $\operatorname{alt}\mathfrak{q} > \operatorname{alt}\mathfrak{p}$. Si $\mathfrak{p}$ es otro ideal, entonces $\operatorname{alt}\mathfrak{p} \geq i$ y $\operatorname{alt}\mathfrak{q} \geq i$.

Finalmente $(x_1, \ldots, x_d)$ es un ideal tal que el único primo que le contiene es $\mathfrak{m}$, por lo que es $\mathfrak{m}$-primario. □

Teorema 1.48 – *Teorema fundamental de la dimensión*: En un dominio noetheriano local $(A, \mathfrak{m})$ son iguales:

1. El mínimo número de generadores de un ideal $\mathfrak{m}$-primario.
2. El orden del polo de $\operatorname{Poin}(\operatorname{gr}_{\mathfrak{m}}(A), t)$ en $t = 1$.
3. El grado del polinomio de Hilbert-Samuel $\chi_{\mathfrak{m}}$.
4. La dimensión de Krull de A.

Definición 1.49: Sea $(A, \mathfrak{m})$ un dominio noetheriano local, y sea $d = k.\dim(A)$. A un conjunto $\alpha_1, \ldots, \alpha_d$ de elementos tales que generan un ideal $\mathfrak{m}$-primario se les dice un ***sistema de parámetros***.

De él se extraen varios corolarios:

Corolario 1.49.1: Sea $(A, \mathfrak{m}, k)$ un dominio noetheriano local. Entonces:

$$k.\dim(A) \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

Demostración: Por el lema de Nakayama, un sistema de generadores de $\mathfrak{m}/\mathfrak{m}^2$ también genera a $\mathfrak{m}^2$; $\mathfrak{m}^2$ es un ideal $\mathfrak{m}$-primario y, por lo tanto, empleando que $k.\dim(A) = \delta(A) \leq$ el mínimo número de generadores de $\mathfrak{m}^2$, se concluye el enunciado. □

Corolario 1.49.2: Sea A un dominio noetheriano y sean $\alpha_1, \ldots, \alpha_r \in A$. Luego todo ideal primo $\mathfrak{p}$ asociado a $(\alpha_1, \ldots, \alpha_r)$ tiene altura $\leq r$.

Demostración: Nótese que $(\alpha_1, \ldots, \alpha_r)$ es $\mathfrak{p}^e$-primario en $A_\mathfrak{p}$, el cual es noetheriano y local, luego $\operatorname{alt}\mathfrak{p} = k.\dim(A_\mathfrak{p}) \leq r$. □

Un caso particular es el siguiente:

Teorema 1.50 – *Teorema de los ideales principales de Krull*: Sea A un dominio noetheriano y sea $\alpha \in A$ tal que no es ni divisor de cero ni inversible. Entonces todo ideal primo minimal $\mathfrak{p}$ que contiene a α tiene altura 1.

Demostración: Por el corolario anterior se cumple que $\operatorname{alt}\mathfrak{p} \leq 1$. Si $\operatorname{alt}\mathfrak{p} = 0$, entonces, por la proposición **??** se cumple que $\mathfrak{p}$ está asociado al cero y que sus elementos son divisores de cero, pero $\alpha \in \mathfrak{p}$ lo que sería absurdo. En consecuencia, necesariamente $\operatorname{alt}\mathfrak{p} = 1$. □

Éste teorema también aparece en la literatura por su nombre original, *Hauptidealsatz*.[3] Al referirnos al *teorema de los ideales principales de Krull* hablaremos tanto del teorema anterior como de su generalización en el corolario 1.49.2.

Teorema 1.51: Sea A un dominio noetheriano y $\mathfrak{p} \lhd A$ de $\operatorname{alt}\mathfrak{p} = r$. Entonces:

1. $\mathfrak{p}$ es un primo asociado minimal a un ideal $(a_1, \ldots, a_r)$ generado por r elementos.
2. Si $b_1, \ldots, b_s \in \mathfrak{p}$, entonces

$$\operatorname{alt}\left(\frac{\mathfrak{p}}{(b_1, \ldots, b_s)}\right) \geq r - s.$$

[3] Del de., teorema (*satz*) de los ideales (*ideal*) principales (*haupt*).

3. Dados $(a_1, \ldots, a_r)$ como en el inciso 1, se satisface que

$$\operatorname{alt}\left(\frac{\mathfrak{p}}{(a_1, \ldots, a_i)}\right) = r - i.$$

Demostración:

1. $A_{\mathfrak{p}}$ es un anillo noetheriano local, así que por el teorema fundamental de la dimensión, elíjanse $a_1, \ldots, a_r$ un sistema de parámetros, es decir, tales que $(a_1, \ldots, a_r)A_{\mathfrak{p}}$ es un ideal $\mathfrak{p}A_{\mathfrak{p}}$-primario. Cada a_i es un producto entre un elemento de $\mathfrak{p}$ (el maximal) y un invertible de $A_{\mathfrak{p}}$, por lo que, sin perdida de generalidad, supondremos que cada $a_i \in \mathfrak{p}$. Finalmente, $\mathfrak{p}$ es un primo asociado minimal de $(a_1, \ldots, a_r)A$ (¿por qué?).

2. Sea $\mathfrak{b} := (b_1, \ldots, b_s)$, $\bar{A} := A/\mathfrak{b}$ y $\bar{\mathfrak{p}} := \mathfrak{p}/\mathfrak{b}$. Digamos que $t := \operatorname{alt}\bar{\mathfrak{p}}$, luego por el inciso anterior, existen $\bar{c}_1, \ldots, \bar{c}_t \in \bar{A}$ tales que $\bar{\mathfrak{p}}$ es un primo asociado minimal a $(\bar{c}_1, \ldots, \bar{c}_t)$ y, así, $\mathfrak{p}$ es un primo asociado minimal a $(b_1, \ldots, b_s, c_1, \ldots, c_t)$; luego $r \leq s + t$ por el teorema de los ideales principales de Krull.

3. $\operatorname{alt}\big(\mathfrak{p}/(a_1, \ldots, a_i)\big) \geq r - i$ por el inciso anterior. El ideal $\mathfrak{p}/(a_1, \ldots, a_i)$ es un primo asociado minimal al ideal $(\bar{a}_{i+1}, \ldots, \bar{a}_r)$.y luego

$$\operatorname{alt}\big(\mathfrak{p}/(a_1, \ldots, a_i)\big) \leq r - i$$

y se concluye la igualdad. □

Corolario 1.51.1: Sea $(A, \mathfrak{m})$ un dominio noetheriano local. Para todo $\beta \in \mathfrak{m}$ se cumple que $k.\dim(A/(\beta)) = k.\dim(A) - 1$.

Demostración: Basta recordar que $k.\dim A = \operatorname{alt}\mathfrak{m}$ y aplicar el teorema anterior. □

Teorema 1.52: Sea A un dominio íntegro noetheriano. Entonces, A es un DFU syss todo ideal primo de altura 1 es principal.

Demostración: $\Longrightarrow$. Sea $\mathfrak{p} \lhd A$ un ideal primo de altura 1 y sea $a \in \mathfrak{p}$. Por factorización única, $a = \prod_{i=1}^{n} \pi_i$ donde cada π_i es primo y, como $\mathfrak{p}$ es un ideal primo, algún $\pi_j \in \mathfrak{p}$. Luego tenemos la cadena $(0) \subset (\pi_j) \subseteq \mathfrak{p}$ y, como $\operatorname{alt}\mathfrak{p} = 1$, vemos que $\mathfrak{p} = (\pi_j)$.

$\Longleftarrow$. Por el teorema **??** basta probar que todo elemento irreducible es primo. Así, pues sea a irreducible (por lo tanto, ni nulo, ni inversible) y sea $\mathfrak{p}$ un ideal primo minimal que contenga a a. Por el teorema de los ideales principales de Krull, $\operatorname{alt}\mathfrak{p} = 1$ y por lo tanto $\mathfrak{p} = (b)$, de modo que $b \mid a$ y, como a es irreducible, $(a) = (b)$ es un ideal primo. □

Teorema 1.53: Sea $A = \bigoplus_{n\in\mathbb{N}} A_n$ un anillo graduado noetheriano.

1. Si $\mathfrak{a} \lhd A$ es un ideal homogéneo y $\mathfrak{p} \in \operatorname{As}(\mathfrak{a})$, entonces $\mathfrak{p}$ también es homogéneo.

2. Si $\mathfrak{p} \lhd A$ es un ideal primo homogéneo de altura r, entonces existe una cadena
$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r = \mathfrak{p}, \tag{1.2}$$
donde cada $\mathfrak{p}_i$ es primo y homogéneo.

Demostración:

1. Por definición $\mathfrak{p} = \operatorname{Ann}(a)$ para algún $a \in A/\mathfrak{a}$, donde $A/\mathfrak{a}$ es un A-módulo graduado. Sea $b \in \mathfrak{p}$, entonces escribamos $a = a_0+a_1+\cdots+a_r$, separado por componentes homogéneas, y $b = b_p+b_{p+1}+\cdots+b_q$. Como $ab = 0$, entonces cada componente homogénea es nula, ergo
$$0 = a_0b_p = a_1b_p + a_0b_{p+1} = a_2b_p + a_1b_{p+1} + a_0b_{p+2} = \cdots,$$
de lo que se obtiene que $0 = a_1b_p^2 = a_2b_p^3 = \cdots$, de lo que se concluye que $ab_p^{r+1} = 0$. En consecuente $b_p^{r+1} \in \mathfrak{p}$ y $b_p \in \mathfrak{p}$. Luego $b - b_p = b_{p+1} + \cdots + b_q \in \mathfrak{p}$ y, por inducción, vemos que cada componente homogénea $b_i \in \mathfrak{p}$.

2. Sea (1.2) una cadena maximal (en longitud) de primos, donde no necesariamente cada $\mathfrak{p}_i$ es homogéneo. Nótese que $\mathfrak{p}_0$ es un primo minimal asociado a (0), luego, por el inciso anterior, se cumple que es homogéneo. Reemplazando A por $A/\mathfrak{p}_0$, podemos suponer que A es dominio íntegro.

   Ahora, procedemos por inducción sobre r. Sea $b_1 \in \mathfrak{p}_{\neq 0}$, un elemento homogéneo, entonces, por el teorema anterior, $\operatorname{alt}(\mathfrak{p}/(b_1)) = r - 1$. Sea $\mathfrak{q} \in \operatorname{As}(b_1)$ minimal tal que $\operatorname{alt}(\mathfrak{p}/\mathfrak{q}) = r - 1$, el cual es homogéneo y no nulo. Por hipótesis inductiva, existe tal cadena para $\mathfrak{p}/\mathfrak{q}$:
$$(0) = \mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_{r-1} = \mathfrak{p}/\mathfrak{q},$$

y luego, extendiendo ideales y añadiendo el ideal (0) al final se obtiene:

$$(0) \subset \mathfrak{q} = \mathfrak{q}_0^e \subset \cdots \subset \mathfrak{q}_{r-1}^e = \mathfrak{p}. \qquad \square$$

Proposición 1.54: Sea $(A, \mathfrak{m})$ un dominio noetheriano local y $\hat{A}$ la compleción $\mathfrak{m}$-ádica de A. Entonces $k.\dim(A) = k.\dim(\hat{A})$.

Demostración: $A/\mathfrak{m}^n \cong \hat{A}/\hat{\mathfrak{m}}^n$, luego $\chi_{\mathfrak{m}}(n) = \chi_{\hat{\mathfrak{m}}}(n)$. $\square$

Proposición 1.55: Sea $(A, \mathfrak{m})$ un dominio noetheriano local, $\{\alpha_1, \ldots, \alpha_d\}$ un sistema de parámetros de A y $\mathfrak{q} := (\alpha_1, \ldots, \alpha_d)$. Sea $f \in A[t_1, \ldots, t_d]$ un polinomio homogéneo de grado $s > 0$ tal que

$$f(\alpha_1, \ldots, \alpha_d) \in \mathfrak{q}^{s+1},$$

entonces todos los coeficientes de f pertenecen a $\mathfrak{m}$.

Demostración: Considere el siguiente epimorfismo:

$$\varphi := \mathrm{ev}_{(\overline{\alpha}_1, \ldots, \overline{\alpha}_d)} \colon (A/\mathfrak{q})[t_1, \ldots, t_d] \longrightarrow \mathrm{gr}_{\mathfrak{q}}(A).$$

Luego, por hipótesis, ya sea f, o alguna de sus proyecciones $\overline{f}$ está en el núcleo de dicho morfismo. Si, por contradicción, alguno de los coeficientes de f no estuviera en $\mathfrak{m}$, entonces sería inversible, luego $\overline{f}$ no es nulo, ni es divisor de cero, ni es inversible, por ende:

$$\begin{aligned} d(\mathrm{gr}_{\mathfrak{q}}(A)) &\leq d((A/\mathfrak{q})[t_1, \ldots, t_d]/(\overline{f})) \\ &= d((A/\mathfrak{q})[t_1, \ldots, t_d]) - 1 \\ &= d - 1, \end{aligned}$$

donde la última igualdad se deduce de lo dicho en el ejemplo 1.39. Pero $d(\mathrm{gr}_{\mathfrak{q}}(A)) = d$, por lo que el último resultado es absurdo. $\square$

Corolario 1.55.1: Si k es un cuerpo, $A \supseteq k$ es un dominio noetheriano local de maximal $\mathfrak{m}$ tal que $k \cong A/\mathfrak{m}$ y $\alpha_1, \ldots, \alpha_d$ son un sistema de parámetros de A, entonces son algebraicamente independientes sobre k.

Demostración: Supongamos que $f(\alpha_1, \ldots, \alpha_d) = 0$ con $f \in k[t_1, \ldots, t_d]$. Si $f \neq 0$, entonces f admitiría una descomposición en factores homogéneos, luego $f_s(\alpha_1, \ldots, \alpha_d) = 0 \in \mathfrak{m}^{s+1}$, por lo que, por la proposición anterior se ha de cumplir que $f_s \in \mathfrak{m}[t_1, \ldots, t_d]$, luego $f_s = 0$ lo que es absurdo. $\square$

Lema 1.56: Sea $(A, \mathfrak{m}, k)$ un dominio noetheriano local de dimensión d. Son equivalentes:

1. $\mathrm{gr}_{\mathfrak{m}}(A) \cong k[t_1, \ldots, t_d]$ (el anillo libre de polinomios).
2. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$.
3. $\mathfrak{m}$ puede generarse por d elementos.

Demostración: Claramente $1 \implies 2$, y $2 \implies 3$ por el lema de Nakayama.

$3 \implies 1$. Sea $\mathfrak{m} = (\alpha_1, \ldots, \alpha_d)$, luego el mapa de evaluación:

$$\mathrm{ev}_{(\alpha_1,\ldots,\alpha_d)} \colon k[t_1, \ldots, t_d] \longrightarrow \mathrm{gr}_{\mathfrak{m}}(A)$$

es un isomorfismo. □

Definición 1.57: Un dominio noetheriano local A se dice ***local regular*** si satisface cualquiera de las condiciones del teorema anterior.

Más adelante definiremos *anillo regular* en más generalidad sin restringirnos a anillos locales.

Proposición 1.58: Sea A un dominio noetheriano local. Entonces A es regular syss $\hat{A}$ es regular.

Demostración: Ya sabemos que A es noetheriano local syss $\hat{A}$ lo es. Más aún, $\mathfrak{m}^e = \hat{\mathfrak{m}}$, por lo que, empleando que $\mathrm{gr}_{\mathfrak{m}}(A) \cong \mathrm{gr}_{\hat{\mathfrak{m}}}(\hat{A})$ se concluye el enunciado. □

La regularidad es una propiedad muy buena entre anillos, veamos un ejemplo:

Teorema 1.59: Todo anillo local regular es un dominio íntegro.

Demostración: Sea A un anillo local regular, luego tiene dimensión finita por el corolario 1.46.1. Vamos a demostrarlo por inducción sobre $d := k.\dim A$. Si $d = 0$ entonces es artiniano y por la proposición A.18 es un cuerpo.

Si $d > 0$, entonces por el lema de Nakayama tenemos que $\mathfrak{m} \neq \mathfrak{m}^2$ y por evitamiento de primos (proposición **??**) encontramos $\alpha \in \mathfrak{m}$ que no está en

nigún primo minimal (que son finitos, corolario A.10.1) y tampoco está en $\mathfrak{m}^2$; así α no es divisor de cero. Sea $B := A/\alpha$, el cual es local con maximal $\mathfrak{n} := \mathfrak{m}^e = \mathfrak{m}B$. Así, por el teorema de ideales principales de Krull, tenemos que $k.\dim B = d-1$ y, por el tercer teorema de isomorfismos,

$$\frac{\mathfrak{n}}{\mathfrak{n}^2} \cong \frac{\mathfrak{m}}{\mathfrak{m}^2 + \alpha A},$$

el cual es la imagen epimórfica de $\mathfrak{m}/\mathfrak{m}^2$, luego puede generarse por $d-1$ elementos y, por lema de Nakayama, $\mathfrak{n}$ puede generarse por $d-1$ elementos y así B es regular.

Por hipótesis inductiva B es un dominio íntegro, así que α es primo y el ideal (α) contiene a algún primo minimal $\mathfrak{q}$ de A. Sea $\beta \in \mathfrak{q}$, luego $\beta = c\alpha$ para algún $c \in A$ y como $\alpha \notin \mathfrak{q}$, entonces $c \in \mathfrak{q}$, por lo que $\mathfrak{q} = \alpha\mathfrak{q}$ y, así, $\mathfrak{q} = \mathfrak{m}\mathfrak{q}$ lo que, por el lema de Nakayama, implica que $\mathfrak{q} = (0)$ y, por lo tanto, A es íntegro. □

§1.4.1 Colongitud. En ésta subsección veremos si podemos ampliar un poquito la definición a dimensión de Krull para módulos y obtener resultados similares al teorema de los ideales principales de Krull.

Definición 1.60: Sea A un dominio y M un A-módulo. Se define la ***dimensión de Krull*** del módulo como

$$k.\dim_A(M) := k.\dim(A/\operatorname{Ann}(M)).$$

Obviaremos el subíndice A de no haber ambigüedad sobre los signos.

Definición 1.61: Sea $(A, \mathfrak{m})$ un dominio noetheriano local, sea $\mathfrak{q} \lhd A$ un ideal propio y M un A-módulo finitamente generado. Se le llama la ***colongitud*** de $\mathfrak{q}$ en M a $\ell(M/\mathfrak{q}M)$.

Nótese que $\mathfrak{q}$ es de colongitud finita en M syss $M/\mathfrak{q}M$ es un A-módulo artiniano lo que, por el corolario A.17.3, corresponde a que $\operatorname{Ann}(M/\mathfrak{q}M) \supseteq \mathfrak{m}^n$ para algún n, lo que equivale a que $\operatorname{Rad}\operatorname{Ann}(M/\mathfrak{q}M) = \mathfrak{m}$, o finalmente, que $\mathfrak{q}M \leq M$ es un submódulo $\mathfrak{m}$-primario.

Proposición 1.62: Sea A un dominio noetheriano, M un A-módulo finitamente generado y $\mathfrak{q} \lhd A$ un ideal. Entonces $\operatorname{Rad}\operatorname{Ann}(M/\mathfrak{q}M) = \operatorname{Rad}(\mathfrak{q} + \operatorname{Ann}(M))$. Si además $(A, \mathfrak{m})$ es local, entonces:

1. $\mathfrak{q}$ tiene colongitud finita en M syss $\mathfrak{q} + \operatorname{Ann}(M) \supseteq \mathfrak{m}^n$ para algún n syss $\mathfrak{q}$ tiene colongitud finita en $A/\operatorname{Ann}(M)$.
2. Dada una sucesión exacta corta $0 \to M_1 \to M_2 \to M_3 \to 0$ se cumple que $\mathfrak{q}$ tiene colongitud finita en M_2 syss $\mathfrak{q}$ tiene colongitud finita en M_1 y en M_3.
3. $k.\dim(M) = d$, donde d es la mínima cantidad de generadores de algún ideal de colongitud finita en M.

Demostración: Por el teorema A.3, probaremos que si $\mathfrak{p} \lhd A$ es un ideal primo, entonces $\mathfrak{p} \supseteq \operatorname{Ann}(M/\mathfrak{q}M)$ syss $\mathfrak{p} \supseteq \mathfrak{q} + \operatorname{Ann}(M)$. Nótese que $\mathfrak{p} \supseteq \operatorname{Ann}(M/\mathfrak{q}M)$ syss $(M/\mathfrak{q}M)_\mathfrak{p} \neq 0$, y $(M/\mathfrak{q}M)_\mathfrak{p} = M_\mathfrak{p}/\mathfrak{q}_\mathfrak{p}M_\mathfrak{p}$, por lo que la última condición equivale, por lema de Nakayama, a que $M_\mathfrak{p} \neq 0$ y $\mathfrak{q}_\mathfrak{p} \subseteq \mathfrak{p}_\mathfrak{p}$, lo que equivale a que $\mathfrak{p}$ contenga a $\mathfrak{q}$ y a $\operatorname{Ann}(M)$ como se quería probar.

1. La primera equivalencia es el mero corolario A.12.1 junto a la discusión previa. La segunda equivalencia es una aplicación del tercer teorema de isomorfismos empleando que
$$\frac{A/\operatorname{Ann}(M)}{\mathfrak{q}(A/\operatorname{Ann}(M))} \cong \frac{A}{\mathfrak{q} + \operatorname{Ann}(M)},$$
luego su aniquilador es $\mathfrak{q} + \operatorname{Ann}(M)$.
2. Es claro que $\operatorname{Ann}(M_2) \subseteq \operatorname{Ann}(M_1), \operatorname{Ann}(M_3)$ de modo que si $\mathfrak{q}$ tiene colongitud finita en M_2, entonces tiene colongitud finita en M_1, M_3.

   Recíprocamente, se induce la siguiente sucesión exacta:
$$\frac{M_1}{\mathfrak{q}M_1} \longrightarrow \frac{M_2}{\mathfrak{q}M_2} \longrightarrow \frac{M_3}{\mathfrak{q}M_3} \longrightarrow 0.$$
   Luego, como $M_1/\mathfrak{q}M_1, M_3/\mathfrak{q}M_3$ tienen longitud finita, entonces $M_2/\mathfrak{q}M_2$ también (por aditividad). □

Corolario 1.62.1: Sea $(A, \mathfrak{m})$ un dominio noetheriano local y sea M un A-módulo finitamente generado. Para todo $\alpha \in \mathfrak{m}$ se cumple
$$k.\dim(M/\alpha M) \geq k.\dim M - 1.$$

Demostración: Llamemos $d := k.\dim(M/\alpha M)$. Por el inciso 3 de la proposición anterior existe un ideal $\mathfrak{q} = (\beta_1, \ldots, \beta_d)$ que tiene colongitud finita en $M/\alpha M$, luego notamos que $M/(\alpha, \beta_1, \ldots, \beta_d)M$ tiene longitud finita y, por el mismo inciso, $k.\dim M \leq 1 + d$. □

§1.4.2 Multiplicidad.

Definición 1.63: Sea $(A, \mathfrak{m})$ un dominio noetheriano local de $k.\dim A =: d$, M un A-módulo finitamente generado y $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario. Luego, se ve que

$$\chi_{\mathfrak{q}}^{M}(n) = \frac{e}{d!}n^d + \cdots \in \mathbb{Q}[x],$$

y se define $e(\mathfrak{q}, M) \in \mathbb{Z}$ el término e en la fórmula, llamado la ***multiplicidad*** de $\mathfrak{q}$ en M. Denotamos $e(\mathfrak{q}) := e(\mathfrak{q}, A)$ y denotamos $e(A) := e(\mathfrak{m})$.

Se puede concluir lo siguiente:

Proposición 1.64: Sea $(A, \mathfrak{m})$ un dominio noetheriano local de $k.\dim A =: d$, M un A-módulo finitamente generado y $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario. Se cumplen:

1. $$e(\mathfrak{q}, M) = \lim_{n} \frac{d!}{n^d}\ell(M/\mathfrak{q}^n M). \tag{1.3}$$
   En particular, si $d = 0$ (i.e., A es artiniano), entonces $e(\mathfrak{q}, M) = \ell(M)$.
2. $e(\mathfrak{q}, M) > 0$ si $k.\dim M = d$ y $e(\mathfrak{q}, M) = 0$ si $k.\dim M < d$.
3. $e(\mathfrak{q}^r, M) = r^d e(\mathfrak{q}, M)$.
4. Si $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$ son $\mathfrak{m}$-primarios, entonces $e(\mathfrak{q}_1, M) \leq e(\mathfrak{q}_2, M)$.

Teorema 1.65: Sea $0 \to N \to M \to P \to 0$ una sucesión exacta de A-módulos finitamente generados. Entonces $e(\mathfrak{q}, M) = e(\mathfrak{q}, N) + e(\mathfrak{q}, P)$.

Demostración: Mirando N como submódulo de M y cocientando todo por $\mathfrak{q}^n$, nótese que

$$\ell\left(\frac{M}{\mathfrak{q}^n M}\right) = \ell\left(\frac{P}{\mathfrak{q}^n P}\right) + \ell\left(\frac{N}{N \cap \mathfrak{q}^m M}\right),$$

por la aditividad de la longitud.

Trivialmente $\mathfrak{q}^n N \subseteq N \cap \mathfrak{q}^n M$ y, por el lema de Artin-Rees

$$N \cap \mathfrak{q}^n M \subseteq \mathfrak{q}^{n-r} N,$$

para algún r fijo y n suficientemente grande. Luego

$$\ell\left(\frac{N}{\mathfrak{q}^n N}\right) \geq \ell\left(\frac{N}{N \cap \mathfrak{q}^n M}\right) \geq \ell\left(\frac{N}{\mathfrak{q}^{n-r} N}\right),$$

por lo que, aplicando la fórmula (1.3) y el teorema del sandwich obtenemos el enunciado. □

Teorema 1.66: Sean $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ los primos minimales de A tales que $k.\dim(A/\mathfrak{p}_i) = d$ (e.g., A es catenario). Entonces:

$$e(\mathfrak{q}, M) = \sum_{i=1}^{r} e(\mathfrak{q}_i/\mathfrak{p}_i, A/\mathfrak{p}_i)\ell_{A_{\mathfrak{p}_i}}(M_{\mathfrak{p}_i}).$$

Notas históricas

El teorema de las intersecciones de Krull fue demostrado originalmente en Krull **[0]** (1938).

2

Álgebras enteras

2.1 Dependencia íntegra

En éste capítulo todas las álgebras se asumen asociativas.

En cierto modo, ya hemos visto que la noción de «álgebra» generaliza las «extensiones de cuerpo», y de que podemos importar varios conceptos de ese mundo como los de elementos algebraicos, trascendencia y su grado, etc., pero siempre con cautela sobre varios detalles: por ejemplo, incluso las álgebras finitamente generadas son meramente módulos y podrían no ser libres, podrían no tener base y demás; pero una cuestión un tanto sutil es que la noción de «ser algebraico» aquí se nos queda corta.

Ejemplo. Considere a $\mathbb{Q}$ como $\mathbb{Z}$-álgebra. Es claro que $\mathbb{Q}$ es algebraico sobre $\mathbb{Z}$ puesto que todo racional $\frac{u}{v} \in \mathbb{Q}$ es raíz de un polinomio $vx-u \in \mathbb{Z}[x]$, pero si tomamos a $\frac{1}{2}$ vemos que la subálgebra generada

$$\mathbb{Z}[1/2] = \left\{ \frac{a}{2^n} \in \mathbb{Q} : a \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

es un $\mathbb{Z}$-módulo que no está finitamente generado. Ésto sucede también para todo racional que no es entero.

Ésto conlleva a una lo siguiente:

Lema 2.1: Sea B una A-álgebra y $\alpha \in B$. Son equivalentes:

1. α es raíz de un polinomio mónico $p(x) \in A[x]$ no constante.
2. El subálgebra $A[\alpha]$ es un A-módulo finitamente generado.
3. $A[\alpha]$ está contenido en un subálgebra C que es un A-módulo finitamente generado.
4. Existe un $A[\alpha]$-módulo fiel sobre que es un A-módulo finitamente generado.

Demostración: $1 \implies 2$. Supongamos que α es raíz de

$$x^{n+1} + c_n x^n + \cdots + c_1 x + c_0.$$

Sabemos que como R-módulo se satisface que $A[\alpha] = \mathrm{Span}_A\{1, \alpha^1, \alpha^2, \dots\}$, pero por el polinomio arriba descrito se tiene que $\alpha^{n+1} \in \mathrm{Span}\{1, \alpha, \dots, \alpha^n\}$ y así también con las potencias superiores de α; de modo que está generado por $\{1, \alpha, \dots, \alpha^n\}$ que es finito.

$2 \implies 3 \implies 4$. Trivial.

$4 \implies 1$. Sea M dicho $A[\alpha]$-módulo fiel que está generado sobre A por $\boldsymbol{m}_1, \dots, \boldsymbol{m}_n$. Luego como $\alpha M \subseteq M$, entonces $\boldsymbol{x} \mapsto \alpha \boldsymbol{x}$ es un endomorfismo de A-módulos y por el teorema de Cayley-Hamilton se obtiene el polinomio mónico deseado. □

Definición 2.2: Sea B una A-álgebra. Un elemento $\alpha \in B$ se dice ***entero*** sobre A. B se dice una A-álgebra ***entera*** si todo elemento de B es entero.

Ejemplo. Consideremos la extensión de anillos $\mathbb{Q}/\mathbb{Z}$ y supongamos que $a/b \in \mathbb{Q}$ es entero. Luego a/b es la raíz de un polinomio de $\mathbb{Z}[x]$ mónico, por el corolario **??** al teorema de la raíz racional se cumple que necesariamente $b = \pm 1$ y que por ende $a/b \in \mathbb{Z}$. Ésto también explica el «desastre» de la subálgebra $\mathbb{Z}[1/2]$.

En éste sentido, el término «elemento entero» también concuerda con nuestra noción de «número entero».

Proposición 2.3: Sea B es una A-álgebra. Si $\alpha \in B$ es entero, entonces $A[\alpha]$ es una extensión entera.

Demostración: Ésto debido a que si $\beta \in A[\alpha]$, entonces $A[\beta] \subseteq A[\alpha]$ el cual es un subálgebra finitamente generado como A-módulo. □

Proposición 2.4: Sea A un dominio íntegro, sea $k := \operatorname{Frac} A$ y sea L/k una extensión de anillos. Sea $\alpha \in L$ algebraico sobre k, entonces existe $c \in A$ tal que $c\alpha \neq 0$ es entero sobre A.

Corolario 2.4.1: Sea A un dominio íntegro, sea $k := \operatorname{Frac} A$ y sea L/k una extensión de anillos. Sea B la clausura íntegra de L/A, entonces $L = \operatorname{Frac} B$.

Teorema 2.5: Sean $C/B/A$ extensiones de anillos. Entonces C/A es una extensión entera syss C/B y B/A son extensiones enteras.

Proposición 2.6: Sea B una A-álgebra. Entonces B es de tipo finito syss es entera y un A-módulo finitamente generado.

Demostración: $\Longleftarrow$. Es claro, pues ser A-módulo finitamente generado implica ser A-álgebra de tipo finito.

$\Longrightarrow$. Sea $\{\alpha_1, \ldots, \alpha_n\}$ un sistema generador de B como A-álgebra. Luego se tiene que

$$A[\alpha_1] \subseteq A[\alpha_1, \alpha_2] \subseteq \cdots \subseteq B$$

es una cadena finita, tal que cada término es una álgebra de tipo finito, finitamente generada como módulo del anterior. □

Proposición 2.7: Sean $C/B/A$ extensiones de anillos, con A noetheriano. Si C es una A-álgebra de tipo finito y se cumple alguno de los siguientes:

(a) C es un B-módulo finitamente generado.

(b) C es entero sobre B.

Entonces B es una A-álgebra de tipo finito.

Demostración: Es claro que las condiciones (a) y (b) son equivalentes, así que supondremos (a). Por hipótesis $C = A[\alpha_1, \ldots, \alpha_n] = \operatorname{Span}_B\{\beta_1, \ldots, \beta_m\}$, luego

$$\alpha_i = \sum_{k=1}^{m} c_{ik}\beta_k, \qquad \beta_i \cdot \beta_j = \sum_{k=1}^{m} d_{ijk}\beta_k,$$

con $c_{ik}, d_{ijk} \in B$. Luego sea $B_0 := A[\{c_{ik}, d_{ijk}\}_{i,j,k}] \subseteq B$, que es una A-álgebra de tipo finito, por lo que B_0 es noetheriano. Nótese que $C = \mathrm{Span}_{B_0}\{\beta_1, \ldots, \beta_m\}$, luego C es un B_0-módulo noetheriano y, B es un B_0-submódulo de C, luego es un B_0-módulo finitamente generado. Finalmente como B_0 es una A-álgebra de tipo finito, entonces B es una A-álgebra de tipo finito. □

Proposición 2.8 (lema de Zariski): Si L/k es una extensión de cuerpos donde L es una k-álgebra de tipo finito, entonces L/k es una extensión finita.

Demostración: Sea $L = k[\alpha_1, \ldots, \alpha_n]$, queremos ver que los α_i's son algebraicos, procedemos por contradicción: luego podemos permutar los índices tales que $\alpha_1, \ldots, \alpha_r$ son trascendentes y algebraicamente independientes y $\alpha_{r+1}, \ldots, \alpha_n$ son algebraicos sobre $F := k(\alpha_1, \ldots, \alpha_r)$. En síntesis, L/k es una k-álgebra de tipo finito y L/F es finitamente generado, por lo que, por el teorema anterior, F es una k-álgebra de tipo finito y $F = k[\beta_1, \ldots, \beta_m]$. Luego para todo $1 \leq i \leq m$ se cumple que $\beta_i = f_i(\alpha_1, \ldots, \alpha_r)/g_i(\alpha_1, \ldots, \alpha_r)$, donde f_i, g_i son polinomios coprimos. Como hay infinitos polinomios irreducibles, entonces debe haber alguno que sea coprimo a todos los g_i's, luego $1/h(\alpha_1, \ldots, \alpha_r) \in F$, pero no puede ser generado como polinomios sobre β_i's, lo que es absurdo. □

Proposición 2.9: Sea $\sigma\colon B \to C$ un homomorfismo de anillos. Si B es un A-álgebra entera, entonces $\sigma[B]$ es entera sobre $\sigma[A]$. Si σ es inyectivo y B/A es extensión anillos, entonces $\sigma[B]/\sigma[A]$ también.

Proposición 2.10: Sea B/A una extensión de anillos, y sea C el conjunto de elementos enteros de B. Entonces C/A es una extensión de anillos.

Demostración: Claramente todo elemento de A es entero sobre A, pues basta considerar el polinomio $x - a$. Ahora hay que probar que C es cerrado bajo sumas y productos. Sean $\alpha, \beta \in B$ enteros. Luego $A[\alpha]$ es finitamente generado como A-módulo y siendo $p(x) \in A[x]$ mónico tal que $p(\beta) = 0$, como $p(x) \in A[\alpha][x]$, entonces $A[\alpha, \beta]$ es entero sobre $A[\alpha]$ y finitamente generado como $A[\alpha]$-módulo. Sean $S, T \subseteq B$ tales que $A[\alpha] = \mathrm{Span}_A S$ y $A[\alpha, \beta] = \mathrm{Span}_{A[\alpha]} T$. Sea

$$U := \{st : s \in S, t \in T\}$$

luego es claro que U es finito y queda al lector comprobar que $A[\alpha, \beta] = \mathrm{Span}_A U$. Como $\alpha + \beta, \alpha \cdot \beta \in A[\alpha, \beta]$, entonces son enteros. □

Definición 2.11: El subanillo C construido en la proposición anterior se le dice la ***clausura íntegra*** de B. Si $C = A$, entonces se dice que A es ***íntegramente cerrado*** sobre B. En particular, decimos que un dominio íntegro A es ***íntegramente cerrado*** (a secas) si lo es sobre $\mathrm{Frac}(A)$.

Proposición 2.12: Sea A un dominio íntegro y un DFU, entonces A es íntegramente cerrado.

Demostración: Al igual que en el caso $\mathbb{Q}/\mathbb{Z}$, se reduce a una aplicación del teorema de las raíces racionales. □

Teorema 2.13: Sea B/A una extensión entera de anillos. Entonces:

1. Si $\mathfrak{b} \trianglelefteq B$ y $\mathfrak{a} := \mathfrak{b} \cap A \trianglelefteq A$, entonces $B/\mathfrak{b}$ es una extensión entera de $A/\mathfrak{a}$.
2. Si S un sistema multiplicativo de A, entonces $S^{-1}B$ es también una extensión entera de $S^{-1}A$.
3. Si S un sistema multiplicativo de A y C es la clausura íntegra de B en A, entonces $S^{-1}C$ es la clausura íntegra de $S^{-1}B$ en $S^{-1}A$.

Proposición 2.14: Sean B/A una extensión entera de dominios íntegros. Entonces A es un cuerpo syss B es un cuerpo.

Demostración: $\Longrightarrow$. Sea $y \in B$ no nulo, entonces existen $a_i \in A$ tales que

$$y^{n+1} + a_n y^n + \cdots + a_1 y + a_0 = 0,$$

luego, como y no es divisor de cero entonces $a_0 \neq 0$, y luego, con un despeje algebraico se obtiene que

$$y^{-1} = -a_0^{-1}(y^n + a_n y^{n-1} + \cdots + a_1) \in B.$$

$\Longleftarrow$. Sea $a \in A_{\neq 0}$, como $a \in B$ y B es cuerpo, entonces $a^{-1} \in B$, luego

$$(a^{-1})^{m+1} + c_n a^{-m} + \cdots + c_1 a^{-1} + c_0 = 0$$

con $c_i \in A$, por lo que, multiplicando por a^m se obtiene que $a^{-1} = -(c_n + \cdots + c_1 a^{m-1} + c_0 a^m) \in A$. □

Proposición 2.15: Sea A un dominio íntegramente cerrado con $k := \mathrm{Frac}\, A$, y sea L/k una extensión finita de cuerpos. Entonces $\alpha \in L$ es entero sobre A syss su polinomio minimal tiene coeficientes en A.

Demostración: Sea $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in k[x]$ el polinomio minimal de α, y sea N la clausura normal de L. Entonces $p(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_n(\alpha))$, donde los σ_j's son todos los k-monomorfismos de L en N. Pero como cada $\sigma_j(\alpha)$ es raíz de $p(x)$, entonces es claro que todos son enteros sobre A, de modo que todos los coeficientes son también enteros sobre A y como A es íntegramente cerrado, entonces pertenecen a A. □

Lema 2.16: Sea B una A-álgebra. Sean $f, g \in B[x]$ mónicos tales que $g \mid f$ y f tiene coeficientes enteros sobre A, entonces g también tiene coeficientes enteros sobre A.

Demostración: Sea B'/B una extensión de anillos tal que $f(x)$ se escinde en B'. Luego se escribe como un producto de factores lineales de sus raíces, las cuales son todas enteras sobre A y g también es un producto de algunos factores, de modo que sus coeficientes también resultan enteros sobre A. □

Proposición 2.17: Sea B una A-álgebra. Si un polinomio en $B[x]$ es entero sobre $A[x]$, entonces sus coeficientes son enteros sobre A.

Demostración: Sea

$$q(t) := t^n + f_{n-1}(x)t^{n-1} + \cdots + f_0(x) \in A[x][t]$$

tal que $q(p(x)) = 0$. Sea $r > \text{máx}_i\{\deg p, \deg f_i\}$. Definamos $p_1(x) := p(x) - x^r$ y sea $q_1(t) := q(t + x^r)$ de modo que $q_1(p_1(x)) = 0$. Expandiendo se tiene que

$$q_1(t) := t^n + g_{n-1}(x)t^{n-1} + \cdots + g_0(x) \in A[x][t]$$

Aplicando $t = p_1(x)$ y reordenando términos se obtiene que

$$g_0 = -p_1 \cdot (p_1^{n-1} + g_{n-1}p_1^{n-2} + \cdots + g_1) \in B[x].$$

Debido a como se eligió a r se cumple que g_0 y p_1 son mónicos, y además se cumple que $p_1 \mid g_0$ de modo que concluimos por el lema anterior. □

Proposición 2.18: Sea A un dominio íntegramente cerrado, entonces $A[x]$ es íntegramente cerrado.

Demostración: Sea $k := \text{Frac}\, A$. Si $f(x) \in k(x) = \text{Frac}(A[x])$ es entero sobre $A[x]$, entonces también lo es sobre $k[x]$, el cual es un DFU y por tanto es íntegramente cerrado, de modo que $f(x) \in k[x]$ y de aquí concluimos por la proposición anterior. □

Corolario 2.18.1: Sea B/A una extensión entera de anillos, y sean $\mathfrak{q} \trianglelefteq B$ y $\mathfrak{p} := \mathfrak{q} \cap A \trianglelefteq A$. Entonces $\mathfrak{q}$ es maximal syss $\mathfrak{p}$ es maximal.

Corolario 2.18.2: Sea B/A una extensión entera de anillos, y sean $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \trianglelefteq B$ primos tales que $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$. Entonces $\mathfrak{q}_1 = \mathfrak{q}_2$.

Demostración: Sea $\mathfrak{p} := \mathfrak{q}_1 \cap A$. Localizando, se obtiene que $B_\mathfrak{p}/A_\mathfrak{p}$ es una extensión entera de anillos y $A_\mathfrak{p}$ es local, así que posee un ideal maximal $\mathfrak{m}$ que es la extensión de $\mathfrak{p}$. Sean $\mathfrak{n}_1, \mathfrak{n}_2$ las extensiones de $\mathfrak{q}_1, \mathfrak{q}_2$ en $B_\mathfrak{p}$, luego $\mathfrak{n}_1^c = \mathfrak{n}_2^c = \mathfrak{m}$, por lo que $\mathfrak{n}_1, \mathfrak{n}_2$ son maximales y por tanto son iguales. □

Teorema 2.19: Sea B/A una extensión entera de anillos, y sea $\mathfrak{p} \trianglelefteq A$ primo. Entonces existe un ideal $\mathfrak{q} \trianglelefteq B$ primo tal que $\mathfrak{p} = \mathfrak{q} \cap A$.

Demostración: Sea $\mathfrak{p} \trianglelefteq A$, consideremos el siguiente diagrama conmutativo dado por la localización:

$$\begin{array}{ccc} A & \xhookrightarrow{\iota} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A_\mathfrak{p} & \xhookrightarrow[\iota]{} & B_\mathfrak{p} \end{array}$$

Sea $\mathfrak{n} \triangleleft B_\mathfrak{p}$ un ideal maximal, luego $\mathfrak{m} := \mathfrak{n} \cap A_\mathfrak{p}$ ha de ser el único ideal maximal de $A_\mathfrak{p}$ y luego definamos $\mathfrak{q} := \beta^{-1}[\mathfrak{n}]$. Pero por la conmutatividad del diagrama se cumple que

$$\mathfrak{q} \cap A = \iota^{-1}[\mathfrak{q}] = (\iota \circ \beta)^{-1}[\mathfrak{n}] = (\alpha \circ \iota)^{-1}[\mathfrak{n}] = \alpha^{-1}[\mathfrak{m}] = \mathfrak{p}. \qquad \square$$

Culminamos ésta sección con los dos teoremas de Cohen y Seidenberg bajo el nombre de «teorema del ascenso» y «del descenso».

Definición 2.20: Sea A un dominio y $\mathfrak{a} \triangleleft A$ un ideal, se define su ***altura***, denotado $\operatorname{alt}\mathfrak{a}$, como el máximo n tal que existen

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n \subseteq \mathfrak{a},$$

donde cada $\mathfrak{p}_i \triangleleft A$ es un ideal primo.

Se puede comprobar $k.\dim A = \sup\{\operatorname{alt}\mathfrak{a} : \mathfrak{a} \triangleleft A\}$ y que $\operatorname{alt}\mathfrak{p} = k.\dim(A_\mathfrak{p})$ para $\mathfrak{p} \triangleleft A$ primo.

Teorema 2.21 (del ascenso de Cohen-Seidenberg): Sea B/A una extensión entera de anillos, y sean

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n \lhd A,$$
$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m \lhd B,$$

dos cadenas de ideales primos, tales que $m < n$ y $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $1 \leq i \leq m$. Luego se puede extender la segunda cadena a

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m \subseteq \cdots \subseteq \mathfrak{q}_n \lhd B$$

con $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $1 \leq i \leq n$.

Demostración: Por inducción basta probar el caso $m = 1 < 2 = n$. Sea $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \lhd A$, y sea $\mathfrak{q}_1 \lhd B$ con las condiciones del enunciado. Luego $\mathfrak{p}_2/\mathfrak{p}_1 \lhd A/\mathfrak{p}_1$ es un ideal primo, y $B/\mathfrak{q}_1$ es una extensión entera de $A/\mathfrak{p}_1$; luego por el teorema anterior, existe $\mathfrak{r} \cap (A/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1$, con $\mathfrak{r} \lhd B/\mathfrak{q}_1$. Para entender el proceso, vea el siguiente diagrama conmutativo:

$$\begin{array}{ccc} A & \xhookrightarrow{\iota_1} & B \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ A/\mathfrak{p}_1 & \xhookrightarrow[\iota_2]{} & B/\mathfrak{q}_1 \end{array}$$

Luego definamos $\mathfrak{q}_2 := \pi_2^{-1}[\mathfrak{r}]$ y se satisface que

$$\begin{aligned} \mathfrak{p}_2 &= \pi_1^{-1}[\mathfrak{p}_2/\mathfrak{p}_1] = \pi_1^{-1}\left[\iota_2^{-1}[\mathfrak{r}]\right] = (\pi_1 \circ \iota_2)^{-1}[\mathfrak{r}] \\ &= (\iota_1 \circ \pi_2)^{-1}[\mathfrak{r}] = \iota_1^{-1}\left[\pi_2^{-1}[\mathfrak{r}]\right] = \iota_1^{-1}[\mathfrak{q}_2] = \mathfrak{q}_2 \cap A. \end{aligned}$$ □

Observación 2.21.1: Más generalmente, si $B \supseteq A$ es una extensión de anillos que satisface el teorema del ascenso se comprueba que $k.\dim B \geq k.\dim A$.

Proposición 2.22: Sea A un dominio íntegro. Son equivalentes:

1. A es íntegramente cerrado.
2. $A_{\mathfrak{p}}$ es íntegramente cerrado para todo $\mathfrak{p} \lhd A$ primo.
3. $A_{\mathfrak{m}}$ es íntegramente cerrado para todo $\mathfrak{m} \lhd A$ maximal.

Lema 2.23: Sea B/A una extensión de anillos, sea $\mathfrak{a} \trianglelefteq A$ y sea C la clausura íntegra de B en A. Considerando $\iota\colon A \to C$, entonces la clausura íntegra de $\mathfrak{a}$ en B es $\mathrm{Rad}(\mathfrak{a}^e)$.

Demostración: Veamos que todo elemento entero está en $\mathrm{Rad}(\mathfrak{a}^e)$: Sea $x \in B$ entero sobre $\mathfrak{a}$, luego

$$x^{n+1} + c_n x^n + \cdots + c_1 x + c_0 = 0$$

para algunos $c_i \in \mathfrak{a}$. Como $x \in C$, entonces $x^{n+1} \in \mathfrak{a}^e$, por lo que $x \in \mathrm{Rad}(\mathfrak{a}^e)$.

Y que todo elemento de $\mathrm{Rad}(\mathfrak{a}^e)$ es entero: Sea $x \in \mathrm{Rad}(\mathfrak{a}^e)$, entonces $x^n \in \mathfrak{a}^e$ para algún n; luego $x^n = \sum_{i=1}^n a_i x_i$ con $x_i \in C$, es decir, $x^n \in \mathfrak{a}[x_1, \ldots, x_n] =: M$. Como $x_i \in C$, entonces M es un $\mathfrak{a}$-módulo finitamente generado, y así $x^n M \subseteq \mathfrak{a}M$. Finalmente x^n es entero sobre $\mathfrak{a}$, y por tanto, x lo es sobre $\mathfrak{a}$. □

Proposición 2.24: Sea B/A una extensión de dominios íntegros, A íntegramente cerrado y $\alpha \in B$ entero sobre $\mathfrak{a} \trianglelefteq A$. Si α es algebraico sobre $k := \mathrm{Frac}(A)$ y su polinomio minimal es

$$x^{n+1} + c_n x^n + \cdots + c_1 x + c_0 = 0$$

entonces $c_i \in \operatorname{Rad} \mathfrak{a}$.

Demostración: Sea K la extensión normal de $k(\alpha)$ y $\alpha_1, \ldots, \alpha_n$ los k-conjungados de α. Más aún, todo α_i es raíz del mismo polinomio mónico con coeficientes en $\mathfrak{a}$, de modo que todos son enteros sobre $\mathfrak{a}$. Luego el polinomio minimal es de la forma $\prod_{i=1}^n (x - \alpha_i)$, de modo que sus coeficientes son potencias de enteros sobre $\mathfrak{a}$, luego están en $\operatorname{Rad} \mathfrak{a}$. □

Teorema 2.25 (del descenso de Cohen-Seidenberg): Sea B/A una extensión entera de anillos, y sean

$$A\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n,$$
$$B\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m,$$

dos cadenas de ideales primos, tales que $m < n$ y $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $1 \leq i \leq m$. Luego se puede extender la segunda cadena a

$$B\mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m \supseteq \cdots \supseteq \mathfrak{q}_n$$

con $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $1 \leq i \leq n$.

Demostración: Por inducción basta probar el caso $m = 1 < 2 = n$. Hay que probar que $\mathfrak{p}_2$ es la contracción de un ideal primo en $B_{\mathfrak{q}_1}$, lo que por la proposición A.6 se reduce a ver que $\mathfrak{p}_2^{ec} = \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A \subseteq \mathfrak{p}_2$.

Sea $x \in \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A$, entonces es de la forma y/s con $y \in \mathfrak{p}_2 B$ y $s \in B \setminus \mathfrak{q}_1$. Nótese que $y \in \mathfrak{p}_2 B \subseteq \operatorname{Rad}(\mathfrak{p}_2 B)$ es entero sobre $\mathfrak{p}_2$, y su polinomio minimal en $k := \operatorname{Frac} A$ es

$$y^{r+1} + a_1 y^r + \cdots + a_r y + a_{r+1} = 0$$

con $c_i \in \operatorname{Rad} \mathfrak{p}_2 = \mathfrak{p}_2$.

Como $x \in A$, entonces $x^{-1} \in k$ y $s = yx^{-1} \in k$. Luego dividiendo la ecuación anterior por x^{-r-1} se obtiene el siguiente polinomio minimal para s:

$$s^{r+1} + b_1 s^r + \cdots + b_r s + b_{r+1} = 0,$$

donde $b_i := a_i/x^i$. Como $s \in B$ y B es entero, entonces s también lo es y en consecuente $b_i \in A$. Si $x \notin \mathfrak{p}_2$ y como $x^i b_i = a_i \in \mathfrak{p}_2$, entonces $b_i \in \mathfrak{p}_2$. Luego $s^{r+1} \in B\mathfrak{p}_2 \subseteq B\mathfrak{p}_1 \subseteq \mathfrak{q}_1$, se concluye que $s \in \mathfrak{q}_1$, lo que es absurdo. En definitiva, $x \in \mathfrak{p}_2$ como se quería probar. □

Observación 2.25.1: Más generalmente, si B/A es una álgebra que satisface el teorema del descenso se comprueba que $k.\dim B \leq k.\dim A$; esto es incondicional ya que $\mathfrak{p}_1 \supset \mathfrak{p}_2$ siempre se elevan a $\mathfrak{q}_1 \supset \mathfrak{q}_2$.

Podemos combinar los teoremas del ascenso y del descenso en el siguiente potente enunciado:

Teorema 2.26: Sea B/A una extensión entera de dominios, entonces $k.\dim A = k.\dim B$.

Y de hecho se puede obtener algo más general:

Corolario 2.26.1: Sea B/A una extensión entera de anillos, donde B es un dominio íntegro y A es íntegramente cerrado. Entonces para todo $\mathfrak{b} \lhd B$ se cumple que

$$\operatorname{alt} \mathfrak{b} = \operatorname{alt}(\mathfrak{b} \cap A).$$

Teorema 2.27: Sea B/A una extensión entera de dominios íntegramente cerrados cuyos cuerpos de fracciones L/K forman una extensión normal. Sea $G := \operatorname{Gal}(L/K)$, entonces:

1. G está en biyección con los A-automorfismos de B.
2. Para todos $\mathfrak{p}, \mathfrak{q}$ ideales primos de B se cumple que $\mathfrak{p} \cap A = \mathfrak{q} \cap A$ syss existe $\sigma \in G$ tal que $\sigma[\mathfrak{p}] = \mathfrak{q}$.

Demostración:

1. En primer lugar, nótese que B es la clausura íntegra de L/A y como B es íntegramente cerrado, entonces es cerrado bajo K-conjugación (pues todo polinomio mónico en $A[x]$ que se anule en algún elemento de B se anula en sus conjugados). Luego $\sigma|_B \colon B \to B$ es un A-automorfismo para todo $\sigma \in G$. Como $L = \mathrm{Frac}(B)$, entonces todo endomorfismo $\tau \colon B \to B$ se extiende de forma única a un endomorfismo $\tau^* \colon L \to L$, lo que prueba la biyección.

2. $\Longleftarrow$. Como todo $\sigma \in G$ fija a K, en particular fija a A y luego

$$\mathfrak{q} \cap A = \sigma[\mathfrak{p}] \cap A = \sigma[\mathfrak{p} \cap A] = \mathfrak{p} \cap A.$$

   $\Longrightarrow$. Lo separaremos en dos casos: si $|G|$ es finito, entonces como $\{\sigma[\mathfrak{p}] : \sigma \in G\}$ es un conjunto finito de ideales primos, debe cumplirse que algún $a \in \mathfrak{q}$ satisface que $a \notin \sigma[\mathfrak{p}]$ para todo $\sigma \in G$, vale decir, $\sigma(a) \notin \mathfrak{p}$ para todo $\sigma \in G$.

   Definamos $b := \prod_{\sigma \in G} \sigma(a)$ y nótese que $\sigma(b) = b$ para todo $\sigma \in G$, luego b es puramente inseparable sobre K, por lo que $b^e \in K$ para algún e. Como $\mathfrak{p}$ es primo, tenemos que $b^e \notin \mathfrak{p}$, pero $b^e \in \mathfrak{q} \cap A$ como se quería ver.

   Si $|G|$ es infinito, supongamos que $\mathfrak{p} \cap A = \mathfrak{q} \cap A$ y definamos una familia $\mathcal{F}$ de pares $(L_\lambda, \sigma_\lambda)$ tales que L_λ/K es una extensión normal y $\sigma_\lambda \in \mathrm{Gal}(L/K)$ es tal que $\mathfrak{q} \cap L_\lambda = \sigma_\lambda[\mathfrak{p} \cap L_\lambda]$. Se denota $(L_\lambda, \sigma_\lambda) \leq (L_\mu, \sigma_\mu)$ cuando $L_\lambda \subseteq L_\mu$ y $\sigma_\mu \restriction L_\lambda = \sigma_\lambda$. Nótese que $(\mathcal{F}, \leq)$ es un conjunto parcialmente ordenado y es claro que toda $\leq$-cadena tiene supremo, luego por el lema de Zorn posee un elemento maximal (L^*, σ^*).

   Si $L \neq L^*$ entonces existe $\alpha \in L \setminus L^*$ y consideramos L' la clausura normal de $L^*(\alpha)/K$, la cual satisface que L'/L^* sea un extensión finita. σ^* se extiende a un K-automorfismo de N, denotado $\bar{\sigma}$. Sea $\mathfrak{p}' := \mathfrak{p} \cap L'$ y $\mathfrak{p}^* := \mathfrak{p} \cap L^*$ (ídem con $\mathfrak{q}$), luego $\mathfrak{q}^* = \sigma^*[\mathfrak{p}^*]$, por definición de $\mathcal{F}$, y

$$\sigma^*[\mathfrak{p}' \cap L^*] = \mathfrak{q}^* = \mathfrak{q}' \cap L^*.$$

   Como L'/L^* es una extensión finita, entonces $\mathrm{Gal}(L'/L^*)$ es finito y por el caso anterior existe $\sigma' \in \mathrm{Gal}(L'/L^*)$ tal que $\sigma'\sigma^*[\mathfrak{p}'] = \mathfrak{q}'$, por

lo que, definiendo $\sigma'' := \sigma^* \circ \sigma'$ se obtiene que $(L', \sigma'') \in \mathcal{F}$ lo que contradice la maximalidad de (L^*, σ^*). Luego $L = L^*$ y $\sigma^*[\mathfrak{p}] = \mathfrak{q}$ como se quería probar. □

§2.1.1 Anillos de Jacobson.

Definición 2.28: Se dice que un anillo A es ***de Jacobson***[1] si todo ideal primo es una intersección de ideales maximales.

Ejemplo. Un anillo local es de Jacobson syss dimensión 0. Si además es noetheriano, entonces es de Jacobson syss es artiniano.

Proposición 2.29: Sea A un dominio, son equivalentes:

1. A es de Jacobson.
2. Si $\mathfrak{p} \lhd A$ es primo, y existe $b \in B := A/\mathfrak{p}$ tal que $B[b^{-1}]$ es cuerpo, entonces B es un cuerpo.

Demostración: $1 \implies 2$. Es fácil notar que B es de Jacobson y es un dominio íntegro, de modo que $\mathfrak{J}(B) = (0)$. Ahora, nótese que un ideal primo $\mathfrak{q} \lhd B[b^{-1}]$ se corresponde con un ideal primo $\mathfrak{p}$ tal que $b \notin \mathfrak{p}$. Como $B[b^{-1}]$ es un cuerpo, su único ideal primo es (0); luego todo ideal primo no nulo de B contiene a b. Luego, si hubiera algún ideal primo $\mathfrak{p}$ no nulo de B, entonces se comprobaría que $b \in \mathfrak{J}(B)$; por lo que, el único ideal primo de B es (0) y es por lo tanto un cuerpo.

$2 \implies 1$. Sea $\mathfrak{q} \lhd A$ y sea $\mathfrak{a}$ la intersección todos los ideales maximales que contienen a $\mathfrak{q}$. Por contradicción, si $\mathfrak{q} \subset \mathfrak{a}$ elijamos $b \in \mathfrak{a} \setminus \mathfrak{q}$. Ahora bien, por el lema de Zorn podemos elegir $\mathfrak{p}$ el ideal maximal de entre los que están en $\mathfrak{q}$ que no contienen a b. Es fácil probar que $\mathfrak{p}$ es primo y no es maximal, luego $B := A/\mathfrak{p}$ no es cuerpo, pero $B[b^{-1}]$ sí lo es puesto que no posee ideales primos no nulos. □

Ahora podemos ver una versión más general del lema de Zariski:

Teorema 2.30 (de los ceros de Hilbert): Sea A un anillo de Jacobson. Si B es una A-álgebra de tipo finito, entonces es de Jacobson. Además, si $\mathfrak{n} \subseteq B$ es maximal, entonces $\mathfrak{m} := \mathfrak{n} \cap A$ es maximal en A y $B/\mathfrak{n}$ es una extensión finita de $A/\mathfrak{m}$.

[1] Ésta definición fue independientemente introducida por W. Krull (1951) que les llama *anillos de Jacobson*, y por O. Goldman (1952) que les llama *anillos de Hilbert*.

Demostración: Veamos un caso sencillo: Si A es un cuerpo y $B = A[x]$, el álgebra polinomial. Sabemos que B es un DIP, luego todo ideal primo no nulo $\mathfrak{n} \subseteq B$ está generado por un único polinomio irreducible mónico f. Es fácil comprobar que $\mathfrak{n}$ es maximal y es claro que $\mathfrak{n} \cap A = (0)$, el único ideal maximal de A. Y claramente $B/\mathfrak{n}$ es una extensión finita de A.

Aún queda probar que B es de Jacobson: Como todo ideal primo no nulo de B es maximal, sólo queda ver que (0) es la intersección del resto de ideales primos. Para ello probaremos que B posee infinitos primos mediante el mismo argumento de Euclides, si $f_1, \ldots, f_r$ son irreducibles en B, entonces $\prod_{i=1}^{r} f_i + 1$ tiene un factor irreducible f_{r+1} que no estaba en la lista original.

Considere ahora el caso en que A es un anillo de Jacobson arbitrario y B está generado por un sólo elemento. Si quisieramos probar que B es de Jacobson por la proposición anterior, veríamos que si existe $b \in B' := B/\mathfrak{p}$ tal que $B'[b^{-1}]$ es cuerpo, entonces B' también. Sustituyendo B por B' y A por $A/\mathfrak{p}^c$ (la contracción) podemos reducirnos al caso en que A es dominio íntegro. En éste caso, querremos probar que si $B[b^{-1}]$ es cuerpo, entonces B es cuerpo y, de hecho, A también es cuerpo.

Como B está generado por un elemento t, entonces vemos que $B = A[x]/\mathfrak{q}$ donde $\mathfrak{q} \lhd A[x]$ es primo. En primer lugar, afirmamos que $\mathfrak{q} \neq (0)$, de lo contrario, $B[b^{-1}] = A[x][b^{-1}]$ es cuerpo. Definiendo $K := \mathrm{Frac}(A)$, notamos que ésto también implica que $K[x][b^{-1}]$ es cuerpo, pero $K[x]$ es de Jacobson por el caso demostrado al principio y $K[x]$ no es cuerpo lo que contradice la caracterización de la proposición anterior. Como $\mathfrak{q} \neq (0)$, entonces $B[b^{-1}] = K[x]/(\mathfrak{q}K)[x]$ el cual es una extensión finita de cuerpos de K.

Dado $f(x) \in \mathfrak{q}$, éste posee una raíz $\alpha \in B$ de modo que

$$f(\alpha) = c_n\alpha^n + \cdots + c_1\alpha + c_0 = 0,$$

nótese que como f posee coeficientes en A, entonces vemos que $B[c_n^{-1}]$ es una extensión entera de $A[c_n^{-1}]$. Como B es una A-álgebra entera, entonces b es raíz de algún polinomio

$$d_0 b^m + \cdots + d_m = 0,$$

donde cada $d_i \in A$. Como B es dominio íntegro, b y sus potencias son no nulas, luego podemos suponer $d_{m-1} \neq 0$. Luego dividiendo por $d_m b^m$ y definiendo $\beta := b^{-1}$ tenemos que

$$(d_0/d_m) + (d_1/d_m)(1/b) + \cdots + (1/b)^m = \beta^m + \cdots + (d_1/d_m)\beta + (d_0/d_m) = 0.$$

Por lo que se comprueba que $B[b^{-1}] = B[\beta]$ es una extensión entera de $A[1/(c_n d_m)]$. Finalmente concluimos por la proposición 2.14 que $A[(c_n d_m)^{-1}]$ es cuerpo y luego A también. Empleando nuevamente 2.14 vemos que como B/A es extensión entera y A es cuerpo, entonces B también.

El caso general sale de aplicar inducción sobre la cantidad de generadores de B. □

Proposición 2.31: Sea A un dominio. Son equivalentes:

1. A es de Jacobson.
2. Para todo $\mathfrak{a} \lhd A$ se cumple que $\operatorname{Rad}\mathfrak{a}$ es la intersección de los ideales maximales que le contienen.
3. Para todo $\mathfrak{a} \lhd A$ se cumple que $\mathfrak{N}(A/\mathfrak{a}) = \mathfrak{J}(A/\mathfrak{a})$.

2.2 Normalización y dimensión

Aquí comenzaremos a ver unos primeros resultados sobre dimensión y cómo calcularla.

Lema 2.32: Sea $f \in K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ no constante. Existen $y_1 := f, y_2, \ldots, y_n \in K[\boldsymbol{x}]$ tales que la extensión $K[\boldsymbol{x}]/K[\boldsymbol{y}]$ es entera. Además:

1. Dado $q \in \mathbb{N}_{\neq 0}$ podemos exigir que $y_j = x_j + x_1^{m_j}$ con $q \mid m_j$ para todo $j > 1$.
2. Si K es infinito, podemos exigir que $y_j = x_j + c_j x_1$ con $c_j \in k$ para todo $j > 1$.

Demostración:

1. Sea $f(\boldsymbol{x}) = \sum_\alpha b_\alpha \boldsymbol{x}^\alpha$ en notación multiíndice. Sea t un múltiplo de q tal que $t > \deg f$, sean $m_j := t^{j-1}$ y sean $y_j := x_j + x_1^{m_j}$ cuando $j \neq 1$. Definimos el *peso* de un multiíndice $w(\alpha) := \sum_{j=1}^n \alpha_j m_j$. Nótese que para monomios $\boldsymbol{x}^\alpha$ y $\boldsymbol{x}^\beta$ de grados $< t$ se cumple que $w(\alpha) > w(\beta)$ syss $(\alpha_n, \ldots, \alpha_1) > (\beta_n, \ldots, \beta_1)$ en orden lexicográfico, de modo que existe un único monomio con peso máximo en f, digamos $\boldsymbol{x}^\gamma$.

   Nótese que todo monomio $\boldsymbol{x}^\alpha$ en f es de la forma:

   $$\boldsymbol{x}^\alpha = x_1^{w(\gamma)} + (\text{términos en } x_1, y_2, \ldots, y_n \text{ de menor grado en } x_1).$$

Luego, sumando sobre todos los monomios de f, se tiene que

$$f = y_1 = a x_1^{w(\gamma)} + (\text{términos en } x_1, y_2, \ldots, y_n \text{ de menor grado en } x_1),$$

de lo que se concluye que x_1 es entero en $K[\boldsymbol{y}]$. Luego $x_j = y_j - x_j^{m_j}$ también es entero en $K[\boldsymbol{y}]$ para todo $j > 1$.

2. Sean $y_j := x_j + c_j x_1$ para $j > 1$ con $c_j \in K$ sin fijar. Sea $d := \deg f$, luego escribiendo f en términos de $\boldsymbol{y}$ se obtiene

$$f(\boldsymbol{y}) = \sum_{\alpha} b_\alpha x_1^{\alpha_1} \prod_{j=2}^{n} (y_j - c_j x_1)^{\alpha_j},$$

expandiendo los términos se obtiene que hay un coeficiente a de x_1^d, pero que bien podría ser nulo. Sea f_d la componente homogénea de $f(\boldsymbol{x})$ de grado d, luego es fácil notar que $a = f_d(1, -c_2, \ldots, -c_n)$. Fijando suficientes coordenadas, obtendremos un polinomio en una sola variable que es no nulo y solo tiene finitas raíces, así que para alguna combinación $c_2, \ldots, c_n$ se cumple que $a \neq 0$ y así vemos que x_1 es entero en $K[\boldsymbol{y}]$. □

Teorema 2.33: Sea K un cuerpo con cuerpo primo k. Sea $\mathfrak{a} \trianglelefteq K[\boldsymbol{x}] = K[x_1, \ldots, x_n]$ con $\operatorname{alt} \mathfrak{a} = r$, entonces existen $y_1, \ldots, y_n \in K[\boldsymbol{x}]$ tales que:

1. $K[\boldsymbol{x}]/K[\boldsymbol{y}]$ es entero.
2. $\mathfrak{a} \cap K[\boldsymbol{y}]$ está generado por $y_1, \ldots, y_r$.
3. $y_{r+i} = x_{r+i} + f_i$ con $f_i \in k[x_1, \ldots, x_r]$ (y si $\operatorname{car} K = p \neq 0$ entonces $f_i \in k[x_1^p, \ldots, x_r^p]$) donde $1 \leq i \leq n - r$.

Demostración: Procedemos por inducción sobre r. El caso $r = 0$ implica que $\mathfrak{a} = (0)$ y luego $y_i := x_i$ basta.

Para el caso inductivo sea $\mathfrak{b} \subseteq \mathfrak{a}$ tal que $\operatorname{alt} \mathfrak{b} = r - 1$ (e.g., $\mathfrak{b} := \mathfrak{a} \cap \mathfrak{p}$, donde $\mathfrak{p}$ es un ideal primo de altura $r - 1$). Luego, por hipótesis inductiva existen $\boldsymbol{y'} := (y'_1, \ldots, y'_n)$ tales que se satisfacen 1, 2 y 3. Nótese que

$$\mathfrak{b} \cap K[\boldsymbol{y'}] = \sum_{i=1}^{r-1} y'_i \cdot K[\boldsymbol{y'}] \subseteq \mathfrak{a} \cap K[\boldsymbol{y'}].$$

Como $K[\boldsymbol{x}]/K[\boldsymbol{y'}]$ es una extensión entera, entonces por el corolario 2.26.1 se cumple que $\operatorname{alt}(\mathfrak{b} \cap K[\boldsymbol{y'}]) = r - 1$ y $\operatorname{alt}(\mathfrak{a} \cap K[\boldsymbol{y'}]) = r$. Luego existe

$f(\boldsymbol{y}') \in \mathfrak{a} \setminus \mathfrak{b}$ y definir $g(\boldsymbol{y}') := f(0, \ldots, 0, y'_r, \ldots, y'_n)$. y aplicar el lema anterior para obtener $g =: y''_r, \ldots, y''_n$ tales que $K[y'_r, \ldots, y'_n]/K[y''_r, \ldots, y''_n]$ es una extensión entera de anillos. Definiendo $y_i := y'_i$ para $0 \leq i \leq r-1$ y $y_{r+i} := y''_{r+i}$ para $0 \leq i \leq n-r$ vemos que se cumple la condición 3. La condición 2 sale de la elección del g y de los y_j's y la condición 1 sale del hecho de que $K[\boldsymbol{x}]/K[\boldsymbol{y}']$ y $K[\boldsymbol{y}']/K[\boldsymbol{y}]$ son extensiones enteras. □

Teorema 2.34 – *Teorema de normalización de Noether*: Sea A una K-álgebra (asociativa y conmutativa) de tipo finito. Entonces existen $x_1, \ldots, x_n \in A$ tales que:

1. $A/K[\boldsymbol{x}]$ es una extensión entera de anillos.
2. $x_1, \ldots, x_n$ son algebraicamente independientes sobre K.

Demostración: Sea A generado por $\{a_1, \ldots, a_n\}$, ésto es equivalente a decir que el homomorfismo:

$$\varphi := \mathrm{ev}_{a_1,\ldots,a_n} \colon K[z_1, \ldots, z_n] =: K[\boldsymbol{z}] \longrightarrow A$$

es suprayectivo. Sea $\mathfrak{a} := \ker \varphi \lhd K[\boldsymbol{z}]$, luego por el teorema anterior se obtiene $\boldsymbol{y}$ tal que $K[\boldsymbol{z}]/K[\boldsymbol{y}]$ es entero y si $\operatorname{alt} \mathfrak{a} = r$ entonces $\mathfrak{a} \cap K[\boldsymbol{y}]$ está generado por $y_1, \ldots, y_r$. Definamos $x_i := \varphi(y_{r+i})$ para $0 \leq i \leq n-r$. Entonces

$$A = K[\boldsymbol{a}] = \varphi[K[\boldsymbol{z}]]/\varphi[K[\boldsymbol{y}]] = K[\boldsymbol{x}]$$

es una extensión entera de anillos. Si hubiera alguna relación $\sum_\alpha c_\alpha \boldsymbol{x}^\alpha = 0$ (en notación multiíndice) ésto significaría que $\sum_\alpha c_\alpha \boldsymbol{y}^\alpha \in \mathfrak{a}$, pero los $x_i = y_{r+i} \notin \mathfrak{a} \cap K[\boldsymbol{y}]$, luego los coeficientes $c_\alpha = 0$, lo que prueba que $x_1, \ldots, x_n$ son algebraicamente independientes sobre K. □

Teorema 2.35: Sea A un dominio íntegro que es una K-álgebra de tipo finito. Si

$$(0) = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_t$$

es una cadena maximal de ideales primos de A (i.e., que no se puede extender a otra cadena), entonces $t = k.\dim A = \operatorname{trdeg}_K A$.

Demostración: Procedemos por inducción sobre t. Por el teorema de normalización de Noether existen $\boldsymbol{x} := (x_1, \ldots, x_n)$ en A, algebraicamente independientes sobre K, tales que $A/K[\boldsymbol{x}]$ es una extensión entera. Si $t = 0$,

entonces $k.\dim(A) = 0$ y A es un cuerpo, luego $K[\boldsymbol{x}]$ también es un cuerpo (por la proposición 2.14) y por ende $n = 0$.

Para el caso inductivo, como $\mathfrak{p}_1 = (f)$ es principal y no es (1) entonces podemos asumir que $f \in K[\boldsymbol{x}]$ es no constante. Luego por el lema 2.32 podemos cambiar los $\boldsymbol{x}$'s por $\boldsymbol{y}$ de modo que los $\boldsymbol{y}$ son algebraicamente independientes sobre K, que $A/K[\boldsymbol{x}]/K[\boldsymbol{y}]$ es entero y tal que $f = y_1 \in \mathfrak{p}_1 \cap K[\boldsymbol{y}]$. Luego el cociente $A/\mathfrak{p}_1$ es entero sobre $K[\boldsymbol{y}]/y_1K[\boldsymbol{y}] \cong K[y_2, \ldots, y_n]$ y aplicamos la hipótesis inductiva para concluir que $t - 1 = n - 1$. □

En capítulos superiores exploraremos la teoría de la dimensión en un contexto más general, pero es bastante motivador ver la regularidad que posee en el contexto de álgebras de tipo finito sobre cuerpos.

Definición 2.36: Sea A un anillo de $k.\dim A =: d < \infty$. Se dice que A es ***catenario*** si toda cadena maximal de primos tiene longitud d. Se dice que A es ***universalmente catenario*** si es noetheriano y toda A-álgebra de tipo finito es catenaria.

Corolario 2.36.1: Sea A un dominio íntegro que es una K-álgebra de tipo finito. Sea $\mathfrak{p} \lhd A$ primo, entonces

$$\operatorname{trdeg}_K(A) = \operatorname{trdeg}_K(A/\mathfrak{p}) + \operatorname{alt}\mathfrak{p}.$$

Además:

1. Si $\mathfrak{m} \lhd A$ es maximal, entonces $L := A/\mathfrak{m}$ es una extensión algebraica de cuerpos de K.

2. A es catenario. En consecuencia, todo cuerpo y toda k-álgebra de tipo finito es universalmente catenario.

Ejemplo. Finalmente, $k.\dim(k[x_1, \ldots, x_n]) = n$.

La propiedad de ser *catenario* es una de las principales cualidades que buscamos en un anillo y los teoremas anteriores son de vital importancia.

Así, tenemos que el caso de k-álgebras de tipo finito es bien comportado, veamos un par de contraejemplos:

Lema 2.37: Sea A un dominio, $B := A[x]$ y $\mathfrak{P} \subseteq \mathfrak{Q} \lhd B$ un par de primos de B tales que $\mathfrak{P} \cap A = \mathfrak{Q} \cap A =: \mathfrak{p} \lhd A$ es un primo. Entonces $\mathfrak{P} = \mathfrak{p}B$.

Demostración: Dividiendo por $\mathfrak{p}B$ podemos suponer que $\mathfrak{p} = (0)$. Localizando por $S := A \setminus \{0\}$, podemos suponer además que $A = k$ es un cuerpo, en cuyo caso es trivial puesto que $k[x]$ es un DIP. □

Proposición 2.38: Sea A un dominio, entonces

$$k.\dim A + 1 \leq k.\dim(A[x]) \leq 2\,k.\dim A + 1.$$

Demostración: Si $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d \lhd A$ es una cadena de primos, entonces definiendo $\mathfrak{P}_i := \mathfrak{p}_i B$ y $\mathfrak{P}_{d+1} := \mathfrak{P}_d + x \cdot A[x]$ se prueba que $k.\dim(A[x]) \geq k.\dim A + 1$.

Si $\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_s \lhd A[x]$ es una cadena de primos, entonces la bajamos mediante $\mathfrak{p}_i := \mathfrak{P}_i \cap A$. Por el lema anterior, no se puede dar que $\mathfrak{p}_i = \mathfrak{p}_{i+1} = \mathfrak{p}_{i+2}$, así pues la cadena original de largo $s+1$ (contando $\mathfrak{P}_0$) se baja a una cadena de largo $\frac{s+1}{2}$, así que

$$\frac{s-1}{2} \leq k.\dim A \iff k.\dim(A[x]) = s \leq 2\,k.\dim A + 1. \qquad \square$$

Lo «desastroso» es que todos los valores en la cota se pueden alcanzar.

Lema 2.39: Sea $\mathfrak{a} \lhd A$ un ideal propio y sea $\mathfrak{p} \lhd A$ un primo $\subseteq$-minimal de los que se contienen a $\mathfrak{a}$. Con $B := A[x]$ se cumple que $\mathfrak{p}B$ es un primo $\subseteq$-minimal de los que contienen a $\mathfrak{a}B$.

Demostración: Sustituyendo A por $A/\mathfrak{a}$ podemos suponer que $\mathfrak{a} = (0)$. Así de existir $\mathfrak{q} \subseteq \mathfrak{p}B$ primo, entonces $\mathfrak{q} \cap A \subseteq \mathfrak{p}$ y por minimalidad se alcanza la igualdad, luego $\mathfrak{q} = \mathfrak{p}B$. □

Proposición 2.40: Sea A un dominio noetheriano y sea $B := A[x]$.

1. Para todo primo $\mathfrak{p} \lhd A$ se tiene que $\operatorname{alt}\mathfrak{p} = \operatorname{alt}(\mathfrak{p}B)$.
2. $k.\dim B = k.\dim A + 1$ y, más generalmente, $k.\dim(A[x_1, \ldots, x_n]) = k.\dim A + n$.

Demostración:

1. Sea $n := \operatorname{alt}\mathfrak{p}$, luego por el teorema fundamental de la teoría de la dimensión, existe un ideal $\mathfrak{q} \lhd A$ que es $\mathfrak{p}$-primario y generado por n elementos. Luego $\mathfrak{p}$ es un primo $\subseteq$-minimal de los que contienen a $\mathfrak{q}$, y luego $\mathfrak{p}B$ es un primo $\subseteq$-minimal de los que contienen a $\mathfrak{q}B$.

Nuevamente se concluye que $\operatorname{alt}(\mathfrak{p}B) \leq n$ y la otra desigualdad es clara.

2. Por inducción es claro que basta probar que $k.\dim B = k.\dim A + 1$, y por la proposición 2.38, basta probar que $k.\dim B \leq k.\dim A + 1$. Sea $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_r \lhd B$ una cadena de longitud maximal, y sea $\mathfrak{p}_i := \mathfrak{P}_i \cap A \lhd A$. Si todos los $\mathfrak{p}_i$'s son distintos, entonces $r \leq k.\dim A$. Si no, entonces sea j el máximo entero tal que $\mathfrak{p}_j = \mathfrak{p}_{j+1}$. Así pues, $\mathfrak{P}_j = \mathfrak{p}_j B$ y $\operatorname{alt}\mathfrak{p}_j = \operatorname{alt}\mathfrak{P}_j \geq j$. Ahora bien, como

$$\mathfrak{p}_j \subset \mathfrak{p}_{j+2} \subset \cdots \subset \mathfrak{p}_r \lhd A,$$

es una cadena de primos, entonces $r - (j+1) + \operatorname{alt}\mathfrak{p}_j \leq k.\dim A$, o equivalentemente, $r \leq k.\dim A + 1$. □

§2.2.1 Anillos normales y completamente normales.

Definición 2.41: Se dice que un anillo A es ***normal*** si para todo primo $\mathfrak{p} \lhd A$ se cumple que $A_{\mathfrak{p}}$ es un dominio íntegramente cerrado.

La proposición 2.22 ahora dice que un dominio íntegro es íntegramente cerrado syss es normal.

Proposición 2.42: Sea A un anillo normal. Se cumplen:

1. A es íntegramente cerrado en su anillo de fracciones totales A_{tot}.
2. Para todo $S \subseteq A$ sistema multiplicativo, entonces $S^{-1}A$ es normal.
3. El anillo polinomial $A[x]$ es normal.
4. Si B es normal, entonces $A \times B$ es normal.

Demostración:

1. Sea $f \in A_{\text{tot}}$ y sea $\mathfrak{a} := \{a \in A : af \in A\}$. Para un primo $\mathfrak{p} \lhd A$ arbitrario, tenemos que $A \subseteq A_{\mathfrak{p}}$ es un A-módulo plano, entonces $A_{\mathfrak{p}} \subseteq A_{\text{tot}} \otimes_A A_{\mathfrak{p}}$ y como $A_{\mathfrak{p}}$ es íntegro normal, entonces $f \otimes 1 \in A_{\mathfrak{p}}$. Sean $a, b \in A$ con $b \notin \mathfrak{p}$ tales que $f \otimes 1 = a \otimes 1/b$, entonces $bf - a = 0 \in (A_{\text{tot}})_{\mathfrak{p}}$, vale decir, existe $c \in A \setminus \mathfrak{p}$ tal que $c(bf - a) = 0$, por lo que $bc \in \mathfrak{a} \setminus \mathfrak{p}$. Así $\mathfrak{a}$ no está contenido en $\mathfrak{p}$, y como aplica para cualquier primo, vemos que $\mathfrak{a} = A$.

2. Trivial.

3. Para todo primo $\mathfrak{q} \lhd A[x]$, sea $\mathfrak{p} := \mathfrak{q}^c = \mathfrak{q} \cap A$, entonces $A_\mathfrak{p}[x]$ es un dominio íntegro normal, por lo que $(A[x])_\mathfrak{q} = (A_\mathfrak{p}[x])_{\mathfrak{q}^e}$ es también normal.

4. Basta notar que los primos de $A \times B$ son los de la forma $\mathfrak{p} \times B$ y $A \times \mathfrak{q}$, donde $\mathfrak{p} \lhd A, \mathfrak{q} \lhd B$ son primos. □

Proposición 2.43: Sea A un anillo con finitos primos minimales (e.g., A noetheriano) y reducido. Son equivalentes:

1. A es normal.

2. A es íntegramente cerrado en A_{tot}.

3. A es el producto de finitos dominios íntegros normales.

Demostración: $3 \implies 1 \implies 2$. Basta aplicar la proposición anterior.

$2 \implies 3$. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ los primos minimales de A. Entonces, sabemos que $A_{\text{tot}} \cong \prod_{i=1}^n A_{\mathfrak{p}_i}$, donde cada $A_{\mathfrak{p}_i}$ es un dominio íntegro de dimensión 0, luego es un cuerpo. Denótese $e_i := (0, \ldots, 1, \ldots, 0)$ el i-ésimo idempotente de A_{tot}.

Ahora biem, como los $\mathfrak{p}_i$'s son finitos y A es reducido, por el teorema chino del resto vemos que

$$A \cong \prod_{i=1}^n A/\mathfrak{p}_i \hookrightarrow \prod_{i=1}^n A_{\mathfrak{p}_i} \cong A_{\text{tot}},$$

donde $A_{\mathfrak{p}_i} = \text{Frac}(A/\mathfrak{p}_i)$. Finalmente, como A es íntegramente cerrado en A_{tot}, contiene a todos los idempotentes e_i's y de esto es fácil corroborar que la extensión de anillos $A/\mathfrak{p}_i \to A_{\mathfrak{p}_i}$ es íntegramente cerrada. □

Definición 2.44: Sea A un dominio íntegro con $K := \text{Frac}\, A$. Un elemento $\beta \in K$ se dice ***casi-entero*** sobre A si existe $a \in A_{\neq 0}$ tal que $a\beta^n \in A$ para todo $n \geq 0$.

Se dice que A es ***completamente normal*** si todo elemento casi-entero de K está en A.

Del mismo modo en que uno puede construir una clausura íntegra de anillos y ver que es un anillo, uno puede probar que existe una *clausura casi-íntegra*, aunque ésta es bastante peor comportada, por ejemplo, puede darse que la clausura casi-íntegra de A no sea completamente normal.

Proposición 2.45: Sea A un dominio íntegro con $K := \operatorname{Frac} A$.

1. Si α, β son casi-enteros, entonces $\alpha + \beta, \alpha\beta$ también lo son.
2. Todo elemento entero de K es casi-entero.
3. Si A es noetheriano, todo elemento casi-entero de K es entero. En consecuencia, si A es noetheriano, entonces es normal syss es completamente normal.

Demostración:

1. Sean $u, v \in A$ tales que $u\alpha^n, v\beta^n \in A$ para todo n. Luego $uv(\alpha\beta)^n \in A$ y $uv(\alpha+\beta)^n \in A$ expandiendo el binomio.
2. Si $\beta \in K$ es entero, entonces el A-módulo $A[\beta]$ es finitamente generado y tiene un sistema generador $\{1, \beta, \ldots, \beta^n\}$. Escogiendo $a \in A$ un denominador común para todos, entonces $a\beta^i \in A$ para $0 \leq i \leq n$, y es fácil ver que $a\beta^j \in A$ con $j > n$.
3. Sea $\beta \in K$ casi-entero y sea $a \in A_{\neq 0}$ tal que $a\beta^n \in A$ para todo $n \geq 0$, es decir, $A[\beta] \subseteq \frac{1}{a}A$ como A-módulos, donde $\frac{1}{a}A$ es claramente finitamente generado; como A es noetheriano, entonces $A[\beta]$ es finitamente generado y β es entero. □

Proposición 2.46: Sea A un anillo completamente normal. Entonces $A[x]$ y $A[[x]]$ también son completamente normales.

Demostración: Sea $K := \operatorname{Frac} A$, entonces $\operatorname{Frac}(A[x]) = K(x)$. Sea $u \in K(x)$ casi entero sobre $A[x]$, entonces $u \in K[x]$ puesto que $K[x]$ es completamente normal (puesto que $K[x]$ es noetheriano y es normal ya que es DFU). Expandamos $u(x) = a_0 + a_1x + \cdots + a_rx^r \in K[x]$ y sea $f(x) := b_0 + b_1x + \cdots b_sx^s \in A[x]$ tal que $fu^n \in A[x]$ para todo n. Luego $b_sa_r^n \in A$ para todo n, es decir, $a_r \in K$ es casi entero sobre A, luego, como A es completamente normal, se concluye que $a_r \in A$. Consideramos $u(x) - a_rx^r$ y por inducción vamos comprobando que cada coeficiente está en A.

Para $A[[x]]$ el razonamiento es análogo. □

§2.2.2 Anillos japoneses.

Definición 2.47: Sea A un dominio íntegro y $K := \operatorname{Frac} A$. Se dice que A es:

J1 Si la clausura íntegra $\mathcal{O}_{K/A}$ es un A-módulo finitamente generado.

J2 o Japonés Si para toda extensión finita L/K, la clausura íntegra $\mathcal{O}_{L/A}$ es un A-módulo finitamente generado.

Se dice que un anillo A es un anillo ***universalmente japonés*** si toda A-álgebra íntegra de tipo finito es un anillo japonés.

Hay varios teoremas que vinculan clausuras íntegras sobre extensiones *separables*; la propiedad de «ser un anillo japonés» es más fuerte y es de gran utilidad en la geometría algebraica.

Ejemplo. Todo cuerpo es un anillo japonés.

Proposición 2.48: Sea A un dominio íntegro normal con $K := \operatorname{Frac} A$. Sea L/K una extensión finita separable de cuerpos y sea $B := \mathcal{O}_{L/A}$. Entonces B es un A-módulo finitamente generado.

En consecuncia, si A es un dominio íntegro normal con $\operatorname{Frac} A$ perfecto (e.g., si $\operatorname{car} A = 0$), entonces A es japonés.

Demostración: Sea $\alpha_1, \ldots, \alpha_n$ una K-base de L y supongamos que cada $\alpha_i \in B$ (podemos multiplicarlo por algún denominador de A). Sea $\beta_1, \ldots, \beta_n$ la K-base dual de L, es decir, tal que $\operatorname{Tr}_{L/K}(\alpha_i \beta_j) = \delta_{ij}$ para todo i, j. Para todo $\gamma \in B$, existen $c_j \in K$ tales que $\gamma = \sum_{j=1}^{n} c_j \beta_j$. Podemos calcular

$$\operatorname{Tr}_{L/K}(\gamma \alpha_i) = \sum_{j=1}^{n} c_j \operatorname{Tr}_{L/K}(\beta_j \alpha_i) = c_i \in A.$$

En conclusión,

$$B \subseteq \beta_1 A + \cdots + \beta_n A.$$

Luego B es un submódulo finitamente generado de A, por ende es un A-módulo noetheriano y es fácil concluir que también es noetheriano como anillo. □

Ejemplo. $\mathbb{Z}$ es un anillo japonés.

Corolario 2.48.1: Sea A un dominio íntegro de $\operatorname{car} A = 0$. Entonces A es japonés syss es universalmente japonés.

Corolario 2.48.2: Sea A un dominio íntegro noetheriano con $k := \operatorname{Frac} A$. Entonces A es universalmente japonés syss para toda extensión L/k puramente inseparable, la clausura íntegra $B := \mathcal{O}_{L/A}$ es un A-módulo finitamente generado.

Demostración: Sea □

Proposición 2.49: Sea k un cuerpo y sea A un dominio íntegro que es una k-álgebra de tipo finito. Dada una extensión finita L de $K := \operatorname{Frac} A$, sea $B := \mathcal{O}_{L/A}$; entonces B es un A-módulo finitamente generado. En resumen, A es japonés y los cuerpos son universalmente japoneses.

Demostración: Por normalización de Noether, A es la extensión entera de algún $k[x_1, \ldots, x_n]$ y B es una extensión entera de $k[\boldsymbol{x}]$, así que podemos suponer que $A = k[\boldsymbol{x}]$. Agrandando L, podemos suponer que L/K es una extensión normal y ahora procedemos por casos:

(i) L/K es separable: Entonces basta aplicar la proposición anterior, pues $k[\boldsymbol{x}]$ es normal ya que k es normal.

(ii) L/K es puramente inseparable: Entonces existe un $q := (\operatorname{car} k)^r$ para algún r, de manera que $y_i^q \in K = k(x_1, \ldots, x_n)$. Así, como y_i^q es una función racional en los x_j's sean $c_1, \ldots, c_m$ los coeficientes que aparecen al expresarlo como fracción. Luego L/K está contenido en

$$L' := k'(x_1^{1/q}, \ldots, x_n^{1/q}), \qquad k' = k(c_1^{1/q}, \ldots, c_m^{1/q}),$$

y la clausura íntegra B' de A en L' es

$$B' = k'[x_1^{1/q}, \ldots, x_m^{1/q}],$$

el cual es un A-módulo libre de rango finito, luego $B \subseteq B'$ es un A-módulo finitamente generado. □

§2.2.3 Aplicación: Teorema de Lindemann-Weierstrass. Es conocido el hecho de que casi todos los números complejos son trascendentes, y de que los dos ejemplos por excelencia son e y π. En ésta sección veremos como emplear las nociones de dependencia íntegra para obtener un teorema que nos dará una demostración de éste conocido dato (y muchos otros ejemplos).

Lema 2.50: Sean $u_1, \ldots, u_n \in \mathbb{A}$ números algebraicos, sea $f(x) = \sum_{j=0}^{t} a_k x^k \in \mathbb{Z}[x]$ un polinomio no nulo tal que $f(u_i) = 0$ para todo i. Sea

$$M := \text{máx}\left\{\sum_{j=0}^{t} |a_j|\,|u_i|^j, \sum_{j=0}^{t} |a_j|\,|u_i|^{j+1} : i = 1, \ldots, n\right\}$$

y sea p un primo con $p > \text{máx}\{|a_0|, 2|u_1|, \ldots, 2|u_n|\}$. Existe un entero N_p no divisible por p y un polinomio $g_p(x) \in \mathbb{Z}[x]$ de grado $< tp$ tal que

$$|N_p e^{u_i} - p g_p(u_i)| < \frac{2M^p}{(p-1)!}.$$

Demostración: Definamos:

$$h(x) := x^{p-1} f(x)^p = \sum_{j=p-1}^{r} b_j x^j,$$

donde $b_{p-1} = a_0^p$ y $r = tp + p - 1$. Ahora emplearemos la serie de potencias de e^x (cf. [**48,** Cor. 1.58]) y notamos que

$$\begin{aligned} j! b_j e^x = &\left(j! b_j + \frac{j!}{1!} b_j x + \cdots + \frac{j!}{(j-p)!} b_j x^{j-p}\right) \\ &+ \left(\frac{j!}{(j-p+1)!} b_j x^{j-p+1} + \cdots + j b_j x^{j-1}\right) \\ &+ b_j x^j \left(1 + \frac{x}{j+1} + \frac{x^2}{(j+1)(j+2)} + \cdots\right) \end{aligned}$$

donde el primer paréntesis se asume nulo si $j \leq p-1$. Nótese que $\frac{j!}{k!} = (j-k)!\binom{j}{k}$ el cual es múltiplo de $p!$ si $0 \leq k \leq j-p$, de modo que el primer paréntesis tiene coeficientes enteros que son múltiplos de $p!$ Defina

$$N_p := \frac{1}{(p-1)!} \sum_{j=p-1}^{r} j! b_j \in \mathbb{Z},$$

el cual satisface que $N_p \equiv b_{p-1} = a_0^p \equiv a_0 \pmod{p}$. Nótese que se ha de cumplir

$$\begin{aligned} (p-1)! N_p e^x &= \sum_{j=p-1}^{r} j! b_j e^x \\ &= p! g_p(x) + \sum_{j=b-1}^{r} \left(\frac{j!}{(j-p+1)!} b_j x^{j-p+1} + \cdots + j b_j x^{j-1}\right) \end{aligned}$$

$$+\sum_{j=p-1}^{r} b_j x^j \left(1+\frac{x}{j+1}+\frac{x^2}{(j+1)(j+2)}+\cdots\right),$$

donde $g_p(x)\in\mathbb{Z}[x]$ y cuyo grado es $\leq r-p=tp-1$. Nótese que las derivadas de h son

$$\begin{aligned}
h'(x) &= \sum_{j=p-1}^{r} j b_j x^{j-1}\\
h''(x) &= \sum_{j=p-1}^{r} j(j-1) b_j x^{j-2} = \sum_{j=p-1}^{r} \frac{j!}{(j-2)!} b_j x^{j-2}\\
&\vdots\\
h^{(p-1)}(x) &= \sum_{j=p-1}^{r} \frac{j!}{(j-p+1)!} b_j x^{j-p+1}.
\end{aligned}$$

luego se obtiene que

$$(p-1)!N_p e^x = p!g_p(x) + (h'(x)+\cdots+h^{(p-1)}(x))+\cdots$$

Ahora bien, como $p>2|u_i|$ se cumple que

$$|1+\frac{u_i}{(j+1)}+\frac{u_i^2}{(j+1)(j+2)}+\cdots| \leq 1+\frac{1}{2}+\frac{1}{2^2}+\cdots=2.$$

Por lo que notamos que

$$|(p-1)!N_p e^{u_i}-p!g_p(u_i)| < 2\sum_{j=p-1}^{r}|b_j|\,|u_i|^j \leq 2|u_i|^{p-1}\left(\sum_{k=0}^{t}|a_j||u_i|^j\right)^p < 2M^p,$$

dividiendo por $(p-1)!$ se concluye el enunciado. □

Teorema 2.51: Si $u_1,\ldots,u_n\in\mathbb{A}$ son números algebraicos distintos, entonces $e^{u_1},\ldots,e^{u_n}$ son $\mathbb{A}$-linealmente independientes.

Demostración: Considere el grupo aditivo $A':=\mathbb{A}$, cuyos elementos denotaremos como a',b',c', etc. para diferenciarlos de los usuales. Su operación es $a'*b'=(a+b)'$, su neutro es el $0'$ y sus inversos $(a')^{-1}=(-a)'$. Ahora considere el álgebra asociada al grupo $\mathbb{A}[A']$ cuyos elementos son sumas formales $\sum_{i=1}^{n} v_i u_i'$, donde la suma es coordenada a coordenada y el producto es

$$(v_1u_1')\cdot(v_2u_2')=v_1v_2(u_1+u_2)'.$$

Nótese que aquí los monomios $u'_1, \ldots, u'_n$ son efectivamente $\mathbb{A}$-linealmente independientes. Ésta manera extraña de entender los elementos recuerda a la propiedad fundamental de la exponencial que dice que $e^{u_1} \cdot e^{u_2} = e^{u_1+u_2}$. De modo que ésto induce el siguiente homomorfismo de $\mathbb{A}$-álgebras:

$$\begin{aligned} \varepsilon\colon \mathbb{A}[A'] &\longrightarrow \mathbb{C} \\ \sum_{i=1}^{n} v_i u'_i &\longmapsto \sum_{i=1}^{n} v_i e^{u_i}, \end{aligned}$$

ahora el enunciado se traduce en comprobar que ε es inyectivo.

En primer lugar, la conmutatividad de A' induce que $\mathbb{A}[A']$ sea una $\mathbb{A}$-álgebra asociativa y conmutativa, veremos que es además un dominio íntegro. Para ello consideramos el orden lexicográfico sobre $\mathbb{C}$:

$$a + b\mathrm{i} \prec c + d\mathrm{i} \iff a < c \vee (a = c \wedge b < d).$$

Es fácil notar que respeta sumas, i.e., si $\alpha \prec \beta$ y $\gamma \prec \delta$, entonces $\alpha + \gamma \prec \beta + \delta$. Luego, un par de elementos $\sum_{i=1}^{n} v_i u'_i$ y $\sum_{j=1}^{m} z_j t'_j$ de $\mathbb{A}[G]$ los podemos escribir con los u_i's y los t_j's en orden creciente, y entonces cuando consideremos el producto notamos que la $\prec$-menor combinación posible es $u_1 + t_1$ la cual tiene coeficiente no nulo.

Sea $\sum_{i=1}^{n} v_i u'_i \in \ker \varepsilon$. Sea $K/\mathbb{Q}$ una extensión finita de Galois tal que $u_i, v_i \in K$ y $G := \mathrm{Gal}(K/\mathbb{Q})$. Consideramos K' el grupo aditivo de K y consideramos la álgebra $K[K']$, la cual es un subanillo de $\mathbb{A}[A']$. Sea $\eta \in G$, nótese que η determina dos automorfismos en $K[K']$:

$$\sigma_\eta\left(\sum_{i=1}^{n} z_i t'_i\right) = \sum_{i=1}^{n} \eta(z_i) t'_i, \qquad \tau_\eta\left(\sum_{i=1}^{n} z_i t'_i\right) = \sum_{i=1}^{n} z_i \big(\eta(t_i)\big)'.$$

Puesto que los η's determinan automorfismos se cumple que si $\sum_{i=1}^{n} z_i t'_i \neq 0$, entonces $\sigma_\eta(\sum_{i=1}^{n} z_i t'_i) \neq 0$. Luego podemos definir:

$$\zeta := \prod_{\eta \in G} \sigma_\eta\left(\sum_{i=1}^{n} v_i u'_i\right) = \prod_{\eta \in G} \sum_{i=1}^{n} \eta(v_i) u'_i \neq 0,$$

como ζ tiene por factor a $\sum_{i=1}^{n} v_i u'_i$, entonces se cumple que $\zeta \in \ker \varepsilon$. Además, por conmutatividad, $\sigma_\eta(\zeta) = \zeta$ para todo $\eta \in G$ lo que significa que los coeficientes de ζ están en $\mathbb{Q}$. Por otro lado, definimos

$$\xi := \prod_{\eta \in G} \tau_\eta(\zeta) \neq 0,$$

el cual también está en $\ker \varepsilon$ y como $\tau_\eta(\xi) = \xi$ para todo $\eta \in G$ se concluye que las indeterminadas están en $\mathbb{Q}$. Escribamos $\xi = \sum_{i=1}^n z_i t_i'$. Nótese que como los coeficientes de ζ están en $\mathbb{Q}$, entonces $z_i \in \mathbb{Q}$. Definiendo $m := |G|$, entonces, promediando se obtiene que

$$\xi = \frac{1}{m} \sum_{\eta \in G} \tau_\eta(\xi) = \sum_{i=1}^n \frac{z_i}{m} \sum_{\eta \in G} \big(\eta(t_i)\big)'.$$

Podemos definir $T'(u) := \sum_{\eta \in G} \big(\eta(u)\big)'$ y renombrar las letras de modo que $\xi = \sum_{i=1}^n z_i T'(t_i)$, donde $z_i \in \mathbb{Q}$, $t_i \in K$ y $T'(t_i) \neq T'(t_j)$ si $i \neq j$ (ésto debido a que la igualdad se alcanza syss son $\mathbb{Q}$-conjugados, en cuyo caso factorizamos los términos necesarios). Nótese que para todo $s, t \in K$ se cumple que:

$$\begin{aligned} T'(s) \cdot T'(t) &= \left(\sum_{\eta \in G} \big(\eta(s)\big)' \right) \cdot \left(\sum_{\rho \in G} \big(\rho(t)\big)' \right) = \sum_{\eta, \rho \in G} \big(\eta(s)\big)' \cdot \big(\rho(t)\big)' \\ &= \sum_{\eta, \rho \in G} \big(\eta(s) + \rho(t)\big)' = \sum_{\rho \in G} \sum_{\eta \in G} \big(\eta(s + \eta^{-1}\rho(t))\big)' \\ &= \sum_{\theta \in G} T'(s + \theta(t)), \end{aligned}$$

donde en la última linea empleamos que $\rho \mapsto \eta^{-1}\rho$ es una biyección en un grupo finito. Ésto nos permite que, tras multiplicar ξ por $T'(-t_1)$ se obtenga una expresión de la forma

$$v_0 + v_1 T'(u_1) + \cdots + v_n T'(u_n) = 0, \tag{2.1}$$

donde, tras limpiar denominadores, podemos suponer que $v_i \in \mathbb{Z}$ y $v_0 \neq 0$.

Como los u_i's son algebraicos podemos suponer que $f(x) \in \mathbb{Z}[x]$ es un polinomio no nulo de grado t tal que se anula en los u_i's (y, por ende, también en sus conjugados); sea p primo y $M > 0$ suficientemente grandes de modo que se satisfagan las hipótesis del lema anterior. Elijamos un entero C tal que Cu_i^j sea un entero algebraico para todo $i \in \{1, \ldots, n\}$ y todo $j \leq t$, luego $C^p g_p(u_i)$ es un entero algebraico para todo i, y $C^p g_p(\eta(u_i))$ también para todo $\eta \in G$.

Considere la fórmula (2.1), aplique el morfismo ε y multiplique por $N_p C^p$:

$$N_p C^p v_0 + N_p C^p \sum_{i=1}^n v_i \cdot \sum_{\eta \in G} e^{\eta(u_i)} = 0.$$

De lo que se sigue que

$$\begin{aligned}\left|N_pC^pv_0 + C^p\sum_{i=1}^{n} v_i \sum_{\eta\in G} pg_p(\eta(u_i))\right| &= \Big|(N_pC^pv_0 - N_pC^pv_0) \\ &\quad + C^p\sum_{i=1}^{n} v_i \sum_{\eta\in G}\left(pg_p(\eta(u_i)) - N_pe^{\eta(u_i)}\right)\Big| \\ &< \frac{2M^pC^pm}{(p-1)!}\sum_{i=1}^{n}|v_i|.\end{aligned}$$

Llamando $L := \sum_{i=1}^{n}|v_i|$ la cual es una constante se concluye que

$$\left|N_pC^pv_0 + C^p\sum_{i=1}^{n} v_i \sum_{\eta\in G} pg_p(\eta(u_i))\right| < \frac{2(MC)^pmL}{(p-1)!},$$

donde los términos a la izquierda son enteros y eligiendo que $p > |N_pv_0|$ vemos que han de ser no nulos; pero eso es absurdo pues el término de la derecha converge a 0. □

Teorema 2.52 – *Teorema de Lindemann-Weierstrass*: Sean

$$u_1, \ldots, u_n \in \mathbb{A}$$

números algebraicos que son $\mathbb{Q}$-linealmente independientes. Entonces $e^{u_1}, \ldots, e^{u_n}$ son $\mathbb{A}$-algebraicamente independientes.

Demostración: Sean $(k_1, \ldots, k_n)$ y $(l_1, \ldots, l_n)$ dos sucesiones distintas de naturales; entonces por $\mathbb{Q}$-independencia lineal se tiene que $\sum_{i=1}^{n} k_iu_i$ y $\sum_{i=1}^{n} l_iu_i$ son números algebraicos distintos, y luego por el teorema anterior se cumple que $(e^{u_1})^{k_1}\cdots(e^{u_n})^{k_n} = e^{\sum_{i=1}^{n} k_iu_i}$ y $e^{\sum_{i=1}^{n} l_iu_i}$ son $\mathbb{A}$-algebraicamente independientes, de modo que es fácil comprobar que todo polinomio no nulo con coeficientes en $\mathbb{A}$ evaluado en las exponenciales nunca se anula. □

Corolario 2.52.1: e y π son números trascendentes.

Notas históricas

La noción de *dependencia íntegra* se debe a Noether **[33]** (1927). Los teoremas del ascenso y del descenso fueron originalmente probados por Krull **[26]**

(1937), pero popularizados y generalizados por el artículo [**14**] (1946) de los estadounidenses **Irvin Sol Cohen** (1917-1955) y **Abraham Seidenberg** (1916-1988), ambos estudiantes doctorales de Oscar Zariski.

El teorema de normalización de Noether fue demostrado en Noether [**32**] (1926) cuando el cuerpo base es infinito, y fue generalizado a cuerpos arbitrarios en Zariski [**38**] (1943). Las generalizaciones adicionales fueron un aporte de M. Nagata en [**29**] y [**30**].

La terminología *anillo japonés* y *universalmente japonés* es originaria de Grothendieck y Dieudonné [**EGA IV$_1$,** págs. 309-310], §0.23; y evidentemente es un tributo a los trabajos de la escuela nipona liderada por Nagata. Se llama un *anillo de Nagata* A a un anillo cuyos cocientes por primos $A/\mathfrak{p}$ sean japoneses; Matsumura [**5**] señala que los términos «anillos de Nagata» y «universalmente japonés» coinciden, pero no es así, ya que, como bien señala Matsumura, ser de Nagata equivale a que toda A-álgebra íntegra finitamente generada (como A-módulo) sea japonés, pero no necesariamente toda A-álgebra íntegra de tipo finito. Nagata [**6**] emplea el término *anillo pseudo-geométrico* para los anillos de Nagata.

El teorema de Lindemann-Weierstrass lo incluímos aquí para dar una breve y linda aplicación de la teoría. El francés **Charles Hermite** (1822-1901) originalmente demostró en [**21**] (1873) que e^u es trascendente cuando $u \neq 0$ es un entero, luego el alemán **Ferdinand von Lindemann** (1852-1939) demostró en [**35**] y [**36**] (1882) que e^u es trascendente si $u \neq 0$ es un número algebraico; y finalmente en [**37**] (1885), el alemán **Karl Weierstrass** (1815-1897) mejoró el resultado al que nosotros enunciamos aquí, aunque su demostración estaba fuertemente inspirada por el trabajo de Lindemann. Las demostraciones han sido arduamente simplificadas desde entonces, la equivalencia empleada es originaria de Alan Baker.

3

Planitud y criterios

La planitud es uno de los conceptos fundamentales en el álgebra conmutativa y la geometría algebraica. En éste capítulo comenzaremos a enfatizar también la intuición geométrica, empleando lenguaje de esquemas para ciertos comentarios.

3.1 Planitud y módulos de presentación finita

Definición 3.1: Un A-módulo M se dice ***de presentación finita*** si posee una presentación libre de la forma

$$A^n \longrightarrow A^m \longrightarrow M \xrightarrow{\psi} 0 \tag{3.1}$$

Observación 3.1.1: Un anillo es noetheriano syss todo módulo finitamente generado es de presentación finita.

Intuitivamente, de la observación anterior se obtiene el siguiente eslógan:

> *Toda propiedad válida para módulos finitamente generados sobre un anillo noetheriano es válida, en mayor generalidad, para módulos de presentación finita sobre anillos.*

Esto no siempre es cierto, pero es la idea central detrás del método de *aproximación noetheriana.*

Proposición 3.2: Sea $0 \to M_1 \to M_2 \to M_3 \to 0$ una sucesión exacta de A-módulos. Se cumplen:

1. Si M_3 es de presentación finita y M_2 es finitamente generado, entonces M_1 es finitamente generado. En consecuencia, si M es de presentación finita, entonces todo epimorfismo $\alpha\colon A^n \to M$ tiene núcleo finitamente generado.

2. Si M_2 es de presentación finita y M_1 es finitamente generado, entonces M_3 es de presentación finita.

3. Si M_1 y M_3 son de presentación finita, entonces M_2 también lo es.

Demostración:

1. Sea $A^n \to A^m \to M_3 \to 0$ una presentación, entonces como el módulo libre A^n es proyectivo construimos el siguiente diagrama conmutativo con filas exactas:

$$\begin{array}{ccccccccc} & & A^n & \longrightarrow & A^m & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \vdots & & \downarrow & & \| & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$$

   y gracias al lema de la serpiente concluimos que

$$\operatorname{coker}(A^n \to M_1) \cong \operatorname{coker}(A^m \to M_2),$$

   como el módulo de la derecha es finitamente generado, por lo que el de la izquierda también lo es.

2. Sea $A^n \to A^m \to M_2 \to 0$ una presentación y sea $A^r \twoheadrightarrow M_1$ un epimorfismo. Como A^r es un módulo proyectivo, podemos factorizar $A^r \to A^m \to M_2$ la composición $A^r \twoheadrightarrow M_1 \twoheadrightarrow M_2$, de modo que $A^{r+n} \to A^m \to M_3 \to 0$ es una presentación.

3. Sean $A^n \twoheadrightarrow M_1$ y $A^m \twoheadrightarrow M_3$ epimorfismos, de modo que podemos formar el siguiente diagrama conmutativo con filas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^n & \longrightarrow & A^{n+m} & \longrightarrow & A^m & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$$

lo que induce, mediante el lema de la serpiente, la sucesión exacta $0 \to \ker\alpha \to \ker\beta \to \ker\gamma \to 0$. Como M_1 y M_3 son de presentación finita, entonces $\ker\alpha$ y $\ker\gamma$ son finitamente generados, por lo que $\ker\beta$ también lo es. También por el lema de la serpiente, β es un epimorfismo. □

La noción de «módulo de presentación finita» tiene una interpretación como «objeto compacto» dentro de la categoría de módulos, por lo que obligatoriamente viene de la mano con la noción categorial de «diagrama filtrado». El siguiente ejemplo será útil:

Ejemplo 3.3: Sea M un A-módulo arbitrario. Considere I la familia de subgrupos finitamente generados de M con el orden parcial dado por la inclusión; esta familia es dirigida puesto que si $S, T \leq M$ son finitamente generados entonces $S + T \leq M$ también. Para $S \leq T \in I$ podemos considerar el homomorfismo inclusión $S \hookrightarrow T$ y con ello vemos que $(S)_{S\in I}$ es un diagrama filtrado de módulos con $\varinjlim_{S\in I} S = M$.

Otro diagrama filtrado opuesto en cierto modo es que dado $S \leq T \in I$ podemos considerar la reducción módulo T en $M/S \twoheadrightarrow (M/S)/(T/S) \cong M/T$ y con ello vemos que $(M/S)_{S\in I}$ forma un diagrama filtrado con $\varinjlim_{S\in I} M/S = 0$. ⌟

Lema 3.4: Para un A-módulo M son equivalentes:

1. M es finitamente generado.
2. Para todo límite filtrado de A-módulos $N = \varinjlim_{i\in I} N_i$, el homomorfismo natural
$$\varinjlim_{i\in I} \operatorname{Hom}_A(M, N_i) \longrightarrow \operatorname{Hom}_A(M, N)$$
es inyectivo.

Demostración: 1 $\implies$ 2. Sea $u_1, \ldots, u_n \in M$ un sistema generador y sea $\varphi\colon M \to N_i$ un homomorfismo tal que al componer con $\pi_i\colon N_i \to N$ se anula. Al evaluar $\pi_i\varphi(u_j) = 0$, entonces necesariamente existe $\ell := \ell_j \geq i$ con $\pi^i_\ell\colon N_i \to N_\ell$ tal que $\pi^i_\ell\varphi(u_j) = 0$. Como hay finitos u_i's podemos escoger $\ell \geq i$ tal que $\pi^i_\ell\varphi(u_j) = 0$ para cada j y, por tanto, $\varphi \circ \pi^i_\ell = 0$.

2 $\implies$ 1. Podemos construir el siguiente diagrama filtrado del ejemplo **??** y obtener que $\varinjlim_S \operatorname{Hom}_A(M, M/S) \cong 0$, donde S recorre los subgrupos finitamente generados de M. Si consideramos el conjunto de flechas $M \to M/S$ dadas por la reducción módulo S, obtenemos que necesariamente $M \to M/S$ se anula para algún S, es decir, $M = S$ es finitamente generado. □

Teorema 3.5: Sea M un A-módulo. Entonces M es de presentación finita syss el funtor $\mathrm{Hom}_A(M,-)$ preserva límites filtrados.

Demostración: $\Longrightarrow$. Sea $A^n \to A^m \to M \to 0$ una presentación finita y sea $N = \varinjlim_i N_i$ un límite filtrado de A-módulos. Basta emplear que $\mathrm{Hom}_A(P,-)$ es exacto por la derecha para todo A-módulo X y que $\mathrm{Hom}_A(N, A^r) \cong N^r$ para todo $r \geq 0$ finito, de modo que construimos el siguiente diagrama conmutativo con filas exactas:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \varinjlim_i \mathrm{Hom}_A(M,N_i) & \longrightarrow & \varinjlim_i \mathrm{Hom}_A(A^m,N_i) & \longrightarrow & \varinjlim_i \mathrm{Hom}_A(A^n,N_i) \\
 & & \downarrow{\scriptstyle \exists!} & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \wr} \\
0 & \longrightarrow & \mathrm{Hom}_A(M,N) & \longrightarrow & \mathrm{Hom}_A(A^m,N) & \longrightarrow & \mathrm{Hom}_A(A^n,N)
\end{array}$$

Así, deducimos que la flecha restante es un isomorfismo por el lema de los cinco.

$\Longleftarrow$. Nótese que siempre podemos construir $M = \varinjlim_i M_i$, donde los M_i's recorren los submódulos de presentación finita de M con las inclusiones. Así, tomando $\mathrm{Id}_M \in \mathrm{Hom}_A(M,M)$ vemos que existe i tal que se factoriza $M \hookrightarrow M_i \hookrightarrow M$, por lo que $M = M_i$ es de presentación finita. □

Recuérdese que dada una sucesión exacta de A-módulos $\mathscr{S}\colon 0 \to M_1 \to M_2 \to M_3 \to 0$ y dado un A-módulo N arbitrario, tenemos que la siguiente sucesión

$$M_1 \otimes_A N \xrightarrow{\alpha} M_2 \otimes_A N \longrightarrow M_3 \otimes_A N \longrightarrow 0$$

es exacta; no obstante, $\mathscr{S} \otimes_A N$ no es exacta en general (equivalentemente, α no suele ser inyectivo).

Se dice que N es un A-módulo ***plano*** (resp. ***fielmente plano***) si $\mathscr{S} \otimes_A N$ es exacto cuando (resp. syss) $\mathscr{S}$ es exacto. Se dice que un homomorfismo de anillos $\varphi\colon A \to B$ es ***plano*** (resp. ***fielmente plano***) si B es un A-módulo plano (resp. fielmente plano).

Teorema 3.6: Sea M un módulo sobre un anillo A. Son equivalentes:

1. M es plano.
2. Para toda sucesión exacta $0 \to N_1 \to N_2$ se cumple que $0 \to N_1 \otimes_A M \to N_2 \otimes_A M$ es exacto.
3. $\mathrm{Tor}_1^A(M,N) = 0$ para todo A-módulo N finitamente generado.

4. $\operatorname{Tor}_1^A(M, A/\mathfrak{a}) = 0$ para todo ideal finitamente generado $\mathfrak{a} \trianglelefteq A$.

4′ Para todo ideal finitamente generado $\mathfrak{a} \trianglelefteq A$ se cumple que $\mathfrak{a} \otimes_A M \cong \mathfrak{a}M$.

5. **Ecuaciones de planitud:** Para toda ecuación $\sum_{i=1}^n a_i u_i = 0$, donde $a_i \in A, u_i \in M$, existen $v_j \in M$ y $b_{ij} \in A$ tales que

$$\sum_{j=1}^m b_{ij} v_j = u_i, \qquad \sum_{i=1}^n a_i b_{ij} = 0.$$

Demostración: $1 \iff 2 \implies 3 + 4$. Trivial.

$3 \implies 2$. Nótese que para verificar que $0 \to N_1 \otimes_A M \xrightarrow{\alpha} N_2 \otimes_A M$ es exacto, hay que verificar que dado un tensor

$$w := \sum_{i=1}^r n_i \otimes m_i \in N_1 \otimes_A M, \qquad n_i \in N_1, m_i \in M$$

tal que $w \neq 0$ se cumple que $\alpha(w) \neq 0$. Definiendo $S := \langle n_1, \ldots, n_r \rangle$ y denotando por $\iota \colon S \hookrightarrow N_2$ a la inclusión, notamos que $\alpha|_{S \otimes_A M} = \iota \otimes_A \operatorname{Id}_M$, por lo que $w \in \ker \alpha$ syss $w \in \ker(\iota \otimes_A \operatorname{Id}_M)$.

$4 \implies 3$. Por hipótesis sabemos que la sucesión $0 \to M \otimes_A \mathfrak{a} \to M$ es exacta para todo $\mathfrak{a} \trianglelefteq A$. Sea $0 \to N \to N'$ una sucesión exacta, donde N es finitamente generado. Entonces existe una cadena de A-submódulos

$$0 =: N_0 \subset N_1 \subset \cdots \subset N_m := N,$$

donde cada $N_{j+1}/N_j = A/a_j A$ para algún $a_j \in A$ (es decir, cada N_{j+1} se obtiene por añadir un elemento a N_j).

Vamos a ver que $\operatorname{Tor}_1^A(M, N_j) = 0$ por inducción sobre j, donde es claro para el caso base $j = 0$. De la sucesión exacta $0 \to N_j \to N_{j+1} \to N_{j+1}/N_j \to 0$ se induce la sucesión exacta

$$0 = \operatorname{Tor}_1^A(M, N_j) \longrightarrow \operatorname{Tor}_1^A(M, N_{j+1}) \longrightarrow \operatorname{Tor}_1^A(M, N_{j+1}/N_j) == 0,$$

como se quería probar.

$1 \implies 5$. Fijemos la ecuación dada, y considere el homomorfismo

$$\begin{aligned} \varphi \colon A^n &\longrightarrow A \\ (x_1, \ldots, x_n) &\longmapsto \sum_{i=1}^n a_i x_i, \end{aligned}$$

y sea $K := \ker\varphi$. Tensorizando por M tenemos $0 \longrightarrow K \otimes_A M \longrightarrow M^n \xrightarrow{\varphi_M} M$. La condición del enunciado se traduce en que $(u_1, \ldots, u_n) \in \ker(\varphi_M) = K \otimes_A M$, es decir

$$(u_1, \ldots, u_n) = \sum_{j=1}^{m} \beta_j \otimes v_j, \qquad \beta_j \in K, v_j \in M.$$

Así cada $\beta_j = (b_{1j}, \ldots, b_{nj})$ y obtenemos el enunciado.

5 $\implies$ 4. Nótese que probar que $\mathrm{Tor}_1^A(M, A/\mathfrak{a}) = 0$ equivale a que $\mathfrak{a} \otimes_A M \cong \mathfrak{a}M$. Claramente tenemos un epimorfismo $\mathfrak{a} \otimes_A M \twoheadrightarrow \mathfrak{a}M$, veamos que es inyectivo: Sean $a_1, \ldots, a_n \in \mathfrak{a} \trianglelefteq A$ y sean $u_1, \ldots, u_n \in M$ tales que $\sum_{i=1}^n a_i u_i = 0 \in M$. Entonces, por hipótesis, existen $b_{ij} \in \mathfrak{a}, v_j \in M$ tales que $\sum_{i=1}^n a_i b_{ij} = 0$ y $\sum_{j=1}^m b_{ij} v_j = u_i$, luego

$$\sum_{i=1}^{n} (a_i \otimes u_i) = \sum_{i=1}^{n} \sum_{j=1}^{m} (a_i \otimes b_{ij} v_j) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_i b_{ij} \right) \otimes v_j = 0. \qquad \square$$

Proposición 3.7: Sea B una A-álgebra y M un B-módulo. Entonces:

1. Si B es (fielmente) plano sobre A y M es (fielmente) plano sobre B, entonces M es (fielmente) plano sobre A.

2. Si M es fielmente plano sobre B y (fielmente) plano sobre A, entonces B es (fielmente) plano sobre A.

3. Si M es (fielmente) plano sobre A, entonces $M \otimes_A B$ es (fielmente) plano sobre B.

Demostración: Para las dos primeras basta saber que para todo A-módulo N se cumple:

$$(N \otimes_A B) \otimes_B M = N \otimes_A (B \otimes_B M) = N \otimes_A M.$$

Para la tercera basta notar que $N \otimes_B (B \otimes_A M) = N \otimes_A M$. $\square$

Definición 3.8: Sea B una A-álgebra y N un A-módulo. Al B-módulo $N \otimes_A B$ se le dice la ***extensión de escalares*** de N en B.

Éstas proposiciones suelen llamarse «cambio de base». Veamos un resultado más fuerte:

Teorema 3.9: Sea B una A-álgebra y M un B-módulo. Son equivalentes:

1. M es plano sobre A.
2. $M_{\mathfrak{q}}$ es plano sobre $A_{\mathfrak{p}}$ para todo $\mathfrak{q} \lhd B$ primo, donde $\mathfrak{p} := \mathfrak{q}^c = \mathfrak{q} \cap A$.
3. $M_{\mathfrak{n}}$ es plano sobre $A_{\mathfrak{m}}$ para todo $\mathfrak{n} \lhd B$ maximal, donde $\mathfrak{m} := \mathfrak{n}^c$.

Demostración: 1 $\implies$ 2. Si $S \subseteq A$ es un sistema multiplicativo y M, N son $S^{-1}A$-módulos, entonces $M \otimes_{S^{-1}A} N = M \otimes_A N$ puesto que

$$\frac{a}{s}\boldsymbol{m} \otimes \boldsymbol{n} = \frac{a}{s}\boldsymbol{m} \otimes \frac{s}{s}\boldsymbol{n} = \frac{s}{s}\boldsymbol{m} \otimes \frac{a}{s}\boldsymbol{n} = \boldsymbol{m} \otimes \frac{a}{s}\boldsymbol{n},$$

para todo $\boldsymbol{m} \in M, \boldsymbol{n} \in N, \frac{a}{s} \in S^{-1}A$. $B_{\mathfrak{q}}$ es una $A_{\mathfrak{p}}$-álgebra de forma canónica, de modo que $M_{\mathfrak{q}}$ es un $A_{\mathfrak{p}}$-módulo. Sea

$$\mathscr{S}\colon 0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

una sucesión exacta corta de B-módulos, luego $\mathscr{S} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{q}} = \mathscr{S} \otimes_A M_{\mathfrak{q}} = (\mathscr{S} \otimes_A M) \otimes_B B_{\mathfrak{q}}$ por extensión de escalares. Como M es plano sobre A, entonces $\mathscr{S} \otimes_A M$ es exacto y, como $B_{\mathfrak{q}}$ es plano sobre B (corolario A.2.1), entonces $(\mathscr{S} \otimes_A M) \otimes_B B_{\mathfrak{q}}$ es plano.

2 $\implies$ 3. Trivial.

3 $\implies$ 1. Basta ver que $- \otimes_A M$ es exacto por la izquierda. Sea $0 \to N \to N'$ una sucesión exacta de A-módulos, y sea K el núcleo de la tensorización por M de modo que

$$0 \longrightarrow K \longrightarrow N \otimes_A M \longrightarrow N' \otimes_A M$$

es exacta. Luego, localizamos todos los módulos en $\mathfrak{n} \lhd B$ maximal:

$$0 \longrightarrow K_{\mathfrak{n}} \longrightarrow N \otimes_A M_{\mathfrak{n}} \longrightarrow N' \otimes_A M_{\mathfrak{n}}.$$

Ahora bien, por extensión de escalares, $N \otimes_A M_{\mathfrak{n}} = N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{n}}$, donde localizar por $\mathfrak{m}$ es exacto y $- \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{n}}$ también es exacto, de modo que $K_{\mathfrak{n}} = 0$ para todo $\mathfrak{n} \lhd B$ maximal y concluimos por la proposición A.2. □

Teorema 3.10: Sea A un dominio y M un A-módulo. Son equivalentes:

1. M es fielmente plano (sobre A).
2. M es plano y $M \otimes_A N \neq 0$ para todo A-módulo $N \neq 0$.
3. M es plano y $\mathfrak{m}M \neq M$ para todo $\mathfrak{m} \lhd A$ maximal.

Demostración: $1 \implies 2$. Considere la sucesion $\mathscr{S}\colon 0 \to N \to 0$. Si $M \otimes_A N = 0$, entonces $\mathscr{S} \otimes_A M$ es exacta, luego como $- \otimes_A M$ refleja exactitud concluimos que $\mathscr{S}$ también es exacta y $N = 0$.

$2 \implies 3$. Sea $N = A/\mathfrak{m} \neq 0$. Nótese que $M \otimes_A A/\mathfrak{m} = M/\mathfrak{m}M \neq 0$ luego $M \neq \mathfrak{m}M$.

$3 \implies 2$. Si $N \neq 0$, sea $\boldsymbol{u} \in N_{\neq 0}$, luego $A \cdot \boldsymbol{u} \cong A/\operatorname{Ann}(\boldsymbol{u})$. Sea $\mathfrak{m} \supseteq \operatorname{Ann}(\boldsymbol{u})$ por el teorema de Krull, luego $M \supset \mathfrak{m}M \supseteq \operatorname{Ann}(\boldsymbol{u})M$ y, por tanto, $M \otimes_A A \cdot \boldsymbol{u} \neq 0$. Como M es plano y $0 \to A\boldsymbol{u} \to N$ es exacto, entonces $0 \to A\boldsymbol{u} \otimes_A M \to N \otimes_A M$ es exacto y $N \otimes_A M \neq 0$.

$2 \implies 1$. Sea $\mathscr{S}\colon N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3$ una sucesión y

$$\mathscr{S} \otimes_A M\colon \qquad N_1 \otimes_A M \xrightarrow{f_M} N_2 \otimes_A M \xrightarrow{g_M} N_3 \otimes_A M$$

es exacta. En primer lugar, nótese que $(f \circ g)_M = 0$, de modo que $\operatorname{Img}(f \circ g) \otimes M = \operatorname{Img}(f_M \circ g_M) = 0$ por lo que $f \circ g = 0$. Luego sea $H := \ker g / \operatorname{Img} f$, nótese que $H \otimes M = \ker(g_M)/\operatorname{Img}(f_M) = 0$ luego $H = 0$ y finalmente $\mathscr{S}$ es exacta. □

Definición 3.11: Sea M un A-módulo, definimos su ***dual*** como $M^\vee := \operatorname{Hom}_A(M, A)$. Dado otro A-módulo N, definimos el siguiente homomorfismo:

$$\begin{aligned} \Phi_{M,N}\colon N \otimes_A M^\vee &\longrightarrow \operatorname{Hom}_A(M, N) \\ n \otimes \varphi &\longmapsto (m \mapsto \varphi(m)n). \end{aligned}$$

Proposición 3.12: Sea P un A-módulo plano. Para todo A-módulo de presentación finita M el homomorfismo $\Phi_{M,P}\colon P \otimes_A M^\vee \to \operatorname{Hom}_A(M, P)$ es un isomorfismo.

Demostración: Sea $F = A^n$ un A-módulo libre finitamente generado. Entonces para todo A-módulo N en general obtenemos que

$$\operatorname{Hom}_A(F, N) = \operatorname{Hom}_A(A^{\oplus n}, N) \cong \operatorname{Hom}_A(A, N)^n \cong N^n \cong N \otimes_A F.$$

En particular, esto prueba con $N = A$ que $F^\vee \cong F$ y uno puede verificar (¡hágalo!) que esto establece que $\Phi_{F,N}$ sea un isomorfismo en general.

Sea M con presentación $A^n \to A^m \to M \to 0$, entonces por contravarianza induce el siguiente diagrama conmutativo con filas exactas:

$$\begin{array}{ccccccc} 0 & \longrightarrow & P \otimes_A M^\vee & \longrightarrow & P \otimes_A (A^n)^\vee & \longrightarrow & P \otimes_A (A^m)^\vee \\ & & \vdots\!\downarrow \exists! & & \downarrow \wr & & \downarrow \wr \\ 0 & \longrightarrow & \operatorname{Hom}_A(M, P) & \longrightarrow & \operatorname{Hom}_A(A^n, P) & \longrightarrow & \operatorname{Hom}_A(A^m, P) \end{array}$$

Así concluimos por el lema de los cinco que $\Phi_{M,P}$ también es un isomorfismo. □

La proposición anterior es cierta, en mayor generalidad, cuando A no es conmutativo y donde M, P son módulos por el mismo lado (quizá cambiando $P \otimes M^\vee$ por $M^\vee \otimes P$).

Adaptando la misma demostración de antes se obtiene lo siguiente:

Proposición 3.13: Sea A un anillo y B una A-álgebra plana. Para todo par de A-módulos M, N con M de presentación finita se satisface que

$$\mathrm{Hom}_A(M, N) \otimes_A B \cong \mathrm{Hom}_B(M \otimes_A B, N \otimes_A B).$$

Corolario 3.13.1: Sea A un anillo, $\mathfrak{p} \in \mathrm{Spec}\, A$ un primo y M, N un par de A-módulos con M de presentación finita. Entonces:

$$\mathrm{Hom}_A(M, N) \otimes_A A_\mathfrak{p} \cong \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}).$$

Teorema 3.14: Sea $(A, \mathfrak{m}, k)$ un dominio local y sea M un A-módulo. Si $\mathfrak{m}$ es nilpotente o M es finitamente generado, entonces M es libre syss es proyectivo syss es plano.

Demostración: Ya sabemos que en general:

$$\text{libre} \implies \text{proyectivo} \implies \text{plano},$$

veamos plano $\implies$ libre: para ello veremos que una base minimal $[v_1], \ldots, [v_n] \in \overline{M} = M/\mathfrak{m}M$ (de elementos k-linealmente independientes) es una base (es decir, son A-linealmente independientes). Emplearemos inducción sobre n.

Para $n = 1$, vemos que $av_1 = 0$, luego existen $b_1, \ldots, b_r \in A$ y $w_1, \ldots, w_r \in M$ tales que $v_1 = \sum_{j=1}^r b_j w_j$ con $ab_j = 0$ para todo j por las ecuaciones de planitud. Proyectando y recordando que $0 \neq [v_1] = \sum_{j=1}^r [b_j]\,[w_j]$ es base, tenemos que $[b_j] \neq 0$ para algún j, por lo que $b_j \notin \mathfrak{m}$ y, por tanto, es invertible; y como $ab_j = 0$ se cumple que $a = 0$.

Si se satisface para $n > 1$ con $\sum_{i=1}^n a_i v_i = 0$ entonces existen $b_{ij} \in A$ y $w_1, \ldots, w_r \in M$ tales que $v_i = \sum_{j=1}^r b_{ij} w_j$ con $\sum_{i=1}^n a_i b_{ij} = 0$. Nuevamente elegimos $[b_{ij}] \neq 0$ el cual es invertible y, reordenando para que $i = n$:

$$a_n = \frac{-1}{b_{nj}} \sum_{i=1}^{n-1} a_i b_{ij},$$

con $c_i := -b_{ij}/b_{nj}$ tenemos que

$$0 = \sum_{i=1}^{n} a_i v_i = a_1(v_1 + c_1 v_n) + a_2(v_2 + c_2 v_n) + \cdots + a_{n-1}(v_{n-1} + c_{n-1} v_n).$$

Como los $v_i + c_i v_n$ son k-linealmente independientes para $1 \leq i < n$, luego son A-linealmente independientes por hipótesis. □

Teorema 3.15: Sea B una A-álgebra plana. Entonces se satisface el teorema de descenso de Cohen-Seidenberg para la extensión de anillos B/A.

3.2 Planitud local

Teorema 3.16: Sea A un anillo, B una A-álgebra noetheriana, M un B-módulo finitamente generado y $\mathfrak{b} \subseteq \mathfrak{J}(B)$ un ideal. Denotando $M_n := M/\mathfrak{b}^{n+1}M$, si cada M_n es un A-módulo plano, entonces M es plano sobre A.

Demostración: Sea $\mathfrak{a} \trianglelefteq A$ un ideal finitamente generado, queremos ver que $\mu\colon \mathfrak{a} \otimes_A M \to M$ es inyectivo. Sea $M' := \mathfrak{a} \otimes_A M$, entonces es un B-módulo finitamente generado (¿por qué?) y, por tanto, es Hausdorff en la topología $\mathfrak{b}$-ádica (teorema de intersecciones de Krull). Para todo $n \geq 0$ definiendo $M'_n := M'/\mathfrak{b}^{n+1}M' = \mathfrak{a} \otimes_A M_n$ y, por tanto, el homomorfismo inducido por cambio de base $M'_n \hookrightarrow M_n$ es inyectivo. Así pues, para cada n tenemos un diagrama conmutativo:

$$\begin{array}{ccc} M' & \xrightarrow{\mu} & M \\ \downarrow & & \downarrow \\ M'_n & \hookrightarrow & M_n \end{array}$$

Si $v \in \ker \mu$, por conmutatividad, tenemos que $v \in \mathfrak{b}^{n+1}M'$ para cada n, y por la propiedad de Hausdorff, necesariamente $v = 0$. □

Definición 3.17: Sea A un anillo y $\mathfrak{a} \trianglelefteq A$ un ideal. Se dice que un A-módulo M es ***$\mathfrak{a}$-ádicamente ideal-separado*** si para todo ideal finitamente generado $\mathfrak{b} \trianglelefteq A$ el tensor $\mathfrak{b} \otimes_A M$ es $\mathfrak{a}$-ádicamente separado.

Observación 3.17.1: Si M es $\mathfrak{a}$-ádicamente separado, entonces también es $\mathfrak{a}$-ádicamente ideal-separado (¿por qué?).

3.3 Planitud genérica y conjuntos abiertos

Uno de los usos más interesantes del concepto de planitud concierne las *fibras* de un morfismo. En lenguaje de anillos, si $\mathfrak{p} \in \operatorname{Spec} A$ es un ideal primo (visto como un punto del espectro), entonces uno puede mirar el cuerpo de restos

$$\Bbbk(\mathfrak{p}) := \operatorname{Frac}(A/\mathfrak{p}) \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}.$$

Si $\varphi\colon A \to B$ es un homomorfismo de anillos, y miramos el morfismo inducido en esquemas afines $f := \varphi^a\colon \operatorname{Spec} B \to \operatorname{Spec} A$, entonces la ***fibra*** de f en el punto $\mathfrak{p} \in \operatorname{Spec} A$ es el anillo $B \otimes_A \Bbbk(\mathfrak{p})$, generalmente visto como $\Bbbk(\mathfrak{p})$-álgebra.

Esta es la definición real y esquemática de fibra, pero como podemos notar, realmente podemos dar la definición sin tener que pasar por esquemas. Damos este comentario para motivar un poco el estudio de $B \otimes_A \Bbbk(\mathfrak{p})$.

Teorema 3.18: Sea $\varphi\colon A \to B$ un homomorfismo de anillos y sea M un B-módulo finitamente generado. Son equivalentes:

1. $M = 0$.
2. $M \otimes_A \Bbbk(\mathfrak{p}) = 0$ para todo $\mathfrak{p} \in \operatorname{Spec} A$.

Si además M es finitamente generado sobre A, entonces son equivalentes a:

3. $M \otimes_A \Bbbk(\mathfrak{m}) = 0$ para todo $\mathfrak{m} \in \operatorname{mSpec} A$.

Demostración: Claramente $1 \implies 2 \implies 3$ en general.

$2 \implies 1$. Por contrarrecíproca, si $M \neq 0$, entonces existe algún $\mathfrak{q} \in \operatorname{Spec} B$ tal que $M_{\mathfrak{q}} \neq 0$. Luego, por el lema de Nakayama, obtenemos que $M \otimes_B \Bbbk(\mathfrak{q}) = M_{\mathfrak{q}}/\mathfrak{q}M_{\mathfrak{q}} \neq 0$. Sea $\mathfrak{p} := \mathfrak{q} \cap A \in \operatorname{Spec} A$, como $\mathfrak{p}M_{\mathfrak{q}} \subseteq \mathfrak{q}M_{\mathfrak{q}}$, entonces vemos que $M_{\mathfrak{q}}/\mathfrak{p}M_{\mathfrak{q}} \neq 0$. Sean $T := B \setminus \mathfrak{q}, S := A \setminus \mathfrak{p}$, los cuales son sistemas multiplicativos y la localización (vista como A-módulo) es por definición $M[S^{-1}] = M_{\mathfrak{p}}$. Como $\varphi[S] \subseteq T$, sobre B tenemos que

$$M_{\mathfrak{q}} := M[T^{-1}] = M[S^{-1}][T^{-1}] = M_{\mathfrak{p}}[T^{-1}],$$

de modo que

$$M_{\mathfrak{q}}/\mathfrak{p}M_{\mathfrak{q}} = (M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}})[T^{-1}] = (M \otimes_A \Bbbk(\mathfrak{p}))[T^{-1}],$$

por lo que $M \otimes_A \Bbbk(\mathfrak{p}) \neq 0$.

$3 \implies 1$. Esto es el lema de Nakayama. □

Teorema 3.19: Sea M un A-módulo finitamente generado. Entonces:

1. Para todo $r \geq 0$, el conjunto

$$U_r := \{\mathfrak{p} \in \operatorname{Spec} A : M_{\mathfrak{p}} \text{ está generado por } \leq r \text{ elementos de } A_{\mathfrak{p}}\}$$

es abierto en $\operatorname{Spec} A$.

2. Si M es de presentación finita (e.g., si M es finitamente generado y A es noetheriano), entonces el conjunto

$$U_L := \{\mathfrak{p} \in \operatorname{Spec} A : M_{\mathfrak{p}} \text{ es un módulo libre sobre } A_{\mathfrak{p}}\}$$

es abierto en $\operatorname{Spec} A$.

Demostración:

1. Supongamos que $\mathfrak{p} \in U_r$, vale decir, que $M_{\mathfrak{p}} = \sum_{i=1}^{r} u_i A_{\mathfrak{p}}$ para algunos $u_i = m_i/b_i \in M_{\mathfrak{p}}$, donde cada $m_i \in M, b_i \in A \setminus \mathfrak{p}$. Como los b_i's son inversibles en $A_{\mathfrak{p}}$, podemos reemplazar los u_i's por m_i's y suponer que todos los generadores yacen en (la imagen de) M. Definamos el homomorfismo de A-módulos

$$\psi := \operatorname{ev}_{\boldsymbol{m}} \colon A^r \to M, \qquad (a_1, \ldots, a_r) \mapsto \sum_{i=1}^{r} a_i m_i,$$

y sea $N := \operatorname{coker} \psi = M/\operatorname{Img} \psi$. Localizando la sucesión exacta $A^r \to M \to N \to 0$, obtenemos

$$A_{\mathfrak{q}}^r \xrightarrow{\psi \otimes_A A_{\mathfrak{q}}} M_{\mathfrak{q}} \longrightarrow N_{\mathfrak{q}} \longrightarrow 0.$$

Y sabemos que para $\mathfrak{q} = \mathfrak{p}$ obtenemos que $N_{\mathfrak{p}} = 0$. Como N es un cociente de M, es finitamente generado y luego $\operatorname{Supp} N$ es un cerrado que no contiene a $\mathfrak{p}$, es decir, que existe un entorno V de $\mathfrak{p}$ tal que para todo $\mathfrak{q} \in V$ vemos que $N_{\mathfrak{q}} = 0$; o en otras palabras, que $V \subseteq U_r$ y, por tanto, U_r es abierto.

2. Sea $\mathfrak{p} \in U_L$, y sea $u_1, \ldots, u_n$ una $A_{\mathfrak{p}}$-base de $M_{\mathfrak{p}}$. Limpiando denominadores podemos suponer que cada $u_i \in M$. Más aún, por el inciso anterior, existe un entorno $\mathfrak{p} \in \mathbf{D}(f)$ tal que para todo $\mathfrak{q} \in \mathbf{D}(f)$ tenemos que $M_{\mathfrak{q}}$ está generado por los u_i's. Así, sustituyendo A, M por

$A[1/f], M[1/f]$ podemos suponer que $M_{\mathfrak{q}}$ está generado por los u_i's para todo primo $\mathfrak{q} \in \operatorname{Spec} A$. Luego $M/\sum_{i=1}^{r} u_i A = 0$ (teorema A.2).

Definiendo $\psi := \mathrm{ev}_{\boldsymbol{u}} \colon A^r \to M$ como antes, y definiendo $K := \ker \psi$ (el cual es finitamente generado) entonces tenemos que $K_{\mathfrak{p}} = 0$ para el $\mathfrak{p} \in U_L$, así que empleando el enunciado con $r = 0$, vemos que $K_{\mathfrak{q}} = 0$ para todo $\mathfrak{q}$ en un entorno V de $\mathfrak{p}$; o equivalentemente, $A_{\mathfrak{q}}^r \cong M_{\mathfrak{q}}$ para todo $\mathfrak{q} \in V$. □

El inciso 2 es una forma de *libertad* o *planitud genérica*, con la única deficiencia que deja espacio para que el conjunto U_L sea vacío. Procedemos a mejorarla.

Teorema 3.20 – *Lema de libertad genérica*: Sea A un dominio íntegro noetheriano, B una A-álgebra de tipo finito y M un B-módulo finitamente generado. Entonces existe $f \in A_{\neq 0}$ tal que $M[1/f] := M \otimes_A A[1/f]$ es un $A[1/f]$-módulo libre.

Demostración: Si $M = 0$, entonces es claramente plano sobre A, así que supongamos que $M \neq 0$. Por descomposición de Lasker-Noether (corolario A.9.1) existe una cadena $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ con $M_{j+1}/M_j \cong B/\mathfrak{q}_i$ para $\mathfrak{q}_i \in \operatorname{Spec} B$. Como los módulos libres son proyectivos, sustituyendo B por $B/\mathfrak{q}_i$ podemos suponer que B es un dominio íntegro y que $M = B$. Si el homomorfismo canónico $\varphi \colon A \to B$ no es inyectivo, entonces $B[1/f] = 0$ para todo $f \in \ker \varphi \setminus \{0\}$ y se satisface el teorema, de modo que suponemos que $\ker \varphi = 0$.

Sea $K := \operatorname{Frac} A$, entonces $B \otimes_A K = K[B]$ es un dominio íntegro (contenido en $\operatorname{Frac} B$) y es una K-álgebra de tipo finito. Por tanto, $d := k.\dim K[B] = \operatorname{trdeg}_K K[B] < \infty$. Procedemos por inducción en d. Por el teorema de normalización de Noether, $K[B]$ contiene d elementos K-algebraicamente independientes $y_1, \ldots, y_d$ tales que $K[B]$ es una extensión entera de $K[\boldsymbol{y}]$; más aún, podemos suponer que cada $y_i \in B$ (¿por qué?). Como B es de tipo finito sobre A, existe $g \in A_{\neq 0}$ tal que $B[1/g]$ es entero sobre $A[1/g][\boldsymbol{y}]$; así sustituyendo A, B por $A[1/g], B[1/g]$ y definiendo $C := A[\boldsymbol{y}]$, podemos suponer que B es un módulo finitamente generado sobre la A-álgebra polinomial C. Así, sean $b_1, \ldots, b_n \in B$ un conjunto maximal de elementos C-linealmente independientes. Tenemos la sucesión exacta

$$0 \longrightarrow C^n \xrightarrow{\mathrm{ev}_{\boldsymbol{b}}} B \longrightarrow N := \operatorname{coker}(\mathrm{ev}_{\boldsymbol{b}}) \longrightarrow 0,$$

donde N es un C-módulo finitamente generado de pura torsión. Como $(C/\mathfrak{p}) \otimes_A K \cong K[C]/\mathfrak{p}K$ para todo $\mathfrak{p} \in \operatorname{Spec} C$, entonces vemos que tiene menor dimensión que $k.\dim K[C] = d$, por lo que la hipótesis inductiva permite

concluir que $N[1/f]$ es libre sobre $A[1/f]$ para algún $f \in A_{\neq 0}$ y, por la sucesión exacta, $B[1/f]$ también. □

Lema 3.21: Sea A un anillo noetheriano, sea $B := A[\beta]$ una A-álgebra generada por un elemento, sea N un B-módulo finitamente generado y $M \leq N$ un A-submódulo finitamente generado tal que $B \cdot M = N$. Entonces $S := N/M$ posee una filtración

$$0 := G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq S, \qquad S = \bigcup_{n\in\mathbb{N}} G_n$$

con la propiedad de que hay finitos A-módulos finitamente generados $T_1, \ldots, T_m$ tales que cada cociente G_{n+1}/G_n es isomorfo a algún T_j.

Demostración: Defínanse

$$G'_n := M + \beta M + \beta^2 M + \cdots + \beta^n M \leq N, \qquad G_n := G'_n/M,$$
$$F_n := \{v \in N : \beta^{n+1} v \in M_n\} \leq N.$$

Claramente $0 \subseteq G_1 \subseteq G_2 \subseteq \cdots$ es una filtración, $S = \bigcup_{n\in\mathbb{N}} G_n$ y $G_{n+1}/G_n \cong N/F_n$. Como $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$ es una cadena ascendente de B-submódulos de N, entonces se estabiliza y, por tanto, los G_{n+1}/G_n's son eventualmente isomorfos entre sí. □

Al siguiente teorema también le llamamos *libertad genérica*.

Teorema 3.22: Sea A un dominio íntegro noetheriano, $C/B/A$ un trío de álgebras de tipo finito; sea M un C-módulo finitamente generado, $N \leq M$ un B-submódulo finitamente generado y $T \leq N$ un A-submódulo finitamente generado. Sea $S := M/(N + T)$. Entonces existe $f \in A_{\neq 0}$ tal que $S[1/f]$ es un $A[1/f]$-módulo libre.

Demostración: Escribamos $B = A[\beta_1, \ldots, \beta_r]$ y $C = B[\gamma_1, \ldots, \gamma_s]$. Procedemos por inducción sobre s, donde $s = 0$ viene dado por el lema de libertad genérica usual. Denotemos $B_j := A[\beta_1, \ldots, \beta_j]$ y $C_j := B[\gamma_1, \ldots, \gamma_j]$.

Supongamos que $s > 0$ y sea $T' := N + T \leq M$. Tenemos la siguiente filtración

$$C_0 T' \subseteq C_1 T' \subseteq \cdots \subseteq C_s T' = CT' \subseteq M.$$

Y, por hipótesis inductiva, existe dicho $f \in A_{\neq 0}$ para los cocientes $C_n T'/C_{n-1} T'$ con $1 \leq n < s$. Por el lema anterior, $C_s T'/C_{s-1} T'$ tiene una filtración con

finitos cocientes no isomorfos, así que aplicamos hipótesis inductiva nuevamente.

Para el último término $M' := M/CT'$ sean $v_1, \ldots, v_m \in M'$ generadores sobre C; sea $M_{s-1} := \sum_{i=1}^{m} v_i C_{s-1}$. Así vemos que $CM_{s-1} = M'$, de modo que el lema anterior nuevamente nos da una filtración con finitos cocientes no isomorfos sobre C_{s-1} y concluimos por hipótesis inductiva. □

Como corolario tenemos lo siguiente:

Teorema 3.23 (planitud genérica): Sea A un dominio íntegro noetheriano y B/A una extensión de anillos de tipo finito. Entonces existe $f \in A_{\neq 0}$ tal que $B[1/f]$ es un $A[1/f]$-módulo libre.

Geométricamente, si $g\colon \operatorname{Spec} B \to \operatorname{Spec} A$ es el morfismo inducido, entonces la restricción $g\colon g^{-1}[\mathbf{D}(f)] \to \mathbf{D}(f)$ es fielmente plano.

Teorema 3.24 (criterio topológico de Nagata): Sea A un anillo noetheriano y $U \subseteq \operatorname{Spec} A$ un conjunto. Entonces U es abierto syss satisface ambas condiciones:

CN1 Para todo $\mathfrak{p} \in U$ y todo $\mathfrak{q} \subseteq \mathfrak{p}$, se cumple que $\mathfrak{q} \in U$.

CN2 Si $\mathfrak{p} \in U$, entonces U contiene un abierto no vacío de $\mathbf{V}(\mathfrak{p})$.

Demostración: $\Longrightarrow$. Trivial.

$\Longleftarrow$. Sean $Z_1, \ldots, Z_r$ las componentes irreducibles de la clausura del complemento $\overline{\operatorname{Spec} A \setminus U}$ y sean $\mathfrak{P}_i \in \operatorname{Spec} A$ tales que $\mathbf{V}(\mathfrak{P}_i) = Z_i$. Si algún $\mathfrak{P}_i \in U$, entonces por CN2 existe algún $W \subset Z_i$ cerrado tal que $U^c \cap Z_i \subseteq W$ y, por lo tanto

$$U^c = \bigcup_{j=1}^{r} (U^c \cap Z_j) \subseteq W \cup \bigcup_{j \neq i}^{n} Z_j,$$

lo que contradice la definición de Z_i. Así que cada $\mathfrak{P}_i \notin U$ y, por CN1, vemos que cada $V_i \subseteq U^c$, por lo que U^c es cerrado. □

La condición **??** se suele expresar como que U es «estable bajo generizaciones», mientras que la condición **??** se suele expresar como que U es «semiconstructible».

Definición 3.25: Sea $\varphi\colon A \to B$ un homomorfismo de anillos y sea $\mathbf{P}$ una propiedad de homomorfismos de anillos locales. El ***conjunto*** o ***locus*** $\mathbf{P}$,

denotado $B_{\mathbf{P}}$, es el conjunto de puntos $\mathfrak{q} \in \operatorname{Spec} B$ tales que la localización $\varphi_{\mathfrak{q}}\colon A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ (donde $\mathfrak{p} := \mathfrak{q} \cap A$) satisface $\mathbf{P}$.

Decimos que $\mathbf{P}$ satisface el ***criterio de Nagata*** si: para todo homomorfismo $A \to B$ con B noetheriano, tal que $(B/\mathfrak{q})_{\mathbf{P}}$ contiene un abierto no vacío de $\operatorname{Spec}(B/\mathfrak{q})$ para todo $\mathfrak{q} \in \operatorname{Spec} B$, se concluye que $B_{\mathbf{P}}$ es abierto.

Por ejemplo, la propiedad $\mathcal{P}$ podría ser «el homomorfismo es plano», y en cuyo caso decimos que B_{flat} es el conjunto o *locus* plano. El enunciado emplea un homomorfismo, aunque la propiedad puede no hacer caso a dicho homomorfismo, por ejemplo, podría simplemente ser la propiedad «B es un anillo regular» y, nuevamente, hablamos del conjunto o locus regular. En cualquier caso, no hay daño en trabajar de manera relativa y tiene sus ventajas geométricas.

Teorema 3.26: Sea A un anillo noetheriano, B una A-álgebra de tipo finito y M un B-módulo finitamente generado. Entonces el conjunto $U := \{\mathfrak{q} \in \operatorname{Spec} B : M_{\mathfrak{q}} \text{ es plano sobre } A\}$ es abierto en $\operatorname{Spec} B$.

§3.3.1 Aplicación: teoremas de dimensión en fibras.

Teorema 3.27: Sea $\varphi\colon A \to B$ un homomorfismo de anillos noetherianos, sea $\mathfrak{q} \in \operatorname{Spec} B$ y $\mathfrak{p} := \mathfrak{q} \cap A \in \operatorname{Spec} A$. Se cumple que

$$\operatorname{alt} \mathfrak{q} \leq \operatorname{alt} \mathfrak{p} + k.\dim(B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}). \tag{3.2}$$

Si además φ es plano (o más generalmente, satisface el teorema del descenso de Cohen-Seidenberg), entonces se alcanza igualdad.

Demostración: Sustituyendo A por $A_{\mathfrak{p}}$ y B por $B_{\mathfrak{q}}$ nos reducimos al caso de $(A, \mathfrak{m}) \to (B, \mathfrak{n})$ un homomorfismo local de anillos noetherianos locales y hay que probar que

$$k.\dim B \leq k.\dim A + k.\dim(B \otimes \Bbbk(\mathfrak{m})).$$

Ahora bien, sea $a_1, \ldots, a_d \in A$ un sistema de parámetros y $b_1, \ldots, b_e \in B$ un conjunto cuyas imágenes conforman un sistema de parámetros de $B \otimes_A \Bbbk(\mathfrak{m})$ con $d := k.\dim A$ y $e := k.\dim(B \otimes_A \Bbbk(\mathfrak{m}))$. Por definición existen $m, n \gg 0$ tales que $\mathfrak{m}^m \subseteq \sum_{i=1}^{d} a_i A$ y $\mathfrak{n}^n \subseteq \mathfrak{m}B + \sum_{j=1}^{e} c_e B$; de modo que

$$\mathfrak{n}^{nm} \subseteq \sum_{i=1}^{d} a_i B + \sum_{j=1}^{e} b_j B,$$

por lo que $k.\dim B \leq d + e$.

Si ahora además $\mathfrak{n} = \mathfrak{q}_0 \supset \cdots \supset \mathfrak{q}_e \supseteq \mathfrak{m}B$ es una cadena maximal de primos en B con la condición de que «$\supseteq \mathfrak{m}B$», entonces solo basta construir otra cadena maximal $\mathfrak{m} = \mathfrak{p}_0 \supset \cdots \supset \mathfrak{p}_d$ en A y extenderla a B mediante el teorema del descenso de Cohen-Seidenberg. □

Teorema 3.28: Sea $\varphi\colon A \to B$ un homomorfismo de anillos noetherianos y sean $\mathfrak{p} \supseteq \mathfrak{q} \in \operatorname{Spec} A$ un par de primos.

1. Si la álgebra B/A satisface el teorema del ascenso de Cohen-Seidenberg, entonces
$$k.\dim(B \otimes_A \Bbbk(\mathfrak{p})) \geq k.\dim(B \otimes_A \Bbbk(\mathfrak{q})).$$

2. Si la álgebra B/A satisface el teorema del descenso de Cohen-Seidenberg, entonces
$$k.\dim(B \otimes_A \Bbbk(\mathfrak{p})) \leq k.\dim(B \otimes_A \Bbbk(\mathfrak{q})).$$

Demostración:

1. Sean $r := k.\dim(B \otimes \Bbbk(\mathfrak{q}))$ y $s := \operatorname{alt}(\mathfrak{p}/\mathfrak{q})$. Por definición, sean $\mathfrak{Q}_0 \subset \mathfrak{Q}_1 \subset \cdots \subset \mathfrak{Q}_r$ una cadena maximal de primos de B con $\mathfrak{Q}_r \cap A \subseteq \mathfrak{q}$. Sean $\mathfrak{q} =: \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_s := \mathfrak{p}$ una cadena de primos de A; entonces por teorema de ascenso la elevamos a una cadena
$$\mathfrak{Q}_r \subset \mathfrak{Q}_{r+1} \subset \cdots \subset \mathfrak{Q}_{r+s} \subseteq B, \qquad \forall j\ \mathfrak{Q}_{r+j} \cap A = \mathfrak{p}_j.$$
Así, con $\mathfrak{P} := \mathfrak{Q}_{r+s}$ satisface que
$$\operatorname{alt}(\mathfrak{P}/\mathfrak{q}B) \geq r + s, \qquad \mathfrak{P} \cap A = \mathfrak{p}.$$
Aplicando el teorema anterior a $A/\mathfrak{q} \to B/\mathfrak{q}B$ concluimos que $\operatorname{alt}(\mathfrak{P}/\mathfrak{q}B) \leq s + k.\dim(B_{\mathfrak{P}} \otimes \Bbbk(\mathfrak{p}))$ y, por tanto,
$$r \leq k.\dim(B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}}) \leq k.\dim(B \otimes \Bbbk(\mathfrak{p})).$$

2. Por inducción, podemos suponer que $\operatorname{alt}(\mathfrak{p}/\mathfrak{q}) = 1$. Sea $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_r$ una cadena de primos con $\mathfrak{P}_0 \cap A \supseteq \mathfrak{p}$ y $\operatorname{alt}(\mathfrak{P}_j/\mathfrak{P}_{j-1}) = 1$; vamos a construir otra cadena $\mathfrak{Q}_0 \subset \cdots \subset \mathfrak{Q}_r$ tal que
$$\mathfrak{Q}_0 \cap A \supseteq \mathfrak{q}, \qquad \forall j \quad \mathfrak{Q}_j \subseteq \mathfrak{P}_j, \qquad \operatorname{alt}(\mathfrak{Q}_j/\mathfrak{Q}_{j-1}) = 1.$$
Para ello, construimos $\mathfrak{Q}_0$ por teorema del descenso. Si $r \geq 1$, entonces considere $a \in \mathfrak{p} \setminus \mathfrak{q}$ y sean $\mathfrak{R}_1, \ldots, \mathfrak{R}_s$ los divisores primos minimales

de $\mathfrak{Q}_0 + aB$, entonces $\operatorname{alt}(\mathfrak{R}_j/\mathfrak{Q}_0) = 1$ (teorema de ideales principales de Krull) y $\operatorname{alt}(\mathfrak{P}_1/\mathfrak{Q}_0) \geq 2$, por lo que existe

$$b \in \mathfrak{P}_1 \setminus \left(\bigcup_{j=1}^{s} \mathfrak{R}_s \right).$$

Sea $\mathfrak{Q}_1$ un divisor primo minimal de $\mathfrak{Q}_0 + bB$ contenido en $\mathfrak{P}_1$, entonces $\operatorname{alt}(\mathfrak{Q}_1/\mathfrak{Q}_0) = 1$ (teorema de Krull) y $\mathfrak{Q}_1 \neq \mathfrak{R}_j$ para todo j, por lo que $a \notin \mathfrak{Q}_1$.

En definitiva, $\mathfrak{Q}_1 \cap A \neq \mathfrak{p}$ y, como $\operatorname{alt}(\mathfrak{p}/\mathfrak{q}) = 1$, entonces $\mathfrak{Q}_1 \cap A = \mathfrak{q}$ como se quería ver. Se aplica un argumento inductivo para contruir recursivamente $\mathfrak{Q}_2, \ldots, \mathfrak{Q}_r$. □

Notas históricas

Los teoremas de libertad y planitud genérica son originales de Grothendieck [**EGA IV$_2$,** pág. 153], lemme 6.9.2 y thm. 6.9.1. La versión de *libertad genérica* que nosotros presentamos es una modificación de Hochster y Roberts **[24].**

4

Teoría de valuación algebraica

En el capítulo 6 de mi libro de Teoría de Números [**47**] estudiamos los valores absolutos clásicos. Los *valores absolutos* (o cuerpos métricos) fueron inventados por Hensel para estudiar a los cuerpos p-ádicos, en éste capítulo damos una generalización más abstracta propuesta por W. Krull, pero por fines pedagógicos se recomienda leer ambos capítulos en conjunto.

4.1 Valores absolutos y cuerpos métricos

Definición 4.1: Un dominio íntegro A se dice un ***anillo de valuación*** si para todo $a \in \mathrm{Frac}(A)^\times$ se cumple que $a \in A$ o $a^{-1} \in A$.

Ejemplo.

- Todo cuerpo es un anillo de valuación.
- $\mathbb{Z}$ no es de valuación, puesto que $2/3 \in \mathbb{Q}$ satisface que $2/3 \notin \mathbb{Z}$ y $3/2 \notin \mathbb{Z}$.
- Considere la localización $\mathbb{Z}_{(p)}$, proponemos que es un anillo de valuación. En efecto, $\mathrm{Frac}(\mathbb{Z}_{(p)}) = \mathbb{Q}$ y para toda fracción reducida $a/b \in \mathbb{Q}$ se cumple que o bien $p \nmid b$, en cuyo caso $a/b \in \mathbb{Z}_{(p)}$, o bien $p \mid b$ y $p \nmid a$, en cuyo caso $b/a \in \mathbb{Z}_{(p)}$.

Proposición 4.2: Sea A un anillo de valuación con $K := \mathrm{Frac}(A)$, entonces:

1. A es un anillo local.
2. Si $A \subseteq B \subseteq K$, entonces B también es de valuación. En consecuencia, toda localización de A también es de valuación.
3. A es íntegramente cerrado.
4. Todo ideal finitamente generado es principal.[1]

Demostración:

1. Sea $\mathfrak{m} := A \setminus A^\times$, es decir, el conjunto de los elementos no inversibles de A. Sea $r \in A$, entonces $rx \in \mathfrak{m}$, pues de lo contrario $x = r(rx)^{-1} \in A^\times$. Sean $x, y \in \mathfrak{m}$ no nulos, sin perdida de generalidad supongamos que $xy^{-1} \in A$, luego $x + y = (1 + xy^{-1})y \in \mathfrak{m}$. En conclusión, $\mathfrak{m}$ es un ideal, luego debe ser un ideal maximal y el único de A.
2. Trivial.
3. Sea $x \in K$ no nulo y entero sobre A, es decir,

$$x^{n+1} + c_n x^n + \cdots + c_0 = 0$$

con $c_i \in A$. Si $x \in A$ entonces no hay nada que probar. Si $x^{-1} \in A$, entonces como $x = -(c_n + c_{n-1}x^{-1} + \cdots + c_0 x^{-n}) \in A$.
4. Basta probar que todo ideal generado por dos elementos es principal. Sea (a, b) un ideal con a, b no nulos. Luego o bien $a/b \in A$ o $b/a \in A$ y entonces o bien $(a, b) = (b)$ o bien $(a, b) = (a)$ resp. □

El nombre «anillo de valuación» sugiere que todo anillo de valuación desciende una valor absoluto en K, pero ésto podría no ser cierto. Para ello, vemos que la complicación está en que las funciones hasta $\mathbb{R}$ son demasiado *concretas* y también demasiado *rígidas*, mientras que buscamos una definición más *abstracta* que sí nos permita establecer una analogía con los valores absolutos.

Definición 4.3: Se dice que $(G, +, \leq)$ es un ***grupo abeliano ordenado*** si $(G, +)$ es un grupo abeliano (en notación aditiva), $(G, \leq)$ es un conjunto linealmente ordenado y:

GAO1. $0 \leq a$ syss $0 \geq -a$.

[1] Un dominio que satisface ésto se le dice un *anillo de Bézout* en literatura especializada.

GAO2. Si $a \leq b$ y $c \leq d$, entonces $a + c \leq b + d$.

En G, para fines prácticos, admitimos el convenio de que $\infty \notin G$ satisface $a + \infty = \infty$. De no haber ambigüedad sobre los signos, obviaremos la operación $+$ y el orden $\leq$.

Es claro que $(\mathbb{R}, +, \leq)$ es un grupo abeliano ordenado y lo son todos sus subgrupos (e.g., $\mathbb{Q}$ y $\mathbb{Z}$).

Definición 4.4: Sea A un anillo y G un grupo abeliano ordenado. Una (G-)***valuación***[a] $v\colon A \to G \cup \{\infty\}$ es una aplicación tal que:

V1. $v(a) = \infty$ syss $a = 0$.

V2. $v(ab) = v(a) + v(b)$.

V3. $v(a + b) = \min\{v(a), v(b)\}$.

A las $\mathbb{Z}$-valuaciones les llamamos también ***valuaciones discretas***.

[a] No existe consenso en la nomenclatura, algunos textos también les llaman *valuaciones* a los valores absoluto. Lang [0] emplea «valor absoluto / valuación», mientras que Jacobson [0] emplea «valuación / valuación exponencial» y Nagata [0] emplea «valuación multiplicativa / aditiva».

Nótese que una valuación se restringe a un homomorfismo de grupos abelianos $A^\times \to G$.

Todo valor absoluto no-arquimediano sobre un cuerpo induce una $\mathbb{R}$-valuación: En efecto, sea $0 < r < 1$ un real arbitrario, entonces $v(x) := \log_r |x|$ es una valuación. La propiedad V1 puede considerarse como por definición, la propiedad V2 se reduce a que el logaritmo convierte productos en sumas y la propiedad V3 es una traducción de la desigualdad ultramétrica.

En el caso de los valores absolutos no-arquimedianos habíamos construido los objetos

$$\mathfrak{o} = \{x \in k : |x| \leq 1\}, \qquad \mathfrak{m} = \{x \in k : |x| < 1\},$$

cuyos análogos en el mundo de las valuaciones son

$$\mathfrak{o} = \{x \in k : v(x) \geq 0\}, \qquad \mathfrak{m} = \{x \in k : v(x) > 0\}.$$

Proposición 4.5: Sea A un dominio íntegro.

1. Sea v una G-valuación en A, entonces existe una única G-valuación $\bar{v}$ en $\mathrm{Frac}(A)$ que extiende a v.

2. Si A es noetheriano y $\mathfrak{p} \lhd A$ primo, entonces $\nu_{\mathfrak{p}}(a) := n$ como el natural tal que $a \in \mathfrak{p}^n$ y $a \notin \mathfrak{p}^{n+1}$ es una valuación discreta sobre A y, por ende, admite una única extensión a $\mathrm{Frac}(A)$. A ésta valuación le decimos la $\mathfrak{p}$-ádica.

Teorema 4.6: Sea A un subanillo de un cuerpo k. Son equivalentes:

1. Existe una valuación v sobre k tal que $A = \{a \in k : v(a) \geq 0\}$.
2. Si $a \in k$ entonces $a \in A$ o $a^{-1} \in A$.
3. A es local, $k = \mathrm{Frac}(A)$ y todo ideal finitamente generado de A es principal.
4. A es local y todo subanillo $A \subset B \subseteq k$ contiene algún $b \in A$ que es inversible en B pero no en A.
5. Para todo subanillo $A \subseteq B \subseteq k$ existe $\mathfrak{p} \lhd A$ primo tal que $B = A_{\mathfrak{p}}$.

Demostración: $1 \implies 2$. Es claro.

$2 \implies 1$. Sean $a, b \in K$. Si $aA \not\subseteq bA$, entonces $b^{-1}a \notin A$, luego $ba^{-1} \in A$ y $bA \subseteq aA$. Así, definamos $G := \{aA : a \in k^\times\}$ y notemos que G es un grupo abeliano mediante cuya operación es $(aA)(bA) := (ab)A$; para distinguir la notación aditiva emplearemos corchetes en los elementos, de modo que:

$$[aA] + [bB] := [(ab)A], \quad 0 := [1A], \quad -[aA] = [a^{-1}A].$$

Así $(G, +, \subseteq)$ es un grupo abeliano ordenado. Finalmente es claro que $v(a) := [aA]$ es una G-valuación en k que satisface lo exigido.

$3 \implies 2$. Sean $a, b \in A$ no nulos y sea $c \in A$ tal que $aA + bA = cA$ (como suma de ideales). Sean $r := a/c$ y $s := b/c$ elementos de k tal que $rA + sA = A$, es decir, $rA, sA \subseteq A$ y por ende son ideales de A; y como A es local, debe cumplirse que alguno de los elementos sea inversible (de lo contrario $rA + sA \subseteq \mathfrak{m}$), digamos que r lo es, vale decir, $r^{-1} = c/a \in A$ y $sr^{-1} = b/a \in A$ (el otro caso implica que $rs^{-1} = a/b \in A$).

$2 \implies 3$. Es claro.

$2 \implies 5$. Sabemos que B es también un anillo de valuación con $\mathrm{Frac}(B) = k$, y por ende tiene un único ideal maximal $\mathfrak{q}$. Sea $B' := A_{\mathfrak{q} \cap A}$ de modo que $A \subseteq B' \subseteq B$ y B' es de valuación. Sea $b \in B \setminus B'$, luego $b^{-1} \in B' \subseteq B$ así que b es inversible en B, pero b^{-1} no lo es en B'. Luego b^{-1} pertenece al ideal maximal de B' que es $(\mathfrak{q} \cap A)B' = \mathfrak{q} \cap B'$ y $b^{-1} \in \mathfrak{q}$, pero los elementos de $\mathfrak{q}$ no son inversibles en B lo cual es absurdo.

$5 \implies 4$. Trivial.

$4 \implies 2$. Sea B la clausura íntegra de A en k. Nótese que $B = A$, de lo contrario existe $b \in A$ que es inversible en B y no en A; así que tomamos $\mathfrak{p} \lhd A$ primo que contenga a b y, por el teorema del ascenso, lo levantamos a un primo $\mathfrak{q} \lhd B$ tal que $\mathfrak{p} = \mathfrak{q} \cap A$, pero $b \in \mathfrak{q}$ y $(1) = (b) = \mathfrak{q} \neq B$ lo que sería absurdo. Luego A es íntegramente cerrado.

Sean $a, b \in A$ tales que b es no nulo y $a/b \notin A$. Luego $C := A[a/b]$ contiene a un elemento $d \in A$ inversible en C que no lo es en A. Por definición:

$$d^{-1} = c_0(a/b)^m + c_1(a/b)^{m-1} + \cdots + c_0, \qquad c_i \in A,$$

luego $b^m = dc_0a^m + dc_1a^{m-1}b + \cdots + dc_mb^m$. Como $d \notin A^\times$, entonces está en el maximal y $1 - dc_m \in A^\times$. Definiendo $d' := d(1 - dc_m)$ y dividiendo por a^m se obtiene que

$$(b/a)^m = d'c_0 + d'c_1(b/a) + \cdots + d'c_{m-1}(b/a)^{m-1},$$

donde $d'c_i \in A$, de modo que b/a es entero en A y $b/a \in A$. □

Definición 4.7: Dado un anillo de valuación A, llamamos su ***grupo de valores*** G, al grupo construido en la demostración anterior.

Puesto que en los grupos abelianos ordenados adjuntamos ésta nueva estructura podemos construir una categoría en donde las flechas son homomorfismos de grupos que son crecientes como funciones; a éstos se les llaman ***orden-homomorfismos***. El grupo de valores de un anillo de valuación es único salvo orden-isomorfismo.

Teorema 4.8: Sea A un anillo de valuación, $K := \mathrm{Frac}(A)$ y $A \subset B \subseteq K$ un subanillo. Sean $\mathfrak{m} := \mathfrak{J}(A), \mathfrak{n} := \mathfrak{J}(B)$, entonces:

1. $\mathfrak{n} \subset \mathfrak{m} \subseteq A \subset B$.
2. $\mathfrak{n}$ es un ideal primo de A y $A_{\mathfrak{n}} = B$.
3. $A/\mathfrak{n}$ es un anillo de valuación del cuerpo $B/\mathfrak{n}$.
4. Sea $\bar{C} \subseteq B/\mathfrak{n}$ un subanillo de valuación y sea

$$C := \bar{C}^e = \{a \in B : a \text{ mód } \mathfrak{n} \in \bar{C}\}.$$

Entonces $C \subseteq K$ es un subanillo de valuación.

Demostración:

1. Sea $b \in \mathfrak{n}$, entonces $b^{-1} \notin B$, luego $b^{-1} \notin A$ y por tanto $b \in \mathfrak{m}$. Además $\mathfrak{n} \neq \mathfrak{m}$ puesto que $A \neq B$.

2. Basta notar que bajo la inclusión $A \hookrightarrow B$, se cumple que $\mathfrak{n} = \mathfrak{n}^c$ y la contracción de ideales primos es primo. El que coincida con la localización lo probamos en el teorema anterior.

3. Sea $\varphi\colon B \to B/\mathfrak{n}$ la proyección canónica. Sea $b \in B \setminus \mathfrak{n}$, si $b \in A$, entonces $\varphi(b) \in A/\mathfrak{n}$. Si $b \notin A$, entonces $b^{-1} \in A$ y $\varphi(b)^{-1} = \varphi(b^{-1}) \in A/\mathfrak{n}$.

4. Sea $a \in K$ tal que $a \notin C$. Si $a \notin B$, entonces $b^{-1} \in \mathfrak{n} \subseteq C$. Si $a \in B$, entonces a mód $\mathfrak{n} \notin \bar{C}$ y a^{-1} mód $\mathfrak{n} \in \bar{C}$ (por ser de valuación), con lo que $a^{-1} \in C$. □

Teorema 4.9: Sea K un cuerpo, $A \subseteq K$ un subanillo, y $\mathfrak{p} \lhd A$ un ideal primo. Existe $A \subseteq B \subseteq K$ un subanillo de valuación de K con $\mathfrak{J}(B) \cap A = \mathfrak{p}$.

Demostración: Si sustituimos A por su localización $A_{\mathfrak{p}}$, podemos suponer que $(A, \mathfrak{p})$ es local. Sea $\mathcal{F}$ la familia de subanillos $A \subseteq C \subseteq K$ tales que $1 \notin \mathfrak{p} \cdot C$. Nótese que $A \in \mathcal{F}$, de modo que $\mathcal{F}$ no es vacía y, por el lema de Zorn, escojamos B un elemento $\subseteq$-maximal de $\mathcal{F}$. Ahora bien, B es de valuación, luego es local de maximal $\mathfrak{m}$ y vemos que $\mathfrak{p} \subseteq \mathfrak{m}$. Además, como $\mathfrak{p} \lhd A$ es maximal, entonces $\mathfrak{m} \cap A = \mathfrak{p}$.

Finalmente hay que probar que B es de valuación. Sea $a \in K \setminus B$. Como $B \subset B[a] \notin \mathcal{F}$, entonces $1 \in \mathfrak{p} \cdot B[a]$ y

$$1 = c_0 + c_1 a + \cdots + c_n a^n,$$

donde cada $c_i \in \mathfrak{p}$. Luego $1 - c_0 \in A^\times$ e invirtiendo se obtiene una relación

$$1 = d_1 a + \cdots + d_n a^n, \tag{4.1}$$

con cada $d_i \in \mathfrak{p}$. Elijamos la relación (4.1) con $n \geq 1$ minimal. Si además $a^{-1} \notin B$, entonces análogamente se obtiene una relación

$$1 = e_1 a^{-1} + \cdots + e_m a^{-m}, \tag{4.2}$$

con cada $e_i \in \mathfrak{p}$ y $m \geq 1$ minimal. Si $n \geq m$, entonces multiplicamos (4.2) por $d_n a^n$ y se la restamos a la ecuación (4.2) para reducir n, y recíprocamente si $n < m$, por lo que es absurdo que $a \notin B$ y $a^{-1} \notin B$. □

Teorema 4.10: Sea K un cuerpo y $A \subseteq K$ un subanillo. Sea B la clausura íntegra de A en K, entonces B es la intersección de todos los anillos de valuación de K que contienen a A.

Demostración: Sea C la intersección de todos los anillos de valuación de K que contienen a A, entonces es claro que $B \subseteq C$. Para probar la inclusión restante, veremos que si $a \notin B$, entonces $a \notin C$.

Sea $b := a^{-1}$. Nótese que el ideal $b \cdot A[b]$ de $A[b]$ es propio: En efecto, si $1 \in b \cdot A[b]$, entonces

$$1 = b(c_n + c_{n-1}b + \cdots + c_0 b^n),$$

para algunos $c_i \in A$. Multiplicando todo por a^{n+1}, se obtiene

$$a^{n+1} = c_n a^n + c_{n-1}a^{n-1} + \cdots + c_0,$$

lo cual contradice que a no es entero sobre A.

Así, por el teorema de Krull existe un ideal $\mathfrak{m} \supseteq b \cdot A[b]$ maximal en $A[b]$ y luego existe $D \supseteq A[b] \supseteq A$ de valuación en K con $\mathfrak{J}(D) \cap A[b] = \mathfrak{m}$ y, por ende, con $a \notin D$. □

Volvemos al estudio de grupos abelianos ordenados:

Definición 4.11: Un grupo abeliano ordenado G se dice ***arquimediano*** si para todo $a, b \in G$ con $a > 0$, existe $n \in \mathbb{N}$ tal que $na > b$.

Proposición 4.12: Sea G un grupo abeliano ordenado. Son equivalentes:

1. G es orden-isomorfo a un subgrupo de $\mathbb{R}$.
2. G es un grupo arquimediano.

Demostración: $1 \implies 2$. Es claro del hecho de que $\mathbb{R}$ es arquimediano y todo subgrupo de un grupo arquimediano es arquimediano.

$2 \implies 1$. Si $G = 0$, entonces es claro. Si no, fijemos $a \in G_{>0}$. Nótese que para todo b podemos definir n_0 como el máximo entero tal que $n_0 a \leq b$. Sea $b_1 := b - n_0 a \geq 0$ y definamos n_1 como el máximo entero tal que $n_1 a \leq 10 b_1$, y así recursivamente. Nótese que $0 \leq n_i < 10$ para todo $i > 0$. Luego definamos la aplicación $\varphi \colon G \to \mathbb{R}$ como:

$$\varphi(b) := n_0 + \sum_{i=1}^{\infty} 10^{-i} n_i.$$

Es fácil comprobar que φ es una función creciente.

Además, φ es inyectiva puesto que si $b < c$, entonces existe $r > 0$ tal que $a < 10^r(c-b)$.

Finalmente, veamos que φ es un homomorfismo de grupos: Para ello, fijemos un entero $r > 0$ y sea $n := \lfloor 10^r \varphi(b) \rfloor$, es decir, $|\varphi(b) - n/10^r| < 1/10^r$ y $na \leq 10^r b < (n+1)a$. Sea $m := \lfloor 10^r \varphi(c) \rfloor$. Así, nótese que

$$(n+m)a \leq 10^r(b+c) < (n+m+2)a \iff \varphi(b+c) - \frac{n+m}{10^r} < \frac{2}{10^r}.$$

Luego, mediante desigualdad triangular:

$$|\varphi(b+c) - \varphi(b) - \varphi(c)| < \frac{4}{10^r},$$

donde el r podemos elegirlo arbitrariamente grande, ergo $\varphi(b+c) = \varphi(b) + \varphi(c)$. □

Teorema 4.13: Sea $(A, \mathfrak{m})$ un anillo de valuación, con grupo de valuación G. Entonces $k.\dim(A) = 1$ syss G es arquimediano y no nulo.

Demostración: $\Longrightarrow$. Sea $0 \neq \alpha \in \mathfrak{m}$ que determina $a := v(\alpha) \in G_{>0}$. Como $\mathfrak{m}$ es el único ideal primo que contiene a α (pues $k.\dim A = 1$), entonces $\mathrm{Rad}(\alpha) = \mathfrak{m}$. Así pues, sea $\beta \in \mathfrak{m}$ que determina $b := v(\beta) \in G_{>0}$; entonces $\beta^n \in (\alpha)$ para algún $n > 0$ (por definición del radical), es decir, $nb > a$.

$\Longleftarrow$. Como $G \neq 0$, entonces A no es cuerpo y $\mathfrak{m} \neq 0$. Sea $\mathfrak{p} \lhd A$ un ideal primo, distinto de $\mathfrak{m}$, veremos que es necesariamente el ideal nulo. Así, sea $\alpha \in \mathfrak{m} \setminus \mathfrak{p}$ y sea $a := v(\alpha) \in G_{>0}$. Supongamos que existe $\beta \in \mathfrak{p}_{\neq 0}$, y sea $b := v(\beta) \in G_{>0}$ y, por ser arquimediano, existe $n \in \mathbb{N}$ tal que $na > b$, es decir, $v(\alpha^n/\beta) > 0$ y $\alpha^n/\beta \in A$, luego $\alpha^n \in (\beta) \subseteq \mathfrak{p}$ y, como $\mathfrak{p}$ es primo, $\alpha \in \mathfrak{p}$ lo que es absurdo. Luego $\mathfrak{p} = (0)$ como se quería ver. □

Definición 4.14: Se dice que un anillo A es un ***dominio de valuación discreta*** si su grupo de valores es orden-isomorfo a $\mathbb{Z}$ (y por ende, está inducido por una valuación discreta).

Teorema 4.15: Sea $(A, \mathfrak{m})$ un anillo de valuación. Son equivalentes:

1. A es un dominio de valuación discreta.
2. A es un DIP.

3. A es noetheriano.

Demostración: $1 \implies 2$. Sea $\mathfrak{a}$ un ideal no nulo. El conjunto $\{v(a) : a \in \mathfrak{a}_{\neq 0}\} \subseteq \mathbb{N}$ es no vacío y por ende tiene un mínimo. Sea $b \in \mathfrak{a}$ un elemento de valuación mínima, luego para todo $c \in \mathfrak{a}$ se cumple que $v(c) \geq v(b)$ y $c/b \in A$, ergo $c \in bA$ y $\mathfrak{a} = (b)$.

$2 \implies 3$. Trivial.

$3 \implies 2$. Un anillo es noetheriano si todo ideal es finitamente generado y, en un anillo de valuación todo ideal finitamente generado es principal.

$2 \implies 1$. Sea $(t) = \mathfrak{m}$ y recuerde que por el teorema de intersecciones de Krull, $\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = (0)$. Así notamos que $\nu_{\mathfrak{m}}$, la valuación $\mathfrak{m}$-ádica, tiene por anillo de valuación a A. □

Definición 4.16: Un dominio A se dice ***normal***[2] si para todo ideal primo $\mathfrak{p} \lhd A$ se cumple que la localización $A_{\mathfrak{p}}$ es un dominio íntegramente cerrado.

La proposición 2.22 nos dice que las nociones de normal e íntegramente cerrado coinciden sobre un dominio íntegro, por lo que ser normal es un poco más general.

Teorema 4.17: Sea A un dominio. Son equivalentes:

1. A es un dominio de valuación discreta.
2. A es un DIP local y no un cuerpo.
3. A es un dominio íntegro noetheriano local, $k.\dim A > 0$ y el ideal maximal es principal.
4. A es un dominio íntegro noetheriano local, $k.\dim A = 1$ y es normal.

Demostración: La implicancia $1 \implies 2$ la hemos probado en el teorema anterior y $2 \implies 3$ es trivial.

$1 \implies 4$. Todo anillo de valuación es local y normal; mientras que todo dominio de valuación discreta es noetheriano y de dimensión 1.

$4 \implies 3$. Como A es noetheriano y no es artiniano, entonces $\mathfrak{m} \neq \mathfrak{m}^2$. Sea $a \in \mathfrak{m} \setminus \mathfrak{m}^2$. Como $k.\dim A = 1$ y A es un dominio íntegro, entonces sus ideales primos son $(0), \mathfrak{m}$. Luego $\mathfrak{m}$ debe ser un ideal primo asociado

[2] Ésta terminología es empleada por Matsumura [**5**] y originaria de Grothendieck. El término es un tanto controversial, puesto que varios autores (e.g., Eisenbud [**3**]) lo reservan como sinónimo de íntegramente cerrado.

a (a) y así, existe $b \in A$ tal que $(a : b) = \mathfrak{m}$ (es decir, $b\mathfrak{m} \subseteq (a)$). Sea $c := ba^{-1} \in K =: \mathrm{Frac}(A)$; nótese que $c \notin A$ (¿por qué?), pero $c\mathfrak{m} \subseteq A$. Definamos $\mathfrak{m}^{-1} := \{d \in K : d\mathfrak{m} \subseteq A\}$. Nótese que $A \subseteq \mathfrak{m}^{-1}$, pero no se alcanza igualdad pues $c \in \mathfrak{m}^{-1}$.

Considere el conjunto $\mathfrak{a} := \mathfrak{m}^{-1}\mathfrak{m}$ y nótese que es un ideal de A que además satisface $\mathfrak{m} \subseteq \mathfrak{a}$. Si $\mathfrak{m} = \mathfrak{a}$, entonces se cumpliría que $c\mathfrak{m} \subseteq \mathfrak{m}$ y, por el lema de Nakayama, se concluiría que c es entero sobre A, pero $c \notin A$ y A es normal; en conclusión $\mathfrak{a} = A$. El conjunto $a\mathfrak{m}^{-1} \subseteq A$ es un ideal y si $a\mathfrak{m}^{-1} \subseteq \mathfrak{m}$, entonces se tendría que $(a) = a\mathfrak{m}^{-1}\mathfrak{m} \subseteq \mathfrak{m}^2$, pero $a \notin \mathfrak{m}^2$. Por ende, $a\mathfrak{m}^{-1} = A$ y multiplicando por $\mathfrak{m}$ obtenemos que $(a) = \mathfrak{m}$.

$3 \implies 1$. Sea $(t) = \mathfrak{m}$. Si t fuese nilpotente, entonces $k.\dim A = 0$, luego $t^n \neq 0$ para todo $n \in \mathbb{N}$. De éste modo, la valuación $\mathfrak{m}$-ádica tiene por grupo de valores a $\mathbb{Z}$. □

Teorema 4.18: Sea $(A, \mathfrak{m}, k)$ un dominio íntegro, local, noetheriano de dimensión 1. Las siguientes son equivalentes:

1. A es un dominio de valuación discreta.
2. A es normal.
3. $\mathfrak{m}$ es un ideal principal.
4. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.
5. Todo ideal propio es una potencia de $\mathfrak{m}$.
6. Existe un $x \in A$ tal que todo ideal propio es de la forma (x^n).

Demostración: $1 \implies 2$. Todo dominio de valuación discreta es de valuación, y todo anillo de valuación es íntegramente cerrado.

$2 \implies 3$. Sea $a \in \mathfrak{m}$ no nulo, entonces (a) es un ideal propio. Como A es decomposible y el único ideal primo de A es $\mathfrak{m}$, entonces (por ser dominio íntegro local de dimensión 1) (a) es $\mathfrak{m}$-primario y existe un n tal que $\mathfrak{m}^{n+1} \subseteq (a)$ y $\mathfrak{m}^n \not\subseteq (a)$. Sea $b \in \mathfrak{m}^n \setminus (a)$, y sea $x = a/b \in K := \mathrm{Frac}(A)$, luego nótese que $x^{-1} \notin A$ (de lo contrario $b = ax^{-1} \in (a)$), por lo que x^{-1} no es entero sobre A y luego $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$, puesto que de lo contrario $\mathfrak{m}$ sería un $A[x^{-1}]$-módulo fiel finitamente generado y x^{-1} sería entero. Finalmente $x^{-1}\mathfrak{m} \subseteq A$, pero entonces $\mathfrak{m} \subseteq x^{-1}\mathfrak{m}$, por lo que $x^{-1}\mathfrak{m} = A$ y $\mathfrak{m} = Ax = (x)$.

¿Por qué?

$3 \implies 4$. Nótese que por el lema de Nakayama, $\mathfrak{m}/\mathfrak{m}^2$ está generado por a lo más un elemento, y las potencias de $\mathfrak{m}$ son distintas, de lo contrario sería nilpotente y entonces sería artiniano y de dimensión cero.

$4 \implies 5$. Si $\mathfrak{a} \lhd A$ es propio, entonces existe un n tal que $\mathfrak{m}^n \subseteq \mathfrak{a}$, luego $A/\mathfrak{m}^n$ es artiniano, por lo que la extensión de $\mathfrak{a}$ es potencia del maximal, luego $\mathfrak{a}$ mismo también debe de serlo.

$5 \implies 6$. Ya vimos que las potencias del maximal son distintas. Sea $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, luego $(x) = \mathfrak{m}^r$ para algún r, y dicho r tiene necesariamente que ser 1, luego $\mathfrak{m}^n = (x^n)$.

$6 \implies 1$. Sea $\mathfrak{m} = (x)$, entonces para todo $a \in A$ ya vimos que $(a) = (x^n)$ para un único n, por lo que definamos $v\colon A_{\neq 0} \to \mathbb{Z}$ como $v(a) = n$, y extendamos $v\colon K^\times \to \mathbb{Z}$ por $v(a/b) = v(a) - v(b)$. Queda al lector comprobar que efectivamente se trata de una valuación discreta. □

Definición 4.19: Si $(A, \mathfrak{m})$ es un dominio de valuación discreta y $\mathfrak{m} = (\pi)$, entonces decimos que π es un ***uniformizador*** de A.

Definición 4.20: Sea A un dominio íntegro y $K := \operatorname{Frac} A$. Se dice que un A-submódulo M de K es un ***ideal fraccionario*** si existe algún $a \in A_{\neq 0}$ tal que $aM \subseteq A$. A los ideales de A (en sentido usual) les diremos ***ideales enteros***. Si $M = bA$ para algún $b \in K$, entonces M se dice un ***ideal (fraccionario) principal***. Para un A-submódulo M se define:

$$(A : M) := \{x \in A : xM \subseteq A\}.$$

(Nótese que M es fraccionario syss $(A : M) \neq (0)$.)

Un A-submódulo M se dice ***inversible*** si existe otro A-submódulo N tal que $MN = A$.

Nótese que si M es inversible y N es una inversa, entonces:

$$N \subseteq (A : M) = (A : M)MN \subseteq AN = N,$$

de modo que $N = (A : M)$. Además si M es inversible, entonces es claro que es finitamente generado (¿por qué?).

Proposición 4.21: Sea A un dominio íntegro, $K := \operatorname{Frac} A$ y $I \subseteq K$ un ideal fraccionario. Son equivalentes:

1. I es inversible.
2. I es finitamente generado y para todo $\mathfrak{p} \lhd A$ primo, $I_\mathfrak{p}$ es principal.
3. I es finitamente generado y para todo $\mathfrak{m} \lhd A$ maximal, $I_\mathfrak{m}$ es principal.

Demostración:

$1 \implies 2$. Ya sabemos que I es finitamente generado. Como es inversible, existen $a_i \in I$ y $b_i \in I^{-1}$ tales que $\sum_{i=1}^{n} a_i b_i = 1$. Para todo ideal primo $\mathfrak{p} \lhd A$, se cumple que $A_\mathfrak{p}$ es local, luego, necesariamente algún $a_i b_i \in A \subseteq A_\mathfrak{p}$ ha de ser invertible (de lo contrario, todos están en el maximal) y luego sea $ab = 1$ donde $a \in I_\mathfrak{p}$ y $b \in I_\mathfrak{p}^{-1}$. Nótese que $I_\mathfrak{p} = aA_\mathfrak{p}$, pues para todo $c \in I_\mathfrak{p}$ tenemos que $c = (cb)a$, donde $cb \in A_\mathfrak{p}$.

$2 \implies 3$. Trivial.

$2 \implies 3$. Si I es finitamente generado, entonces $(I^{-1})_\mathfrak{p} = (I_\mathfrak{p})^{-1}$ para todo ideal primo $\mathfrak{p}$. La inclusión $\subseteq$ es clara, veamos $\supseteq$: si $I = a_1 A + \cdots + a_n A$, entonces para todo $b \in (I_\mathfrak{p})^{-1}$ se cumple que $a_i b \in A_\mathfrak{p}$, luego existe $c_i \in A \setminus \mathfrak{p}$ tal que $a_i b c_i \in A$. Eligiendo $c := c_1 \cdots c_n$, vemos que $a_i(bc) \in A$ para todo i, luego $bc \in I^{-1}$ y $b \in (I^{-1})_\mathfrak{p}$ como se quería probar.

Así pues, sea $\mathfrak{a} := I \cdot I^{-1}$. Si I no fuese invertible, entonces $\mathfrak{a} \subseteq \mathfrak{m}$ para algún ideal maximal, y luego $I_\mathfrak{m} \cdot (I_\mathfrak{m})^{-1} = I_\mathfrak{m} \cdot (I^{-1})_\mathfrak{m} \subseteq \mathfrak{m} A_\mathfrak{m}$ lo cual es absurdo. □

Teorema 4.22: Sea A un dominio íntegro noetheriano y $\mathfrak{p} \lhd A$ un ideal primo. Si $\mathfrak{p}$ es inversible, entonces $\operatorname{alt} \mathfrak{p} = 1$ y $A_\mathfrak{p}$ es un dominio de valuación discreta.

Demostración: Si $\mathfrak{p}$ es inversible, entonces $\mathfrak{p}A_\mathfrak{p}$, el ideal maximal de $A_\mathfrak{p}$, es principal y finalmente, por el teorema 4.17 vemos que $A_\mathfrak{p}$ es dominio de valuación discreta; así, $\operatorname{alt} \mathfrak{p} = k.\dim(A_\mathfrak{p}) = 1$. □

Teorema 4.23: Sea A un dominio noetheriano normal. Entonces:

1. Todos los primos asociados a los ideales principales tienen altura 1.
2. $A = \bigcap_{\operatorname{alt} \mathfrak{p} = 1} A_\mathfrak{p}$, donde $\mathfrak{p}$ recorre los ideales primos de A.

Demostración:

1. Sea $a \in A_{\neq 0}$ y sea $\mathfrak{p} \in \operatorname{As}(aA)$, entonces, existe $b \in A$ tal que $(aA : b) = \mathfrak{p}$. Sea $\mathfrak{m} := \mathfrak{p}A_\mathfrak{p}$, de modo que $(aA_\mathfrak{p} : b) = \mathfrak{m}$ y luego, $b/a \in \mathfrak{m}^{-1}$ y $b/a \notin A_\mathfrak{p}$. Si se cumple que $ba^{-1} \cdot \mathfrak{m} \subseteq \mathfrak{m}$, entonces empleando el teorema de Cayley-Hamilton obtenemos que que ba^{-1} es entero en $A_\mathfrak{p}$, lo que es absurdo pues $A_\mathfrak{p}$ es íntegramente cerrado. Luego $ba^{-1}\mathfrak{m} = A_\mathfrak{p}$, se tiene que $\mathfrak{m}^{-1}\mathfrak{m} = A_\mathfrak{p}$ y, por el teorema anterior, $\operatorname{alt} \mathfrak{m} = \operatorname{alt} \mathfrak{p} = 1$.
2. Sean $a, b \in A_{\neq 0}$. Basta probar que si $b \in aA_\mathfrak{p}$ para todo ideal primo $\mathfrak{p}$ de altura 1, entonces $b \in aA$. Sean $\operatorname{As}(a) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ y sea $aA =$

$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ una descomposición primaria minimal con $\operatorname{Rad} \mathfrak{q}_i = \mathfrak{p}_i$. Como $\operatorname{alt} \mathfrak{p}_i = 1$, entonces $b \in aA_{\mathfrak{p}_i} \cap A = \mathfrak{q}_i$ por el teorema A.14 y finalmente $b \in \bigcap_{i=1}^n \mathfrak{q}_i = aA$. □

Definición 4.24: Un dominio A se dice ***de Dedekind*** si es un dominio íntegro en donde todo ideal fraccionario no nulo es inversible.

Teorema 4.25: Sea A un dominio íntegro. Son equivalentes:

1. Todo ideal fraccionario no nulo es inversible.
2. A es un cuerpo o es noetheriano normal de dimensión 1.
2′. Para todo ideal maximal $\mathfrak{m} \lhd A$ (no nulo) se cumple que $A_{\mathfrak{m}}$ es un dominio de valuación discreta.
3. Todo ideal entero no nulo se escribe como producto de (finitos) ideales primos.

Demostración: 1 $\implies$ 2. Un cuerpo no tiene ideales fraccionarios no nulos así que estamos bien, así que supondremos que A no es un cuerpo. Como todo ideal primo no nulo $\mathfrak{p}$ es inversible, entonces $\mathfrak{p}$ es finitamente generado y por el teorema de Cohen, A es noetheriano. Además, como $\mathfrak{p}$ es inversible, entonces $A_{\mathfrak{p}}$ es dominio de valuación discreta y luego es íntegramente cerrado, por lo que, A es normal. Finalmente, sabemos que $k.\dim A = \sup\{\operatorname{alt} \mathfrak{p} : \mathfrak{p} \lhd A \text{ primo}\} = 1$.

2 $\implies$ 1. Supongamos que A no es cuerpo y sea $(0) \neq \mathfrak{p}$ un ideal primo. Luego $A_{\mathfrak{p}}$ es un dominio íntegro noetheriano local, de dimensión 1 y normal; luego es un DIP local. Así, todo ideal fraccionario no nulo es principal en las localizaciones y luego es inversible por la proposición 4.21.

Claramente 2 $\implies$ 2′ por el teorema 4.17. Y 2′ $\implies$ 2 puesto que, por el teorema 2.22 se ve que A es normal, para cualquier $\mathfrak{m} \lhd A$ se cumple que $k.\dim A = k.\dim(A_{\mathfrak{m}})$ y si $A_{\mathfrak{m}}$ es dominio de valuación discreta, entonces $k.\dim(A_{\mathfrak{m}}) = 1$ y, finalmente, A es noetheriano pues tiene dimensión finita.

1 $\implies$ 3. Si $\mathfrak{a} = A$, entonces puede verse como un producto vacío y si $\mathfrak{a}$ es primo, entonces le consideramos como el producto de sí mismo. Como A es noetheriano podemos emplear inducción sobre cadenas descendentes: sea $\mathfrak{a}$ tal que todo ideal $\mathfrak{b} \supset \mathfrak{a}$ se escribe como producto de ideales primos. Sea $\mathfrak{p} \supseteq \mathfrak{a}$ maximal, luego $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq A$. Si $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, entonces como $\mathfrak{p}^{-1}\mathfrak{p} = A$, entonces $\mathfrak{a}\mathfrak{p} = \mathfrak{a}$, lo cual es absurdo por el lema de Nakayama. Así que $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$, y por inducción, $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, luego $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_m \cdot \mathfrak{p}$.

3 $\implies$ 1. Ésta demostración es por pasos:

(i) Sean I, J ideales fraccionarios. I, J son inversibles syss IJ lo es: Claramente $\implies$, veamos $\impliedby$. Sea $L := IJ$, entonces $A = L^{-1}L$. Como $J^{-1}I^{-1}L \subseteq A$, entonces $J^{-1}I^{-1} \subseteq L^{-1}$. Como $L^{-1}IJ \subseteq A$, entonces $L^{-1}I \subseteq J^{-1}$ y análogamente $L^{-1}J \subseteq I^{-1}$. Por ello, $L^{-1} = L^{-1}(L^{-1}IJ) \subseteq J^{-1}I^{-1}$ y se alcanza igualdad.

Así pues, finalmente nótese que

$$A = L^{-1}L = (I^{-1}I)(J^{-1}J),$$

donde $I^{-1}I, J^{-1}J \trianglelefteq A$; por lo que ambos ideales deben ser A, de lo contrario hay inclusiones estrictas.

(ii) Sea $\mathfrak{p}$ un ideal primo no nulo. Si $\mathfrak{a} \supset \mathfrak{p}$, entonces $\mathfrak{a}\mathfrak{p} = \mathfrak{p}$: Basta probarlo para ideales de la forma $\mathfrak{a} = \mathfrak{p} + (a)$, donde $a \notin \mathfrak{p}$. Basta demostrar la inclusión $\mathfrak{p} \subseteq \mathfrak{a}\mathfrak{p}$. Considere $\mathfrak{a}^2 = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ y $(a^2) + \mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, donde $\mathfrak{p}_i, \mathfrak{q}_j$ son ideales primos. Nótese que cada $\mathfrak{p}_i, \mathfrak{q}_j$ contiene estrictamente a $\mathfrak{p}$ (¿por qué?). Sea $\bar{A} := A/\mathfrak{p}$ y denotemos por $\overline{()}$ la proyección de los ideales en $\bar{A}$. Luego

$$\bar{\mathfrak{p}}_1 \cdots \bar{\mathfrak{p}}_n = \bar{a}^2\bar{A} = \bar{\mathfrak{q}}_1 \cdots \bar{\mathfrak{q}}_m. \tag{4.3}$$

Como los ideales principales son inversibles, empleando el paso anterior, concluimos que cada $\bar{\mathfrak{p}}_i, \bar{\mathfrak{q}}_j$ es inversible y, además, es un ideal primo (¿por qué?). Tras reordenar supongamos que $\bar{\mathfrak{p}}_1$ es minimal entre los $\bar{\mathfrak{p}}_i$ y por evitamiento de primos (proposición **??**) vemos que, tras reordenar, $\bar{\mathfrak{q}}_1 \subseteq \bar{\mathfrak{p}}_1$. Empleando otra vez evitamiento de primos llegamos a que $\bar{\mathfrak{p}}_i \subseteq \bar{\mathfrak{q}}_1 \subseteq \bar{\mathfrak{p}}_1$, con lo que, por minimalidad, $\bar{\mathfrak{q}}_1 = \bar{\mathfrak{p}}_1$.

Multiplicando ambos lados de (4.3) por $\bar{\mathfrak{p}}_1^{-1}$, obtenemos que $\bar{\mathfrak{p}}_2 \cdots \bar{\mathfrak{p}}_n = \bar{\mathfrak{q}}_2 \cdots \bar{\mathfrak{q}}_m$. Por inducción obtenemos que $n = m$ y que los productos son los mismos salvo permutación. Como los $\mathfrak{p}_i, \mathfrak{q}_j$'s contenían a $\mathfrak{p}$, entonces salvo reordenar concluimos que $\mathfrak{p}_i = \mathfrak{q}_i$, y así $\mathfrak{p} + (a^2) = \big(\mathfrak{p} + (a)\big)^2 = \mathfrak{p}^2 + a\mathfrak{p} + (a)$. Luego para todo $b \in \mathfrak{p}$, vemos que

$$b = c + ad + a^2e, \qquad c \in \mathfrak{p}^2, d \in \mathfrak{p}, e \in A.$$

Como $a \notin \mathfrak{p}$, entonces $e \in \mathfrak{p}$. Luego $\mathfrak{p} \subseteq (\mathfrak{p} + (a))\mathfrak{p} = \mathfrak{a}\mathfrak{p}$.

(iii) Dado $a \in A_{\neq 0}$, toda factorización $aA = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ es tal que los $\mathfrak{p}_i$'s son maximales. En efecto, los $\mathfrak{p}_i$'s son inversibles por el paso 1, y si $\mathfrak{a} \supset \mathfrak{p}_i$, entonces $\mathfrak{a}\mathfrak{p}_i = \mathfrak{p}_i$ por el paso anterior, luego $\mathfrak{a} = A$.

(iv) Sea $\mathfrak{p} \lhd A$ un ideal primo no nulo, $a \in \mathfrak{p}_{\neq 0}$. Dada una factorización $aA = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, entonces $\mathfrak{p}_i \subseteq \mathfrak{p}$ y por el paso anterior $\mathfrak{p}_i$'s son maximales, así que $\mathfrak{p}$ también y es inversible por el paso (i) . Así, concluimos que todo ideal primo no nulo es inversible, y luego los ideales fraccionarios no nulos también. □

Ahora veremos la propiedad fundamental de los dominios de Dedekind:

Proposición 4.26: En un dominio de Dedekind A, los ideales fraccionarios no nulos forman un grupo abeliano J_A y los ideales fraccionarios no nulos principales P_A un subgrupo.

Proposición 4.27: Sea A un dominio íntegro noetheriano de $k.\dim A = 1$. Entonces todo ideal no nulo puede expresarse de manera única como producto de ideales primarios de radicales distintos.

Demostración: Sea $\mathfrak{a} \lhd A$ un ideal impropio, por el teorema A.14 se cumple que $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$, donde $\mathfrak{q}_i$ es $\mathfrak{p}_i$-primario. Como $k.\dim A = 1$ y A es un dominio íntegro, entonces todo ideal primo es maximal, luegos los $\mathfrak{p}_i$'s son ideales maximales distintos, y por ende, son coprimos. Luego, como los radicales de los $\mathfrak{q}_i$'s son coprimos, entonces ellos lo son y por el teorema chino del resto se cumple que

$$\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i = \prod_{i=1}^n \mathfrak{q}_i.$$

Para ver la unicidad, supongamos que $\mathfrak{a} = \prod_{i=1}^m \mathfrak{r}_i$, de modo que por el mismo argumento, $\mathfrak{a} = \bigcap_{i=1}^m \mathfrak{r}_i$, donde los $\mathfrak{r}_i$'s conforman una familia aislada, luego se concluye por unicidad de la representación (teorema A.15). □

Nótese que el anillo A de la hipótesis anterior puede no ser de Dedekind, puesto que podría no ser normal.

Proposición 4.28: En un dominio de Dedekind A, un ideal entero $\mathfrak{q} \lhd A$ que es $\mathfrak{p}$-primario, donde $\mathfrak{p}$ es un ideal primo no nulo, es de la forma $\mathfrak{p}^n$ para algún $n \in \mathbb{N}$.

Demostración: En primer lugar, si $\mathfrak{q}$ es $\mathfrak{p}$-primario, entonces por el teorema A.14, vemos que $\mathfrak{q} = \mathfrak{q}_\mathfrak{p} \cap A$ y $\mathfrak{q}_\mathfrak{p} \lhd A_\mathfrak{p}$ es $\mathfrak{p}A_\mathfrak{p}$-primario, donde $A_\mathfrak{p}$ es dominio de valuación discreta, luego por el teorema 4.18, vemos que $\mathfrak{q}_\mathfrak{p} = \mathfrak{p}^n A_\mathfrak{p}$ para algún $n \in \mathbb{N}$ y $\mathfrak{p}^n A_\mathfrak{p} \cap A = \mathfrak{p}^n$. □

Teorema 4.29: En un dominio de Dedekind, todo ideal fraccionario no nulo $I \in J_A$ se escribe forma única (salvo permutación) como

$$I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n},$$

donde los $\mathfrak{p}_i$'s son ideales primos distintos, cada $\alpha_i \in \mathbb{Z}_{\neq 0}$.

Corolario 4.29.1: En un dominio de Dedekind A, el grupo de los ideales fraccionarios no nulos J_A es un grupo abeliano libre que tiene por base los ideales primos.

Claramente, los ideales fraccionarios principales forman un subgrupo, así que:

Definición 4.30: Dado un dominio de Dedekind A, se define su ***grupo de clases de ideales*** o ***grupo de Picard*** al cociente:

$$\mathrm{Pic}(A) := J_A/P_A.$$

En la teoría algebraica de números se estudian ejemplos de dominios de Dedekind y se calculan explícitamente sus grupos de Picard.

Veamos otra consecuencia de la factorización única de ideales:

Corolario 4.30.1: Sea A un dominio de Dedekind. Son equivalentes:

1. A es un DIP.
2. Cada ideal primo es principal.
3. A es un DFU.

Incluímos otra discusión de dominios de Dedekind en la sección §5.3.1 de **[45].** En particular el **[45,** teo. 5.48] ofrece otra prueba mediante álgebra homológica de que un dominio de Dedekind es DIP syss es DFU.

Teorema 4.31: Un dominio de Dedekind con finitos primos es un DIP.

Demostración: Sea A un dominio de Dedekind. Si no posee primos no nulos, es un cuerpo y es trivialmente un DIP. De lo contrario, sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ todos los ideales primos no nulos. Por el teorema chino del resto, la proyección:

$$A \twoheadrightarrow A/\mathfrak{p}_1^2 \times A/\mathfrak{p}_2 \times \cdots \times A/\mathfrak{p}_n$$

es suprayectiva, luego existe $a \in A$ tal que

$$a \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2, \qquad \forall j \neq n \quad a \notin \mathfrak{p}_j.$$

Sea $\mathfrak{a} := (a)$, entonces vemos que $\mathfrak{a} \subseteq \mathfrak{p}_1$, pero $\mathfrak{a} \not\subseteq \mathfrak{p}_1^2$ y $\mathfrak{a} \not\subseteq \mathfrak{p}_j$ para $j \neq 1$, así que la factorización única de primos demuestra que $(a) = \mathfrak{a} = \mathfrak{p}_1$. Análogamente se prueba que todos los $\mathfrak{p}_j$'s son principales y, por el corolario anterior, A es DFU. □

§4.1.1 Extensiones de dominios de Dedekind. Veremos dos métodos para estudiar extensiones de dominios de Dedekind.

Lema 4.32: Sea A un dominio de valuación discreta, $K := \operatorname{Frac} A$ y L/K una extensión de cuerpos tal que $L^q \subseteq K$ para algún q. Entonces $B := \mathcal{O}_{L/A}$ es un dominio de valuación discreta.

Demostración: En primer lugar veremos que B es local. Sea $\mathfrak{p} \lhd B$ un ideal primo tal que $\mathfrak{m} := \mathfrak{p} \cap A \lhd A$ es el único ideal maximal. Sea $S := A \setminus \mathfrak{m}$, sabemos que $A = A_{\mathfrak{m}} = S^{-1}A$, que $S^{-1}L = L$, así que la clausura íntegra de A en L es $S^{-1}B$. Veremos que $S^{-1}B = B_{\mathfrak{p}}$, la inclusión $\subseteq$ es obvia. Sea $\alpha/\beta \in B_{\mathfrak{p}}$, donde $\beta \notin \mathfrak{p}$, luego $\beta^q \in A$ y $\beta^q \notin \mathfrak{m}$, por lo que $\alpha/\beta = \alpha\beta^{q-1}/\beta^q \in S^{-1}B$.

Sea π un uniformizador de A y $\mathfrak{m} \lhd B$ su único ideal maximal, luego $\mathfrak{m}^q \lhd A$ es un ideal propio de A y, por lo tanto, es de la forma $\mathfrak{m}^q = \pi^n A$ para algún $n > 0$. Sea $\alpha \in \mathfrak{m}$ tal que $\alpha^q = \pi^n$, veremos que $\alpha B = \mathfrak{m}$: Sea $\beta \in B$, luego $\beta^q = u\pi^d$ para algunos $u \in A^\times$ y $d \in \mathbb{N}$ Sea $d = nt + r$ con $0 \leq r < n$, entonces $(\beta\alpha^{-t})^q = u\pi^d\pi^{-nt} = u\pi^r \in A$, de lo que concluimos que $\beta\alpha^{-t} \in B$ y claramente $\beta\alpha^{-t} \notin \mathfrak{m}$, por lo que $w := \beta\alpha^{-t}$ es inversible. Así $\beta = w\alpha^t$ para unos únicos $w \in B^\times$ y $t \in \mathbb{N}$, y es fácil notar que B es un dominio de valuación discreta. □

Teorema 4.33: Sea A un dominio de Dedekind, $K := \operatorname{Frac} A$ y L/K una extensión finita de cuerpos. Sea B la clausura íntegra de A en L, entonces B es un dominio de Dedekind.

Demostración: Sea L_s la clausura separable de L y sea C la clausura íntegra de A en L_s. Nótese que B es la clausura íntegra de C en L, así que podemos separar la demostración en el caso de extensiones separables y puramente inseparables.

Probaremos que B es noetheriano, normal y de dimensión 1 por el teorema 4.25. Claramente B es normal por definición de clausura íntegra. Y para ver que tiene dimensión 1 basta invocar el teorema 2.26.

El hecho de que B sea noetheriano lo separaremos en dos casos:

(a) L es separable: Entonces B es un A-módulo finitamente generado por la proposición 2.48, y luego es un A-módulo noetheriano; en particular es noetheriano como anillo.

(b) L es puramente inseparable: En éste caso, directamente consideraremos un ideal $\mathfrak{n} \lhd B$ maximal y veremos que $B_{\mathfrak{n}}$ es un dominio de valuación discreta. Para ello, sea $\mathfrak{m} := \mathfrak{n} \cap A$ el cual es maximal, y nótese que $A_{\mathfrak{m}}$ es un dominio de valuación discreta. Por lo anterior, es fácil notar que $B_{\mathfrak{n}}$ es la clausura íntegra de $A_{\mathfrak{m}}$, así que es un dominio de valuación discreta como se quería ver. □

El teorema anterior lo podemos mejorar ligeramente haciendo un estudio más minucioso.

Lema 4.34: Sea A un dominio íntegro noetheriano de $k.\dim A = 1$, sea $K := \operatorname{Frac} A$ y sea M un A-módulo libre de torsión tal que $\dim_K(M \otimes_A K) =: d < \infty$. Entonces, para todo $a \in A_{\neq 0}$ se tiene que

$$\ell(M/aM) \leq d \cdot \ell(A/aA).$$

Demostración: Veremos dos casos:

(a) M es finitamente generado: Sean $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_d \in M$ tales que son A-linealmente independientes y definamos $E := \sum_{i=1}^{d} \boldsymbol{u}_i A$. Así, para todo $\boldsymbol{v} \in M$ existe $a \in A_{\neq 0}$ tal que $a\boldsymbol{v} \in E$. Sea $C := M/E$, el cual también es un A-módulo finitamente generado, y luego existe $a \in A_{\neq 0}$ tal que $a \cdot C = 0$ (¿por qué?). Luego por el corolario A.9.1 existe una cadena de submódulos

$$0 = C_0 \subset C_1 \subset \cdots \subset C_m = C,$$

donde cada $C_i/C_{i-1} \cong A/\mathfrak{p}_i$, donde los $\mathfrak{p}_i$'s necesariamente son maximales. Luego $\ell(C) = m < \infty$ y para todo $a \in A_{\neq 0}$ y todo $n \in \mathbb{N}$ tenemos la sucesión exacta:

$$E/a^n E \longrightarrow M/a^n M \longrightarrow N/a^n N \longrightarrow 0$$

que induce que $\ell(M/a^nM) \leq \ell(E/a^nE) + \ell(C)$.

Ahora bien, es claro que $a^iM/a^{i+1}M \cong M/a$, por lo que, obtenemos que $n\ell(M/aM) \leq n\ell(E/aE) + \ell(C)$ y, tirando límites, se ve que necesariamente $\ell(M/aM) \leq \ell(E/aE)$. Nótese que $E \cong A^d$, de modo que $\ell(E/aE) = d\ell(A/aA)$ como se quería probar.

(b) Caso general: Denotemos $\overline{M} := M/aM$ y sea $\overline{N} = \sum_{i=1}^r A\bar{u}_i \leq \overline{M}$, donde $\bar{u}_i$ es la proyección de algunos $u_i \in M$. Sea $M_1 := \sum_{i=1}^r Au_i$, entonces por el caso anterior, se tiene:

$$\ell\left(\sum_{i=1}^r A\bar{u}_i\right) = \ell\left(\frac{M_1}{M_1 \cap aM}\right) \leq \ell(M_1/aM_1) \leq d\ell(A/aA).$$

Finalmente, como el lado derecho es independiente del $\overline{N}$, por lo que, se comprueba la desigualdad. □

Teorema 4.35 (Krull-Akizuki): Sea A un dominio íntegro noetheriano de $k.\dim A = 1$, sea $K := \operatorname{Frac} A$, sea L/K una extensión finita de cuerpos y sea $A \subseteq B \subseteq L$ un subanillo. Entonces B es noetheriano de $k.\dim B \leq 1$ y para todo ideal $\mathfrak{b} \trianglelefteq B$ no nulo, $B/\mathfrak{b}$ es un A-módulo artiniano de longitud finita.

Demostración: Reemplacemos L por $\operatorname{Frac} B$ y fijemos $d := [L : K]$. Así B es un A-módulo libre de torsión y se cumple que $\ell_A(B/aB) < \infty$. Sea $\mathfrak{b} \trianglelefteq B$ un ideal no nulo, dado $\beta \in \mathfrak{b}_{\neq 0}$ se cumple que es K-algebraico, luego se satisface que

$$c_n\beta^n + c_{n-1}\beta^{n-1} + \cdots + c_1\beta + c_0 = 0$$

con $c_i \in A$ y, como es un dominio íntegro, podemos suponer que $c_0 \neq 0$. Así, notamos que $a := c_0 \in \mathfrak{b} \cap A$, luego

$$\ell_A(B/\mathfrak{b}) \leq \ell_A(B/aB) < \infty.$$

Más aún, como $\ell_B(\mathfrak{b}/aB) \leq \ell_A(\mathfrak{b}/aB) \leq \ell_A(B/aB) < \infty$ vemos que $\mathfrak{b}/aB$ es un B-módulo finitamente generado, luego $\mathfrak{b}$ es finitamente generado y así B es noetheriano. Sea $\mathfrak{p} \lhd B$ un primo no nulo, luego hemos visto que $\ell_B(B/\mathfrak{p}) < \infty$, así que $B/\mathfrak{p}$ es un B-módulo artiniano, luego un anillo artiniano y un dominio íntegro, es decir, un cuerpo, por lo que, $\mathfrak{p}$ es maximal; y así concluimos que $k.\dim B \leq 1$. □

Corolario 4.35.1: Sea A un dominio íntegro noetheriano de $k.\dim A = 1$, sea $K := \operatorname{Frac} A$ y sea L/K una extensión finita de cuerpos. Entonces $B := \mathcal{O}_{L/A}$ es un dominio de Dedekind.

§4.1.2 Lema de Hensel y anillos henselianos. El llamado lema de Hensel es una de las herramientas más importantes en teoría de cuerpos de clases y ha probado ser de extrema utilidad. En primer lugar introducimos un glosario de las distintas versiones en las que se puede encontrar el lema de Hensel:

Teorema 4.36: Sea $(A, \mathfrak{m}, k)$ un anillo local y fijemos $|\,| := |\,|_{\mathfrak{m}}$ el valor absoluto $\mathfrak{m}$-ádico. Son equivalentes:

1. Sea $f(x) \in A[x]$ mónico. Si existe a_0 tal que $f(a_0) \equiv 0 \pmod{\mathfrak{m}}$, entonces existe $a \equiv a_0 \pmod{\mathfrak{m}}$ tal que $f(a) = 0$.
2. Sea $f(x) \in A[x]$ mónico. Si existe a_0 tal que $|f(a_0)| < 1$ y $|f'(a_0)| = 1$, entonces existe $a \equiv a_0 \pmod{\mathfrak{m}}$ tal que $f(a) = 0$.
3. Sea $f(x) \in A[x]$ mónico. Si existe a_0 tal que $|f(b)| < |f'(b)|^2$, entonces existe un único $a \in A$ tal que $f(a) = 0$ y $|a - b| < |f'(b)|$.
4. Sea $f(x) \in A[x]$ mónico. Si $f \equiv g_0 h_0 \pmod{\mathfrak{m}}$ con g_0 mónico y $g_0, h_0 \in k[x]$ coprimos (en $k[x]$), entonces existen $g, h \in A[x]$ tales que $f = gh$, $g \equiv g_0$ y $h \equiv h_0 \pmod{\mathfrak{m}}$.

Teorema 4.37 – *Lema de Hensel*: Dado un cuerpo métrico no-arquimediano completo k. Su anillo de valuación $\mathfrak{o}$ es henseliano.

Demostración: Sean $f_j(x) \in \mathfrak{o}[x]$ polinomios tales que

$$f(x+y) = f(x) + f_1(x)y + f_2(x)y^2 + \cdots \in \mathfrak{o}[x, y],$$

donde los f_i's vendrán dados por expandir un binomio de Newton en cada monomio original. Se puede comprobar que $f_1(x) = f'(x)$. Luego, por el enunciado, existe $b_0 \in \mathfrak{o}$ tal que

$$f(a_0) + b_0 f_1(a_0) = 0,$$

luego, definamos $a_1 := a_0 + b_0$ y notemos que por desigualdad ultramétrica

$$|f(a_1)| = |f(a_0 + b_0)| \leq \max_{j \geq 2} |f_j(a_0) b_0^j|,$$

como $f_j(a_0) \in \mathfrak{o}$ entonces $|f_j(a_0)| \leq 1$, luego

$$|f(a_1)| \leq |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2} < |f(a_0)|,$$

además de que $|b_0| < |f'(a_0)|$. Del mismo modo se nota que

$$|f'(a_1) - f'(a_0)| \leq |b_0| < |f'(a_0)|.$$

Luego se cumple que $|f'(a_1)| = |f'(a_0)|$. Ahora podemos volver a elegir un b_1 con las mismas propiedades, en particular, notando que $|f(a_1)| < |f(a_0)| \leq |f'(a_0)|^2 = |f'(a_1)|^2$, y así recursivamente comprobamos que

$$|f(a_{n+1})| \leq |b_n|^2 = \frac{|f(a_n)|^2}{|f'(a_n)|^2} = \frac{|f(a_n)|^2}{|f'(a_0)|^2},$$

como $|f'(a_0)|^2$ es solo una constante, entonces vemos que $|f(a_n)| \to 0$ y luego, por la igualdad superior, $b_n \to 0$, de modo que $(a_n)_n$ es una sucesión fundamental que converge a una raíz de f (¿por qué está en $\mathfrak{o}$?). □

Lema 4.38: Sea K un cuerpo, con $A \subseteq K$ de valuación y sea $\alpha \in K^\times$. Sea $\mathfrak{m}$ el ideal maximal de A, entonces $\mathfrak{m}[\alpha] \neq A[\alpha]$ o $\mathfrak{m}[\alpha^{-1}] \neq A[\alpha^{-1}]$.

Demostración: Procedamos por contradicción: Si $\mathfrak{m}[\alpha] = A[\alpha]$ y $\mathfrak{m}[\alpha^{-1}] = A[\alpha^{-1}]$, entonces se cumple que $1 \in \mathfrak{m}[\alpha] \cap \mathfrak{m}[\alpha^{-1}]$, vale decir

$$\begin{aligned} u_0 + u_1\alpha + \cdots + u_n\alpha^n &= 1 \\ v_0 + v_1\alpha^{-1} + \cdots + v_m\alpha^{-m} &= 1 \end{aligned} \tag{4.4}$$

para algunos $u_i, v_i \in \mathfrak{m}$. Podemos asumir que n, m son los mínimos exponentes para los que se cumple lo anterior y que $n \geq m$ (de lo contrario, sustituimos «α» por «α^{-1}») luego podemos reescribir la segunda fórmula a que

$$(1 - v_0)\alpha^m = v_1\alpha^{m-1} + \cdots + v_{m-1}\alpha + v_m,$$

como $\mathfrak{m}$ es el único anillo maximal de A, entonces $1 - v_0 \in A^\times$, luego dividiendo por dicho término y multiplicando por α^{n-m} se obtiene que:

$$\alpha^n = w_0\alpha^{n-m} + w_1\alpha^{n-m+1} + \cdots + w_m\alpha^{n-1},$$

sustituyendo en (4.4) se obtiene una expresión con grado menor, lo que contradice la minimalidad de n. □

Lema (AE) 4.39: Sea K un cuerpo y L un cuerpo algebraicamente cerrado. Entonces K posee un subanillo propio A con un homomorfismo $f\colon A \to L$ tal que A es de valuación y es un subanillo maximal que satisface éstas propiedades.

Demostración: Emplearemos el lema de Zorn: sea $\mathcal{F}$ la familia de los pares (B, g) donde $g\colon B \to L$ es un homomorfismo. Se denota que

$$(B_1, g_1) \preceq (B_2, g_2) \iff B_1 \subseteq B_2 \wedge g_2 \restriction B_1 = g_1.$$

Sea $\{(B_i, g_i)\}_{i\in I}$ una $\preceq$-cadena, luego nótese que

$$B := \bigcup_{i\in I} B_i, \qquad g := \bigcup_{i\in I} g_i.$$

la cual está bien definida pues los g_i's son compatibles por ser cadena, y además claramente es un homomorfismo desde B a L, como se quería comprobar.

Finalmente, por lema de Zorn, $\mathcal{F}$ posee un elemento $\preceq$-maximal (A, f). Nótese que $f[A]$ es un subanillo de L, luego es un dominio íntegro; definiendo $\mathfrak{m} := \ker f$, por el primer teorema de isomorfismos se cumple que $f[A] \cong A/\mathfrak{m}$, luego $\mathfrak{m}$ es un ideal primo. Por la propiedad universal de la localización se satisface que $\bar{f}\colon A_{\mathfrak{m}} \to L$ con $A_{\mathfrak{m}} \subseteq K$, pero por maximalidad de A se concluye que $A = A_{\mathfrak{m}}$, luego A es local y $\mathfrak{m}$ es su ideal maximal. □

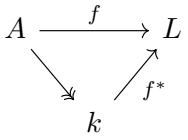
Teorema (AE) 4.40: Sea K un cuerpo, entonces existe $A \subset K$ anillo de valuación con $\mathrm{Frac}(A) = K$.

Demostración: Por el lema anterior, sea A el anillo construído y sea $\mathfrak{m}$ su anillo maximal. Hay que probar que $\mathrm{Frac}(A) = K$: Sea $\alpha \in K^\times$, entonces por el lema previo al anterior y sin perdida de generalidad se satisface que

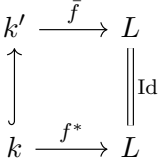
$$\mathfrak{m}[\alpha] \subset A[\alpha] =: A'.$$

Por teorema de Krull se cumple que $\mathfrak{m}[\alpha] \subseteq \mathfrak{m}' \lhd A'$. Definamos $k := A/\mathfrak{m}$ y $k' := A'/\mathfrak{m}'$ los cuales son cuerpos; nótese que $k' = k[\overline{\alpha}]$, donde $\overline{\alpha}$ es la proyección de α en k (por ser un cociente); más aún, como los anillos de valuación son íntegramente cerrados, entonces k'/k es una extensión finita.

Por el primer teorema de isomorfismos, y recordando que $\mathfrak{m} = \ker f$ se tiene que el siguiente diagrama conmuta:



así mismo, como k'/k es finita y L es normal, entonces:

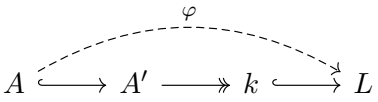


Pre-componiendo $\bar{f}$ con la proyección obtenemos $\pi \circ \bar{f} \colon A' \to L$ la cual extiende a $f \colon A \to L$, lo que, por maximalidad, implica que $A = A'$ y por ende $\alpha \in A$ como se quería probar. □

Corolario (AE) 4.40.1: Sea K un cuerpo, y $A \subseteq K$ un subanillo. Entonces, la clausura íntegra C de A en K es la intersección de todos los anillos de valuación contenidos en K que contienen a A.

Demostración: Sea $A \subseteq V \subseteq K$ con V de valuación, luego como V es íntegramente cerrado, entonces $C \subseteq V$.

Sea $\alpha \notin C$, luego como α no es entero sobre A, se cumple que $\alpha \notin A[\alpha^{-1}] =: A'$; es decir, α^{-1} no es inversible en A', por lo que, por el teorema de Krull está contenido en un ideal maximal $\mathfrak{m} \lhd A'$. Definamos $k := A'/\mathfrak{m}$, luego podemos definir L como la clausura algebraica de L y luego tenemos el siguiente homomorfismo de anillos:



Siguiendo el proceso del lema y teorema anteriores podemos extender $A \subseteq V$ y $\varphi^* \colon V \to L$ tal que V es de valuación. Como $\varphi(\alpha^{-1}) = 0$, entonces $\alpha \notin V$. □

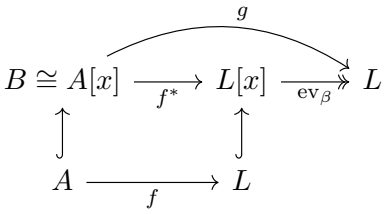
Proposición (AE) 4.41: Sea B/A una extensión de dominios íntegros con B una A-álgebra de tipo finito. Sea $v \in B_{\neq 0}$ existe un $u \in A_{\neq 0}$ tal que todo homomorfismo de anillos $f \colon A \to L$ con L un cuerpo algebraicamente cerrado y con $f(u) \neq 0$ se puede extender a $g \colon B \to L$ tal que $g(v) \neq 0$.

Demostración: Por inducción sobre la cantidad minimal de generadores de B como A-álgebra podemos reducirlo al caso $B = A[\alpha]$.

(a) $\underline{\alpha \text{ es trascendente:}}$ Sea $v = c_n\alpha^n + \cdots + c_1\alpha + c_0$ con $c_i \in A$; definamos $u := c_n$. Como L es algebraicamente cerrado, entonces es infinito y así existe β tal que

$$f(c_n)\beta^n + \cdots + f(c_1)\beta + f(c_0) \neq 0.$$

Como $B \cong A[x]$ (el anillo de polinomios), entonces considere el siguiente diagrama:



Luego g satisface lo requerido.

(b) $\underline{\alpha \text{ es algebraico:}}$ Luego tomando $k := \mathrm{Frac}(A)$, entonces como α es algebraico, se cumple que $\alpha, v^{-1} \in k(\alpha)$ son algebraicos. Por la proposición 2.4 se satisface que $c\alpha, c'v^{-1}$ son enteros sobre A para algunos $c, c' \in A$, luego:

$$a_n\alpha^n + \cdots + a_1\alpha + c_0 = 0$$
$$b_m v^{-m} + \cdots + b_1 v^{-1} + b_0 = 0$$

definamos $u := a_n b_m$. Si $f\colon A \to L$ es un homomorfismo de anillos con $f(u) \neq 0$, entonces podemos extender la función a $f_1\colon A[u^{-1}] \to L$. Más aún, por el teorema anterior se puede extender a $f_2\colon V \to L$, donde V es de valuación. Como $a_n^{-1} = a_n u^{-1} \in A[u^{-1}]$, entonces α es entero en $A[u^{-1}]$, análogamente v^{-1} también. Como V es íntegramente cerrado, entonces $\alpha, v^{-1} \in V$. Además como B/A es entero, entonces $v \in V$, luego $v \in V^\times$ y por tanto $f_2(v) \neq 0$. □

Aquí damos la tercera demostración del lema del teorema (débil) de ceros de Hilbert:

Corolario (AE) 4.41.1: Sea L/k una extensión de cuerpos con L una k-álgebra de tipo finito. Entonces L/k es una extensión finita.

4.2 Dominios de valuación discreta y de Dedekind

Lema 4.42: Sea A un dominio íntegro noetheriano de dimensión 1. Entonces son equivalentes:

1. A es íntegramente cerrado.
2. Todo ideal $\mathfrak{p}$-primario es de la forma $\mathfrak{p}^n$.
3. Toda localización $A_\mathfrak{p}$, con $\mathfrak{p} \neq (0)$, es un dominio de valuación discreta.

Demostración: $1 \iff 3$. Por el teorema anterior y la proposición 4.2.
$2 \iff 3$. Aplicar el teorema anterior, y el hecho de que hay una correspondencia entre ideales primos tras localizar, y $\mathfrak{p}$-primarios. □

Definición 4.43: Se le llama un ***dominio de Dedekind*** a un dominio que satisfaga cualquiera de las condiciones del lema anterior.

Ejemplo. $\mathbb{Z}$ es un dominio de Dedekind y más generalmente todo DIP es de Dedekind. Nótese que los cuerpos *no* son dominios de Dedekind, puesto que tienen dimensión 0.

Corolario 4.43.1: En un dominio de valuación discreta, todo ideal puede escribirse de manera única como producto de ideales primos.

Definición 4.44: Un ***cuerpo de números*** es una extensión finita $K/\mathbb{Q}$, y su ***anillo de enteros*** es la clausura íntegra de $\mathbb{Z}$ en K.

Teorema 4.45: El anillo de enteros A de un cuerpo de números algebraicos K es un dominio de Dedekind.

Demostración: Como $A \subseteq K$ que es un cuerpo, entonces A es un dominio íntegro. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una $\mathbb{Q}$-base de K, entonces $A \subseteq \sum_{i=1}^n \mathbb{Z}\alpha_i$, de modo que A es un $\mathbb{Z}$-módulo finitamente generado, por tanto es noetheriano. Finalmente, sea $\mathfrak{p} \lhd A$ primo no nulo, luego $\mathfrak{p}^c \subseteq \mathbb{Z}$ es primo y por el corolario 2.18.2 se satisface que es no vacío en $\mathbb{Z}$, luego su contracción es maximal, así que por el colorario 2.18.1 se cumple que $\mathfrak{p}$ es maximal. □

Definición 4.46: Sea A un dominio íntegro y $K := \operatorname{Frac} A$. Se dice que un A-submódulo M de K es un ***ideal fraccionario*** si existe algún $x \in A_{\neq 0}$

tal que $xM \subseteq A$. A los ideales de A (en sentido usual) les diremos ***ideales enteros***. Si $M = yA$ para algún $y \in K$, entonces M se dice un ***ideal principal***. Para un A-submódulo M se define:

$$(A : M) := \{x \in A : xM \subseteq A\}.$$

(Nótese que M es fraccionario syss $(A : M) = (0)$.)

Un A-submódulo M se dice ***inversible*** si existe otro A-submódulo N tal que $MN = A$.

Proposición 4.47: Sea A un dominio íntegro local. Entonces A es un dominio de valuación discreta syss todo ideal fraccionario no nulo es inversible.

Demostración: $\Longrightarrow$. Sea $\mathfrak{m} \lhd A$ maximal, luego $\mathfrak{m} = (x)$. Sea $M \neq (0)$ un ideal fraccionario, como $(A : M)$ es un ideal entero, entonces $(A : M) = (y)$ y $M \cdot (A : M) \subseteq A$ el cual también es un ideal entero, entonces sea $(x^r) = M \cdot (A : M)$. También sea $v(y) = s$, entonces finalmente $M = (x^{r-s})$.

$\Longleftarrow$. Si todo ideal fraccionario fuese inversible, entonces sería finitamente generado, luego A es noetheriano. Hay que probar que todo ideal entero es potencia de $\mathfrak{m}$ maximal. De lo contrario, empleando el lema de Zorn, existiría $\mathfrak{a}$ maximal en la familia de los que no son una potencia de $\mathfrak{m}$. Luego $\mathfrak{a} \subset \mathfrak{m}$ y

$$\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{m} = A,$$

por lo que $\mathfrak{m}^{-1}\mathfrak{a}$ es un ideal impropio entero y $\mathfrak{m}^{-1}\mathfrak{a} \supset \mathfrak{a}$. Si $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a}$, entonces $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$ y por el lema de Nakayama $\mathfrak{a} = (0)$. Si no, $\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{a}$ y entonces $\mathfrak{m}^{-1}\mathfrak{a}$ es una potencia de $\mathfrak{m}$ lo que es absurdo. □

Teorema 4.48: Sea A un dominio íntegro. Entonces A es de Dedekind syss todo ideal fraccionario no nulo es inversible.

Demostración: $\Longrightarrow$. Sea M un ideal fraccionario no nulo y sea $\mathfrak{m} \lhd A$ maximal. Luego $A_{\mathfrak{m}}$ es un dominio de valuación discreta y $M_{\mathfrak{m}}$ es inversible. Finalmente, como A es noetheriano, se concluye que M es inversible.

$\Longleftarrow$. Si todo ideal entero es inversible, entonces es finitamente generado, por lo que A es noetheriano. Sea $A_{\mathfrak{p}}$ y sea $(0) \neq \mathfrak{b} \lhd A_{\mathfrak{p}}$. Luego $\mathfrak{a} := \mathfrak{b}^c = \mathfrak{b} \cap A$ es inversible, luego $\mathfrak{b} = \mathfrak{a}_{\mathfrak{p}}$ también y por la proposición anterior, $A_{\mathfrak{p}}$ es un dominio de valuación discreta, y por tanto, A es de Dedekind. □

Corolario 4.48.1: Sea A un dominio de Dedekind. Entonces los ideales fraccionarios no nulos de A forman un grupo.

5

Profundidad

En éste capítulo se introduce la noción fundamental de *profundidad* y, con ella, la de nuevas clases de anillos. Éste capítulo comienza a depender de métodos homológicos.

5.1 Sucesiones regulares

Definición 5.1: Sea M un A-módulo. Se dice que un elemento $a \in A$ es M***-regular*** si $au \neq 0$ cuando $u \in M_{\neq 0}$. Una tupla de elementos $a_1, a_2, \ldots, a_n$ conforma una ***sucesión*** M***-regular*** si:

SR1. a_1 es M-regular y cada a_r es $M/(a_1, \ldots, a_{r-1})M$-regular.

SR2. $M \neq (a_1, a_2, \ldots, a_n)M$.

Si $a_1, a_2, \ldots, a_n$ satisface SR1, pero no necesariamente SR2, entonces se dice ***débilmente*** M***-regular***. Si $\mathfrak{a} \trianglelefteq A$ es un ideal tal que $\mathfrak{a} \supseteq (a_1, \ldots, a_n)$, entonces decimos que la sucesión es M-(débilmente) regular en $\mathfrak{a}$.

Nótese que la definición depende *a priori* del orden de la tupla. Un elemento A-regular no es más que un elemento que no es divisor de cero.

Lema 5.2: Sea M un A-módulo. Si $a_1, \ldots, a_n$ es una sucesión M-regular y existen $u_i \in M$ tales que

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = 0,$$

entonces cada $u_i \in (a_1, \ldots, a_n)M$.

Demostración: Procedemos por inducción sobre n. Si $n = 1$, entonces $a_1u_1 = 0$ implica que $u_1 = 0 \in a_1M$ por regularidad. Si $n > 1$, entonces como a_n es $M/(a_1, \ldots, a_{n-1})M$-regular, entonces podemos cancelar y

$$u_n = \sum_{i=1}^{n-1} a_i v_i,$$

de modo que $\sum_{i=1}^{n-1} a_i(u_i + a_n v_i) = 0$ y por hipótesis inductiva tenemos que $u_i + a_n v_i \in (a_1, \ldots, a_{n-1})M$ y, por lo tanto, $u_i \in (a_1, \ldots, a_n)M$ para cada i. □

Teorema 5.3: Sea M un A-módulo. Dada una sucesión M-regular $a_1, \ldots, a_n$ y exponentes $\nu_1, \ldots, \nu_n \in \mathbb{N}_{\neq 0}$, entonces la sucesión $a_1^{\nu_1}, \ldots, a_n^{\nu_n}$ es M-regular.

Demostración: Por inducción basta probar que $a_1^\nu, a_2, \ldots, a_n$ sea M-regular. Esto lo haremos por otra inducción sobre ν, donde el caso base está listo.

Claramente a_1^ν es M-regular. Supongamos que $a_1^\nu, \ldots, a_{i-1}$ es M-regular. Sea $v \in M$ tal que $a_i v \equiv 0 \pmod{a_1^\nu, \ldots, a_{i-1}}$, es decir

$$a_i v = a_1^\nu u_1 + a_2 u_2 + \cdots + a_{i-1}u_{i-1},$$

y, por hipótesis inductiva sobre i, tenemos que $v = a_1^{\nu-1}w_1 + a_2 w_2 + \cdots + a_{i-1}w_{i-1}$, luego

$$a_1^{\nu-1}(a_1u_1 - a_i w_1) + a_2(u_2 - a_i w_2) + \cdots + a_{i-1}(u_{i-1} - a_i w_{i-1}) = 0,$$

así que $a_1u_1 - a_i w_1 \in (a_1^{\nu-1}, a_2, \ldots, a_{i-1})M$ por el lema anterior y, así, $a_i w_1 \in (a_1^{\nu-1}, \ldots, a_{i-1})M$ y, por M-regularidad de a_i, tenemos que $w_1 \in (a_1, \ldots, a_{i-1})$ y finalmente $v \in (a_1^\nu, a_2, \ldots, a_{i-1})M$ □

Al considerar $M \otimes A[x_1, \ldots, x_n]$, con $\boldsymbol{x}$ indeterminadas formales, se cumple que sus elementos se comportan como «polinomios con variables en M»; esto será útil para lo siguiente:

Lema 5.4: Sea M un A-módulo y sea $\{a_1, \ldots, a_n\} \subseteq A$ un conjunto tales que $\mathfrak{a}M \neq M$ con $\mathfrak{a} := (a_1, \ldots, a_n)$. Son equivalentes:

1. Para todo polinomio $F(\boldsymbol{x}) \in M \otimes_A A[\boldsymbol{x}]$ homogéneo de grado ν, si $F(\boldsymbol{a}) \in \mathfrak{a}^{\nu+1}M$ entonces todos los coeficientes de F están en $\mathfrak{a}M$.

2. Para todo polinomio $F(\boldsymbol{x}) \in M \otimes_A A[\boldsymbol{x}]$ homogéneo, si $F(\boldsymbol{a}) = 0$ entonces todos los coeficientes de F están en $\mathfrak{a}M$.

3. El epimorfismo

$$\varphi\colon (M/\mathfrak{a}M)[\boldsymbol{x}] \longrightarrow \operatorname{gr}_{\mathfrak{a}} M = \bigoplus_{\nu\geq 0} \mathfrak{a}^\nu M/\mathfrak{a}^{\nu+1}M$$

es un isomorfismo.

Demostración: $1 \implies 2$. Sea $F(\boldsymbol{x})$ tal que $F(\boldsymbol{a}) \in \mathfrak{a}^{\nu+1}M$, luego existe $G(\boldsymbol{x}) \in M[\boldsymbol{x}]$ homogéneo de grado $\nu+1$ tal que $F(\boldsymbol{a}) = G(\boldsymbol{a})$. Escribamos $G(\boldsymbol{x}) = \sum_{i=1}^n x_i G_i(\boldsymbol{x})$, donde cada $G_i(\boldsymbol{x})$ es homogéneo de grado ν, y así $H(\boldsymbol{x}) := F(\boldsymbol{x}) - \sum_{i=1}^n a_i G_i(\boldsymbol{x})$ es homogéneo de grado ν y $H(\boldsymbol{a}) = 0$. Si $H(\boldsymbol{x}) \in (\mathfrak{a}M)[\boldsymbol{x}]$, como los $a_i \in \mathfrak{a}M$, entonces $F(\boldsymbol{x}) \in (\mathfrak{a}M)[\boldsymbol{x}]$.

$2 \implies 1$. Trivial.

$1 \implies 3$. Nótese que es la definición de que $\ker\varphi = 0$. □

Definición 5.5: Sea M un A-módulo. Un conjunto $a_1, \ldots, a_n \in A$ se dice una ***sucesión M-cuasirregular*** si satisface las condiciones del lema anterior.

Ésta definición no depende en principio de un orden.

Teorema 5.6: Sea M un A-módulo, $\{a_1, \ldots, a_n\} \subseteq A$ un subconjunto y $\mathfrak{a} := (a_1, \ldots, a_n)$. Entonces:

1. Si $a_1, \ldots, a_n$ es M-cuasirregular y $b \in A$ es tal que $(\mathfrak{a}M : b) = \mathfrak{a}M$, entonces $(\mathfrak{a}^\nu M : b) = \mathfrak{a}^\nu M$ para todo $\nu > 0$.

2. Toda sucesión M-regular es M-cuasirregular.

3. Supongamos que $M, M/a_1M, M/(a_1,a_2)M, \ldots, M/(a_1,\ldots,a_{n-1})M$ son de Hasudorff en la topología $\mathfrak{a}$-ádica. Si $a_1, \ldots, a_n$ es una sucesión M-cuasirregular, entonces también es M-regular.

Demostración:

1. Procedemos por inducción sobre ν: El caso base es por construcción y si $\nu > 1$ y $u \in M$ es tal que $ub \in \mathfrak{a}^\nu M$, entonces como $u \in \mathfrak{a}^{\nu-1}M$ (¿por qué?) vemos que existe un polinomio homogéneo $F(\boldsymbol{x}) \in M[\boldsymbol{x}]$ de grado $\nu - 1$ tal que $u = F(\boldsymbol{a})$. Como $bu = bF(\boldsymbol{a}) \in \mathfrak{a}^\nu M$, entonces

los coeficientes de F están en $(\mathfrak{a}M : b) = \mathfrak{a}M$ y, por cuasirregularidad, $u \in \mathfrak{a}^\nu M$.

2. Procedemos por inducción sobre n: El caso base es fácil de probar, así que supongamos que $a_1, \ldots, a_{n-1}$ es M-cuasirregular. Fijemos la tupla de indeterminadas $\boldsymbol{x} := (x_1, \ldots, x_{n-1})$ y $\boldsymbol{a} := (a_1, \ldots, a_{n-1})$. Sea $F(\boldsymbol{x}, y) \in M[\boldsymbol{x}, y]$ un polinomio homogéneo de grado ν tal que $F(\boldsymbol{a}, a_n) = 0$. Probaremos que $F(\boldsymbol{x}, y) \in \mathfrak{a}M[\boldsymbol{x}, y]$ por inducción sobre ν. Escribamos $F(\boldsymbol{x}, y) = G(\boldsymbol{x}) + yH(\boldsymbol{x}, y)$, donde G, H son homogéneos de grados $\nu, \nu - 1$ resp. Así, por el inciso anterior,

$$H(\boldsymbol{a}, a_n) \in \big((a_1, \ldots, a_{n-1})^\nu M : a_n\big) = (a_1, \ldots, a_{n-1})^\nu M \subseteq \mathfrak{a}^\nu M,$$

de modo que, por hipótesis inductiva sobre ν, todos los coeficientes de H están en $\mathfrak{a}M$. Además, como $H(\boldsymbol{a}, a_n) \in (a_1, \ldots, a_{n-1})^\nu M$, existe $h(\boldsymbol{x}) \in M[\boldsymbol{x}]$ homogéneo de grado ν, tal que $H(\boldsymbol{a}, a_n) = h(\boldsymbol{a})$ y así, defínase

$$g(\boldsymbol{x}) := G(\boldsymbol{x}) + a_n h(\boldsymbol{x}).$$

Como $\boldsymbol{a}$ es M-cuasirregular, tenemos que $g(\boldsymbol{x})$ tiene coeficientes en $(a_1, \ldots, a_{n-1})M$, luego $G(\boldsymbol{x})$ tiene coeficientes en $\mathfrak{a}M$ como se quería probar.

3. Si $a_1 u = 0$, entonces $u \in \mathfrak{a}M$, luego $u = \sum_{i=1}^n a_i v_i$ y $\sum_{i=1}^n a_1 a_i v_i = 0$, y, por lo tanto, $v_i \in \mathfrak{a}M$ y $u \in \mathfrak{a}^2 M$; por inducción vemos que $u \in \bigcap_{\nu \in \mathbb{N}} \mathfrak{a}^\nu M = 0$, donde la igualdad es la definición de ser «de Hausdorff $\mathfrak{a}$-ádicamente», y así vemos que a_1 es M-regular.

   Sea $M_1 := M/a_1 M$. Nótese que, por inducción, basta probar que $a_2, \ldots, a_n$ forma una sucesión M_1-cuasirregular (que $M \neq \mathfrak{a}M$ se sigue de ser «Hausdorff»). Sea $F(x_2, \ldots, x_n) \in M[\boldsymbol{x}]$ homogéneo de grado ν tal que $F(\boldsymbol{a}) \in a_1 M$, digamos $F(\boldsymbol{a}) = a_1 u$ y supongamos que $u \in \mathfrak{a}^i M$ con $i < \nu$. Sea $u = G(a_1, \boldsymbol{a})$, donde $G(y, \boldsymbol{x}) \in M[y, \boldsymbol{x}]$ es homogéneo de grado i y $F(\boldsymbol{a}) = a_1 G(a_1, \boldsymbol{a})$.

   Si $i < \nu - 1$, entonces $G(\boldsymbol{x}) \in \mathfrak{a}M[\boldsymbol{x}]$, de modo que $u \in \mathfrak{a}^{i+1} M$. Por lo tanto, $u \in \mathfrak{a}^{\nu-1} M$. Si $i = \nu - 1$, entonces $F(\boldsymbol{x}) - yG(y, \boldsymbol{x}) \in \mathfrak{a}M[y, \boldsymbol{x}]$ y, como F no contiene a y, tenemos que $F(\boldsymbol{x}) \in \mathfrak{a}M[y, \boldsymbol{x}]$. Finalmente F mód $a_1 M[y, \boldsymbol{x}] \in (a_2, \ldots, a_n)M[y, \boldsymbol{x}]$ como se quería probar. □

El inciso 3 parece técnico y particular, pero he aquí dos casos importantes donde se satisfacen las hipótesis:

(α) Si A es noetheriano, M es finitamente generado y $\mathfrak{a} \subseteq \mathfrak{J}(A)$. (Esto se sigue del lema de Nakayama junto con el teorema de las intersecciones de Krull.)

(β) Si A es graduado, M es un A-módulo graduado y cada a_i es homogéneo de grado > 0.

Corolario 5.6.1: Sea A un dominio noetheriano, M un A-módulo y $a_1, \ldots, a_n$ una sucesión M-regular. Si se satisface (α) o (β), entonces toda permutación de $a_1, \ldots, a_n$ también es M-regular.

Ejemplo 5.7: Sea k un cuerpo y $A := k[x, y, z]$. Sea $a_1 := x(y-1)$, $a_2 := y$ y $a_3 := z(y-1)$. Nótese que $(a_1, a_2, a_3) = (x, y, z) \neq A$ y que a_1, a_2, a_3 forman una sucesión A-regular, pero a_1, a_3, a_2 no es A-regular. ⌟

Veamos otro camino mediante planitud:

Proposición 5.8: Sea A un anillo, M un A-módulo, $\varphi\colon A \to B$ una A-álgebra y N un B-módulo que es plano sobre A. Dada $\boldsymbol{a} := (a_1, \ldots, a_n)$ una sucesión débilmente M-regular se cumplen:

1. $\boldsymbol{a}$ y $\varphi(\boldsymbol{a})$ son débilmente $(M \otimes_A N)$-regulares.
2. Si $\boldsymbol{a}$ es $(M \otimes_A N)$-regular, entonces $\varphi(\boldsymbol{a})$ también.

Ojo, el enunciado parece un poco redundante, pero $\boldsymbol{a}$ es una sucesión en A y $\varphi(\boldsymbol{a})$ es una sucesión en B; como $M \otimes_A N$ es un A-B-bimódulo, realmente otorga regularidad en dos sentidos distintos.

Demostración: La multiplicación escalar por a_i en $M \otimes_A N$ es la misma que por $\varphi(a_i)$, así que reducimos todo al caso de $\boldsymbol{a}$. Que a_1 sea M-regular equivale a que $M \xrightarrow{\times a_1} M$ sea inyectivo, luego $M \otimes_A N \xrightarrow{\times a_1} M \otimes_A N$ también por planitud, y concluimos por un argumento inductivo. □

Corolario 5.8.1: Sea A un anillo noetheriano, M un A-módulo finitamente generado y $\boldsymbol{a}$ una sucesión M-regular en $\mathfrak{a}$.

1. Para todo primo $\mathfrak{p} \in \operatorname{Supp} M$ con $\mathfrak{p} \supseteq \mathfrak{a}$, se cumple que $\boldsymbol{a}$ es $M_{\mathfrak{p}}$-regular.
2. Si $(A, \mathfrak{m})$ es local, entonces $\boldsymbol{a}$ es $\hat{M}$-regular.

Demostración: Basta notar que las álgebras $A \to A_{\mathfrak{p}}$ y $A \to \hat{A}$ son planas y aplicar la proposición anterior. □

Proposición 5.9: Sea A un anillo, M un A-módulo y $\boldsymbol{a}$ una sucesión M-regular con $\mathfrak{a} := \sum_{i=1}^{n} a_i A$. Entonces, toda sucesión exacta

$$N_\bullet: \qquad N_2 \xrightarrow{\varphi_2} N_1 \xrightarrow{\varphi_1} N_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

induce una sucesión exacta

$$N_2/\mathfrak{a}N_2 \longrightarrow N_1/\mathfrak{a}N_1 \longrightarrow N_0/\mathfrak{a}N_0 \longrightarrow M/\mathfrak{a}M \longrightarrow 0.$$

Demostración: Por inducción basta probar el caso $\boldsymbol{a} = a_1$. Como tensorizar es exacto por la derecha, entonces para verificar que $N_\bullet \otimes A/a$ es exacto en N_1. Si $\overline{\varphi_1}(\overline{u}) \equiv 0 \pmod{a}$, entonces $\varphi_1(u) = av$ para algún $v \in N_0$ y, por tanto, $a\varphi_0(v) = 0$ por exactitud de $N_\bullet$. Como a es N_0-regular, entonces $\varphi_0(v) = 0$, luego $v = \varphi_1(u')$ para algún $u' \in N_1$. Así pues $\varphi_1(u - au') = 0$, de modo que $u - au' \equiv u = \varphi_2(w) \pmod{a}$. □

Proposición 5.10: Sea A un anillo y sea

$$N_\bullet: \qquad \cdots \xrightarrow{\mathrm{d}_{m+1}} N_m \xrightarrow{\mathrm{d}_m} \cdots \longrightarrow N_1 \xrightarrow{\mathrm{d}_1} N_0 \longrightarrow 0$$

una sucesión exacta de A-módulos. Si $\boldsymbol{a} := (a_1, \ldots, a_n)$ es una sucesión débilmente N_i-regular para todo i, entonces $N_\bullet \otimes_A A/(a_1, \ldots, a_n)$ es una sucesión exacta.

Demostración: Definamos $K_m := \ker(\mathrm{d}_{m-1}) = \mathrm{Img}(\mathrm{d}_m)$, entonces podemos ver que $\boldsymbol{a}$ es débilmente K_i-regular para todo i. Luego basta aplicar lo anterior a la sucesión

$$N_{i+2} \longrightarrow N_{i+1} \longrightarrow N_i \longrightarrow K_i \longrightarrow 0. \qquad \square$$

Esto nos da otra prueba, más sencilla, del corolario 5.6.1 para $(A, \mathfrak{m})$ local:

Demostración: Nótese que el axioma SR2 es independiente de las permutaciones así que basta reducirnos a probarlo para sucesiones débilmente M-regulares. Es claro que podemos restringirnos al caso de trasposiciones, y finalmente al caso de trasponer a_1, a_2. Sea K el núcleo de la multiplicación por a_2 en M y sea $u \in K$ tal que $u \in a_1 M$, es decir, $u = a_1 v$, luego $a_2 u = a_1(a_2 v) = 0$, luego $a_2 v = 0$, de modo que $u \in a_2 K$. Así vemos que $K = u_2 K$ y, por el lema de Nakayama, tenemos que $K = 0$ como se quería ver. □

Lema 5.11: Sea A un dominio noetheriano, M un A-módulo finitamente generado y $\mathfrak{a} \lhd A$ un ideal tal que $\mathfrak{a}M \neq M$. Para todo $n > 0$ son equivalentes:

1. Si N es un A-módulo finitamente generado tal que todo $\mathfrak{p} \in \operatorname{Supp} N$ satisface que $\mathfrak{p} \supseteq \mathfrak{a}$, entonces $\operatorname{Ext}^i_A(N, M) = 0$ para todo $i < n$.

2. $\operatorname{Ext}^i_A(A/\mathfrak{a}, M) = 0$ para todo $i < n$.

3. Existe un A-módulo N finitamente generado con $\operatorname{Supp} N = \{\mathfrak{p} \lhd A \text{ primo} : \mathfrak{p} \supseteq \mathfrak{a}\}$ tal que $\operatorname{Ext}^i_A(N, M) = 0$ para todo $i < n$.

4. Existe una sucesión M-regular $a_1, \ldots, a_n$ de longitud n en $\mathfrak{a}$.

Demostración: $1 \implies 2 \implies 3$. Trivial.

$3 \implies 4$. Por definición, $\operatorname{Ext}^0_A(N, M) = \operatorname{Hom}_A(N, M) = 0$. Si no existiese ningún elemento M-regular en $\mathfrak{a}$, entonces $\mathfrak{a} \subseteq \bigcup \operatorname{As}(M)$ y, como $\operatorname{As}(M)$ es finito pues A es noetheriano, entonces $\mathfrak{a} \subseteq \mathfrak{p}$ para algún $\mathfrak{p} \in \operatorname{As}(M)$ por evitamiento de primos. Luego existe una inyección $A/\mathfrak{p} \to M$ y, localizando en $\mathfrak{p}$ se tiene que $\operatorname{Hom}_{A_\mathfrak{p}}(k, M_\mathfrak{p}) \neq 0$, donde $k := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Como $\mathfrak{p} \in \operatorname{Supp}(N)$ por hipótesis, tenemos que $N_\mathfrak{p} \neq 0$ y, por el lema de Nakayama, $N_\mathfrak{p}/\mathfrak{p}N_\mathfrak{p} = N \otimes_A k \neq 0$. De modo que $N \otimes_A k$ es un k-espacio vectorial no nulo, luego $\operatorname{Hom}_k(N \otimes_A k, k) \neq 0$. Finalmente, componiendo:

$$N_\mathfrak{p} \longrightarrow N \otimes_A k \longrightarrow k \longrightarrow M_\mathfrak{p}$$

vemos que $\big(\operatorname{Hom}_A(N, M)\big)_\mathfrak{p} \cong \operatorname{Hom}_{A_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p}) \neq 0$, lo que es absurdo. Así que, $\mathfrak{a}$ contiene un elemento M-regular a_1. Como $M/\mathfrak{a}M \neq 0$ por hipótesis, entonces $M_1 := M/a_1M \neq 0$, así que la sucesión exacta:

$$0 \longrightarrow M \xrightarrow{\times a_1} M \longrightarrow M_1 \longrightarrow 0 \tag{5.1}$$

implica que $\operatorname{Ext}^i_A(N, M_1) = 0$ con $i < n-1$, luego por inducción construimos una sucesión M_1-regular $a_2, \ldots, a_n$.

$4 \implies 1$. Sea $a_1, \ldots, a_n$ una sucesión M-regular, y considerando la misma sucesión (5.1) y por inducción, vemos que $\operatorname{Ext}^i_A(N, M_1) = 0$ para $i < n - 1$, así que induce la sucesión exacta:

$$0 \longrightarrow \operatorname{Ext}^i_A(N, M) \xrightarrow[=\times a_1]{\operatorname{Ext}^i_A(N, \times a_1)} \operatorname{Ext}^i_A(N, M), \qquad (i < n)$$

y como $\operatorname{Ext}^i_A(N,M)$ se anula con elementos de $\operatorname{Ann}(N)$, empleamos que los elementos de $\mathfrak{p} \in \operatorname{Supp} N$ contienen a $\operatorname{Ann}(N)$ y, por hipótesis, $\mathfrak{p} \supseteq \mathfrak{a}$, por lo que, $\mathfrak{a} \subseteq \operatorname{Rad}\big(\operatorname{Ann}(N)\big)$ y, por lo tanto, $a_1^{\nu_1}$ anula a $\operatorname{Ext}^i_A(N,M)$ para algún ν_1 suficientemente grande. Así, vemos que $\operatorname{Ext}^i_A(N,M) = 0$ con $i < n$. □

Teorema 5.12 (Rees): Sea A un dominio noetheriano, M un A-módulo finitamente generado y $\mathfrak{a} \lhd A$ un ideal, tales que $M \neq \mathfrak{a}M$. La longitud de una sucesión M-regular maximal es un natural n bien definido, dado por

$$\forall i < n \quad \operatorname{Ext}^i_A(A/\mathfrak{a}, M) = 0, \qquad \operatorname{Ext}^n_A(A/\mathfrak{a}, M) \neq 0.$$

Definición 5.13: Sea A un dominio noetheriano, M un A-módulo finitamente generado y $\mathfrak{a} \lhd A$ un ideal. Se le llama la ***$\mathfrak{a}$-profundidad*** de M a la máxima longitud de una sucesión M-regular o bien a

$$\operatorname{prof}(\mathfrak{a}, M) := \text{mín}\{i : \operatorname{Ext}^i_A(A/\mathfrak{a}, M) \neq 0\}.$$

Si $(A, \mathfrak{m})$ es local, entonces denotamos $\operatorname{prof} M = \operatorname{prof}_A M := \operatorname{prof}(\mathfrak{m}, M)$, a la que llamamos ***profundidad*** de M (a secas).

Complementario a la profundidad, se tiene la siguiente definición:

Definición 5.14: Sea A un dominio noetheriano y $M \neq 0$ un A-módulo finitamente generado. Se define la ***calidad***[1] de M como:

$$\operatorname{calidad} M := \text{ínf}\{i \in \mathbb{N} : \operatorname{Ext}^i_A(M, A) \neq 0\}.$$

Si $\mathfrak{a} \lhd A$ es un ideal propio, entonces $\operatorname{calidad} \mathfrak{a} := \operatorname{calidad}(A/\mathfrak{a})$.

El lema 5.11, nos dice que $\operatorname{calidad} M = \operatorname{prof}(\operatorname{Ann}(M), M)$.

Definición 5.15: Sea A un anillo y M un A-módulo. Una ***resolución proyectiva*** (resp. ***resolución libre***) es una sucesión exacta:

$$P_\bullet: \quad \cdots \longrightarrow P_n \xrightarrow{\mathrm{d}_n} \cdots \longrightarrow P_1 \xrightarrow{\mathrm{d}_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

donde cada P_i es un módulo proyectivo (resp. libre). Si $P_j = 0$ para todo $j > n$, pero $P_n \neq 0$, entonces decimos que $P_\bullet$ es una resolución finita de largo n. Dualmente una ***resolución inyectiva*** es una sucesión exacta:

[1] eng. *grade*. La traducción de éste término bien podría ser «nivel, calidad», como «nota, calificación» o como «grado, curso». Como es más frecuente el uso de *grado* y *nivel* en otros contextos, optamos por *calidad*; evidentemente es una traducción no estándar.

$$Q^\bullet: \qquad 0 \longrightarrow M \longrightarrow Q^0 \xrightarrow{\mathrm{d}^0} Q^1 \xrightarrow{\mathrm{d}^1} \cdots,$$

donde cada Q^i es un modulo inyectivo.

Se dice que M tiene ***dimensión proyectiva*** $d := \operatorname{proj\,dim}_A M$ si posee alguna resolución proyectiva finita de largo d y toda resolución proyectiva $P_\bullet$ satisface que $P_d \neq 0$. De no existir dicho d, denotamos $\operatorname{proj\,dim}_A M = \infty$. Obviaremos el subíndice de no haber ambigüedad.

Se dice que M tiene ***dimensión inyectiva*** $e := \operatorname{inj\,dim}_A M$ si posee alguna resolución inyectiva finita de largo e y toda resolución inyectiva $Q^\bullet$ satisface que $Q^e \neq 0$. De no existir dicho e, denotamos $\operatorname{inj\,dim}_A M = \infty$. Obviaremos el subíndice de no haber ambigüedad.

Proposición 5.16: Sea A un dominio noetheriano. Para todo A-módulo finitamente generado $M \neq 0$ se tiene que $\operatorname{calidad} M \leq \operatorname{proj\,dim} M$.

Teorema 5.17: Sea A un dominio noetheriano, y sean M, N un par de A-módulos finitamente generados. Supongamos que $M \neq 0$, $j := \operatorname{calidad} M$ y $l := \operatorname{proj\,dim} N \leq j$, entonces

$$\forall i < j - l \quad \operatorname{Ext}^i_A(M, N) = 0.$$

Demostración: La demostración es por inducción sobre l. Si $l = 0$, entonces N es proyectivo y, por tanto, es el sumando directo de un módulo libre A^n, por lo que podemos suponer que $N = A$, en cuyo caso es por definición de calidad. Si $l > 0$, basta elegir una sucesión exacta $0 \longrightarrow N_1 \longrightarrow L_0 \longrightarrow N_0 \longrightarrow 0$, donde N_1 es un A-módulo finitamente generado con $\operatorname{proj\,dim} N_1 = l - 1$, y L_0 es proyectivo, por lo que, por inducción se sabe que:

$$\forall i < j \quad \operatorname{Ext}^i_A(M, L_0) = 0, \qquad \forall i < j - l \quad \operatorname{Ext}^{i+1}_A(M, N_1) = 0. \qquad \square$$

Lema 5.18: Sea A un anillo y M, N un par de A-módulos finitamente generados. Entonces $\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp} M \cap \operatorname{Supp} N$.

Demostración: Para todo primo $\mathfrak{p} \lhd A$ se cumple que

$$\begin{aligned}(M \otimes_A N)_\mathfrak{p} &\cong (M \otimes_A N) \otimes_A A_\mathfrak{p} \cong (M \otimes_A N) \otimes_A (A_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p}) \\ &\cong M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p}.\end{aligned}$$

Así pues, la afirmación se reduce al siguiente enunciado:

(*) Si $(A, \mathfrak{m}, k)$ es local, entonces $M \otimes_A N = 0$ syss $M = 0$ o $N = 0$.
$\Longleftarrow$. Trivial.
$\Longrightarrow$. Por contrarrecíproca, si $M \neq 0 \neq N$, entonces $M \otimes_A k = E/\mathfrak{m}E \neq 0$ por el lema de Nakayama. Luego $M \otimes_A k$ es un k-espacio vectorial de dimensión finita y

$$0 \neq (M \otimes_A k) \otimes_k (N \otimes_A k) = (M \otimes_A N) \otimes_A k,$$

de modo que $M \otimes_A N \neq 0$. □

Proposición 5.19: Sea A un anillo local noetheriano y M un A-módulo finitamente generado. Para toda sucesión M-regular $a_1, \ldots, a_r$ se cumple que

$$k.\dim\big(M/(a_1, \ldots, a_r)M\big) = k.\dim M - r.$$

Demostración: Por teorema de los ideales principales de Krull, tenemos que $\geq$. Por otro lado, supongamos que a es un elemento M-regular, entonces $\operatorname{Supp}(M/aM) = \operatorname{Supp} M \cap \operatorname{Supp}(A/aA)$ y, como a es M-regular, entonces no está en ningún primo $\subseteq$-minimal de $\operatorname{Supp} M$. Luego $k.\dim(M/aM) \leq k.\dim M - 1$ y por inducción se concluye el enunciado. □

Casualmente, en algunos casos nos referiremos a la proposición anterior como teorema de ideales principales de Krull.

5.2 Fórmulas homológicas

Podemos sonsacar un poco más de información a la profundidad:

Definición 5.20: Sea $(A, \mathfrak{m}, k)$ un anillo local noetheriano y $M \neq 0$ un A-módulo finitamente generado de $\operatorname{prof} M =: d < \infty$. Definimos su ***tipo*** $t_A(M) := \dim_k \operatorname{Ext}^d_A(k, M)$.

Proposición 5.21: Sean $(A, \mathfrak{m}, k)$, $(B, \mathfrak{n}, l)$ un par de anillos locales noetherianos y $\varphi\colon A \to B$ un homomorfismo. Sean M_A, N_B módulos finitamente generados con N plano sobre A. Entonces:

1. $\dim_l \operatorname{Hom}_B(l, M \otimes_A N) = \dim_k \operatorname{Hom}_A(k, M) \cdot \dim_l \operatorname{Hom}_B(l, N/\mathfrak{m}N)$.
2. Si $\boldsymbol{b} = (b_1, \ldots, b_n)$ es $(N/\mathfrak{m}N)$-regular (en B), entonces es $(M \otimes_A N)$-regular y $N/(b_1, \ldots, b_n)N$ es plano sobre A.
3. $\operatorname{prof}_B(M \otimes_A N) = \operatorname{prof}_A M + \operatorname{prof}_B(N/\mathfrak{m}N)$.

4. $t_B(M \otimes_A N) = t_A(M) \cdot t_B(N/\mathfrak{m}N)$.

Demostración:

1. Sea $C := B/\mathfrak{m}B = B \otimes_A k$, entonces existe un isomorfismo natural:

$$\mathrm{Hom}_B(l, \mathrm{Hom}_B(C, M \otimes_A N)) \cong \mathrm{Hom}_B(l, M \otimes_A N),$$

puesto que ambos módulos se identifican con $U := \{u \in M \otimes_A N : u\mathfrak{n} = 0\}$. Como N es plano sobre A, se tiene el siguiente isomorfismo natural

$$\mathrm{Hom}_B(C, M \otimes_A N) = \mathrm{Hom}_B(B \otimes_A k, M \otimes_A N) \cong \mathrm{Hom}_A(k, M) \otimes_A N.$$

Ahora bien, como $\mathrm{Hom}_A(k, M)$ es un k-espacio vectorial, entonces $\mathrm{Hom}_A(k, M) \cong k^s$ para algún $s \geq 0$, luego $\mathrm{Hom}_A(k, M) \otimes_A N \cong (N/\mathfrak{m}N)^s$, lo que demuestra el enunciado.

2. Para todo ideal $\mathfrak{b} \lhd B$ se tiene que $(M \otimes_A N)/\mathfrak{b}(M \otimes_A N) \cong M \otimes_A (N/\mathfrak{b}N)$. Así empleando inducción podemos reducirnos al caso de $n = 1$ y $b := b_1$.

Por el teorema de intersecciones de Krull tenemos que $\bigcap_{i=0}^{\infty} \mathfrak{m}^i(M \otimes_A N) = 0$. Supongamos que $bu = 0$ para algún $u \in (M \otimes N)_{\neq 0}$, entonces existe un i tal que

$$u \in \mathfrak{m}^i(M \otimes N) \setminus \mathfrak{m}^{i+1}(M \otimes N),$$

de modo que b es un divisor de cero en $\mathfrak{m}^i(M \otimes N)/\mathfrak{m}^{i+1}(M \otimes N)$. Considerando la inclusión $\iota\colon \mathfrak{m}^i M \to M$, por planitud de N vemos que $\mathfrak{m}^i M \otimes N \to M \otimes N$ es inyectivo y su imagen es $\mathfrak{m}^i(M \otimes N)$, de modo que aplicando el mismo razonamiento para $\mathfrak{m}^{i+1}$ nos da el isomorfismo:

$$\frac{\mathfrak{m}^i(M \otimes N)}{\mathfrak{m}^{i+1}(M \otimes N)} \cong \frac{\mathfrak{m}^i M}{\mathfrak{m}^{i+1} M} \otimes N \cong k^t \otimes N \cong (N/\mathfrak{m}N)^t,$$

para algún $t \geq 0$. Y como b es $(N/\mathfrak{m}N)$-regular, entonces debe ser regular en $\mathfrak{m}^i(M \otimes N)/\mathfrak{m}^{i+1}(M \otimes N)$.

Para verificar que N/bN es plano, basta considerar sucesiones exactas cortas $\mathscr{S}\colon\ 0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ de A-módulos finitamente generados. Como N es plano, entonces $\mathscr{S} \otimes_A N$ es exacto y, por la proposición 5.8, se tiene que b es $(M_3 \otimes N)$-regular y, por la proposición 5.9, vemos que $\mathscr{S} \otimes_A N/bN$ es exacto.

Citar el por qué.

3 y 4. Sea $\boldsymbol{a} := (a_1, \ldots, a_m)$ una sucesión M-regular maximal y $\boldsymbol{b} := (b_1, \ldots, b_n)$ una sucesión $(N/\mathfrak{m}N)$-regular maximal. Por 5.8 vemos que $\varphi(\boldsymbol{a})$ es $(M \otimes N)$-regular y, por el inciso anterior, $\boldsymbol{b}$ es $(\overline{M} \otimes N)$-regular, donde $\overline{M} := M/\boldsymbol{a}M$. Ahora bien, como

$$(M/\boldsymbol{a}M) \otimes_A N \cong \frac{M \otimes N}{\varphi(\boldsymbol{a})(M \otimes N)}$$

tenemos que $\varphi(\boldsymbol{a}), \boldsymbol{b}$ (la sucesión concatenada) es $(\overline{M} \otimes N)$-regular. Definiendo $N_1 := N/\boldsymbol{b}N$, se ve que $N_1/\mathfrak{m}N_1 \cong \overline{N}/\boldsymbol{b}\overline{N}$ y

$$\frac{M \otimes N}{\big(\varphi(\boldsymbol{a}), \boldsymbol{b}\big)(M \otimes N)} \cong \overline{M} \otimes N_1.$$

Demostrar éstas igualdades siguiendo a Serre [7].

Finalmente sabemos que

$$\operatorname{Hom}_A(k, \overline{M}) \cong \operatorname{Ext}^m_A(k, M), \qquad \operatorname{Hom}_B(l, \overline{N}/\boldsymbol{b}\overline{N}) \cong \operatorname{Ext}^n_B(l, \overline{N})$$
$$\operatorname{Hom}_B(l, \overline{M} \otimes N_1) \cong \operatorname{Ext}^{m+n}_B(l, M \otimes N).$$

De modo que el inciso 1 implica la igualdad sobre los tipos y, en particular, $\operatorname{Ext}^{m+n}_B(l, M \otimes N) \neq 0$, por lo que, se satisface la igualdad de profundidad por el teorema de Rees. □

Definición 5.22: Sea $(A, \mathfrak{m}, k)$ un anillo local noetheriano y M un A-módulo finitamente generado. Definamos

$$\mu(M) := \dim_k(M \otimes_A k) = \dim_k(M/\mathfrak{m}M).$$

Denotemos $\beta_0 := \mu(M)$, es decir, β_0 es el mínimo número de generadores de M y podemos construir un epimorfismo $\varphi_0 \colon A^{\beta_0} \to M$. Denotemos $\beta_1 := \mu(\ker \varphi_0)$ y construyamos un epimorfismo $\varphi_1 \colon A^{\beta_1} \to \ker \varphi_0$, así podemos construir una ***resolución libre minimal*** de M:

$$L_\bullet \colon \qquad \cdots \longrightarrow A^{\beta_1} \xrightarrow{\varphi_1} A^{\beta_0} \xrightarrow{\varphi_0} M \longrightarrow 0.$$

Empleando el hecho de que los módulos libres son proyectivos es fácil ver que $L_\bullet$ es único salvo isomorfismo de complejos de cadenas, así también se verifica que el número β_i es independiente de las elecciones de los φ_j's y se denomina el ***i-ésimo número de Betti***.

Proposición 5.23: Sea $(A, \mathfrak{m}, k)$ un anillo local noetheriano, M un A-módulo finitamente generado y

$$L_\bullet: \qquad \cdots \longrightarrow L_1 \xrightarrow{\varphi_1} L_0 \xrightarrow{\varphi_0} M \longrightarrow 0.$$

una resolución libre. Son equivalentes:

1. $L_\bullet$ es una resolución libre minimal.
2. $\varphi_i[L_i] \subseteq \mathfrak{m}L_{i-1}$ para todo $i \geq 1$.
3. $\operatorname{rang}_A L_i = \dim_k \operatorname{Tor}_i^A(M,k)$ para todo $i \geq 0$.
4. $\operatorname{rang}_A L_i = \dim_k \operatorname{Ext}_A^i(M,k)$ para todo $i \geq 0$.

Demostración: La equivalencia 1 $\iff$ 2 es por el lema de Nakayama. Como $\operatorname{Tor}_i^A(M,k) \cong H_i(L_\bullet \otimes_A k)$ vemos que se satisface 3 syss $\varphi_i \otimes_A k = 0$, lo que equivale a 2. La equivalencia 2 $\iff$ 4 se deduce de que $\operatorname{Ext}_A^i(M,k) \cong H^i(\operatorname{Hom}_A(M,k))$. □

Corolario 5.23.1: Sea $(A,\mathfrak{m},k)$ un anillo local noetheriano y M un A-módulo finitamente generado. Entonces $\beta_i(M) = \dim_k \operatorname{Tor}_i^A(M,k)$ y

$$\operatorname{proj\,dim} M = \sup\{i : \operatorname{Tor}_i^A(M,k) \neq 0\}.$$

En consecuencia, M admite una resolución libre finita syss $\operatorname{proj\,dim} M < \infty$.

Teorema 5.24 – *Fórmula de Auslander-Buchsbaum*: Sea $(A,\mathfrak{m},k)$ un anillo local noetheriano y sea $M \neq 0$ un A-módulo finitamente generado. Si $\operatorname{proj\,dim} M < \infty$, entonces

$$\operatorname{proj\,dim} M + \operatorname{prof} M = \operatorname{prof} A.$$

Demostración: Procedemos por inducción sobre $h := \operatorname{proj\,dim} M$. Si $h = 0$, entonces M es proyectivo y, por tanto, es libre (teo. A.8), luego es trivial. Si $h = 1$, entonces sea

$$0 \longrightarrow A^m \xrightarrow{\mu} A^n \xrightarrow{\varepsilon} M \longrightarrow 0 \tag{5.2}$$

una resolución minimal de M, de modo que podemos escribir a μ en representación matricial con entradas en $\mathfrak{m}$. Luego, (5.2) induce una sucesión exacta mediante $\operatorname{Ext}_A^\bullet(k,-)$:

$$\cdots \longrightarrow \operatorname{Ext}_A^i(k,A^m) \xrightarrow{\mu_*} \operatorname{Ext}_A^i(k,A^n) \xrightarrow{\varepsilon_*} \operatorname{Ext}_A^i(k,M) \longrightarrow \cdots$$

y como $\operatorname{Ext}^i_A(k, A^m) \cong \operatorname{Ext}^i_A(k, A)^m$, se nota que μ_* se expresa por la misma matriz que μ (¿por qué?). No obstante, como las entradas de μ_* están en $\mathfrak{m}$, aniquilan a k, de modo que se induce la sucesión exacta:

$$0 \longrightarrow \operatorname{Ext}^i_A(k, A)^n \xrightarrow{\varepsilon_*} \operatorname{Ext}^i_A(k, M) \xrightarrow{\mu_*} \operatorname{Ext}^{i+1}_A(k, A)^m \longrightarrow 0$$

para todo i. Como $\operatorname{prof} M = \operatorname{ínf}\{i : \operatorname{Ext}^i_A(k, M) \neq 0\}$ se nota que $\operatorname{prof} M = \operatorname{prof} A - 1$ como se quería ver.

El caso general $h > 0$ sale construyendo la sucesión exacta

$$0 \longrightarrow M' \longrightarrow A^n \longrightarrow M \longrightarrow 0,$$

donde $\operatorname{proj\,dim} N = \operatorname{proj\,dim} M - 1$ y aplicando inducción. □

Definición 5.25: Sea A un anillo noetheriano y M un A-módulo finitamente generado. Se dice que M posee una ***resolución libre finita*** (abrev., r.l.f.) si posee una resolución libre

$$L_\bullet: \qquad \cdots \longrightarrow L_1 \xrightarrow{\varphi_1} L_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

donde existe $n_0 \in \mathbb{N}$ tal que $L_n = 0$ para $n \geq n_0$. Como A es noetheriano es fácil notar que solo basta exigir que L_0 sea finitamente generado para que todo el resto también, y podemos definir la ***característica de Euler*** de M como:

$$\chi_A(M) := \sum_{j=0}^{\infty} (-1)^j \operatorname{rang} L_j.$$

Por ejemplo, si M es libre, entonces $\chi(M) = \operatorname{rang} M$. Por ésta razón, algunos autores (e.g., Bruns y Herzog [**2**]) le llaman a χ el «rango» de M.

Vamos a dar una descripción alternativa de la característica de Euler:

Definición 5.26: Sea A un anillo y M un A-módulo finitamente generado. Si $M \otimes_A A_{\text{tot}}$ es un A_{tot}-módulo libre, entonces definimos $r(M) := \operatorname{rang}_{A_{\text{tot}}}(M \otimes_A A_{\text{tot}})$.

Lema 5.27: Sea A un anillo semilocal y M un A-módulo proyectivo finitamente generado. Son equivalentes:

1. M es libre de rango r.

2. $M_{\mathfrak{m}}$ es libre de rango constante r para todo $\mathfrak{m} \lhd A$ maximal.

Demostración: Claramente $1 \implies 2$, veamos la recíproca. Procedemos por inducción sobre r, el caso base $r = 0$ es trivial.

Como $M \neq 0$, por evitamiento de primos existe $u \in M$ tal que $u \notin \mathfrak{m}M_{\mathfrak{m}}$ para todo $\mathfrak{m} \lhd A$ maximal. Como $M_{\mathfrak{m}}$ es libre, entonces u está contenido en una $A_{\mathfrak{m}}$-base de $M_{\mathfrak{m}}$, de modo que $(M/uA)_{\mathfrak{m}}$ es libre de rango $r-1$ para todo $\mathfrak{m}$; por hipótesis inductiva vemos que M/uA es libre de rango $r-1$. Así pues, $M \cong (uA) \oplus (M/uA)$ (pues M/uA es proyectivo), de modo que uA es un A-módulo proyectivo. Sea $\varphi\colon A \to uA$ el epimorfismo natural, el cual induce $\varphi_{\mathfrak{m}}\colon A_{\mathfrak{m}} \to (uA)_{\mathfrak{m}}$ un isomorfismo para todo $\mathfrak{m} \lhd A$ maximal, luego $\ker(\varphi_{\mathfrak{m}}) = (\ker\varphi)_{\mathfrak{m}} = 0$ implica que φ es, de hecho, un isomorfismo, y así M es libre de rango r. □

Proposición 5.28: Sea A un anillo noetheriano y M un A-módulo con una r.l.f. $L_1 \xrightarrow{\varphi} L_0 \longrightarrow M \longrightarrow 0$. Entonces son equivalentes:

1. $r(M) = r < \infty$.
2. M posee un A-submódulo N libre de rango r, tal que M/N es de torsión.
3. Para todo $\mathfrak{p} \in \operatorname{As} M$ se cumple que $M_{\mathfrak{p}}$ es un libre de rango r.
4. $\operatorname{Img}\varphi$ es un A-submódulo libre de L_0 y $\operatorname{rang}(\operatorname{Img}\varphi) = \operatorname{rang} L_0 - r$.

Demostración: $1 \implies 2$. Sea $u_1, \ldots, u_r \in M$ tales que forman una A_{tot}-base de $M \otimes_A A_{\mathrm{tot}}$, entonces $N := \sum_{i=1}^{r} u_i A$ satisface lo pedido.

$2 \implies 1$. Trivial.

$3 \iff 1$. Nótese que A_{tot} es semilocal y que las localizaciones $(A_{\mathrm{tot}})_{\mathfrak{n}}$ respecto a ideales maximales $\mathfrak{n} \lhd A_{\mathrm{tot}}$ corresponden a localizaciones $A_{\mathfrak{p}}$ respecto a ideales asociados maximales $\mathfrak{p} \in \operatorname{As}(A)$. Luego la equivalencia se sigue del lema anterior.

$3 \iff 4$. Debido a la equivalencia $1 \iff 3$ podemos sustituir la hipótesis 4 por «$(\operatorname{Img}\varphi)_{\mathfrak{p}}$ es libre de rango $\operatorname{rang} L_0 - r$ para todo $\mathfrak{p} \in \operatorname{As} A$». Luego, basta considerar la siguiente sucesión exacta

$$0 \longrightarrow (\operatorname{Img}\varphi)_{\mathfrak{p}} \longrightarrow (L_0)_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow 0.$$

Así es fácil notar que $M_{\mathfrak{p}}$ es libre syss $(\operatorname{Img}\varphi)_{\mathfrak{p}}$ para todo primo asociado $\mathfrak{p} \in \operatorname{As} A$. □

Proposición 5.29: Sea A un anillo noetheriano y sea $0 \to M_1 \to M_2 \to M_3 \to 0$ una sucesión exacta de A-módulos. Si dos de los módulos M_1, M_2, M_3

poseen r.l.f.'s, el tercero también y se tiene que $r(M_1) + r(M_3) = r(M_2)$. En consecuencia, $r(-)$ es una función aditiva y $r(M) = \chi(M)$.

Demostración: Por la proposición anterior, podemos localizar por los primos asociados maximales, de modo que podemos suponer que A es local de $\operatorname{prof} A = 0$. Luego es fácil comprobar que si dos de tres módulos son libres, el tercero también y concluimor por la proposición anterior. □

Esta equivalencia tiene un corolario bastante interesante:

Teorema 5.30: Sea A noetheriano. Para todo A-módulo M con r.l.f. se tiene que $\chi(M) \geq 0$.

También se puede relajar la hipótesis de noetherianidad sobre A (cfr. Matsumura **[5,** págs. 159-160]).

Teorema 5.31 (Auslander-Buchsbaum): Sea A un anillo noetheriano y sea M un A-módulo con r.l.f. Son equivalentes:

1. $\operatorname{Ann} M \neq 0$.
2. $\chi(M) = 0$.
3. $\operatorname{Ann} M$ contiene un elemento A-regular.

Demostración: 1 $\implies$ 2. Por contrarrecíproca, si $\chi(M) > 0$, entonces $\chi(M_{\mathfrak{p}}) > 0$ para todo primo $\mathfrak{p} \in \operatorname{As} A$ y tenemos que $M_{\mathfrak{p}} \neq 0$. Por la proposición 5.28, tenemos que $M_{\mathfrak{p}}$ es libre sobre $A_{\mathfrak{p}}$, luego $\mathfrak{a} := \operatorname{Ann} M$ satisface que $\mathfrak{a}_{\mathfrak{p}} = \operatorname{Ann}(M_{\mathfrak{p}}) = 0$. Sea $\mathfrak{b} := \operatorname{Ann} \mathfrak{a}$, de modo que $\mathfrak{b} \nsubseteq \mathfrak{p}$ y, como ello aplica para todos los primos asociados, vemos que $\mathfrak{b}$ contiene un elemento A-regular (¿por qué?). Finalmente como $\mathfrak{a}\mathfrak{b} = 0$ se concluye que $\mathfrak{a} = 0$.

2 $\implies$ 3. Si $\chi(M) = 0$, entonces nuevamente por la proposición 5.28 tenemos que $M_{\mathfrak{p}} = 0$ para todo primo asociado $\mathfrak{p} \in \operatorname{As} A$, de modo que $\operatorname{Ann} M \nsubseteq \mathfrak{p}$ para todo $\mathfrak{p} \in \operatorname{As} A$ y, por tanto, contiene un elemento A-regular.

3 $\implies$ 1. Trivial. □

Corolario 5.31.1: Sea A un anillo local noetheriano y $0 \neq \mathfrak{a} \lhd A$ tal que $\operatorname{proj\,dim}_A \mathfrak{a} < \infty$. Entonces $\mathfrak{a}$ contiene un elemento A-regular.

Antes de estudiar anillos de Cohen-Macaulay, veremos una noción bastante útil:

Definición 5.32: Sea A un anillo Se dice que un A-módulo M es ***perfecto*** si calidad $M = \operatorname{proj\,dim} M$.

Proposición 5.33: Sea A un anillo noetheriano y sea M un A-módulo perfecto. Para todo primo $\mathfrak{p} \in \operatorname{Supp} M$ son equivalentes:

1. $\mathfrak{p}$ es un primo asociado de M.
2. $\operatorname{prof}_{A_\mathfrak{p}}(A_\mathfrak{p}) = \text{calidad } M$.

Además, calidad $\mathfrak{p} =$ calidad M para todos los primos asociados.

Demostración: Se tiene en general que

$$\text{calidad } M \leq \text{calidad } M_\mathfrak{p} \leq \operatorname{proj\,dim}(M_\mathfrak{p}) \leq \operatorname{proj\,dim} M, \tag{5.3}$$

y, por la fórmula de Auslander-Buchsbaum, tenemos que

$$\operatorname{prof}_{A_\mathfrak{p}}(M_\mathfrak{p}) + \operatorname{proj\,dim}_{A_\mathfrak{p}}(M_\mathfrak{p}) = \operatorname{prof}(A_\mathfrak{p}).$$

Si M es perfecto, entonces $\operatorname{prof}_{A_\mathfrak{p}}(M_\mathfrak{p}) = 0$ syss $\text{calidad}_{A_\mathfrak{p}}(M_\mathfrak{p}) = \operatorname{prof}(A_\mathfrak{p})$, como se quería ver. □

5.3 Anillos de Cohen-Macaulay

Teorema 5.34 (Ischebeck): Sea $(A, \mathfrak{m})$ un dominio local noetheriano y sean M, N un par de A-módulos finitamente generados no nulos. Sea $p := \operatorname{prof} M, r := k.\dim N$, entonces:

$$\forall i < p - r \quad \operatorname{Ext}^i_A(N, M) = 0.$$

Demostración: La demostración es por inducción sobre r. Si $r = 0$, entonces $\operatorname{Rad}\operatorname{Ann} M = \mathfrak{m}$, por tanto, $\operatorname{Supp} M = \{\mathfrak{m}\}$ y concluimos por el lema 5.11.

Si $r > 0$, entonces por descomposición de Lasker-Noether (corolario A.9.1) existe una cadena

$$0 := N_0 \subset N_1 \subset \cdots \subset N_n =: N, \quad N_j/N_{j-1} \cong A/\mathfrak{p}_j,$$

donde cada $\mathfrak{p}_j \lhd A$ es primo. Así pues, es fácil notar que si $\operatorname{Ext}^i_A(N_j/N_{j-1}, M) = 0$ para todo j y todo $i < p-r$, entonces $\operatorname{Ext}^i_A(N, M) = 0$ para todo $i < p-r$. De éste modo, podemos reducirnos al caso $N = A/\mathfrak{p}$ con $\mathfrak{p} \lhd A$ primo. Como $r > 0$, existe $a \in \mathfrak{m} \setminus \mathfrak{p}$ tal que

$$0 \longrightarrow N \xrightarrow{\times a} N \longrightarrow N_1 := A/(\mathfrak{p}, a) \longrightarrow 0$$

donde $k.\dim N_1 < r$ por el teorema de los ideales principales de Krull, así que tenemos que $\operatorname{Ext}^i_A(N_1, M) = 0$ para $i < p - r + 1$. Luego, para $i < p - r$ tenemos la sucesión exacta:

$$0 \longrightarrow \operatorname{Ext}^i_A(N, M) \xrightarrow{\times a} \operatorname{Ext}^i_A(N, M) \longrightarrow \operatorname{Ext}^{i+1}_A(N_1, M) = 0,$$

como $a \in \mathfrak{m}$, por el lema de Nakayama, se concluye $\operatorname{Ext}^i_A(N, M) = 0$. □

Teorema 5.35: Sea A un dominio noetheriano local y M un A-módulo finitamente generado. Para todo $\mathfrak{p} \in \operatorname{As} M$ se cumple que $k.\dim(A/\mathfrak{p}) \geq \operatorname{prof} M$.

Demostración: Basta notar que si $\mathfrak{p} \in \operatorname{As} M$, entonces $\operatorname{Ext}^0_A(A/\mathfrak{p}, M) = \operatorname{Hom}_A(A/\mathfrak{p}, M) \neq 0$, de modo que $\operatorname{prof} M - k.\dim(A/\mathfrak{p}) \not\geq 1$ por el teorema de Ischebeck. □

Definición 5.36: Sea $(A, \mathfrak{m})$ un dominio local noetheriano y sea M un A-módulo finitamente generado. Decimos que M es un ***módulo de Cohen-Macaulay*** si $M = 0$ o $\operatorname{prof} M = k.\dim M$, además decimos que M es ***de Cohen-Macaulay maximal*** si $k.\dim M = k.\dim A$. Decimos que A es un ***anillo de Cohen-Macaulay*** si es un A-módulo de Cohen-Macaulay.

Definición 5.37: Sea A un anillo y M un A-módulo. Se dice que un primo $\mathfrak{p}$ asociado a M es un ***primo encajado*** de M si no es asociado minimal, vale decir, si existe $\mathfrak{q} \in \operatorname{As} M$ tal que $\mathfrak{p} \supset \mathfrak{q}$. Un ***primo encajado*** de A, es un primo encajado del A-módulo A.

Teorema 5.38: Sea $(A, \mathfrak{m})$ un dominio local noetheriano y $M \neq 0$ un A-módulo finitamente generado. Se cumplen:

1. Si M es de Cohen-Macaulay, entonces para todo $\mathfrak{p} \in \operatorname{As} M$ se tiene que $k.\dim(A/\mathfrak{p}) = \operatorname{prof} M = k.\dim M$. En consecuencia, M no tiene primos encajados.

2. Sea $a_1, \ldots, a_n \in \mathfrak{m}$ una sucesión M-regular y defínase

   $$M' := M/(a_1, \ldots, a_n)M.$$

   Entonces M es de Cohen-Macaulay syss M' lo es.

3. Si M es de Cohen-Macaulay, entonces para todo primo $\mathfrak{p} \lhd A$ se cumple que $M_\mathfrak{p}$ es un $A_\mathfrak{p}$-módulo de Cohen-Macaulay. Además, si $M_\mathfrak{p} \neq 0$, entonces $\operatorname{prof}(\mathfrak{p}, M) = \operatorname{prof}_{A_\mathfrak{p}}(M_\mathfrak{p})$

Demostración:

1. Basta notar que

$$\begin{aligned} k.\dim M = k.\dim(M/\operatorname{Ann}(M)) &= \sup\{k.\dim(A/\mathfrak{p}) : \mathfrak{p} \in \operatorname{As}(M)\} \\ &\geq \text{ínf}\{k.\dim(A/\mathfrak{p}) : \mathfrak{p} \in \operatorname{As}(M)\} \geq \operatorname{prof} M, \end{aligned}$$

   y como $k.\dim M = \operatorname{prof} M$ porque M es de Cohen-Macaulay, concluímos.

2. Por el lema de Nakayama, $M = 0$ syss $M' = 0$. Por definición, $\operatorname{prof} M' = \operatorname{prof} M - r$ y por teorema de los ideales principales de Krull (prop. 5.19) tenemos que $k.\dim(M') = k.\dim M - r$.

3. Si $M_\mathfrak{p} = 0$ todo es trivial, así que supongamos que $M_\mathfrak{p} \neq 0$. Como $\mathfrak{p} \supseteq \operatorname{Ann} M$ vemos que

$$k.\dim(M_\mathfrak{p}) \geq \operatorname{prof}(M_\mathfrak{p}) \geq \operatorname{prof}(\mathfrak{p}, M),$$

   así que basta probar que $d := \operatorname{prof}(\mathfrak{p}, M) \geq k.\dim(M_\mathfrak{p})$.

   Procedemos por inducción sobre d. En el caso $d = 0$ tenemos que $\mathfrak{p} \subseteq \mathfrak{q}$ para algún $\mathfrak{q} \in \operatorname{As} M$. Pero $\operatorname{Ann}(M) \subseteq \mathfrak{p} \subseteq \mathfrak{q}$ y los primos asociados a M son exactamente los primos $\subseteq$-minimales que contienen a $\operatorname{Ann}(M)$, luego es claro.

   En el caso $d > 0$, sea a un elemento M-regular y sea $N := M/aM$. Como la localización es un funtor exacto, entonces a es $M_\mathfrak{p}$-regular, así que

$$k.\dim(N_\mathfrak{p}) = k.\dim(M_\mathfrak{p}/aM_\mathfrak{p}) = k.\dim(M_\mathfrak{p}) - 1$$

   por ideales principales de Krull y $\operatorname{prof}(\mathfrak{p}, N) = \operatorname{prof}(\mathfrak{p}, M) - 1$. Por hipótesis inductiva, N es de Cohen-Macaulay, así concluimos. □

Teorema 5.39: Sea $(A, \mathfrak{m})$ un anillo de Cohen-Macaulay local. Se cumplen:

1. Para toda sucesión $a_1, \ldots, a_r \in \mathfrak{m}$ son equivalentes:

   (*a*) La sucesión es A-regular.

(*b*) Para todo $i \leq r$ se cumple que $\operatorname{alt}(a_1, \ldots, a_i) = i$.

(*c*) $\operatorname{alt}(a_1, \ldots, a_r) = r$.

(*d*) Se pueden añadir elementos $a_{r+1}, \ldots, a_n \in \mathfrak{m}$ con $n := k.\dim A$ de modo que $a_1, \ldots, a_n$ forman un sistema de parámetros de A.

2. Para todo ideal propio $\mathfrak{a} \lhd A$ se tiene

$$\operatorname{alt}\mathfrak{a} = \operatorname{calidad}\mathfrak{a}, \qquad \operatorname{alt}\mathfrak{a} + k.\dim(A/\mathfrak{a}) = k.\dim A.$$

3. A es catenario.

Demostración:

1. Defínase $\mathfrak{a} := (a_1, \ldots, a_r)$.

   $(a) \implies (b)$. Por teorema de los ideales principales de Krull, tenemos que $\operatorname{alt}\mathfrak{a} \leq r$. Si la sucesión es A-regular, entonces vamos probando por inducción sobre i que $\operatorname{alt}(a_1, \ldots, a_i) = i$.

   $(b) \implies (c)$. Trivial.

   $(c) \implies (d)$. Si $r = k.\dim A$, entonces es trivial. Si $r < k.\dim A$, entonces $\mathfrak{m}$ no es un primo $\subseteq$-minimal que contiene a $\mathfrak{a}$ (por teorema de los ideales principales de Krull), luego existe $a_{r+1} \in \mathfrak{m}$ tal que no pertenece a ningún primo asociado minimal de $\mathfrak{a}$ y así continuamos recursivamente.

   $(d) \implies (a)$. Basta probar que todo sistema de parámetros $b_1, \ldots, b_n$ es una sucesión A-regular. Si $\mathfrak{p} \in \operatorname{As} A$, entonces $k.\dim(A/\mathfrak{p}) = n$ por el teorema anterior, inciso 1; luego $b_1 \notin \mathfrak{p}$. Así pues, b_1 es A-regular. Definiendo $\overline{A} := A/b_1A$, entonces es un anillo de Cohen-Macaulay (por el teorema anterior, inciso 2) y de dimensión $n-1$ (por ideales principales de Krull) y $\bar{b}_2, \ldots, \bar{b}_n$ forman una sucesión $\overline{A}$-regular y concluimos por inducción.

2. Sea $\mathfrak{a}$ de $\operatorname{alt}\mathfrak{a} = r$. Entonces podemos construir una sucesión $a_1, \ldots, a_r \in \mathfrak{a}$ tal que $\operatorname{alt}(a_1, \ldots, a_i) = i$ para $1 \leq i \leq r$, de modo que, por el inciso anterior, es una sucesión A-regular. Luego $\operatorname{alt}\mathfrak{a} = r \leq \operatorname{calidad}\mathfrak{a}$. Recíprocamente, para toda sucesión A-regular $b_1, \ldots, b_s \in \mathfrak{a}$ se tiene que $\operatorname{alt}(b_1, \ldots, b_s) \leq \operatorname{alt}\mathfrak{a}$, por lo que $\operatorname{calidad}\mathfrak{a} \leq \operatorname{alt}\mathfrak{a}$ y se alcanza la igualdad.

   Por definición,

$$\operatorname{alt}\mathfrak{a} = \operatorname{ínf}\{\operatorname{alt}\mathfrak{p} : \mathfrak{p} \supseteq \mathfrak{a}\}, \qquad k.\dim(A/\mathfrak{a}) = \sup\{k.\dim(A/\mathfrak{p}) : \mathfrak{p} \supseteq \mathfrak{a}\},$$

por lo que basta probar que $\operatorname{alt}\mathfrak{p} + k.\dim(A/\mathfrak{p}) = k.\dim A$ para $\mathfrak{p} \lhd A$ primo. Como $k.\dim A = \operatorname{prof} A = n$, entonces $r := \operatorname{alt}\mathfrak{p} = k.\dim(A_{\mathfrak{p}}) = \operatorname{prof}(\mathfrak{p}, A)$, por el teorema anterior. Así pues, existe una sucesión A-regular $a_1, \ldots, a_r \in \mathfrak{p}$, de modo que $A/(a_1, \ldots, a_r)$ es de Cohen-Macaulay y dimensión $n - r$ y $\mathfrak{p}$ es un primo asociado minimal a $(a_1, \ldots, a_r)$, por lo que $k.\dim(A/\mathfrak{p}) = n - r$ como se quería probar.

3. Ejercicio para el lector. □

Teorema 5.40: Sea $(A, \mathfrak{m}, k)$ un anillo noetheriano local. Entonces $\operatorname{prof} A = \operatorname{prof} \hat{A}$ y, en consecuencia, A es de Cohen-Macaulay syss $\hat{A}$ lo es.

Demostración: Para probar la igualdad de profundidad, empleamos la equivalencia con Ext y vemos que

$$\operatorname{Ext}^i_A(A/\mathfrak{m}, A) \otimes_A \hat{A} = \operatorname{Ext}^i_{\hat{A}}(\hat{A}/\hat{\mathfrak{m}}, \hat{A}).$$

La parte de «en consecuencia» es porque $k.\dim A = k.\dim \hat{A}$ (prop. 1.54). □

Definición 5.41: Se dice que un dominio A es un ***anillo de Cohen-Macaulay*** si para todo primo $\mathfrak{p} \lhd A$ se cumple que $A_{\mathfrak{p}}$ es de Cohen-Macaulay local.

Éste proceso de dar una definición $\mathcal{P}$ para anillos locales, y luego generalizarlo diciendo que un anillos satisfacen $\mathcal{P}$ syss todas sus localizaciones satisfacen $\mathcal{P}$ es muy común en álgebra conmutativa (y en teoría de esquemas). El teorema 5.38 nos da lo siguiente:

Corolario 5.41.1: Un anillo A es de Cohen-Macaulay syss para todo maximal $\mathfrak{m} \lhd A$ se cumple que $A_{\mathfrak{m}}$ es de Cohen-Macaulay.

Definición 5.42: Sea A un dominio noetheriano. Se dice que un ideal $\mathfrak{a} \lhd A$ es ***puro***[2] si $\operatorname{alt}\mathfrak{p} = \operatorname{alt}\mathfrak{a}$ para todo $\mathfrak{p} \in \operatorname{As}_A(A/\mathfrak{a})$.

Por definición, todo ideal puro es tal que $A/\mathfrak{a}$ no posee primos encajados. Nótese que por el teorema 5.38, inciso 1, se tiene que en todo anillo de Cohen-Macaulay, el ideal (1) es puro.

[2] eng. *unmixed*. Se opta (de manera inoficial) por el término *puro* en lugar de «sin mezclar» porque hace un paralelo con la definición de espacio topológico de *dimensión (combinatórica) pura*.

Teorema 5.43: Sea A un dominio noetheriano. Son equivalentes:

1. A es de Cohen-Macaulay.
2. **Teorema de la pureza:** Si $\mathfrak{a} = (a_1, \ldots, a_r)$ es un ideal de $\operatorname{alt} \mathfrak{a} = r$, entonces es puro.

Demostración: $1 \implies 2$. Sea A de Cohen-Macaulay y sea $\mathfrak{a} = (a_1, \ldots, a_r)$ de altura r. Sea $\mathfrak{p} \in \operatorname{As}_A(A/\mathfrak{a})$. Luego, podemos localizar y ver que $A_\mathfrak{p}$ es de Cohen-Macaulay local con $\mathfrak{p}^e$ maximal, y, luego, $\overline{A} := A_\mathfrak{p}/\mathfrak{a}$ también es de Cohen-Macaulay. Pero, claramente $(1) \trianglelefteq \overline{A}$ es de Cohen-Macaulay, luego es puro, por lo que $\operatorname{alt} \mathfrak{p} = \operatorname{alt} \mathfrak{a}$, como se quería probar.

$2 \implies 1$. Sea $\mathfrak{p} \lhd A$ un ideal de altura r, luego existen $a_1, \ldots, a_r \in \mathfrak{p}$ tales que $\operatorname{alt}(a_1, \ldots, a_i) = i$ para todo $i \leq r$. Por definición, $(a_1, \ldots, a_i)$ es puro, por lo que $a_{i+1} \notin \mathfrak{q}$ para todo $\mathfrak{q}$ asociado a $A/(a_1, \ldots, a_i)$. Así pues, $a_1, \ldots, a_r$ es una sucesión A-regular en $\mathfrak{p}$, por lo que

$$r \leq \operatorname{prof}(A_\mathfrak{p}) \leq k.\dim(A_\mathfrak{p}) = r,$$

por lo que $A_\mathfrak{p}$ es de Cohen-Macaulay. □

La equivalencia anterior, pese a parecer técnica, es altamente útil.

Teorema 5.44: Si A es de Cohen-Macaulay, entonces $A[x_1, \ldots, x_n]$ también. En consecuencia, todo anillo que es de Cohen-Macaulay y todo cociente suyo son universalmente catenarios.

Demostración: Basta probar que $B := A[x]$ es de Cohen-Macaulay. Sea $\mathfrak{n} \lhd B$ un ideal maximal y sea $\mathfrak{m} := \mathfrak{n} \cap A$, entonces $B_\mathfrak{n}$ es una localización de $A_\mathfrak{m}[x]$, así que sustituyendo A con $A_\mathfrak{m}$ (el cual es de Cohen-Macaulay por teorema 5.38), podemos suponer que $(A, \mathfrak{m}, k)$ es de Cohen-Macaulay local. Así pues, $B/\mathfrak{m}B \cong k[x]$, de modo que $\mathfrak{n}/\mathfrak{m}B$ es un ideal principal generado por un polinomio mónico irreducible $g(x) \in k[x]$. Sea $f(x) \in A[x]$ un polinomio mónico tal que $f(x) \equiv g(x) \pmod{\mathfrak{m}}$, entonces $\mathfrak{n} := (\mathfrak{m}, f)$. Sea $a_1, \ldots, a_n$ un sistema de parámetros de A, de modo que $a_1, \ldots, a_n, f$ forman un sistema de parámetros de $B_\mathfrak{n}$. Como B es un A-módulo plano, entonces la sucesión A-regular $a_1, \ldots, a_n$ es también B-regular. Sea $\overline{A} := A/(a_1, \ldots, a_n)$, luego la imagen de $f(x)$ es mónico en $\overline{A}[x]$ y, por tanto, es $\overline{A}[x]$-regular, de modo que $a_1, \ldots, a_n, f$ es una sucesión B-regular y

$$\operatorname{prof}(B_\mathfrak{n}) \geq \operatorname{prof}(\mathfrak{n}, B) \geq n + 1 = k.\dim(B_\mathfrak{n}).$$ □

Una equivalencia similar al del teorema de la pureza es «pureza de calidad»:

Teorema 5.45: Sea A un anillo de Cohen-Macaulay y M un A-módulo finitamente generado con $\operatorname{proj\,dim} M < \infty$.

1. Si M es perfecto, entonces es un módulo de Cohen-Macaulay.
2. Si A es local y M es de Cohen-Macaulay, entonces es perfecto.

Demostración: Sea M perfecto y $\mathfrak{p} \in \operatorname{Supp} M$, entonces $M_{\mathfrak{p}}$ es perfecto (cfr. demostración de 5.33), de modo que podemos reducirnos al caso de A local. Por la fórmula de Auslander-Buchsbaum $\operatorname{proj\,dim} M = k.\dim A - \operatorname{prof} M$, mientras que por el teorema 5.39 vemos que $\operatorname{calidad} M = k.\dim A - k.\dim M$. Así concluimos que la igualdad $\operatorname{prof} M = k.\dim M$ se da syss $\operatorname{proj\,dim} M = \operatorname{calidad} M$. □

Mediante el teorema de la pureza es fácil verificar a mano que todo anillo local regular es Cohen-Macaulay, pero veremos otro camino empleando planitud.

Proposición 5.46: Sean $(A, \mathfrak{m}, k)$ y $(B, \mathfrak{n})$ un par de anillos locales noetherianos con $\varphi\colon A \to B$ un homomorfismo. Sean M un A-módulo finitamente generado y N un B-módulo finitamente generado que es plano sobre A. Entonces $M \otimes_A N$ es de Cohen-Macaulay (sobre A) syss M es de Cohen-Macaulay y $N/\mathfrak{m}N \cong N \otimes_A k$ es de Cohen-Macaulay sobre B.

Demostración: Esto se deduce de, por un lado, calcular la profundidad del tensor (prop. 5.21) y, por otro, calcular la dimensión del tensor; y concluir pues $\operatorname{prof} S \leq k.\dim S$. □

Teorema 5.47: Sea A un anillo noetheriano, M un A-módulo finitamente generado y sea $B := A[\boldsymbol{x}]$ o $B := A[[\boldsymbol{x}]]$. Entonces M es de Cohen-Macaulay (sobre A) syss $M \otimes_A B$ es de Cohen-Macaulay sobre B.

Demostración: Por inducción nos reducimos al caso de una sola indeterminada $\boldsymbol{x} = x$.

$\Longleftarrow$. En ambos casos, x es $(M \otimes B)$-regular, $B/(x) \cong A$ y $(M \otimes B)/x(M \otimes B) \cong M$.

$\Longrightarrow$. Sea $\mathfrak{m} \lhd B$ un maximal, y sea $\mathfrak{p} := \mathfrak{m} \cap A$. Como A es Cohen-Macaulay, es catenario y luego es fácil verificar que $B_{\mathfrak{m}}/\mathfrak{p}B_{\mathfrak{m}}$ es un dominio

Revisar conclusión, Bruns y Herzog [2, pág. 60].

de valuación discreta, luego es regular y Cohen-Macaulay, por lo que, basta aplicar la proposición anterior. □

Teorema 5.48: Todo anillo local regular es de Cohen-Macaulay.

§5.3.1 Complejos de Koszul y módulos de Cohen-Macaulay.

Definición 5.49: Dado un anillo A y una tupla $\boldsymbol{a} := (a_1, \dots, a_n) \in A^n$, definimos el ***complejo de Koszul*** $(K_\bullet(\boldsymbol{a}), \mathrm{d}_\bullet)$ como prosigue: $K_0 := A$, $K_p := \bigoplus_\beta Ae_\beta$ donde $\beta := (\beta_1, \dots, \beta_p)$ con $1 \leq \beta_1 < \cdots < \beta_p \leq n$ para $1 \leq p \leq n$ y $K_p = 0$ en otro caso. El diferencial $\mathrm{d}_p \colon K_p \to K_{p-1}$ con $1 \leq p \leq n$ se define sobre la base como:

$$\mathrm{d}_p(e_{\beta_1,\dots,\beta_p}) := \sum_{r=1}^{p} (-1)^{r-1} a_{\beta_r} e_{\beta_1,\dots,\beta_{r-1},\beta_{r+1},\dots,\beta_p},$$

es fácil comprobar que $\mathrm{d}_{p+1} \circ \mathrm{d}_p = 0$. Para un A-módulo M se define $K_\bullet(\boldsymbol{a}, M) := K_\bullet(\boldsymbol{a}) \otimes_A M$ y para un complejo $C_\bullet$ se define $C_\bullet(\boldsymbol{a}) := K_\bullet(\boldsymbol{a}) \otimes_A C_\bullet$. Los (módulos) de ***homología de Koszul*** son:

$$H_p^{\mathrm{K}}(\boldsymbol{a}, M) := H_p(K_\bullet(\boldsymbol{a}, M)) = \frac{\ker(\mathrm{d}_p)}{\mathrm{Img}(\mathrm{d}_{p+1})}.$$

Una pequeña aclaración es que el producto tensorial de complejos $C_\bullet$ y $D_\bullet$ se define:

$$(C_\bullet \otimes_A D_\bullet)_n := \bigoplus_{p+q=n} C_p \otimes_A D_q,$$

con el diferencial, definido sobre el sistema generador:

$$\forall a \in C_p, b \in D_q, \quad \mathrm{d}_n(a \otimes b) := \mathrm{d}_p^C a \otimes b + (-1)^p a \otimes \mathrm{d}_q^D b.$$

Ejemplo 5.50: Sea A un dominio y M un A-módulo.

1. Dado un elemento $a \in A$, entonces

$$K_\bullet(a)\colon \qquad \cdots \longleftarrow 0 \longleftarrow A \xleftarrow{\times a} A \longleftarrow 0 \longleftarrow \cdots$$

2. Dada una tupla $\boldsymbol{a} := (a_1, \dots, a_n) \in A^n$ que genera el ideal $\mathfrak{a} \trianglelefteq A$, se cumple que

$$H_0^{\mathrm{K}}(\boldsymbol{a}, M) = M/\mathfrak{a}M, \qquad H_n^{\mathrm{K}}(\boldsymbol{a}, M) \cong \{u \in M : \mathfrak{a} \subseteq \operatorname{Ann} u\}. \qquad \lrcorner$$

Teorema 5.51: Sea A un dominio, $a \in A$ un elemento y $C_\bullet$ un complejo de A-módulos. Entonces existe una sucesión exacta

$$0 \longrightarrow C_\bullet \longrightarrow C_\bullet(a) \longrightarrow C_\bullet[-1] \longrightarrow 0,$$

de complejos que induce la sucesión exacta larga:

$$\cdots \longrightarrow H_p(C_\bullet) \longrightarrow H_p(C_\bullet(a)) \longrightarrow H_{p-1}(C_\bullet) \xrightarrow{\partial} H_{p-1}(C_\bullet) \longrightarrow \cdots$$

donde $\partial([u]) = [(-1)^{p-1}au]$ es el homomorfismo conector.

5.4* Anillos de Gorenstein

Lema 5.52: Sea A un dominio, M un A-módulo y $n \geq 0$ un entero. Son equivalentes:

1. $\operatorname{inj\,dim} M \leq n$.
2. Para todo ideal $\mathfrak{a} \trianglelefteq A$ se tiene que $\operatorname{Ext}_A^{n+1}(A/\mathfrak{a}, M) = 0$.

Si además A es noetheriano, entonces son equivalentes a:

3. Para todo primo $\mathfrak{p} \trianglelefteq A$ se tiene que $\operatorname{Ext}_A^{n+1}(A/\mathfrak{p}, M) = 0$.

Demostración: $1 \implies 2$. Basta recordar que el $\operatorname{Ext}_A^\bullet(A/\mathfrak{a}, M)$ se calcula mediante resoluciones inyectivas.

$2 \implies 1$. Procedemos por inducción. Si $n = 0$ entonces empleando la sucesión exacta $0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0$ vemos que $\operatorname{Ext}^1(A/\mathfrak{a}, M) = 0$ implica que $\operatorname{Hom}(A, M) \to \operatorname{Hom}(\mathfrak{a}, M)$ es un epimorfismo y, por lo tanto, M es inyectivo por el criterio de Baer.

Si $n > 0$, sea $Q^\bullet$ una resolución inyectiva de M y sea $C := \operatorname{coker}(Q^{n-2} \to Q^{n-1})$, de modo que tenemos la siguiente sucesión exacta:

$$C^\bullet: \qquad 0 \longrightarrow M \longrightarrow Q^0 \longrightarrow Q^1 \longrightarrow \cdots \longrightarrow Q^{n-1} \longrightarrow C \longrightarrow 0$$

donde cada Q^i es inyectivo. Es fácil comprobar que $\operatorname{Ext}_A^{n+1}(A/\mathfrak{a}, M) \cong \operatorname{Ext}^1(A/\mathfrak{a}, C)$ de modo que, nuevamente aplicando el criterio de Baer, obtenemos que C es inyectivo y, por lo tanto, $C^\bullet$ es una resolución inyectiva de M de largo n y, equivalentemente, $\operatorname{inj\,dim} M \leq n$.

$3 \iff 2$. La implicancia $2 \implies 3$ es obvia. Para la recíproca, empleamos descomposición de Lasker-Noether (corolario A.9.1) para ver que si N es un

A-módulo finitamente generado, entonces admite una cadena $0 = N_0 \subset N_1 \subset \cdots \subset N_m = N$ donde cada $N_i/N_{i-1} \cong A/\mathfrak{p}_i$ con $\mathfrak{p}_i \lhd A$ primo. Así pues, vemos que $\mathrm{Ext}^{n+1}(A/\mathfrak{p}, M) = 0$ para todo $\mathfrak{p} \lhd A$ primo, implica que $\mathrm{Ext}^{n+1}(N, M) = 0$ para todo A-módulo finitamente generado N, en particular, para $A/\mathfrak{a}$ con $\mathfrak{a} \trianglelefteq A$ ideal cualquiera. □

Lema 5.53: Sea A un anillo, sean M, N un par de A-módulos y sea $a \in A$ un elemento que es A-regular, M-regular y tal que $aN = 0$. Denotando $\overline{A} := A/aA$ y $\overline{M} := M/aM$, se tiene:

1. $\mathrm{Hom}_A(N, M) = 0$ y $\mathrm{Ext}^{n+1}_A(N, M) \cong \mathrm{Ext}^{n+1}_{\overline{A}}(N, \overline{M})$ para todo $n \geq 0$.
2. Para todo $n \geq 0$ se cumple $\mathrm{Ext}^n_A(M, N) \cong \mathrm{Ext}^n_{\overline{A}}(\overline{M}, N)$.
3. Para todo $n \geq 0$ se cumple $\mathrm{Tor}^A_n(M, N) \cong \mathrm{Tor}^{\overline{A}}_n(\overline{M}, N)$.

Demostración:

1. Para la primera afirmación basta construir el siguiente diagrama conmutativo:

$$\begin{array}{ccc} N & \xrightarrow{\varphi} & M \\ {\scriptstyle \times a}\downarrow \quad \downarrow 0 & & \downarrow{\scriptstyle \times a} \\ N & \xrightarrow[\varphi]{} & M \end{array}$$

□

5.5 Homologías

Definición 5.54: Sea A un anillo noetheriano y sea $j \in \mathbb{N}$, se definen las siguientes condiciones:

(S_j) Para todo primo $\mathfrak{p} \lhd A$ se cumple que $\mathrm{prof}(A_\mathfrak{p}) \geq \mathrm{mín}\{j, \mathrm{alt}\,\mathfrak{p}\}$, o equivalentemente para todo primo de calidad$(\mathfrak{p}) < j$, se cumple que $A_\mathfrak{p}$ es de Cohen-Macaulay.

Más generalmente, dado un A-módulo M, decimos que M satisface (S_j) si para todo $\mathfrak{p} \lhd A$ se cumple que $\mathrm{prof}(M_\mathfrak{p}) \geq \mathrm{mín}\{j, \mathrm{alt}\,\mathfrak{p}\}$.

(R_j) Para todo primo $\mathfrak{p} \lhd A$ de $\mathrm{alt}\,\mathfrak{p} \leq j$, se cumple que $A_\mathfrak{p}$ es regular.

La condición R_j se dice como «regular en codimensión $\leq j$».

Ejemplo.
- (S_0) siempre es cierta y podría pensarse que (S_∞) significa que el anillo es de Cohen-Macaulay.
- Se satisface (S_1) syss los primos de calidad $\mathfrak{p} = \operatorname{prof}(\mathfrak{p}, A) = 0$ (i.e., aquellos que sólo contienen divisores de cero) tienen $\operatorname{alt}\mathfrak{p} = 0$ syss los asociados del (0) tienen altura 0 syss A no tiene primos encajados.
- Se satisface (S_2) syss A y A/fA no tienen primos encajados, donde f recorre todos los elementos A-regulares.

Lema 5.55: Sea A un anillo noetheriano y M un A-módulo finitamente generado. Entonces M no tiene primos encajados syss M satisface (S_1).

Proposición 5.56: Un anillo noetheriano A es reducido syss satisface (R_0) y (S_1).

Demostración: $\Longrightarrow$. Si A es noetheriano, entonces para todo primo $\mathfrak{p} \lhd A$ de $\operatorname{alt}\mathfrak{p} = 0$, tenemos que $A_\mathfrak{p}$ es artiniano y reducido, luego es un cuerpo y, por tanto, es regular y se satisface (R_0).

Sea $\mathfrak{p}$ un primo de $\operatorname{alt}\mathfrak{p} \geq 1$ y sea $B := A_\mathfrak{p}$. Si su maximal $\mathfrak{m} := \mathfrak{J}(B)$ fuese un primo encajado, existiría $b \in \mathfrak{m}$ tal que $\operatorname{Ann} b = \mathfrak{m}$ y, por tanto, $b^2 = 0$ lo que es absurdo pues B es reducido. Así se satisface (S_1).

$\Longleftarrow$. Basta probar que $A_\mathfrak{p}$ es reducido para todo primo $\mathfrak{p} \lhd A$. Si $\operatorname{alt}\mathfrak{p} = 0$, entonces $A_\mathfrak{p}$ es regular (R_0), por lo que es un cuerpo y es reducido. Si $\operatorname{alt}\mathfrak{p} \geq 1$, entonces $\operatorname{prof}(A_\mathfrak{p}) \geq 1$ por (S_1), luego existe $a \in \mathfrak{p}A_\mathfrak{p}$ que no es divisor de cero (y limpiando denominadores, podemos suponer $a \in \mathfrak{p}$), o equivalentemente, tal que $A_\mathfrak{p} \to A_\mathfrak{p}[1/a]$ es inyectivo. Ahora bien, $A_\mathfrak{p}[1/a]$ se encaja dentro del producto de sus localizaciones, de modo que $A_\mathfrak{p}$ admite un monomorfismo a $\prod_\mathfrak{q} A_\mathfrak{q}$, donde $\mathfrak{q} \subset \mathfrak{p}$ y $a \notin \mathfrak{q}$. Por inducción sobre la altura de $\mathfrak{q}$ podemos ver que $A_\mathfrak{p}$ es reducido como se quería probar. □

Teorema 5.57 – *Criterio de normalidad de Serre*: Un anillo noetheriano A es normal syss satisface (R_1) y (S_2).

Demostración: $\Longrightarrow$. Sea $\mathfrak{p} \lhd A$ un ideal primo. Si $\operatorname{alt}\mathfrak{p} = 0$, entonces $A_\mathfrak{p}$ es íntegro y artiniano, luego es un cuerpo y es regular. Si $\operatorname{alt}\mathfrak{p} = 1$, entonces $A_\mathfrak{p}$ es normal, noetheriano y de dimensión 1, luego es un dominio de valuación discreta y así es regular, y además, es de Cohen-Macaulay por el teorema 5.48.

$\Longleftarrow$. Por la proposición anterior, A es reducido. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ los primos minimales de A, entonces $(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ y

$$A \hookrightarrow A_{\text{tot}} \cong \prod_{i=1}^{r} \operatorname{Frac}(A/\mathfrak{p}_i).$$

Veremos que A es íntegramente cerrado en A_{tot}: sea $(a/b) \in A_{\text{tot}}$ entero sobre A, vale decir, tal que existe

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \cdots + c_1(a/b) + c_0 = 0, \qquad c_i \in A,$$

o equivalentemente, $a^n + \sum_{i=0}^{n-1} c_i a^{n-i} b^i = 0$ y hay que probar que $a \in bA$. Como b no es divisor de cero, entonces es A-regular y el ideal bA es puro de altura 1 por (S_2), de modo que basta probar que $a \in bA_{\mathfrak{p}}$ para todo $\mathfrak{p}$ primo de $\operatorname{alt} \mathfrak{p} = 1$. Pero $A_{\mathfrak{p}}$ es regular por (R_1) y, por tanto, es normal. □

Definición 5.58: Sea $(A, \mathfrak{m}, k)$ un anillo local. Para todo homomorfismo de A-módulos $\varphi\colon M \to N$ denotamos $\overline{\varphi}\colon M \otimes_A k \to N \otimes_A k$. Dado un A-módulo finitamente generado M, un complejo:

$$(L_\bullet, \mathrm{d}_\bullet)\colon \qquad \cdots \longrightarrow L_n \xrightarrow{\mathrm{d}_n} \cdots \longrightarrow L_1 \xrightarrow{\mathrm{d}_0} L_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

se dice una ***resolución libre minimal*** si:

RLM1. Cada L_i es un A-módulo libre de rango finito.

RLM2. $\overline{\mathrm{d}_i} = 0$, es decir, $\mathrm{d}_i[L_i] \subseteq \mathfrak{m}L_{i-1}$.

RLM3. $\overline{\varepsilon}\colon L_1 \otimes_A k \to M \otimes_A k$ es un isomorfismo o, equivalentemente, ε es suprayectivo y $\ker(\varepsilon) \subseteq \mathfrak{m}M$.

Proposición 5.59: Sea A un anillo local y sea M un A-módulo finitamente generado.

1. Todo par de resoluciones libres minimales son isomorfas (como complejos).

2. Si $\boldsymbol{a} := (a_1, \ldots, a_n)$ es una sucesión A-regular, entonces el complejo de Koszul $K_\bullet(\boldsymbol{a})$ es una resolución libre minimal de $A/(a_1, \ldots, a_n)$.

3. Todo A-módulo finitamente generado posee una resolución libre minimal.

Lema 5.60: Sea $(A, \mathfrak{m}, k)$ un anillo local, sea M un A-módulo finitamente generado y sea $L_\bullet$ una resolución libre minimal de M. Entonces:

1. $\dim_k \operatorname{Tor}_i^A(M,k) = \operatorname{rang}_A L_i$ para todo i.
2. $\operatorname{proj\,dim} M = \sup\{i : \operatorname{Tor}_i^A(M,k) \neq 0\} \leq \operatorname{proj\,dim}_A k$.
3. Si $M \neq 0$ y $r := \operatorname{proj\,dim} M < \infty$, entonces para todo A-módulo finitamente generado $N \neq 0$ se cumple que $\operatorname{Ext}_A^r(M,N) \neq 0$.

Lema 5.61: Sean A un anillo y $n \geq 0$ un entero. Son equivalentes:

1. $\operatorname{proj\,dim} M \leq n$ para todo A-módulo M.
2. $\operatorname{proj\,dim} M \leq n$ para todo A-módulo M finitamente generado.
3. $\operatorname{inj\,dim} M \leq n$ para todo A-módulo M.
4. $\operatorname{Ext}_A^{n+1}(M,N) = 0$ para todo par de A-módulos M, N.

Definición 5.62: Sea A un anillo, llamamos su ***dimensión global***[3]

$$\begin{aligned}\operatorname{gl\,dim} A :&= \sup\{\operatorname{proj\,dim} M : A\text{-módulo } M\}\\ &= \sup\{\operatorname{inj\,dim} M : A\text{-módulo } M\}.\end{aligned}$$

Teorema 5.63 – *Teorema de regularidad de Serre*: Sea A un anillo local noetheriano. Son equivalentes:

1. A es regular.
2. $\operatorname{gl\,dim} A = k.\dim A$.
3. $\operatorname{gl\,dim} A < \infty$.

En cuyo caso, si $\mathfrak{p} \lhd A$ es primo, entonces $A_\mathfrak{p}$ también es regular.

Definición 5.64: Se dice que un anillo A es ***regular*** si para todo primo $\mathfrak{p} \lhd A$ se cumple que $A_\mathfrak{p}$ es local regular.

De éste modo, el teorema anterior nos dice que extiende a la definición usual.

[3] Grothendieck y Dieudonné [**EGA IV$_1$**] le llama *dimensión cohomológica* y le denota $\operatorname{dim\,coh} A$, u otros autores emplean $\operatorname{cd} A$.

Corolario 5.64.1: Todo anillo regular es Cohen-Macaulay y normal.

Demostración: Para ver que todo anillo regular es Cohen-Macaulay, basta reducirlo al caso local. Para ver que es normal, basta aplicar el criterio de normalidad de Serre, notando que (R_∞) es trivial y (S_∞) también por ser de Cohen-Macaulay. □

Ejemplo. $\mathbb{Z}$ es un anillo regular, luego es Cohen-Macaulay y, en particular, es universalmente catenario.

Notas históricas

Los métodos homológicos fueron arduamente desarrollados, y con buenos resultados, por el duo estadounidense **Maurice Auslander** y **David Buchsbaum**: por ejemplificar, la noción de *sucesión (cuasir)regular* la introdujeron ellos en [**13**] (1958). La noción de *calidad* es original de Rees [**34**] (1957). En la versión original de Serre [**7**] empleaba «codimensión homológica» para «profundidad»; en la traducción al inglés de C. Chin se modificó, pues la nomenclatura nunca pegó en la literatura.

La definición de *anillo de Cohen-Macaulay* es originaria de O. Zariski y P. Samuel, en tributo a los matemáticos I.S. Cohen y al británico **Fracis Sowerby Macaulay** (1862-1937). La denominación deriva de que Macaulay demostró que las álgebras polinomiales sobre un cuerpo satisfacen el teorema de la pureza, y I.S. Cohen probó que los anillos locales regulares también.

6

Derivaciones

6.1 Módulo de diferenciales de Kähler

Definición 6.1 – *Derivación*: Sea $f\colon k \to A$ una k-álgebra y sea M un A-módulo. Una aplicación $D\colon A \to M$ se dice una ***k-derivación*** si para todo $a, b \in A$:

D1. $D(a+b) = D(a) + D(b)$ (linealidad).

D2. $D(ab) = b\,D(a) + a\,D(b)$ (regla de Leibniz).

D3. $D(f(\lambda)) = 0$ para todo $\lambda \in k$.

Si A es un anillo arbitrario, decimos que D es una ***derivación*** si es una $\mathbb{Z}$-derivación. Denotamos por $\mathrm{Der}_k(A, M)$ al conjunto de k-derivaciones desde A a M, $\mathrm{Der}_k(A) := \mathrm{Der}_k(A, A)$ y obviamos el subíndice si $k = \mathbb{Z}$.

Ejemplo. Nótese que toda función $D\colon A \to M$ que satisface D1 y D2 es una $\mathbb{Z}$-derivación pues

$$D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1) \implies D(1) = 0.$$

Y $\mathbb{Z}$ está generado (como grupo) por 1.

Nótese que las derivaciones *no* son, en general, homomorfismos de A-módulos,

de lo contrario $D(a) = D(a \cdot 1) = a \cdot D(1) = 0$. No obstante, la condición D3 implica que sí son homomorfismos de k-módulos.

En el capítulo de teoría de Galois ya vimos las derivadas formales, pero en un contexto multivariable será necesario introducir el concepto de derivadas *parciales* formales:

Definición 6.2: Sean $\boldsymbol{x} = (x_1, \ldots, x_n)$ una tupla de indeterminadas. Dado $f(\boldsymbol{x}) \in k[\boldsymbol{x}]$ e $i \in \{1, \ldots, n\}$, entonces podemos ver $f(\boldsymbol{x}) = f(\boldsymbol{y})(x_i) =: g(x_i) \in k[\boldsymbol{y}][x_i]$, donde $\boldsymbol{y}$ es la tupla $\boldsymbol{x}$ sin la i-ésima coordenada, y definir

$$\frac{\partial f}{\partial x_i}(\boldsymbol{x}) := g'(x_i) \in k[\boldsymbol{y}][x_i] = k[\boldsymbol{x}].$$

Es decir, denotando $g(x_i) = \sum_{j=0}^{m} g_j x_i^j$ con $g_j \in k[\boldsymbol{y}]$ se tiene que

$$\frac{\partial f}{\partial x_i}(\boldsymbol{x}) = \sum_{j=1}^{m} j g_j x_i^{j-1} \in k[\boldsymbol{x}].$$

La regla de Leibniz nos permite notar que si $D_i \colon k[\boldsymbol{x}] \to k[\boldsymbol{x}]$ es la k-derivación dada por $D_i(x_j) = \delta_{ij}$, entonces $D_i(f(\boldsymbol{x})) = \frac{\partial f}{\partial x_i}(\boldsymbol{x})$.

Proposición 6.3: $\mathrm{Der}_k(A, -) \colon \mathsf{Mod}_A \to \mathsf{Set}$ determina un funtor:

$$\begin{array}{ccc} M & & \mathrm{Der}_k(A, M) \\ {\scriptstyle f}\downarrow & \xRightarrow{\mathrm{Der}_k(A,-)} & \downarrow{\scriptstyle h^f} \\ N & & \mathrm{Der}_k(A, N) \end{array}$$

Antes de introducir el objeto principal, veamos lo siguiente:

Lema 6.4: Sea $f \colon k \to A$ una k-álgebra y M un A-módulo. Entonces $A * M := A \oplus M$ con la multiplicación

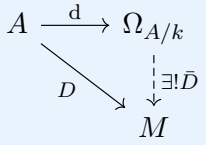
$$(a, \boldsymbol{m}) \cdot (b, \boldsymbol{n}) := (ab, a\boldsymbol{n} + b\boldsymbol{m})$$

es una k-álgebra; con $\lambda \mapsto (f(\lambda), \vec{0})$.

Proposición 6.5: Toda k-derivación $D \colon A \to M$ determina un k-monomorfismo $\iota_D \colon A \to A * M$ dado por $\iota_D(a) := (a, Da)$ tal que $\iota_D \circ \pi_A = \mathrm{Id}_A$. Recíprocamente, dado un k-monomorfismo $\psi \colon A \to A * M$ tal que $\psi \circ \pi_A = \mathrm{Id}_A$, entonces $\psi \circ \pi_M \colon A \to M$ es una k-derivación.

Teorema 6.6: Existe un par $(\Omega_{A/k}, \mathrm{d})$ tal que:

1. $\mathrm{d}\colon A \to \Omega_{A/k}$ es una k-derivación.
2. Para toda k-derivación $D\colon A \to M$ existe un único homomorfismo de A-módulos $\bar{D}\colon \Omega_{A/k} \to M$ tal que $D = \mathrm{d} \circ \bar{D}$. Es decir, tal que el siguiente diagrama conmuta:



En resumen, $\mathrm{Der}_k(A, -)$ es un funtor representable que está representado por $\Omega_{A/k}$.

Demostración: En primer lugar, considere el siguiente epimorfismo de k-álgebras:

$$\begin{aligned} \mu\colon A \otimes_k A &\longrightarrow A \\ a \otimes b &\longmapsto ab. \end{aligned}$$

Luego definamos lo siguiente:

$$\mathfrak{a} := \ker \mu, \quad \Omega_{A/k} := \mathfrak{a}/\mathfrak{a}^2, \quad B := (A \otimes_k A)/\mathfrak{a}^2.$$

Como $\mathfrak{a}^2 \subseteq \ker \mu$, entonces se induce la siguiente sucesión exacta (en Alg_k):

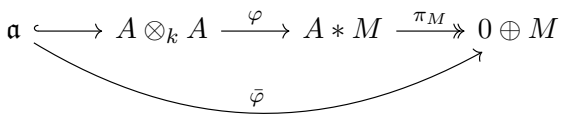
$$0 \longrightarrow \Omega_{A/k} \xrightarrow{\iota} B \xrightarrow{\bar{\mu}} A \longrightarrow 0$$

Definiendo $\lambda_i\colon A \to B$ dados por $\lambda_1(a) := a \otimes 1 \pmod{\mathfrak{a}^2}$ y $\lambda_2(a) := 1 \otimes a \pmod{\mathfrak{a}^2}$ vemos que $\lambda_i \circ \bar{\mu} = \mathrm{Id}_A$, de modo que la sucesión de arriba se escinde. Definamos $\mathrm{d} := \lambda_2 - \lambda_1\colon A \to B$, por exactacitud de la sucesión de arriba, vemos que, de hecho, $\mathrm{d}\colon A \to \Omega_{A/k}$.

Veamos que $(\Omega_{A/k}, \mathrm{d})$ es efectivamente el objeto representado: Sea $D \in \mathrm{Der}_k(A, M)$, entonces determina un k-homomorfismo:

$$\begin{aligned} \varphi\colon A \otimes_k A &\longrightarrow A * M \\ a \otimes b &\longmapsto (ab, aDb). \end{aligned}$$

Nótese que φ es el homomorfismo diagonal $\mu\Delta\iota_D$. De modo que, si nos restringimos al $\ker \mu = \mathfrak{a}$ obtenemos una aplicación que se anula en la primera coordenada. Y podemos definir:



Ahora bien, $(0 \oplus M)^2 = 0$ (con multiplicación en $A * M$), de modo que $\mathfrak{a}^2 \subseteq \ker \bar{\varphi}$ e induce un homomorfismo de A-módulos $\bar{D}\colon \mathfrak{a}/\mathfrak{a}^2 = \Omega_{A/k} \to M$. Para todo $a \in A$ notemos que

$$\begin{aligned}\bar{D}(\mathrm{d}a) &= \bar{D}(1 \otimes a - a \otimes 1 \text{ mód } \mathfrak{a}^2) = \varphi(1 \otimes a) - \varphi(a \otimes 1) \\ &= \pi_M(a, D(a)) - \pi_M(a, D(1)) = \pi_M(0, Da) = Da.\end{aligned}$$

De modo que $\mathrm{d} \circ \bar{D} = D$ como se quería probar.

Ahora queremos ver la unicidad de $\bar{D}$. Para ello probaremos algo distinto: sea $a \otimes b \in \mathfrak{a}$, nótese que $ab \otimes 1 \in \mathfrak{a}$ también. Nótese que $\Omega_{A/k}$ es un A-módulo con la multiplicación por $a \otimes 1$, y nótese que

$$a \otimes b = (a \otimes 1)(1 \otimes b - b \otimes 1) + ab \otimes 1,$$

de modo que si $\omega = \sum_{i=1}^n a_i \otimes b_i \in \mathfrak{a}$, entonces

$$\omega = \sum_{i=1}^n a_i \,\mathrm{d}b_i + \sum_{i=1}^n (a_i b_i \otimes 1) = \sum_{i=1}^n a_i \,\mathrm{d}b_i + \cancelto{0}{\left(\sum_{i=1}^n a_i b_i\right)} \otimes 1 = \sum_{i=1}^n a_i \,\mathrm{d}b_i.$$

En consecuente, $\Omega_{A/k}$ está generado por los diferenciales $\{\mathrm{d}a : a \in A\}$. Luego la unicidad de $\bar{D}$ es clara. □

Definición 6.7: Al $(\Omega_{A/k}, \mathrm{d}_{A/k})$ le llamamos el ***módulo de diferenciales de Kähler*** de A sobre k. Para todo $a \in A$ llamamos a $\mathrm{d}_{A/k}a \in \Omega_{A/k}$ el ***diferencial*** de a. Obviamos el subíndice en $\mathrm{d}_{A/k}$ de no haber ambigüedad.

De la demostración probamos:

Corolario 6.7.1: El A-módulo $\Omega_{A/k}$ está generado por $\{\mathrm{d}a : a \in A\}$. Más aún, si k es un cuerpo y A es una k-álgebra de tipo finito, entonces $\Omega_{A/k}$ está generado por a lo más $\mathrm{trdeg}_k(A)$ elementos.

Demostración: Probaremos la segunda afirmación: Si $A = k[a_1, \ldots, a_n]$ para algunos $a_i \in A$, entonces todo $b \in A$ es de la forma $b = f(\boldsymbol{a})$ donde $f(\boldsymbol{x}) \in k[\boldsymbol{x}]$. Luego es fácil notar que

$$\mathrm{d}b = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(\boldsymbol{a}) \,\mathrm{d}a_i.$$ □

Ejemplo. Si $A = k[x_1, \ldots, x_n]$, entonces $\Omega_{A/k}$ es un A-módulo libre generado por los n elementos $\mathrm{d}x_1, \ldots, \mathrm{d}x_n$. Por la demostración anterior, es claro que éstos elementos generan el módulo, y como existe una derivación $D_i \colon A \to A$ tal que $D_i(x_j) = \delta_{ij}$, entonces vemos que los elementos $\mathrm{d}x_i$ son A-linealmente independientes.

Definición 6.8: Una k-álgebra A se dice 0-***suave*** sobre k si para toda k-álgebra B, todo ideal $\mathfrak{n} \trianglelefteq B$ tal que $\mathfrak{n}^2 = 0$ y todo k-homomorfismo $u \colon A \to B/\mathfrak{n}$ existe un k-homomorfismo $v \colon A \to B$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} A & \xrightarrow{u} & B/\mathfrak{n} \\ \uparrow & \overset{v}{\swarrow} & \uparrow\!\uparrow \\ k & \dashrightarrow & B \end{array} \tag{6.1}$$

Una k-álgebra A se dice 0-***no ramificada*** sobre k si existe a lo más un k-homomorfismo $v \colon A \to B$ tal que el diagrama (6.1) conmuta. Una k-álgebra A se dice 0-***étale*** sobre k si es 0-suave y 0-no ramificada.

Proposición 6.9: A es 0-no ramificada sobre k syss $\Omega_{A/k} = 0$.

Demostración: $\Longrightarrow$. Por la proposición 6.5 hay una correspondencia entre $\mathrm{Der}_k(A, M)$ y k-homomorfismos $\varphi \colon A \to A * M$ tales que

$$\begin{array}{ccc} A & = & A = \frac{A*M}{M} \\ \uparrow & \overset{\varphi}{\swarrow} & \uparrow\!\uparrow \\ k & \dashrightarrow & A * M \end{array}$$

conmuta. Por definición de 0-no ramificada, φ es único y luego $0 = \mathrm{Der}_k(A, M) \cong \mathrm{Hom}_A(\Omega_{A/k}, M)$ por lo que $\Omega_{A/k} = 0$.

$\Longleftarrow$. Mirando la construcción de $\Omega_{A/k}$ recordamos que $\mathfrak{a}/\mathfrak{a}^2$ se anula en $(A \otimes_k A/\mathfrak{a}) =: B$, luego obtenemos:

$$\begin{array}{ccc} A & \rightsquigarrow & A = \frac{A \otimes_k A/\mathfrak{a}}{\mathfrak{a}/\mathfrak{a}^2} \\ \uparrow & \overset{\lambda_1}{\underset{\lambda_2}{\swarrow}} & \uparrow \bar{\mu} \\ k & \dashrightarrow & B \end{array}$$

de modo que $\lambda_1 = \lambda_2$ y $\mathrm{d} = 0$, por lo que, $\Omega_{A/k} = 0$. $\square$

Teorema 6.10 – *Primera sucesión fundamental*: Dados $f\colon k \to A, g\colon A \to B$ homomorfismos de anillos, se tiene la siguiente sucesión exacta (en Mod_B):

$$\Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \longrightarrow 0 \tag{6.2}$$

donde $\alpha(\mathrm{d}_{A/k}a \otimes b) = b \cdot \mathrm{d}_{B/k}g(a)$ y $\beta(\mathrm{d}_{B/k}b) = \mathrm{d}_{B/A}b$ para todo $a \in A, b \in B$. Además, si B es 0-suave sobre A, entonces la siguiente sucesión

$$0 \longrightarrow \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \longrightarrow 0 \tag{6.3}$$

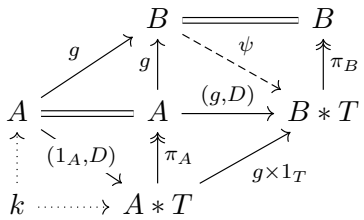
es exacta y se escinde.

Demostración: Por la proposición **??**, basta ver que la sucesión:

$$\mathrm{Der}_k(A, M) \xleftarrow{h_\alpha} \mathrm{Der}_k(B, M) \xleftarrow{h_\beta} \mathrm{Der}_A(B, M) \longleftarrow 0$$

es exacta (en Mod_B) para todo B-módulo M.

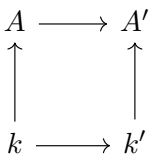
Si B es 0-suave, nos piden probar que h_α es además un epimorfismo. Para ello, sea $D \in \mathrm{Der}_k(A, M)$, entonces, por la correspondencia de la proposición 6.5 extraemos el siguiente diagrama conmutativo:



donde la existencia de ψ viene de la definición de 0-suave. Nuevamente la correspondencia 6.5 nos da una derivación lo que demuestra que h_α es epimorfismo. □

Veamos unos ejemplos sencillos:

Proposición 6.11: Dado el siguiente diagrama conmutativo de anillos:



Entonces:

1. Existe un homomorfismo canónico de A-módulos $\Omega_{A/k} \to \Omega_{A'/k'}$ y un homomorfismo canónico de A'-módulos $\Omega_{A/k} \otimes_A A' \to \Omega_{A'/k'}$.

2. Si $A' = A \otimes_k k'$, entonces el último homomorfismo del inciso anterior es un isomorfismo:

$$\Omega_{A'/k'} \cong \Omega_{A/k} \otimes_k k' \cong \Omega_{A/k} \otimes_A A'.$$

3. Si $S \subseteq A$ es un sistema multiplicativo, entonces $\Omega_{S^{-1}A/k} \cong S^{-1}\Omega_{A/k}$. En particular, si $\mathfrak{p} \lhd A$ es un primo, entonces $\Omega_{A_\mathfrak{p}/k} \cong (\Omega_{A/k})_\mathfrak{p}$.

Demostración:

1. El primer homomorfismo sale del siguiente diagrama conmutativo:

$$\begin{array}{ccc} A & \xrightarrow{\mathrm{d}_{A/k}} & \Omega_{A/k} \\ {\scriptstyle\varphi}\downarrow & & \vdots\,{\scriptstyle\exists!\psi} \\ A' & \xrightarrow[\mathrm{d}_{A'/k'}]{} & \Omega_{A'/k'} \end{array}$$

   donde $\varphi \circ \mathrm{d}_{A'/k'} \colon A \to \Omega_{A'/k'}$ es una k-derivación, de modo que induce la existencia y unicidad del A-homomorfismo ψ.

   Por cambio de base, tenemos

$$\mathrm{Hom}_{A'}(\Omega_{A/k} \otimes_A A', \Omega_{A'/k'}) \cong \mathrm{Hom}_A\left(\Omega_{A/k}, \mathrm{Hom}_{A'}(A', \Omega_{A'/k'})\right) \cong \mathrm{Hom}_A(\Omega_{A/k}, \Omega_{A'/k'}),$$

   y entonces mandamos ψ mediante estos isomorfismos (los cuales son todos canónicos).

2. En la demostración del teorema 6.6 construimos el ideal $\mathfrak{a} \lhd A \otimes_k A$ de modo que tenemos la sucesión exacta

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \otimes_k A \longrightarrow A \longrightarrow 0$$

   la cual se escinde (¿por qué?), de modo que tensorizamos por k' y tenemos la sucesión exacta

$$0 \longrightarrow \mathfrak{a} \otimes_k k' \longrightarrow A \otimes_k A \otimes k' = A' \otimes_{k'} A' \longrightarrow A' \longrightarrow 0.$$

Ahora, $\Omega_{A'/k'} = (\mathfrak{a} \otimes_k k')/(\mathfrak{a}^2 \otimes_k k') \cong \mathfrak{a}/\mathfrak{a}^2 \otimes_k k' = \Omega_{A/k} \otimes_k k'$ como se quería ver.

3. Este se deduce de notar que $S^{-1}A$ es una A-álgebra 0-étale y luego aplicar la primera sucesión fundamental. □

Teorema 6.12 – *Segunda sucesión fundamental*: Sea $f\colon k \to A$ un homomorfismo de anillos y considere $B = A/\mathfrak{m}$, donde $\mathfrak{m} \lhd A$ no es necesariamente un ideal maximal. La siguiente sucesión es exacta (en Mod_B):

$$\begin{aligned} \mathfrak{m}/\mathfrak{m}^2 &\xrightarrow{\ \delta\ } \Omega_{A/k} \otimes_A B \xrightarrow{\ \alpha\ } \Omega_{B/k} \longrightarrow 0 \\ x \text{ mód } \mathfrak{m}^2 &\longmapsto \mathrm{d}_{A/k}x \otimes 1. \end{aligned} \tag{6.4}$$

Además, si B es 0-suave sobre k, entonces la siguiente sucesión

$$0 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\ \delta\ } \Omega_{A/k} \otimes_A B \xrightarrow{\ \alpha\ } \Omega_{B/k} \longrightarrow 0 \tag{6.5}$$

es exacta y se escinde.

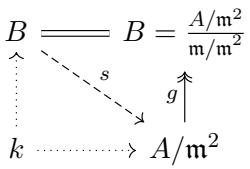
En primer lugar, nótese que en éste caso la proyección $g\colon A \to A/\mathfrak{m} = B$ es un epimorfismo, de modo que es fácil comprobar que el homomorfismo de B-módulos α de (6.2) es un epimorfismo; luego por exactitud $\Omega_{B/A} = 0$.

Demostración: La exactitud de (6.4) equivale, por la proposición **??**, a que para todo B-módulo arbitrario M se cumpla que la siguiente sucesión sea exacta:

$$\mathrm{Hom}_B(\mathfrak{m}/\mathfrak{m}^2, M) \xleftarrow{\ h_\delta\ } \mathrm{Der}_k(A, M) \xleftarrow{\ h_\alpha\ } \mathrm{Der}_k(B, M) \longleftarrow 0$$

Tenemos que $\ker(h_\alpha) = 0$ por la sucesión exacta 6.3. Sea $D \in \mathrm{Der}_k(A, M)$, nótese que $h_\delta(D) = 0$ equivale a que D se anule en $\mathfrak{m}$, de modo que podemos considerar a D como una k-derivación sobre $A/\mathfrak{m} = B$; lo que prueba la exactitud.

Si B es 0-suave sobre k, entonces debido al siguiente diagrama:



vemos que la sucesión exacta $0 \to \mathfrak{m}/\mathfrak{m}^2 \to A/\mathfrak{m}^2 \to B \to 0$ se escinde. Ahora bien, $g \circ s\colon A/\mathfrak{m}^2 \to A/\mathfrak{m}^2$ es un homomorfismo de B-módulos que se anula en $\mathfrak{m}/\mathfrak{m}^2$. Luego $D := 1 - g \circ s\colon A/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2$ es una k-derivación. Dado $\psi \in \mathrm{Hom}_B(\mathfrak{m}/\mathfrak{m}^2, M)$, entonces la composición:

$$D'\colon A \twoheadrightarrow A/\mathfrak{m}^2 \xrightarrow{D} \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\psi} M$$

es una k-derivación y para todo $x \in \mathfrak{m}$, denotando $\bar{x} := x$ mód $\mathfrak{m}^2$ se cumple:

$$D'(x) = \psi(D(\bar{x})) = \psi(\bar{x} - s(g(\bar{x}))) = \psi(\bar{x}),$$

de modo que h_δ es suprayectivo y basta sustituir $M = \mathfrak{m}/\mathfrak{m}^2$ para comprobar que la sucesión (6.5) se escinde. □

Teorema 6.13: Sea L/K una extensión algebraica separable de cuerpos. Entonces L es 0-étale sobre K y para todo subcuerpo $k \subseteq K$ se cumple que $\Omega_{L/k} = \Omega_{K/k} \otimes_K L$.

Demostración: Sea $0 \to \mathfrak{n} \to B \to B/\mathfrak{n} \to 0$ una extensión de K-álgebras con $\mathfrak{n}^2 = 0$ y sea $u\colon L \to B/\mathfrak{n}$ un K-homomorfismo fijo.

Dada una subextensión finita $L/L'/K$, por el teorema del elemento primitivo, tenemos que $L' = K(\alpha)$; sea f el polinomio minimal de α, entonces $L' = K[x]/(f)$ y $f'(\alpha) \neq 0$. Queremos elevar $u|_{L'}\colon L' \to B/\mathfrak{n}$ de forma única, para lo cual buscamos un elemento $\beta \in B$ tal que $f(\beta) = 0$ (para mandar $\alpha \mapsto \beta$) y β mód $\mathfrak{n} = u(\alpha)$. Sea β cualquier elemento tal que β mód $\mathfrak{n} = u(\alpha)$, entonces $f(\beta) \equiv u(f(\alpha)) = 0 \pmod{}n$ por lo que $f(\beta) \in \mathfrak{n}$. Para todo $\eta \in \mathfrak{n}$, expandiendo mediante binomios de Newton y recordando que $\eta^2 = 0$ se obtiene que

$$f(\beta + \eta) = f(\beta) + f'(\beta)\eta.$$

Ahora bien, $f'(\alpha) \in L$ es inversible y, como u es homomorfismo de álgebras, $u(f'(\alpha)) = f'(\beta)$ mód $\mathfrak{n}$ es inversible en $B/\mathfrak{n}$, pero como $\mathfrak{n} \subseteq \mathfrak{N}(B) \subseteq \mathfrak{J}(B)$, entonces $f'(\beta)$ es inversible en B. Definamos $\eta := -f(\beta)/f'(\beta) \in \mathfrak{n}$ y claramente $f(\beta + \eta) = 0$. Luego el K-homomorfismo $v_\alpha\colon K(\alpha) \to B$ dado por $v_\alpha(\alpha) = \beta + \eta$ factoriza a u y, de la construcción, es claramente único. Luego si hacemos variar $\alpha \in L$ llegamos a la existencia y unicidad de v_α de modo que definimos

$$\begin{aligned} v\colon L &\longrightarrow B \\ \alpha &\longmapsto v_\alpha(\alpha) \end{aligned}$$

(¿por qué está bien definido?) el cual cumple lo exigido.

Que $\Omega_{L/k} = \Omega_{K/k} \otimes_K L$ se deduce de la sucesión (6.3). □

En particular, el último teorema aplica siempre que $\operatorname{car} K = 0$.

Teorema 6.14: Sea K un cuerpo de $\operatorname{car} K =: p > 0$ y sea $0 \neq D \in \operatorname{Der}(K)$. Entonces:

1. $1, D, D^2, \ldots, D^{p-1}$ son K-linealmente independientes (donde D^i denota composición).
2. La aplicación $c_0 + c_1 D + \cdots + c_{p-1} D^{p-1}$ es una derivación syss cada $c_i = 0$.

Demostración: Para todo $a \in K$ denotemos $\mu_a(x) := ax$. Por regla de Leibniz $D(ax) = aDx + xDa$, o equivalentemente, $\mu_a \circ D = a \cdot D + \mu_{D(a)}$ y se puede probar (¡hágalo!) que en general

$$\mu_a \circ D^n = a \cdot D^n + \cdots = \sum_{j=0}^{n} \binom{n}{j} D^{n-j}(a) \cdot D^j,$$

(con el convenio de que $D^0 = \mathrm{Id}_K$).

1. Sea $n < p$ tal que $1, D, \ldots, D^{n-1}$ son K-linealmente independientes, pero D^n es linealmente dependiente a los anteriores. Luego
$$D^n = c_{n-1} D^{n-1} + \cdots + c_1 D + c_0. \tag{6.6}$$
Sea $a \in K$ tal que $D(a) \neq 0$. Entonces precompongamos por μ_a:
$$\mu_a \circ D^n = a \cdot D^n + nD(a) \cdot D^{n-1} + \cdots = ac_{n-1} \cdot D^{n-1} + \cdots$$
donde $\cdots$ representa combinaciones lineales de $1, D, \ldots, D^{n-2}$. Restamos a ambos lados la igualdad (6.6) multiplicada por a y reordenando términos obtenemos que
$$nD(a) \cdot D^{n-1} = \cdots$$
lo cual contradice la hipótesis de que $1, D, \ldots, D^{n-1}$ son linealmente independientes.

2. Supongamos, por contradicción, que $E := c_n D^n + \cdots + c_1 D + c_0$ es una derivación. En primer lugar, vemos que $0 = E(1) = c_0$, así que $n > 1$. Elegimos $a \in K$ tal que $D(a) \neq 0$ y precomponemos por μ_a:
$$a \cdot E + \mu_{E(a)} = \mu_a \circ E = ac_n \cdot D^n + (nD(a)c_n + ac_{n-1}) D^{n-1} + \cdots,$$
donde $\cdots$ nuevamente denota combinaciones lineales de $1, D, \ldots, D^{n-2}$. Como los D^i's son linealmente independientes, entonces hay una igualdad entre los coeficientes y en particular $nD(a)c_n = 0$ lo cual es absurdo pues ningún término es nulo. □

6.2 Separabilidad

Definición 6.15: Se dice que una k-álgebra A es ***separable*** si para toda extensión de cuerpos L/k se cumple que el álgebra $A \otimes_k L$ es reducida (i.e., no tiene nilpotentes).

Proposición 6.16: Sea k un cuerpo.

1. Si A es separable sobre k, entonces toda subálgebra $B \subseteq A$ también es separable.
2. A es separable syss toda subálgebra $B \subseteq A$ de tipo finito es separable.
3. A es separable syss para toda extensión L/k de tipo finito se cumple que la álgebra $A \otimes_k L$ es reducida.
4. Si A es separable, entonces para toda extensión de cuerpos L/k se cumple que $A \otimes_k L$ es separable sobre k.

Sea k un cuerpo y sea A una k-álgebra finitamente generada (como k-espacio vectorial). Para todo $\alpha \in A$, denotemos por $\mu_\alpha(x) := \alpha x$ el cuál es una k-transformación lineal, luego recuerde que

$$\mathrm{Tr}_{A/k}(\alpha) := \mathrm{tr}(\mu_\alpha).$$

Luego, la aplicación $(a, b) \mapsto \mathrm{Tr}_{A/k}(ab)$ es una forma bilineal y podemos definir:

Definición 6.17: Sea A una k-álgebra finitamente generada y sea $B := (\alpha_1, \ldots, \alpha_n)$ una k-base (lineal) ordenada de A. Se define el ***discriminante*** de A respecto a B como

$$\Delta_B(A/k) := \det\left([\mathrm{Tr}_{A/k}(\alpha_i\alpha_j)]_{ij}\right).$$

Si bien el discriminante de A depende de la elección de base, éste es único salvo cuadrados no nulos. En particular, el discriminante es nulo en una base syss lo es en todas.

Teorema 6.18: Sea k un cuerpo y A una k-álgebra finitamente generada. A es separable syss el discriminante de A es no nulo en alguna base (y luego en todas).

Demostración: $\Longleftarrow$. Demostraremos la contrarrecíproca: supongamos que A no es separable. Sea L/k una extensión finita de cuerpos y sea $A' := A \otimes_k L$ tal que $\mathfrak{N}(A') \neq 0$. Luego, A' es un L-espacio vectorial de dimensión finita y podemos elegir una base $X := (\beta_1, \ldots, \beta_n)$ tal que $\mathrm{Span}_L\{\beta_1, \ldots, \beta_r\} = \mathfrak{N}(A')$. Es fácil notar que $\mathrm{tr}(\beta_i\beta_j) = 0$ para $i \leq r$ y todo j (ésto debido a que $\beta_i\beta_j$ es nilpotente), luego $\Delta\, X = 0$.

$\Longrightarrow$. Sea $L := k^{\mathrm{alg}}$, entonces podemos considerar la álgebra $A \otimes_k L$, la cual es reducida. Así que podemos suponer, sin perdida de generalidad, que k es algebraicamente cerrado y A es reducida. Como A está finitamente generada, entonces $0 = \mathrm{trdeg}_k(A) = k.\dim(A)$ por lo que A es un dominio artiniano reducido y por el corolario A.17.1 es isomorfo a un producto directo de cuerpos, cada uno isomorfo a k, ergo $A = e_1k + \cdots + e_nk$ con $e_i \cdot e_j = \delta_{ij}$. Claramente $\Delta(\{e_1, \ldots, e_n\}) = 1 \neq 0$. □

Definición 6.19: Dada una extensión de cuerpos K/k, se le llama una ***base de trascendencia separable*** $\Gamma \subseteq K$ a una base de trascendencia tal que $K/k(\Gamma)$ es una extensión algebraica separable. De existir, se dice que K/k está ***separablemente generada***.

Teorema 6.20: Sea k un cuerpo. Una extensión de cuerpos K/k separablemente generada es una k-álgebra separable.

Demostración:

(a) Si K/k es una extensión algebraica: Entonces toda subextensión finita $K/K'/k$ es separable (como extensión) y, por el criterio anterior, basta ver que el discriminante es no nulo.

Por el teorema del elemento primitivo $K' = k(\gamma)$, luego $X := \{1, \gamma, \ldots, \gamma^{n-1}\}$ es una k-base lineal de K'. Sean $\{\sigma_1, \ldots, \sigma_n\}$ los k-monomorfismos de K' a su clausura normal y definamos $A := [\sigma_i(\gamma^{j-1})]_{ij}$. Nótese que

$$(A^t \cdot A)_{ij} = \sum_{\ell=1}^{n} \sigma_\ell(\gamma^{i-1})\sigma_\ell(\gamma^{j-1}) = \sum_{\ell=1}^{n} \sigma_\ell(\gamma^{i-1}\gamma^{j-1}) = \mathrm{Tr}_{K'/k}(\gamma^{i-1}\gamma^{j-1}).$$

De modo que $\Delta(X) = \det(A^t \cdot A) = \det(A)^2$. Por otro lado, $A = [\sigma_i(\gamma)^{j-1}]_{ij}$ de modo que es de hecho una matriz de Vandermonde y su determinante es (prop. **??**)

$$\det(A) = \prod_{i<j}(\sigma_j(\gamma) - \sigma_i(\gamma)),$$

el cual es no nulo, pues γ es separable, luego sus conjugados son todos distintos.

(b) Para el caso general, sea Γ una base de trascendencia de separación. Sea L/k una extensión de cuerpos arbitraria. Nótese que

$$k(\Gamma) \otimes_k L \leq \operatorname{Frac}(k[\Gamma] \otimes_k L) = \operatorname{Frac}(L[\Gamma]) = L(\Gamma),$$

el cual es un cuerpo, luego $k(\Gamma) \otimes_k L$ es un dominio íntegro y, en particular, es reducido. Luego

$$K \otimes_k L = K \otimes_{k(\Gamma)} (k(\Gamma) \otimes_k L) \leq K \otimes_{k(\Gamma)} L(\Gamma),$$

pero $K/k(\Gamma)$ es una extensión algebraica separable, luego es una álgebra separable por el caso (a), y luego $K \otimes_{k(\Gamma)} L(\Gamma)$ es un anillo reducido. □

De modo que nuestra definición de separable extiende a la antigua definición.

Definición 6.21: Sea k un cuerpo de $\operatorname{car} k =: p > 0$. Se define para todo $n \in \mathbb{N}$:

$$k^{p^{-n}} := \{\alpha \in k^{\text{alg}} : \alpha^{p^n} \in k\}, \qquad k^{p^{-\infty}} := \bigcup_{n \in \mathbb{N}} k^{p^{-n}}.$$

A $k^{p^{-\infty}}$ le decimos la ***clasura perfecta*** de k.

Es fácil comprobar que $k^{p^{-\infty}}$ es la mínima extensión de cuerpos de k que es un cuerpo perfecto.

Teorema 6.22: Sea k un cuerpo de $\operatorname{car} k =: p > 0$ y sea K/k una extensión de cuerpos de tipo finito. Son equivalentes:

1. K es separable sobre k.
2. La álgebra $K \otimes_k k^{1/p}$ es reducida.
3. K está separablemente generado sobre k.

Demostración: $1 \implies 2$ es trivial y ya probamos $3 \implies 1$.

$2 \implies 3$. Sea $K = k(\alpha_1, \ldots, \alpha_n)$ el cual es algebraico sobre $k' := k(\alpha_1, \ldots, \alpha_r)$ puramente trascendente sobre k, donde $\{\alpha_{r+1}, \ldots, \alpha_q\}$ son separables sobre k' y $\beta := \alpha_{q+1}$ es inseparable sobre k'. Así pues, sea

$f(y^p) \in k'[y]$ el polinomio minimal de β. Los coeficientes de f están en k' por lo que son funciones racionales; limpiando denominadores obtenemos un polinomio irreducible $F(x_1, \dots, x_r, y) \in k[\boldsymbol{x}, y]$ tal que $F(\alpha_1, \dots, \alpha_r; \beta^p) = 0$.

Ahora bien, si $\partial F/\partial x_i = 0$ para todo $1 \leq i \leq r$, entonces tendríamos que $F(\boldsymbol{x}, y) = G(\boldsymbol{x}, y)^p$ con $G(\boldsymbol{x}, y) \in k^{1/p}[\boldsymbol{x}, y]$ y entonces:

$$k(\alpha_1, \dots, \alpha_r; \beta) \otimes_k k^{1/p} = \frac{k[\boldsymbol{x}, y]}{(F(\boldsymbol{x}, y))} \otimes_k k^{1/p} = \frac{k^{1/p}[\boldsymbol{x}, y]}{(G(\boldsymbol{x}, y)^{1/p})},$$

el cual es un subanillo de $K \otimes_k k^{1/p}$ que no es reducido. Luego, reordenando términos, suponemos que $\partial F/\partial x_1 \neq 0$ y, por ende, α_1 es separable algebraico sobre $k(\alpha_2, \dots, \alpha_r; \beta)$. Intercambiando α_1, β tenemos que $\alpha_{r+1}, \dots, \alpha_{q+1}$ es separable algebraico sobre k' y, por inducción, vemos que $\alpha_{r+1}, \dots, \alpha_n$ lo es. □

Teorema 6.23: Si k es un cuerpo perfecto entonces toda extensión de cuerpos K/k es separable y toda k-álgebra A es separable syss es reducida.

Demostración: El teorema **??** ahora dice que k es perfecto si $\operatorname{car} k = 0$ o si $\operatorname{car} k =: p > 0$ y $k = k^{1/p}$. Luego, para toda subextensión $K' \subseteq K$ de tipo finito sobre k tenemos que $K' \otimes_k k^{1/p} = K'$ el cual es reducido, luego K es una álgebra separable. Más en general, dada una k-álgebra A arbitraria podemos suponerla de tipo finito y ver que A es noetheriano reducido, luego su anillo de fracciones totales $K = K_1 \times \cdots \times K_r$ es un producto de cuerpos, por el corolario A.17.2, con cada K_i/k una extensión de cuerpos, que son separables; de modo que K es una álgebra separable y como $A \subseteq K$ también. □

Lema 6.24: Dada una extensión L/k con K, K' extensiones intermedias, son equivalentes:

1. Si $\alpha_1, \dots, \alpha_r \in K$ son k-linealmente independientes, entonces son K'-linealmente independientes.
2. Si $\beta_1, \dots, \beta_r \in K'$ son k-linealmente independientes, entonces son K-linealmente independientes.
3. El homomorfismo canónico $\varphi\colon K \otimes_k K' \to K[K']$ es un isomorfismo.

Demostración: $1 \implies 3$. Es claro que φ es un epimorfismo, así que basta ver que $\ker \varphi = 0$. Sea $\gamma = \sum_{i=1}^n \alpha_i \otimes \beta_i \in \ker \varphi$ y reordenemos términos de modo que $\alpha_1, \dots, \alpha_r$ sean k-linealmente independientes y $\alpha_{r+1}, \dots, \alpha_m$ estén

generados por los anteriores. Luego nótese que cambiando los β_i's tenemos que $\gamma = \sum_{i=1}^{r} \alpha_i \otimes \beta_i'$. Nótese que $\varphi(\gamma) = \sum_{i=1}^{r} \alpha_i \beta_i' = 0$, pero como los α_i's son K'-linealmente independientes, se cumple que cada $\beta_i' = 0$ y $\gamma = 0$.

$3 \implies 1$. Basta seguir un procedimiento similar. Nótese que por simetría tenemos $2 \iff 3$. □

Definición 6.25: Dada una extensión L/k con K, K' extensiones intermedias, se dice que K, K' son ***k-linealmente disjuntos*** si se cumplen las condiciones del lema anterior.

Como observación, podemos notar que el homomorfismo canónico es, siempre, un epimorfismo. Si $K \otimes_k K'$ es un cuerpo, entonces necesariamente el homomorfismo canónico es también un monomorfismo. Más aún, si $K \otimes_k K'$ es un dominio íntegro, entonces siempre es un cuerpo, así que la condición anterior puede reducirse a ésta.

Corolario 6.25.1: Sean $L/K/k$ extensiones de cuerpos y sea $S \subseteq L$ un conjunto de elementos K-algebraicamente independientes. Entonces K y $k(S)$ son linealmente disjuntos sobre K.

Una aplicación del cambio de base para tensores (proposición **??**) da:

Teorema 6.26: Sea Ω/k una extensión de cuerpos con $M/L/k$ y K/k extensiones intermedias. Luego M y K son k-linealmente disjuntos syss L y K son k-linealmente disjuntos, y $K \vee L$ y M son L-linealmente disjuntos (ver fig. 6.1).

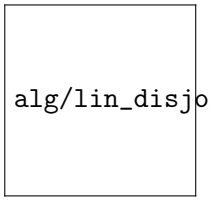


Figura 6.1

Teorema 6.27 (de Mac Lane): Sea K/k una extensión de cuerpos y sea $L := K^{\text{alg}}$.

1. Si K/k es separable, entonces K y $k^{p^{-\infty}}$ son linealmente disjuntos.
2. Si K y $k^{p^{-n}}$ son linealmente disjuntos para algún $n > 0$, entonces K/k es separable.

DEMOSTRACIÓN:

1. Sean $\alpha_1, \ldots, \alpha_n \in K$ tales que $\sum_{i=1}^n \alpha_i \beta_i = 0$ para algunos $\beta_i \in k^{p^{-\infty}}$. Sea $\tilde{k} := k(\beta_1, \ldots, \beta_n)$. Nótese que $\tilde{k}/k$ es una extensión finita y que $\tilde{k}^{p^n} \subseteq k$ para un n suficientemente grande. Como K es separable, entonces $A := K \otimes_k \tilde{k}$ es reducido. Nótese que A es un K-módulo finitamente generado, luego $k.\dim A = 0$, por lo que es artiniano.
2. Nótese que $K \otimes_k k^{p^{-1}}$ está contenido en $K \otimes_k k^{p^{-n}}$ el cual es un cuerpo, luego es reducido y K es separable. □

§6.2.1 Bases diferenciales.

Teorema 6.28: Sea L/K una extensión de cuerpos, donde $L = K(\alpha_1, \ldots, \alpha_n)$; sea $D \in \mathrm{Der}(K)$ y sean $\beta_1, \ldots, \beta_n \in L$. Sea $\mathfrak{a}$ el núcleo de la evaluación $K[\boldsymbol{x}] \to K(\alpha_1, \ldots, \alpha_n)$ y sean $(f_1, \ldots, f_s) = \mathfrak{a}$. Para todo $f \in K[\boldsymbol{x}]$ definamos:

$$F_f := Df + \sum_{i=1}^n \beta_i \cdot \frac{\partial f}{\partial x_i} \in K(\beta_1, \ldots, \beta_n)[\boldsymbol{x}].$$

Entonces, existe una extensión de D a $D' \in \mathrm{Der}(L)$ tal que $D'(\alpha_i) = \beta_i$ syss para todo f_i se cumple que $F_{f_i}(\alpha_1, \ldots, \alpha_n) = 0$.

DEMOSTRACIÓN: $\Longrightarrow$. Como los f_j's generan $\mathfrak{a}$ tenemos que $f_j(\alpha_1, \ldots, \alpha_n) = 0$, luego $D'(f_j(\alpha_1, \ldots, \alpha_n)) = 0$. Por otro lado, es fácil ver que, para todo polinomio $f \in K[\boldsymbol{x}]$ se tiene que $D'(f(\alpha_1, \ldots, \alpha_n)) = F_f(\alpha_1, \ldots, \alpha_n)$.

$\Longleftarrow$. Sea $f \in \mathfrak{a}$ de modo que $f = \sum_{j=1}^s h_j f_j$ para algunos $h_j \in K[\boldsymbol{x}]$. Entonces

$$\begin{aligned} F_f &= \sum_{j=1}^s (f_j\, Dh_j + h_j Df_j) + \sum_{j=1}^s \sum_{i=1}^n \beta_i \cdot \left(f_j \frac{\partial h_j}{\partial x_i} + h_j \frac{\partial f_j}{\partial x_i} \right), \\ &= \sum_{j=1}^s (f_j \cdot F_{h_j} + h_j \cdot F_{f_j}) \end{aligned}$$

evaluando en $F_f(\alpha_1, \ldots, \alpha_n) = 0$. Por definición, tenemos que si $g_1(\alpha_1, \ldots, \alpha_n) = g_2(\alpha_1, \ldots, \alpha_n)$ entonces $g_1 - g_2 \in \mathfrak{a}$ y luego $F_{g_1}(\alpha_1, \ldots, \alpha_n) = F_{g_2}(\alpha_1, \ldots, \alpha_n)$,

de modo que la expresión $D'(g(\alpha_1,\ldots,\alpha_n)) := F_g(\alpha_1,\ldots,\alpha_n)$ está bien definida. □

Corolario 6.28.1: Sea D una derivación sobre un cuerpo K y sea $L = K(\alpha)$ una extensión simple de cuerpos. Entonces:

(a) Si α es trascendente: para todo $\beta \in L$ existe una extensión D' de D tal que $D'(\alpha) = \beta$.

(b) Si α es separable: existe una única extensión de D a L.

(c) Si $\operatorname{car} K =: p > 0$ y $\alpha^p \in K$: D admite alguna extensión syss $D(\alpha^p) = 0$. En cuyo caso, para todo $\beta \in L$ existe una extensión D' de D tal que $D'(\alpha) = \beta$.

Demostración: Sea $\operatorname{ev}_\alpha\colon K[x] \to L$ y $\mathfrak{a} := \ker \operatorname{ev}_\alpha$. Si α es trascendente, entonces $\mathfrak{a} = (0)$ y claramente se cumplen las condiciones del teorema anterior. En todo caso $\mathfrak{a} = (f)$, pues $K[x]$ es un DIP. Si α es separable, entonces $\frac{\partial f}{\partial x} \neq 0$ lo cual induce la unicidad del β elegido, y si $\alpha^p \in K$, entonces $f(x) := x^p - \alpha^p$, su derivada es $\frac{\partial f}{\partial x} = 0$ y $Df = 0$. □

Definición 6.29: Sea K/k una extensión de cuerpos con $\operatorname{car} k =: p > 0$. Un conjunto $S \subseteq K$ se dice ***p*-independiente** si para todos $s_1,\ldots,s_m \in S$ distintos, se cumple que

$$[K^p(k)(s_1,\ldots,s_m) : K^p(k)] = p^m.$$

Un conjunto p-independiente maximal de K/k se dice una ***p*-base**.

Teorema 6.30: Sea K/k una extensión de cuerpos de tipo finito con $\operatorname{car} k =: p > 0$.

1. Todo conjunto p-independiente de K/k está contenido en una p-base.

2. Sea $S \subseteq K$. Llamemos el conjunto p-monomios de S como:

$$\Gamma_S := \{s_1^{n_1}\cdots s_m^{n_m} : s_i \in S, 0 \leq n_i < p\}.$$

   S es una p-base syss Γ_S es una base de $K/K^p(k)$ como espacio vectorial.

   En consecuencia, si S es una p-base, entonces $K^p(S) = K$.

3. Dada una p-base S, existe una biyección:

$$\phi\colon \mathrm{Der}_k(K) \longrightarrow \mathrm{Func}(S;K)$$

tal que para todo $s \in S$ y toda derivación $D \in \mathrm{Der}_k(K)$ se cumple que $Ds = \phi(D)(s)$.

4. En particular, $\dim_K(\mathrm{Der}_k(K)) = |S|$.

Demostración: La primera es una aplicación del lema de Zorn.

Para la segunda, sea $\beta \in K$. Nótese que $\beta^p \in K^p$, por lo que β es raíz de $x^p - \beta^p$ lo que prueba que $[K^p(\beta) : K^p] \in \{1, p\}$, luego aplique transitividad de grado. Ahora bien, puede darse que $\beta \in K^p$

Veamos la 3: Sea $L_0 := K^p(k)$ y $L_i := L_0(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$ para $1 \leq i \leq n$. Nótese que necesariamente $[K : L_i] = p$, de modo que, por el corolario 6.28.1, existe una derivación $D_i \in \mathrm{Der}_{L_i}(K)$ tal que $D_i(s_i) = 1$. Veremos que los $\{D_1, \ldots, D_n\}$ forman una K-base de $\mathrm{Der}_k(K)$. Claramente son linealmente independientes (basta ver que $D_j(s_i) = \delta_{ij}$) y son un sistema generador puesto que dado $D \in \mathrm{Der}_k(D)$ se define $u_i := D(s_i)$ y vemos que $D - \sum_{j=1}^n u_j D_j$ es una derivación que vale 0 en todo s_i y todo L_0 y $K = L_0(s_1, \ldots, s_n)$.

Para probar la 2, nótese que la descripción ya define un ϕ que es, además, claramente inyectivo por las observaciones anteriores, luego basta probar que es suprayectivo. Para ello, nótese que toda derivación sobre k, también es una derivación sobre $K^p(k)$ y $K/K^p(k)$ es una extensión puramente inseparable, luego aplicamos el corolario 6.28.1 para concluir. □

Definición 6.31: Dada una extensión de cuerpos K/k, entonces $\Omega_{K/k}$ es un K-espacio vectorial generado por los diferenciales $\{\mathrm{d}x : x \in K\}$, por lo que existe un subconjunto $B \subseteq K$ tal que $\{\mathrm{d}b : b \in B\}$ es una K-base de $\Omega_{K/k}$. Éste conjunto B se dice una ***base diferencial*** de K/k.

Nótese lo siguiente: una base diferencial es un conjunto de elementos k-linealmente independientes.

Teorema 6.32: Dada una extensión de cuerpos K/k, entonces:

1. Si $\mathrm{car}\, k = 0$, una base diferencial es lo mismo que una base de trascendencia.

2. Si $\mathrm{car}\, k =: p > 0$, una base diferencial es lo mismo que una p-base.

Demostración:

1. Sean $\alpha_1, \ldots, \alpha_n \in K$ tales que $\mathrm{d}\alpha_1, \ldots, \mathrm{d}\alpha_n \in \Omega_{K/k}$ son k-linealmente independientes, veamos que tienen que ser algebraicamente independientes. Si existe $0 \neq f(\boldsymbol{x}) \in k[\boldsymbol{x}]$ tal que $f(\alpha_1, \ldots, \alpha_n) = 0$ con f de grado minimal. Sin perdida de generalidad supongamos que x_1 aparece en f, de modo que $f_1 := \frac{\partial f}{\partial x_1} \neq 0$ es un polinomio tal que $f_1(\alpha_1, \ldots, \alpha_n) \neq 0$. Luego tenemos que

$$0 = \mathrm{d}f = \sum_{i=1}^{n} f_i(\alpha_1, \ldots, \alpha_n)\, \mathrm{d}\alpha_i,$$

   de modo que los $\mathrm{d}\alpha_i$'s son linealmente dependientes.

   De faltar elementos trascendentes, aplicamos el corolario 6.28.1 para notar que deben pertenecer a la base diferencial. Como la característica es nula, si B es una base de trascendencia de K/k, entonces la extensión $K/k(B)$ es algebraica separable, por lo que toda derivación se extiende de manera única por el mismo corolario.

2. Ésto es el tercer inciso del teorema 6.30. □

Teorema 6.33: Sea K/k una extensión de cuerpos. Son equivalentes:

1. K/k es separable.
2. Para todo subcuerpo $k' \subseteq k$ se cumple que $\Omega_{k/k'} \otimes_k K \to \Omega_{K/k'}$ es un monomorfismo.
3. Para todo subcuerpo $k' \subseteq k$ y toda base diferencial B de k/k', existe una base diferencial de K/k' que contiene a B.
4. $\Omega_k \otimes_k K \to \Omega_K$ es un monomorfismo.
5. Para todo K-módulo M, toda derivación $\phi\colon k \to M$ se extiende a una derivación $\phi^*\colon K \to M$.

Demostración: Son claras: 2 $\iff$ 3 y 2 $\implies$ 4 $\iff$ 5. Si $\operatorname{car} k = 0$ entonces 1 y 3 siempre se cumplen, así que supondremos que $\operatorname{car} k =: p > 0$.

1 $\implies$ 3. Por el teorema de Mac Lane, K y $k^{1/p}$ son linealmente disjuntos sobre k. Aplicando el endomorfismo $\alpha \mapsto \alpha^p$, vemos que K^p y k son linealmente disjuntos sobre k^p, luego por el teorema 6.26 vemos que $K^p(k')$ y k son linealmente disjuntos sobre $k^p(k')$. Sea B una p-base de k/k', entonces

los p-monomios Γ_B son $k^p(k')$-linealmente independientes (teorema 6.30), luego son $K^p(k')$-linealmente independientes, por ende, B es un conjunto p-independiente de K/k' y se extiende a una p-base.

4 $\implies$ 1. Sea B una p-base de k sobre su cuerpo primo Π, entonces los p-monomios Γ_B son una k^p-base de k. Como B es una base diferencial, $\{\mathrm{d}x : x \in B\}$ es una k-base de Ω_k, luego por el enunciado se cumple que es K-linealmente independiente, de modo que los p-monomios Γ_B son K^p-linealmente independientes, por lo que, $k \otimes_{k^p} K^p \cong k(K^p)$, luego k, K^p son linealmente disjuntos sobre k^p y, por el teorema de Mac Lane, K^p/k^p es una extensión separable y K/k también. □

Definición 6.34: Sea k un cuerpo de $\operatorname{car} k =: p > 0$. Una ***p*-base absoluta** es una p-base de $k/\mathbb{F}_p$.

Teorema 6.35: Sea k un cuerpo de $\operatorname{car} k =: p > 0$ y sea K/k una extensión. Entonces K es 0-étale sobre k syss toda p-base absoluta de k es una p-base absoluta de K.

Demostración: $\Longleftarrow$. Sea C una k-álgebra con $\mathfrak{n} \lhd C$ tal que $\mathfrak{n}^2 = 0$, y sea $u\colon K \to C/\mathfrak{n}$ un k-homomorfismo continuo. Dado $\alpha \in K$, sea $\beta \in C$ tal que $\beta \bmod \mathfrak{n} = u(\alpha)$.

$$\begin{array}{ccc} K & \xrightarrow{u} & C/\mathfrak{n} \\ {\scriptstyle i}\uparrow & & \uparrow\!\!\uparrow \\ k & \xhookrightarrow[j]{} & C \end{array}$$

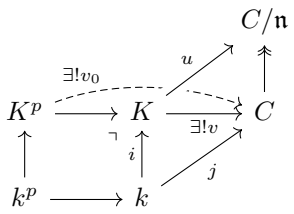
Si $\beta' \equiv \beta \pmod{\mathfrak{n}}$, entonces como C es k-álgebra, debe darse que $\operatorname{car} C = p$ y, por el sueño del aprendiz,

$$(c \in \mathfrak{n}) \quad \beta' = \beta + c \implies (\beta')^p = \beta^p + c^p = \beta^p.$$

De ello, se sigue que el valor de β^p es independiente de la elección de β. Así, definimos $v_0\colon K^p \to C$ dado por $v_0(\alpha^p) := \beta^p$ y notamos que $v_0 \restriction k^p = j \restriction k^p$. Luego, como K/k es separable, tenemos que

$$K = K^p[k] = K^p \otimes_{k^p} k,$$

de modo que construimos el siguiente diagrama:



La unicidad de v es relativa a v_0, y v_0 es claramente única por construcción.

$\Longrightarrow$. Si K/k es 0-étale, entonces K/k es 0-no ramificada por lo que $\Omega_{K/k} = 0$ y, por 0-suavidad, se cumple que $\Omega_K = \Omega_k \otimes_k K$ de lo que se sigue que se preservan p-bases absolutas. □

Teorema 6.36: Sea K/k una extensión separable de cuerpos de $\operatorname{car} k =: p > 0$, y sea B una p-base de K/k. Entonces B es k-algebraicamente independiente y K es 0-étale sobre $k(B)$.

Demostración: Procedemos por contradicción. Si la tupla $\boldsymbol{b} := (\beta_1, \ldots, \beta_n)$ de elementos de B es k-algebraicamente dependiente, entonces sea $0 \neq f(x_1, \ldots, x_n) \in k[\boldsymbol{x}]$ de grado minimal d tal que $f(\boldsymbol{b}) = 0$. Escribamos

$$f(\boldsymbol{x}) := \sum_{\alpha} g_\alpha(x_1^p, \ldots, x_n^p)\boldsymbol{x}^\alpha,$$

donde $\alpha = (\alpha_1, \ldots, \alpha_p)$ recorre los multiíndices con cada $0 \leq \alpha_i < p$. Como $\boldsymbol{b}$ es p-independiente, entonces cada $g_\alpha(\boldsymbol{b}^p) = 0$ y como

$$d \geq \deg(g_\alpha(\boldsymbol{x}^p)) + \alpha_1 + \cdots + \alpha_n,$$

entonces por minimalidad de f, se debe tener que $f(\boldsymbol{x}) = g_{0,\ldots,0}(\boldsymbol{x}^p)$. Luego, podemos escribir $f(\boldsymbol{x}) = h(\boldsymbol{x})^p$, donde $h(\boldsymbol{x}) \in k^{1/p}[\boldsymbol{x}]$. Como K y $k^{1/p}$ son k-linealmente disjuntos por el criterio de Mac Lane, entonces los monomios de grado $< d$ sobre $\boldsymbol{b}$ son $k^{1/p}$-linealmente independientes puesto que son k-linealmente independientes. Así que $h(\boldsymbol{x}) = 0$ y, por tanto, $f(\boldsymbol{x}) = 0$, lo que es absurdo. □

Teorema 6.37: Sea K/k una extensión de cuerpos. Entonces la extensión es separable syss K es 0-suave sobre k.

Demostración: $\Longrightarrow$. Sea B una base diferencial de K/k. La extensión $k(B)/k$ es puramente trascendente y es claro, por definición, que $k(B)$ es 0-étale sobre k. Más aún, $K/k(B)$ es 0-étale: para verlo hay que separar en

dos casos, si $\operatorname{car} k = 0$ se sigue de que la extensión es algebraica separable y si $\operatorname{car} k > 0$ se hace empleando el criterio de las p-bases absolutas agrandando B. Por transitividad, K/k es 0-suave.

$\Longleftarrow$. Si K/k es 0-suave, entonces $\Omega_k \otimes_{\mathbb{F}_p} K \to \Omega_K$ es un monomorfismo por la primera sucesión exacta fundamental (6.3) y concluimos por el teorema 6.33. □

Lema 6.38: Sea L/K una extensión de cuerpos. Son equivalentes:

1. L y K^{alg} (vistos dentro de L^{alg}) son K-linealmente disjuntos. Equivalentemente, $L \otimes_K K^{\mathrm{alg}}$ es un dominio íntegro.
2. $L \cap K^{\mathrm{alg}} = K$ y L es separable sobre K.
3. $L \otimes_K L'$ es un dominio íntegro para toda extensión L'/K.

Demostración: $1 \implies 2$. Es claro que si L/K es regular, entonces L/K es separable. Supongamos que $L \cap K^{\mathrm{alg}} \neq K$, entonces nótese que $(L \cap K^{\mathrm{alg}}) \otimes_K K^{\mathrm{alg}}$ no es un cuerpo, puesto que para todo $\alpha \in (L \cap K^{\mathrm{alg}}) \setminus K$ se cumple que $\alpha \otimes 1 - 1 \otimes \alpha$ es un elemento no nulo que tiene imagen nula bajo el K-homomorfismo canónico.

$2 \implies 3$. Lo probaremos por contradicción: Si $L \otimes_K L'$ no es un dominio íntegro, entonces sean $\sum_{i=1}^n a_i \otimes b_i, \sum_{j=1}^m c_j \otimes d_j$ elementos no nulos cuyo producto es 0. Sea $L'' := K(b_1, \ldots, b_n, d_1, \ldots, d_m)$, de modo que podemos suponer que la extensión es de tipo finito. Elijamos L_0/K una extensión de tipo finito con grado de trascendencia minimal y elijamos $L/L_1/K$ una extensión intermedia de tipo finito tal que $L_1 \otimes_K L_0$ no es un dominio íntegro. Nótese que $L_1 \cap K^{\mathrm{alg}} = K$ y L_1 también es separable sobre K.

Completar demostración [**0,** pág. 95].

$3 \implies 1$. Trivial. □

Definición 6.39: Sea L/K una extensión de cuerpos. Se dice que L/K es una ***extensión regular*** si $L \otimes_K K^{\mathrm{alg}}$ es un dominio íntegro (y, en consecuente, un cuerpo). Un dominio íntegro R/K se dice una regular sobre K si $\operatorname{Frac}(R)/K$ es una extensión regular de cuerpos.

Teorema 6.40: Sea Ω/k una extensión de cuerpos. Entonces:

1. Si $L/K/k$ son extensiones intermedias y L/k es regular, entonces K/k también.
2. Si $L/K/k$ son extensiones intermedias, si L/K y K/k son regulares, entonces L/k también.

3. Si L, K son extensiones intermedias k-linealmente disjuntas y K/k es regular, entonces $K \vee L/L$ es regular.

4. Si L, K son extensiones intermedias k-linealmente disjuntas, y K/k y L/k son regulares, entonces $K \vee L/k$ es regular.

Demostración:

1. Claramente $K \otimes_k k^{\mathrm{alg}} \leq L \otimes_k k^{\mathrm{alg}}$.

2. Por cambio de base, $L \otimes_k k^{\mathrm{alg}} = L \otimes_K (K \otimes_k k^{\mathrm{alg}}) \cong L \otimes_K (K \vee k^{\mathrm{alg}})$. Como $K \vee k^{\mathrm{alg}}/K$ es una extensión de cuerpos, entonces $L \otimes_k k^{\mathrm{alg}}$ es un dominio íntegro.

3. Como K, L son linealmente disjuntos, entonces $K \vee L \cong K \otimes_k L$. Sea L'/L una extensión de cuerpos arbitraria, por cambio de base $K \vee L \otimes_L L' \cong K \otimes_k L'$, donde L'/k es una extensión de cuerpos, por lo que es un dominio íntegro.

4. Aplíquese incisos 2 y 3. □

6.3 Suavidad formal y teoremas de Cohen

Definición 6.41: Sea B una A-álgebra con la topología $\mathfrak{b}$-ádica. Se dice que B es $\mathfrak{b}$-***suave*** si para toda A-álgebra C, todo ideal $\mathfrak{n} \lhd C$ tal que $\mathfrak{n}^2 = (0)$, y todo A-homomorfismo continuo $u\colon B \to C/\mathfrak{n}$ donde $C/\mathfrak{n}$ tiene la topología discreta (i.e., un homomorfismo tal que $u[\mathfrak{b}^n] = \{0\}$ para algún $n \in \mathbb{N}$) existe un A-homomorfismo $v\colon B \to C$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} B & \xrightarrow{u} & C/\mathfrak{n} \\ \uparrow & \overset{v}{\searrow} & \uparrow\uparrow \\ A & \dashrightarrow & C \end{array} \tag{6.7}$$

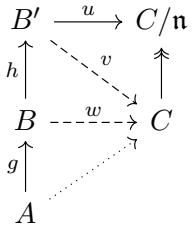
B se dice $\mathfrak{b}$-***no ramificado*** si existe a lo más un v tal que el diagrama (6.7) conmuta, y B se dice $\mathfrak{b}$-***étale*** si es $\mathfrak{b}$-suave y $\mathfrak{b}$-no ramificado.

Ésta condición es más restrictiva mientras más pequeño sea el ideal $\mathfrak{b}$.

Teorema 6.42: Sean $A \xrightarrow{g} B \xrightarrow{h} B'$ homomorfismos de anillos, donde B es un anillo con la topología $\mathfrak{b}$-ádica, B' es un anillo con la topología $\mathfrak{b}'$-ádica y h es continuo. Si B es $\mathfrak{b}$-suave (resp. $\mathfrak{b}$-no ramificado) sobre A y B'

es $\mathfrak{b}'$-suave (resp. $\mathfrak{b}'$-no ramificado) sobre B, entonces B' es $\mathfrak{b}'$-suave (resp. $\mathfrak{b}'$-no ramificado) sobre A.

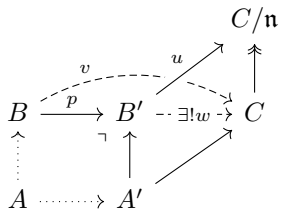
Demostración: Sea C una A-álgebra, un ideal $\mathfrak{n} \lhd C$ tal que $\mathfrak{n}^2 = 0$ y sea $u\colon B \to C/\mathfrak{n}$ un A-homomorfismo continuo. Entonces construimos el siguiente diagrama conmutativo:



Como B es $\mathfrak{b}$-suave sobre A y $hu\colon B \to C/\mathfrak{n}$ es un A-homomorfismo continuo, entonces admite una elevación $w\colon B \to C$, de modo que C es una B-álgebra canónica. Como B' es $\mathfrak{b}'$-suave sobre B y $u\colon B' \to C/\mathfrak{n}$ es un B-homomorfismo continuo, entonces admite una elevación $v\colon B' \to C$. Queda al lector ver el caso de ser no ramificado. □

Teorema 6.43: Sea A un anillo, B, A' un par de A-álgebras y sea $B' := A' \otimes_A B$. Si B es $\mathfrak{b}$-suave (resp. $\mathfrak{b}$-no ramificado) sobre A, entonces B' es $\mathfrak{b}B'$-suave (resp. $\mathfrak{b}B'$-no ramificado) sobre A'.

Demostración: Sea C una A'-álgebra con un ideal $\mathfrak{n} \lhd C$ tal que $\mathfrak{n}^2 = (0)$, y sea $u\colon B' \to C/\mathfrak{n}$ un homomorfismo continuo de A'-álgebras, vale decir, tal que $u[\mathfrak{b}^n B'] = (0)$. Sea $p\colon B \to B'$ el homomorfismo canónico ($b \mapsto 1 \otimes b$), es claro que $p \circ u\colon B \to C/\mathfrak{n}$ es un homomorfismo continuo de A-álgebras, luego admite una elevación que induce un homomorfismo $B' \to C$, puesto que B' es un coproducto:



La unicidad de w es relativa a fijar una elección de v; de aquí se sigue el cambio de base de la ramificación formal. □

Ahora nos encaminamos al teorema de estructura de Cohen.

Lema 6.44: Sea $(A, \mathfrak{m}, K)$ un dominio local. Son equivalentes:

1. $\operatorname{car} A = \operatorname{car} K$.

2. A contiene un subcuerpo (en particular, un subcuerpo primo).

Definición 6.45: Un dominio local A que satisface lo anterior se dice ***equicaracterístico***.

Nótese que para un anillo local $(A, \mathfrak{m}, K)$ hay cuatro posibilidades:

(a) $\operatorname{car} A = 0, \operatorname{car} K = 0$.

(b) $\operatorname{car} A = p, \operatorname{car} K = p > 0$.

(c) $\operatorname{car} A = 0, \operatorname{car} K = p > 0$.

(d) $\operatorname{car} A = p^n, \operatorname{car} K = p > 0$.

Los casos (a) y (b) ocurren si el anillo es equicaracterístico. Si A es íntegro no puede suceder (d).

El primer problema a resolver es el siguiente:

Definición 6.46: Sea $(A, \mathfrak{m}, K)$ un dominio local y fijemos $\pi\colon A \to K$. Un subcuerpo $K' \subseteq A$ se dice un ***cuerpo de coeficientes*** de A si $\pi|_{K'}\colon K' \to K$ es un isomorfismo. Se dice que K' es un ***cuerpo de cuasicoeficientes*** si K es 0-étale sobre K' (bajo π).

Teorema 6.47: Sea $(A, \mathfrak{m}, K)$ un dominio local equicaracterístico. Se cumplen:

1. A posee un cuerpo de cuasicoeficientes.

2. Si A es completo, entonces contiene un cuerpo de coeficientes.

3. Si K es una extensión separable de un subcuerpo $k \subseteq A$, entonces A posee un cuerpo de cuasicoeficientes K' tal que $K' \supseteq k$.

4. Si K' es un cuerpo de cuasicoeficientes de A, entonces existe un único cuerpo de coeficientes L de la compleción $\hat{A}$ tal que $L \supseteq K'$.

Demostración: Es relativamente claro que basta probar las dos últimas, puesto que todos los cuerpos primos son perfectos.

3. Sea $B := \{\xi_1, \xi_2, \xi_3, \dots\}$ una base diferencial de K/k y para cada ξ_i elíjase $x_i \in A$ tales que $x_i \operatorname{mód} \mathfrak{m} = \xi_i$. Por el teorema 6.36 se cumple que B es k-algebraicamente independiente, luego el subanillo $k[x_1, x_2, \dots] \subseteq A$ corta a $\mathfrak{m}$ en (0), por lo que A contiene el subcuerpo $K' := k(x_1, x_2, \dots)$. Identificando K' con su imagen $k(B) \subseteq K$ vemos que es 0-étale sobre K' y así K' es de cuasicoeficientes.

4. Basta construir el siguiente diagrama:

$$\begin{array}{ccc} K & = & \hat{A}/\hat{\mathfrak{m}} \\ \uparrow & \overset{\exists! v}{\nearrow} & \uparrow\uparrow \\ K' & \longrightarrow & \hat{A} \end{array}$$

y notar que $v[K]$ es el cuerpo de coeficientes buscado. □

Si además exigimos a A que sea noetheriano, entonces tendrá dimensión finita y el ideal maximal será finitamente generado por un conjunto $x_1, \dots, x_n$; de modo que $A \cong K[[x_1, \dots, x_n]]/\mathfrak{a}$. Ésta es una primera versión del teorema de Cohen, pero nótese que puede fallar si A no fuese equicaracterístico: el ejemplo más trivial es el anillo de los enteros p-ádicos $\mathbb{Z}_p$ que no contiene ningún cuerpo de coeficientes; en esencia esto es el prototipo de la única alternativa al caso equicaracterístico.

Definición 6.48: Se dice que un dominio de valuación discreta A de $\operatorname{car} A = 0$ es un ***p*-anillo** si el primo $p \in \mathbb{Z} \subseteq A$ es un uniformizador.

Teorema 6.49: Sea $(A, \pi A, k)$ un dominio de valuación discreta. Para toda extensión de cuerpos K/k existe un dominio de valuación discreta $(B, \pi B, K)$ que contiene a A.

Demostración: Sea $B := \{x_i\}_{i \in I}$ una base de trascendencia de K y sea $k_1 := k(B)$. Sean $\{X_i\}_{i \in I}$ un conjunto de indeterminadas en biyección con B, y sean $A' := A[\{X_i\}_i]$ y $A_1 := (A')_{\pi A'}$. Ahora bien, A' es un A-módulo libre y, por tanto, es Hausdorff en la topología π-ádica, luego A_1 también. Nótese que $(A_1, \pi A_1, k_1)$ es un dominio de valuación discreta que contiene a A. Así, reemplazando A por A_1, podemos suponer que K/k es una extensión algebraica.

Sea $L := (\operatorname{Frac} A)^{\mathrm{alg}}$ y sea $\mathcal{F}$ el conjunto de pares (B, φ) tales que B es un dominio de valuación discreta, $\varphi\colon B \to K$ es un A-homomorfismo con

$\ker B = \mathfrak{J}(B) = \pi B$. Denotaremos $(B,\varphi) \preceq (C,\psi)$ si $B \subseteq C$ y $\psi|_B = \varphi$. Es fácil notar que toda $\preceq$-cadena en $\mathcal{F}$ posee cota superior (la unión de cadenas de subanillos es un subanillo, y los A-homomorfismos se van pegando), por lo que, por el lema de Zorn, elegimos un $\preceq$-maximal (B,φ).

Sea $K' := \varphi[B] \subseteq K$ y veamos que $K = K'$. De lo contrario, sea $\beta \in K \setminus K'$, luego sea $g(x) \in K'[x]$ su polinomio minimal y sea $f(x) \in B[x]$ mónico tal que $f(x) \bmod \pi = g(x)$; es fácil notar que $f(x)$ es irreducible en $B[x]$, luego también lo es en $(\operatorname{Frac} B)[x]$. Sea $\alpha \in L$ una raíz de $f(x)$ y sea $B' := B[\alpha]$ (vale decir, $B' = B[x]/(f(x))$), luego

$$B'/\pi B' = B[x]/(\pi, f(x)) = K'[x]/(g(x)) = K'[\beta],$$

el cual es un cuerpo. Como B' es una extensión entera de B, entonces todo ideal maximal de B' contiene a $\pi B'$ el cual es maximal, así que B' es local y es noetheriano por ser un B-módulo finitamente generado, luego B' es un dominio de valuación discreta. Esto contradice la $\preceq$-maximalidad de B, por lo que necesariamente $K' = K$. □

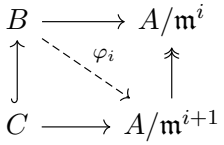
Aplicando el teorema anterior con $A = \mathbb{Z}_{(p)}$, vemos que para todo cuerpo K de $\operatorname{car} K =: p > 0$ siempre existe algún dominio de valuación discreta B con $B/pB = K$.

Teorema 6.50: Sea $(A, \mathfrak{m}, K)$ un anillo local completo. Dado un p-anillo (B, pB, k) y un monomorfismo $\varphi_0 \colon k \to K$, siempre existe un homomorfismo de anillos locales $\varphi \colon B \to A$ tal que

$$\begin{array}{ccc} k & \xhookrightarrow{\varphi_0} & K \\ \uparrow & & \uparrow \\ B & \xrightarrow{\varphi} & A \end{array}$$

Demostración: Definamos $C := \mathbb{Z}_{(p)}$. Como B es un p-anillo, entonces el homomorfismo canónico $\mathbb{Z} \to B$ induce que $C \subseteq B$. Además, también tenemos que el homomorfismo canónico $\mathbb{Z} \to A$ se extiende a un homomorfismo local $C \to A$. Nótese que $\mathbb{F}_p \otimes_C B = B/pB = k$ es una extensión separable de $\mathbb{F}_p$, luego es 0-suave sobre $\mathbb{F}_p$ (teorema 6.37) y además B es un C-módulo libre de torsión, luego es plano, por lo que tenemos que B es pB-suave sobre C. Así, comenzando con el homomorfismo $B \to K = A/\mathfrak{m}$, vamos recursivamente elevando el homomorfismo:

Demostrar o citar el teorema de Grothendieck, [**5,** pág. 222].



luego, los φ_i's inducen un homomorfismo $B \to \varprojlim_i A/\mathfrak{m}^i = \hat{A} \cong A$ como se buscaba. □

Corolario 6.50.1: Fijado un cuerpo K de $\operatorname{car} K =: p > 0$, existe un único p-anillo completo (salvo isomorfismo) B tal que $B/pB \cong K$.

Demostración: La existencia viene dada por el teorema 6.49 empleando $A = \mathbb{Z}_{(p)}$ y completando de ser necesario. Sean B, B' dos p-anillos dados con la propiedad deseada, luego el teorema anterior nos da un homomorfismo local $\varphi\colon B \to B'$ que induce la identidad en los cuerpos de restos; así que $B' = \varphi[B] + pB'$, pero claramente $\varphi(p) = p$, así que, por completitud de B se sigue que φ es suprayectivo mientras que la inyectividad se sigue de que $p^n B \nsubseteq \ker \varphi$. □

Definición 6.51: Sea $(A, \mathfrak{m}, k)$ un anillo local completo no equicaracterístico y sea $p := \operatorname{car} k > 0$. Un subanillo $\Lambda \subseteq A$ se dice un ***anillo de coeficientes*** si $(\Lambda, p\Lambda)$ es noetheriano local completo y

$$\Lambda/p\Lambda \cong k \iff A = \Lambda + \mathfrak{m}.$$

Nótese que, en la definición, Λ siendo noetheriano y teniendo maximal principal $\mathfrak{m} = p\Lambda$ tiene dos posibilidades: o bien Λ es un de valuación discreta (dimensión 1) o bien es artiano (dimensión 0) y con nilpotentes.

Teorema 6.52: Sea $(A, \mathfrak{m}, k)$ un anillo local completo con $p := \operatorname{car} k > 0$. Entonces A tiene un subanillo de coeficientes Λ y, más aún, si $\operatorname{car} A = 0$, entonces Λ es un dominio de valuación discreta.

Demostración: Por el corolario anterior existe un único p-anillo completo B tal que $B/pB \cong k$. Empleando dicho isomorfismo y el teorema anterior construimos un homomorfismo local $\varphi\colon B \to A$ y definimos $\Lambda := \varphi[B]$. Es fácil ver que Λ satisface lo exigido, y si $\operatorname{car} A = 0$ entonces necesariamente φ debe ser inyectivo (¿por qué?). □

Teorema 6.53: Sea $(A, \mathfrak{m}, k)$ un anillo local completo.

1. Si $\mathfrak{m}$ es finitamente generado, entonces A es noetheriano.
2. Si A es noetheriano, entonces es el cociente de algún anillo regular local. En particular, A es universalmente catenario.
3. Si A es noetheriano, y es equicaracterístico o bien un dominio íntegro, entonces existe un subanillo $A' \subseteq A$ que satisface lo siguiente:
   a) $(A', \mathfrak{n})$ es un anillo regular local completo.
   b) $A'/\mathfrak{n} \cong k$.
   c) A es un A'-módulo finitamente generado.

Demostración: Por el teorema anterior sea $\Lambda \subseteq A$ un anillo de coeficientes.

1. Sea $\mathfrak{m} = (a_1, \ldots, a_n)A$, sea $\boldsymbol{a} := (a_1, \ldots, a_n) \in A^n$ la tupla y $\boldsymbol{x} := (x_1, \ldots, x_n)$ una tupla de indeterminadas. Luego, todo $b \in A$ es de la forma $b = f(\boldsymbol{a})$ para alguna serie de potencias $f(\boldsymbol{x}) \in \Lambda[[\boldsymbol{x}]]$. Así que $A \cong \Lambda[[\boldsymbol{x}]]/\mathfrak{a}$, el cual es noetheriano.
2. Sabemos que Λ es el cociente de un p-anillo B, luego $A \cong B[[\boldsymbol{x}]]/\mathfrak{b}$ para algún ideal $\mathfrak{b}$, y B es local regular, luego $B[[\boldsymbol{x}]]$ también y A también. Que A sea universalmente catenario se sigue de que:
   $$\text{regular local} \implies \text{Cohen-Macaulay} \implies \text{universalmente catenario.}$$
3. Sea $n := k.\dim A$. Si A es equicaracterístico, elegimos $\beta_1, \ldots, \beta_n$ un sistema de paramétros arbitrario. Si A es dominio íntegro de $\operatorname{car} A = 0$ y $p := \operatorname{car} k > 0$, entonces elegimos un sistema de parámetros $\beta_1, \ldots, \beta_n$ con $\beta_1 = p$ (esto se puede, pues A es catenario). En ambos casos, $B = \Lambda$ (donde B es el p-anillo del inciso anterior) y definimos $A' := B[[y]]$. Nótese que A' es la imagen del B-homomorfismo:
   $$\operatorname{ev}_{\beta_1,\ldots,\beta_n} \colon B[[Y_1, \ldots, Y_n]] \longrightarrow A,$$
   (donde si $\beta_1 = p$, se elimina Y_1). Sea $\mathfrak{n} := \sum_{i=1}^{n} \beta_i A' \lhd A'$ y es claro que $A'/\mathfrak{n} \cong k$. Como $A/\mathfrak{m} \cong A'/\mathfrak{n}$, entonces todo A-módulo tiene la misma longitud respecto a A' que a A; en particular, $\operatorname{gr}(A) = A/\mathfrak{n}A$ es un $A'/\mathfrak{n}A'$-módulo finitamente generado (¿por qué?) y A es Hausdorff en la topología $\mathfrak{n}$-ádica, luego por la proposición 1.31 se cumple que A es un A'-módulo finitamente generado.

   Así que la extensión A/A' es entera y $n = k.\dim A = k.\dim A'$. Como $k.\dim(B[[\boldsymbol{Y}]]) = n$ y B es un dominio íntegro, entonces debe darse que $\ker(\text{ev}) = 0$, de lo contrario, $k.\dim(A') < n$ lo que sería absurdo. □

Notas históricas

Éste es uno de los capítulos más contemporáneos del libro. Las nociones de *suavidad, ramificación* y *étale* son originales de Grothendieck y Dieudonné **[EGA IV$_1$],** las elecciones de la terminología tienen su origen en su interpretación geométrica y se enfatizan en mis apuntes de geometría algebraica.

Los *teoremas de estructura de Cohen* son uno de los resultados centrales del álgebra conmutativa y fueron demostrados por I. S. Cohen en su tesis doctoral **[15]** (1946). La vida de Irvin Sol Cohen es relativamente trágica. Siendo un joven brillante y realizando importantes contribuciones al álgebra conmutativa, siempre fue sumamente crítico de sí y sesgado por su ambición se suicidó el febrero de 1955. Zariski comentó de su muerte (vid., **[43,** pág. 64]):

> Hay demasiadas cosas que son necesarias para ser un buen científico y una persona creativa, dejado a su propio criterio, Cohen se encontraba demasiado improductivo. Altamente crítico de sí y de los otros, creía que nada que había escrito podía superar su tesis. Se comenzó a involucrar en demasía en el álgebra abstracta, hasta que subió a un punto sin suelo a sus pies. Se tornó decepcionado de su propio trabajo y, finalmente y fatalmente, de sus competencias.[1]

En su honor, a veces a los p-anillos completos se les denomina *anillos de Cohen*; no obstante, nosotros desistimos de dicha terminología para no confundir con los anillos de Cohen-Macaulay.

[1] *Many things are necessary to make a good scientist, a creative man, and left on his own Cohen found himself unproductive. Highly critical of himself and others, he believed that nothing he ever wrote was as good as his thesis. He became increasingly involved with abstract algebra until he found himself at a certain point without ground under his feet. He became disappointed in his work and, finally, fatally, in his own ability.*

A

Preliminares

A.1 Preliminares algebraicos

Proposición A.1: Si A es noetheriano y S es un sistema multiplicativo de A, entonces $S^{-1}A$ también es noetheriano.

Proposición A.2: Sea M un A-módulo. Entonces las siguientes son equivalentes:

1. $M = 0$.
2. $M_{\mathfrak{p}} = 0$ para todo $\mathfrak{p} \trianglelefteq A$ primo.
3. $M_{\mathfrak{m}} = 0$ para todo $\mathfrak{m} \trianglelefteq A$ maximal.

Corolario A.2.1: $S^{-1}A$ es un A-módulo plano.

Teorema A.3: Sea $\mathfrak{a} \trianglelefteq A$, entonces:

1. $\mathrm{Rad}(\mathfrak{a}) = \bigcap\{\mathfrak{p} : \mathfrak{a} \subseteq \mathfrak{p} \trianglelefteq A,\ \mathfrak{p} \text{ primo}\}$.
2. $\mathfrak{a}$ es un ideal radical syss $A/\mathfrak{a}$ es un anillo reducido.

Proposición A.4: Para todo par de ideales $\mathfrak{a}, \mathfrak{b}$ en A se cumple:

1. Para todo $\mathfrak{a} \trianglelefteq A$ se cumple que $\mathfrak{a} \subseteq \mathrm{Rad}(\mathfrak{a}) \trianglelefteq A$.

2. $\mathrm{Rad}(\mathrm{Rad}(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a})$, es decir, todo radical de un ideal es un ideal radical.
3. $\mathrm{Rad}(\mathfrak{a} \cdot \mathfrak{b}) = \mathrm{Rad}(\mathfrak{a} \cap \mathfrak{b}) = \mathrm{Rad}(\mathfrak{a}) \cap \mathrm{Rad}(\mathfrak{b})$.
4. $\mathrm{Rad}(\mathfrak{a}) = (1)$ syss $\mathfrak{a} = (1)$.
5. $\mathrm{Rad}(\mathfrak{a} + \mathfrak{b}) = \mathrm{Rad}(\mathrm{Rad}(\mathfrak{a}) + \mathrm{Rad}(\mathfrak{b}))$.
6. Si $\mathfrak{p}$ es primo, entonces $\mathrm{Rad}(\mathfrak{p}^n) = \mathfrak{p}$ para todo $n > 0$.
7. $\mathfrak{a} + \mathfrak{b} = (1)$ syss $\mathrm{Rad}(\mathfrak{a}) + \mathrm{Rad}(\mathfrak{b}) = (1)$.

Definición A.5: Sean S, T submódulos de un A-módulo M, entonces denotamos:

$$(S : T) := \{a \in A : aT \subseteq S\}.$$

Más aún, se define el ***aniquilador*** o *anulador* de T como

$$\mathrm{Ann}(T) := (0 : T).$$

Proposición A.6: Sea $\varphi\colon A \to B$ un morfismo de anillos, y sea $\mathfrak{p} \trianglelefteq A$ primo. Entonces $\mathfrak{p}$ es la contracción de un ideal primo syss es la contracción de un ideal.

Teorema A.7 – *Teorema de Cayley-Hamilton*: Sea M un A-módulo finitamente generado, $\varphi\colon M \to M$ un endomorfismo y $\mathfrak{a}$ un ideal de A tales que $\varphi[M] \subseteq \mathfrak{a}M$. Entonces, se cumple que

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

(como morfismos) para algunos $a_i \in \mathfrak{a}$.

Teorema A.8: Sea $(A, \mathfrak{m})$ un dominio local. Entonces todo A-módulo proyectivo es libre.

Proposición A.9: Sea A un dominio noetheriano y M un A-módulo no nulo.

1. Todo $\mathrm{Ann}(\boldsymbol{x})$ con $\boldsymbol{x} \in M_{\neq 0}$ está contenido en algún ideal asociado a M.
2. Los divisores de cero de M son $\bigcup \mathrm{As}(M)$.

Corolario A.9.1 (descomposición de Lasker-Noether): Sea A un dominio noetheriano, M un A-módulo finitamente generado, entonces existe una cadena de submódulos $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ tal que $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ donde cada $\mathfrak{p}_i \lhd A$ es un ideal primo.

Teorema A.10: Sea A un dominio noetheriano y M un A-módulo finitamente generado. Entonces:

1. $\mathrm{As}(M)$ es un conjunto finito.
2. $\mathrm{As}(M) \subseteq \mathrm{Supp}(M)$.
3. Los elementos $\subseteq$-minimales de $\mathrm{As}(M)$ y $\mathrm{Supp}(M)$ coinciden.

Corolario A.10.1: Todo dominio noetheriano tiene finitos primos minimales.

Teorema A.11: Sea A un dominio noetheriano y M un A-módulo finitamente generado. Un submódulo $N \leq M$ es primario syss $\mathrm{As}(M/N)$ sólo posee un elemento $\mathfrak{p}$; en cuyo caso, el ideal $\mathfrak{a} := \mathrm{Ann}(M/N)$ es primario y $\operatorname{Rad}\mathfrak{a} = \mathfrak{p}$.

Proposición A.12: Si $\operatorname{Rad}\mathrm{Ann}(M)$ es maximal, entonces M es coprimario. En particular, las potencias de un ideal maximal $\mathfrak{m}$ son ideales $\mathfrak{m}$-primarios.

Corolario A.12.1: En un anillo noetheriano A, dados $\mathfrak{q}, \mathfrak{m} \trianglelefteq A$ con $\mathfrak{m}$ maximal, son equivalentes:

1. $\mathfrak{q}$ es $\mathfrak{m}$-primario.
2. $\operatorname{Rad}\mathfrak{q} = \mathfrak{m}$.
3. Existe algún $n \in \mathbb{N}_{\neq 0}$ tal que $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$.

Definición A.13: Un submódulo $N \leq M$ se dice ***reducible*** si existen $N_1, N_2 \leq M$ tales que $N = N_1 \cap N_2$ y $N \notin \{N_1, N_2\}$; de lo contrario se dice ***irreducible***.

Teorema A.14: Sea A un dominio noetheriano y M un A-módulo finitamente generado.

1. Todo submódulo irreducible es primario.

2. Todo submódulo admite una descomposición primaria minimal. En particular, todo ideal de A es decomposible.

3. Dada una descomposición irredundante de $N \leq M$:

$$N = \bigcap_{i=1}^{r} N_i,$$

donde cada N_i es $\mathfrak{p}_i$-primario, se cumple que $\mathrm{As}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

En consecuencia toda descomposición primaria minimal tiene la misma longitud y los mismos radicales.

4. Dado $N < M$, su $\mathfrak{p}$-componente primaria viene dada por $\lambda_{\mathfrak{p}}^{-1}[N_{\mathfrak{p}}]$ donde $\lambda_{\mathfrak{p}} \colon M \to M_{\mathfrak{p}}$ es el monomorfismo canónico.

Teorema A.15: Sea $\mathfrak{a}$ un ideal decomposible con descomposición minimal $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ y con $\mathfrak{p}_i := \operatorname{Rad} \mathfrak{q}_i$. Si $\mathcal{F} := \{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_j}\}$ es una familia aislada, entonces $\bigcap_{j=1}^{m} \mathfrak{q}_{i_j}$ es independiente de la descomposición.

Teorema A.16: Sea M un A-módulo y N un submódulo de M. Entonces N y M/N son noetherianos (resp. artinianos) syss M es noetheriano (resp. artiniano).

Proposición A.17: Sea A un dominio donde $(0) = \prod_{i=1}^{n} \mathfrak{m}_i$, donde $\mathfrak{m}_i$ son ideales maximales (posiblemente iguales). Entonces A es noetheriano syss es artiniano.

Corolario A.17.1: Un dominio es artiniano reducido syss se escribe de forma única como producto directo de finitos cuerpos.

Corolario A.17.2: Un dominio noetheriano reducido A es tal que su anillo de fracciones totales K es un producto directo de finitos cuerpos.

Corolario A.17.3: Sea A un dominio noetheriano y M un A-módulo finitamente generado. Son equivalentes:

1. M tiene longitud finita (es un módulo artiniano).

2. $\mathrm{Ann}(M) \supseteq \prod_{i=1}^{n} \mathfrak{m}_i$ para algunos $\mathfrak{m}_i$ ideales maximales.

3. Si $\mathfrak{p} \supseteq \operatorname{Ann}(M)$ es un ideal primo, entonces $\mathfrak{p}$ es maximal.

4. $A/\operatorname{Ann}(M)$ es artiniano.

Proposición A.18: Sea $(A, \mathfrak{m}, k)$ un dominio artiniano local. Son equivalentes:

1. A es un DIP.

2. $\mathfrak{m}$ es principal.

3. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

A.2 La topología de Zariski y esquemas afines

Definición A.19: Sea A un anillo. Denotamos por $\operatorname{Spec} A$ al conjunto de sus ideales primos. Dado un ideal $\mathfrak{a} \trianglelefteq A$ definimos

$$\mathbf{V}(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \supseteq \mathfrak{a}\} \subseteq \operatorname{Spec} A.$$

Lema A.20: Sea A un anillo, y sean $\mathfrak{a}, \mathfrak{b}, \mathfrak{a}_i$ ideales sobre A. Se cumplen:

1. $\mathbf{V}(0) = \operatorname{Spec} A, \mathbf{V}(1) = \varnothing$.

2. $\mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) = \mathbf{V}(\mathfrak{a} \cdot \mathfrak{b})$.

3. $\bigcap_{i \in I} \mathbf{V}(\mathfrak{a}_i) = \mathbf{V}\left(\sum_{i \in I} \mathfrak{a}_i\right)$.

Definición A.21: Por el lema anterior, los conjuntos de la forma $\mathbf{V}(\mathfrak{a})$ conforman los cerrados de una topología, llamada la ***topología de Zariski*** sobre $\operatorname{Spec} A$. Siempre veremos a $\operatorname{Spec} A$ como espacio topológico.

La motivación de crear un diccionario algebraico-geométrico es principalmente gracias a O. Zariski y A. Weil. Antes de ellos, no es que la geometría y el álgebra estuviesen desconectados, ni que la geometría algebraica no existiese, pero la relación entre ambas disciplinas era mucho más unidireccional, el álgebra era visto como una herramienta para la geometría, mientras que Zariski logró emplear sus conocimientos geométricos para revolucionar el álgebra. Este diccionario se enriquece arduamente tras la llegada de los esquemas, emergiendo tópicos como los de la suavidad formal o la cohomología local.

Bibliografía

Las fechas empleadas son aquellas de la primera publicación o del primer registro de Copyright.

Álgebra conmutativa

1. Atiyah, M. F. y McDonald, I. G. *Introduction to Commutative Algebra* (Addison-Wesley, 1969).
2. Bruns, W. y Herzog, J. *Cohen-Macaulay rings* (Cambridge University Press, 1998).
3. Eisenbud, D. *Commutative Algebra with a View Toward Algebraic Geometry* (Springer Science+Business Media, 1994).

EGA IV_1. Grothendieck, A. y Dieudonné, J. *Éléments de Géométrie Algébrique.* IV.1: *Étude locale des schémas et des morphismes de schémas* **20** (Publ. Math. IHÉS, 1964).

4. Matsumura, H. *Commutative Algebra* `https://github.com/AareyanManzoor/Matsumura-Commutative-Algebra` (W.A. Benjamin, Inc., 1969).
5. Matsumura, H. *Commutative Ring Theory* trad. por Reid, M. *Cambridge Studies in Advanced Mathematics* **8** (Cambridge University Press, 1986).
6. Nagata, M. *Local Rings* (Interscience, 1962).
7. Serre, J.-P. *Local Algebra* (Springer-Verlag Berlin Heidelberg, 1965).
8. Zariski, O. y Samuel, P. *Commutative Algebra* 2 vols. (D. Van Nostrand, 1958).

Otros recursos

EGA IV_2. GROTHENDIECK, A. y DIEUDONNÉ, J. *Éléments de Géométrie Algébrique.* IV.2: *Étude locale des schémas et des morphismes de schémas* **24** (Publ. Math. IHÉS, 1965).

9. JANUSZ, G. J. *Algebraic Number Fields* 2.ª ed. *Graduate Studies in Mathematics* **7** (American Mathematical Society, 1973).

Documentos históricos

10. ABEL, N. H. *Mémoire sur les equations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré* en *Oeuvres complètes de Niels Henrik Abel* (eds. SYLOW, L. y LIE, S.) **1** (Cambridge University Press, 1824), 28-33. doi:10.1017/CBO9781139245807.004.

11. ABEL, N. H. *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré* en *Oeuvres complètes de Niels Henrik Abel* (eds. SYLOW, L. y LIE, S.) **1** (Cambridge University Press, 1826), 28-33. doi:10.1017/CBO9781139245807.008.

12. ABEL, N. H. Mémoire sur une classe particulière d'équations résolubles algébriquement. *J. Reine Angew. Math.* doi:10.1515/crll.1829.4.131 (1829).

13. AUSLANDER, M. y BUCHSBAUM, D. A. Codimension and Multiplicity. *Ann. Math.* **68,** 625-657. doi:10.2307/1970159 (1958).

14. COHEN, I. S. y SEIDENBERG, A. Prime ideals and integral dependence. *Bull. Amer. Math. Soc.* **52,** 252-261. doi:10.1090/S0002-9904-1946-08552-3 (1946).

15. COHEN, I. S. On the structure and ideal theory of complete local rings. *Trans. Amer. Math. Soc.* **59,** 54-106. doi:10.1090/S0002-9947-1946-0016094-3 (1946).

16. DEDEKIND, R. Sur la théorie des nombres entiers algébriques. *Bull. Sci. Math. et Astronomiques.* doi:10.1007/978-3-322-98606-1_3 (1876).

17. DIRICHLET, P. G. L. *Vorlesungen über Zahlentheorie* (ed. DEDEKIND, R.) (Braunschweig, 1863).

18. GALOIS, É. *Des équations primitives qui sont solubles par radicaux* en *The mathematical writings of Évariste Galois* (ed. NEUMANN, P. M.) (European Mathematical Society, 1830), 169-191.

19. GALOIS, É. *Mémoire sur les conditions de résolubilité des équations par radicaux* en *The mathematical writings of Évariste Galois* (ed. NEUMANN, P. M.) (European Mathematical Society, 1830), 105-135.
20. GAUSS, C. F. *Disquisitiones Arithmeticae* trad. por RUIZ ZÚÑIGA, A. https://archive.org/details/disquisitiones-arithmeticae-carl-f.-gauss-espanol (Universidad de Costa Rica, 1801).
21. HERMITE, C. Sur la fonction exponencielle. *C. R. Acad. Sci.* **77,** 18-24. doi:10.1017/CBO9780511702778.012 (1873).
22. HILBERT, D. Ueber die Theorie der algebraischen Formen. *Math. Ann.* doi:10.1007/BF01208503 (1890).
23. HILBERT, D. Ueber die vollen Invariantensysteme. *Math. Ann.* doi:10.1007/978-3-642-52012-9_19 (1893).
24. HOCHSTER, M. y ROBERTS, J. L. Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. *Adv. Math.* **13,** 115-175. doi:10.1016/0001-8708(74)90067-X (1974).
25. KRONECKER, L. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. Reine Angew. Math.* doi:10.1515/crll.1882.92.1 (1882).
26. KRULL, W. Beiträge zur Arithmetik kommutativer Integritätsbereiche. III. Zum Dimensionsbegriff der Idealtheorie. *Math. Z.* **42,** 745-766. https://eudml.org/doc/168748 (1937).
27. KUMMER, E. E. *De Numeris Complexis, Qui Radicibus Unitatis Et Numeris Integris Realibus Constant* (Kessinger Publishing, 1844).
28. KUMMER, E. E. Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist. *Kgl. Preuss. Akad. Wiss* (1856).
29. NAGATA, M. Some Remarks on Local Rings. *Nagoya Math. J.* **6,** 53-58. doi:10.1017/S0027763000016974 (1953).
30. NAGATA, M. A General Theory of Algebraic Geometry Over Dedekind Domains, I: The Notion of Models. *Amer. J. Math.* **78,** 78-116. doi:10.2307/2372486 (1956).
31. NOETHER, E. Idealtheorie in Ringbereichen. *Math. Ann.* doi:10.1007/978-3-642-39990-9_19 (1921).
32. NOETHER, E. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik *p*. *Nachr. Ges. Wiss. Göttingen,* 28-35. https://eudml.org/doc/59193 (1926).
33. NOETHER, E. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. *Math. Ann.* **96,** 26-61. doi:10.1007/BF01209152 (1927).

34. REES, D. The grade of an ideal or module. *Math. Proc. Cambridge Phil. Soc.* **53,** 28-42. doi:10.1017/S0305004100031960 (1957).

35. Von LINDEMANN, F. Über die Ludolph'sche Zahl. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* **2,** 679-682 (1882).

36. Von LINDEMANN, F. Über die Zahl π. *Math. Ann.* **20,** 213-225. doi:10.1007/bf01446522 (1882).

37. WEIERSTRASS, K. Zu Lindemann's Abhandlung. "Über die Ludolph'sche Zahl". *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* **5,** 1067-1085. doi:10.1007/978-1-4757-3240-5_23 (1885).

38. ZARISKI, O. Foundations of a general theory of birational correspondence. *Trans. Amer. Math. Soc.* **53,** 490-542. doi:10.1090/S0002-9947-1943-0008468-9 (1943).

Historia

39. EDWARDS, H. M. The Genesis of Ideal Theory. *Archive for History of Exact Sciences.* doi:10.1007/bf00327914 (1980).

40. GROTHENDIECK, A. *Cosechas y Siembras* trad. por NAVARRO, J. A. http://matematicas.unex.es/~navarro/res/ (1986).

41. KIERNAN, B. M. The development of Galois theory from Lagrange to Artin. *Archive for History of Exact Sciences.* doi:10.1007/BF00327219 (1971).

42. KLINE, M. *Mathematical Thought from Ancient to Modern Times* 3 vols. (Oxford University Press, 1972).

43. PARIKH, C. *The unreal life of Oscar Zariski* (Springer Science+Business Media, 2008).

Libros de autoría propia

44. CUEVAS, J. *Geometría algebraica* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/geo-alg/geometria-algebraica.pdf (2022).

45. CUEVAS, J. *Teoría de categorías y álgebra homológica* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/cats/teoria-categorias.pdf (2022).

46. CUEVAS, J. *Teoría de Conjuntos* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/conjuntos/conjuntos.pdf (2022).

47. CUEVAS, J. *Teoría de Números* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/teo-numeros/main.pdf (2022).

48. CUEVAS, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).

Índice alfabético

Lista de tareas pendientes