Álgebra

José Cuevas Barrientos

19 de diciembre de 2022

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 **[7],** aunque recomiendo mucho más la lectura del Aluffi **[1]** para principiantes. Materiales más completos y extensos lo son los tomos de Rotman **[11]** y, uno de mis preferidos, Jacobson **[6].**

Luego podemos detenernos a materiales más específicos de determinados temas: **[5]** 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 **[8].** Sobre el álgebra conmutativa, el libro de Atiyah y McDonald **[16]** es la introducción estándar, y el material más sintético de todos; de él se recomienda pasar a Eisenbud **[17]** que es mucho más extenso, pero mantiene una estrecha relación con la geometría algebraica; también el Matsumura **[18]** es una buena continuación, pero el más completo (y por tanto más difícil) es su otro libro **[19].**

Parte I.

Álgebra Abstracta Elemental

1

Teoría de grupos

Comenzaremos el capítulo con dar una breve introducción a la teoría de números, la cual servirá tanto para ilustrar como para poder definir ciertos conceptos que nos serán útiles.

1.1 Estructuras algebraicas

En el libro sobre teoría de conjuntos vimos como mediante variados modelos se pueden formalizar las matemáticas mediante el objeto de los conjuntos (o las clases). No obstante, varios matemáticos (incluidos Cantor mismo) describen a estos elementos como *amorfos* en el sentido de que podrían ser o representar cualquier cosa sin ninguna clase de patrón e importancia. En este sentido surge el concepto de las *estructuras algebraicas*, como conjuntos dotados de propiedades que generan objetos que resultan de interés y que son manejables. Se comenzará este libro analizando una de las estructuras más básicas (pero no menos importantes o interesantes):

Definición 1.1 – *Grupos*: Una función $\cdot : G^2 \to G$ sobre un conjunto G se dice que cumple:

Asociatividad Para todo $x, y, z \in G$ se cumple $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Elemento neutro Existe $e \in G$ tal que para todo $x \in G$ se cumple $e \cdot x = x \cdot e = x$.

Conmutatividad Para todo $x, y \in G$ se cumple $x \cdot y = y \cdot x$.

Además se dice que un elemento $x \in G$ es *invertible* (donde G posee neutro e) si existe $y \in G$ tal que $x \cdot y = y \cdot x = e$, en cuyo caso al y le decimos una *inversa* de x.

Un par $(G, \cdot)$ se dice:

Semigrupo Si $\cdot$ es asociativa.

Monoide Si $(G, \cdot)$ es semigrupo y posee neutro.

Grupo Si $(G, \cdot)$ es monoide y todo elemento es invertible.

Además se agrega el sufijo *abeliano* si $(G, \cdot)$ es conmutativo.

De aquí en adelante abreviaremos $xy = x \cdot y$.

Ejemplo. Son grupos:

- $(\{e\}, \cdot)$, donde $e \cdot e := e$. A éste grupo le decimos el *grupo trivial*.
- $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Q}, +)$ y $(\mathbb{R}, +)$.
- $(\mathbb{Q}_{\neq 0}, \cdot)$ y $(\mathbb{R}_{\neq 0}, \cdot)$.
- Si p es primo, entonces $(\mathbb{Z}_p \setminus \{0\}, \cdot)$.
- Si $X \neq \varnothing$, entonces $(\mathrm{Sym}(X), \circ)$ [las biyecciones de X con la composición] es un grupo.

Los cuatro primeros incisos son grupos abelianos.

Teorema 1.2: Sea $(G, \cdot)$ una estructura algebraica:

1. Si posee elemento neutro es único.

Si es semigrupo:

2. La inversa de un elemento invertible es única, por lo que le denotamos como a^{-1}.
3. La inversa de un elemento a invertible es también invertible y, de hecho, $(a^{-1})^{-1} = a$.
4. El producto de invertibles es invertible y
$$(ab)^{-1} = b^{-1}a^{-1}.$$

Si es grupo entonces:

5. Posee *cancelación* por la izquierda y derecha:

$$ab = ac \iff b = c, \quad ab = cb \iff a = c.$$

En virtud de este teorema, denotaremos 1 al neutro de un grupo en general para mantener la notación multiplicativa (excepto en ejemplos concretos claro).

Definición 1.3: Si $(G, \cdot)$ es un grupo de neutro e, y $(a_i)_{i\in\mathbb{N}}$ es una sucesión en G, vamos a definir por recursión:

$$\prod_{k=1}^{1} a_k = a_1, \quad \prod_{k=1}^{n+1} a_k = \left(\prod_{k=1}^{n} a_k\right) \cdot a_{n+1}.$$

En este caso la expresión $\prod_{k=1}^{n}$ se lee como "producto de índice k desde 1 hasta n", donde el n se dice el super-índice o punto de fin. Si el punto de final es menor al de partida, entonces por definición el producto es el neutro.

Si la operación sobre G es $+$ usamos Σ en lugar de Π.

Proposición 1.4 (Asociatividad generalizada): Si $g_1, \ldots, g_n \in G$ y $1 \leq k < n$, entonces

$$\prod_{i=1}^{n} g_i = \left(\prod_{i=1}^{k} g_i\right) \cdot \left(\prod_{i=k+1}^{n} g_i\right).$$

Pista: Se hace por inducción. □

Ésto nos dice que podemos hacer un producto finito en el orden que queramos.

Proposición 1.5: Sea $(S, \cdot)$ un semigrupo tal que

1. Si para todo $a, b \in S$ existen $x, y \in S$ tales que $ax = b$ e $ya = b$, entonces S es un grupo.

2. Si es finito entonces es grupo syss posee cancelación por la izquierda y la derecha.

Definición 1.6 – *Subgrupo*: Sea G un grupo. Se dice que $S \subseteq G$ es subgrupo si $(S, \cdot \restriction S^2)$ es grupo, lo que denotaremos por $S \leq G$.

Ejemplo. Sea G un grupo, entonces $\{1\}$ y G son subgrupos de G a los que llamamos *impropios*. Los subgrupos de G que no son impropios se dicen *propios*.

En general, dada cualquier tipo de estructura añadiremos el prefijo *sub-* para indicar que es subconjunto de otra estructura con la que comparte propiedades.

Teorema 1.7 (Criterio de subgrupos): $S \leq G$ syss es no vacío y para todo $x, y \in S$ se cumple que $xy^{-1} \in S$.

Corolario 1.8: La intersección arbitraria de subgrupos es un subgrupo. Además nunca es vacía pues 1 siempre pertenece a la intersección de subgrupos.

Definición 1.9 – *Subgrupo generado*: Dado $S \subseteq G$ se denota $\langle S \rangle$ a

$$\langle S \rangle := \bigcap \{H : S \subseteq H \leq G\}$$

Es decir, al mínimo subgrupo (bajo la inclusión) de G que le contiene. Si $S = \{x_1, \ldots, x_n\}$ nos permitiremos abreviar $\langle x_1, \ldots, x_n \rangle := \langle S \rangle$.

Corolario 1.10: $S \leq G$ syss $\langle S \rangle = S$.

Proposición 1.11: Para todo $x \in \langle S \rangle$, se cumple que

$$x = x_1 x_2 \cdots x_n$$

donde para todo $i \leq n$ se cumple que x_i o x_i^{-1} pertenece a S.

Teorema 1.12: Sean $A, B \leq G$, tales que $A \cup B \leq G$, entonces $A \subseteq B$ o $B \subseteq A$.

Demostración: Si son iguales, entonces el resultado está probado. De lo contrario, sin perdida de generalidad supongamos que $a \in A \setminus B$, demostraremos que $B \subset A$.

Sea $b \in B$, como $A \cup B$ es grupo, entonces $ab \in A \cup B$, ergo, $ab \in A$ o $ab \in B$. No obstante, $ab \notin B$ pues de lo contrario como $b^{-1} \in B$ entonces $a \in B$, lo que es absurdo. Como $ab, a^{-1} \in A$ entonces $b \in A$. □

Proposición 1.13: Si $\{H_i : i \in I\}$ es una $\subseteq$-cadena[1] de subgrupos, entonces $H := \bigcup_{i\in I} H_i$ es un subgrupo, y de hecho es el mínimo subgrupo que contiene a todos los H_i.

Demostración: Sea $x, y \in H$, por definición hay un par de subgrupos H_x y H_y en la familia tales que $x \in H_x$ e $y \in H_y$. Luego como es linealmente ordenado, entonces $H_x \subseteq H_y$ o $H_y \subseteq H_x$, luego $H_z := H_x \cup H_y$ pertenece a la familia y contiene a x, y, luego $xy^{-1} \in H_z \subseteq H$, por lo que $H \leq G$ por el criterio.

La parte de ser «el mínimo que contiene a la familia» queda al lector. □

Definición 1.14 – *Potencias y generadores*: Sea $x \in G$ y $n \in \mathbb{Z}$, entonces se le llama n-ésima potencia de x a:

$$x^n = \begin{cases} \prod_{i=1}^{n} x & n > 0 \\ 1 & n = 0 \\ (x^{-1})^{-n} & n < 0 \end{cases}$$

Al emplear notación aditiva se denota «nx» en lugar de «x^n».

Se dice que B es una base si genera a G, i.e., si $\langle B\rangle = G$. Un grupo G que posee una base finita se dice un *grupo finitamente generado*. Un grupo se dice *cíclico* si posee una base singular. Se define el orden de un elemento x, denotado por $\operatorname{ord} x$, como el mínimo natural n tal que $x^n = 1$ y de no existir ningún natural que satisfaga dicha condición se define como de orden 0.

Corolario 1.15: Se cumplen:

1. Los grupos cíclicos son abelianos.

2. Todo subgrupo de un grupo cíclico es también cíclico.

3. Si $\operatorname{ord} x \neq 0$, entonces $\operatorname{ord} x = |\langle x\rangle|$.

[1] Es decir, tal que para todo $i, j \in I$ se cumple que $H_i \subseteq H_j$ o $H_j \subseteq H_i$.

Ejemplo.
- $(\mathbb{Z}, +)$ es un grupo cíclico, cuyo generador es el 1 y de orden 0.
- $(\mathbb{Z}_n, +)$ es un grupo cíclico, cuyo generador es el 1 y de orden n.

Ejemplo. Considere el grupo $(\mathbb{Q}, +)$ y veamos que no es finitamente generado. Sea $H \subseteq \mathbb{Q}$ finito, nótese que el 0 siempre puede ser generado por otro elemento así que lo podemos sacar. Sea n el máximo de los denominadores de $H_{\neq 0}$ (donde $m/n \in H$ con m, n coprimos), luego sea p el primer primo mayor que n. Luego $1/p \notin H$ y si $1/p \in \langle H \rangle$, entonces

$$\frac{1}{p} = \frac{a_1}{n_1} + \frac{a_2}{n_2} + \cdots + \frac{a_m}{n_m} = \frac{a_1(n_2 \cdots n_m) + a_2(n_1 n_3 \cdots n_m) + \cdots + a_m(n_1 \cdots n_{m-1})}{n_1 n_2 \cdots n_m}.$$

Luego $p \mid n_1 n_2 \cdots n_m$, pero por el lema de Euclides, necesariamente $p \mid n_i$ para algún i, pero ésto es absurdo por construcción.

Proposición 1.16: Dado $a \in G$ y $n \in \mathbb{Z}_{\neq 0}$, se cumple que

$$\operatorname{ord}(a^n) = \frac{\operatorname{ord} a}{\operatorname{mcd}(\operatorname{ord} a, n)} = \frac{\operatorname{mcm}(\operatorname{ord} a, n)}{n}.$$

Proposición 1.17: Si $a, b \in G$ conmutan, entonces

$$\operatorname{ord}(ab) = \operatorname{mcm}(\operatorname{ord} a, \operatorname{ord} b).$$

Proposición 1.18: Si G es un grupo tal que todo elemento no neutro tiene orden 2, entonces G es abeliano.

Demostración: Sean $g, h \in G$, luego

$$gh = gh(hg \cdot hg) = hg. \qquad \square$$

Teorema (AE) 1.19: Si G tiene una base finita, entonces todo subgrupo propio está contenido en un subgrupo maximal.

Demostración: La demostración aplica el lema de Zorn. Sea $S \lneq G$ y $B := \{g_1, \ldots, g_n\}$ base de G, entonces sea $S_k := \langle S, g_1, g_2, \ldots, g_k \rangle$ de modo que

$$S = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_n = G.$$

Elijamos S_m como el subgrupo más grande distinto de G, luego sea

$$\mathcal{F} := \{H : S_m \leq H \lneq G \wedge g_{m+1} \notin H\}$$

entonces $\mathcal{F}$ es un conjunto parcialmente ordenado por la inclusión, y toda cadena tiene supremo por la proposición anterior (1.13), luego por el lema de Zorn tiene un elemento maximal M que es subgrupo no tiene a g_{m+1} (de modo que es distinto de G), contiene a S y es trivial ver que M es un subgrupo maximal. □

Definición 1.20 – *Morfismos*: Decimos que una aplicación $\varphi\colon (G,\cdot) \to (H,\star)$ entre grupos es un *homomorfismo de grupos* si para todo $a, b \in G$:

$$\varphi(a \cdot b) = \varphi(a) \star \varphi(b).$$

A esto se le agrega el prefijo *mono-*, *epi-* e *iso-* si es inyectiva, suprayectiva y biyectiva resp. Dos grupos se dicen *isomorfos* si existe un isomorfismo entre ambos, lo que se escribe como $G \cong H$. Cuando queramos decir que un morfismo es un mono- o epimorfismo diremos que es mónico o épico resp.

Si $\varphi\colon G \to G$ se le añade el prefijo *endo-* y si además resulta ser biyectiva, entonces se le añade el prefijo *auto-*. Esta nomenclatura se aplica a todos los otros morfismos en álgebra.

Visualmente denotamos los monomorfismos por $\hookrightarrow$, los epimorfismos por $\twoheadrightarrow$ y los isomorfismos por $\rightsquigarrow$ (algunos usan $\xrightarrow{\sim}$).

Se le llama *kernel* (*núcleo* en alemán) a la preimagen del 1:

$$\ker\varphi := \varphi^{-1}[\{1\}] = \{g \in G : \varphi(g) = 1\}.$$

Ejemplo.

- En todo grupo G, la identidad $x \mapsto x$ es un automorfismo.
- En todo grupo abeliano, la inversa $x \mapsto x^{-1}$ es un automorfismo.
- En $(\mathbb{Q},+)$ se cumple que $f(x) = kx$ con $k \neq 0$ también es un automorfismo.
- En $(\mathbb{Z},+)$ la función $f(x) = 2x$ es un endomorfismo mónico pero no épico, pues 1 no tendría preimagen.

Proposición 1.21: Si $\varphi\colon G \to H$ es un isomorfismo, entonces:

1. G y H comparten cardinalidad.
2. φ^{-1} es también un isomorfismo.
3. Para todo $g \in G$ se cumple que $\text{ord}(\varphi(g)) = \text{ord}(g)$.
4. G es abeliano syss H lo es.

Teorema 1.22: Sea $G = \langle g \rangle$, entonces:

1. Si es finito y $|G| = m$, entonces $G = \{1, g, g^2, \ldots, g^{m-1}\}$ y $g^n = e$ syss $m \mid n$.
2. Si G es infinito, entonces $(G, \cdot) \cong (\mathbb{Z}, +)$.
3. Si G es finito, entonces $G \cong \mathbb{Z}_m$

Definición 1.23 – *Clases laterales*: Dados dos subconjuntos A, B de G, se define

$$AB := \{xy : x \in A, y \in B\}$$

Si alguno es el conjunto singular $A = \{a\}$, omitiremos las llaves, de modo que $aB := \{a\} \cdot B$ y $Ab := A \cdot \{b\}$.

Lema 1.24: Sea $H \leq G$ y $a, b \in G$, entonces

1. $a \in aH$.
2. $aH = bH$ o $aH \cap bH = \varnothing$.
3. $a \equiv b \pmod{H_-}$ dado por $a^{-1}b \in H$ y $a \equiv b \pmod{H_+}$ dado por $ab^{-1} \in H$ son relaciones de equivalencia.
4. $|aH| = |bH| = |Hb| = |Ha|$.

Demostración: Probaremos la segunda, esto es que si no son disjuntos entonces son iguales. Sea $c \in aH \cap bH$, por definición, $c = ax = by$ con $x, y \in H$, luego $b = a(xy^{-1})$ donde $xy^{-1} \in H$ por el criterio de subgrupo. □

Denotaremos G/H_- al conjunto cociente de G bajo la relación de equivalencia que es la congruencia módulo H_-. Denotamos $[G : H]$ al cardinal de G/H_- o de G/H_+ (que son iguales). Notemos que bajo estas definiciones, la notación $\mathbb{Z}_n$ tiene sentido.

Teorema 1.25 – *Teorema de Lagrange*: Sea $H \leq G$ con G finito, entonces

$$|H|\,[G:H] = |G|.$$

En base al teorema de Lagrange, llamamos *índice* de un subgrupo H al valor de $[G:H]$.

Corolario 1.26: El orden de todo elemento de un grupo finito es un divisor de su cardinal.

Corolario 1.27: Todo grupo de cardinal p primo es cíclico y, en consecuente, isomorfo a $\mathbb{Z}_p$.

Definición 1.28: Denotamos por $\mathbb{Z}_n^\times$ (léase "grupo multiplicativo" o "unidades de n") al conjunto de todos los elementos coprimos a n de $\mathbb{Z}_n$. Queda al lector demostrar que $(\mathbb{Z}_n^\times, \cdot)$ es un grupo abeliano de neutro 1.

Llamamos $\phi : \mathbb{N}_{\geq 2} \to \mathbb{N}$ a la función ϕ o indicatriz de Euler que mide el cardinal del grupo multiplicativo de m, es decir:

$$\phi(n) := |\mathbb{Z}_n^\times|$$

Teorema 1.29 (Euler-Fermat): Si a coprimo a n, entonces

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Corolario 1.30 (Pequeño teorema de Fermat): Sea $a \in \mathbb{Z}_p$ no nulo, entonces

$$a^{p-1} \equiv 1, \quad a^p \equiv a \pmod{p}.$$

Teorema 1.31 – *Teorema chino del resto*: Si $(n;m) = 1$, entonces

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm},$$

donde un isomorfismo f es de la siguiente forma: dados p, q tales que $pn + qm = 1$, entonces

$$f(x,y) := ypn + xqm.$$

Demostración: Probemos que la función propuesta es, en efecto, un isomorfismo. La construcción utiliza la identidad de Bézout que requiere que los valores sean coprimos, veamos que f está bien definida: si $x' = x + an$ e $y' = y + bm$, entonces

$$\begin{aligned} f(x', y') &= (y + bm)pn + (x + an)qm \\ &= ypn + xqm + nm(aq + bp) \equiv f(x, y) \pmod{nm}. \end{aligned}$$

Ahora veamos que f es inyectiva: Si

$$\begin{aligned} f(a, b) &\equiv f(c, d) \\ aqm + bpn &\equiv cqm + dpn \\ (a - c)qm &\equiv np(d - b) \pmod{nm}. \end{aligned}$$

Osea $(a - c)qm = np(d - b) + snm = n(p(d - b) + sm)$, luego $n \mid (a - c)qm$, pero $(n; qm) = 1$, luego por lema de Euclides, $n \mid a - c$ lo que equivale a que $a \equiv c \pmod{n}$. Es análogo que $b \equiv d \pmod{m}$, que es lo que se quería probar.

Como f es inyectiva entre dos conjuntos finitos equipotentes, entonces es biyectiva, luego es isomorfismo. □

Corolario 1.32: Si $(n; m) = 1$, entonces

$$\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times,$$

en particular $\phi(n)\phi(m) = \phi(nm)$.

Proposición 1.33: Si p primo entonces $\phi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$. Luego, si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, entonces

$$\phi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right).$$

1.2 Ejemplos de grupos

§1.2.1 Grupos simétrico y alternante. Dados nuestros conocimientos en teoría de conjuntos debería de ser fácil probar que $(\mathrm{Func}(S), \circ)$ es siempre un monoide y para que cumpla ser un grupo debemos considerar el subgrupo de los elementos invertibles, es decir, el conjunto de las permutaciones de S, el cual denotamos por $\mathrm{Sym}(S)$.

Es fácil probar que $\mathrm{Sym}(S) \cong \mathrm{Sym}(T)$ syss $|S| = |T|$, así que como representante general denotaremos S_n al grupo simétrico sobre $\{1, 2, \ldots, n\}$.

Proposición 1.34: Se cumple:

1. $|S_n| = n!$
2. S_n no es abeliano con $n \geq 3$.
3. $S_i \leq S_j$ para todo $i < j$.

Teorema 1.35 – *Teorema de Cayley*: Para todo grupo finito G de cardinal n se cumple que

$$G \cong H \leq S_n.$$

Demostración: Vamos a definir $\varphi_a : G \to G$ como $f_a(x) = xa$. Sigue que

$$(f_a \circ f_b)(x) = f_b(f_a(x)) = f_b(xa) = (xa)b = x(ab) = f_{ab}(x).$$

Es decir, que $f_{ab} = f_a \circ f_b$. Nótese que las aplicaciones f_a son biyectivas pues admiten inversa f_a^{-1}. Finalmente $\varphi(a) = f_a$ es un monomorfismo cuya imagen forma un subgrupo de S_n, que es lo que se quería probar. □

La importancia del teorema de Cayley, también y apropiadamente llamado teorema de representación de grupos finitos, es que nos permite describir a los grupos finitos en término de los grupos simétricos, destacando la importancia de éstos últimos.

Definición 1.36 (Órbitas y ciclos): Dado $\sigma \in \mathrm{Sym}(S)$ y $a \in S$, diremos que la órbita de a es la tupla ordenada

$$(a, \sigma(a), \sigma^2(a), \ldots)$$

En particular, como $\mathrm{Sym}(S)$ es siempre de cardinal finito, entonces toda permutación es de orden finito, por ende, todas las órbitas lo son. Diremos que una órbita es trivial si posee un único elemento. Los elementos de órbitas triviales se llaman *puntos fijos*.

Diremos que una permutación es un *ciclo* syss todas sus órbitas son triviales excepto una. En cuyo caso, denotaremos a la permutación mediante su órbita no-trivial, por ejemplo, la permutación

$$\{(1,1),(2,3),(3,5),(4,4),(5,2),(6,6)\} \in \mathrm{Sym}(6)$$

se denotará como $(2,3,5)$, $(3,5,2)$ o $(5,2,3)$. **Ojo:** los ciclos están ordenados, no es lo mismo $(2,3,5)$ que $(5,3,2)$. Los ciclos de orden 2 se denominarán *trasposiciones*.

Dos ciclos se dicen *disjuntos* si sus órbitas no-triviales lo son.

Teorema 1.37: Se cumplen:

1. El orden de los ciclos es el cardinal de su órbita no trivial.
2. La inversa de un ciclo $(a_1, a_2, \ldots, a_{n-1}, a_n)$ es $(a_n, a_{n-1}, \ldots, a_2, a_1)$.
3. Dos ciclos disjuntos conmutan.
4. Toda permutación de S_n excepto Id, puede escribirse como el producto de ciclos disjuntos dos a dos.
5. El orden de un producto de ciclos disjuntos dos a dos es el mínimo común múltiplo de todos sus ordenes.
6. Las trasposiciones forman una base para S_n.
7. Si $\sigma \in S_n$ y $(a_1, \ldots, a_n)$ es un ciclo, entonces
$$\sigma^{-1}(a_1, \ldots, a_n)\sigma = (\sigma(a_1), \ldots, \sigma(a_n)).$$

Demostración:

4. Dada una permutación de S_n distinta de la identidad, luego posee alguna órbita no trivial. Finalmente se deduce que se puede escribir como la composición de todos los ciclos derivados de sus órbitas no triviales, los cuales son disjuntos dos a dos.
5. Queda al lector.
6. Por la 4, basta probar que todo ciclo está generado por trasposiciones, lo que se hace notando que
$$(a_1, a_2, \ldots, a_n) = (a_1, a_2)(a_1, a_3)\cdots(a_1, a_n). \qquad \square$$

Signo de una permutación.

Lema 1.38: Si $\sigma \in S_n$ cumple que
$$\sigma = \prod_{i=1}^{n} \tau_{1,i} = \prod_{i=1}^{m} \tau_{2,i}$$
donde $\tau_{j,i}$ es una trasposición, entonces $n \equiv m \pmod 2$.

Demostración: En dicha situación podemos mover todo de un lado al otro y escribir:

$$1 = \left(\prod_{i=1}^{n} \tau_{1,i}\right)\left(\prod_{i=1}^{m} \tau_{2,(m-i+1)}^{-1}\right) = \tau_{1,1}\tau_{1,2}\cdots\tau_{1,n}\tau_{2,m}^{-1}\tau_{2,m-1}^{-1}\cdots\tau_{2,1}^{-1}.$$

Por ende, se reduce a probar que el producto de impares trasposiciones nunca es 1.

Supongamos que 1 puede ser el producto de un número impar de trasposiciones, entonces sea n el mínimo impar que lo cumpla. Es claro que n no puede ser 1, luego sea $(\tau_i)_{i=1}^n$ una sucesión de trasposiciones cuyo producto es 1, luego sean $(a_i, b_i) := \tau_i$ donde $a_i < b_i$ para que esté bien definido. Notemos que la primera trasposición mueve a a_1 a b_1, así que alguna otra debe mover a b_1, es decir, $b_1 = a_i$ o b_i para algún $i > 1$. Así usaremos que

$$(a,b)(c,d) = (c,d)(a,b), \quad (a,b)(b,c) = (b,c)(a,b)$$

Para mover ese a_i o b_i a la segunda trasposición, y de paso, renombraremos $a_2 := b_1$ y b_2 como aquél que le acompañaba. Ahora tenemos que

$$1 = (a_1, b_1)(b_1, b_2)\tau_3 \cdots \tau_n.$$

a) Caso 1 ($b_2 = a_1$): En este caso $\tau_1 = \tau_2$ y luego se cancelan pues las trasposiciones son de orden dos, luego 1 se escribe con $n-2$ trasposiciones con $n-2$ impar, lo que contradice la minimalidad de n.

b) Caso 2 ($b_2 \neq a_1$): Aquí utilizamos una de las propiedades señaladas para ver que

$$1 = (b_1, b_2)(a_1, b_2)\tau_3 \cdots \tau_n$$

luego iteramos el paso anterior y reordenamos de forma que $\tau_3 = (b_2, b_3)$. Como el producto es la identidad, podemos reordenar e iterar el proceso varias veces pero llega un punto en el que $b_i = a_1$ en cuyo caso las dos trasposiciones se cancelaran y contradicen la minimalidad de n. □

Definición 1.39: Si una permutación σ se puede escribir como un producto de n trasposiciones, entonces $\operatorname{sgn}\sigma := (-1)^n$. Las permutaciones de signo 1 se dicen *pares* y el resto *impares*.

Notemos que la identidad es par, y las trasposiciones impares. Un ciclo de longitud n es de paridad $(-1)^{n+1}$.

Proposición 1.40: Se cumple que $\operatorname{sgn} : S_n \to (\{\pm 1\}, \cdot)$ es un homomorfismo, es decir, $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau$.

Corolario 1.41: El signo se conserva entre inversas y conjugados.

Como vimos, el signo es un morfismo de grupos, esto es importante porque significa que el kernel del signo, es decir el conjunto de permutaciones pares, es un subgrupo normal del simétrico. Luego denotamos

$$A_n := \{\sigma \in S_n : \operatorname{sgn}\sigma = 1\}.$$

Proposición 1.42: Se cumple:

1. Para $n > 2$, se cumple que $|A_n| = \frac{n!}{2}$.
2. $A_i \leq A_j$ para todo $2 < i < j$.
3. A_4 es no abeliano y en consecuencia todo A_n con $n \geq 4$ lo es.

§1.2.2 Grupo diedral. Consideremos un polígono de n lados (o n-gono) regular y enumeremos sus vértices. Pongamos reglas: claramente no admitimos la posibilidad de deformar el polígono, de manera que, por ejemplo, el vértice 2 siempre está entre el vértice 1 y el vértice 3. Los vértices se «leen» en sentido horario y siempre hay un vértice líder o principal por el cuál se comienzan a enumerar el resto. Así, llamamos grupo diedral al conjunto de todas las isometrías posibles en el polígono, en particular, como indicamos que lo que nos interesa es el ordenamiento de los vértices, entonces traslaciones no afectan a la figura, sino que sólo lo hacen las rotaciones y las reflexiones:

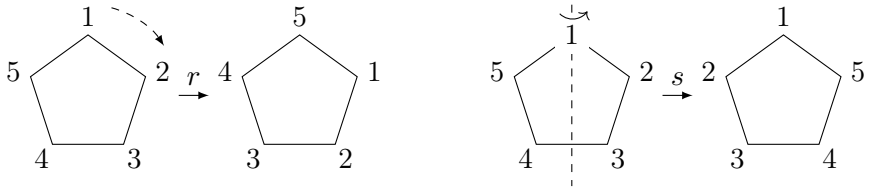


Figura 1.1. Ejemplo con un pentágono.

En esencia esto representa a un grupo, sin embargo, hay que formalizar esta idea, y para ello, definiremos:

Definición 1.43 – *Grupo diedral o diédrico*: Fijado un $n > 2$, se definen $r := (1, 2, \dots, n)$ [una rotación] y

$$s = \begin{cases} (2,n)(3,n-1)\cdots(k,k+1) & n = 2k+1 \\ (2,n)(3,n-1)\cdots(k-1,k+1) & n = 2k \end{cases}$$

[una reflexión en torno al 1]. Luego $D_{2n} := \langle r, s \rangle$ es el grupo diedral.

Proposición 1.44: Para todo grupo diedral se cumple:

1. En D_{2n} se cumple que $\operatorname{ord} r = n$ y $\operatorname{ord} s = 2$.
2. $rs = sr^{-1}$ y más generalmente $r^k s = sr^{-k}$. Esto equivale a que $srs^{-1} = r^{-1}$ y que $\operatorname{ord}(r^k s) = 2$.
3. El grupo no es abeliano, por ende tampoco es cíclico.
4. $|D_{2n}| = 2n$.

1.3 Representaciones de grupos finitos

§1.3.1 Teoremas de isomorfismos. Éstos teoremas son herramientas casi-universales en el álgebra. Realizaremos la demostración en el contexto de teoría de grupos, pero no la repetiremos en el contexto de anillos ni módulos, pues son análogas.

Lema 1.45: Sea $N \leq G$. Entonces son equivalentes:

1. Para todo $x \in G$ se cumple que $xNx^{-1} \subseteq N$.
2. Para todo $x \in G$ se cumple que $xNx^{-1} = N$.
3. Para todo $x \in G$ se cumple que $xN = Nx$.

Demostración: Basta considerar $y := x^{-1}$ para obtener que $yNy^{-1} \subseteq N$, luego $N \subseteq xNx^{-1}$. □

Definición 1.46: Dos elementos de un grupo $a, b \in G$ se dicen *conjugados* si existe $x \in G$ tal que $x^{-1}ax = b$.

Se dice que un subgrupo $N \leq G$ es *normal*, denotado $N \trianglelefteq G$, syss para todo $x \in G$ se cumple que $xN = Nx$.

Proposición 1.47: Si $\varphi\colon G \to H$ es un homomorfismo, entonces $\ker\varphi \trianglelefteq G$.

Teorema 1.48: Si $N \trianglelefteq G$, entonces la relación $x \sim y$ dada por $xN = yN$ determina una clase de equivalencia. Más aún, G/N posee estructura de grupo, la proyección sobre clases de equivalencia $\pi\colon G \to G/N$ es un epimorfismo de anillos y $\ker\pi = N$.

Demostración: Para comprobar que G/N posee estructura de grupo basta notar que empleando que $yN = Ny$ se obtiene que

$$(xN)(yN) = x(Ny)N = x(yN)N = (xy)(NN) = (xy)N,$$

donde es claro que $N \cdot N = N$. De éste modo es fácil comprobar que π es además homomorfismo de anillos, y es trivial que es suprayectivo. Finalmente sea $x \in \ker\pi$, vale decir, $xN = 1 \cdot N$, luego $x \in xN = N$; y es claro que si $x \in N$, entonces $x \in \ker\pi$. □

Proposición 1.49: Un homomorfismo de grupos $\varphi\colon G \to H$ es inyectivo syss $\ker\varphi = \{1\}$.

Demostración: Claramente se tiene que $\implies$. El recíproco viene dado de que si $\varphi(x) = \varphi(y)$, entonces

$$1 = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1})$$

luego $xy^{-1} \in \ker\varphi$, por lo que $xy^{-1} = 1$ y $x = y$. □

Ésto estrecha la relación entre núcleos y subgrupos normales. Antes de seguir veamos un par de otras definiciones:

Definición 1.50: Se le llama *centralizador* $Z(S)$ de S al conjunto de todos los elementos que conmutan con todos los elementos de S, i.e.

$$Z(S) := \{x \in G : \forall g \in S\ (xg = gx)\},$$

al centralizador de todo G, se le dice el *centro*. Llamamos *normalizador* $\mathrm{N}_G(S)$ de un conjunto S a los elementos que fijan al conjunto bajo

conjugación, i.e.,

$$\mathrm{N}_G(S) := \{x \in G : x^{-1}Sx = S\}.$$

Llamamos clase de conjugación $C_G(S)$ de S al conjunto de todos los conjugados de S.

Proposición 1.51: Se cumple:

1. $N \trianglelefteq G$ syss $\mathrm{N}_G(N) = G$ syss $C_G(N) = \{N\}$.
2. Si $S, T \subseteq G$, entonces $Z(S \cup T) = Z(S) \cap Z(T)$. En particular,
$$Z(S) = \bigcap_{g \in S} Z(g).$$
3. $H \leq G$ es abeliano syss $H \subseteq Z(H)$. En particular, G es abeliano syss $Z(G) = G$.
4. $Z(g) = N(g)$.
5. Si $S \subseteq G$ entonces $Z(S) \leq \mathrm{N}_G(S) \leq G$.
6. Si $H \leq G$ entonces $H \trianglelefteq \mathrm{N}_G(H) \leq G$. Más aún si $N \leq G$ es tal que $H \trianglelefteq N$, entonces $N \subseteq \mathrm{N}_G(H)$.
7. $N \leq Z(G)$ implica $N \trianglelefteq G$, en particular, $Z(G) \trianglelefteq G$.
8. $C_G(x) = \{x\}$ syss $x \in Z(G)$. Más generalmente $C_G(S) = \{S\}$ syss $S \subseteq Z(G)$.

Teorema 1.52: Todo subgrupo de índice dos es normal.

Demostración: Sea $N \leq G$ tal que $[G : N] = 2$. Es decir, N posee dos clases laterales: una es necesariamente N y la otra ha de ser $G \setminus N$ (dado que las clases de N forman una partición de G). Luego si $x \in N$, entonces $xN = N = Nx$; si no, entonces $xN = G \setminus N = Nx$. □

Proposición 1.53: Se cumple:

1. Para todo $S \subseteq G$ se cumple que $|C_G(S)| = [G : \mathrm{N}_G(S)]$.
2. El conjugado de la inversa es la inversa del conjugado. Más generalmente las potencias del conjugado son el conjugado de la potencia.

3. El orden se preserva bajo conjugados.

Demostración:

1. Veamos que $x \equiv y \pmod{Z(g)}$ implica $x^{-1}y \in Z(g)$, ergo
$$(x^{-1}y)g = g(x^{-1}y) \iff xgx^{-1} = ygy^{-1}.$$
Esto se traduce a decir que las clases de equivalencia determinadas por $Z(g)$ se componen de los elementos que generan el mismo conjugado. Es claro que todo conjugado puede escribirse como $x^{-1}gx$, y lo anterior prueba que se determinásemos una aplicación entre ambos conjuntos esta sería inyectiva y suprayectiva, i.e., biyectiva, luego los conjuntos son equipotentes.

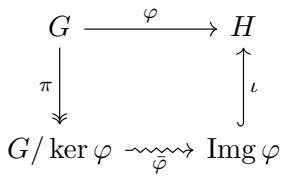
2. Sea $a \in G$ y $c \in G$ arbitrario, de forma que $b := c^{-1}ac$, luego por la propiedad anterior se cumple que $b^k = c^{-1}a^kc$, por lo que si $n := \operatorname{ord} a$, entonces $b^n = c^{-1}a^nc = c^{-1}ec = e$. Por lo que $\operatorname{ord} b \leq \operatorname{ord} a$. Pero notemos que $a = (c^{-1})^{-1}bc^{-1}$, por lo que $\operatorname{ord} a \leq \operatorname{ord} b$. En conclusión, $\operatorname{ord} a = \operatorname{ord} b$. □

Proposición 1.54: Para $n \geq 3$ se cumple que $Z(S_n) = \langle 1 \rangle$ y que $Z(D_{2n}) = \langle 1 \rangle$ si n impar, y $Z(D_{2n}) = \left\langle r^{n/2} \right\rangle$ si n par.

Demostración: El centro de los grupos diedrales queda al lector. Sea $\sigma \in S_n$ no unitario, luego existe un par $i \neq j$ tales que $\sigma(i) = j$. Como $n \geq 3$ existe un k distinto de ambos, luego $(j,k)\sigma \neq \sigma(j,k)$, pues basta considerar la imagen de i en cada caso. □

Teorema 1.55 – *Primer teorema de isomorfismos*: Sea $\varphi\colon G \to H$ un morfismo de grupos con $N := \ker\varphi \trianglelefteq G$, entonces $\bar{\varphi}\colon G/N \to \operatorname{Img}\varphi$ dado por $\bar{\varphi}(x) := \varphi(xN)$ resulta ser un isomorfismo.

En figura de diagrama conmutativo:



Corolario 1.56: Si $\varphi\colon G \to H$ es epimorfismo, entonces $G/\ker\varphi \cong H$.

Teorema 1.57 – *Segundo teorema de isomorfismos*: Sean $H \leq G$ y $K \trianglelefteq G$, entonces $H \cap K \trianglelefteq H$ y de hecho

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Demostración: Sea $\varphi : H \to HK/K$ definida por $\varphi(h) := hK$ es un epimorfismo de grupos pues $hkK \in HK/K$, pero $hkK = hK = \varphi(h)$.

Luego, busquemos el kernel de φ. Notemos que $1 \in \ker\varphi$ y $\varphi(1) = K$, asimismo, para todo $k \in K$ se cumple que $\varphi(k) = K$, luego $H \cap K \subseteq \ker\varphi$ y ya hemos visto que la otra implicancia también se da, luego por el primer teorema de isomorfismos se cumple el enunciado. □

Teorema 1.58 – *Tercer teorema de isomorfismos*: Sean $K \leq H \trianglelefteq G$ y $K \trianglelefteq G$, entonces

$$\frac{G}{H} \cong \frac{G/K}{H/K}.$$

Demostración: Al igual que con la demostración del segundo teorema, vamos a tratar de aplicar el primer teorema:

Los elementos de $(G/K)/(H/K)$ son de la forma $gK(H/K)$, luego $\varphi\colon G \to (G/K)/(H/K)$ dado por $\varphi(g) := (gK)(H/K)$ es un epimorfismo de grupos, donde el $x \in G$ pertenece al kernel syss $gK \in H/K$, i.e, $g \in H$. □

Ahora introducimos un nuevo lenguaje que permite re-escribir los teoremas de isomorfismos:

Definición 1.59 (Sucesión exacta): Dada una sucesión de morfismos:

$$\cdots \longrightarrow G_i \xrightarrow{\varphi_i} G_{i+1} \xrightarrow{\varphi_{i+1}} G_{i+2} \longrightarrow \cdots$$

Se dice que es *exacta* si $\operatorname{Img}\varphi_i = \ker\varphi_{i+1}$ para todo $i \in \mathbb{Z}$ (para el cuál estén definidos). Una sucesión exacta se dice *corta* si es finita.

Proposición 1.60: Se cumple:

1. $f\colon G \to H$ es inyectiva syss $0 \longrightarrow G \xrightarrow{f} H$ es exacta.
2. $f\colon G \to H$ es suprayectiva syss $G \xrightarrow{f} H \longrightarrow 0$ es exacta.

3. Si $H \trianglelefteq G$, entonces

$$H \overset{\iota}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} G/H$$

es una sucesión exacta corta.

4. Dados $f\colon H \to G$ y $g\colon G \to J$ morfismos de grupos, se cumple que

$$0 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} J \longrightarrow 0$$

es exacta syss existe $N \trianglelefteq G$ tal que el siguiente diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \xrightarrow{f} & G & \xrightarrow{g} & J & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \mathrm{Id} & & \downarrow & & \\ 0 & \longrightarrow & N & \xhookrightarrow{\iota} & G & \xrightarrow{\pi} & G/N & \longrightarrow & 0 \end{array}$$

conmuta.

Si bien el segundo teorema de isomorfismos no se aplica en casos más generales, la relación entre cardinales si es generalizable:

Teorema 1.61: Sean, $H, K \leq G$ finito, entonces

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Demostración: Sea $f : H \times K \to HK$ dada por $f(h,k) = hk$. Claramente f es suprayectiva. Sean $(h_1,k_1);(h_2,k_2) \in H \times K$, luego $f(h_1,k_1) = f(h_2,k_2)$ implica que $u := k_1 k_2^{-1} = h_1^{-1} h_2 \in H \cap K$. Luego es trivial probar que $hk = h'k'$ syss existe $u \in H \cap K$ tal que $h' = hu$ y $k' = u^{-1}k$. Con lo que $|f^{-1}[hk]| = |(hu, u^{-1}k) : u \in H \cap K| = |H \cap K|$.

Luego se cumple que

$$H \times K = \bigcup_{x \in HK} f^{-1}[x] \implies |H|\,|K| = |HK|\,|H \cap K|. \qquad \square$$

Proposición 1.62: Si $H_1 \trianglelefteq G_1$ y $H_2 \trianglelefteq G_2$, entonces

$$\frac{G_1 \times G_2}{H_1 \times H_2} \cong \frac{G_1}{H_1} \times \frac{G_2}{H_2}.$$

Demostración: Se comienzan por definir los siguientes epimorfismos en base al siguiente diagrama conmutativo:

$$G_1 \times G_2 \overset{\pi_1}{\twoheadrightarrow} G_1 \twoheadrightarrow \frac{G_1}{H_1}$$

y análogamente con $\pi_2 : G_1 \times G_2 \to G_2/H_2$. Luego $\pi := (\pi_1, \pi_2)$ es un epimorfismo de kernel $H_1 \times H_2$ que por el primer teorema de isomorfismos prueba el enunciado. □

Teorema 1.63 – *Teorema de la correspondencia*: Si $\varphi\colon G \twoheadrightarrow H$, entonces

$$\begin{aligned} \Phi\colon \{S : S \leq H\} &\longrightarrow \{S : \ker\varphi \leq S \leq G\} \\ S &\longmapsto \varphi^{-1}[S] \end{aligned}$$

cumple las siguientes propiedades, para S_1, S_2 subgrupos de H:

1. Φ es biyectiva.
2. $S_1 \subseteq S_2$ implica $\Phi(S_1) \subseteq \Phi(S_2)$.
3. $S_1 \trianglelefteq S_2$ implica $\Phi(S_1) \trianglelefteq \Phi(S_2)$.
4. Si $S_1 \leq S_2$, entonces $[S_2 : S_1] = [\Phi(S_2) : \Phi(S_1)]$.

Demostración:

1. (i) Φ es inyectiva: Sean $S_1 \neq S_2$ subgrupos de H. Entonces si $x \in S_2 \setminus S_1$, e y es tal que $\varphi(y) = x$, de modo que $y \in \Phi(S_2)$, e $y \notin \Phi(S_1)$ pues si $y \in \Phi(S_1) = \varphi^{-1}[S_1]$, entonces $\varphi(y) \in S_1$, lo que es absurdo.

   (ii) Φ es suprayectiva: Sea S tal que $\ker\varphi \leq S \leq G$. Luego $L := \varphi[S] \leq H$, y $\Phi(L) \supseteq S$. Más aún, si $x \in \Phi(L)$, entonces $y = \varphi(x)$ con $y \in L$, ergo existe $z \in S$ tal que $y = \varphi(z)$. Luego

   $$1 = yy^{-1} = \varphi(xz^{-1}) \implies xz^{-1} \in \ker\varphi \subseteq S.$$

   Finalmente, como S es subgrupo, se tiene que $(xz^{-1}) \cdot z = x \in S$, i.e., $\Phi(L) \subseteq S$ y se cumple la igualdad.

2. Ésto es trivial pues en general, si $A \subseteq B$, entonces $f^{-1}[A] \subseteq f^{-1}[B]$.

3. Sea $g \in \Phi(S_1)$ y $h \in \Phi(S_2)$, entonces por definición entonces $\varphi(h^{-1}gh) = \varphi(h)^{-1}\varphi(g)\varphi(h)$, pero $\varphi(h) \in S_2$ y $\varphi(g) \in S_1$, y como $S_1 \trianglelefteq S_2$, entonces $\varphi(h^{-1}gh) \in S_1$, luego $h^{-1}gh \in \Phi(S_1)$.

4. Sean $S_1 \leq S_2$, entonces tenemos $n_G := [S_2 : S_1]$ y $n_H := [\Phi(S_2) : \Phi(S_1)]$. Sea $g \in \Phi(S_2)$, luego $g \in h\Phi(S_1)$ con $h \in \Phi(S_2)$. Luego $\varphi(g) \in \varphi[h\Phi(S_1)] = \varphi(h) \cdot \varphi[\Phi(S_1)] = \varphi(h)S_1$, en conclusión, $n_H \leq n_G$. Como Φ es biyectiva, podemos usar Φ^{-1} para probar el converso. □

§1.3.2 Productos directos y semidirectos de grupos.

Teorema 1.64: Sean $H, K \leq G$, entonces:

1. $HK \leq G$ syss $HK = KH$.
2. $H \trianglelefteq G$ o $K \trianglelefteq G$ implica $HK \leq G$.
3. $H \trianglelefteq G$ y $K \trianglelefteq G$ implica $HK \trianglelefteq G$.

Demostración:

1. $\Longrightarrow$. Sea $hk \in HK$, como $H, K, HK \leq G$; entonces $h^{-1} \in H, k^{-1} \in G$ y $(h^{-1}k^{-1})^{-1} = kh \in HK$, luego $KH \subseteq HK$. Análogamente se prueba la otra implicancia y por doble contención los conjuntos son iguales.

   $\Longleftarrow$. Sean $x, y \in HK$ por ende existen $h_1, h_2 \in H$ y $k_1, k_2 \in K$ tales que $x = h_1k_1$ e $y = h_2k_2$. Luego $xy^{-1} = h_1(k_1k_2^{-1})h_2^{-1}$. Se cumple que $(k_1k_2^{-1})h_2 \in KH = HK$, por ende $(k_1k_2^{-1})h_2 = h_3k_3$, finalmente como $H \leq G$ entonces $h_1h_3 \in H$ y $xy^{-1} = h_1(k_1k_2^{-1})h_2 = h_1h_3k_3 \in HK$ que es el criterio del subgrupo.

2. Sin perdida de generalidad supongamos que $H \trianglelefteq G$, entonces $kh = khk^{-1}k = h'k$ con $h' \in H$ por ser conjugado de un elemento de H, luego $KH = HK$.

3. Por el inciso anterior se cumple que $HK \leq G$ y para todo $x \in G$ se cumple que $x^{-1}hkx = (x^{-1}hx)(x^{-1}kx)$. □

Ejemplo. Consideremos D_6, aquí $\langle s \rangle$ y $\langle rs \rangle$ son subgrupos (ambos de cardinal 2), de modo que

$$S := \langle s \rangle \cdot \langle rs \rangle = \{e, s, rs, srs = r^2\}.$$

Pero S tiene cardinal 4, luego no puede ser subgrupo pues $4 \nmid 6$ (por teorema de Lagrange).

Definición 1.65 (Conmutador): Definamos el conmutador $[x, y] := x^{-1}y^{-1}xy$, que satisface que $xy = yx[x, y]$, luego $xy = yx$ syss $[x, y] = 1$.

Teorema 1.66: Si $N, M \trianglelefteq G$ tales que $N \cap M = \{1\}$, entonces $nm = mn$ con $n \in N$ y $m \in M$.

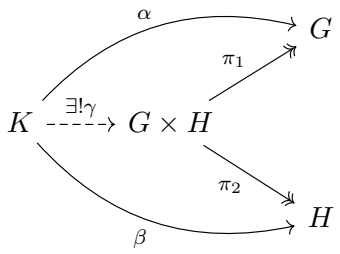
Demostración: Notemos que $[n, m] = (n^{-1}m^{-1}n)m = n^{-1}(m^{-1}nm)$, donde $n^{-1}mn \in M$ y $m^{-1}nm \in N$ por ser normales. Como $[n, m] \in N \cap M = \{1\}$, entonces $[n, m] = 1$, luego conmutan. □

Definición 1.67 – *Producto directo de grupos*: Sean $(G, \cdot), (H, *)$ grupos, entonces se define su *producto directo*, denotado $(G \times H, \star)$, al grupo con la operación tal que

$$(a, b) \star (c, d) = (a \cdot c, b * d).$$

Proposición 1.68: Sean G, H grupos, entonces:

1. $G \times H$ es también un grupo y las proyecciones $\pi_1(g, h) := g$ y $\pi_2(g, h) := h$ son homomorfismos de grupos.
2. Si K es un grupo y $\alpha\colon K \to G$ y $\beta\colon K \to H$ son homomorfismos de grupos, entonces la diagonal $\gamma := \alpha\Delta\beta\colon K \to G \times H$ es el único homomorfismo de grupos que hace que el siguiente diagrama:



conmuta.

En consecuencia, el producto directo de grupos es un producto categorial.

La particularidad de la última observación es que se repetirá varias veces en matemáticas.

Teorema 1.69: Sean $H, K \leq G$ tales que:

1. $HK = G$.
2. $H \cap K = \{1\}$.
3. $hk = kh$ para todos $h \in H, k \in K$.

Entonces $\varphi : H \times K \to G$ dado por $\varphi(h,k) := hk$ es un isomorfismo.

Proposición 1.70: El producto directo de dos grupos abelianos es abeliano.

Teorema 1.71 – *Teorema fundamental de los grupos abelianos*: Si G es abeliano finitamente generado, entonces existen primos $p_1, \ldots, p_n$ (posiblemente iguales) y naturales no nulos $\alpha_1, \ldots, \alpha_n, \beta$ tales que

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}} \times \mathbb{Z}^{\beta}.$$

En particular, se cumple para grupos abelianos finitos.

Demostración: Sea $\langle g_1, \ldots, g_k \rangle$ una base de G, de modo que se comprueba que los subgrupos $N_i := \langle g_i \rangle$ son disjuntos dos a dos, y son normales pues G es abeliano. Luego $G \cong N_1 \times N_k$, pero como N_i es cíclico, entonces $N_i \cong \mathbb{Z}$ o $N_i \cong \mathbb{Z}_m$. Podemos agrupar todos los $\mathbb{Z}$s que encontremos, y si $N_i \cong \mathbb{Z}_m$ entonces $m = q_1^{\gamma_1} \cdots q_j^{\gamma_j}$ donde los q_is son primos distintos y los γ_is son naturales no nulos, luego por teorema chino del resto:

$$\mathbb{Z}_m \cong \mathbb{Z}_{q_1^{\gamma_1}} \times \cdots \times \mathbb{Z}_{q_j^{\gamma_j}}$$

Finalmente agrupando todo nos da el enunciado. □

Corolario 1.72: Todo grupo abeliano posee subgrupos de todos los divisores de su cardinal.

Veamos dos aplicaciones de ésto:

Proposición 1.73: Todo grupo de cardinal 4 es $\mathbb{Z}_4$ o $K_4 := \mathbb{Z}_2 \times \mathbb{Z}_2$. A K_4 se conoce como el «grupo de Klein».

Demostración: Por el teorema de Lagrange para cada elemento no neutro existen dos posibilidades: Que tenga orden 2 o 4. Si alguno tiene orden 4, entonces el grupo es cíclico y es $\mathbb{Z}_4$. Si todos tienen orden 2, entonces el grupo

es abeliano (por la proposición 1.18) y por ende se escribe como producto de grupos cíclicos y luego es fácil ver que es K_4. □

Proposición 1.74: Todo grupo de cardinal 6 es $\mathbb{Z}_6$ (si es abeliano) o D_6 (si no lo es). En consecuente, $S_3 \cong D_6$.

Demostración: Nuevamente por Lagrange cada elemento puede tener orden 1, 2, 3 o 6. Si es abeliano luego es $\mathbb{Z}_2 \times \mathbb{Z}_3$ o $\mathbb{Z}_6$, pero por el teorema chino del resto $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Si no es abeliano, entonces debe poseer elementos de orden 1, 2 o 3; pero no todos deben ser de orden 2, pues sería abeliano, así que existe $y \in G$ de orden 3, de modo que $\langle y \rangle$ tiene índice 2, luego es normal y sus clases laterales son $\langle y \rangle$ y $x\langle y \rangle$ donde x tiene orden 2. Notemos que luego todo elemento de G se ve como $x^p y^q$ donde $p, q \in \mathbb{Z}$, pero como no es abeliano entonces $xy \neq yx$, ergo, $xy = y^2 x$ y $xyx = y^{-1}$. Pero entonces $\varphi\colon G \to D_6$ dado por $\varphi(x) = s$ y $\varphi(y) = r$ demuestra ser isomorfismo. □

Lema 1.75: Si N, A son grupos y $\alpha : A \to \mathrm{Aut}(N)$ es un morfismo de grupos, entonces $G := N \times A$ con la operación $\cdot$ definida por

$$(n, a) \cdot (m, b) := (n \cdot \alpha_a(m), ab)$$

es un grupo.

Demostración: Veamos que se cumplen las propiedades:

(i) **Asociatividad:** Sean $(n, a), (m, b), (p, c) \in G$, entonces

$$\begin{aligned}[(n, a)(m, b)](p, c) &= (n\alpha_a(m), ab)(p, c) = (n\alpha_a(m)\alpha_{ab}(p), abc) \\ &= (n\alpha_a(m\alpha_b(p)), a(bc)) = (n, a)(m\alpha_b(p), bc) \\ &= (n, a)[(m, b)(p, c)].\end{aligned}$$

(ii) **Neutro:** Probablemente lo es $(1, 1)$, probemoslo:

$$(n, a)(1, 1) = (n\alpha_a(1), a) = (n, a) = (1\alpha_1(n), a) = (1, 1)(n, a).$$

(iii) **Inverso:** Sea $(n, a) \in G$, y definamos $b := a^{-1}$, luego un inverso debe ser (m, b) con algún m. Notemos $(n, a)(m, b) = (n\alpha_a(m), 1) = (1, 1)$, luego $\alpha_a(m) = n^{-1}$ por lo que

$$m = \alpha_a^{-1}(n^{-1}) = \alpha_b(n^{-1}).$$

Finalmente, $(m, b)(n, a) = (m\alpha_b(n), 1) = (\alpha_b(n^{-1}n), 1) = (1, 1)$. □

Definición 1.76 – *Producto semidirecto*: Sean N, A como en el lema anterior, llamamos al grupo generado el *semiproducto* de N, A y le denotamos por $N \rtimes_\alpha A$.

Proposición 1.77: Si N, A son grupos y α es el morfismo trivial, es decir, $\alpha_a = \mathrm{Id}$ para todo $a \in A$, entonces $N \rtimes_\alpha A = N \times A$ [es decir, el producto directo es un caso particular del producto semidirecto].

Proposición 1.78: Sea $n > 2$, entonces $\alpha : \mathbb{F}_2 \to \mathbb{Z}_n$, donde $\alpha_0 = \mathrm{Id}$ y $\alpha_1(x) = -x$. Entonces $\mathbb{Z}_n \rtimes_\alpha \mathbb{F}_2 \cong D_{2n}$.

Demostración: Definamos $r := (1,0)$ y $s := (0,1)$, entonces se cumple que

$$r^2 = (1,0)(1,0) = (1 + \alpha_0(1), 0) = (2,0)$$

y así por inducción se deduce que $r^k = (k \mod n, 0)$, de modo que $\operatorname{ord} r = n$. Y $s^2 = (0,1)(0,1) = (0 + \alpha_1(0), 1 + 1) = (0,0)$, por lo que $\operatorname{ord} s = 2$. Finalmente, veamos que

$$\begin{aligned} srs &= (0,1)(1,0)(0,1) = (0 + \alpha_1(1), 1)(0,1) = (-1,1)(0,1) \\ &= (-1 + \alpha_1(0), 0) = (-1,0) = r^{-1}. \end{aligned}$$ □

En consecuencia, podemos notar que el producto semidirecto de grupos abelianos puede ser no-abeliano.

Proposición 1.79: Si $G = N \rtimes_\alpha A$, entonces

- $N_G := N \times \{1\} \trianglelefteq G$.
- $A_G := \{1\} \times A \leq G$.
- $N_G \cap A_G = \{1\}$.
- $N_G \cdot A_G = G$.
- Para todo $a \in A, n \in N$ se cumple que $(1,a)^{-1}(n,1)(1,a) =$

§1.3.3 Acciones, ecuación de clases y p-grupos.

Definición 1.80 – *Acción*: Una acción de un grupo G sobre un conjunto S no vacío arbitrario es un morfismo $\alpha\colon G \to \mathrm{Sym}(S)$. Es decir

α_g con $g \in G$ es una permutación de S, y cumplen que

$$\alpha_{xy} = \alpha_x \circ \alpha_y,$$

de ésto se deduce que $\alpha_1 = \mathrm{Id}_S$. Podemos definir que $\ker \alpha := \{g \in G : \alpha_g = \mathrm{Id}_S\}$.

Diremos que una acción es *fiel* si α es inyectiva, lo que equivale a ver que $\ker \alpha = \{1\}$.

Dada una acción α de G sobre S, entonces definimos los siguientes conjuntos:

$$\mathrm{Orb}_a := \{\alpha_g(a) : g \in G\}, \quad \mathrm{Stab}_a := \{g \in G : \alpha_g(a) = a\}$$

a los que llamamos órbita y estabilizador de a resp.

Decimos que una acción es *transitiva* si para todo $a \in S$ se cumple que $\mathrm{Orb}_a = S$.

Ejemplos. Son acciones:

- El morfismo $\alpha\colon G \to \mathrm{Sym}(S)$ para un conjunto S arbitrario con $\alpha_g = \mathrm{Id}$. Ésta acción se llama la *acción trivial*. Nótese que no es fiel y que las órbitas de cada elemento son singulares.
- El morfismo $\alpha\colon G \to \mathrm{Sym}(G)$ dado por $\alpha_g(x) = xg$, llamada la *acción producto*. Ésta es fiel y transitiva; y de hecho ésta es la que se emplea para probar el teorema de Cayley.
- El morfismo $\alpha\colon G \to \mathrm{Sym}(G)$ dado por $\alpha_g(x) = g^{-1}xg$, llamada la *acción por conjugación*. Se cumple que $\ker \alpha = Z(G)$.
- El morfismo $\alpha\colon \mathrm{Sym}(S) \to \mathrm{Sym}(S)$ dado por $\alpha_\sigma(x) = \sigma(x)$ es una acción fiel y transitiva.
- El morfismo $\alpha\colon \mathbb{F}_2 \to \mathrm{Sym}(G)$, donde G es grupo, dado por $\alpha_0(x) = x$ y $\alpha_1(x) = x^{-1}$. Nótese que α no es fiel syss todo elemento no-neutro tiene orden 2.

Definición 1.81: Si consideramos la acción por conjugación de un grupo G denotamos por $\mathrm{C}_G(x)$ y $Z(x)$ a la órbita y al estabilizador de x bajo ésta acción, los cuales se llaman conjugador y centralizador de x resp.

Lema 1.82: Dos clases de conjugación o son iguales o son disjuntas.

Demostración: Sean $x, y \in G$ y sea $z \in C_G(x) \cap C_G(y)$, luego, existen $g_1, g_2 \in G$ tales que $g_1^{-1} x g_1 = g_2^{-1} y g_2$, ergo $y = (g_1 g_2^{-1})^{-1} x (g_1 g_2^{-1})$ y por ende $C_G(y) \subseteq C_G(x)$. El caso converso es análogo y por doble inclusión se concluye que los conjuntos son iguales. □

Teorema 1.83 – *Ecuación de clases*: Para todo grupo finito G, existen $g_1, \ldots, g_k \in G \setminus Z(G)$ tales que

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : Z(g_i)].$$

Demostración: Por el lema anterior, el conjunto de clases de conjugación de un grupo determina una partición estricta de él, luego, en un caso finito, hay finitos conjuntos no vacíos, ergo elegimos representantes aleatorios de cada clase. Para toda clase de conjugación puede darse que $|C_G(x)| = 1$, o $|C_G(x)| > 1$, el primer caso equivale a pertenecer al centro, mientras que el segundo equivale a no pertenecer al centro. Luego como las clases determinan una partición estricta, basta sumar los cardinales de las clases de conjugación, y notemos que todos los elementos cuya clase es singular pertenecen al centro, ergo se cumple la fórmula del enunciado. □

Definición 1.84: Se dice que G es un p-grupo si posee de cardinal alguna potencia de p. También se dice que H es un p-subgrupo de G si $H \leq G$ y H es un p-grupo.

Corolario 1.85: Todo p-grupo posee centro no trivial.

Teorema 1.86: Si $G/Z(G)$ es cíclico entonces G es abeliano. Luego $|G/Z(G)|$ no es primo.

Demostración: Si $G/Z(G)$ es cíclico, entonces todos sus elementos son de la forma $g^n Z(G)$ con un g fijo, luego todo $x \in G$ se escribe como $g^n z$ con $z \in Z(G)$. Luego es fácil comprobar que x conmuta con todo elemento de G. □

Corolario 1.87: Se cumplen:

1. Si G tiene cardinal p^2 con p primo, entonces G es isomorfo a $\mathbb{Z}_{p^2}$ o $\mathbb{Z}_p^2$.

2. Si G tiene cardinal pq con p, q primos y tiene centro no-trivial, entonces es cíclico.

1.4 Teoremas de Sylow

§1.4.1 Acciones.

Teorema 1.88: Si G actúa sobre S, entonces:

1. $\mathrm{Stab}_a \leq G$.
2. El conjunto de órbitas de los elementos forman una partición estricta de S.
3. Para todo $a \in S$ y $g \in G$ se cumple que
$$\mathrm{Stab}_{\alpha_g(a)} = g^{-1}\mathrm{Stab}_a g$$
Ergo, los estabilizadores son conjugados.
4. Existe una biyección entre G/Stab_a y Orb_a, en particular si G es finito, entonces
$$|G| = |\mathrm{Orb}_a|\,|\mathrm{Stab}_a|$$

Demostración:

1. Ejercicio para el lector.
2. Basta ver que si dos órbitas no son disjuntos entonces son iguales, para ello si $a, b \in S$ basta probar que $\mathrm{Orb}_a \subseteq \mathrm{Orb}_b$. Sea $c \in \mathrm{Orb}_a \cap \mathrm{Orb}_b$, de forma que existen $g_1, g_2 \in G$ tales que
$$c = \alpha_{g_1}(a) = \alpha_{g_2}(b)$$
Ahora, sea $d := \alpha_g(a)$, entonces $d = \alpha_g(\alpha_{g_1}^{-1}(c)) = \alpha_{gg_1^{-1}g_2}(b)$, ergo $d \in \mathrm{Orb}_b$.
3. Ejercicio para el lector.
4. Prefijado un $a \in S$, vamos a definir $H := \mathrm{Stab}_a, K := \mathrm{Orb}_a$ y $\varphi : G/H_- \to K$ como $\varphi(gH) = \alpha_g(a)$. En primer lugar, veamos que está bien definida, si $x \equiv y \pmod{H}$, entonces existe $h \in H$ tal que $xh = y$, luego
$$\alpha_y(a) = \alpha_{xh}(a) = \alpha_x(\alpha_h(a)) = \alpha_x(a).$$
Queda al lector probar que φ es una biyección. □

Corolario 1.89: Si G actúa sobre S, donde S es finito, entonces existen $x_1, \ldots, x_n$ tales que

$$|S| = \sum_{i=1}^{n} |\mathrm{Orb}_{x_i}| = \sum_{i=1}^{n} [G : \mathrm{Stab}_{x_i}].$$

Definición 1.90 (Puntos fijos): En general, se dice que x es un punto fijo de una endo-función f si $f(x) = x$. Si G actúa sobre S, entonces se denota $\mathrm{Fix}_g(S)$ al conjunto de puntos fijos de la permutación α_g. Denotamos $\mathrm{Fix}_G(S)$ al conjunto de puntos fijos bajo cualquier permutación de la acción, es decir:

$$\mathrm{Fix}_g(S) := \{x \in S : \alpha_g(x) = x\}, \quad \mathrm{Fix}_G(S) := \bigcap_{g \in G} \mathrm{Fix}_g(S).$$

Teorema 1.91: Si G es un p-grupo que actúa sobre S finito, entonces

$$|S| \equiv |\,\mathrm{Fix}_G(S)| \pmod{p}$$

Demostración: Por la ecuación de órbitas se cumple que

$$|S| = \sum_{i=1}^{n} |\mathrm{Orb}_{x_i}|,$$

nótese que como G es un p-grupo y Stab_{x_i} un p-subgrupo, entonces $|\mathrm{Orb}_x| = |G/\mathrm{Stab}_x|$ siempre es una potencia de p (que incluye $p^0 = 1$). Si es una potencia no nula entonces $|\mathrm{Orb}_x| \equiv 0 \pmod{p}$, si $|\mathrm{Orb}_x| = 1$ entonces es un punto fijo global y $x \in \mathrm{Fix}_G(S)$. □

Corolario 1.92: Si G, un p-grupo, actúa sobre S que no es de cardinal múltiplo de p, entonces S posee al menos un punto fijo global.

§1.4.2 Teoremas de Sylow. Los teoremas de Sylow son un conjunto de cuatro teoremas[2] bastante importantes para la teoría de grupos finitos. De antemano advierto que la mayoría de demostraciones de los teoremas hace uso de las acciones de grupos, así que relea dicha sección las veces necesarias para entenderlos mejor.

Además nos referiremos a los teoremas de Sylow por números romanos, e.g., Sylow I.

[2] A veces el cuarto se considera una variación del tercero.

Teorema 1.93 – *Teorema de Cauchy*: Si p divide al cardinal de G, entonces G contiene un elemento de orden p, y por ende, un subgrupo de cardinal p.

Demostración: Si G es abeliano, entonces ya hemos probado que posee subgrupos de todos los divisores de su cardinal.

Si G no es abeliano: Supongamos por contradicción que esto no pasa, entonces sea G el grupo de cardinalidad mínima tal que contradice el enunciado. Notemos que todos sus subgrupos deben tener cardinal que no es divisible por p, de lo contrario, poseen un elemento de orden p por la minimalidad del cardinal de G. Por el teorema de Lagrange, para todo $H \leq G$ se cumple que $|G| = |H|\,|G/H|$, luego p divide a $|G/H|$ para todo subgrupo H de G. Luego por ecuación de clases, se cumple que p divide a $|G/Z(g_i)|$, luego divide al cardinal del centro, pero como asumimos que G no posee subgrupos propios cuyo cardinal sea un múltiplo de p, entonces $Z(G) = G$, luego G es abeliano, lo que es absurdo. □

Corolario 1.94: Si todos los elementos no-neutros de un grupo G tienen orden p, entonces G es un p-grupo.

Definición 1.95 – *p-subgrupo de Sylow*: Dado un grupo de cardinal n y un primo p tal que $p \mid n$ se dice que un subgrupo $H \leq G$ es un p-subgrupo de Sylow si $|H| = p^m$ con $m := \nu_p(n)$. Denotaremos $\mathrm{Syl}_p(G)$ al conjunto de p-subgrupos de Sylow de G.

Teorema 1.96 – *Primer teorema de Sylow*: Todo grupo finito G contiene un p-subgrupo de Sylow para todo p primo. Osea, $\mathrm{Syl}_p(G) \neq \varnothing$.

Demostración: Lo demostraremos por inducción fuerte sobre el cardinal de G. El cual es de la forma $p^\alpha m$ con $p \nmid m$. También asumiremos que $\alpha > 0$, pues dicho caso es trivial.

Caso 1 (p divide a $Z(G)$). Luego $Z(G)$ como es abeliano, posee un elemento de orden p que genera un subgrupo cíclico N que es normal (por ser subgrupo del centro), ergo G/N es grupo de cardinal $p^{\alpha-1}m$. Luego, por inducción G/N contiene un p-subgrupo de Sylow que denotaremos por $\bar{P}$. Luego sea $P := \{g \in G : gN \in \bar{P}\}$. Probaremos que P es un p-subgrupo de Sylow:

P es subgrupo: Es claro que $1 \in P$, luego no es vacío. Sean $u, v \in P$, luego $uv^{-1} \in P$, pues $\bar{P}$ es un subgrupo de G/N. **P es de Sylow:** Sea φ :

$P \to \bar{P}$ tal que $\varphi(g) = gN$, como φ es un epimorfismo, por el primer teorema de isomorfismos se cumple que $|P/\ker\varphi| = |\bar{P}|$ y $\ker\varphi = N \cap P = N$, luego $|P| = |N|\,|\bar{P}| = p \cdot p^{\alpha-1} = p^\alpha$.

Caso 2 (p no divide a $Z(G)$). Por la ecuación de clases se cumple que hay alguna clase de conjugación no trivial cuyo cardinal no es múltiplo de p y como son de la forma $[G : Z(g)]$ entonces hay algún $|Z(g)| = p^\alpha n$ y por inducción fuerte, contiene un p-subconjunto de Sylow que lo es de G. □

Teorema 1.97: Todo grupo no abeliano de orden $2p$ con p primo impar es isomorfo a D_{2p}.

Demostración: Por el primer teorema de Sylow G posee un 2-subconjunto y un p-subconjunto de Sylow, que son cíclicos, ergo se escriben como $\langle x\rangle$ y $\langle y\rangle$, y se cumple que

$$|\,\langle x\rangle\,\langle y\rangle\,| = \frac{\operatorname{ord}(x)\cdot\operatorname{ord}(y)}{|\,\langle x\rangle \cap \langle y\rangle\,|}$$

Como los valores son enteros, la intersección sólo puede tener cardinalidad 1, 2, p o $2p$, por contención, debe tener cardinalidad 1 o 2, y queda al lector probar que el otro caso es imposible. Luego $G = \langle x, y\rangle$ y por ende es isomorfo a D_{2p}. □

Teorema 1.98 – *Segundo teorema de Sylow*: Todos los p-subgrupos de Sylow de un grupo finito son conjugados. En consecuencia, si P, es un p-subgrupo de Sylow, entonces

$$|\operatorname{Syl}_p(G)| = [G : Z(P)].$$

Demostración: Sea Q otro p-subgrupo de Sylow, entonces consideremos la acción del producto por la derecha de Q (un p-grupo) sobre G/P (un grupo cuyo cardinal no es múltiplo de p), luego $\operatorname{Fix}_Q(G/P)$ es no vacío, es decir, existe un $g \in G$ tal que para todo $q \in Q$ se cumple que $Pgq = Pg$, o más bien, que $qg \in Pg$ para todo $q \in Q$. Luego $Q \subseteq g^{-1}Pg$ y por cardinalidad se comprueba que ambos conjuntos son iguales. □

Corolario 1.99: G posee un único p-subgrupo de Sylow syss es éste es normal.

Definición 1.100 – *Grupo simple*: Se dice que un grupo es *simple* si su único subgrupo normal impropio es el trivial.

Ejemplo. Los grupos cíclicos de orden primo son simples.

Corolario 1.101: Un grupo de cardinal mp con p primo y $p \nmid m$ no es simple.

Teorema 1.102 – *Tercer teorema de Sylow*: Si $|G| = p^k m$ con $p \nmid m$, entonces

$$n_p \equiv 1 \pmod{p} \quad \text{y} \quad n_p \mid m$$

donde $n_p := |\operatorname{Syl}_p(G)|$.

Demostración: Consideremos la acción de $P \in \operatorname{Syl}_p(G)$ (un p-grupo) sobre $\operatorname{Syl}_p(G)$ por conjugación. Luego se tiene que

$$|\operatorname{Syl}_p(G)| = n_p \equiv |\operatorname{Fix}_P(\operatorname{Syl}_p(G))| \pmod{p}$$

Probaremos ahora, por contradicción, que P es el único punto fijo de su acción. Sea $Q \in \operatorname{Syl}_p(G)$ distinto de P tal que es punto fijo. Por definición, para todo $g \in P$ se cumple que $g^{-1}Qg = Q$, luego $P \leq \operatorname{N}_G(Q) \leq G$. Luego, podemos ver que Q y P son p-subgrupos de Sylow de $\operatorname{N}_G(Q)$, y Q es normal, luego por el corolario anterior $P = Q$. En conclusión $|\operatorname{Fix}_P(\operatorname{Syl}_p(G))| = 1$.

Consideremos la acción de G sobre $\operatorname{Syl}_p(G)$ por conjugación. Luego $n_p \mid p^k m = |G|$ y n_p es coprimo a p (por el inciso anterior), por ende, por lema de Euclides, $n_p \mid m$. □

En general n_p representerá a la cantidad de p-subgrupos de Sylow de un grupo finito prefijado.

Teorema 1.103 – *Cuarto teorema de Sylow*: Se cumple que $n_p := |G/\operatorname{N}_G(P)|$ donde $P \in \operatorname{Syl}_p(G)$.

Pista: Relea el último paso en la demostración anterior. □

Lema 1.104: Si G es finito y tal que $n_p! < |G|$, entonces G no es simple.

Demostración: Supongamos que se da aquello, luego consideremos la acción $\alpha : G \to \operatorname{Sym}(\operatorname{Syl}_p(G)) \cong S_{n_p}$ dada por $\alpha_g(N) = g^{-1}Ng$. Ésta acción,

vista como homomorfismo de grupos, es claramente no trivial y además como $|G| > |S_{n_p}| = |n_p!|$, entonces no puede ser inyectiva, luego $\ker \alpha \notin \{\{1\}, G\}$ y es normal. □

Proposición 1.105: No hay grupos de cardinalidad < 60 que sean simples y no-abelianos.

Demostración: En primer lugar todo grupo de cardinalidad p, pq con p, q primos distintos es abeliano. Si su cardinalidad es p^n, entonces su centro es siempre es no trivial y es normal. Aplicando el lema anterior se descartan casi todos los números exceptuando 30 y 56, así que veamoslos de manera separada:

i) $\underline{30 = 2 \cdot 3 \cdot 5}$: Si $n_3 \neq 1 \neq n_5$, entonces $n_3 = 10$ y $n_5 = 6$. Cada 3- y 5-subgrupo de Sylow es cíclico y cada uno de ellos contiene al neutro así que hay exactamente $10 \cdot (3-1) = 20$ elementos de orden 3 y $6 \cdot (5-1) = 24$ elementos de orden 5, pero $20 + 24 > 30$, contradicción.

ii) $\underline{56 = 2^3 \cdot 7}$: Si $n_2 \neq 1 \neq n_7$, entonces $n_7 = 8$ y hay $8 \cdot 6 = 48$ elementos de orden 7. Además, dado un K 2-subgrupo de Sylow, nótese que no posee elementos de orden 7 (pues sus elementos sólo pueden tener orden $\{1, 2, 4, 8\}$) y posee 8 elementos dando 56. Pero como hay más de un 2-subgrupo de Sylow, entonces existe $g \notin K$ de orden no 7, es decir, el grupo tiene al menos 57 elementos, lo cuál es imposible. □

1.5 Otros tópicos de grupos

§1.5.1 Grupos libres y presentación. Un grupo libre viene a ser algo así como un grupo con la cantidad mínima de relaciones entre sí.

Definición 1.106: Sea G un grupo, se dice que un subconjunto $X \subseteq G$ es una *base* si toda aplicación $f\colon X \to H$ donde H es un grupo se extiende a un único homomorfismo de grupos $f^*\colon G \to H$. Un grupo se dice *libre* si posee una base.

Un subconjunto $X \subseteq G$ se dice *libre* si para toda sucesión finita $x_1, \ldots, x_n \in X$ donde $x_i \neq x_{i+1}$, y toda sucesión $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ tales que $x_1^{\alpha_1} \cdots x_n^{\alpha_n} = 1$ se cumple que $\alpha_1 = \cdots = \alpha_n = 0$.

Lo que queremos ver es que ser una base y ser un sistema generador libre son lo mismo.

Otra manera útil de escribir que G es un grupo libre de base X es mediante la siguiente fórmula:

$$\mathrm{Hom}(G, H) \approx \mathrm{Func}(X, G), \tag{1.1}$$

donde $\approx$ significa equipotencia de conjuntos.

Teorema 1.107: Para todo conjunto S existe un grupo, denotado $F(S)$, tal que S es un sistema generador libre de $F(S)$.

Demostración: Definimos $\bar{S} := S \times \{+1, -1\}$ donde $()^{-1} \colon \bar{S} \to \bar{S}$ es tal que $(x, \pm 1)^{-1} = (x, \mp 1)$. Denotamos $x := (x, +1)$ y $x^{-1} := (x, -1)$, donde $x \in S$. Una palabra (no reducida) es un elemento de la forma $w := xxyx^{-1}y^{-1}yx^{-1}$, o formalmente una tupla ordenada finita de $\bar{S}$, donde su longitud viene dada por la de tupla ordenada, denotada $|w| = 7$. El gran problema es que las palabras no reducidas pueden tener partes redundantes pues en el ejemplo anterior:

$$xxyx^{-1}\underline{y^{-1}y}x^{-1} = xxyx^{-1}x^{-1}$$

Así, definimos una reducción elemental[3] $R_e \colon \bar{S}^{<\omega} \to \bar{S}^{<\omega}$ como prosigue: Si la palabra tiene largo 0 ó largo 1, entonces no hace nada. Si la palabra w es más larga busca el primer índice i tal que $w_i^{-1} = w_{i+1}$ y elimina los elementos en dichas posiciones, si no existe tal i entonces no hace nada. Cada reducción elemental o quita dos elementos, o no hace nada; entonces la longitud mínima posible de $R_e^n(w)$ es $|w|/2n$, por lo que luego de $N_w := \lfloor |w|/2 \rfloor + 1$ iteraciones, debería fijar a w. Finalmente se define la reducción total $R \colon \bar{S}^{<\omega} \to \bar{S}^{<\omega}$ como $R(w) := R_e^{N_w}(w)$ de manera que es seguro que $R_e(R(w)) = R(w)$.

Se denota por $F(S)$ al conjunto de palabras sin reducir fijadas por R. Para ver que $F(S)$ es un grupo se denota por $\cup$ a la concatenación de palabras sin reducir, luego $w_1 \cdot w_2 := R(w_1 \cup w_2)$, por ello a los elementos de $F(S)$ los concideramos palabras irreductibles, aunque dicho adjetivo calificativo será obviado. $F(S)$ es un grupo pues claramente es asociativa, el neutro es $1 := ()$ [palabra vacía], los inversos vienen dados por revertir el orden de la palabra e invertir sus elementos (lo que sigue siendo irreductible). □

Fundamentalmente $F(S)$ es el prototipo de un grupo libre, pero aún no lo probamos.

[3]Recordar que $\bar{S}^{<\omega}$ es el conjunto de todas las tuplas ordenadas finitas (incluyendo la tupla vacía) de $\bar{S}$.

Teorema 1.108: Un subconjunto $X \subseteq G$ es una base syss es un sistema generador libre. En cuyo caso, todo elemento de G o es 1 o se escribe de forma única como $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, donde $x_i \neq x_{i+1}$ y los α's son no nulos.

Demostración: Veamos que si X es libre, su subgrupo generado satisface la segunda propiedad: Sea $g \in \langle X \rangle$, si $g = 1$ entonces no se escribe de otra forma por definición de ser libre. Si $g \neq 1$ y se tienen las dos siguientes representaciones:

$$g = x_1^{\alpha_1} \cdots x_n^{\alpha_n} = y_1^{\beta_1} \cdots y_m^{\beta_m}.$$

Luego se cumple que

$$1 = g^{-1}g = x_n^{-\alpha_n} \cdots x_1^{-\alpha_1} y_1^{\beta_1} \cdots y_m^{\beta_m},$$

por definición de ser libre ésto implica que $x_1 = y_1$ y nos queda:

$$1 = x_n^{-\alpha_n} \cdots x_2^{-\alpha_2} y_1^{\beta_1 - \alpha_1} y_2^{\beta_2} \cdots y_m^{\beta_m},$$

y también por ser libre se cumple que $\beta_1 - \alpha_1 = 0$, o lo que es equivalente, $\alpha_1 = \beta_1$; por lo que cancelamos el término y seguimos así para deducir que $x_i = y_i$ y que $\alpha_i = \beta_i$.

$\Longleftarrow$. Sea X un sistema generador libre y sea $f : X \to H$ una aplicación hacia un grupo H. Definamos:

$$f^*(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) := f(x_1)^{\alpha_1} \cdots f(x_n)^{\alpha_n}, \quad f^*(1) = 1$$

donde $x_i \neq x_{i+1}$ y $\alpha_i \in \mathbb{Z}_{\neq 0}$. Veamos que f^* posee todas las propiedades exigidas:

i) f^* está bien definida por la unicidad de la escritura de los elementos de G.

ii) f^* es un homomorfismo: Sean $g_1, g_2 \in G$. Si alguno es neutro entonces es claro que $f^*(g_1 g_2) = f^*(g_1) f^*(g_2)$. Luego poseen escritura única

$$g_1 = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, g_2 = y_1^{\beta_1} \cdots y_m^{\beta_m}.$$

Ahora demostramos que se cumple la propiedad por inducción sobre m. El caso $m = 1$ se cumple separando por el caso de si $y_1 = x_n$:

$$\begin{aligned} f^*(g_1 g_2) &= f^*(x_1^{\alpha_1} \cdots x_n^{\alpha_n} y_1^{\beta_1}) = f^*(x_1^{\alpha_1} \cdots x_n^{\alpha_n + \beta_1}) \\ &= f(x_1)^{\alpha_1} \cdots f(x_n)^{\alpha_n + \beta_1} = f(x_1)^{\alpha_1} \cdots f(x_n)^{\alpha_n} f(y_1)^{\beta_1} = f^*(g_1) f^*(g_2). \end{aligned}$$

Y si $y_1 \neq x_n$ es trivial.

Luego el caso inductivo queda al lector.

$\Longrightarrow$. Sea X una base de G que genera el subgrupo H. Luego sea $\iota\colon X \to H$ la función inclusión, con lo que se extiende a un homomorfismo $f\colon G \to H$. Pero además, como $H \leq G$ se cumple que la inclusión $g\colon H \to G$ es un homomorfismo. Así $(f \circ g)\colon G \to G$ es una extensión de la inclusión $X \to G$ que es la identidad por unicidad y que implica que g es suprayectiva (que era la inclusión), así que $H = G$.

Más aún, sea $\mathrm{Id}\colon X \to X \subseteq F(X)$ una biyección, donde $F(X)$ es un grupo donde X es libre, entonces se extiende a un único homomorfismo $f^*\colon G \to F[X]$. Si f^* no fuera un monomorfismo, entonces tendría kernel no trivial y sea $g \in G$ un elemento no neutro tal que $f^*(g) = 1$, y se cumple que

$$1 = f^*(g) = f^*(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = f(x_1)^{\alpha_1} \cdots f(x_n)^{\alpha_n}$$

luego como en $F[X]$ se cumple que X es libre, entonces $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. □

Teorema 1.109: Si G, H son grupos libres de bases X, Y resp. Entonces:

1. $|X| = |Y|$ implica $G \cong H$.
2. (AE) $G \cong H$ implica $|X| = |Y|$.

Demostración:

1. Sea $f\colon X \to Y$ biyección, luego se extiende a un homomorfismo $f^*\colon G \to H$ y lo mismo con $(f^{-1})^*\colon H \to G$. Luego $f^* \circ (f^{-1})^*\colon G \to G$ es un endomorfismo que fija a X, pero notemos que la identidad también lo es y por unicidad se cumple que $f^* \circ (f^{-1})^* = \mathrm{Id}_G$ y análogamente, lo que prueba que $(f^*)^{-1} = (f^{-1})^*$, por ende f^* es un isomorfismo.

2. Se separa por casos, sea X finito. Sea $\varphi\colon G \to H$ un isomorfismo de grupos, y sea $f \in \mathrm{Hom}(H, \mathbb{Z}_2)$, luego se cumple $\varphi \circ f \in \mathrm{Hom}(G, \mathbb{Z}_2)$ y es fácil ver que $f \mapsto \varphi \circ f$ es un isomorfismo entre los grupos $\mathrm{Hom}(H, \mathbb{Z}_2) \cong \mathrm{Hom}(G, \mathbb{Z}_2)$, ergo

   $$2^{|X|} = |\,\mathrm{Hom}(G, \mathbb{Z}_2)| = |\,\mathrm{Hom}(H, \mathbb{Z}_2)| = 2^{|Y|}$$

   lo que comprueba el caso finito.

   Si X es infinito, entonces $|G| = |F(X)| = |X|^{<\infty} = |X| = |F(Y)| = |Y|$. □

Definición 1.110: Por el teorema anterior llamamos *rango* de un grupo libre al cardinal de cualquiera de sus bases. En general si κ es un número cardinal denotamos $F(\kappa)$ al grupo libre de rango κ, que es único salvo isomorfismos.

Una aplicación de los grupos libres como tal son las demostraciones de la paradoja de Banach-Tarski (véase **[58,** §A.1.2.]).

Teorema 1.111: Todo grupo es isomorfo a un cociente de un grupo libre.

Demostración: Sea G un grupo, entonces sea $\mathrm{Id}\colon G \to G$, luego se extiende de forma única a un epimorfismo $f\colon F(G) \to G$ y por el primer teorema de isomorfismos se cumple que $F(G)/\ker f \cong G$. □

Definición 1.112: Sea $R \subseteq F(X)$, entonces R se dice un conjunto de *relaciones* sobre X. Se dice que un generador Y de un grupo G *satisface* las relaciones R si existe una aplicación $f\colon X \to Y$ cuya extensión $f^*\colon F(X) \to G$ satisface que $R \subseteq \ker f^*$.

Dado un conjunto de relaciones R sobre X, y siendo N la envoltura normal de R (el subgrupo normal mínimo que contiene a R), se denota al *grupo generado por los generadores X y las relaciones R* a

$$\langle X : R\rangle := F(X)/N.$$

Si G es un grupo que cumple que $G \cong \langle X : R\rangle$, entonces la expresión de la derecha se dice una *presentación* de G.

Ésto nos permite construir o enunciar grupos de manera sencilla, que está bien definida. A ello le sumamos el siguiente resultado para concluir que ciertos grupos generados con relaciones son de hecho las presentaciones de otros ejemplos conocidos.

Teorema 1.113 (von Dyck): Sea $G = \langle X : R\rangle$ y sea H un grupo con un generador que satisface las relaciones R, luego existe un epimorfismo $f : G \to H$.

Demostración: Sea Y el generador de H que satisfaga las relaciones R. Por definición, existe una aplicación $f\colon X \to Y$ cuya extensión $f^*\colon F(X) \to H$ con $R \subseteq \ker f^* \trianglelefteq G$. Como f^* es un epimorfismo, por el primer teorema de isomorfismos se cumple que $\bar{f}\colon F(X)/\ker f^* \to H$ sea un isomorfismo.

Luego por definición de envoltura normal se cumple que $N \trianglelefteq \ker f^*$, luego por tercer teorema de isomorfismos se tiene que el siguiente diagrama

$$\begin{array}{ccc} G = \dfrac{F(X)}{N} & \dashrightarrow\!\!\!\!\!\!\twoheadrightarrow & H \\ \Big\downarrow \pi & & \Big\uparrow \\ \dfrac{F(X)/N}{\ker f^*/N} & \rightsquigarrow & \dfrac{F(X)}{\ker f^*} \end{array}$$

conmuta, del que se deriva el epimorfismo deseado. □

§1.5.2 Grupos resolubles.

Definición 1.114 (Series de grupos): Dado un grupo G se le dice *serie normal* de subgrupos a una cadena de inclusiones estrictas

$$G =: G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}.$$

En una serie se le llama *factores* a los términos G_i/G_{i+1}. Una serie es estricta si $G_i \neq G_j$ para todo $i \neq j$. Una serie se dice abeliana (resp. cíclica) si todos los factores lo son.

Una serie se dice *de composición* si es estricta y los factores son simples (lo que equivale a ver que G_i es un subgrupo normal maximal en G_{i+1}).

Proposición 1.115: Se cumplen:

1. Todo grupo finito posee una serie de composición.
2. Toda serie normal estricta puede extenderse a una serie de composición.

Demostración: Para ello basta probar la primera propiedad. Supongamos que fuera falsa, entonces sea G un grupo que no posee serie de composición de cardinalidad mínima. Luego G no puede ser simple, así que posee una subgrupo normal N. N posee una serie de composición

$$N \rhd N_1 \rhd \cdots N_k = \{1\}$$

y si G/N no es simple, entonces también posee una serie de composición que, por el teorema de la correspondencia, se traduce en una serie $G \rhd G_1 \rhd \cdots \rhd G_m = N$ cuyos factores son simples, ergo, pegando las dos series se obtiene una serie de composición para G.

□

Definición 1.116: Llamaremos *subgrupo derivado* G' al conjunto de todos los conmutadores de G.

Proposición 1.117: Se cumplen:

1. $G' \trianglelefteq G$ y G/G' es abeliano.
2. Si $N \trianglelefteq G$, entonces G/N es abeliano syss $G' \leq N$.

Demostración: Probaremos la 2: $\Longrightarrow$. Por definición $xy \equiv yx \pmod{N}$ para todo $x, y \in G$. De modo que $[x, y] = (yx)^{-1}xy \in N$ lo que prueba que $G' \leq N$.
$\Longleftarrow$. Si $G' \leq N$, entonces, por el tercer teorema de los isomorfismos, se cumple que

$$\frac{G}{N} \cong \frac{G/G'}{N/G'}$$

que es abeliano pues el lado derecho es el cociente de un grupo abeliano. □

Lema 1.118: Si G es finito, entonces son equivalentes:

1. Todas las series de composición de G son abelianas.
2. G posee una serie cíclica.
3. G posee una serie abeliana.
4. Existe un n tal que el n-ésimo derivado de G es trivial.

Demostración: Es claro que (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3).
(3) $\Longrightarrow$ (1). Por el corolario, si G posee una serie abeliana

$$G \rhd G_1 \rhd \cdots \rhd \{1\}$$

tal que G_i/G_{i+1} no es simple, entonces sea $\{1\} \neq N/G_{i+1} \lhd G_i/G_{i+1}$, luego insertar $G_i \rhd N \rhd G_{i+1}$ extiende a la serie y

$$\frac{N}{G_{i+1}} \leq \frac{G_i}{G_{i+1}}, \qquad \frac{G_i}{N} \cong \frac{G_i/G_{i+1}}{N/G_{i+1}}$$

por lo que los factores siguen siendo abelianos. Iterando el proceso se llega a una serie de composición abeliana.
(4) $\Longrightarrow$ (3). Entonces se cumpliría que

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

con $G_{i+1} := G_i'$ es una serie normal cuyos factores son abelianos.

(3) $\implies$ (4). Si G posee la serie de composición

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{e\}$$

abeliana, entonces $G' \leq H_1$ y luego $G'' \leq H_1' \leq H_2$, y más generalmente, $G^{(k)} \leq H_k$, de modo que $G^{(n)} = \{e\}$. □

Definición 1.119 – *Grupo resoluble*: Un grupo es resoluble si cumple las condiciones del lema anterior.

Corolario 1.120: Un grupo simple y no-abeliano es no resoluble.

Teorema 1.121: Se cumple:

1. Si G es resoluble y $H \leq G$, entonces H es resoluble.
2. Si G es resoluble y $N \trianglelefteq G$, entonces G/N es resoluble.
3. Si $N \trianglelefteq G$ es tal que N y G/N son resolubles, entonces G también lo es.
4. Si $H, K \leq G$ son resolubles y $H \trianglelefteq G$, entonces HK es resoluble.

Demostración:

1. Sea $G \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$ una serie abeliana, veremos que

$$G \cap H = H \trianglerighteq G_1 \cap H \trianglerighteq \cdots \trianglerighteq \{1\}$$

es una serie abeliana. Nótese que

$$\frac{G_i \cap H}{G_{i+1} \cap H} = \frac{G_i \cap H}{G_{i+1} \cap (G_i \cap H)} \cong \frac{G_{i+1}(G_i \cap H)}{G_{i+1}} \leq \frac{G_i}{G_{i+1}},$$

donde el último es abeliano, y la equivalencia viene dada por el segundo teorema de isomorfismos.

2. Sea $G \rhd G_1 \rhd \cdots \rhd G_n := \{1\}$ una serie abeliana. Luego

$$GN/N \trianglerighteq G_1N/N \trianglerighteq \cdots \trianglerighteq G_nN/N := \{e\}$$

es una serie abeliana pues

$$\frac{G_iN/N}{G_{i+1}N/N} \cong \frac{G_iN}{G_{i+1}N} \cong \frac{G_i(G_{i+1}N)}{G_{i+1}N}$$
$$\cong \frac{G_i}{G_i \cap G_{i+1}N} \cong \frac{G_i/G_{i+1}}{(G_i \cap G_{i+1}N)/G_{i+1}}$$

donde el último es un cociente de un grupo abeliano, por ende es abeliano.

3. Si N es resoluble, entonces posee una serie de composición abeliana

$$N \rhd N_1 \rhd \cdots \rhd N_n = \{e\}$$

y lo mismo aplica para G/N, pero por el teorema de correspondencia, una cadena decreciente de subgrupos normales en G/N se traduce en una cadena en G terminando en N. Luego se construye una serie de composición abeliana en G uniendo la serie de G/N con la de N.

4. Nótese que $HK \trianglerighteq H$, donde H es resoluble y $HK/H \cong K/(H \cap K)$ es resoluble por ser cociente de K que es resoluble. □

Definición 1.122: Dos series de composición para un grupo G:

$$G \rhd G_1 \rhd \cdots \rhd G_p = \{1\}, \quad G \rhd H_1 \rhd \cdots \rhd H_q = \{1\}$$

se dicen *equivalentes* si $p = q$ y los factores son isomorfos tras una permutación.

Queremos probar que todas las series de composición de un grupo (si las tiene) son equivalentes. Si se restringe al caso de grupos finitos, entonces la demostración es más sencilla, pero veremos aquí una demostración más general que luego se adaptará con toda naturalidad a otros contextos.

Lema 1.123 (de Zassenhaus o de *la mariposa*): Sean $A \trianglelefteq A^*$ y $B \trianglelefteq B^*$ tales que A^*, B^* son subgrupos de G. Entonces:

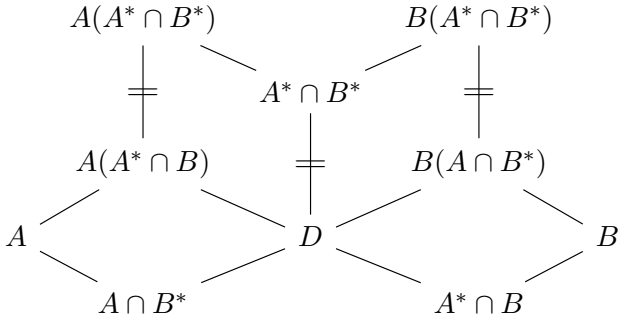
1. $A(A^* \cap B) \trianglelefteq A(A^* \cap B^*)$.
2. $B(B^* \cap A) \trianglelefteq B(B^* \cap A^*)$.
3. $\dfrac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \dfrac{B(B^* \cap A^*)}{B(B^* \cap A)}$.

Demostración: En primer lugar, veamos que $A \cap B^* \trianglelefteq A^* \cap B^*$: Sea $c \in A \cap B^*$ y $x \in A^* \cap B^*$, entonces $x^{-1}cx \in A$ puesto que $c \in A$, $x \in A^*$ y $A \trianglelefteq A^*$. Como $c, x \in B^*$, entonces claramente $x^{-1}cx \in B^*$, así que $x^{-1}cx \in A \cap B^*$. Análogamente se tiene que $A^* \cap B \trianglelefteq A^* \cap B^*$. Luego definiendo $D := (A^* \cap B)(A \cap B^*)$ se cumple que $D \trianglelefteq A^* \cap B^*$ por ser el producto de subgrupos normales.

Formalmente probaremos que:

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{A^* \cap B^*}{D}$$

de lo que sigue el resultado principal por el siguiente diagrama de retículos:[4]



Para ello basta aplicar el segundo teorema de isomorfismos con $H := A^* \cap B^*$ y $K := A(A^* \cap B)$. □

Definición 1.124: Dada una serie normal $G \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$, se le llama un *refinamiento* a otra serie normal $G \rhd G'_1 \rhd \cdots \rhd G'_m = \{1\}$ tal que la primera es un subconjunto de la segunda.

Teorema 1.125 (de refinamiento de Schreier): Dos series normales de un mismo grupo poseen al menos un refinamiento equivalente.

Demostración: Sean

$$G \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_p = \{1\}, \quad H \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_q = \{1\}$$

dos series normales de G. Para todo $0 \leq i \leq p$ y todo $0 \leq j \leq q$ definamos:

$$G_{ij} := G_{i+1}(G_i \cap H_j), \qquad H_{ji} := H_{j+1}(G_i \cap H_j).$$

[4]Éste diagrama fue introducido por Lang en [**7**] y fue la razón de que él le nombrara el «lema de la mariposa».

Luego se cumple que G_{ij} es un refinamiento de G puesto que:

$$\cdots \trianglerighteq G_i = G_{i0} \trianglerighteq G_{i1} \trianglerighteq \cdots \trianglerighteq G_{iq} = G_{i+1} = G_{i+1,0} \trianglerighteq \cdots$$

Ahora bien, aplicando el lema de Zassenhaus para $G_{i+1} \trianglelefteq G_i$ y $H_{j+1} \trianglelefteq H_j$ se obtiene que

$$\frac{G_{i,j}}{G_{i,j+1}} = \frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \cong \frac{H_{j+1}(H_j \cap G_i)}{H_{j+1}(H_j \cap G_{i+1})} = \frac{H_{j,i}}{H_{j,i+1}}.$$

De lo que se concluye que ambos refinamientos son equivalentes. □

Teorema 1.126 – *Teorema de Jordan-Hölder.* Todas las series de composición de un grupo (si existen) son equivalentes.

Una característica es que veremos que los grupos alternantes son simples, pero para demostrarlo bastan varios lemas:

Lema 1.127: Si $n \geq 3$, entonces A_n está generado por los ciclos de longitud 3.

Demostración: Por definición todo elemento de A_n es una permutación par, que podemos separar en productos de dos trasposiciones. Luego o $(a,b)(a,c) = (a,b,c)$ o $(a,b)(c,d) = (a,b,c)(c,a,d)$. □

Lema 1.128: Si $n \geq 5$, y $N \trianglelefteq A_n$ contiene un ciclo de longitud 3, entonces $N = A_n$.

Demostración: Sea τ un ciclo de longitud 3 en N, luego existe $\sigma \in S_n$ tal que

$$\sigma^{-1}\tau\sigma = (1,2,3).$$

Si $\sigma \in A_n$, entonces $(1,2,3) \in N$, de lo contrario $\sigma' := \sigma(4,5) \in A_n$ y

$$\sigma'^{-1}\tau\sigma' = (4,5)\sigma^{-1}\tau\sigma(4,5) = (4,5)(1,2,3)(4,5) = (1,2,3).$$

Luego es fácil deducir que todos los otros ciclos de longitud 3 están en N, luego $N = A_n$. □

Teorema 1.129: Si $n \geq 5$, entonces A_n es simple.

Demostración:

i) A_5 es simple: Si $\{1\} \neq N \trianglelefteq A_5$, entonces un elemento no neutro de N es de la forma (a,b,c), $(a,b)(c,d)$ o (a,b,c,d,e).
En el primer caso el lema prueba que $N = A_5$.
Si $(a,b)(c,d) \in N$, entonces con $\sigma := (a,b,e)$ se cumple

$$\sigma^{-1}(a,b)(c,d)\sigma = (b,e)(c,d) \in N,$$

luego $(a,b)(c,d)\cdot(b,e)(c,d) = (b,a,e) \in N$ y $N = A_5$.
Si $(a,b,c,d,e) \in N$, entonces con $\sigma := (a,b)(d,e)$ se cumple

$$\sigma^{-1}(a,b,c,d,e)\sigma = (a,c,e,d,b) \in N,$$

luego $(a,b,c,d,e)(a,c,e,d,b) = (b,e,c) \in N$ y $N = A_5$.

ii) A_n es simple con $n > 5$: Será por inducción sobre n, donde el caso base está probado. En primer lugar identificaremos A_n con el subgrupo de A_{n+1} de las permutaciones que tienen al $n+1$ como punto fijo. De este modo si $N \trianglelefteq A_{n+1}$, entonces $N \cap A_n \trianglelefteq A_n$. Si $N \cap A_n = A_n$, entonces N contiene a un ciclo de longitud 3 y $N = A_{n+1}$. Si $N \cap A_n = \{1\}$, entonces si $\sigma \in N_{\neq 1}$ entonces $\sigma(n+1) =: p \neq n+1$. Como σ no puede ser una trasposición (pues sería impar), y tampoco puede ser un 3-ciclo, entonces existen q, r; distintos entre sí y distintos de $p, n+1$; tales que $\sigma(q) = r$. Sean u, v distintos entre sí y distintos de $p, q, r, n+1$. Luego si $\tau := (p, n+1)(q, r, u, v)$ entonces $\eta := \tau^{-1}\sigma\tau$. Nótese que $\eta(p) = n+1$, de modo que $\sigma\eta \in N \cap A_n$, pero $\eta(r) = u$, luego $(\sigma\eta)(q) = u$ con lo que $\sigma\eta \neq 1$, por lo que $N = \{1\}$, completando la minimalidad de A_{n+1}. □

Corolario 1.130: Si $n \geq 5$, entonces A_n no resoluble y, en consecuencia, S_n tampoco lo es.

Queda de ejercicio probar que S_1, S_2, S_3 y S_4 sí son resolubles.

Proposición 1.131: A_5 es el primer (en cardinalidad) grupo simple no abeliano y grupo no soluble.

Demostración: Ya vimos que A_5 es simple, y ver que todo grupo de cardinalidad menor no puede ser simple y no-abeliano quedo demostrado al final de la sección de teoremas de Sylow.

Sea G un grupo no soluble de cardinalidad mínima, entonces sería no abeliano, pero no simple (pues A_5 es el primero), luego posee un subgrupo normal N y N es soluble por tener menos elementos que G y lo mismo sucede con G/N, luego G es soluble. □

2

Anillos y cuerpos

La teoría de anillos y cuerpos es bastante importante para el álgebra, en ciertos aspectos comparte similitudes con la teoría de grupos, sin embargo, a diferencia de ésta, la gran mayoría de la literatura no concuerda sobre temas como las definiciones básicas en la teoría de anillos. Ésto se debe a una inconclusa batalla entre aplicaciones y similitudes, algunas definiciones permiten mayor fuerza entre los resultados obtenidos, mientras que las otras hacen ligeros sacrificios para conservar una clara simetría entre los anillos y los grupos; en éste texto se opta por la segunda.

Una de las cosas que más difieren es en si considerar la inclusión de la unidad en un anillo como fundamental. Libros como [**1**] definen anillo con neutro multiplicativo y «anllo» (en inglés, *rng*), sin i, a dichas estructuras sin inversos. Ésta no es práctica de éste libro, pero se le señala al lector tenerla en cuenta.

2.1 Definiciones elementales

Definición 2.1 – *Anillo, cuerpo, dominio*: Se dice que una terna $(A, +, \cdot)$ es un anillo si $(A, +)$ es un grupo abeliano (cuyo neutro denotaremos «0», y donde el inverso de a le denotaremos $-a$), $(A_{\neq 0}, \cdot)$ un semigrupo (cuyo posible neutro se denota «1», y donde el inverso de a

se denota a^{-1}) y para todo x, y, z se cumple que

$$x(y+z) = xy + xz.$$

(distributividad de $\cdot$ respecto de $+$).

Si $(A_{\neq 0}, \cdot)$ posee neutro o es conmutativo le diremos anillo unitario o conmutativo resp. Si $x \in A$ posee inverso respecto de $\cdot$, entonces diremos que es ***invertible*** o que es una *unidad*. Denotaremos por $A^\times$ al conjunto de elementos invertibles de un anillo unitario A. Si A es un anillo unitario, y además $A^\times = A_{\neq 0}$, entonces diremos que es un anillo de división.

Si A es un anillo unitario conmutativo, entonces diremos que es un ***dominio***; y si es de división conmutativo, entonces diremos que es un ***cuerpo***.

Si $x, y \in A$ son no nulos y $xy = 0$ entonces diremos que x, y son ***divisores de cero*** y, en particular, x es un divisor izquierdo e y es un divisor derecho. A se dice un ***dominio íntegro*** si es un dominio sin divisores de cero.

Cabe destacar que como se exige que $(A_{\neq 0}, \cdot)$ sea un semigrupo y dijimos que el conjunto vacío no cuenta como estructura algebraica estamos exigiendo a que todo anillo tenga al menos dos elementos y que en todo cuerpo $1 \neq 0$. Ejemplos de cuerpos lo son $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{Z}_p, +, \cdot)$. Nótese que $(\mathbb{Z}_n, +, \cdot)$ es anillo, pero no siempre cuerpo, pues si n posee divisores propios p, q entonces p, q son divisores de cero.

Teorema 2.2: En todo anillo se cumple:

1. $a0 = 0a = 0$ (aniquilador o absorbente).
2. $a(-b) = (-a)b = -ab$ (ley de signos).
3. $(-a)(-b) = ab$.
4. $-(a+b) = -a + (-b)$

Teorema 2.3: Si A es un anillo unitario, entonces:

1. $(A^\times, \cdot)$ es un grupo.
2. Los divisores de cero (si los posee) no son invertibles.

Corolario 2.4: Todo cuerpo es un dominio íntegro.

Ejemplo. $\mathbb{Z}$ es un dominio íntegro que no es cuerpo.

De ahora en adelante se supondrá que $\Bbbk$ representa un cuerpo con operaciones $+, \cdot$, neutro aditivo 0 y multiplicativo 1.

Proposición 2.5: Si A es un anillo y $a \in A_{\neq 0}$, entonces a no es divisor de cero izquierdo (resp. derecho) syss para todo $b, c \in A$ se cumple que $ab = ac$ (resp. $ba = ca$) implica $b = c$.

Definición 2.6: Se dice que una cuádrupla $(A, +, \cdot, \leq)$ es un ***anillo ordenado*** si $(A, +, \cdot)$ es un anillo linealmente ordenado por $\leq$ tal que

- $a \leq b \implies a + c \leq b + d$.
- $a, c \geq 0 \implies ac \geq 0$.

Se les dice ***positivos*** (resp. ***negativos***) a los elementos mayores (resp. menores) o iguales al 0. Denotaremos $A_{\geq 0}$ a los elementos de A positivos para ser consistentes con nuestra notación. Algunos libros denotan A^+, A^- al conjunto de elementos positivos y negativos resp. Se le añade el prefijo *estrictamente* si son distintos del cero.

Teorema 2.7: Sea A un anillo ordenado, entonces se cumple:

1. $a \leq b$ syss $b - a \geq 0$.
2. $a \leq b$ y $c \leq d$ implica $a + c \leq b + d$.
3. $a < b$ y $c \leq d$ implica $a + c < b + d$.
4. $a \leq b$ syss $-b \leq -a$.
5. $a \geq 0$ syss $-a \leq 0$.
6. $a \leq b$ y $c \geq 0$ implica $ac \leq bc$.
7. $a \leq b$ y $c \leq 0$ implica $bc \leq ac$.
8. $a^2 \geq 0$.
9. $1 > 0$.

Definición 2.8 – *Subanillo, ideal*: Se dice que $\varnothing \neq B \subseteq A$ es un ***subanillo*** de A, denotado $B \leq A$, si B es cerrado bajo las operaciones de A y sus elementos poseen inverso aditivo.

Se dice que un subanillo $\mathfrak{a}$ de A es un ***ideal***, denotado $\mathfrak{a} \trianglelefteq A$, si para todo $x \in \mathfrak{a}$ y todo $a \in A$, se cumple que $ax, xa \in \mathfrak{a}$ (también denotado como que $A\mathfrak{a}, \mathfrak{a}A \subseteq \mathfrak{a}$). En general denotamos los ideales con caracteres góticos.

Para todo anillo A se cumple que $\{0\} \leq A$, a él le diremos subanillo trivial; cabe notar que todo subanillo no trivial de A es un anillo. Además $\{0\}, A \trianglelefteq A$, a éstos le decimos ***ideales impropios***.

Proposición 2.9: Si $1 \in B \leq A$ (como anillo), entonces $B^\times \leq A^\times$ (como grupos).

Proposición 2.10 (Criterio del subanillo): $B \subseteq A$ es un subanillo syss para todo $x, y \in B$ se cumple:

- $x - y \in B$.
- $xy \in B$.

Lema 2.11: La intersección arbitraria de subanillos (resp. ideales) es un subanillo (resp. ideal).

Definición 2.12: Luego, dado un conjunto $S \subseteq A$ se denota:

$$\langle S \rangle := \bigcap \{B : S \subseteq B \leq A\}, \quad (S) := \bigcap \{\mathfrak{a} : S \subseteq \mathfrak{a} \trianglelefteq A\}.$$

A los ideales de la forma (x) se les dice ***principales***. Es fácil ver que $(0) = \{0\}$, y si A es unitario entonces $(1) = A$. Le llamamos ***dominio de ideales principales*** (abreviado DIP) a un dominio cuyos ideales sean todos principales.

Ejemplo. $\mathbb{Z}$ es un DIP.

Proposición 2.13: Si $\mathcal{F}$ es una familia no vacía de subanillos (resp. ideales) linealmente ordenado por inclusión, entonces $S := \bigcup \mathcal{F}$ es un subanillo (resp. ideal).

Demostración: Sean $x, y \in S$, luego $x \in S_x \in \mathcal{F}$ e $y \in S_x \in \mathcal{F}$, luego $S_x \subseteq S_y$ o $S_y \subseteq S_x$, en particular $S_z := S_x \cup S_y \in \mathcal{F}$ y contiene a ambos x, y. Como S_z es un subanillo, entonces $x - y \in S_z \subseteq S$ y $xy \in S_z \subseteq S$, luego S es subanillo por el criterio.

En el caso de ideales, también es trivial ver que si $x \in S_x \subseteq S$, entonces $\lambda x, x\lambda \in S_x \subseteq S$, de modo que S es también ideal. □

Proposición 2.14: Si $\varnothing \neq S \subseteq A$ conmutativo, entonces

$$(S) = \left\{ \sum_{i=1}^{n} \lambda_i s_i : \forall i \ (s_i \in S, \lambda_i \in A) \right\}.$$

En general, si tenemos un conjunto finito $(x_i)_{i=1}^n$ y unos valores arbitrarios $\lambda_i \in A$ a los que llamamos *ponderaciones*, entonces a los elementos de la forma

$$\sum_{i=1}^{n} \lambda_i x_i = \lambda_1 x_1 + \cdots + \lambda_n x_n,$$

les decimos *combinaciones lineales* de los x_i. Éstos van a ser, sobretodo, importantes en el álgebra lineal, ésto también forja un paralelo entre éste y aquél capítulo.

La proposición anterior dice que el ideal generado por un subconjunto S no vacío de un anillo es el conjunto de todas las posibles combinaciones lineales de elementos de S.

Proposición 2.15: Todo ideal $\mathfrak{a}$ de un anillo unitario A es propio syss no contiene elementos invertibles.

Corolario 2.16: Un dominio A es un cuerpo syss no posee ideales propios, es decir, si sus únicos ideales son (0) y A. En particular, todo cuerpo es un DIP.

Definición 2.17 – *Morfismos*: Una aplicación $\varphi\colon A \to B$ entre anillos se dice un ***homomorfismo (de anillos)*** si para todo $a, b \in A$ se cumple:

1. $f(a+b) = f(a) + f(b)$.
2. $f(ab) = f(a)f(b)$.

3. $f(1) = f(1)$ si A, B son unitarios.

Definimos el kernel de un morfismo de anillos como $\ker\varphi := \varphi^{-1}[\{0\}]$.

Proposición 2.18: Sean A, B, C anillos. Entonces:

1. $\mathrm{Id}\colon A \to A$ es un homomorfismo de anillos.
2. Si $f\colon A \to B$ y $g\colon B \to C$ son homomorfismos, entonces $f \circ g\colon A \to B$ también lo es.

En consecuencia, los anillos y los homomorfismos de anillos constituyen una categoría denotada Rng.

Proposición 2.19: Si $\varphi\colon A \to B$ es un homomorfismo de anillos. Entonces:

1. $\varphi(0_A) = 0_B$.
2. Si φ es suprayectiva y A es unitario, entonces B también y $\varphi(1_A) = 1_B$.
3. Se cumple que $\mathrm{Img}\,\varphi \leq B$ y $\ker\varphi \trianglelefteq A$.
4. Si A es un cuerpo, entonces φ es o inyectiva o es nula. Si B es unitario, entonces φ siempre es inyectiva.
5. $\varphi[A^\times] \subseteq B^\times$.

De esta forma se cumple una especial reciprocidad entre la teoría de grupos y la de anillos. Los subgrupos son como los subanillos, y los subgrupos normales son como los ideales.

Lema 2.20: Dado $\mathfrak{a} \trianglelefteq A$ propio, se cumple que $a \equiv b \pmod{\mathfrak{a}}$ dado por $(b-a) \in \mathfrak{a}$ es una relación de equivalencia. Esta relación cumple que si $a \equiv c$ y $b \equiv d \pmod{\mathfrak{a}}$, entonces $a + b \equiv c + d$ y $ab \equiv cd \pmod{\mathfrak{a}}$.

Teorema 2.21: Dado $\mathfrak{a} \trianglelefteq A$ propio, entonces $(A/\mathfrak{a}, +, \cdot)$ es también un anillo.

Lema 2.22: Si $\mathfrak{a} \trianglelefteq A$ y $\mathfrak{b} \trianglelefteq A$, entonces $\mathfrak{a} + \mathfrak{b} \trianglelefteq A$.

Teorema 2.23 – *Teoremas de isomorfismos*: Sean A, B anillos y $\varphi : A \to B$ un morfismo, luego:

I $A/\ker\varphi \cong \operatorname{Img}\varphi$.

II Si $\mathfrak{a} \trianglelefteq A$ y $\mathfrak{b} \trianglelefteq A$, entonces

$$\frac{\mathfrak{a}+\mathfrak{b}}{\mathfrak{a}} \cong \frac{\mathfrak{a}}{\mathfrak{a}\cap\mathfrak{b}}.$$

III Si $\mathfrak{b} \trianglelefteq \mathfrak{a} \trianglelefteq A$ y $\mathfrak{b} \trianglelefteq A$, entonces

$$\frac{A}{\mathfrak{b}} \cong \frac{A/\mathfrak{b}}{\mathfrak{a}/\mathfrak{b}}.$$

IV (de la correspondencia) Si $\mathfrak{a} \trianglelefteq A$, entonces el morfismo $\pi : A \to A/\mathfrak{a}$ induce una biyección

$$\begin{aligned}\Phi\colon \{\mathfrak{b} : \mathfrak{a} \subseteq \mathfrak{b} \trianglelefteq A\} &\longrightarrow \{\mathfrak{b} : \mathfrak{b} \trianglelefteq A/\mathfrak{a}\}\\ \mathfrak{b} &\longmapsto \pi[\mathfrak{b}] = \mathfrak{b}/\mathfrak{a}\end{aligned}$$

tal que $\mathfrak{b}, \mathfrak{c} \trianglelefteq A$ con $\mathfrak{b} \subseteq \mathfrak{c}$ syss $\Phi(\mathfrak{b}) \subseteq \Phi(\mathfrak{c})$.

Corolario 2.24: Si $\varphi : A \to B$ es morfismo, entonces:

1. φ inyectiva syss $\ker\varphi = \{0\}$.
2. φ suprayectiva syss $A/\ker\varphi \cong B$.

Definición 2.25 – *Dominio euclídeo*: Sea A un dominio íntegro ordenado es un ***dominio euclídeo*** syss existe una función $d : A_{\neq 0} \to \mathbb{N}$, llamada ***norma euclídea***, si cumple los siguientes axiomas:

1. Si $a, b \in A_{\neq 0}$ entonces $d(a) \leq d(ab)$.
2. Si $a, b \in A_{\neq 0}$ existen $q, r \in A$ tales que $b = aq + r$, con $d(r) < d(a)$ o $r = 0$.

Obsérvese que $\mathbb{Z}$ es un dominio euclídeo, donde la norma euclídea es evidentemente el valor absoluto.

Teorema 2.26: Todo dominio euclídeo es un DIP.

Demostración: Sea A un dominio euclídeo de norma d. Sea I un ideal no-trivial de A y $a \in I$ el elemento tal que $d(a) = \min(d[I])$.

Si $b \in I$, existen $q, r \in A$ tales que $b = aq + r$, con $d(r) < d(a)$ o $r = 0$ por definición de norma euclídea. Como I es ideal, $aq \in I$, por ende, $r = b - aq \in I$. Como a es el mínimo de d en I, nos queda que $r = 0$; es decir, $b = aq \in I$, luego $I = (a)$. □

Teorema 2.27: Sea A un dominio íntegro, entonces son equivalentes:

(1) Todo ideal de A está finitamente generado.

(2) Para toda cadena ascendente de ideales de A

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

existe n tal que para todo $m \geq n$ se da $\mathfrak{a}_n = \mathfrak{a}_m$.

(3) Toda familia no-vacía de ideales de A admite un $\subseteq$-maximal.[1]

Demostración: (1) $\implies$ (2). Sea $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ una cadena ascendente de ideales de A, entonces, $\mathfrak{b} := \bigcup_{i=0}^{\infty} \mathfrak{a}_i$ (la unión de los ideales) es también un ideal. Por (1), $\mathfrak{b}$ posee un generador finito X. Luego, todo elemento de X pertenece a algún $\mathfrak{a}_i$, por ende, eventualmente se cumple que $X \subseteq \mathfrak{a}_n$, no obstante, $\mathfrak{b} = (X) \subseteq \mathfrak{a}_n$, por lo tanto se cumple el enunciado de (2) como se quería.

(2) $\implies$ (3). Veamos que dicho $\mathfrak{a}_n$ en la cadena de la prop. (2) corresponde al elemento máximo (en particular, el maximal) de dicha cadena, por ende, ambas expresiones son equivalentes.

(3) $\implies$ (1). Si el ideal $\mathfrak{a}$ de A no fuese finitamente generado, podríamos considerar $a_0 \in \mathfrak{b}$ y ver que $(a_0) \subset \mathfrak{b}$, luego, podríamos extraer $a_1 \in \mathfrak{b} \setminus (a_0)$ tal que $(a_0, a_1) \subset \mathfrak{b}$ y así sucesivamente para obtener una cadena infinita sin un elemento maximal. □

Definición 2.28 – *Anillo noetheriano*: Un dominio íntegro es un ***anillo noetheriano*** si cumple con las condiciones del teorema 2.27.

Corolario 2.29: Todo DIP es noetherinao.

[1] Véase [**56,** Def. 2.3]

§2.1.1 Teorema del binomio.

Definición 2.30: Dado n natural se define por recursividad:

$$0! := 1, \quad (n+1)! = (n+1) \cdot n!$$

A ésta función se le dice *factorial* de n.

Dados n, m naturales con $n \geq m$ se denota por $\binom{n}{m}$ (léase "n elige m") a

$$\binom{n}{m} := \frac{n!}{m!(n-m)!}.$$

Proposición 2.31: Se cumple:

1. $$\binom{n}{m} = \binom{n}{n-m}.$$

2. $$\binom{n}{0} = \binom{n}{n} = 1, \qquad \binom{n}{1} = n.$$

3. Si $m < n$, entonces

$$\binom{n}{m} + \binom{n}{m+1} = \binom{n+1}{m+1}$$

(regla de Pascal).

4. $\binom{n}{m}$ siempre es un número natural.

Demostración:

3.

$$\begin{aligned}
\binom{n}{m} + \binom{n}{m+1} &= \frac{n!}{m!(n-m)!} + \frac{n!}{(m+1)!(n-m-1)!} \\
&= \frac{n!}{m!(n-m)(n-m-1)!} + \frac{n!}{(m+1)m!(n-m-1)!} \\
&= \frac{(m+1)n! + (n-m)n!}{(m+1)m!(n-m)(n-m-1)!} \\
&= \frac{(n+1)n!}{(m+1)!(n-m)!} = \binom{n+1}{m+1}.
\end{aligned}$$

4. Se demuestra para todo m por inducción sobre n aplicando la regla de Pascal. □

Teorema 2.32 – *Teorema del binomio de Newton*: Sean $x, y \in A$ y $n \in \mathbb{N}$ donde A es un dominio, entonces:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Pista: Lo probaremos por inducción sobre n, notemos que la identidad es clara para $n \in \{0,1\}$. Para ello, el procedimiento es el siguiente:

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k+1} \\
&= x^{n+1} + \sum_{k=0}^{n-1}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=1}^{n}\binom{n}{k}x^k y^{n-k+1} + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}x^k y^{n-k+1} + \sum_{k=1}^{n}\binom{n}{k}x^k y^{n-k+1} + y^{n+1} \\
&= \binom{n+1}{n+1}x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^k y^{n-k+1} + \binom{n+1}{0}y^{n+1} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{(n+1)-k}.
\end{aligned}$$

Lo que completa la demostración. □

§2.1.2 Característica.

Lema 2.33: Si A es unitario, entonces existe un único homomorfismo $\varphi\colon \mathbb{Z} \to A$.

Pista: Basta construir φ por recursión empleando que $\varphi(1) = 1$. □

Definición 2.34: Si A es unitario le llamamos su ***característica***, denotado por $\operatorname{car} A$, al $n \in \mathbb{N}$ tal que $\ker \varphi = n\mathbb{Z}$, donde φ es el morfismo del lema anterior.

En particular, los anillos unitarios de característica n conforman su propia subcategoría, denotada Ring_n.

Corolario 2.35: La característica de un dominio íntegro es o 0 o un número p primo.

Proposición 2.36: Si A, B son unitarios y existe un $\phi\colon A \to B$ morfismo de anillos, entonces $\operatorname{car} B \mid \operatorname{car} A$.

Teorema 2.37: Si $\Bbbk$ es un cuerpo, entonces:

1. Si $\operatorname{car} \Bbbk = p$, entonces existe un único morfismo $\phi\colon \mathbb{F}_p \to \Bbbk$.
2. Si $\operatorname{car} \Bbbk = 0$, entonces existe un único morfismo $\phi\colon \mathbb{Q} \to \Bbbk$.

En consecuencia, $\mathbb{Q}$ es el objeto inicial de Fld_0 y $\mathbb{F}_p$ el de Fld_p.

Definición 2.38: Sea p un número primo o $p = 0$. Se le llama ***cuerpo primo*** de característica p a $\mathbb{F}_p$ si $p \neq 0$, o a $\mathbb{Q}$ si $p = 0$.

Teorema 2.39 (Sueño del aprendiz): Si $\operatorname{car} \Bbbk = p \neq 0$, entonces para todo $x, y \in \Bbbk$ se cumple que

$$(x + y)^p = x^p + y^p.$$

Pista: Para ésto se debe ocupar un poco de teoría de números para ver que los coeficientes binomiales $\binom{p}{k}$ son múltiplos de p. □

2.2 Divisibilidad en anillos

Curiosamente ya hemos visto como el conjunto de números enteros admite las ideas de divisibilidad, y en la siguiente sección sobre como esta propiedad se mantiene en polinomios racionales. El objetivo de esta sección es generalizar dicha propiedad en términos del álgebra moderna, también se pretende profundizar en teoría de números en el reino de la aritmética modular; por supuesto, comencemos con una definición:

Definición 2.40 – *Divisibilidad*: Sea A un dominio con $a, b \in A$. Escribimos $a \mid b$ cuando existe $q \in A$ tal que $b = aq$. Si dos elementos cumplen que $a \mid b$ y $b \mid a$, diremos que son ***asociados***.

Todas las propiedades de divisibilidad en enteros se conservan. Cabe destacar que podemos generalizar una propiedad de los enteros y notar que toda unidad u divide a todo elemento de A. Asimismo, dos elementos son asociados syss el segundo es el producto del primero por una unidad.

Los divisores de un elemento se clasifican en: ***impropios*** que son las unidades y los asociados de si mismo; y ***propios***.

Definición 2.41 – *Irreducibles y primos*: Sea A un dominio. Diremos que un elemento es ***irreducible*** syss es es no nulo, no es inversible, y no posee divisores propios. Un elemento que no sea nulo ni inversible y que no sea irreducible se dice ***reducible***.

Diremos también que un elemento p es ***primo*** syss $p \mid ab$ implica $p \mid a$ o $p \mid b$.

De esta forma, podemos ver que todo dominio A se divide en su elemento nulo, sus unidades, sus elementos reducibles y sus irreducibles.

En caso de los enteros podemos ver que la noción de primo e irreductible concuerdan (cf. lema de Euclides), pero ese no es siempre el caso.

Teorema 2.42: En un dominio íntegro A todo primo es irreducible.

Demostración: Sea $p = xy$ un primo de A con $x, y \in A$. Por construcción, $xy \mid p$, lo que implica, $x \mid p$ e $y \mid p$. También $p \mid xy$, por definición, $p \mid x$ o $p \mid y$. Luego, alguno de los dos (x o y) está asociado con p, por ende, el otro es una unidad; es decir, p es irreducible. □

Definición 2.43: Un dominio A se dice que posee la:

Propiedad de factorización: Cuando todo reducible puede expresarse como producto de irreducibles.

Unicidad de factorización: Cuando todo reducible x puede expresarse como producto de primos. Y además si

$$x = p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m$$

son factorizaciones por primos, entonces $n = m$ y existe una permutación $\sigma \in S_n$ tal que p_i y $q_{\sigma(i)}$ son asociados.

Un dominio que admite ambas anteriores se dice un ***dominio de factorización única*** (abreviado, DFU).

Si no se comprende la unicidad, déjeme aclarárselo con un ejemplo. El número 6 puede descomponerse en factores irreductibles como:

$$6 = 2 \cdot 3 = (-3) \cdot (-2),$$

nótese que podemos reordenar los elementos (por medio de la permutación) y ver que el 2 y el -2 son asociados, por tanto, no corresponde a una «factorización distinta». En general, si A es DFU entonces todo elemento podrá escribirse de la forma

$$n = u \prod_{i=0}^{k} p_i^{\alpha_i},$$

donde u es una unidad, p_i es un elemento irreducible y para $i \neq j$ se da que p_i no está asociado con p_j.

El teorema fundamental de la aritmética señala que $\mathbb{Z}$ es un DFU.

Teorema 2.44: En un DFU un elemento es primo syss es irreducible.

Teorema 2.45: Todo anillo noetheriano A posee la propiedad de factorización. Si además todo irreducible es primo, entonces A es DFU.

Demostración: Lo probaremos por contrarrecíproca, vale decir, probaremos que si A no posee la propiedad de factorización entonces A no sería noetheriano.

Comencemos por construir un conjunto S que contiene: el cero, las unidades de A, sus elementos irreducibles y los productos finitos entre irreducibles. Luego, supongamos que $B := A \setminus S$ fuese no-vacío, de manera que existe $x \in B$; como x es reducible, existen $y, z \in A$ no-inversibles tales que $x = yz$, y por lo menos alguno pertenece a B.

Utilizando esta información, crearemos una secuencia de elementos de B tales que $x_0 = x$ y $x_{n+1} \mid x_n$ con ambos siempre en B. En general, para $m > n$ se tiene que $x_m \mid x_n$, pero $x_n \nmid x_m$.

Luego, el conjunto $I = \{a : \exists n \in \mathbb{N}\ x_n \mid a\}$ es un ideal y veremos que no puede ser finitamente generado. Para ello, consideremos que los elementos $y_0, \ldots, y_k$ son pertenecientes a I. Por lo tanto, debe existir un $m \in \mathbb{N}$ tal que $x_m \mid y_i$ para todo $0 \leq i \leq k$. Dicho conjunto no puede generar el conjunto, pues de lo contrario $x_m \mid x_n$ para todo $n \in \mathbb{N}$ lo que es una contradicción.

Para la segunda afirmación, supondremos que n es un elemento con dos factorizaciones

$$n = \prod_{i=0}^{j} p_i = \prod_{i=0}^{k} q_i,$$

como las factorizaciones son iguales, podemos decir que se dividen entre sí, por ende, $p_0 \mid \prod_{i=0}^{k} q_i$ y, como p_0 es primo, $p_0 \mid q_i$ para algún $i = 0, \ldots, k$. Construyamos la permutación σ tal que $p_0 \mid q_{\sigma(0)}$, pero como ambos son irreductibles, son asociados. Por cancelación, nos queda que $\prod_{i=1}^{j} p_i = \prod_{i=1}^{k} q_{\sigma(i)}$ y repetimos la operación j veces para comprobar el teorema. □

Definición 2.46: Sea A un anillo. Diremos que un ideal $\mathfrak{p}$ en A es ***primo*** syss $\mathfrak{p} \neq A$ y si para todo $ab \in \mathfrak{p}$ se cumple que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

Diremos que un ideal $\mathfrak{m}$ en A es ***maximal*** syss $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ implica que $\mathfrak{m} = \mathfrak{a}$ o $\mathfrak{a} = A$.

Teorema (AE) 2.47 (Cohen): Un dominio A es noetheriano syss todo ideal primo de A es finitamente generado.

Demostración: $\Longrightarrow$. Trivial.

$\Longleftarrow$. Lo haremos por contrarrecíproca. Sea $\mathcal{F}$ la familia de ideales que no sean finitamente generados, entonces claramente toda $\subseteq$-cadena en $\mathcal{F}$ tiene cota superior, luego por lema de Zorn se cumple que $\mathcal{F}$ tiene un elemento $\subseteq$-maximal $\mathfrak{m}$.

Veamos que $\mathfrak{m}$ es, de hecho, un ideal primo por contradicción: Supongamos que existen a, b tales que $ab \in \mathfrak{m}$ y $a, b \notin \mathfrak{m}$. Luego $\mathfrak{m} + (a) \supset \mathfrak{m}$ así que ha de ser finitamente generado:

$$\mathfrak{m} + (a) = (m_1 + \lambda_1 a, \ldots, m_n + \lambda_n a)$$

para $m_i \in \mathfrak{m}$ y $\lambda_i \in A$. Definamos también $\mathfrak{n} := \{r \in A : ra \in \mathfrak{m}\}$, luego $\mathfrak{m} \subseteq \mathfrak{n}$ y $b \in \mathfrak{n}$, así que

$$\mathfrak{m} \subset \mathfrak{m} + (b) \subseteq \mathfrak{n},$$

luego $\mathfrak{n}$ es también finitamente generado. Probaremos que $\mathfrak{m} = (m_1, \ldots, m_n) + \mathfrak{n}a$: Es claro que $(m_1, \ldots, m_n) \subseteq \mathfrak{m}$ y que $\mathfrak{n}a \subseteq \mathfrak{m}$. Por otro lado, sea $z \in \mathfrak{m} \subseteq \mathfrak{m} + (a)$, de modo que

$$z = \sum_{j=1}^{n} (m_j + \lambda_j a)\mu_j = \sum_{j=1}^{n} \mu_j m_j + \left(\sum_{j=1}^{n} \mu_j \lambda_j \right) a,$$

donde el primer sumando está en $(m_1, \ldots, m_n)$ por definición, y el segundo sumando está en $\mathfrak{m}$, de modo que el factor que acompaña a a está, efectivamente, en $\mathfrak{n}$. □

Proposición 2.48: Sea $\varphi\colon A \to B$ un homomorfismo de anillos. Si $\mathfrak{p}$ es un ideal primo de B, entonces $\varphi^{-1}[\mathfrak{p}]$ es un ideal primo de A.

Teorema 2.49: Un ideal $\mathfrak{p}$ en un dominio A es primo syss $A/\mathfrak{p}$ es un dominio íntegro.

Demostración: $\Longrightarrow$. Nótese que como $\mathfrak{p} \neq A$, entonces $1 \notin \mathfrak{p}$, luego $[1] \neq 0$, es decir, $A/\mathfrak{p}$ es un dominio. Si $a, b \in A/\mathfrak{p}$ cumplen que $[a][b] = [ab] = 0$, entonces $ab \in \mathfrak{p}$ lo que implica que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$ por definición de primo, de modo que o $[a] = 0$ o $[b] = 0$, por lo que el dominio es íntegro.

$\Longleftarrow$. Es análogo. □

Teorema 2.50: Un ideal $\mathfrak{m}$ en un dominio A es maximal syss $A/\mathfrak{m}$ es un cuerpo.

Demostración: $\Longrightarrow$. Como $\mathfrak{m} \neq A$, $A/\mathfrak{m}$ es un dominio. Supongamos que $\mathfrak{a}$ es un ideal de $A/\mathfrak{m}$ y $\pi : A \to A/\mathfrak{m}$ es un homomorfismo de anillos, entonces $\mathfrak{b} := f^{-1}(\mathfrak{a})$ es un ideal que satisface que $\mathfrak{m} \subseteq \mathfrak{b} \subseteq A$, luego $\mathfrak{m} = \mathfrak{b}$ o $\mathfrak{b} = A$. En el primer caso, $\mathfrak{a}$ corresponde al ideal trivial (0). En el segundo, corresponde al ideal (1). Luego por el corolario 2.16 es un cuerpo.

$\Longleftarrow$. Es análogo. □

Corolario 2.51: En un dominio A, todo ideal maximal es primo.

Si se asume AE veremos que todo dominio posee al menos un ideal maximal (véase teorema 2.78).

Lema 2.52: Sea A un dominio íntegro y $a, p \in A$ no nulo, entonces:

1. p es primo syss (p) es un ideal primo.
2. a es irreducible syss (a) es maximal entre los ideales principales.
3. En un DIP: a es irreducible syss (a) es maximal.

Como un DIP es un dominio, vemos que efectivamente todo irreductible es primo. Lo que sumado al teorema 2.45 nos da:

Teorema 2.53: Todo DIP es un DFU.

Definición 2.54: Sea A un DFU, entonces definiremos un ***máximo común divisor*** (mcd) entre dos números $a, b \in A$ como el producto de todos los primos que dividen a ambos elevados al mínimo exponente en cada caso. Análogamente definimos un ***mínimo común múltiplo*** (mcm) entre ambos como el producto de todos los primos que dividen a cualquiera de los dos elevados al máximo exponente en cada caso.

Nótese que siempre, todos los mcd's y mcm's resp. son asociados entre sí.

Teorema 2.55 (Identidad de Bézout): Sea A un DIP con $a_0, \ldots, a_n \in A$; luego sea m un mcd, entonces

$$(m) = \sum_{i=0}^{n} (a_i) = (a_0, \ldots, a_n);$$

en particular, existen $\lambda_0, \ldots, \lambda_n \in A$ tales que

$$\sum_{i=0}^{n} \lambda_i a_i = m.$$

Demostración: Definamos que $(m) = \sum_{i=0}^{n}(a_0)$, probaremos que m es un mcd de dicha secuencia. Evidentemente $m \mid a_i$ para $i = 0, \ldots, n$ y si d es un divisor común, entonces $(m) \subseteq (d)$ lo que implica $m \mid d$. Como el resto de mcd's son asociados, también están contenidos en (m); por simetría, el ideal de todos los mcd's concuerda y es el mismo. □

Nótese que conceptos como los de ser coprimos se mantienen.

Ahora probaremos una versión más abstracta del teorema chino del resto, para lo cual necesitamos una pequeña definición previa:

Definición 2.56: Si $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$, entonces se denota

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{k=1}^{n} \alpha_k \beta_k : \forall k \ \alpha_k \in \mathfrak{a}, \beta_k \in \mathfrak{b} \right\}.$$

A veces nos referiremos a $\mathfrak{a} \cdot \mathfrak{b}$ como «producto de ideales» para evitar confusiones.

Proposición 2.57: Si $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$, entonces $\mathfrak{a} \cdot \mathfrak{b} \trianglelefteq A$ y $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

Proposición 2.58: Se cumplen:

1. Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos de A y $\mathfrak{a} \trianglelefteq A$. Luego si $\mathfrak{a} \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, entonces $\mathfrak{a} \subseteq \mathfrak{p}_j$ para algún j.

2. Sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de A y $\mathfrak{p} \trianglelefteq A$ primo. Si $\bigcap_{i=1}^{n} \mathfrak{a}_i \subseteq \mathfrak{p}$, entonces $\mathfrak{a}_j \subseteq \mathfrak{p}$ para algún j. Más aún, si $\bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{p}$, entonces $\mathfrak{a}_j = \mathfrak{p}$ para algún j.

Demostración:

1. Probaremos por inducción la contrarrecíproca, vale decir:

$$\forall i \; \mathfrak{a} \not\subseteq \mathfrak{p}_i \implies \mathfrak{a} \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

   Claramente se satisface el caso base $n = 1$. Supongamos que aplica para n: Luego, por hipótesis inductiva, sea

$$x_j \in \mathfrak{a} \setminus \sum_{\substack{i=1 \\ i \neq j}}^{n+1} \mathfrak{p}_i.$$

   Si algún $x_j \notin \mathfrak{p}_j$, entonces estamos listos. Si no, entonces

$$y := \sum_{j=1}^{n+1} \prod_{\substack{i=1 \\ i \neq j}}^{n+1} x_i$$

   es un elemento de $\mathfrak{a}$ que no está en ningún $\mathfrak{p}_i$.

2. Probaremos la contrarrecíproca: Sea $x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ para todo i. Luego $\prod_{i=1}^{n} x_i \in \prod_{i=1}^{n} \mathfrak{a}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i$, y además $\prod_{i=1}^{n} x_i \notin \mathfrak{p}$, por definición de ideal primo.

   Más aún, si $\bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{p}$, entonces $\mathfrak{a}_j \subseteq \mathfrak{p}$ para algún j por la afirmación anterior, pero $\mathfrak{p} \subseteq \mathfrak{a}_j$ (por ser igual a la intersección); por lo que $\mathfrak{p} = \mathfrak{a}_j$. □

El lector atento reconocerá en el primer inciso la misma clase de técnicas que Euclides emplea para probar la infinitud de los números primos. A la proposición anterior, que será útil más adelante en contexto del álgebra conmutativa, se le conoce como *evitamiento de primos*.

Teorema 2.59 – *Teorema chino del resto*: Si A es un dominio y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq A$, entonces

$$\begin{aligned} \varphi\colon A &\longrightarrow A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n \\ a &\longmapsto (a+\mathfrak{a}_1, \ldots, a+\mathfrak{a}_n) \end{aligned}$$

es un homomorfismo de anillos con $\ker\varphi = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n$. Más aún:

1. Si $\mathfrak{a}_i + \mathfrak{a}_j = A$ para todo $i \neq j$, entonces $\prod_{i=1}^n \mathfrak{a}_i = \ker\varphi = \bigcap_{i=1}^n \mathfrak{a}_i$.
2. φ es suprayectiva syss $\mathfrak{a}_i + \mathfrak{a}_j = A$ para todo $i \neq j$.
3. φ es inyectiva syss $\bigcap_{i=1}^n \mathfrak{a}_i = (0)$.

Demostración: Ver que φ es un homomorfismo de anillos es trivial y

$$a \in \ker\varphi \iff a \in \mathfrak{a}_1, a \in \mathfrak{a}_2, \ldots, a \in \mathfrak{a}_n \iff a \in \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n.$$

La otra parte la demostraremos para $n = 2$, pero el resto de casos es análogo: Si $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, entonces existen $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2$ tales que $a_1 + a_2 = 1$. Luego

$$\varphi(a_1) = ([0], [a_1 + a_2 - a_1]) = ([0], [1]), \quad \varphi(a_2) = ([1], [0]).$$

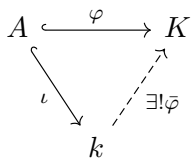
Luego, para todo $(b + \mathfrak{a}_1, c + \mathfrak{a}_2)$ se cumple que $ba_1 + ca_2$ es una preimagen. La otra implicancia es claramente deducible de manera similar.

Para ver la otra igualdad basta probar que $\ker\varphi \subseteq \mathfrak{a}_1 \cdot \mathfrak{a}_2$ (por la proposición anterior), lo que se da pues si $d \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, entonces $db_1 + db_2 = d(b_1 + b_2) = d \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$. □

Corolario 2.60: Si A es un dominio y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq A$, entonces el homomorfismo φ del teorema anterior se restringe a un homomorfismo de grupos

$$\varphi\colon A^\times \longrightarrow (A/\mathfrak{a}_1)^\times \times \cdots \times (A/\mathfrak{a}_n)^\times.$$

Teorema 2.61: Todo dominio íntegro A está contenido en un cuerpo k, tal que si $\varphi : A \hookrightarrow K$ con K cuerpo, entonces existe un único homomorfismo $\bar{\varphi} : k \hookrightarrow K$. Es decir, se satisface el siguiente diagrama:



Demostración: Consideremos $A \times A_{\neq 0}$ con la relación

$$(a,b) \sim (c,d) \iff ad = bc,$$

que resulta ser de equivalencia. Luego sea k su conjunto cociente, donde denotamos $a/b := [a,b]$. Definamos las siguientes operaciones sobre k:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Entonces $(k,+,\cdot)$ corresponde a un cuerpo, veamoslo:

i) $(k,+)$ es un grupo abeliano, cuyo neutro es $0/1$: Como el producto y la suma de A conmutan, es claro que la suma de k también. La asociatividad queda al lector, pero también es inducida por la asociatividad y distributividad de las operaciones de A. Es fácil notar que $0/a = 0/1$ para todo $a \in A_{\neq 0}$ lo que demuestra que $a/b + 0/1 = (a \cdot 1 + b \cdot 0)/b = a/b$. Y finalmente $a/b + (-a)/b = (ab + (-a)b)/(b^2) = 0/b^2 = 0$.

ii) $(k,\cdot)$ es un grupo abeliano: Ésto es lo más facil, ya que k se comporta bien con el producto. Para ello, nótese que $a/a = 1/1 =: 1$ por definición de la relación $\sim$. Además si $a/b \neq 0$, entonces necesariamente $a \neq 0$, por lo que $b/a \in k$ y $(a/b)^{-1} = b/a$.

iii) $+$ y $\cdot$ admiten distributividad: Queda de ejercicio al lector.

Así, sea $\iota : A \to k$ dada por $\iota(a) = a/1$, claramente corresponde a un homomorfismo inyectivo.

Sea $\varphi : A \to K$; entonces sea $\bar{\varphi}(a/b) := \varphi(a) \cdot \varphi(b)^{-1}$, queda al lector comprobar que efectivamente es un homomorfismo de anillos bien definido e inyectivo. □

Corolario 2.62: Si A es un dominio íntegro y k, k' son dos cuerpos como en el teorema anterior, entonces existe un isomorfismo natural entre ambos.

Definición 2.63: Por el corolario anterior se denota por $\mathrm{Frac}(A)$ al cuerpo dado en la demostración del teorema, al que llamamos ***cuerpo de fracciones*** de A.

El lector atento habrá notado dos cosas: La primera es que la construcción de $\mathrm{Frac}(A)$ es exactamente la misma que de $\mathbb{Q}$ desde $\mathbb{Z}$, es decir, podríamos definir $\mathbb{Q} := \mathrm{Frac}(\mathbb{Z})$. La segunda es que la condición segunda del teorema es

una condición minimal propia de las categorías, de hecho, podríamos construir una categoría de los cuerpos que extienden a A y lo que nos dice el teorema es que dicha categoría posee un objeto inicial; en este sentido el corolario es trivial.

2.3 Polinomios

Un polinomio viene a representar objetos de la forma

$$2x + 1; \quad 5xy + 6z^3; \quad 15x^2 + 3y + 2x$$

y así, y para ello surgen dos representaciones incompatibles: la analítica y la algebraica.

Para explicarlo en términos sencillos me serviré de una analogía: imagina que queremos definir el concepto de un platillo gastronómico, para ello podrías definirlo o en base a una receta o en base al resultado final. La primera es la visión de los algebristas sobre los polinomios, la segunda la de los analistas; ambas son útiles dentro de sus contextos. Dado que la receta corresponde a una manipulación de los ingredientes, y nuestros *ingredientes* son los números de nuestras estructuras, puede darse que queramos modificar una estructura, ya sea extendiéndola o contrayéndola, lo que equivale a cambiar los ingredientes. Ésto es fatal para el platillo final, ya que es muy dificil extraer la receta del resultado para permitirnos encontrar una manera *natural* de ver la transformación del platillo; sin embargo, la receta no tiene problema, ya que basta con re-ejecutar el proceso para obtener el platillo modificado sin mayores esfuerzos.

Ejemplo (informal). Consideremos que trabajamos en $\mathbb{F}_p$ y se define el polinomio $f(x) := x^{p^2} - x^p$. Por el pequeño teorema de Fermat es fácil ver que toma 0 en todo punto, ¿deberíamos entonces extender el polinomio como el constante 0? Consideremos $\mathbb{F}_{\mathrm{i}} := \{a + \mathrm{i}b : a, b \in \mathbb{F}_p\}$ donde $\mathrm{i}^2 = -1$ y para tomar un ejemplo en concreto, sea $p = 3$; luego $f(\mathrm{i}) = \mathrm{i}^9 - \mathrm{i}^3 = \mathrm{i} - (-\mathrm{i}) = 2\mathrm{i} \neq 0$. Queda al lector explicar cuándo se replica este fenómeno.

Definición formal. Aquí haremos un enredado ejercicio para poder definir a los polinomios como *recetas*, debido a su complejidad se deja como opcional. Para la construcción de los polinomios, primero construiremos una versión más rudimentaria: los ***monomios***. El término «-nomio» significa adecuadamente «término», de manera que queremos algo de la forma x^2y, por ejemplificar, sin preocuparse aún de «los números que acompañan los monomios», llamados ***coeficientes***.

Definiremos S como un conjunto cualquiera que contiene a las indeterminadas (usualmente denotadas x, y, etc.). Y denotaremos $\eta\colon S \to \mathbb{N}$ a una función que representará un monomio, que a cada indeterminada le asigna su exponente. Luego algo como x^2y se representa por la función

$$\eta(s) := \begin{cases} 2, & s = x \\ 1, & s = y \\ 0, & s \notin \{x, y\} \end{cases}$$

Si se admite que ϵ_x es la función que da 1 cuando la indeterminada del argumento y del indice son iguales, y cero en otro caso, entonces podemos denotar $\eta = 2\epsilon_x + 1\epsilon_y$. Denotamos M al conjunto de todos los monomios.

Definición 2.64 – *Polinomio*: Finalmente, dado un anillo A y un conjunto de indeterminadas S, denotaremos $A[S]$ al conjunto de todas las aplicaciones $f\colon M \to A$ tal que $M \setminus f^{-1}[0]$ es finito, es decir, tal que tan sólo finitos monomios poseen coeficientes no nulos. En definitiva f representa a la expresión

$$f(u_1)x_1^{u_1(x_1)} \cdots x_n^{u_1(x_n)} + \cdots + f(u_m)x_1^{u_m(x_1)} \cdots x_n^{u_m(x_n)}.$$

Definimos el grado (en inglés, *degree*) de un polinomio, como la mayor suma de exponentes por término, formalmente

$$\deg f = \max\{u(x_1) + \cdots + u(x_n) : f(u) \neq 0\}$$

Digamos que el grado de f es d, si hay un sólo término de f de grado d diremos que el coeficiente de dicho término es llamado ***coeficiente lider***. Si el coeficiente lider es 1, se dice que el polinomio es ***mónico***.

Además definimos $+, \cdot$ sobre $A[S]$ de la siguiente forma, para todo $\eta \in M$

$$(f+g)(\eta) := f(\eta) + g(\eta), \quad (f \cdot g)(\eta) := \sum_{\substack{\kappa,\lambda \in M \\ \kappa+\lambda=\eta}} f(\kappa) \cdot g(\lambda).$$

Cabe destacar que puede darse el caso que dado un polinomio no-constante de una sola indeterminada f exista un $x \in A$ tal que $f(x) = 0$, en ese caso decimos que x es una ***raíz*** del polinomio.

En realidad, todo este proceso corresponde a una formalidad para la construcción absoluta de los polinomios, en lo sucesivo, sólo los denotaremos

mediante sus representaciones, por ejemplo

$$f(x) = \sum_{i\geq 0} a_i x^i$$

el cual pertenece a $A[x]$. Por lo general se suelen usar polinomios de una única variable por su simpleza, cabe destacar que si estos poseen un grado digamos n, entonces es por que el término x^n es el mayor con coeficiente no nulo.

Sean $f, g \in A[x]$, entonces

$$(f+g)(x) := f(x) + g(x) = \sum_{i\geq 0} (a_i + b_i) x^i$$

$$(f \cdot g)(x) := f(x) \cdot g(x) = \sum_{k\geq 0} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Proposición 2.65: Si A un anillo (resp. anillo unitario, anillo conmutativo), entonces $(A[x], +, \cdot)$ lo es.

Demostración: Es evidente que $(A[x], +)$ es un grupo abeliano, la asociatividad del producto se demuestra con

$$\begin{aligned}(fg)h &= \sum_{v\geq 0} \left(\sum_{u+k=v} \left(\sum_{i+j=u} a_i b_j \right) c_k \right) x^v = \sum_{v\geq 0} \left(\sum_{i+j+k=v} a_i b_j c_k \right) x^v \\ &= \sum_{v\geq 0} \left(\sum_{i+w=v} a_i \sum_{j+k=w} b_j c_k \right) x^v = f(gh).\end{aligned}$$

La distributividad es simple, puede comprobarla manualmente. Si A es unitario, entonces $1(x) := 1 \in A[x]$ que es, asimismo, una unidad. La conmutatividad es trivial. □

Podemos afirmar sencillamente que $\deg(f+g) \leq \text{máx}(\deg f, \deg g)$ y $\deg(fg) \leq \deg f + \deg g$.

Teorema 2.66: Sean $f, g \in A[x]$ no nulos, de grados n y m respectivamente, tales que a_n, b_m no son divisores de cero, entonces

$$\deg(fg) = \deg f + \deg g.$$

En consecuencia, si A es un dominio íntegro y S un conjunto de indeterminadas, entonces $A[S]$ es también un dominio íntegro.

Demostración: Notemos que como a_n, b_m son no nulos y no divisores de cero, se da $\sum_{i+j=n+m} a_i b_j = a_n b_m \neq 0$, pues para todo $i > n$ y $j > m$ ocurre $a_i = b_j = 0$, es decir, $\deg(fg) \leq \deg f + \deg g$, por tricotomía, $\deg(fg) = \deg f + \deg g$. □

Cabe destacar que como todo polinomio de una indeterminada posee coeficientes en el anillo, todo polinomio de $(n+1)$ indeterminadas es realmente un polinomio de una con coeficiente en el anillo de polinomios de n indeterminadas, es decir, $A[x_1, \ldots, x_n, x_{n+1}] = A[x_1, \ldots, x_n][x_{n+1}]$.

Teorema 2.67: Si A es un dominio íntegro y S un conjunto de indeterminadas, entonces $A[S]^\times = A^\times$.

Demostración: Por el teorema 2.66 vemos que multiplicar polinomios sólo incrementa el grado de éste, por ende, el polinomio debe ser constante para ser invertible, luego, debe ser una unidad de A. □

De no tratarse de un dominio íntegro, entonces el resultado anterior falla:

Ejemplo. Considere $A = \mathbb{Z}/4\mathbb{Z}$ y $f(x) = 1 + 2x \in A[x]$. Luego, nótese que $f(x)^2 = 1 + 2 \cdot 2x + 2^2 x^2 = 1$, es decir, $f(x) \in A[x]^\times$.

Una de las ventajas de los polinomios es que son expresiones algebraicas y, por lo tanto, admiten una noción de evaluación:

Teorema 2.68: Sean A, B dominios, sea $\phi\colon A \to B$ un homomorfismo de anillos tal que $\phi(1) = 1$, S un conjunto de indeterminadas y $v\colon S \to B$ una función arbitraria. Entonces existe un único homomorfismo de anillos $\Phi\colon A[S] \to B$ tal que $\Phi|_S = v$ y $\Phi|_A = \phi$.

Demostración: Como los polinomios ocupan finitas indeterminadas podemos tomar $p, q \in A[S]$ y suponer que se escriben de la forma:

$$p = \sum_{i=1}^{m} a_i x_1^{k_{i,1}} \cdots x_n^{k_{i,n}}, \qquad q = \sum_{i=1}^{m} b_i x_1^{k_{i,1}} \cdots x_n^{k_{i,n}}.$$

Nótese que no perdemos generalidad suponiendo que los exponentes y las indeterminadas son las mismas ya que podemos agregar coeficientes nulos.

Luego, definimos:

$$\Phi(p) := \sum_{i=1}^{m} \phi(a_i) v(x_1)^{k_{i,1}} \cdots v(x_n)^{k_{i,n}},$$

y veamos que es, de hecho, un homomorfismo de anillos:

$$\begin{aligned}
\Phi(p+q) &= \sum_{i=1}^{m} \phi(a_i + b_i) v(x_1)^{k_{i,1}} \cdots v(x_n)^{k_{i,n}} = \Phi(p) + \Phi(q) \\
\Phi(p \cdot q) &= \Phi\left(\sum_{i,j}^{m} a_i b_j x_1^{k_{i,1}+k_{j,1}} \cdots x_n^{k_{i,n}+k_{j,n}} \right) \\
&= \sum_{i,j}^{m} \Phi(a_i b_j x_1^{k_{i,1}+k_{j,1}} \cdots x_n^{k_{i,n}+k_{j,n}}) \\
&= \sum_{i,j}^{m} \phi(a_i)\phi(b_j) v(x_1)^{k_{i,1}+k_{j,1}} \cdots v(x_n)^{k_{i,n}+k_{j,n}} = \Phi(p)\Phi(q).
\end{aligned}$$

La unicidad se sigue del hecho de que, de haber otro homomorfismo, debe coincidir primero en los monomios, luego respetar los coeficientes y así se llega a concluir que debe tener la misma forma. □

En el caso de que $S = (x_1, \ldots, x_n)$ y $v(x_i) = \alpha_i$ para todo i, entonces solemos denotar dicho homomorfismo como:

$$\mathrm{ev}_{\alpha_1,\ldots,\alpha_n} \colon A[x_1, \ldots, x_n] \longrightarrow A.$$

Similar a como en la sección 1.3 introducimos la división de números mediante un algoritmo, veremos que los polinomios comparten dicha propiedad:

Teorema 2.69 – *Algoritmo de división polinómica*: Sea A un anillo con $\alpha \in A[x]$ un polinomio no nulo cuyo coeficiente director es una unidad de A y $\beta \in A[x]$ cualquiera. Existen unos únicos polinomios $q, r \in A[x]$ tales que

$$\beta(x) = \alpha(x) \cdot q(x) + r(x), \quad 0 \leq \deg r < \deg \alpha$$

DEMOSTRACIÓN: Diremos que $n := \deg \alpha$ y $m := \deg \beta$. Si $n > m$ entonces $q = 0$ y $r = \beta$. De caso contrario ($n \leq m$), lo probaremos por inducción sobre m.

Caso $m = 0$: ocurre con $\beta(x) = b_0$ y $\alpha(x) = a_0$, con a_0 unidad, por tanto, $q(x) = a_0^{-1}b_0$.

Caso m: Consideremos que $\beta(x) = b_0 + \cdots + b_m x^m$ y $\alpha(x) = a_0 + \cdots + a_n x^n$, luego $\alpha a_n^{-1} b_m x^{m-n} = \sum_{i=0}^{n} a_i a_n^{-1} b_m x^{m-n+i}$ posee mismo término director, por ende, existen $q, r \in A[x]$ tales que:

$$\beta - \alpha a_n^{-1} b_m x^{m-n} = \alpha q + r$$

(por hipótesis inductiva, pues el polinomio de la izquierda tiene grado a lo más $m-1$). Finalmente, pasamos el término de α a la derecha para obtener que

$$\beta(x) = \alpha(x) \cdot (a_n^{-1} b_m x^{m-n} + q(x)) + r(x)$$

que satisface todas nuestras restricciones.

La unicidad de q, r se produce pues si existiese otro par $q', r' \in A[x]$ se tendría que

$$\alpha q + r = \alpha q' + r' \iff \alpha(q - q') = r' - r$$

como son distintos, son no nulos, por lo tanto, $\deg(r' - r) < \deg \alpha \leq \deg \alpha + \deg(q - q')$ lo que es absurdo. □

Nuevamente, a $q(x), r(x)$ les llamamos ***cociente*** y ***resto*** resp. De igual forma, si el resto en la división entre $\beta(x)$ sobre $\alpha(x)$ escribiremos $\alpha(x) \mid \beta(x)$ como si de números enteros se tratase.

Corolario 2.70: Si A es un cuerpo, entonces $A[x]$ es un dominio euclídeo cuya norma es el grado.

Teorema 2.71: Si A es un dominio íntegro, entonces $A[x]$ es un DIP syss A es un cuerpo.

Demostración: El corolario anterior prueba $\Longleftarrow$, así que probaremos la recíproca: Sea $a \in A$ no nulo, entonces (x, a) es un ideal de $A[x]$, pero como $A[x]$ es DIP existe $p \in A[x]$ tal que $(x, a) = (p)$. En consecuencia existe $q \in A[x]$ tal que $a = pq$ y como a es un polinomio constante, p, q han de serlo. También existe $r \in A[x]$ tal que $x = pr$, pero con $r = sx$ con lo que $ps = 1 \in (p)$.
Por identidad de Bézout existen $u, v \in A[x]$ tales que $1 = ux + va$, pero 1 es un polinomio constante luego $u = 0$ y $va = 1$ con $v \in A$ como se quería probar. □

Teorema 2.72 – *Regla de Ruffini*: Sea A un anillo con $p(x) \in A[x]$ y $a \in A$. Luego la división de $p(x)$ con $(x-a)$ es la constante $p(a)$. Una consecuencia es que $(x-a) \mid p(x)$ syss a es una raíz de p.

Teorema 2.73: Sea A un anillo con $p(x) \in A[x]$ de grado n, entonces p tiene, a lo sumo, n raíces.

Teorema 2.74 (Wilson): Si p es primo, entonces

$$(p-1)! \equiv -1 \pmod{p}.$$

Demostración: Por definición $(p-1)! = 1 \cdot 2 \cdots (p-1)$ que corresponde al producto de todo $\mathbb{Z}_p^\times$. Nótese que $x \in \mathbb{Z}_p^\times$ es su propia inversa syss $x = x^{-1}$ syss x es raíz de $x^2 - 1$. Dicho polinomio se expresa $x^2 - 1 = (x-1)(x+1)$ de modo que sus raíces son ± 1. En conclusión:

$$(p-1)! \equiv 1 \cdot (-1) = -1 \pmod{p}. \qquad \square$$

Teorema 2.75 (Algoritmo de Horner-Ruffini): Sean A un dominio íntegro con $x_0 \in R$ y $p(x) \in A[x]$ un polinomio de la forma $p(x) = a_0 + \cdots + a_n x^n$. Defínase la secuencia, de forma inductiva (a la inversa):

$$b_n := a_n, \quad b_i = a_i + b_{i+1} x_0;$$

entonces se cumple que

$$p(x) = (x - x_0)(b_n x^{n-1} + \cdots + b_1) + b_0$$

Demostración: Para ver el funcionamiento del algoritmo, nótese que el polinomio puede escribirse como

$$p(x) = a_0 + x(a_1 + \cdots x(a_{n-1} + x a_n) \cdots). \qquad \square$$

Un ejemplo rápido de aplicación es dividir el polinomio $3x^2 + 2x + 1$ sobre $x + 1 = x - (-1)$:

Podemos ver que es correcto, pues

$$(x - (-1))(3x + (-1)) + 2 = 3x^2 - x + 3x - 1 + 2 = 3x^2 + 2x + 1.$$

	3	2	1
-1		$3 \cdot -1 = -3$	$-1 \cdot -1 = 1$
	3	$2 + (-3) = -1$	$1 + 1 = 2$

Figura 2.1. Aplicación del algoritmo de Horner-Ruffini.

Teorema 2.76 – *Polinomio de interpolación de Lagrange*: Sea A un cuerpo con $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$. Existe un único polinomio $f \in A[x]$ de grado menor a n tal que $f(a_i) = b_i$ para todo $i = 1, \ldots, n$; y está dado por la fórmula[a]

$$f(x) = \sum_{i=1}^{n} b_i \frac{P_i(x)}{P_i(a_i)}, \quad P_i(x) = \frac{\prod_{j=1}^{n}(x - a_j)}{x - a_i}. \tag{2.1}$$

[a] En análisis matemático, la expresión $P_i(a_i)$ estaría indeterminada por ser del tipo «0/0», no obstante, aquí se realiza la disivión polinómica primero y luego se efectúa la aplicación en el punto a_i. Dicho de otro modo, no se indetermina y se entiende que se erradica el factor $x - a_i$ del producto.

Demostración: Es fácil ver que $P_i(a_j) = 0$ cuando $i \neq j$, por lo que, el polinomio de Lagrange efectivamente cumple con las condiciones indicadas. Para ver que es el único de grado menor a n, consideremos que $g(x) \in A[x]$ también cumpliese con las condiciones, luego $(f-g)(x)$ sería un polinomio de grado menor que n con n raíces, lo que es imposible por el teorema 2.73. □

Teorema 2.77 – *Teorema de bases de Hilbert*: Si A es un anillo noetheriano, entonces $A[x_1, \ldots, x_n]$ lo es.

Demostración: Esencialmente sólo nos basta probar que si A es noetheriano, $A[x]$ lo es. Pues la generalización se reduce a simple inducción.

Sea $\mathfrak{b}$ un ideal de $A[x]$, entonces definiremos $\mathfrak{a}_i$ como el conjunto de todos los coeficientes directores de los polinomios de $\mathfrak{b}$ de grado i (más el cero).

Es fácil ver que $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ (pues basta multiplicar por x el polinomio que justifica que $a_i \in \mathfrak{a}_i$ para ver que pertenece también a $\mathfrak{a}_{i+1}$). Aplicando la definición de noetheriano, existe un n tal que $\mathfrak{a}_n$ es el maximal.

Sea $\mathfrak{a}_i = (a_{i0}, \ldots, a_{im})$ (nótese que si $\mathfrak{a}_i$ se puede generar con menos de i elementos, podemos rellenar con generadores redundantes).

Luego sea p_{ij} un polinomio en $\mathfrak{b}$ de grado i tal que todo coeficiente de grado k sea a_{kj}. Definamos $\mathfrak{c} := (p_{ij} : i = 0, \ldots, n; j = 0, \ldots, m)$. Evidentemente $\mathfrak{c} \subseteq \mathfrak{b}$.

Sea f un polinomio de grado k contenido en $\mathfrak{b}$, probaremos que $f \in \mathfrak{c}$ por inducción sobre k. Si $k > n$, vemos que el coeficiente director de los polinomios $x^{k-n}p_{n0}, \ldots, x^{k-n}p_{nm}$ son $a_{n0}, \ldots, a_{nm}$ que definen $\mathfrak{a}_k = \mathfrak{a}_n$, luego, existen $b_0, \ldots, b_m \in A$ tales que

$$q := b_0 x^{k-n} a_{n0} + \cdots + b_m x^{k-n} a_{nm}$$

es un polinomio que comparte coeficiente director y grado con f (y además pertenece a $\mathfrak{b}$), luego, $f - q$ es de grado menor que q y por hipótesis inductiva, pertenece a $\mathfrak{c}$. El argumento es análogo si $k \leq n$. Con esta información se concluye que $\mathfrak{b} \subseteq \mathfrak{c}$ lo que, por tricotomía, implica que $\mathfrak{b} = \mathfrak{c}$. Más concretamente, demostramos que todo ideal de $A[x]$ está finitamente generado. □

Ejemplo. Tomemos a $\mathbb{R}$ que es cuerpo y por ende noetheriano. Luego si $S := \{x_1, x_2, x_3, \ldots\}$ que es infinito, se nota que $\mathbb{R}[S]$ no es noetheriano, pues $\mathfrak{a} := (S)$ es un ideal propio (pues todo polinomio de $\mathfrak{a}$ es nulo o de grado ≥ 1), pero no es finitamente generado.

Veamos una aplicación de los anillos de polinomios:

Teorema 2.78: Son equivalentes:

1. **El axioma de elección**.
2. Todo ideal propio de un dominio está contenido en un ideal maximal.
3. **Teorema de Krull:** Todo dominio tiene un ideal maximal.

Demostración: (1) $\implies$ (2). Sea $\mathcal{F}$ la familia de los ideales propios de un dominio D que contienen a un ideal $\mathfrak{a}$ fijo. Como $\mathfrak{a} \in \mathcal{F}$ se da que es una familia no vacía parcialmente ordenada y toda cadena tiene supremo (su unión por la proposición 2.13) luego $\mathcal{F}$ tiene un elemento maximal que es un ideal.

(2) $\implies$ (3). Basta notar que (0) es un ideal propio en todo dominio.

(3) $\implies$ (1). En particular veremos que el teorema de Krull equivale a la siguiente proposición:

> Si $\mathcal{F}$ es una partición de un conjunto E, entonces existe K tal que para todo $S \in \mathcal{F}$ se cumple que $S \cap K$ es singular.

Para ello diremos que K es una *dispersión* de $\mathcal{F}$ si corta a todo miembro de $\mathcal{F}$ en a lo más un elemento. En este sentido AE equivale a ver que para toda familia $\mathcal{F}$ existe una dispersión maximal.

Sea $\mathcal{S}$ el conjunto de todas las dispersiones de $\mathcal{F}$ y $R := \mathbb{Q}[E]$ (donde consideramos a los elementos de E como indeterminadas) y definimos

$$T := \bigcup\{(D) : D \in \mathcal{S}\}, \quad U := T^c = \bigcap\{(D)^c : D \in \mathcal{S}\}$$

Nótese que D es simplemente un conjunto de monomios «x_i», luego (D) es un ideal y es primo (¿por qué?). Como U es la intersección de complementos de ideales primos se cumple que es cerrado bajo productos (de lo contrario $p, q \in U$ cumplirían que $p \cdot q \in T$ que estaría en un ideal primo de T, por lo que $p \in T$ o $q \in T$, contradiciendo que $p, q \in U$).

Consideremos $R \cdot U^{-1} \leq \mathrm{Frac}(R)$, es decir, $R \cdot U^{-1}$ como subanillo del cuerpo de fracciones de R. Entonces $R \cdot U^{-1}$ es un dominio y por el teorema de Krull posee un ideal maximal $\mathfrak{m}$. Luego $\mathfrak{a} := \mathfrak{m} \cap R$ es claramente un ideal de R, y además es maximal y disjunto de U; en consecuencia $\mathfrak{a} \subseteq T$.

Sea $K := \mathfrak{a} \cap E$, entonces $(K) = \mathfrak{a}$: Para probar ésto demostraremos primero un dato útil: Sea $c := q_1 a_1 + \cdots + q_n a_n$ una combinación lineal con $q_i \in \mathbb{Q}$ y $a_i \in R$, entonces c se dice una combinación *conservativa* si los monomios de a_i son también monomios de c. Por ejemplo, $c = (x - y) + y$ no es conservativa, pero $c = (x^2 + y^2) + z^2$ sí. Sea $a + \lambda b$ una combinación lineal con $a, b \in R$ y $\lambda \in \mathbb{Q}$, entonces es conservativa si $\lambda > |r_i/s_i|$, donde r_i, s_i son los coeficientes de a, b resp., donde m_i es un monomio que a, b tienen en común.

Sea $p \in \mathfrak{a}$ un polinomio no nulo y sea m un monomio de p, veremos que alguna indeterminada de m está en K. Sea $q \in \mathfrak{a}$ otro polinomio y elijamos λ tal que $c := p + \lambda q$ es una combinación lineal conservativa. Como c es combinación de elementos en $\mathfrak{a}$, entonces $c \in \mathfrak{a} \subseteq (D)$, donde D es alguna dispersión. Luego todos los monomios de c están en (D), y por consecuente $m, q \in (D)$; además $q + \mu m \in D$ para todo $\mu \in R$. En consecuente $\mathfrak{a} \subseteq \mathfrak{a} + Rm \subseteq T$ y como $\mathfrak{a} + Rm$ es un ideal propio, entonces $\mathfrak{a} = \mathfrak{a} + Rm$ y $m \in \mathfrak{a}$; es decir, alguna indeterminada de m está en $\mathfrak{a}$ y luego en K. Finalmente $m \in (K)$ y como aplica para todo monomio de p, entonces $p \in (K)$ como se quería probar.

K es una dispersión: Sean $x, y \in K$ distintos, luego $x + y \in \mathfrak{a}$ y como $\mathfrak{a} \subseteq (D)$, donde D es alguna dispersión, se cumple que $x + y \in (D)$ y $x, y \in D$. Como x, y son distintos y D es dispersión, entonces $x \in E_x$ e $y \in E_y$ donde $E_x, E_y \in \mathcal{F}$ son distintos. Finalmente K es una dispersión maximal puesto que su ideal es maximal. □

2.4 Divisibilidad de polinomios

Definición 2.79 (Contenido): Sea A un DFU, definimos la aplicación $c\colon A[x] \to \mathcal{P}(A)$, llamada ***contenido del polinomio***, como aquella tal que sea d el mcd de los coeficientes no-nulos de $f \in A[x]$, entonces $c(f) = (d)$. Definimos que $c(0) = (0)$.

Decimos que un polinomio es ***primitivo*** syss $c(f) = (1)$, es decir, si sus coeficientes no nulos son coprimos. En particular, todo polinomio mónico es primitivo.

Teorema 2.80 – *Teorema de las raíces racionales*: Sea A un DFU, $K := \mathrm{Frac}(A)$ y $p(x) \in A[x]$ un polinomio no-constante:

$$p(x) = \sum_{i=0}^{n} c_i x^i.$$

Si $\alpha = a/b$, con $a, b \in A$ coprimos, es una raíz de $p(x)$, entonces $a \mid c_0$ y $b \mid c_n$.

Demostración: Como $\alpha = a/b$ es una solución

$$\sum_{i=0}^{n} \frac{a^i}{b^i} c_i = 0,$$

multiplicando por b^n y aplicando técnicas de despeje obtenemos las dos ecuaciones siguientes:

$$a^n c_n = -b \sum_{i=0}^{n-1} a^i b^{n-1-i} c_i$$
$$b^n c_0 = -a \sum_{i=1}^{n-1} a^{i-1} b^{n-i} c_i,$$

en las cuales, evidentemente los factores resultan ser elementos de A, por lo que, $b \mid a^n c_n$ y $a \mid b^n c_0$, pero como a, b son coprimos, nos resulta que $b \mid c_n$ y $a \mid c_0$ tal como lo indica el enunciado. □

Esto es útil tanto para buscar raíces racionales que con aplicar la regla de Ruffini simplifican los polinomios, como para comprobar la irracionalidad de ciertas raíces; en particular para otorgar otra demostración que $\sqrt{2} \notin \mathbb{Q}$, pero que se generaliza a que para todo primo p se cumple que $\sqrt{p} \notin \mathbb{Q}$.

Corolario 2.81: Si $p(x) \in \mathbb{Q}[x]$ es mónico, entonces sus raíces (si las tiene) son enteras.

Lema 2.82 (de primitividad de Gauss): Sea A un DFU con $f, g \in A[x]$ primitivos, entonces $f \cdot g$ es primitivo.

Demostración: Sean $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ y $g(x) = b_0 + \cdots + b_m x^m$, entonces $f \cdot g(x) = c_0 + \cdots + c_{n+m} x^{n+m}$. Sea p un número primo y digamos que divide a todos los a_i con $i < u$ y los b_i con $i < v$, entonces

$$p \mid c_{u+v} - a_u b_v = \sum_{i=0}^{u-1} b_i c_{u+v-i} + \sum_{i=0}^{v-1} b_{u+v-i} c_i$$

debido a que p divide los términos en rojo. Pero como $p \nmid a_u, b_v$ concluimos que $p \nmid c_{u+v}$. □

Teorema 2.83: Sean $f, g \in A[x]$ y $k \in A$, entonces

1. $c(kf) = (k)c(f)$.
2. $c(fg) = c(f)c(g)$.

Demostración:

1. Por propiedades del mcd.
2. Consideremos que $c(f) = a$, $c(g) = b$; por lo que $f = af^*$, $g = bg^*$ con f^*, g^* primitivas. Entonces $c(fg) = c((ab)f^*g^*) = (ab)c(f^*g^*)$. Pero por lema de primitividad de Gauss, f^*g^* es primitiva, por ende el teorema. □

Lema 2.84: Sea A un DFU con K su cuerpo de cocientes y $f, g \in A[x]$ polinomios primitivos no-constantes. f y g son asociados en $K[x]$ syss lo son en $A[x]$.

Demostración: Si lo son, entonces existen $a, b \in A$ no-nulos tales que $f = (a/b)g$, es decir, $af = bg$. Observe que

$$(a) = (a)c(f) = c(af) = c(bg) = (b)c(g) = (b),$$

por lo que a, b son asociados y existe una unidad $u \in A$ tal que $b = au$. Con esto $af = bg = aug$, por cancelación, nos queda que, efectivamente, f, g son asociados en $A[x]$. □

Teorema 2.85: Si $f \in \mathbb{k}[x]$ es de grado 2 o 3, entonces es irreductible syss no posee raíces.

Demostración: Por regla de Ruffini es claro que si es irreductible no posee raíces. Para el caso recíproco basta considerar que toda posible factorización incluye un término de grado 1. □

Teorema 2.86 – *Criterio de Irreducibilidad de Gauss*: Sea A un DFU, $K := \mathrm{Frac}(A)$ y $f \in A[x]$ un polinomio primitivo no constante. f es irreducible en $A[x]$ syss lo es en $K[x]$.

Demostración: $\Longleftarrow$. Éste caso es trivial.

$\Longrightarrow$. Supongamos que f es reducible en $K[x]$, pero no en $A(x)$, por lo que $f = gh$ con $g, h \in K[x]$. Esto significa que

$$g(x) = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i, \quad h(x) = \sum_{i=0}^{m} \frac{c_i}{d_i} x^i$$

con b_i, c_i no-nulos. Definamos $b := \prod_{i=0}^{n} b_i$ y $\tilde{b}_i := b/b_i$ con lo que $g_1(x) = \sum_{i=1}^{n} a_i \tilde{b}_i x^i$ de contenido u, por lo que $g_2 := g_1/u$. Por lo que $g = (b/u)g_2$ y $h = (d/v)h_2$, es decir,

$$f = \frac{bd}{uv} g_2 h_2$$

como u, v son no nulos, f y $g_2 h_2$ son primitivos asociados en $K[x]$, luego lo son en $A[x]$. □

Proposición 2.87: Sea k un cuerpo, $p(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ un polinomio y $A := k[x_1, \ldots, x_{n-1}]$. Escribamos p como un polinomio $p(x_n) \in A[x_n]$:

$$p(x_n) = a_0(x_1, \ldots, x_{n-1}) + \cdots + a_m(x_1, \ldots, x_{n-1}) x_n^m,$$

donde cada $a_i(x_1, \ldots, x_{n-1}) \in A$. Si $p(x_n)$ es primitivo y no puede factorizarse en polinomios de grado menor, entonces $p(x_1, \ldots, x_n)$ es irreducible.

Demostración: Sea $p(x_n) = g(x_n)h(x_n)$, luego alguno debe tener grado nulo, digamos $g(x_n)$. Como $p(x_n)$ es primitivo, entonces $g(x_n)$ es invertible. En consecuente, $p(x_1, \ldots, x_n)$ es irreducible en $A[x_n] = A[x_1, \ldots, x_n]$. □

Corolario 2.88: Sea k un cuerpo, $g, h \in k[x_1, \ldots, x_n]$ polinomios coprimos, y sea

$$f(x_1, \ldots, x_n, y) = yg(x_1, \ldots, x_n) + h(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n, y],$$

entonces f es irreducible en $k[x_1, \ldots, x_n, y]$.

Demostración: Basta notar que f es lineal en $A[y]$ con $A = k[x_1, \ldots, x_n]$, de modo que no puede factorizarse en polinomios de grado menor y como g, h son coprimos, entonces f es primitivo. □

Lema 2.89: Sea A un DFU, $k = \text{Frac}(A)$ y $f(x) \in k[x]$ no nulo. Entonces existe $c(f) \in k$ tal que $f = c(f)f^*$ con $f^* \in A[x]$ primitivo. Más aún, si existiera otro $q \in k$ tal que $f/q \in A[x]$ es primitivo, entonces existe $u \in A^\times$ tal que $q = uc(f)$.

Demostración: Denotemos

$$f(x) = \frac{a_n}{b_n}x^n + \cdots + \frac{a_0}{b_0} \in k[x],$$

donde $a_i, b_i \in A$ son coprimos para todo i. Sea $p := b_0 \cdots b_n$ tal que $pf \in A[x]$, y sea d el contenido de pf, de modo que $(p/d)f \in A[x]$ es primitivo. Luego sea $c(f) := d/p$ y vemos que satisface lo pedido.

La unicidad queda al lector. □

Proposición 2.90: Sea k un cuerpo y sea

$$f(x, y) = y^n + \frac{g_{n-1}(x)}{h_{n-1}(x)}y^{n-1} + \cdots + \frac{g_0(x)}{h_0(x)} \in k(x)[y],$$

con g_i, h_i coprimos. Sea $f^*(x, y) \in k[x][y]$ el polinomio primitivo asociado a f, entonces $\deg_y(f^*) = n$ y

$$\text{máx}\{g_i(x), h_i(x) : i \in \{0, 1, \ldots, n-1\}\} \leq \deg_x(f^*).$$

Donde $\deg_x(f^*)$ (resp. $\deg_y(f^*)$) representa la mayor potencia de x (resp. y) en f^*.

Demostración: Empleando $c(f)$ como en el lema, se obtiene que $f^* \in k[x][y]$ como se quería. Más aún, $c(f)$ es un mcm de $h_0, \ldots, h_n$; de modo que $c(f) = u_i h_i$ con $u_i \in k[x]$ para todo i. Así pues, nos queda que

$$f^*(x, y) = c(f)f(x, y) = c(f)y^n + u_{n-1}(x)g_{n-1}(x)y^{n-1} + \cdots u_0(x)g_0(x) \in k[x][y],$$

de modo que si $m := \deg_x(f^*)$, entonces

$$m = \text{máx}\{\deg_x(c(f)), \deg_x(u_i) + \deg_x(g_i)\}.$$

Como $h_i \mid c(f)$, entonces $\deg_x(h_i) \leq m$ para todo i, y es claro que $\deg_x(g_i) \leq m$ para todo i. □

Teorema 2.91: Si A es un DFU y S es un conjunto arbitrario (posiblemente infinito) de indeterminadas, entonces $A[S]$ es un DFU.

Demostración: Veamos primero el caso finito, el cual, por inducción, se reduce a ver que $A[x]$ es un DFU: Sea $p(x) \in A[x]$ un polinomio que no es inversible ni nulo, luego $p(x) = cq(x)$, de modo que $q(x)$ es primitivo. Como A es un DFU, c admite descomposición única, así que toda descomposición de $p(x)$ sólo depende de $q(x)$. Asumamos que $q(x)$ posee dos factorizaciones

$$q(x) = q_1(x) \cdots q_n(x) = r_1(x) \cdots r_m(x)$$

en irreducibles. Luego, dichas factorizaciones en irreducibles lo son en $K[x]$ por el criterio anterior, donde $K := \text{Frac}(A)$; pero $K[x]$ es un DFU, luego las factorizaciones son equivalentes en $K[x]$ y claramente también lo son en $A[x]$.

Para el caso infinito basta notar que si un polinomio posee dos factorizaciones, éstas yacen en un anillo de polinomios de finitas indeterminadas, luego son equivalentes. □

Teorema 2.92 – *Criterio de Irreducibilidad de Eisenstein*: Sean A un DFU, $K := \text{Frac}(A)$ y $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ no-constante. Sea $p \in A$ un primo, luego f es irreducible en K si:

1. $p \nmid a_n$.
2. $p \mid a_i$ para $i = 0, 1, \ldots, n-1$.
3. $p^2 \nmid a_0$.

Demostración: Supondremos que $f = af^*$ con f^* primitiva (a es una unidad en K), de modo que si fuese reducible en K existirían $g = \sum_{i=0}^{r} b_i x^i$, $h = \sum_{i=0}^{s} c_i x^i \in A[x]$ primitivos, no constantes, tales que $f^* = gh$. Nótese que $a_0^* = b_0 c_0$, por lo que $p \mid b_0$ o $p \mid c_0$, pero no ambos (restricción por construcción), por ello supondremos el primer caso.

p no puede dividir todos los b_i por ser g primitiva, así que digamos que sea k el primer índice tal que $p \nmid b_k$ con $0 < k \leq r < n$. Sabemos que $p \mid a_k = \sum_{i+j=k} b_i c_j$, además de dividir todos los términos individualmente a excepción del último, por lo que, p divide a la resta (que da como resultado $b_k c_0$), pero $p \nmid b_k$ y $p \nmid c_0$, lo que sería absurdo. □

Teorema 2.93: Sea A un dominio con $a \in A$ invertible y $b \in A$ cualquiera, entonces $p(x)$ es irreductible syss $p(ax + b)$ lo es.

Demostración: Para demostrarlo veremos que $f : A[x] \to A[x]$ donde $f(p(x)) = p(ax + b)$ es un isomorfismo de anillos. Es claro que es un homomorfismo, y como $g(x) = ax + b$ es una biyección, comprobamos el enunciado. □

Ejemplo 1 (polinomios ciclotómicos): Para todo p primo, llamamos polinomio ciclotómico p-ésimo a

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1},$$

veamos que son irreductibles en $\mathbb{Q}[x]$: Es una aplicación directa del criterio de Eisenstein usando la composición

$$\Phi_p(x + 1) = \frac{(x + 1)^p - 1}{x} = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k.$$

Nótese que el polinomio es mónico, así que p no divide al coeficiente director, mientras que el término constante es p así que $p^2 \nmid p$, y para el resto basta notar que el denominador es de la forma $n!$ con $n < p$, así que no «cancela» el término con p, luego $p \mid \binom{p}{n}$.

Usualmente se suelen aplicar en conjunto el criterio de Eisenstein con el teorema anterior para demostrar la irreductibilidad de un polinomio. Por ejemplo, utilizando el mismo polinomio que en la aplicación del algoritmo de Horner-Ruffini, $p(x) = 3x^2 + 2x + 1$, probaremos que es irreductible en $\mathbb{Q}$, primero multiplicamos todos los términos por 3 para obtener $3p(x) = 9x^2 + 6x + 3$, luego consideremos el polinomio

$$3p\left(\frac{x + 1}{3}\right) = (x + 1)^2 + 2(x + 1) + 3 = x^2 + 4x + 6.$$

que es irreductible por criterio de Eisenstein. Recuerde que 3 es una unidad de $\mathbb{Q}$ y como el polinomio original es primitivo, entonces es irreductible también en $\mathbb{Z}$.

Teorema 2.94 (criterio de irreducibilidad por reducción): Sea $\sigma\colon A \to B$ un homomorfismo entre dominios íntegros. Sean $K := \operatorname{Frac}(A)$ y $L := \operatorname{Frac}(B)$. Sea $f \in A[x]$ un polinomio tal que $\sigma(f) \neq 0$ y $\deg \sigma(f) = \deg f$. Entonces si $\sigma(f)$ es irreducible en $L[x]$, entonces $f \neq g \cdot h$ con $g, h \in A[x]$ y $\deg g, \deg h \geq 1$.

Demostración: Por contrarrecíproca: si $f = g \cdot h$ con $g, h \in A[x]$ y $\deg g, \deg h \geq 1$, entonces $\sigma(f) = \sigma(g)\sigma(h)$. Ahora bien, es claro que $\deg \sigma(g) \leq \deg g$ y $\deg \sigma(h) \leq \deg h$, pero como $\deg \sigma(f) = f$, entonces se concluye la igualdad en el caso anterior. Y sabemos que $L[x]^\times = L^\times$, por lo que $\sigma(g), \sigma(h)$ no son inversibles y por ende son divisores propios de $\sigma(f)$, es decir, $\sigma(f)$ es reducible. □

Ejemplo. Veamos que el polinomio $p(x) := x^3 + x + 1 \in \mathbb{Z}[x]$ es irreducible. Consideremos $\pi\colon \mathbb{Z} \to \mathbb{F}_2$ que es un homomorfismo, y recordemos que $\mathbb{F}_2$ es un cuerpo. Luego veamos que $\pi(p(x)) = x^3 + x + 1 = p(x) \in \mathbb{F}_2$ es irreducible. Como $p(x)$ es cúbico basta ver que no tiene raíces y $p(0) \equiv 1$ y $p(1) \equiv 1$ (mód 2), así que efectivamente es irreducible en $\mathbb{F}_2$; luego es irreducible en $\mathbb{Z}[x]$ por el criterio por reducción.

Ejemplo 2: Consideremos el polinomio $p(x) := x^4 + 1 \in \mathbb{Z}[x]$. En primer lugar, nótese que

$$(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

de modo que por el criterio de Eisenstein (con $p = 2$) se concluye que es irreducible en $\mathbb{Z}[x]$.

Ahora procedemos a probar que $p(x)$ es reducible en todo $\mathbb{F}_p[x]$ por casos:

(a) Si $-1 = a^2$ (incluye a $p = 2$): Entonces

$$x^4 + 1 = x^4 - a^2 = (x^2 - a)(x^2 + a).$$

(b) Si $p \neq 2$ y $2 = b^2$: Entonces

$$x^4 + 1 = (x^2 + 1)^2 - (bx)^2 = (x^2 + 1 - bx)(x^2 + 1 + bx).$$

(c) En otro caso: Si -1 y 2 no son cuadrados, como $\mathbb{F}_p^\times$ es cíclico, se concluye que -2 ha de ser un cuadrado. En particular $-2 = c^2$ y:

$$x^4 + 1 = (x^2+1)^2 - (cx)^2 = (x^2 + 1 - cx)(x^2 + 1 + cx).$$

Corolario 2.95: Sea A un DFU, $K := \mathrm{Frac}(A)$ y $p(x) \in A[x]$ un polinomio no-constante mónico, entonces $\alpha \in K$ es una raíz de p syss $\alpha \in A$.

§2.4.1 Raíces básicas.

Definición 2.96: Dado $\alpha \in \Bbbk$, decimos que β es una n-ésima raíz de α si $\beta^n = \alpha$ o alternativamente si β es raíz del polinomio $x^n - \alpha$.

Lema 2.97: Si β es una raíz cuadrada de α, entonces $-\beta$ y β son todas las raíces cuadradas de α.

Teorema 2.98 (Fórmula cuadrática): Si $p(x) = x^2 + rx + s$, entonces llamamos definimos $\Delta := r^2 - 4s$ como el ***discriminante*** de $p(x)$. Finalmente p tiene raíces syss existe α raíz cuadrada de Δ, en cuyo caso las raíces de p son

$$\frac{-r+\alpha}{2}, \quad \frac{-r-\alpha}{2}.$$

Demostración: Es fácil comprobar que éste es el caso, pero la deducción viene de que si

$$\begin{aligned} x^2 + rx + s = 0 &\iff x^2 + 2x \cdot \frac{r}{2} = -s \\ &\iff x^2 + 2x \cdot \frac{r}{2} + \frac{r^2}{4} = \left(x - \frac{r}{2}\right)^2 = \frac{r^2}{4} - s = \frac{\Delta}{4} \end{aligned}$$

Luego si α es raíz de Δ, entonces $\pm\alpha/2 = x - r/2$ y así se deduce el enunciado. □

Corolario 2.99: Un polinomio de grado 2 es irreductible syss su discriminante no posee raíces cuadradas.

2.5 Números complejos

Rigurosamente los números complejos emergen por las llamadas extensiones de Kronecker, que se ven más adelante, de modo que se introduce la

unidad imaginaria i como raíz del polinomio real irreductible x^2+1. Aquí haremos una definición alternativa de los números complejos que permitirá al lector acostumbrarse a ellos.

Definición 2.100 – *Números complejos*: Se define $\mathbb{C}$ como el conjunto $\mathbb{R}^2$ con las operaciones:

$$(a,b)+(c,d) := (a+c, b+d), \quad (a,b)\cdot(c,d) := (ac-bd, ad+bc).$$

Usualmente denotamos $(a,b) = a+\mathrm{i}b$. Pues $(1,0)$ se comporta como el neutro multiplicativo, $(0,0)$ como el neutro aditivo e $\mathrm{i}^2 = (0,1)^2 = (-1,0) = -1$. También se definen las funciones $\mathrm{Re}, \mathrm{Im} : \mathbb{C} \to \mathbb{R}$ como

$$\mathrm{Re}(a+\mathrm{i}b) = a, \quad \mathrm{Im}(a+\mathrm{i}b) = b,$$

las que se llaman ***parte real*** e ***imaginaria***, resp.

También, denotamos

$$|a+\mathrm{i}b| := \sqrt{a^2+b^2}, \quad \overline{a+\mathrm{i}b} := a-\mathrm{i}b,$$

donde a $|z|$ se le dice el ***valor absoluto*** de z y a $\overline{z}$ su ***conjugado*** de z.

Proposición 2.101: Para todo $z, w \in \mathbb{C}$ se cumple:

1. $|z| = 0$ syss $z = 0$.
2. $\overline{\overline{z}} = z$.
3. $|\overline{z}| = |z|$.
4. $z + \overline{z} = 2\,\mathrm{Re}\, z$ y $z - \overline{z} = 2\,\mathrm{Im}\, z$.
5. $\overline{z+w} = \overline{z} + \overline{w}$ y $\overline{z\cdot w} = \overline{z}\cdot\overline{w}$. En otras palabras, $\overline{\cdot}$ es un automorfismo de cuerpos.
6. $x \in \mathbb{R}$ syss $\overline{x} = x$ syss $\overline{\mathrm{i}x} = -x$.
7. $z\cdot\overline{z} = |z|^2$.
8. $|zw| = |z|\,|w|$.

Teorema 2.102: $(\mathbb{C}, +, \cdot)$ es un cuerpo.

Demostración: Lo único que no es obvio es que la existencia de los inversos multiplicativos, lo cual se consigue notando que si $z \in \mathbb{C}_{\neq 0}$, entonces $z^{-1} = \overline{z}/|z|^2$ mediante las propiedades anteriores. □

Teorema 2.103: La aplicación $x \mapsto (x, 0)$ es un monomorfismo de cuerpos. Esto se interpreta como que $\mathbb{C}$ contiene un subcuerpo isomorfo a $\mathbb{R}$.

Proposición 2.104: Todo complejo tiene raíz cuadrada. En consecuencia, todo polinomio cuadrático es reductible en los complejos.

Proposición 2.105: Si $P, Q \in \mathbb{C}[x]$, entonces:

1. Para todo $z \in \mathbb{C}$ que $\overline{P}(\overline{z}) = \overline{P(z)}$.
2. $P \in \mathbb{R}[x]$ syss $P(z) = \overline{P}(z)$.
3. Si $R := P \cdot Q$, entonces $\overline{R} = \overline{P} \cdot \overline{Q}$.
4. Si $P \in \mathbb{R}[x]$ tiene raíz compleja z, entonces $\overline{z}$ también es raíz.
5. $P \cdot \overline{P} \in \mathbb{R}[x]$.

Definición 2.106: Se define la función $\operatorname{cis} : \mathbb{R} \to \mathbb{C}$ tal que

$$\operatorname{cis}\theta := \cos\theta + \mathrm{i}\sin\theta.$$

Y se define $\arg : \mathbb{C}_{\neq 0} \to (-\pi, \pi]$ así:

$$\arg(x + \mathrm{i}y) = \begin{cases} \arctan(y/x), & x > 0 \\ \arctan(y/x) + \pi, & x < 0 \wedge y \geq 0 \\ \arctan(y/x) - \pi, & x < 0 \wedge y < 0 \\ \pi/2, & x = 0 \wedge y > 0 \\ -\pi/2, & x = 0 \wedge y < 0 \end{cases}$$

Proposición 2.107: Si $z \in \mathbb{C}_{\neq 0}$, entonces $z = |z| \operatorname{cis}(\arg z)$.

Teorema 2.108 – *Teorema de De Moivre*: Si $u = r \operatorname{cis}\alpha$ y $v = s \operatorname{cis}\beta$, entonces

$$u \cdot v = rs \operatorname{cis}(\alpha + \beta). \tag{2.2}$$

En particular
$$u^n = r^n \operatorname{cis}(n\alpha). \tag{2.3}$$

Demostración: Basta notar que

$$\begin{aligned} u \cdot v &= rs(\operatorname{cis}\alpha \cdot \operatorname{cis}\beta) \\ &= rs(\cos\alpha\cos\beta - \sin\alpha\sin\beta + \mathrm{i}(\sin\alpha\cos\beta + \cos\alpha\sin\beta)) \\ &= rs(\cos(\alpha+\beta) + \mathrm{i}\sin(\alpha+\beta)) = rs\operatorname{cis}(\alpha+\beta) \end{aligned}$$

como se quería probar. □

Corolario 2.109: Todo $z \in \mathbb{C}$ tiene una raíz n-ésima compleja, dada por
$$|z|^{1/n} \operatorname{cis}\left(\frac{\arg z}{n}\right).$$

Definición 2.110: Sea $n > 1$, entonces se le llaman ***raíces n-ésimas de la unidad*** a los $z \in \mathbb{C}$ tales que $z^n = 1$. Se denota también
$$\zeta_n := \operatorname{cis}(2\pi/n) = \cos(2\pi/n) + \mathrm{i}\sin(2\pi/n),$$
de modo que todas las raíces n-ésimas de la unidad son simplemente las potencias de ζ_n.

§2.5.1 El teorema fundamental del álgebra I. Usando un poco de cálculo diferencial de una variable se otorga una demostración al teorema fundamental del álgebra.

Lema 2.111: Si $f \in \mathbb{C}[x]$ es no constante, entonces $|f(z)| \to \infty$ si $|z| \to \infty$. Dicho de otro modo, para todo $R > 0$ existe $r > 0$ tal que para todo $|z| \geq r$ se cumple que $|f(z)| \geq R$.

Demostración: En particular probaremos que
$$\lim_{|z|\to\infty} \frac{|f(z)|}{|z|^n} = |c_n|$$
Esto se cumple pues si
$$f(z) = c_n z^n + \cdots + c_1 z + c_0$$
entonces
$$\frac{|f(z)|}{|z|^n} \geq |c_n| + |c_{n-1}|\,|z|^{-1} + \cdots + |c_0|\,|z|^{-n}$$

lo que converge a $|c_n|$ y que

$$|f(z)| \geq |c_n|\,|z|^n - |z|^{n-1}(|c_{n-1}| + \cdots + |c_0|\,|z|^{1-n})$$

Luego, basta exigir que $|z| > 1$ para ver que

$$\frac{|f(z)|}{|z|^n} \geq |c_n| - \frac{1}{|z|}(|c_{n-1}| + \cdots + |c_1| + |c_0|)$$

de lo que se concluye el enunciado. □

Lema 2.112: Para todo $f \in \mathbb{C}[x]$ no constante, existe x_0 que minimiza $|f(x_0)|$.

Demostración: Sea $R := |f(0)| + 1$, por el lema anterior existe r tal que para todo $|z| \leq r$ se cumple que $|f(z)| \leq R$. Luego como la imagen continua de compactos es compacta, entonces $|f|$ alcanza su mínimo en $\overline{B}_r(0)$, que es mínimo en todo el dominio. □

Teorema 2.113 – *Teorema fundamental del álgebra*: Todo polinomio no constante en $\mathbb{C}$ tiene al menos una raíz.

Demostración: Por el lema anterior todo polinomio alcanza su mínimo en módulo, así que probaremos que ese mínimo no puede ser no nulo. Sea $f \in \mathbb{C}[x]$ y x_0 el punto que le minimiza a un valor no nulo. Reemplazando $g(x) := f(x_0 + x)/|f(x_0)|$ se obtiene que $g(0) = 1$, basta probar que el mínimo de g no es 1. Sea k el mínimo natural no nulo tal que g posee un término no nulo con z^k, es decir, que g es de la forma

$$g(z) = 1 + az^k + \cdots,$$

luego, si α es una k-ésima raíz de a, entonces

$$g(\alpha z) = 1 - z^k + z^{k+1}h(z)$$

donde $h \in \mathbb{C}[x]$.
Por desigualdad triangular

$$|g(\alpha z)| \leq |1 - z^k| + |z|^{k+1}|h(z)|,$$

luego si x es un real tal que $x \in [0, 1)$, entonces

$$|g(\alpha x)| \leq 1 - x^k(1 - x|h(x)|)$$

por lo que, por límites existe un $x_1 \in (0, 1)$ tal que $x_1|h(x_1)| < 1$, por ende, $|g(\alpha x_1)| < 1$ contradiciendo la minimalidad de $g(0) = 1$. □

Notas históricas

La teoría de anillos surge principalmente como una herramienta para el desarrollo de la teoría algebraica de números en el siglo XIX. Varios matemáticos comienzan a buscar estrategias para una demostración del *Último Teorema de Fermat*. Aquí, la primera contribución fue el descubrimiento de los números complejos por **Carl Friedrich Gauss**. Inspirados en las técnicas de Gauss, dos matemáticos buscan encontrar generalizaciones o extensiones de los enteros para abordar el problema, lo que culmina en dos grandes teorías: la de los «divisores» por Kronecker (del que hablaremos más adelante), y la de los «ideales» de Dedekind.

Kronecker comienza a estudiar la idea de añadir números (irracionales) a $\mathbb{Q}$, lo que denomina «números ideales» (en sentido de «no reales»); mientras que **Richard Dedekind**, quién era estudiante de Gauss, estudia un remplazo de la propiedad de factorización única (los aquí llamados DFU's) mediante una «factorización» de unos conjuntos especiales que llama *ideales* en paralelo al trabajo de Kronecker. Ambos llegaron, independientemente, a priorizar el lugar de los ideales primos en sustitución de los números primos. Ésto sería introducido en **[37],** originalmente publicado en 1863, pero Dedekind añadiría sus capítulos suplementarios presentando su teoría de factorización en las reediciones de 1871, 1879 y 1893 respectivamente.

La definición de ideal, junto con la de *anillo*, vienen incluídas en la reedición de 1871. No obstante, Dedekind pensó al pasar de los años que «no había un sola persona interesada en leer su teoría de ideales». El problema, le pareció a Dedekind, tenía que ver con que el libro de Dirichlet tenía fines pedagógicos distintos y estaba dirigido a otra clase de audiencia, por lo cual, Dedekind consideró pertinente recolectar sus aportes en el artículo **[36]** (1876). En las otras reediciones, Dedekind se esmeró en volver su teoría más accesible y en la tercera (1879) incluye una versión general de lo que se conoce popularmente como el *lema de Gauss*, o aquí como el *criterio de irreducibilidad de Gauss*.

La teoría de Kronecker se enfoca en tratar de conseguir una identidad de Bézout sobre anillos arbitrarios,[2] o lo más cercano posible, resultado en su *teoría de divisores* (o de divisibilidad). Una revolución importante a principios del siglo XX fue la reescritura de ambas teorías por **Emmy Noether** –quien añade anotaciones a las obras de Dedekind calificando a ambas de «demasiado complicadas»–, unificándolas en el estudio de los «anillos con la

[2] Anillos en donde vale la identidad de Bézout se conocen como *anillos de Bézout*. Una equivalencia sencilla es que un anillo es de Bézout syss todo ideal finitamente generado es principal.

condición de la cadena ascendente» los cuales más tarde pasan a llamarse *anillos noetherianos* en su honor.

El teorema de las bases de Hilbert fue demostrado por **David Hilbert** en [**42**] (1890). El nombre se debe a que un sistema generador es referido como *una base* de dicho ideal. La demostración original de Hilbert era bastante no constructiva, vale decir, si bien acierta a que todo ideal en $k[x_1, \ldots, x_n]$ es finitamente generado, no construye generadores explícitos, lo cual pareció irritar al matemático Paul Gordan quién exclamó «¡Ésto no es matemáticas sino teología!». Un par de años más tarde, Hilbert dió otra demostración en [**43**] (1893) que ahora sí resultaba ser constructiva. Gordan recapacitó y, de hecho, simplificó la demostración original (no constructiva) de Hilbert en un artículo suyo y agregó «Me he convencido de que hasta la Teología tiene sus ventajas».

3

Módulos y vectores

Uno de los objetivos del álgebra lineal es el de poder desarrollar las llamadas ecuaciones lineales, para las cuales introduciremos objetos vitales bajo los nombres de *vectores* y *matrices* que se vuelven fundamentales en el contexto del álgebra lineal.

3.1 Módulos

Definición 3.1: Dado un anillo unitario A, diremos que una terna $(M, +, \cdot)$ es un ***A*-módulo** (izquierdo) si $+\colon M^2 \to M$ y $\cdot\colon A \times M \to M$ tales que $(M, +)$ es un grupo abeliano (de neutro $\vec{0}$) y para todo $\boldsymbol{u}, \boldsymbol{v} \in M$ y $\alpha, \beta \in A$ se cumple:

1. $\alpha(\beta \boldsymbol{u}) = (\alpha\beta)\boldsymbol{u}$.
2. $1\boldsymbol{u} = \boldsymbol{u}$.
3. $\alpha(\boldsymbol{u} + \boldsymbol{v}) = \alpha\boldsymbol{u} + \alpha\boldsymbol{v}$.
4. $(\alpha + \beta)\boldsymbol{u} = \alpha\boldsymbol{u} + \beta\boldsymbol{u}$.

Si A es un anillo de división entonces diremos que M es un ***A*-espacio vectorial** y a los elementos de M les diremos *vectores* y a los de A *escalares*.

En general, denotaremos los elementos de los A-módulos con letras negritas,

a los escalares con fuente normal y como excepción al $\vec{0}$ con una flechita.

Proposición 3.2: Si M es un A-módulo, entonces:

1. Para todo $\alpha \in A$ se cumple que $\alpha \cdot \vec{0} = \vec{0}$.
2. Para todo $\boldsymbol{v} \in M$ se cumple que $0 \cdot \boldsymbol{v} = \vec{0}$.
3. Para todo $\boldsymbol{v} \in M$ se cumple que $(-1)\boldsymbol{v} = -\boldsymbol{v}$.

Ejemplo 3: Son A-módulos:

- A^n con la suma y el producto por escalar coordenada a coordenada.
- $\mathrm{Func}(S; A)$ con $(f+g)(s) := f(s) + g(s)$ y $(\alpha f)(s) := \alpha \cdot f(s)$ para $\alpha \in A$ y $s \in S$.
- $A[S]$ de forma análoga a $\mathrm{Func}(S; A)$.
- I con la suma y el producto, donde I es ideal de A.
- B, donde B es un anillo tal que A es subanillo de B.

Ejemplo 4: Todo grupo abeliano es un $\mathbb{Z}$-módulo: Sea G abeliano, entonces consideramos $\boldsymbol{u} + \boldsymbol{v} := \boldsymbol{u} * \boldsymbol{v}$ (donde $*$ es la operación de grupo de G) y $n\boldsymbol{u} := (\boldsymbol{u})^n$. La notación engorrosa es solamente para ilustrar el sentido de ésta afirmación. Claramente «$(G, +)$» es un grupo abeliano de neutro «$\vec{0}$» y nótese que ya hemos probado en el primer capítulo que todos los axiomas son ciertos; ésto es lo que motiva el uso de «notación aditiva» al tratarse de grupos abelianos.

Definición 3.3 – *Morfismos de módulos*: Una aplicación $f\colon M \to N$ se dice un morfismo de A-módulos si para todo $\boldsymbol{u}, \boldsymbol{v} \in M$ y $\lambda \in A$ se comprueba

$$f(\boldsymbol{u} + \boldsymbol{v}) = f(\boldsymbol{u}) + f(\boldsymbol{v}), \quad f(\lambda \boldsymbol{u}) = \lambda f(\boldsymbol{u}).$$

Nuevamente la nomenclatura categórica se extiende a morfismos de módulos. El conjunto de morfismos de A-módulos desde M a N se denota por $\mathrm{Hom}_A(M, N)$.

Un morfismo entre espacios vectoriales se dice una ***función lineal***.

Proposición 3.4: Sea M un A-módulo. Entonces:

1. $\mathrm{Id}_M \colon M \to M$ es un morfismo de A-módulos.

2. La composición de morfismos de A-módulos es también un morfismo de A-módulos.

En consecuencia, los A-módulos (como objetos) y los morfismos de A-módulos (como flechas) conforman una categoría, denotada Mod_A. Ésto también aplica para k-espacios vectoriales, cuya categoría se denota Vect_k.

Ejemplo. Sean M, N un par de A-módulos. Entonces $\mathrm{Hom}_A(M, N)$ es un A-módulo. La construcción es similar a la de $\mathrm{Func}(S; A)$.

Proposición 3.5: Dados X, Y no vacíos se cumple que $\mathrm{Func}(X; A) \cong \mathrm{Func}(Y; A)$ syss $|X| = |Y|$. Luego, dado un cardinal κ denotamos A^κ a un A-módulo $\mathrm{Func}(S; A)$ genérico[1] con $|S| = \kappa$.

Definición 3.6 – *Submódulo*: Dado M un A-módulo, se dice que N es submódulo de M (denotado $N \leq M$) si N es también un A-módulo. Trivialmente, M y $\{\vec{0}\}$ son submódulos de M y se dicen ***impropios***. Un submódulo se dice ***simple*** (o ***irreductible***) si no admite submódulos propios.

Teorema 3.7 (Criterio del submódulo): N es submódulo del A-módulo M syss N es no vacío y para todo $\boldsymbol{u}, \boldsymbol{v} \in N$ y todo $\lambda \in A$ se cumpla que $\lambda \boldsymbol{u} + \boldsymbol{v} \in N$.

Lema 3.8: La intersección de submódulos es un submódulo.

Definición 3.9: Si $S \subseteq M$ donde M es un A-módulo, se le llama ***submódulo generado por*** S a

$$\langle S \rangle := \bigcap \{N : S \subseteq N \leq M\}.$$

Se dice que S es un ***sistema generador*** de M si $\langle S \rangle = M$.

[1] En particular consideramos la representación ordinal-conjuntista de κ.

Proposición 3.10: Se cumple que

$$\langle S\rangle = \left\{ \sum_{i=1}^{n} \lambda_i \boldsymbol{x}_i : \forall i \ (\lambda_i \in A \wedge \boldsymbol{x}_i \in S) \right\}.$$

Proposición 3.11: Si N es un submódulo del A-módulo M, entonces $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{N}$ definido porque $\boldsymbol{x} - \boldsymbol{y} \in N$ es una relación de equivalencia, bajo la cuál se denota por M/N al conjunto cociente que también resulta ser un A-módulo.

Teorema 3.12 – *Teoremas de isomorfismos*: Se cumple:

I Si M, N son A-módulos y $\varphi\colon M \to N$ un morfismo, entonces

$$\frac{M}{\ker \varphi} \cong \operatorname{Img} \varphi.$$

II Si S, T son submódulos del A-módulo M, entonces

$$\frac{S}{S \cap T} \cong \frac{S+T}{T}.$$

III Si $S \leq T \leq M$, entonces

$$\frac{M}{T} \cong \frac{M/S}{T/S}.$$

IV (de la correspondencia) Si $N \leq M$, entonces:

$$\begin{aligned} \{T : N \leq T \leq M\} &\longrightarrow \{S : S \leq M/N\} \\ T &\longmapsto T/N \end{aligned}$$

es una biyección. Más aún, $S \subseteq T$ syss $\frac{S+N}{N} \leq \frac{T+N}{N}$.

Definición 3.13 (Suma de submódulos): Si $\{N_i\}_{i\in I}$ son submódulos de M, entonces se define su suma como

$$\sum_{i\in I} N_i := \left\langle \bigcup_{i\in I} N_i \right\rangle,$$

en particular $S + T := \langle S \cup T\rangle$.

Se dice que una familia de submódulos $\{N_i\}_{i\in I}$ es ***independiente*** si para todo $i \in I$ se cumple que $N_i \cap \sum_{j\neq i} N_j = \{0\}$. La suma de una familia independiente de submódulos se dice ***directa*** y se denota como $\bigoplus_{i\in I} N_i$.

Teorema 3.14: Sea M un A-módulo y $\{N_i\}_{i\in I}$ una familia de submódulos tales que $M = \sum_{i\in I} N_i$, son equivalentes:

a) $M = \bigoplus_{i\in I} N_i$.

b) Si $\sum_{i\in I} \boldsymbol{m}_i = \vec{0}$ con $\boldsymbol{m}_i \in N_i$ para todo $i \in I$, entonces $\boldsymbol{m}_i = \vec{0}$.

c) Para todo $\boldsymbol{m} \in M$ existen unos únicos $\boldsymbol{m}_i \in N_i$ para cada $i \in I$ tales que

$$\boldsymbol{m} = \sum_{i\in I} \boldsymbol{m}_i.$$

Demostración: *a*) $\implies$ *b*). Procedemos a demostrarlo por contradicción, supongamos que existe un subconjunto $J \subseteq I$ tal que

$$\sum_{j\in J} \boldsymbol{m}_j = \vec{0}$$

con $\boldsymbol{m}_j \neq \vec{0}$ para todo $j \in J$. Tomemos un $j_0 \in J$ tal que $\boldsymbol{m}_{j_0} \neq \vec{0}$, evidentemente $\boldsymbol{m}_{j_0} = \sum_{j\in J\setminus\{j_0\}} -\boldsymbol{m}_j$. Luego

$$\boldsymbol{m}_{j_0} \in N_{j_0} \cap \sum_{j\in J\setminus\{j_0\}} N_j \subseteq N_{j_0} \cap \sum_{i\in I\setminus\{j_0\}} N_i.$$

b) $\implies$ *c*). Consideraremos el siguiente homomorfismo

$$\begin{aligned} f\colon \prod_{i\in I} N_i &\longrightarrow M \\ (\boldsymbol{m}_i)_{i\in I} &\longmapsto \sum_{i\in I} \boldsymbol{m}_i, \end{aligned}$$

por construcción, sabemos que corresponde a un epimorfismo, y la propiedad *b*) nos asegura que $\ker f = (\vec{0})_{i\in I}$, por ende es un monomorfismo.

c) $\implies$ *a*). También por contradicción, sea $\boldsymbol{m} \in M$ con dos descomposiciones

$$\boldsymbol{m} = \sum_{i\in I} \boldsymbol{m}_i = \sum_{i\in I} \boldsymbol{n}_i.$$

Luego para algún $i \in I$ ha de darse que $\boldsymbol{m}_i \neq \boldsymbol{n}_i$, luego

$$\vec{0} \neq \boldsymbol{m}_i - \boldsymbol{n}_i = \sum_{j \neq i} \boldsymbol{n}_j - \boldsymbol{m}_j$$

luego $\boldsymbol{m}_i - \boldsymbol{n}_i \in N_i \cap \sum_{j \neq i} N_j$ que es absurdo. □

3.2 Módulos libres y bases

Definición 3.15: Sea M un A-módulo con $X \subseteq M$. Diremos que X es ***libre*** o que sus elementos son ***linealmente independientes*** syss la ecuación

$$\lambda_0 \boldsymbol{x}_0 + \cdots + \lambda_n \boldsymbol{x}_n = \vec{0}$$

se da con $\boldsymbol{x}_i \in X$ distintos dos a dos y $\lambda_i \in A$ siempre que $\lambda_i = 0$ para todo $i = 0, \ldots, n$. De lo contrario decimos que el conjunto está ***ligado*** o que hay elementos que son ***linealmente dependientes*** entre sí.

Si, X es un conjunto libre y además es un sistema generador, diremos que X es una ***base*** de dicho módulo. Si M posee alguna base, entonces, se dice que es ***libre***.

Ejemplo 5: Es fácil notar que con la suma y producto normal $\mathbb{Q}$ es un $\mathbb{Z}$-módulo, sin embargo, no es libre (¿por qué?).

§3.2.1 Finitamente generados.

Definición 3.16: Se dice que un A-módulo M es ***finitamente generado*** si posee un sistema generador finito. Otra manera de decir lo mismo, pero que será útil más adelante, es que existe alguna tupla $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ tal que el morfismo de módulos

$$\begin{aligned} \varphi \colon A^n &\longrightarrow M \\ (\lambda_1, \ldots, \lambda_n) &\longmapsto \lambda_1 \boldsymbol{x}_1 + \cdots \lambda_n \boldsymbol{x}_n \end{aligned}$$

es suprayectivo.

Ejemplo. Consideremos $\mathbb{Q}[x]$ que, como ya vimos, corresponde a un $\mathbb{Q}$-espacio vectorial o un $\mathbb{Q}$-módulo. Nótese sin embargo que no está finitamente generado, puesto que si $\{p_1(x), \ldots, p_n(x)\}$ es un subconjunto finito de polinomios sobre $\mathbb{Q}$ basta tomar d como el grado máximo entre ellos y notar que $x^{d+1} \in \mathbb{Q}[x]$ no está generado por ellos.

Teorema 3.17: Sea M un A-módulo, entonces $M \cong A^n$ syss posee una base de cardinal n.

Demostración: Notemos que si X es una base cualquiera de M, entonces

$$M = \bigoplus_{\boldsymbol{x}\in X} \langle \boldsymbol{x} \rangle;$$

luego es isomorfo a $\prod_{\boldsymbol{x}\in X} \langle \boldsymbol{x} \rangle$ y $\langle \boldsymbol{x} \rangle \cong A$ trivialmente para todo $\boldsymbol{x} \in X$. □

Desde aquí en adelante veremos resultados casi exclusivamente para espacios vectoriales:

Lema 3.18: Si S es ligado en un espacio vectorial, entonces existe un $\boldsymbol{v} \in S$ que es generado por el resto, es decir, tal que $\boldsymbol{v} \in \langle S \setminus \{\boldsymbol{v}\} \rangle$.

Teorema 3.19: Si G es un sistema generador ligado, entonces $\boldsymbol{v} \in G$ está generado por el resto de G syss $G \setminus \{\boldsymbol{v}\}$ es un sistema generador. Si S es libre en un espacio vectorial y $\boldsymbol{v}$ no es generado por S, entonces $S \cup \{\boldsymbol{v}\}$ es libre.

Corolario 3.20: Todo sistema generador finito en un espacio vectorial contiene una base. En consecuencia, todo espacio vectorial finitamente generado es libre.

Teorema 3.21: Todo par de bases de un espacio vectorial finitamente generado posee el mismo cardinal.

Demostración: Sean $X := \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ e Y bases tal que $|X| \leq |Y|$ (en principio, Y podría ser infinito). Sea $\boldsymbol{y}_1 \in Y$ cualquiera, como $\boldsymbol{y}_1 \in V = \langle X \rangle$, entonces existen $\alpha_{1,i} \in \Bbbk$ tales que

$$\boldsymbol{y}_1 = \sum_{i=1}^{n} \alpha_{1,i} \boldsymbol{x}_i$$

como $\boldsymbol{y}_1 \neq 0$ algún $\alpha_{1,i}$ ha de ser no nulo y reordenando supongamos que $\alpha_{1,1} \neq 0$, luego

$$\boldsymbol{x}_1 = \frac{1}{\alpha_{1,1}} \boldsymbol{y}_1 - \sum_{i=2}^{n} \frac{\alpha_{1,i}}{\alpha_{1,1}} \boldsymbol{x}_i,$$

llamando $B_0 := X$ y $B_1 := B_0 \setminus \{\boldsymbol{x}_1\} \cup \{\boldsymbol{y}_1\}$, como $X \subseteq \langle B_1 \rangle$, entonces B_1 es base y posee n elementos.

Análogamente se escoge $\boldsymbol{y}_2 \in Y \subseteq V = \langle B_1 \rangle$, luego existen $\alpha_{2,i} \in \Bbbk$ tales que

$$\boldsymbol{y}_2 = \alpha_{2,1}\boldsymbol{y}_1 + \sum_{i=2}^{n} \alpha_{2,i}\boldsymbol{x}_i$$

notamos que algún $\alpha_{2,i}$ con $i > 1$ ha de ser no nulo y reordenamos para que $\alpha_{2,2} \neq 0$, luego

$$\boldsymbol{x}_2 = \frac{1}{\alpha_{2,2}} - \left(\frac{\alpha_{2,1}}{\alpha_{2,1}}\boldsymbol{y}_1 + \sum_{i=3}^{n} \frac{\alpha_{2,i}}{\alpha_{2,2}}\boldsymbol{x}_i \right),$$

de modo que si $B_2 := B_1 \setminus \{\boldsymbol{x}_2\} \cup \{\boldsymbol{y}_2\}$ entonces B_2 es base.

Iterando el proceso anterior, B_n resulta ser base y estar formado solamente a partir de elementos de Y, luego $Y = B_n$ pues de tener elementos aparte sería ligado y es claro que B_n posee n elementos. □

Corolario 3.22: Todo conjunto libre en un espacio vectorial finitamente generado se puede extender a una base.

Definición 3.23 – *Dimensión*: Si V es un $\Bbbk$-espacio vectorial y sus bases son equipotentes, entonces denotamos por $\dim_{\Bbbk} V$ al cardinal de cualquiera de ellas.

Corolario 3.24: Si S es libre en un espacio vectorial de dimensión finita n y S posee n elementos, entonces S es base.

Teorema 3.25: Si V, W son $\Bbbk$-espacios vectoriales que comparten dimensión finita, entonces son isomorfos. En consecuencia si $n := \dim_{\Bbbk} V$, entonces $V \cong \Bbbk^n$.

Definición 3.26 – *Base canónica*: Se le llama ***base canónica*** de $\Bbbk^n$ como $\Bbbk$-espacio vectorial a la base ordenada $(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$ donde

$$\boldsymbol{e}_i := (0, \ldots, \underset{(i)}{1}, \ldots, 0).$$

Por ejemplo, la base canónica de $\Bbbk^2$ es

$$\boldsymbol{e}_1 := (1,0), \qquad \boldsymbol{e}_2 := (0,1).$$

La base canónica será útil ya que en lugar de hablar de espacios vectoriales abstractos de dimensión finita podemos simplemente usar a $\Bbbk^n$ con la base canónica.

§3.2.2 Espacios de dimensión infinita. Es sencillo notar que para todo cuerpo $\Bbbk$ se cumple que $\Bbbk[x]$ es un $\Bbbk$-espacio vectorial y que $\{1, x, x^2, \dots\}$ es una base, sin embargo, generalizar sus propiedades es mucho más difícil que en el caso finito e inevitablemente hay que recurrir al axioma de elección.

Teorema 3.27: Son equivalentes:

1. **El axioma de elección.**
2. Todo conjunto libre en un espacio vectorial está contenido en una base.
3. Todo espacio vectorial es un módulo libre.

Demostración: (1) $\implies$ (2). Aplicamos el lema de Zorn: Sea S un conjunto libre, luego se define $\mathcal{F}$ como la familia de conjuntos libres que contienen a S, es claro que $\mathcal{F}$ está parcialmente ordenado por la inclusión, y por el lema anterior un elemento maximal de $\mathcal{F}$ sería una base que conteniera a S. Sea $\mathcal{C}$ una cadena de $\mathcal{F}$ hay que probar que $T := \bigcup \mathcal{C} \in \mathcal{F}$ para poder aplicar el lema de Zorn, y es claro que $S \subseteq T$, luego sólo falta probar que T es libre, lo que queda al lector (Hint: Use prueba por contradicción).

(2) $\implies$ (3). Trivial.

(3) $\implies$ (1). Probaremos que implica el axioma de elecciones múltiples, que es equivalente al AE: Sea $\{X_i : i \in I\}$ una familia de conjuntos no vacíos, hemos de probar que existe $\{F_i : i \in I\}$ tal que $F_i \subseteq X_i$ y los F_is son finitos. Definamos $X := \bigcup_{i\in I} X_i$, si $\Bbbk$ es un cuerpo arbitrario, entonces $\Bbbk(X)$ es el cuerpo de polinomios con indeterminadas en X. Se le llama i-grado de un monomio a la suma de exponentes de las indeterminadas de X_i. Se dice que una función racional $f \in \Bbbk(X)$ es i-homogéneo de grado d si todos los monomios del denominador tienen un i-grado común de n y los del numerador un i-grado común de $n+d$. Denotamos K al subconjunto de $\Bbbk(X)$ conformado por las funciones racionales i-homogéneas de grado 0 para todo $i \in I$; K resulta ser un subcuerpo estricto de $\Bbbk(X)$ (¿por qué?), luego $\Bbbk(X)$ es un K-espacio vectorial. Finalmente denotamos por V al K-subespacio de

$\Bbbk(X)$ generado por X, y por B a una base de V.
Por definición de B y en particular para $x \in X_i$ existe un subconjunto finito $B(x)$ de B tal que

$$x = \sum_{v \in B(x)} \lambda_{v,x} v$$

donde $\lambda_{v,x} \in K_{\neq 0}$. Nótese que si $y \in X_i$ es distinto de x, entonces

$$y = (y/x)\, x = \sum_{v \in B(x)} (y/x \cdot \lambda_{v,x}) v$$

donde $y/x \cdot \lambda_{v,x} \in K_{\neq 0}$, luego los $B(x)$ y los $\lambda_{v,x}/x$ son fijos para un X_i fijo, por lo que le denotamos por B_i y $\beta_{v,i}$ resp.
Finalmente $\beta_{v,i}$ es i-homogéneo de grado -1 y j-homogéneo de grado 0 para todo $j \neq i$. Así que $\beta_{v,i}$ debe tener finitos términos de X_i, luego llamamos F_i al subconjunto de X_i que tienen términos en algún $\beta_{v,i}$ para algún $v \in B_i$. □

Teorema 3.28: Son equivalentes:

1. **El axioma de elección**.

2. En un espacio vectorial, todo generador contiene una base.

Pista: Siga la prueba anterior. □

Ejemplo 6 (bases de Hamel): Si se asume el AE, $\mathbb{R}$ como $\mathbb{Q}$-espacio vectorial tiene una base H, usualmente llamada ***de Hamel***. Queda al lector probar que todas las bases de Hamel no son ni finitas ni numerables. No sólo es complejo, sino imposible construir manualmente una base de Hamel, puesto que se ha demostrado que la existencia de esta base es independiente a la teoría elemental ZF. Algunos textos prueban que las bases de Hamel son conjuntos tan «raros» que las hay tanto Lebesgue-medibles como no.

Teorema (AE) 3.29: Todo par de bases de un espacio vectorial son equipotentes.

Demostración: Sean X, Y bases del espacio, podemos suponer que ambas son infinitas, pues el caso restante ya fue probado. Para todo $x \in X$ admitamos que Y_x es un subconjunto finito de Y tal que $x \in \langle Y_x \rangle$, notemos que $Y' := \bigcup_{x \in X} Y_x$ cumple que $X \subseteq \langle Y' \rangle$, de modo que Y' es base, luego $Y = Y'$. Como se asume AE cada Y_x puede ser enumerado y como son finitos

los índices han de ser naturales, de modo que se puede definir $f\colon Y \to X \times \mathbb{N}$ tal que $f(y)$ es un par (x, i) donde y es el i-ésimo elemento de Y_x. Nótese que f es inyectiva, para finalizar, como X es infinito y se asume AE se cumple que $\aleph_0 \leq |X|$, de modo que $|X \times \mathbb{N}| = |X|$ y existe una biyección $g : X \times \mathbb{N} \to X$, luego $f \circ g : Y \to X$ es una inyección, y análogamente se construye otra inyección desde X a Y. Finalmente, por el teorema de Cantor-Schröder-Bernstein, existe una biyección entre X e Y, que es lo que se quería probar. □

Observe que, al contrario del caso finito, un conjunto libre puede tener cardinal la dimensión y no ser base. En efecto, basta tomar una base de cardinal infinito y quitarle un elemento cualquiera como ejemplo.

§3.2.3 Fórmulas con la dimensión.

Teorema 3.30: Si V es un espacio vectorial y $W \leq V$, entonces:

1. $\dim V = \dim W + \dim(V/W)$.
2. Si $\dim V = \dim W$ y es finito, entonces $V = W$.

Demostración:

1. Sea B_W una base de W, sabemos que se puede extender a una base B_V de V, simplemente basta ver que $B := \{[\boldsymbol{v}] : \boldsymbol{v} \in B_V \setminus B_W\}$ conserva el cardinal deseado y que es base de V/W. Sean $\boldsymbol{u}, \boldsymbol{v} \in B_V \setminus B_W$, si $[\boldsymbol{u}] = [\boldsymbol{v}]$ entonces $\boldsymbol{u} - \boldsymbol{v} \in W$, luego B_V sería ligado lo que es absurdo, análogamente se prueba que B es libre. Para notar que B es un sistema generador, basta considerar que todo $[\boldsymbol{v}] \in V/W$ se escribe como

$$\boldsymbol{v} = \sum_{i=1}^{n} \lambda_i \boldsymbol{e}_i$$

donde $e_i \in B_V$, luego

$$[\boldsymbol{v}] = \sum_{i=1}^{n} \lambda_i [\boldsymbol{e}_i],$$

donde $[\boldsymbol{e}_i]$ o pertenece a B, o es nulo, en cuyo caso podemos omitirle. De este modo, es claro que B es base.

2. Si B es base de W y tiene el mismo cardinal de $\dim V$ que es finito, entonces es base de V, de modo que $V = \langle B \rangle = W$. □

Teorema 3.31 – *Fórmula de Grassman*: Si $A, B \leq V$ con V un espacio vectorial, entonces

$$\dim A + \dim B = \dim(A + B) + \dim(A \cap B).$$

Teorema 3.32: Si $f : V \to W$ es lineal, entonces

$$\dim V = \dim(\ker f) + \dim(\operatorname{Img} f).$$

3.3 Matrices y transformaciones lineales

Teorema 3.33: Sea $f : X \to N$ donde X es base de un A-módulo M y N es otro A-módulo. Entonces existe un único homomorfismo de módulos $\bar{f} : M \to N$ tal que $\bar{f}|_X = f$.

Teorema 3.34: Si $f \in L(V, W)$, entonces:

1. f es inyectiva syss $\ker f = \{0\}$.
2. f es suprayectiva syss su imagen contiene a alguna base, y por ende a todas ellas.
3. En particular, si $n := \dim V = \dim W < +\infty$ entonces f es un isomorfismo de módulos syss es inyectiva o suprayectiva, lo que se reduce a ver que $\dim \ker f = 0$ o $\dim \operatorname{Img} f = n$.

Corolario 3.35: Dos espacios vectoriales son isomorfos syss comparten dimensión.

Definición 3.36: Si $B := (e_i)_{i \in I}$ es una base (ordenada) de un A-módulo M, entonces $\pi_i^B : M \to A$ son la serie de aplicaciones tal que para todo $v \in M$ se cumple que

$$v = \sum_{i \in I} \pi_i^B(v) e_i.$$

Sabemos que para cada $i \in I$, las proyecciones π_i^B están bien definidas. Se define $\pi^B : M \to A^I$ la función tal que $\pi^B(v) := (\pi_i^B(v))_{i \in I}$.

De este modo si $v = 2e_1 + 3e_2 - 1e_3$ donde $B := (e_1, e_2, e_3)$ es una base ordenada de un módulo que contiene a v, entonces $\pi^B(v) = (2, 3, -1)$.

Proposición 3.37: Si $X := (x_1, \ldots, x_n)$ es base ordenada de M, entonces

1. Para todo i se cumple que π_i^X es un funcional.
2. Para todo i, j se cumple que $\pi_i^X(x_j) = \delta_{ij}$.
3. π^X es un isomorfismo con A^n.

Por ello en lugar de denotar un A-módulo de dimensión finita denotaremos A^n.

Supongamos entonces que si $f : M \to N$ es un morfismo de módulos y M es libre, entonces f queda completamente determinado por una tupla de N correspondiente a la imagen de la base. Si además N es libre, entonces cada vector de N puede escribirse como una tupla de valores del anillo A. En sintesis, si el dominio y codominio son libres todo el homomorfismo se reduce a tuplas de tuplas de valores de A. Esto sucede más fácilmente si nos restringimos a espacios vectoriales, y en particular si éstos son de dimensión finita, en cuyo caso se cumple que toda la transformación lineal puede reducirse a $n \cdot m$ escalares, donde n es la dimensión del dominio y m la del codominio.

Definición 3.38 – *Matrices*: Una matriz M sobre un anillo unitario A de orden $n \times m$ es una función $M : \{1, \ldots, n\} \times \{1, \ldots, m\} \to A$, donde solemos denotar $M(i, j)$ como M_{ij}. a éstos últimos valores les decimos sus *coeficientes*. El conjunto de matrices sobre A de $n \times m$ se denota $\mathrm{Mat}_{n\times m}(A)$. El conjunto $\mathrm{Mat}_{n\times m}(A)$ es un A-módulo, en donde:

1. $(B + C)_{ij} := B_{ij} + C_{ij}$ para todo $B, C \in \mathrm{Mat}_{n\times m}(A)$.
2. $(\lambda B)_{ij} := \lambda B_{ij}$ para todo $B \in \mathrm{Mat}_{n\times m}(A)$ y $\lambda \in A$.

La diagonal de una matriz se le llama al conjunto de coeficientes de coordenadas (i, i).

Si $B \in \mathrm{Mat}_{n\times m}(A)$ y $C \in \mathrm{Mat}_{m\times p}(A)$, se define su producto interno como:

$$(B \cdot C)_{ij} := \sum_{k=1}^{m} B_{ik} C_{kj}$$

Dado $B \in \mathrm{Mat}_{n\times m}(A)$ se define su ***matriz traspuesta*** como $B^t \in \mathrm{Mat}_{m\times n}(A)$ tal que $(B^t)_{i,j} := B_{j,i}$.

Se les llama matrices:

Cuadradas A las de orden $n \times n$. Se denota $\mathrm{Mat}_n(A) := \mathrm{Mat}_{n\times n}(A)$.

Simétricas A las matrices cuadradas B tal que $B = B^t$.

Antisimétricas A las matrices cuadradas B tal que $B = -B^t$.

Diagonales A las que tienen coeficientes nulos en todas las coordenadas exceptuando tal vez la diagonal.

Escalares A las matrices diagonales que en la diagonal sólo contienen un valor escalar.

Identidad A la matriz escalar con valor 1. La matriz identidad de orden $n \times n$ se denota I_n.

Nula A la matriz escalar con valor 0.

Por lo general, denotaremos los valores de la matriz en una tabla, por ejemplo

$$M := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \in \mathrm{Mat}_{2\times 3}(\mathbb{Q})$$

donde $M_{2,1} = 4$.

Cabe destacar que si

$$B_{ij} = f(i,j)$$

para todo i, j; entonces también denotaremos

$$B = [f(i,j)]_{ij}$$

de modo que, por ejemplo

$$I_n = [\delta_{ij}]_{ij}.$$

En general admitiremos que A^n corresponde a $\mathrm{Mat}_{1\times n}(A)$, de modo que $\pi^X(\boldsymbol{v}) \in \mathrm{Mat}_{1\times n}(A)$.

Proposición 3.39: $\mathrm{Mat}_{n\times m}(A)$ es un A-módulo libre de rango nm.

Proposición 3.40: Si B, C, D son matrices de orden apropiado en cada caso, se cumple:

1. $B \cdot (C \cdot D) = (B \cdot C) \cdot D$ (asociatividad).
2. $B \cdot (C + D) = B \cdot C + B \cdot D$ (distributividad izquierda).
3. $(B + C) \cdot D = B \cdot D + C \cdot D$ (distributividad derecha).
4. Si B es de orden $n \times m$, entonces $I_n \cdot B = B \cdot I_m = B$ (neutro).
5. $\mathrm{Mat}_n(A)$ es un anillo unitario de neutro aditivo la matriz nula y neutro multiplicativo la matriz identidad.

Proposición 3.41: Si B, C son matrices de orden apropiado en cada caso, se cumple:

1. $(B^t)^t = B$.
2. $(B + C)^t = B^t + C^t$.
3. $(\lambda B)^t = \lambda B^t$ para todo $\lambda \in A$.
4. Si A es conmutativo, entonces $(B \cdot C)^t = C^t \cdot B^t$.
5. Si B es cuadrada e invertible, entonces $(B^{-1})^t = (B^t)^{-1}$.

Definición 3.42: Si $f \in L(\Bbbk^n, \Bbbk^m)$, y $X := (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n), Y := (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ son bases ordenadas de $\Bbbk^n$ y $\Bbbk^m$ resp., entonces denotamos $\mathrm{M}_X^Y(f)$ a la matriz de orden $n \times m$ a aquella tal que sus columnas son las imagenes ordenadas de la base X, dicho de otro modo que $\mathrm{M}_X^Y(f) := \left[\pi_j^Y\left(f(\boldsymbol{x}_i)\right)\right]_{ij}$.

Teorema 3.43: Sean $f \in L(\Bbbk^n, \Bbbk^m)$, X e Y bases ordenadas de $\Bbbk^n$ y $\Bbbk^m$ resp., entonces $B = \mathrm{M}_X^Y(f)$ syss para todo $\boldsymbol{v} \in \Bbbk^n$ se cumple:

$$\pi^Y(f(\boldsymbol{v})) = \pi^X(\boldsymbol{v}) \cdot B.$$

Demostración: $\Longrightarrow$. Sea $X = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$, $\boldsymbol{v} = \sum_{i=1}^n v_i \boldsymbol{x}_i$ y $B := \mathrm{M}_X^Y(f)$, luego como f es lineal se cumple que

$$f(\boldsymbol{v}) = \sum_{i=1}^n v_i f(\boldsymbol{x}_i).$$

Las proyecciones son también lineales, luego

$$\pi_j^Y(f(\boldsymbol{v})) = \sum_{i=1}^{n} v_i \pi_j^Y[f(\boldsymbol{x}_i)] = \sum_{i=1}^{n} v_i b_{ij} = (\pi^X(\boldsymbol{v}) \cdot B)_{1j},$$

como se quería probar.

$\Longleftarrow$. Si se cumple para todo vector, en particular se cumple para los vectores de la base X y claramente

$$\left(\mathrm{M}_X^Y(f)\right)_{ij} = \pi_j^Y(f(\boldsymbol{x}_i)) = \sum_{k=1}^{n} \delta_{ik} b_{kj} = b_{ij}$$

ergo $B = \mathrm{M}_X^Y(f)$. □

Ejemplo (matriz cambio de base). Sea V un $\Bbbk$-espacio vectorial de dimensión n. Sean $X, Y = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ bases ordenadas de V, luego

$$\pi^X(\boldsymbol{v}_i) = \pi^X(\mathrm{Id}(\boldsymbol{v}_i)) = \pi^Y(\boldsymbol{v}_i) \cdot \mathrm{M}_Y^X(\mathrm{Id}) = \boldsymbol{e}_i \, \mathrm{M}_Y^X(\mathrm{Id}) = [\mathrm{M}_X^Y(\mathrm{Id})]_{i,*}.$$

Teorema 3.44: Si f, g son funciones lineales y X, Y, Z son bases ordenadas adecuadas a las dimensiones en cada caso, se cumple:

1. $\mathrm{M}_X^X(\mathrm{Id}) = I_n$, donde $n = |X|$.
2. Para todo λ escalar se cumple $\mathrm{M}_X^Y(\lambda f) = \lambda \, \mathrm{M}_X^Y(f)$.
3. $\mathrm{M}_X^Y(f + g) = \mathrm{M}_X^Y(f) + \mathrm{M}_X^Y(g)$.
4. $\mathrm{M}_X^Z(f \circ g) = \mathrm{M}_X^Y(f) \cdot \mathrm{M}_Y^Z(g)$.
5. Son equivalentes:
   a) f es invertible.
   b) Para algún par de bases ordenadas X, Y se da que $\mathrm{M}_X^Y(f)$ es invertible.
   c) Para todo par de bases ordenadas X, Y se da que $\mathrm{M}_X^Y(f)$ es invertible.
6. $L(\Bbbk^n, \Bbbk^m) \cong \mathrm{Mat}_{n \times m}(\Bbbk) \cong \Bbbk^{nm}$. En particular, $L(\Bbbk^n, \Bbbk) \cong \Bbbk^n$.

Los últimos dos son los que justifican la definición de matrices.

Ejemplo. Si X, Y son bases ordenadas de $\mathbb{k}^n$, entonces

$$I_n = \mathrm{M}_X^X(\mathrm{Id}) = \mathrm{M}_X^Y(\mathrm{Id}) \cdot \mathrm{M}_Y^X(\mathrm{Id}).$$

Luego si $B \in \mathrm{Mat}_n(\mathbb{k})$ es invertible, entonces representa a una única matriz de cambio de base. De hecho, todo endomorfismo $f \in L(\mathbb{k}^n)$ está representado por la familia

$$\mathrm{M}_Y^Y(f) = \mathrm{M}_Y^X(\mathrm{Id}) \cdot \mathrm{M}_X^X(f) \cdot \mathrm{M}_X^Y(\mathrm{Id}).$$

Teorema 3.45: Si $B \in \mathrm{Mat}_n(\mathbb{k})$, entonces son equivalentes:

1. B es invertible.
2. Para todo $\boldsymbol{v} \in \mathbb{k}^n$ se cumple que $\boldsymbol{v} \cdot B = 0$ implica $\boldsymbol{v} = 0$.

Demostración: $\Longrightarrow$. Si B es invertible entonces sea B^{-1} su inversa, luego $v = (v \cdot B)B^{-1} = 0 \cdot B^{-1} = 0$.

$\Longleftarrow$. Si X es la base canónica, entonces $f(\boldsymbol{v}) := \boldsymbol{v} \cdot B$ claramente es lineal y cumple que $B = \mathrm{M}_X^X(f)$ (¿por qué?). Si $f^{-1}(\mathbf{0}) = \{\mathbf{0}\}$, entonces $\dim \ker f = 0$, luego $\dim \mathrm{Img}\, f = n$ y f es una biyección, luego es invertible, y por el teorema anterior, cualquiera de sus representaciones matriciales (en particular, B) lo son. □

3.4 Determinante

Definición 3.46 – *Forma multilineal*: Se dice que una función $f : (A^n)^n \to A$ es una ***forma multilineal*** si es lineal coordenada a coordenada, es decir, si para todo $v_1, \ldots, v_n, v \in A^n$ y todo $\lambda \in A$ se cumple que

$$f(v_1, \ldots, \underset{(i)}{v_i + \lambda v}, \ldots, v_n) = f(v_1, \ldots, v_n) + \lambda f(v_1, \ldots, \underset{(i)}{v}, \ldots, v_n).$$

Además, una forma multilineal se dice ***antisimétrica*** si intercambiar dos vectores de coordenadas cambia el signo, es decir si

$$f(v_1, \ldots, \underset{(i)}{v_i}, \ldots, \underset{(j)}{v_j}, \ldots, v_n) = -f(v_1, \ldots, \underset{(i)}{v_j}, \ldots, \underset{(j)}{v_i}, \ldots, v_n).$$

Y también se dice ***alternada*** si es nula si un vector aparece en más de

una coordenada, es decir si

$$f(v_1, \ldots, \underset{(i)}{v}, \ldots, \underset{(j)}{v}, \ldots, v_n) = 0.$$

Proposición 3.47: Si f es una forma multilineal entonces:

1. Toma valor nulo si alguna coordenada es nula.
2. Si es alternada, entonces es antisimétrica.
3. Si es antisimétrica y el campo escalar no tiene característica 2, entonces es alternada.
4. Es antisimétrica syss para todo $\sigma \in S_n$ y todo $(v_1, \ldots, v_n) \in (A^n)^n$ se cumple:
$$f(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = (\operatorname{sgn}\sigma) \cdot f(v_1, \ldots, v_n).$$

Teorema 3.48: Para todo $a \in A$ existe una única forma multilineal f tal que $f(e_1, \ldots, e_n) = a$. Y de hecho, si todo $v_i := (v_{i1}, \ldots, v_{in})$, entonces dicha forma multilineal viene dada por

$$f(v_1, \ldots, v_n) = a \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \cdot v_{1\sigma(1)} \cdots v_{n\sigma(n)}.$$

DEMOSTRACIÓN: Utilizando la notación del enunciado $v_i = \sum_{j=1}^n v_{ij} e_j$, luego

$$\begin{aligned} f(v_1, \ldots, v_n) &= \sum_{j=1}^n v_{1j} f(e_j, v_2, \ldots, v_n) \\ &= \sum_{j_1=1}^n \sum_{j_2=1}^n v_{1j_1} v_{2j_2} f(e_{j_1}, e_{j_2}, v_3, \ldots, v_n) \\ &= \sum_{j_1=1}^n \cdots \sum_{j_n=1}^n v_{1j_1} \cdots v_{nj_n} f(e_{j_1}, \ldots, e_{j_n}). \end{aligned}$$

Notemos que podemos reemplazar los j_k por funciones desde $\{1, \ldots, n\}$ a $\{1, \ldots, n\}$, sin embargo, si las funciones no son inyectivas, entonces nos queda la forma multilineal de una tupla con coordenadas repetidas, lo que por

definición de alternada es nulo, luego podemos solo considerar los j_k como permutaciones de n elementos y nos queda:

$$\begin{aligned} f(v_1, \ldots, v_n) &= \sum_{\sigma \in S_n} v_{1\sigma(1)} \cdots v_{n\sigma(n)} f(e_{\sigma(1)}, \ldots, e_{\sigma(n)}) \\ &= a \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot v_{1\sigma(1)} \cdots v_{n\sigma(n)} \end{aligned}$$ □

Nótese que en lugar de considerar el dominio como un espacio $(A^n)^n$, se puede reemplazar por $\mathrm{Mat}_n(A)$ que es isomorfo.

Definición 3.49 – *Determinante*: Se define la función determinante $\det\colon \mathrm{Mat}_n(A) \to A$ como la única forma multilineal tal que $\det(I_n) = 1$. Algunos textos usan $|B|$, pero éste **no**, para evitar confusiones.

Algo que destacar es que el cálculo de matrices se vuelve, en casos generales, exponencialmente más complejo de acuerdo a las dimensiones de las matrices, ésto es fácil de ver ya que $|S_n| = 2^n$, luego el determinante comprende una herramienta sólo en casos particulares, en matrices pequeñas o en contextos teóricos.

Proposición 3.50 (Cálculo de determinantes): Si B es una matriz, entonces:

1. Intercambiar columnas (o filas) cambia el signo de su determinante.
2. La matriz generada por ultiplicar una columna (o fila) por λ tiene determinante $\lambda \det B$.
3. Sumarle a una columna (resp. fila) λ-veces otra columna (resp. fila) distinta no varía el determinante.
4. Si para todo $i < j$ (o que $j < i$) se cumple que $b_{ij} = 0$, entonces $\det B = b_{11} b_{22} \cdots b_{nn}$.

Proposición 3.51: Para toda matriz B cuadrada se cumple $\det(B^t) = \det(B)$.

Teorema 3.52: Para todos $B, C \in \mathrm{Mat}_n(\Bbbk)$ se cumple que $\det(BC) = \det B \det C$.

DEMOSTRACIÓN: Probaremos que $f(B) := \det(BC)$ es una forma multilineal alternada. Para ello denotaremos B como una tupla de vectores que corresponden a sus columnas, es decir, $B = (B_1, \ldots, B_n)$, donde $B_1 = (b_{11}, \ldots, b_{1n})$. Luego si $B' := (B_1, \ldots, B_u + \lambda \boldsymbol{v}, \ldots, B_n)$, $D := BC$ y $D' := B'C$, entonces

$$D'_{ij} = \sum_{k=1}^{n} B'_{ik} C_{kj}$$

luego si $i \neq u$, entonces $D'_{ij} = D_{ij}$. Si $i = u$, entonces $D'_{u,*} = D_{u,*} + \lambda(\boldsymbol{v}C)_*$, y como el determinante es multilineal sobre columnas y filas (por traspuesta) se comprueba también la multilinealidad de f.

Para ver que es alternada notamos que si B repite columnas, D repite filas, luego como el determinante es alternado también por filas, f toma valor nulo.

Finalmente para calcular la constante a evaluamos en I_n lo que da $\det C$ y comprueba el enunciado. □

Definición 3.53 (Menor complemento): Dada una matriz $B \in \mathrm{Mat}_n(A)$ con $n > 1$, se le llama ***menor complemento***, denotado $M_{ij}(B)$, de la coordenada (i, j) al determinante de la matriz resultante de eliminar la i-ésima fila y j-ésima columna de B.

Proposición 3.54: Si $B \in \mathrm{Mat}_n(A)$ con $n > 1$, entonces para todo $i, j \leq n$ se cumple que

$$\det B = \sum_{k=1}^{n} (-1)^{i+k} b_{ik} M_{ik}(B) = \sum_{k=1}^{n} (-1)^{k+j} b_{kj} M_{kj}(B). \tag{3.1}$$

Definición 3.55 (Matriz adjunta): Dada una matriz $B \in \mathrm{Mat}_n(A)$ con $n > 1$, se le llama ***matriz adjunta***, denotado $\operatorname{adj} B$, a la matriz

$$\operatorname{adj} B := \left[(-1)^{i+j} M_{ji}(B)\right]_{ij}.$$

Teorema 3.56: Para todo $B \in \mathrm{Mat}_n(D)$ con $n > 1$ se cumple que

$$B \cdot \operatorname{adj} B = \operatorname{adj} B \cdot B = (\det B) \cdot I_n. \tag{3.2}$$

En consecuencia, B es invertible syss $\det B$ es invertible, en cuyo caso, $B^{-1} = \frac{1}{\det B} \operatorname{adj} B$. Si D es un cuerpo, la condición se reduce a notar

que las matrices invertibles son las de determinante no nula.

Proposición 3.57: Se cumple:

1. $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$

2. $\operatorname{adj} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$

3. $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - (afh + bdi + ceg)$ (regla de Sarrus).

Una técnica de mnemotecnia se basa en la fig. 3.1, donde las diagonales verdes se suman y las rojas se restan.

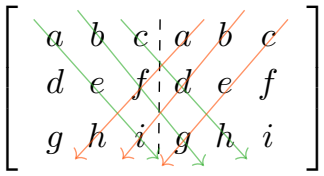


Figura 3.1. Regla de Sarrus.

Veamos un ejemplo del cálculo de una matriz que será útil más adelante:

Proposición 3.58: Sean $a_1, \ldots, a_n \in A$. Entonces:

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{i<j} (a_j - a_i).$$

A ésta se le llama la ***matriz de Vandermonde***.

Demostración: La demostración es por inducción sobre n: El caso $n = 1$ es trivial. Para los casos mayores emplearemos las operaciones elementales

sobre matrices para notar lo siguiente:

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & 0 \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-2}(a_2-a_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-2}(a_n-a_1) \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & a_2-a_1 & a_2(a_2-a_1) & \cdots & a_2^{n-2}(a_2-a_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n-a_1 & a_n(a_n-a_1) & \cdots & a_n^{n-2}(a_n-a_1) \end{vmatrix}$$

$$= \begin{vmatrix} a_2-a_1 & a_2(a_2-a_1) & \cdots & a_2^{n-2}(a_2-a_1) \\ a_3-a_1 & a_3(a_3-a_1) & \cdots & a_3^{n-2}(a_3-a_1) \\ \vdots & \vdots & \ddots & \vdots \\ a_n-a_1 & a_n(a_n-a_1) & \cdots & a_n^{n-2}(a_n-a_1) \end{vmatrix}$$

$$= (a_2-a_1)\begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-2} \\ a_3-a_1 & a_3(a_3-a_1) & \cdots & a_3^{n-2}(a_3-a_1) \\ \vdots & \vdots & \ddots & \vdots \\ a_n-a_1 & a_n(a_n-a_1) & \cdots & a_n^{n-2}(a_n-a_1) \end{vmatrix}$$

$$= (a_n-a_1)\cdots(a_2-a_1)\begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-2} \\ 1 & a_3 & \cdots & a_3^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-2} \end{vmatrix}$$

finalmente concluimos por hipótesis inductiva. □

§3.4.1 Invariantes: traza y polinomio característico. Existen una serie de números que podemos asociar a una matriz, pero más aún, preferiríamos que se pudieran asociar a endofunciones lineales. Presentaremos la noción de matrices similares y los invariantes salvo similaridad son los valores que nos interesan.

Definición 3.59: Sea k un cuerpo y $n \in \mathbb{N}_{\neq 0}$, se denota por $\mathrm{GL}(n,k) := \mathrm{Mat}_n(k)^\times$ que, por el teorema anterior, corresponde al conjunto de matrices de determinante no nulo.

Dos matrices cuadradas $A, B \in \mathrm{Mat}_n(k)$ se dicen ***similares*** si existe $C \in \mathrm{GL}(n,k)$ tal que $C^{-1}AC = B$.

Proposición 3.60: Dos matrices $A, B \in \mathrm{Mat}_n(k)$ son similares syss existe una base ordenada $X := (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ tal que $\mathrm{M}_X^X(A) = B$.

Corolario 3.61: Dos matrices similares comparten determinante.

Pista: Se sigue del teorema 3.52. □

Definición 3.62: Dada una matriz $B \in \mathrm{Mat}_n(\Bbbk)$ se define su ***traza*** como

$$\operatorname{tr} B := \sum_{k=1}^{n} b_{kk}.$$

Proposición 3.63: Sean $A, B \in \mathrm{Mat}_n(\Bbbk)$ y $\lambda \in \Bbbk$, entonces:

1. $\operatorname{tr}(A^t) = \operatorname{tr} A$.
2. $\operatorname{tr}(\lambda A) = \lambda \operatorname{tr} A$.
3. $\operatorname{tr}(A + B) = \operatorname{tr} A + \operatorname{tr} B$.
4. $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

Demostración: Todas son triviales exceptuando la última:

$$\operatorname{tr}(AB) = \sum_{k=1}^{n} (A \cdot B)_{kk} = \sum_{k=1}^{n} \sum_{j=1}^{n} a_{kj} b_{jk} = \sum_{j=1}^{n} \sum_{k=1}^{n} b_{jk} a_{kj} = \operatorname{tr}(BA). \qquad \square$$

Corolario 3.64: Dos matrices similares comparten traza.

Ya hemos visto que el determinante de una matriz es de hecho una expresión polinómica en términos de los coeficientes de la matriz. Ésto nos sirve para construir un polinomio que también es relevante para nuestros fines:

Definición 3.65: Dada una matriz $B \in \mathrm{Mat}_n(\Bbbk)$, se define su ***polinomio característico*** como

$$\psi_B(x) := \det(x \cdot I_n - B) \in k[x].$$

Proposición 3.66: Dos matrices similares comparten polinomio característico.

Proposición 3.67: Sea $A \in \mathrm{Mat}_n(\Bbbk)$ y sea $\psi_A(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in \Bbbk[x]$. Entonces $\det A = (-1)^n c_0$ y $\operatorname{tr} A = -c_{n-1}$.

DEMOSTRACIÓN: El primero es trivial puesto que $c_0 = \psi_A(0) = \det(-A)$. Para el segundo, considere que, por definición, el polinomio característico corresponde al determinante de una matriz de la forma:

$$\begin{bmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{bmatrix}$$

Ahora, nótese que podemos expresarlo como

$$\psi_A(x) = (x - a_{11}) \cdots (x - a_{nn}) + g(x),$$

donde $g(x) \in k[x]$ tiene grado $\leq n - 2$. De aquí es fácil extraer el valor de c_{n-1} y comprobar lo pedido. □

§3.4.2 Rango de matrices.

Definición 3.68: Dada $A \in \mathrm{Mat}_{n\times m}(\Bbbk)$ se le dice ***rango por filas*** (resp. por columnas) a la dimensión del subespacio generado por sus vectores fila (resp. vectores columna).

Lema 3.69: El rango por filas, el rango por columnas y la dimensión de la imagen de una matriz concuerdan.

DEMOSTRACIÓN: Sean r_f y r_c el rango por filas y por columnas resp. de una matriz fijada $A \in \mathrm{Mat}_{n\times m}(\Bbbk)$. Sin perdida de generalidad supongamos que las filas están ordenadas de tal manera que las primeras r_f son linealmente independientes, luego para todo i se cumple que

$$A_{i,*} = \sum_{k=1}^{r_f} \lambda_{ik} A_{k,*}$$

es decir que para todo i, j:

$$A_{ij} = \sum_{k=1}^{r_f} \lambda_{ik} A_{kj}.$$

Donde $\lambda_{ij} = \delta_{ij}$ si $i \leq r_f$; en definitiva si $B := [\lambda_{ij}]_{ij}^t$ que es una matriz de $r_f \times n$ vemos que se cumple que

$$A = B^t A \iff A^t = A^t B \iff A_{*,j} = \sum_{k=1}^{r_f} A_{jk}^t B_{k,*}$$

Luego $(B_{k,*})_{k=1}^{r_f}$ es un sistema generador de las columnas de A, es decir, $r_c \leq r_f$. Análogamente se deduce la otra desigualdad. □

Definición 3.70: Se le dice ***rango***, denotado $\operatorname{rang}(A)$, de una de una matriz A al rango por filas o columnas.

Corolario 3.71: Para toda matriz A se cumple que $\operatorname{rang}(A) = \operatorname{rang}(A^t)$.

Teorema 3.72: Dada $A \in \operatorname{Mat}_{n\times m}(\Bbbk)$ cualquiera, y sean $B \in \operatorname{Mat}_n(\Bbbk)$ y $C \in \operatorname{Mat}_m(\Bbbk)$ invertibles. Entonces $\operatorname{rang}(A) = \operatorname{rang}(BA) = \operatorname{rang}(AC)$.

De éste modo también podemos definir el rango para transformaciones lineales ya que sería independiente de la base.

Proposición 3.73: Una matriz de $n \times n$ es invertible syss tiene rango n.

Teorema 3.74: Si $A \in \operatorname{Mat}_{n\times m}(\Bbbk)$ y $B \in \operatorname{Mat}_{m\times p}(\Bbbk)$, entonces

$$\operatorname{rang}(AB) \leq \operatorname{rang}(A), \qquad \operatorname{rang}(AB) \leq \operatorname{rang}(B).$$

Nótese que en este sentido el rango de una matriz sirve como indicador de qué tan «invertible» es.

Definición 3.75: Dada una matriz $A \in \operatorname{Mat}_{n\times m}(R)$. Una submatriz B está dado por un par de inyecciones $\sigma\colon \{1,\dots,n'\} \to \{1,\dots,n\}$ y $\tau\colon \{1,\dots,m'\} \to \{1,\dots,m\}$ tal que $B = [A_{\sigma(i),\tau(j)}]_{ij} \in \operatorname{Mat}_{n'\times m'}(R)$.

Por ejemplo, si consideramos

$$A := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

entonces algunas de sus submatrices son:

$$\begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 3 \\ 8 & 9 \end{bmatrix}.$$

Ésta definición puede parecer extraña, pero es útil para lo siguiente:

Proposición 3.76: El rango de una matriz A, es el mayor n tal que existe una submatriz de A de tamaño $n \times n$ inversible.

Demostración: Sea A de dimensiones $u \times v$. Claramente si A posee una submatriz de $n \times n$ inversible, entonces necesariamente $\operatorname{rang} A \geq n$. Por otro lado, si $\operatorname{rang} A = m$, entonces es porque sus filas generan un subespacio S de dimensión m; luego podemos elegir m de ellas tal que sean linealmente independientes y, por tanto, sean base de S. Así tenemos una submatriz de dimensiones $m \times v$ en A de rango m; luego hacemos lo mismo con las columnas y obtenemos una submatriz de $m \times m$ en A de rango m, vale decir, una submatriz inversible; por lo que $\operatorname{rang} A \leq n$. □

Uno podría ahora preguntarse la razón filosófica (o algebraica, para precisar) del hecho de que el determinante, la traza y el polinomio característico sean invariantes tan favorables entre las matrices. Una explicación parcialmente satisfactoria puede encontrarse en el estudio de las álgebras exteriores (cf. §10.2.1).

Notas históricas

Una anécdota divertida: Es consabido que Lewis Carroll fue un escritor y matemático, y a partir de su noviazgo con Alice Liddell escribió sus famosas novelas *Alicia en el país de las maravillas* y *Alicia a través del espejo*. Éstos agradaron tanto a la Reina Victoria que le mandó una carta a Carroll informándole que Su Majestad estaría complacida de leer cualquier otra obra de su autoría. Carroll le envió una copia de su *Tratado elemental sobre determinantes*.

Parte II.

Teoría de Anillos y Módulos

4

Extensiones de cuerpo

4.1 Extensiones algebraicas

Definición 4.1 – *Extensión de cuerpos*: Dado un cuerpo k se dice que K es una ***extensión de cuerpos*** de k si K tiene un subcuerpo isomorfo a k, lo que abreviamos diciendo que K/k es una extensión.

Si K es una extensión de cuerpo, entonces con las operaciones usuales se puede ver como un k-espacio vectorial, de modo que llamamos su ***grado*** a $[K : k] := \dim_k(K)$. Si $g = [K : k]$, entonces podemos expresarlo empleando el siguiente *diagrama de retículos*:

$$\begin{array}{c} K \\ {\scriptstyle g}\big| \\ k \end{array}$$

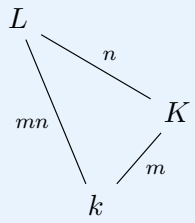
Dada una extensión K del cuerpo k, un elemento $\alpha \in K$ se dice ***k-algebraico*** si existe $f \in k[x]$ tal que $f(\alpha) = 0$, de lo contrario se dice ***k-trascendente***. Una extensión K se dice k-algebraica si todos sus elementos lo son, de lo contrario, K se dice k-trascendente. De no haber ambigüedad obviamos el «k-».

Hay varias cosas que queremos lograr: una de las cuales es establecer una categoría bien definida con las extensiones de cuerpo.

Teorema 4.2: Si W es un K-espacio vectorial y K/k es una extensión de cuerpos, entonces W es un k-espacio vectorial y

$$\dim_k(W) = \dim_K(W) \cdot [K : k].$$

Teorema 4.3 – *Teorema de transitividad de grados*: Si $L/K/k$ son cuerpos, entonces $[L : k] = [L : K] \cdot [K : k]$. En diagrama de retículos:



Otros autores se refieren al teorema anterior como la *ley de torres*, por el correspondiente diagrama de retículos.

Teorema 4.4: Toda extensión de grado finito es algebraica.

Demostración: Sea K extensión de k de grado n. Si $n = 1$, entonces es trivial. De lo contrario sea $\alpha \notin k$ y consideremos $S := \{1, \alpha, \ldots, \alpha^n\}$.
Si alguna potencia de α se repite, digamos $\alpha^i = \alpha^j$, entonces $f(x) := x^j - x^i$ hace algebraico a α. De lo contrario, como S tiene $n+1$ elementos no puede ser base, ergo existen $c_i \in k$ tales que son no nulos y

$$\sum_{i=0}^{n} c_i \alpha^i = c_n \alpha^n + \cdots + c_1 \alpha + c_0 = 0,$$

pero luego $f(x) := \sum_{i=0}^{n} c_i x^i$ es claramente un polinomio que hace que α sea algebraico; por ende, K es algebraico. □

En principio parece muy específico el acto de clasificar elementos entre *algebraicos* y *trascendentes* de esa forma, sin embargo, hay una razón bastante natural para hacerlo.

Teorema 4.5 – *Teorema de extensión de Kronecker*: Sea k un cuerpo con $f(x) \in k[x]$ no constante y sin raíces, entonces existe una extensión K/k que posee una raíz de $f(x)$.

Demostración: Si $f(x)$ es no constante entonces y no posee raíces como $k[x]$ es un DFU entonces se puede factorizar mediante irreductibles que tampoco tienen raíz, en particular sea $g(x)$ uno de ellos. Como $(g(x))$ es un ideal maximal, entonces $K := k[x]/(g(x))$ resulta ser un cuerpo.

Nótese que para todo $a \in k$ se tiene que $[a] \in K$, y es claro que la función $y \mapsto [y]$ es un monomorfismo de cuerpos. Luego, denotamos nuestra raíz como $\alpha := [x]$ (recordad que las clases de equivalencias son de polinomios de $k[x]$), como el anillo cociente es respecto a $g(x)$ que divide a $f(x)$ tenemos que

$$0 = [f(x)] = \sum_{i\geq 0}[a_i][x]^i = \sum_{i\geq 0} a_i\alpha^i = f(\alpha),$$

osea que α es una raíz de f en K. □

Cabe destacar que diremos que un elemento es una ***raíz cuadrada*** de a syss es la raíz de $x^2 - a$. Asimismo diremos que es ***raíz cúbica*** cuando es raíz de $x^3 - a$ y, en general, que es una n***-ésima raíz*** cuando es raíz de $x^n - a$. *Ojo* que ésto no tiene nada que ver con la función real $\sqrt[n]{x}$, pues se define de otra manera (ver def. 1.50 de [Top]).

Definición 4.6: Sea k un cuerpo con $f(x) \in k[x]$ un polinomio no-constante sin raíz. Entonces denotando α como una raíz de f, entonces $k(\alpha)$ es la extensión de k construida en condiciones de la demostración anterior.

Nótese que para todo $f(x) \in k[x]$,

$$[f(x)] = \sum_{i\geq 0}[a_i][x]^i = \sum_{i\geq 0} a_i\alpha^i = f(\alpha),$$

es decir, que la extensión que hemos construido resulta ser el cuerpo de polinomios de α (de ahí la notación). De igual manera podríamos construir una extensión con un polinomio que si tuviese raíz, pero es inmediato notar que es el mismo k.

Teorema 4.7: Si K/k es una extensión de cuerpos y $\alpha \in K$ es algebraico, entonces:

1. Existe un único polinomio mónico irreductible $f(x) \in k[x]$ tal que $f(\alpha) = 0$. Al que llamaremos ***polinomio minimal*** de α sobre k.
2. Si $g(x) \in k[x]$ cumple que $g(\alpha) = 0$, entonces $f(x) \mid g(x)$.

3. $\mathrm{ev}_\alpha\left[k[x]\right] = \mathrm{ev}_\alpha\left[k(x)\right] = \{r(\alpha) : r(x) \in k[x] \wedge \deg r < \deg f\}$
4. $k(\alpha)/k$ es una extensión finita, de hecho $[k(\alpha) : k] = \deg f =: n$ y $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es base para $k(\alpha)$.

Demostración:

1. Consideremos $\pi := \mathrm{ev}_\alpha \colon k[x] \to k(\alpha)$ dada por $\pi(g(x)) = g(\alpha)$. Claramente π es un epimorfismo de anillos, luego $\ker \pi$ es un ideal de $k[x]$, y como éste es un PID, entonces es generado por un polinomio $f(x)$. Como $k(\alpha) \cong k[x]/(f(x))$ es un dominio íntegro, entonces $(f(x))$ es primo y $f(x)$ es irreductible.
2. Supongamos que $g(x)$ tiene a α de raíz, entonces $g(x) \in \ker \pi = (f(x))$, luego $f(x) \mid g(x)$. Si $g(x)$ es irreductible, entonces g y f son asociados, pero cómo exigimos que el polinomio sea mónico se comprueba la unicidad.
3. Se deduce de la construcción de la extensión de Kronecker.
4. Veamos que la base explicitada en efecto lo es, dado que los elementos de $k(\alpha)$ son de la forma $g(\alpha)$ con $\deg g < n$, entonces se deduce que el conjunto propuesto es un sistema generador. Por otro lado, es libre pues si no lo fuese habría un polinomio no nulo $r(x)$ tal que $r(\alpha) = 0$ y $\deg r \leq n - 1 < n$ lo que contradice la definición de $f(x)$. □

El teorema anterior nos dice que en un sentido $k(\alpha)$ es la *mínima* extensión de cuerpos que contiene a α. En el teorema 4.13 veremos una generalización del teorema anterior que no depende del cuerpo base.

Corolario 4.8: Sea K/k una extensión de cuerpos y sean $\alpha, \beta \in K$ algebraicos, entonces

$$[k(\alpha, \beta) : k] \leq [k(\alpha) : k] \cdot [k(\beta) : k].$$

En consecuencia si $S \subseteq K$ es finito y algebraico, entonces $k(S)/k$ es una extensión finita.

Demostración: Por transitividad de grados sabemos que

$$[k(\alpha, \beta) : k] = [k(\beta)(\alpha) : k(\beta)] \cdot [k(\beta) : k],$$

por ende basta notar que $[k(\beta)(\alpha) : k(\beta)] \leq [k(\alpha) : k]$. Para ello, el teorema anterior demuestra que $[k(\alpha) : k] = \deg f$, donde $f(x) \in k[x]$ es el polinomio

minimal de α. Pero $f(x) \in k(\beta)[x]$, así que por el teorema anterior se cumple que es múltiplo del polinomio minimal $g(x)$ en $k(\beta)$, por lo que $[k(\beta)(\alpha) : k(\beta)] = \deg g \leq \deg f = [k(\alpha) : k]$. □

Ejemplo. Considere $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Primero nótese que el $\mathbb{Q}$-polinomio minimal de $\sqrt{2}$ y $\sqrt{3}$ son resp.:

$$f(x) = x^2 - 2, \quad g(x) = x^2 - 3.$$

Para notar que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ hay que ver que $g(x)$ no tiene raíces en $\mathbb{Q}(\sqrt{2})$. Para ello nótese que

$$g(a + b\sqrt{2}) = a^2 + 2ab\sqrt{2} + 2b^2 - 3$$

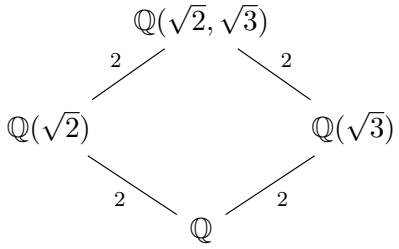
como $\mathbb{Q}(\sqrt{2})$ es un $\mathbb{Q}$-espacio vectorial de base $\{1, \sqrt{2}\}$ se concluye que

$$\begin{aligned} a^2 + 2b^2 - 3 &= 0, \\ 2ab &= 0. \end{aligned}$$

De la segunda línea se comprueba que $a = 0$ o $b = 0$. Si $b = 0$, entonces se reduce al caso de $g(x)$ en $\mathbb{Q}$ que sabemos no tiene solución. Si $a = 0$, entonces nos queda que

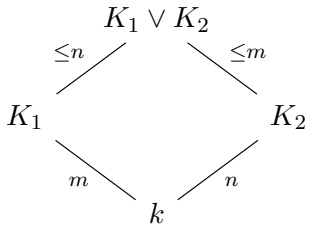
$$r(x) := 2x^2 - 3 = 0$$

Pero por criterio de Eisenstein el polinomio $r(x)$ es irreducible, luego no tiene raíces. En conclusión $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Luego $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$ y por el corolario $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Así se concluye que:



Definición 4.9: Sean $L/K_1/k$ y $L/K_2/k$ extensiones de cuerpo. Entonces $K_1 \cap K_2$ y $K_1 \vee K_2 := K_1(K_2) = K_2(K_1)$ son k-extensiones de cuerpo.

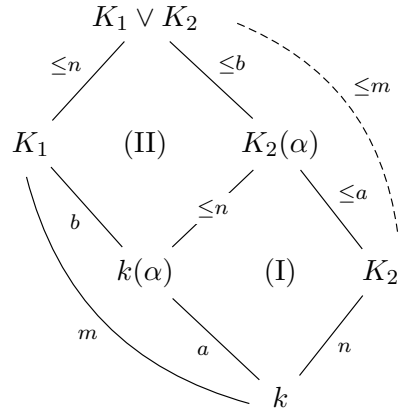
Proposición 4.10: Sean $L/K_1/k$ y $L/K_2/k$ extensiones de cuerpo con K_1, K_2 finitas. Entonces se satisface el siguiente diagrama de retículos:



Demostración: Lo demostraremos por inducción fuerte sobre $n + m$: El caso base $1 + 1$ es trivial, ya que $K_1 = K_2 = k$ y $K_1 \vee K_2 = k$.

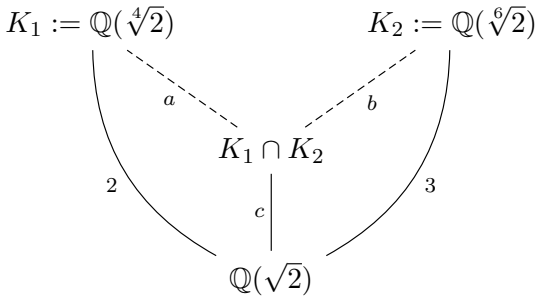
Hagamos la siguiente observación: Si $K_1 = k(\alpha)$, entonces el enunciado se satisface. La demostración es la misma del corolario 4.8, se toma el polinomio minimal de α y se nota que es también tiene raíz en $K_1 \vee K_2 = K_2(\alpha)$ como polinomio de K_2.

Para el caso general, si $K_1 = k$ es trivial. Si no, sea $\alpha \in K_1 \setminus k$, entonces como K_1 es finita, entonces es algebraica y se cumple que $[K_1 : k] = m = [K_1 : k(\alpha)] \cdot [k(\alpha) : k]$. Luego la demostración consiste en construir el siguiente diagrama de retículos:



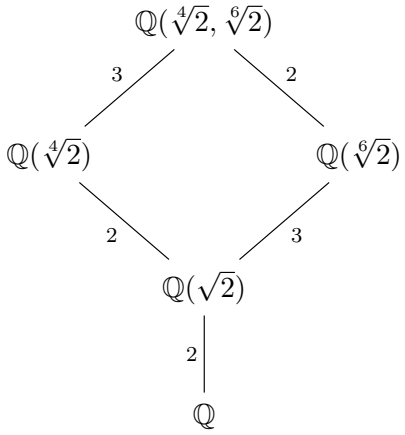
donde el diamante (I) sale de la observación, mientras que el diamante (II) sale por hipótesis inductiva. □

Ejemplo. Consideremos $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$. Nótese que como $f(x) := (x^4 - 2)$ y $(x^6 - 2)$ son $\mathbb{Q}$-irreducibles por el criterio de Eisenstein, entonces $\mathbb{Q}(\sqrt[4]{2})$ y $Q(\sqrt[6]{2})$ tienen grados 4 y 6 resp. ¿Será que $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$ sea de grado $4 \cdot 6 = 24$? La respuesta es que no, para ver ésto primero nótese que $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}) \cap \mathbb{Q}(\sqrt[6]{2})$ puesto que $\sqrt[4]{2}^2 = \sqrt[6]{2}^3 = \sqrt{2}$. Luego, mírese el siguiente diagrama de retículos:



De modo que $c \mid 2$ y $c \mid 3$, es decir, $c = 1$.

También nótese que el mismo diagrama sugiere que $\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[6]{2})$, puesto que de lo contrario, se tendría la torre $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4n = 6$ y no existe un n entero que la satisfaga. Luego $[\mathbb{Q}(\sqrt[6]{2}, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] > 1$ y por el corolario es ≤ 2. Por ende el diagrama de retículos se ve así:



y en conclusión $[\mathbb{Q}(\sqrt[6]{2}, \sqrt[4]{2}) : \mathbb{Q}] = 12$

Teorema 4.11: Si $L/K/k$ son extensiones de cuerpos, entonces L/k es algebraica syss L/K y K/k lo son.

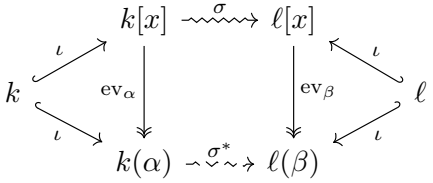
Demostración: $\Longrightarrow$. Si L/k es algebraica, claramente K/k lo es y como k es subcuerpo de K se comprueba que L/K lo es.

$\Longleftarrow$. Si $\alpha \in L$ entonces α es K-algebraico, luego sean $\beta_1, \ldots, \beta_n$ los coeficientes de su polinomio minimal, luego α es algebraico sobre $k(\beta_1, \ldots, \beta_n)$, por ende $k(\beta_1, \ldots, \beta_n)[\alpha]/k(\beta_1, \ldots, \beta_n)$ es finita, y como los β_i son k-algebraicos, entonces $k(\beta_1, \ldots, \beta_n)/k$ es finito, finalmente $k(\beta_1, \ldots, \beta_n, \alpha)/k$ es finito y luego algebraico. $\square$

Corolario 4.12: Si K/k es una extensión de cuerpos, entonces el conjunto de elementos algebraicos de K es un cuerpo.

Demostración: Basta notar que si α, β son algebraicos sobre K, entonces $k(\alpha, \beta)/k$ es finita, luego algebraica y por ende $\alpha + \beta$, $\alpha \cdot \beta$ y α/β (si $\beta \neq 0$) lo son. □

Teorema 4.13: Sean K/k y L/ℓ extensiones de cuerpo con $\sigma\colon k \to \ell$ un isomorfismo de cuerpo, que induce un morfismo de anillos $\sigma\colon k[x] \to \ell[x]$. Si $\alpha \in K$ es algebraico, entonces sea $f \in k[x]$ su polinomio minimal. Si L contiene una raíz β de $\sigma f(x)$, entonces σ se extiende un isomorfismo de extensiones $\sigma^*\colon k(\alpha) \to \ell(\beta)$ con $\sigma^*(\alpha) = \beta$, es decir, existe un σ^* tal que el siguiente diagrama



conmuta (en Ring).

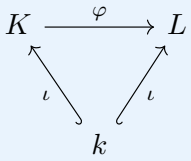
Demostración: Sea $\phi\colon k[x] \to k[\alpha]$ el morfismo de evaluación, i.e., tal que $\phi(g) = g(\alpha)$. Es claro que $\ker \phi$ es el ideal $(f(x))$, luego por el primer teorema de isomorfismos $k[x]/(f(x)) \cong k[\alpha]$.

En primer lugar veamos que $\sigma f(x)$ ha de ser el polinomio minimal de β en l. Luego, análogamente $l[x]/(\sigma f(x)) \cong l[\alpha]$.

Finalmente $\omega\colon k[x] \to l[x]$ que fija a la identidad induce un isomorfismo $k[x]/(f(x)) \cong l[x]/(\sigma f(x))$, de lo que se concluye que $k[\alpha] \cong l[\beta]$. □

Ésto nos motiva a formular la siguiente definición:

Definición 4.14: Sean K/k y L/k extensiones de cuerpo. Entonces decimos que una función $\varphi\colon K \to L$ es un un ***k-morfismo*** si es un homomorfismo de anillos tal que $\varphi(\alpha) = \alpha$ para todo $\alpha \in k$, es decir, si el siguiente diagrama



conmuta (en Ring). Las extensiones de cuerpos sobre k, como objetos, y los k-morfismos, como flechas, conforman una categoría denotada por Ext_k.

Se le llama ***grupo de Galois*** de K, denotado por $\mathrm{Gal}(K/k)$, al conjunto $\mathrm{Aut}_{\mathsf{Ext}_k}(K)$; vale decir, $\mathrm{Gal}(K/k)$ son los k-automorfismos de K.

Corolario 4.15: Sea K/k una extensión de cuerpo, donde $K = k(\alpha)$ y $f(x) \in k[x]$ es el polinomio minimal de α. Entonces $|\operatorname{Gal}(K/k)|$ es la cantidad de raíces distintas de $f(x)$; en particular,

$$|\operatorname{Gal}(K/k)| \leq [K : k],$$

donde $|\operatorname{Gal}(K/k)| = [K : k]$ syss $f(x)$ se factoriza en distintos polinomios lineales.

Demostración: Sean $\alpha_1, \ldots, \alpha_n$ todas las raíces de $f(x)$ en K. Por el teorema anterior siempre existe un único k-automorfismo $\sigma_{ij} \colon k(\alpha_i) \to k(\alpha_j)$ tal que $\sigma_{ij}(\alpha_i) = \alpha_j$. Así pues, para cada j notemos que σ_{1j} es un k-automorfismo distinto, por lo que $|\operatorname{Gal}(K/k)| \geq n$. Al mismo tiempo si σ es un k-automorfismo, entonces $f\big(\sigma(\alpha)\big) = \sigma\big(f(\alpha)\big) = 0$, de modo que $\sigma(\alpha) = \alpha_i$, pero el teorema anterior prueba la unicidad de σ, con lo que $|\operatorname{Gal}(K/k)| = n$. Como $n \leq \deg f$ se comprueba la desigualdad.

Ya vimos que $|\operatorname{Gal}(K/k)|$ es la cantidad de raíces de $f(x)$, así que la equivalencia es clara. □

Definición 4.16 (k-conjugados): Dados α, β algebraicos sobre k, se dice que son k-conjugados si comparten el polinomio minimal.

Teorema 4.17: Dados α, β algebraicos sobre k, entonces son k-conjugados syss existe un k-isomorfismo $\sigma \colon k(\alpha) \to k(\beta)$ tal que $\sigma(\alpha) = \beta$. Más aún, $\sigma(\alpha)$ siempre es un k-conjugado de α.

Ejemplo. El polinomio ciclotómico p-ésimo, con $p > 2$, es irreducible luego carece de raíces, así que construyamos $\mathbb{Q}(\omega)$ donde ω es una raíz.

Como $\Phi_p(x)\cdot(x-1) = x^p - 1$, entonces todas las raíces del polinomio son raíces p-ésimas de la unidad, ergo $\omega^p = 1$, luego $(\omega^2)^p = 1^2 = 1$, por lo que ω^2 también es raíz de $\Phi_p(x)$. De hecho, se concluye que todas las raíces de $\Phi_p(x)$ son $\omega^1, \omega^2, \ldots, \omega^{p-1}$; luego ellos son k-conjugados.

Teorema 4.18: Si K/k es finito, entonces $\mathrm{Gal}(K/k)$ también.

Demostración: Sea $S := \{\alpha_1, \ldots, \alpha_n\}$ tal que $K = k(S)$. Sea $\sigma \in \mathrm{Gal}(K/k)$ y $f \in k[S]$, como σ es un k-automorfismo se cumple $\sigma(f(\alpha_1, \ldots, \alpha_n)) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$. Notemos que todo elemento en K es de la forma $f(\alpha_1, \ldots, \alpha_n)$, luego dos k-automorfismos coinciden syss lo hacen en S.

Sea f_i el polinomio minimal de α_i, entonces $f(\alpha_i) = 0 = \sigma(f(\alpha_i)) = f(\sigma(\alpha_i))$. Y se sabe que un polinomio no nulo tiene finitas raíces, luego σ sólo puede tomar finitos valores en α_i. Finalmente sólo hay finitas posibilidades para σ, luego $\mathrm{Gal}(K/k)$ es finito. □

4.2 Extensiones normales y separables

§4.2.1 Cuerpos de escisión.

Definición 4.19: Se dice que un polinomio $f \in k[x]$ ***se escinde***[a] en una extensión de cuerpos K/k, si existen $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$ tales que

$$f(x) = \alpha_0(x-\alpha_1)\cdots(x-\alpha_n).$$

También llamamos ***cuerpo de escisión*** de f sobre k a la extensión K/k tal que f escinde en K y $K = k(\alpha_1, \ldots, \alpha_n)$.

[a] eng. *splits*.

Teorema 4.20: Si $\sigma\colon k \to k'$ es un isomorfismo de cuerpos, K es un cuerpo de escisión de $f(x) \in k[x]$ y K' de $\sigma(f)(x)$, entonces se extiende σ a $\bar{\sigma}\colon K \to K'$ como isomorfismo. En consecuencia, todo par de cuerpos de escisión de un mismo polinomio son k-isomorfos.

Demostración: No perdemos generalidad al suponer que f es irreductible. Lo haremos por inducción sobre el grado de f, donde el caso $n = 1$ es trivial.

Sea f de grado $n+1$, sea α_{n+1} una raíz en K y sea β_{n+1} una raíz de $\sigma(f)$ en K'. Como $\alpha_{n+1}, \beta_{n+1}$ son k-conjugados, entonces existe $\sigma^*\colon k(\alpha_{n+1}) \to k'(\beta_{n+1})$ que extiende a σ. Luego sea $f(x) = (x-\alpha_{n+1})g(x)$ de modo que

K es un cuerpo de escisión de $g(x)$ (de grado n) en $k(\alpha_{n+1})$ y K' lo es de $\sigma^*(g(x))$ en $k'(\beta_{n+1})$; por lo que, por hipótesis inductiva, existe $\bar{\sigma}$ que extiende a σ^* (que extiende a σ) tal que $\bar{\sigma}\colon K \to K'$ es un isomorfismo de cuerpos. □

Proposición 4.21: Si $f \in k[x]$ es de grado $n \geq 1$, entonces posee un cuerpo de escisión y ésta tiene grado a lo más $n!$

Pista: Usar inducción. □

Ejemplo. Consideremos el polinomio

$$\Phi_7(x) := \frac{x^7 - 1}{x - 1} = 1 + x + x^2 + \cdots + x^6$$

que es irreducible por ser ciclotómico. Si ω es alguna raíz de Φ_7, entonces $\mathbb{Q}(\omega)$ es su cuerpo de escisión y tiene grado 6.

Consideremos ahora el polinomio

$$f(x) := x^6 - 2$$

que posee una raíz $\sqrt[6]{2}$. Nótese que $f(x)$ **no** se escinde en $\mathbb{Q}(\sqrt[6]{2})$. En primer lugar, como $\sqrt{2} \in \mathbb{Q}(\sqrt[6]{2})$ se tiene que

$$f(x) = (x^3 - \sqrt{2})(x^3 + \sqrt{2})$$

Y ahora podemos ver que

$$(x^3 - \sqrt{2}) = (x - \sqrt[6]{2})(x^2 + \sqrt[6]{2}x + \sqrt[3]{2}),$$

el término en rojo es cuadrático y sabemos que tiene raíces syss su discriminante tiene raíces, el cual es

$$\sqrt[6]{2}^2 - 4\sqrt[3]{2} = -3\sqrt[3]{2}.$$

Como $\sqrt[6]{2} \in \mathbb{R}$ se tiene que $\mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{R}$ y $\mathbb{R}$ no posee raíces de números negativos, así que $\mathbb{Q}(\sqrt[6]{2})$ tampoco; y por tanto el polinomio no se escinde.

Definición 4.22 – *Extensión normal*: Se dice que una extensión de cuerpos K/k es ***normal*** si para todo $f \in k[x]$ irreductible con alguna raíz en K se escinde en K.

Lema 4.23: Si $L/F/K/k$ son extensiones algebraicas de cuerpo de modo que F es un cuerpo de escisión de algún polinomio $f(x) \in k[x]$. Entonces si $\sigma\colon K \to L$ es un k-monomorfismo se cumple que $\sigma[K] \subseteq F$ y σ se extiende a un k-automorfismo de F, y en consecuencia, se extiende a un k-automorfismo de L. En diagramas conmutativos:

$$\begin{array}{ccc} F & \overset{\sigma^*}{\rightsquigarrow} & F \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Id}} \\ K & \xrightarrow{\sigma} & F \\ \uparrow & & \uparrow \\ k & \xrightarrow[\mathrm{Id}]{} & k \end{array}$$

Demostración: Supongamos que $f(x) = \alpha_0(x-\alpha_1)\cdots(x-\alpha_n)$ de modo que $F = k(\alpha_1,\dots,\alpha_n)$. Sea $K' := \sigma[K]$ y $F' := K'(\alpha_1,\dots,\alpha_n)$. Notemos que por definición K, K' son isomorfos, así que por el teorema anterior $\bar{\sigma}\colon F \to F'$ es un k-isomorfismo que exitiende a σ.

Sea $\beta \in K$, como $F = K(\alpha_1,\dots,\alpha_n)$, entonces existe $g(x_1,\dots,x_n) \in K[x_1,\dots,x_n]$ tal que $g(\alpha_1,\dots,\alpha_n) = \beta$, pero como los α_is son k-conjugados, entonces

$$\bar{\sigma}(\beta) = \bar{\sigma}(h(\alpha_1,\dots,\alpha_n)) = h(\bar{\sigma}(\alpha_1),\dots,\bar{\sigma}(\alpha_n)),$$

donde $\bar{\sigma}$ es una permutación de los α_i, de modo que $F' = \bar{\sigma}(F) \subseteq F$. En consecuencia $F' = F$ y $\bar{\sigma}$ es un k-automorfismo. □

Teorema 4.24: Una extensión finita K/k es normal syss es el cuerpo de escisción de algún polinomio.

Demostración: $\Longleftarrow$. Sea $f(x) \in k[x]$ el polinomio tal que K es su cuerpo de escisión. Sea $g(x) \in k[x]$ irreductible en $k[x]$ pero con raíz $\alpha \in K$. Sea L el cuerpo de escisión de g sobre K, de modo que si las raíces de $g(x)$ son $\alpha_1,\dots,\alpha_n$, entonces $L = K(\alpha_1,\dots,\alpha_n)$. Como α_i y α son k-conjugados, existe $\sigma\colon k(\alpha) \to k(\alpha_i) \subseteq L$ un k-isomorfismo, luego por el lema $k(\alpha_i) \subseteq K$, y como los $\alpha_i \in K$, $g(x)$ se escinde en K.

$\Longrightarrow$. Sea K/k normal. Como K/k es finita, existen $\alpha_1,\dots,\alpha_n$ tales que $K = k(\alpha_1,\dots,\alpha_n)$. Si $f_i(x)$ denota el polinomio minimal de α_i sobre k, entonces vemos que K se escinde en $f(x) := f_1(x)\cdots f_n(x)$ y es fácil ver que K es de hecho su cuerpo de escisión. □

Definición 4.25: Sea K/k una extensión finita. Entonces N se dice una ***clausura normal*** de K si $N/K/k$ es extensión y si $N/N'/K/k$ es tal que N' es normal, entonces $N' = N$.

Proposición 4.26: Toda extensión finita posee una clausura normal que es única salvo isomorfismo.

Demostración: Sea $K = k(\alpha_1, \ldots, \alpha_n)$ y $f_i(x) \in k[x]$ el polinomio minimal de α_i resp. Entonces sea $g(x) := \prod_{i=1}^{n} f_i(x) \in k[x]$, luego el cuerpo de escisión N de $g(x)$ es una extensión normal de K. Sea N' otra extensión normal de K, entonces todos los $f_i(x)$ se escinden en N', así que se da que N'/N es extensión. Así se concluye que necesariamente la clausura normal de K sea un cuerpo de escisión de $g(x)$, que es único salvo isomorfismo. □

§4.2.2 Extensiones separables.

Definición 4.27 (Polinomio derivado): Si D es un dominio íntegro y

$$f(x) = \sum_{k=0}^{n} a_k x^k \in D[x]$$

llamamos ***polinomio derivado*** de $f(x)$, denotado por $f'(x)$, a

$$f'(x) := \sum_{k=1}^{n} k a_{k-1} x^{k-1}.$$

Proposición 4.28: Si D es un dominio íntegro, entonces para todo $f, g \in D[x]$ y $\lambda \in D$:

1. $(\lambda f)' = \lambda f'$.
2. $(f + g)' = f' + g'$.
3. $(fg)' = f'g + fg'$.
4. $(f/g)' = \dfrac{f'g - fg'}{g^2}$.

Definición 4.29: Se dice que la ***multiplicidad*** de una raíz α de un polinomio $f(x) \in D[x]$ es el máximo entero n tal que $(x - \alpha)^n \mid f(x)$. Si una raíz es de multiplicidad 1, entonces se dice que es una raíz ***simple***.

Teorema 4.30: Dado D un dominio íntegro y α raíz de $f(x) \in D[x]$. α es una raíz simple syss $f'(\alpha) \neq 0$.

Demostración: Supongamos que el grado de α en f es n de modo que $f(x) = (x-\alpha)^n g(x)$ y $g(\alpha) \neq 0$, luego

$$f'(\alpha) = n(x-\alpha)^{n-1}g(x) + (x-\alpha)^n g'(x) = n(x-\alpha)^{n-1}g(x)$$

lo cual es no nulo syss $n-1=0$, i.e., si α es una raíz simple. □

Definición 4.31: Sea K/k una extensión de cuerpos. Un elemento algebraico $\alpha \in K$ se dice ***separable*** syss es la raíz simple de su polinomio minimal. Un elemento algebraico $\alpha \in K$ se dice ***puramente inseparable*** syss es la única raíz de su polinomio minimal. Nótese que un $\alpha \in K$ algebraico es separable y puramente inseparable syss $\alpha \in k$.

Si todos los elementos de K son separables (resp. puramente inseparables), entonces K se dice una ***extensión separable*** (resp. ***puramente inseparable***). Se dice que k es ***perfecto*** si todas sus extensiones de cuerpo son separables.

Nótese que el hecho de que un cuerpo sea perfecto sólo se verifica en sus extensiones algebraicas puesto que no tiene sentido hablar de elementos trascendentes separables o no.

De momento no nos enfocaremos en extensiones puramente inseparables, pero jugarán un rol más adelante; en esencia nos permitirán analizar las extensiones finitas (o algebraicas) de cuerpos al tener que ver los casos de separables y puramente inseparables.

Ejemplo 7: Consideremos $k := \mathbb{F}_p(t)$ como cuerpo. Estudiemos el polinomio $f(x) := x^p - t \in k[x]$. Nótese que para todo $\alpha \in k$ se cumple que $(x-\alpha)^p = x^p - \alpha^p$, luego si ω es una raíz de $f(x)$ en alguna extensión K/k se cumple que $f(x) = (x-\omega)^p$. Notemos que dicho polinomio es irreducible (al menos en el caso de $p=2$), de modo que K/k no es una extensión separable, dado que ω no lo es.

Proposición 4.32: Sea k un cuerpo de característica p. Entonces $\mathrm{Frob}_k(a) = a^p$ es un endomorfismo, conocido como el ***endomorfismo de Frobenius***. Y si Frob_k es suprayectivo, entonces Frob_k es un automorfismo.

Proposición 4.33: Sea D un dominio íntegro y $f(x) \in D[x]$ un polinomio no constante, entonces:

1. Si $\operatorname{car} D = 0$, entonces $f'(x) \neq 0$.
2. Si $\operatorname{car} D = f$, entonces $f'(x) = 0$ syss $f(x) = g(x^p)$ con $g(x) \in D[x]$.

Teorema 4.34: Se cumple:

1. Todo cuerpo de característica nula es perfecto.
2. Si $\operatorname{car} k = p$, entonces k es perfecto syss Frob_k es un automorfismo.
3. Todo cuerpo finito es perfecto.

Demostración:

1. Sea $\alpha \in K$ algebraico, cuyo polinomio minimal es $f(x)$. Si $f'(\alpha) = 0$, entonces $f(x) \mid f'(x)$, pero como $f'(x) \neq 0$ esto no tiene sentido por grados de polinomios.
2. $\Longleftarrow$. Sea $\alpha \in K/k$ algebraico y cuyo polinomio minimal es $f(x)$. Asumiremos que $f'(x) = 0$ de modo que $f(x) = g(x^p)$. Sea $g(x) = \sum_{i=0}^{n} a_i x^i$. Como Frob_k es endo-, existen b_i tales que $a_i = b_i^p$, luego

$$f(x) = g(x^p) = \sum_{i=0}^{n} a_i (x^p)^i = \sum_{i=0}^{n} b_i^p (x^i)^p = \sum_{i=0}^{n} (b_i x^i)^p = \left(\sum_{i=0}^{n} b_i x^i \right)^p,$$

   por lo que f no es irreductible, contradicción.

   $\Longrightarrow$. Sea k perfecto y sea $a \in k$ arbitrario. Luego sea b una raíz p-ésima de a, es decir, un elemento tal que b es raíz de $x^p - a$. Construyamos $k(b)$, luego sea $f(x)$ el polinomio minimal de b. Sabemos que b es raíz de $(x-a)^p$, por ende $f(x) \mid (x-a)^p$ de modo que $f(x) = (x-a)^n$ para algún $1 \leq n \leq p$. Pero como k es separable se cumple que b es raíz simple, ergo $n = 1$ y $x - b \in k[x]$ de modo que $b \in k$.
3. Corolario del 2. □

Alguien puede reclamar que en el ej. 7 vimos que la extensión $\mathbb{F}_p(t, \omega)$ no es separable, pero ésto ocurre como extensión de $\mathbb{F}_p(t)$, nótese que $\mathbb{F}_p(t, \omega)$ no es una extensión algebraica de $\mathbb{F}_p$.

Teorema 4.35: Existe una correspondencia biunívoca entre cuerpos finitos y números de la forma p^n con p primo y $n \geq 1$. Es decir, para todo p primos y $n \geq 1$ existe un único cuerpo de cardinalidad p^n y todo cuerpo tiene cardinalidad de esa forma.

Demostración: Sea k un cuerpo finito, luego tiene característica p y es un $\mathbb{F}_p$-espacio vectorial de dimensión finita n, luego su cardinalidad es de la forma p^n.

Sea $f(x) := x^{p^n} - x \in \mathbb{F}_p[x]$, luego su polinomio derivado es $p'(x) = -1 \neq 0$. Luego sea $k/\mathbb{F}_p$ el cuerpo de escisión de $\mathbb{F}_p$, entonces k tiene al menos p^n elementos por ser separable. Además, $(\mathrm{Frob}_k)^n(x) = x^{p^n} = x$ por el sueño del aprendiz, así que todo elemento en k es raíz de $f(x)$; en definitiva, k tiene exactamente p^n elementos.

Sea $L/\mathbb{F}_p$ un cuerpo de cardinalidad p^n, luego $L^\times$ es un grupo finito de cardinalidad $p^n - 1$, por lo que, por teorema de Lagrange, $g^{p^n-1} = 1$ para todo $g \in L^\times$, o equivalentemente, $g^{p^n} = g$. Luego $p(x)$ se escinde en L y L resulta ser el cuerpo de escisión de $p(x)$, por lo que $L \cong K$. □

Denotamos por $\mathbb{F}_{p^n}$ al único cuerpo de cardinalidad p^n salvo isomorfismo.

Teorema 4.36: Sea L/k una extensión finita de cuerpos. Son equivalentes:

1. L/k es separable.

2. $L = k(\alpha_1, \ldots, \alpha_n)$ donde cada α_i es separable.

4.3 Teoría y extensiones de Galois

La pregunta que motiva el estudio de la teoría de Galois es acerca de estudiar el grupo $\mathrm{Gal}(K/k)$. En el teorema 4.18 vimos que ha de ser finito en extensiones finitas y el teorema 4.17 nos caracteriza los k-automorfismos en términos de las raíces de un polinomio minimal. Sin embargo, podrían darse varias situaciones desfavorables: podría ser que las raíces se repitan y, por lo tanto, que el grupo esté más restringido, o podría darse que un polinomio no se escinda y luego no podamos conjugar las raíces a causa de no tenerlas. Por ello, reorientaremos el problema:

Definición 4.37: Sea K/k una extensión finita, entonces se denota por $\mathrm{N}(K/k)$ a la cantidad de k-monomorfismos desde K hasta su clausura normal.

Proposición 4.38: Sea α algebraico, entonces $\mathrm{N}(k(\alpha)/k) = [k(\alpha) : k]$ si α es separable y $\mathrm{N}(k(\alpha)/k) < [k(\alpha) : k]$ si no.

En general nos enfocaremos en cuerpos separables, pero aún así le dedicaremos un par de teoremas al caso inseparable:

Teorema 4.39: Sea k un cuerpo de $\operatorname{car} k =: p \neq 0$. Un polinomio $f(x) \in k[x]$ de grado > 1 irreducible es inseparable syss $f(x)$ es un polinomio en x^p. Sea $q = p^e$ la máxima potencia de p tal que $f(x)$ es un polinomio en x^q, entonces:

1. Para toda raíz α de $f(x)$ (en alguna extensión K/k) se cumple que α^q es separable en k.

2. Todas las raíces de $f(x)$ son separables en $k(\beta_1, \ldots, \beta_n)$, donde los β_i's son las q-ésimas raíces de los coeficientes de $f(x)$.

3. La multiplicidad de todas las raíces (en un cuerpo de escisión de $f(x)$) es q.

Demostración: Sea N la clausura normal de $f(x)$ sobre k, se cumple que

$$f(x) = \prod_{i=1}^{r} (x - \alpha_i)^{m_i}$$

donde α_i son las raices distintas de $f(x)$ y $m_i > 0$. Sea $\sigma \in \operatorname{Gal}(N/k)$, entonces

$$f(x) = \sigma f(x) = \prod_{i=1}^{r} (x - \sigma(\alpha_i))^{m_i}$$

por lo que los m_i's son todos iguales y digamos que valen m.

Si $\alpha := \alpha_i$ no es separable, entonces α es raíz común de $f(x)$ y $f'(x)$; pero por definición del polinomio minimal se debe cumplir entonces que $f'(x) = 0$, por lo que $f(x) = g(x^p)$ con $g(x) \in k[x]$. Además, claramente $\deg g < \deg f$. Luego procedemos recursivamente hasta encontrar el n más grande tal que $f(x) = h(x^{p^n})$, de modo que $q = p^n$, necesariamente $h'(x) \neq 0$ y α^q ha de ser una raíz separable de h. Lo mismo aplica para todas las raíces. Definiendo $\beta_i := \alpha_i^q$ vemos que se cumplen todas las condiciones exigidas. □

Corolario 4.40: Sea $f(x) \in k[x]$ irreducible y sea K/k su cuerpo de escisión, entonces las multiplicidades de sus raíces (en K) son iguales. En particular, si f tiene una raíz simple es separable y si f tiene una sola raíz puramente inseparable entonces ésta tiene por grado alguna potencia de $p = \operatorname{car} k$.

Corolario 4.41: Sea k un cuerpo de $\operatorname{car} k =: p \neq 0$ y sea K/k una extensión de cuerpos. Entonces:

1. Si K es inseparable, entonces $p \mid [K : k]$.
2. Si K es puramente inseparable, entonces $[K : k]$ es una potencia de p.

Definición 4.42 – *Extensión de Galois*: Se dice que K/k es una extensión de Galois si es normal y separable.

Sea $H \leq \operatorname{Gal}(K/k)$, entonces llamamos ***cuerpo fijado*** por H a

$$F(H) := \{a \in K : \forall \sigma \in H \ \sigma(a) = a\}.$$

Y si $K/L/k$, entonces llamamos el ***grupo fijado*** por L a

$$H_L := \{\sigma \in \operatorname{Gal}(K/k) : \forall a \in L \ \sigma(a) = a\}.$$

Nótese que para $\mathbb{Q}$ basta que una extensión sea normal para que sea de Galois.

Teorema 4.43: Sea $L/K/k$ una extensión normal, entonces $\mathrm{N}(L/k) = \mathrm{N}(L/K)\,\mathrm{N}(K/k)$.

Demostración: En ésta demostración N representa la clausura normal de K, de modo que $\mathrm{N}(K/k) := |\operatorname{Hom}_k(K, N)|$. Nótese que L/K y L/k son normales, de modo que $\mathrm{N}(L/K) = |\operatorname{Gal}(L/K)|$.

Sea $\sigma \in \operatorname{Hom}_k(K, N)$, por el lema 4.23 se ha de cumplir que σ se extiende a un k-automorfismo $\sigma^* \in \operatorname{Gal}(L/k)$, por lo tanto, el problema se reduce a ver que hay $\mathrm{N}(L/K)$ posibles extensiones.

Sean τ_1, τ_2 dos posibles extensiones de σ. Es decir, τ_1, τ_2 son k-automorfismos de L, pero entonces $\tau_1 \circ \tau_2^{-1} \colon L \to L$ es un k-automorfismo que de hecho fija a K, es decir, $\tau_1 \circ \tau_2^{-1} \in \operatorname{Gal}(L/K)$. Y así podemos concluir. □

Teorema 4.44: Sea K/k una extensión finita. Entonces:

1. $|\operatorname{Gal}(K/k)| \leq \mathrm{N}(K/k)$.
2. Si K/k es separable, entonces $\mathrm{N}(K/k) = [K : k]$.
3. Si K/k no es separable, entonces $\mathrm{N}(K/k) \mid [K : k]$.
4. Si K/k es de Galois, entonces $|\operatorname{Gal}(K/k)| = [K : k]$.

Demostración: Si K es de Galois, entonces sea $K = k(\alpha_1, \ldots, \alpha_n)$. Luego aplicando el teorema anterior se tiene que

$$\begin{aligned}\mathrm{N}(K/k) &= \mathrm{N}(K/k(\alpha_1,\alpha_2))\,\mathrm{N}(k(\alpha_1,\alpha_2),k)\\ &= \mathrm{N}(K/k(\alpha_1,\alpha_2))\,\mathrm{N}(k(\alpha_1,\alpha_2),k(\alpha_1))\,\mathrm{N}(k(\alpha_1),k)\\ &= \mathrm{N}(K/k(\alpha_1,\alpha_2))[k(\alpha_1,\alpha_2):k(\alpha_1)][k(\alpha_1):k]\\ &= \mathrm{N}(K/k(\alpha_1,\alpha_2))[k(\alpha_1,\alpha_2):k].\end{aligned}$$

luego podemos seguir iterando y aplicar la transitividad de grados para concluir que el enunciado aplica. Si K no es separable se reemplazan las igualdades por divisibilidades y el mismo razonamiento aplica.

Si K no es normal, entonces sea N su clausura normal. Por el teorema anterior y el caso normal se cumple que

$$[N:k] = \mathrm{N}(N/k) = \mathrm{N}(N/K)\,\mathrm{N}(K/k) \leq [N:K]\,\mathrm{N}(K/k),$$

por lo que se concluye que también aplica. □

Una pregunta curiosa sería ver si el converso es cierto. La respuesta es que sí y la veremos en un teorema más adelante.

Teorema 4.45 – *Teorema del elemento primitivo*: Toda extensión finita separable es simple.

Demostración: Sea K/k la extensión de cuerpos. Si k es finito, entonces $K^\times$ es un grupo cíclico (por el teorema 4.69 más adelante) por lo que tiene un generador γ y claramente $K = k(\gamma)$.

Si k es infinito: Por inducción basta probar el caso cuando K/k está generado por dos elementos. Así pues, sea $K = k(\alpha,\beta)$, queremos probar que $K = k(\gamma)$. Sea A el conjunto de todos los pares (α',β'), donde α',β' son k-conjugados de α y β resp. Si $(\alpha_1,\beta_1),(\alpha_2,\beta_2) \in A$, entonces existe a lo más un $u \in k$ tal que $\alpha_1 + u\beta_1 = \alpha_2 + u\beta_2$. Como A es finito y k infinito, entonces existe un $v \in k$ tal que $\alpha_1 + v\beta_1 \neq \alpha_2 + v\beta_2$ para todo $(\alpha_1,\beta_1),(\alpha_2,\beta_2) \in A$.

Sea $\gamma := \alpha + v\beta$ y sean σ,τ dos k-monomorfismos de K en una clausura normal de K. Luego, como $(\sigma(\alpha),\sigma(\beta)),(\tau(\alpha),\tau(\beta)) \in A$, entonces

$$\sigma(\gamma) = \sigma(\alpha) + v\sigma(\beta) \neq \tau(\alpha) + v\tau(\beta) = \tau(\gamma).$$

Es decir, γ posee $\mathrm{N}(K/k)$ conjugados. Pero como K es separable, entonces vemos que

$$[k(\gamma):k] = \mathrm{N}(k(\gamma)/k) = \mathrm{N}(K/k) = [K:k].$$

Luego, como $K/k(\gamma)$ es una extensión de cuerpos de dimensión 1 se concluye la igualdad. □

Corolario 4.46: Sea L/k una extensión finita de cuerpos. Definamos L_s como los elementos de L que son separables sobre k. Entonces L_s/k es una extensión finita separable y L/L_s es una extensión finita puramente inseparable.

Demostración: Nótese que L_s es cuerpo porque dados $\alpha, \beta \in L$ separables con $\beta \neq 0$ se cumple que $\alpha + \beta, \alpha \cdot \beta$ y α/β son elementos de $k(\alpha, \beta)$ el cual es separable. La finitud del grado se sigue de ser subextensión. Más aún, $L_s = k(\gamma)$ por el teorema anterior. Veamos que L/L_s es puramente inseparable, de lo contrario, existiría $\alpha \in L$ que es inseparable en L_s, pero no es la única raíz de su polinomio minimal. Luego, considerando una potencia adecuada, se cumple que α^q es separable en L_s y luego lo es en k, y finalmente $\alpha_q \in L_s$. □

A L_s le decimos la ***clausura separable*** de k en L.

Proposición 4.47: Para toda extensión K/k y todo $H \leq \mathrm{Gal}(K/k)$ se cumple que $F(H)$ es un cuerpo y $k \leq F(H) \leq K$.

Teorema 4.48: Una extensión finita K/k es de Galois syss

$$F(\mathrm{Gal}(K/k)) = k.$$

Demostración: $\Longrightarrow$. Sea $\alpha \in K$, hemos de probar que existe un k-isomorfismo de K que mueve a α. Sea $f(x)$ su polinomio minimal, como K es de escisión sobre $f(x)$ contiene a todas sus raíces, así que si existe otra raíz β de $f(x)$ existe un k-isomorfismo tal que $\sigma(\alpha) = \beta$. Si no existe otra raíz entonces $f(x) = (x - \alpha)^n$ y por separabilidad $n = 1$ por lo que $\alpha \in k$.

$\Longleftarrow$. Sea $\alpha \in K \setminus k$ de polinomio minimal $f(x)$. Sean $\alpha_1, \ldots, \alpha_n$ todas las raíces distintas de $f(x)$ en K, entonces definimos

$$g(x) := (x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$$

que satisface que $g(x) \mid f(x)$ por construcción.

Sea $\sigma \in \mathrm{Gal}(K/k)$. Como $\sigma(\alpha_i) = \alpha_j$ por ser k-conjugados, entonces se cumple que $(g \circ \sigma)(x) = \prod_{i=1}^{n}(x - \sigma(\alpha_i)) = g(x)$ de modo que todos los coeficientes de $g(x)$ están fijados por un k-automorfismo σ cualquiera, de modo que los coeficientes de $g(x)$ *deben* estar en k.

Luego, como α es raíz de $g(x) \in k[x]$ se cumple que $f(x) \mid g(x)$. Pero entonces $f(x)$ y $g(x)$ están asociados, y como ambos son mónicos entonces

son iguales, probando que f se escinde en K (luego es normal) y que sus raíces son simples (luego es separable). □

Lema 4.49 (de independencia de Dedekind): Sean $\sigma_1, \ldots, \sigma_n$ automorfismos de un cuerpo K. Si $\sum_{i=1}^n c_i\sigma_i(a) = 0$ para todo $a \in K$, entonces $c_1 = c_2 = \cdots = c_n = 0$.

Demostración: Lo demostraremos por inducción sobre n. El caso base es trivial pues $c_1\sigma_1(1) = c_1 = 0$. Supongamos que $\sum_{i=1}^n c_i\sigma_i(a) = 0$ para todo a, si algún c_i es nulo, el resto lo son por inducción. Como $\sigma_1 \neq \sigma_n$, entonces existe $b \in K$ no nulo tal que $\sigma_1(b) \neq \sigma_n(b)$. Nótese que como b es invertible se cumple que el enunciado equivale a que para todo $a \in K$ se cumple que

$$\sum_{i=1}^n c_i\sigma_i(ba) = \sum_{i=1}^n c_i\sigma_i(b) \cdot \sigma_i(a) = 0.$$

Como $\sigma_i(b) \neq 0$, entonces todos los coeficientes que acompañan a $\sigma_i(a)$ siguen siendo no nulos. Luego se cumple que

$$\sum_{i=1}^n c_i(1 - \sigma_n(b^{-1})\sigma_i(b))\sigma_i(a) = \sum_{i=1}^n c_i\sigma_i(a) + \sum_{i=1}^n c_i\sigma_n(b^{-1})\sigma_i(b)\sigma_i(a) = 0,$$

sin embargo, $c_i(1-\sigma_n(b^{-1})\sigma_i(b))$ tiene un coeficiente nulo en el índice $i = n$, por lo que, por hipótesis de inducción se cumple que $1 - \sigma_n(b^{-1})\sigma_i(b) = 0$ para todo i, lo que implica que $\sigma_1(b) = \sigma_n(b)$ que es absurdo. □

Teorema 4.50: Sea K/k una extensión de cuerpos con $H \leq \mathrm{Gal}(K/k)$ entonces

$$[K : F(H)] = |H|.$$

En consecuncia, K/k finita es de Galois syss $|\mathrm{Gal}(K/k)| = [K : k]$.

Demostración: Lo haremos por contradicción suponiendo que $\{a_1, \ldots, a_m\}$ es una $F(H)$-base de K, y $H = \{\sigma_1, \ldots, \sigma_n\}$. Supongamos que $m < n$: Entonces la aplicación

$$\begin{aligned} f : K^n &\longrightarrow K^m \\ (x_1, \ldots, x_n) &\longmapsto \left(\sum_{i=1}^n x_i\sigma_i(a_1), \sum_{i=1}^n x_i\sigma_i(a_2), \ldots, \sum_{i=1}^n x_i\sigma_i(a_m)\right) \end{aligned}$$

es lineal y $n = \dim_K(K^n) = \dim(\ker f) + \dim(\mathrm{Img}\, f) \leq \dim(\ker f) + m$, de modo que $\dim(\ker f) \neq 0$ y el kernel es no vacío y por ende posee un elemento $(c_1, \ldots, c_n) \neq \vec{0}$. Nótese que por definición de base todo $\beta \in K$ se escribe como $\beta = \sum_{i=1}^{m} \lambda_i a_i$ con $\lambda_i \in F(H)$, luego como los λ_i están fijos bajo los k-automorfismos, se cumple que

$$\sum_{j=1}^{n} c_j \sigma_j(\beta) = \sum_{j=1}^{n} \sum_{i=1}^{m} c_j \lambda_i \sigma_j(a_i) = \sum_{i=1}^{m} \lambda_i \left(\sum_{j=1}^{n} c_j \sigma_j(a_i) \right) = 0$$

que es nulo, pues los términos en rojo lo son por definición de $(c_1, \ldots, c_n)$. Pero por el lema de independencia de Dedekind se cumple que los c_j's son nulos lo que es absurdo.

Supongamos que $m > n$: Considerando un truco similar al anterior construimos:

$$\begin{aligned} f : K^{n+1} &\longrightarrow K^n \\ (x_1, \ldots, x_{n+1}) &\longmapsto \left(\sum_{i=1}^{n+1} x_i \sigma_1(a_i), \ldots, \sum_{i=1}^{n+1} x_i \sigma_n(a_i) \right) \end{aligned}$$

tal que posee kernel no vacío y Elegimos $(c_1, \ldots, c_{n+1}) \neq \vec{0}$ que pertenezca al kernel tal que posea la máxima cantidad de coordenadas nulas, podemos elegirlas de tal modo que $c_1, \ldots, c_p$ sean no nulos y $c_{p+1}, \ldots, c_{n+1}$ lo sean, aunque nótese que $p > 1$.

Como H es subgrupo, entonces contiene a la identidad, y supongamos que ésta ocupa el j-ésimo lugar; luego como $\sum_{i=1}^{n+1} c_i a_i = 0$ se concluye que no todos los c_i's están en $F(H)$ (pues los a_i's son linealmente independientes). Luego, como $c_p \neq 0$ multiplicamos por c_p^{-1} para asumir que $c_p = 1$. También podemos reordenar los c_i's de tal modo que $c_1 \notin F(H)$; por lo que existe algún σ_h tal que $\sigma_h(c_1) \neq c_1$. Nótese que como H es grupo, el producto $\tau \mapsto \tau \circ \sigma_h$ es una permutación, de modo que al aplicar σ_h a las n-tuplas, de modo que

$$\forall j \in \{1, \ldots, n\} \quad \sum_{i=1}^{n+1} \sigma_h(c_i) \sigma_j(a_i) = 0$$

finalmente notamos que

$$\forall j \in \{1, \ldots, n\} \quad \sum_{i=1}^{n+1} (c_i - \sigma_h(c_i)) \sigma_j(a_i) = 0$$

por lo que $d_i := c_i - \sigma_h(c_i)$ conforman una tupla del kernel. Sin embargo, nótese que $d_p, d_{p+1}, \ldots, d_n$ son todos nulos, contradiciendo la maximalidad de ceros de $(c_1, \ldots, c_{n+1})$. □

Corolario 4.51: Sea L/k una extensión finita normal. Sea L_s la clausura separable de k en L y sea L_i el conjunto de elementos puramente inseparables de L/k. Entonces:

1. L_i/k es una extensión finita puramente inseparable.
2. L está generado por L_s y L_i.
3. L/L_i es una extensión de Galois y $\mathrm{Gal}(L/k) = \mathrm{Gal}(L/L_i)$.
4. $[L : L_i] = [L_s : k]$ y $[L : L_s] = [L_i : k]$.

Demostración:

1. Sea $K := F\big(\mathrm{Gal}(L/k)\big)$ el cuerpo fijado, veremos que $K = L_i$. Sea $a \in K$ que no es puramente inseparable sobre k, entonces a no es la única raíz de su polinomio minimal y por lo tanto posee un k-conjugado b tal que $b \neq a$. Luego existe $\sigma \in \mathrm{Gal}(L/k)$ tal que $\sigma(a) = b \neq a$ lo que contradice que $a \in K$. Ésto prueba que $K \subseteq L_i$ y la otra inclusión también es clara puesto que los puramente inseparables sólo poseen un k-conjugado.
2. Sea $L_0 := L_s \vee L_i$ y nótese que L/L_0 es una extensión de cuerpos. Como L/L_s es puramente inseparable, entonces L/L_0 es puramente inseparable. Como L/L_i es separable, entonces L/L_0 también debe ser separable. Finalmente $L = L_0$ es la única extensión separable y puramente inseparable de L_0.
3. La demostración anterior prueba que $\mathrm{Gal}(L/k) = \mathrm{Gal}(L/L_i)$ y también vimos que $F\big(\mathrm{Gal}(L/L_i)\big) = L_i$, de modo que la extensión es de Galois por el teorema 4.48.
4. Nótese que $[L : L_i] = |\mathrm{Gal}(L/L_i)| = |\mathrm{Gal}(L/k)| = [L_s : k]$ y la otra igualdad se sigue de la transitividad de grados. □

Teorema 4.52 – *Teorema fundamental de la teoría de Galois*: Sea K/k una extensión finita de Galois. Denotando $G := \mathrm{Gal}(K/k)$ y

$$\{L : K/L/k \text{ extensiones}\} \underset{F(H)}{\overset{\mathrm{Gal}(K/L)}{\rightleftarrows}} \{H : H \leq G\}$$

entonces:

1. $F(H)$ y H_L son biyecciones, la una la inversa de la otra. Más aún, si $H_1 < H_2 \leq G$, entonces $K \supseteq F(H_2) \supset F(H_1)$, y si $k \subseteq L_1 \subset L_2 \subseteq K$, entonces $\mathrm{Gal}(K/L_1) > \mathrm{Gal}(K/L_2)$. En consecuencia, F es un funtor contravariante biyectivo:

$$\begin{array}{ccc} L_2 & & H_2 \\ \uparrow & \overset{\mathrm{Gal}(K/L)}{\Longrightarrow} & \downarrow \\ & \underset{F(H)}{\Longleftarrow} & \\ L_1 & & H_1 \end{array}$$

2. Si $K/L/k$, entonces K/L es de Galois.

3. Si $K/L/k$, entonces L/k es de Galois syss $\mathrm{Gal}(K/L) \trianglelefteq G$.

4. Si $K/L/k$ y L/k es de Galois, entonces

$$\begin{aligned} r\colon \mathrm{Gal}(K/k) &\longrightarrow \mathrm{Gal}(L/k) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

   es un epimorfismo de grupos y $\ker r = \mathrm{Gal}(K/L)$. En consecuencia, $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L) \cong \mathrm{Gal}(L/k)$.

5. Si $H_1, H_2 \leq \mathrm{Gal}(K/k)$, entonces

$$F(\langle H_1, H_2\rangle) = F(H_1) \cap F(H_2), \quad F(H_1 \cap H_2) = F(H_1) \vee F(H_2).$$

Demostración:

2. Como K/k es normal, entonces es el cuerpo de escisión de $f(x) \in k[x]$. Luego $f(x) \in L[x]$ y claramente K es el cuerpo de escisión de $f(x)$. Luego K/L es de Galois pues es normal y separable.

1. Probaremos que la una es la inversa de la otra. Sea $K/L/k$, como K/L es de Galois, entonces $F(\mathrm{Gal}(K/L)) = L$.

   Por otro lado, sea $H \leq \mathrm{Gal}(K/k)$, entonces claramente $H \leq \mathrm{Gal}(K/F(H))$. Más aún $K/F(H)$ es de Galois, por lo que $|H| = [K : F(H)] = |\mathrm{Gal}(K/F(H))|$, y como H es finito, se da que $\mathrm{Gal}(K/F(H)) = H$.

3. $\Longrightarrow$. Si L/k es de Galois, entonces es normal. Sea $\sigma \in \mathrm{Gal}(K/L)$ y $\tau \in \mathrm{Gal}(K/k)$, entonces $\tau^{-1} \in \mathrm{Gal}(K/k)$. Sea $\alpha \in L$, nótese que τ^{-1} manda α a sus k-conjugados, luego $\tau^{-1}(\alpha) \in L$. Como σ fija a L se cumple que $\sigma\big(\tau^{-1}(\alpha)\big) = \tau^{-1}(\alpha)$ y en consecuente, $\tau\big(\sigma(\tau^{-1}(\alpha))\big) = \alpha$, por lo que $\tau^{-1}\sigma\tau \in \mathrm{Gal}(K/L)$. Es decir, $\mathrm{Gal}(K/L) \trianglelefteq \mathrm{Gal}(K/k)$ por definición de subgrupo normal.

   $\Longleftarrow$. Sea $\alpha \in L$ y sea $f(x) \in k[x]$ su polinomio minimal. Para probar que L/k es normal, basta ver que todos los k-conjugados de α están en L. Luego sea β un k-conjugado de α, sabemos que existe $\tau \in \mathrm{Gal}(K/k)$ tal que $\tau^{-1}(\alpha) = \beta$.

   Como $F(\mathrm{Gal}(K/L)) = L$, basta ver que todo σ fija a β. Sea $\sigma \in \mathrm{Gal}(K/L)$, entonces

$$\tau\big(\sigma(\tau^{-1}(\alpha))\big) = \tau(\sigma(\beta)) = \alpha \iff \sigma(\beta) = \tau^{-1}(\alpha) = \beta.$$

4. Ejercicio para el lector.

5. Basta notar que $\langle H_1, H_2\rangle$ es el mínimo subgrupo que contiene a H_1, H_2 y que $F(H_1) \cap F(H_2)$ es el máximo subcuerpo contenido en $F(H_1)$ y $F(H_2)$. □

4.4 Cuerpos algebraicamente cerrados

Lema 4.53: Sea K/k una extensión de cuerpos, entonces son equivalentes:

1. K no tiene extensiones algebraicas distintas de sí mismo.
2. Todo polinomio no constante de K tiene raíz.
3. Los polinomios irreductibles de K son de grado 1.
4. Todo polinomio de K se escinde.
5. K contiene un subcuerpo tal que la extensión K/k es algebraica y todo polinomio de $k[x]$ se escinde en K.

Demostración: 1 $\Longrightarrow$ 2. Sea $f(x) \in K[x]$ un polinomio no constante, luego éste posee un factor irreductible $g(x)$ de manera que existe una extensión $K(\alpha)/K$ con una raíz α de $g(x)$, pero $K(\alpha) = K$ puesto que toda extensión finita es algebraica, de modo que $\alpha \in K$.

$2 \implies 3$. Sea $f(x) \in K[x]$ con $\deg f > 1$. Entonces $f(x)$ posee raíz α y por Ruffini se satisface que $(x-\alpha) \mid f(x)$, por lo que $f(x)$ no es irreductible.

$3 \implies 4$. Basta notar que K es un DFU y aplicar descomposición en factores irreducibles.

$4 \implies 5$. Basta tomar $K = k$.

$5 \implies 1$. Sea L/K una extensión y $\alpha \in L$ un elemento algebraico, probaremos que $\alpha \in K$. Por definición existe un polinomio $f(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$ tal que α es raíz de $f(x)$. Como K/k es algebraico, entonces $K(c_0, \ldots, c_n)$ es una extensión finita y claramente $[K(c_0, \ldots, c_n; \alpha) : K(c_0, \ldots, c_n)] < \infty$ de modo que α es k-algebraico y, por lo tanto, es raíz de un polinomio $g(x) \in k[x]$. Pero como $g(x)$ se escinde en K, entonces $\alpha \in K$. Si L es una extensión algebraica, todos sus elementos lo son, luego todos están en K y en consecuencia $L = K$. □

Definición 4.54 – *Cuerpo algebraicamente cerrado*: Un cuerpo K es algebraicamente cerrado si cumple alguna (y por ende todas) las condiciones del lema anterior.

Dado un cuerpo k, se dice que una extensión K/k es una ***clausura algebraica*** de k si K/k es una extensión algebraica y K es algebraicamente cerrado.

Nótese que por el lema probar que K escinde los polinomios de k basta para notar que K es una clausura algebraica.

Teorema 4.55: Sea K/k una extensión algebraicamente cerrada, entonces

$$L := \{\alpha \in K : \alpha \text{ es } k\text{-algebraico}\}$$

es un cuerpo y de hecho L/k es una clausura algebraica.

Demostración: Ya vimos que L forma una extensión de cuerpo (por el teorema 4.11) y es claro que es algebraica, así pues basta notar que es algebraicamente cerrado.

Sea $f(x) \in k[x]$ no constante, entonces f se escinde en K por definición de algebraicamente cerrado, luego

$$f(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_n),$$

luego $\alpha_0 \in k \subseteq L$ y cada α_i es k-algebraico, luego está en L.

Como L/k es una extensión algebraica tal que todo polinomio de k se escinde en L, se concluye que L es algebraicamente cerrado. □

Teorema 4.56: Si k es finito, entonces no es algebraicamente cerrado. Conversamente, todo cuerpo algebraicamente cerrado es infinito.

Demostración: Si k es finito entonces sea $k = \{\alpha_1, \ldots, \alpha_n\}$, luego $f(x) := 1 + \prod_{i=1}^{n}(x - \alpha_i)$ es un polinomio no nulo que vale 1 en todo k, por lo que no tiene raíces en k y por ende, k no puede ser algebraicamente cerrado. □

Teorema (TUF) 4.57: Todo cuerpo posee una clausura algebraica.

Demostración: Sea k un cuerpo. Ésta demostración emplea un truco atribuido a Artin. La idea será seguir la demostración de las extensiones de Kronecker, pero introduciendo todas las raíces en simultáneo.

Sea $\mathcal{P}$ el conjunto de polinomios de $k[x]$ no constantes. Luego sea $y_- : \mathcal{P} \to S$ una biyección, es decir, todo elemento de S se denota por $y_{f(x)}$ donde $f(x) \in \mathcal{P}$. Así, construyamos $k[S]$, es decir, el anillo de polinomios cuyas variables son los y_p's. Y construyamos el siguiente ideal:

$$\mathfrak{a} := \big(f(y_p) : f(x) \in \mathcal{P}\big).$$

1. $\mathfrak{a}$ es un ideal propio, es decir, $1 \notin \mathfrak{a}$: Procedamos por contradicción: supongamos que $1 \in \mathfrak{a}$, entonces existen $\lambda_i \in k[S]$ y $f_i \in \mathcal{P}$ tales que

   $$\lambda_1 f_1(y_{f_1}) + \cdots + \lambda_n f_n(y_{f_n}) = 1.$$

   Nótese que como cada λ_i posee finitos monomios, cada uno con finitas variables, en definitiva hay solo finitas variables en la ecuación anterior que podemos suponer son $F := \{y_{f_1}, y_{f_2}, \ldots, y_{f_n}, z_1, z_2, \ldots, z_m\}$.

   Luego, la combinación lineal también vale en $k[F]$, pero he aquí un truco: Como hay finitos polinomios f_i's, entonces existe una extensión finita L/k tal que $\alpha_i \in L$ es raíz de f_i resp. Como $k \subseteq L$, entonces la ecuación también vale en $L[F]$. Pero evaluando y_{f_i} en α_i y z_j en 0 se obtiene que

   $$\lambda_1(\alpha_1, \ldots, \alpha_n, 0, \ldots, 0)f_1(\alpha_1) + \cdots + \lambda_n(\alpha_1, \ldots, \alpha_n, 0, \ldots, 0)f_n(\alpha_n) = 1$$

   donde cada término en rojo vale cero por definición de α_i, es decir, $0 = 1$; lo que es absurdo.

2. Por el teorema de Krull, existe $\mathfrak{m} \supseteq \mathfrak{a}$ que es un ideal maximal. Luego $K_0 := k[S]/\mathfrak{m}$ es un cuerpo que extiende a k.

2.* *(Si se quiere evitar el AE.)*[1] Como $\mathfrak{a}$ es ideal propio, existe $\mathfrak{p}$ primo que le contiene. Luego $k[S]/\mathfrak{p}$ es un dominio íntegro y, por lo tanto, $K_0 := \mathrm{Frac}(k[S]/\mathfrak{p})$ es una extensión de cuerpos de k.

3. Veamos que cada polinomio en k no constante posee una raíz en K_0: En efecto, sea $f(x) \in \mathcal{P}$, luego $\alpha := [y_f]$ satisface que

$$f(\alpha) = [f(y_f)] = 0$$

puesto que $f(y_f) \in \mathfrak{a} \subseteq \mathfrak{m}$.

4. Iterando la construcción podemos definir K_1 que extiende a K_0 y tal que todo polinomio no constante en K_0 tiene raíz. Y así construir K_2, y K_3, y así sucesivamente.

   Finalmente definamos $K := \bigcup_{n\in\mathbb{N}} K_n$. Éste extiende a todos los K_i's y por consecuente también al cuerpo inicial k. Más aún, K es algebraicamente cerrado: Para probarlo, sea $f(x) \in K[x]$ no constante, luego posee finitos coeficientes los cuales están contenidos en algún K_n para un n suficientemente grande, es decir, $f(x) \in K_n[x]$. Pero por construcción, existe $\alpha \in K_{n+1}[x]$ que es raíz de $f(x)$ y $\alpha \in K_{n+1} \subseteq K$.

5. Como K/k es algebraicamente cerrado, por el teorema 4.55 admite un subcuerpo que es una clausura algebraica de k, que es lo que se quería probar. □

Teorema (AE) 4.58: Las clausuras algebraicas de k son k-isomorfas.

Demostración: Sean $K_1/k, K_2/k$ clausuras algebraicas de k. La idea será aplicar el lema de Zorn sobre las subextensiones de K_1 para construir el isomorfismo. Primero definamos

$$\mathcal{F} := \{(L, \tau) : K_1/L/k \text{ extensión y } \tau\colon L \to K_2 \ k\text{-morfismo}\},$$

y también definamos la relación $\preceq$ sobre $\mathcal{F}$:

$$(L_1, \sigma_1) \preceq (L_2, \sigma_2) \iff L_1 \subseteq L_2 \wedge \sigma_2|_{L_1} = \sigma_1.$$

Nótese que $\preceq$ es un orden parcial. Tenemos que comprobar que toda $\preceq$-cadena C está acotada superiormente, para ello nótese que

$$L := \bigcup_{(K_i,\sigma_i)\in C} K_i$$

[1] Idea original de Banaschewski **[0]** (1992).

y $\sigma\colon L \to K_2$ dado por $\sigma(\alpha) = \tau_i(\alpha)$ donde $\alpha \in K_i$ donde $(K_i, \sigma_i) \in C$. Así pues (L, σ) es una cota superior de C (¿por qué?).

Luego, por el lema de Zorn se cumple que $\mathcal{F}$ tiene un elemento $\subseteq$-maximal (M, σ). Veamos que $M = K_1$: Sea $\alpha \in K_1$, entonces α es k-algebraico, luego es la raíz de un polinomio $f(x)$. Sea $M' := \sigma[M] \subseteq K_2$, se cumple que existe β raíz de $\sigma f(x)$ (por ser algebraicamente cerrado). Luego, por el teorema se tiene que

$$\begin{array}{ccc} M(\alpha) & \overset{\sigma^*}{\rightsquigarrow} & M'(\beta) \\ \uparrow & & \uparrow \\ M & \underset{\sigma}{\rightsquigarrow} & M' \end{array}$$

por lo que $(M, \sigma) \preceq \big(M(\alpha), \sigma^*\big)$. Pero como M es maximal se da la igualdad y $\alpha \in M$.

Finalmente, veamos que $\sigma\colon K_1 \to K_2$ es suprayectiva: Sea $\beta \in K_2$, luego β es k-algebraico así que es la raíz de $f(x) \in k[x]$. Como $f(x)$ se escinde en K_1 y σ manda raíces de $f(x)$ en raíces de $f(x)$, se ha de cumplir que β tiene preimagen. Como σ es suprayectiva e inyectiva (por ser k-morfismo), entonces es biyección, luego isomorfismo. □

También podemos probar a mano el caso finito y evitar el uso de elección:

Teorema 4.59: Si k posee una clausura algebraica que es finita como extensión, entonces todas sus clausuras son isomorfas.

Demostración: Si K_1/k es clausura algebraica finita de k, entonces $K_1 = k(\alpha_1, \ldots, \alpha_n)$ donde cada α_i es raíz de $f_i(x) \in k[x]$. Luego sea $g(x) := f_1(x)f_2(x)\cdots f_n(x) \in k[x]$. Entonces K_1 es el cuerpo de escisión de $g(x)$ y así se puede concluir el enunciado. □

Definición 4.60: En consecuencia de los teoremas anteriores se denota por k^{alg} a la clausura algebraica de k.

Se denota por $\mathbb{A} := \mathbb{Q}^{\text{alg}}$ a la clausura algebraica de $\mathbb{Q}$, a cuyos elementos llamamos ***números algebraicos***.

De la construcción de la clausura algebraica, y dado que éstas son isomorfas, podemos notar otro dato útil:

Proposición 4.61: Sea k un cuerpo, su clausura algebraica tiene cardinalidad $|k^{\text{alg}}| = k + \aleph_0$.

De ello, podemos deducir que $\mathbb{A}$ es numerable, por lo cual $\mathbb{C}$ debe contener números $\mathbb{Q}$-trascendentes (¡y de hecho, la mayoría lo son!). Los ejemplos usuales son e y π, los cuales tratamos en la sección §10.4.3.

§4.4.1 Aplicación: El teorema fundamental del álgebra II. Aquí veremos una aplicación de las extensiones de cuerpo que hemos estudiado.

Teorema 4.62: Sea R un cuerpo ordenado con las siguientes propiedades:

1. Todo $\alpha \in R_{\geq 0}$ posee raíz cuadrada.
2. Todo polinomio de grado impar en R posee alguna raíz en R.

Sea $K := R(i)$, donde i es una raíz del polinomio $x^2 + 1$, entonces K es algebraicamente cerrado. En particular $\mathbb{C}$ lo es.

Demostración: Como R es un cuerpo de característica nula, entonces es perfecto. Sea L/R una extensión de cuerpo finita que podemos suponer normal (¿por qué?), luego de Galois. Como es de Galois $|\operatorname{Gal}(L/R)| = [L : R] = 2^n m$ con m impar.

Por el primer teorema de Sylow, existe H un 2-subgrupo de Sylow de modo que $[L : F(H)] = |H| = 2^n$ y $[F(H) : R] = m$. Como $F(H)/R$ es de grado impar, entonces sus elementos son algebraicos de grado impar, i.e., cuyos polinomios minimales son de grado impar, lo cual es absurdo pues sabemos que tiene raíces en R. En conclusión L debe ser de grado una potencia de 2.

Como $[L : R] = 2^n$, se tiene que posee un subgrupo H tal que $[L : F(H)] = |H| = 2^{n-1}$ y $[F(H) : R] = 2$, luego $F(H) = K$. Así L es extensión de cuerpos de K. Luego, existe H' tal que $[L : F(H')] = 2^{n-2}$ y $[F(H') : K] = 2$ lo cual es imposible pues todo polinomio cuadrático de K es reducible. □

4.5 Otras aplicaciones

§4.5.1 Norma y traza. Ya vimos en las secciones anteriores que más que trabajar en extensiones normales, podemos sustituir los k-automorfismos por k-morfismos hasta su clausura normal. De éste modo se obtiene lo siguiente:

Definición 4.63: Sea K/k una extensión finita y sea $\alpha \in K$. Nótese que $m_\alpha(x) := \alpha \cdot x$ es una k-transformación lineal sobre K y como K es de dimensión finita se pueden definir la ***norma***, la ***traza*** y el ***polinomio característico*** de α como:

$$\mathrm{Tr}_{K/k}(\alpha) := \mathrm{tr}(m_\alpha), \qquad \mathrm{Nm}_{K/k}(\alpha) := \det(m_\alpha),$$
$$\psi_{\alpha,K/k}(t) := \psi_{m_\alpha}(t) \in k[t]$$

Usualmente la definición es otra, más relacionada con la conjugación, pero veremos que ambas coinciden.

Proposición 4.64: Sea K/k una extensión finita y sean $\alpha, \beta \in K$, entonces:

$$\mathrm{Tr}_{K/k}(\alpha+\beta) = \mathrm{Tr}_{K/k}(\alpha) + \mathrm{Tr}_{K/k}(\beta), \quad \mathrm{Nm}_{K/k}(\alpha\cdot\beta) = \mathrm{Nm}_{K/k}(\alpha)\cdot\mathrm{Nm}(\beta).$$

Teorema 4.65: Dada una extensión finita K/k, N su clausura normal de K y sea $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_k(K, N)$. Entonces para todo $\alpha \in K$ se satisface que

$$\mathrm{Nm}_{K/k}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{Tr}_{K/k}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$
$$\psi_{\alpha,K/k}(t) = (t - \sigma_1(\alpha)) \cdots (t - \sigma_n(\alpha))$$

Demostración: Por la proposición 3.67 basta demostrar la identidad con el polinomio característico. Sea $\alpha \in K$ un elemento primitivo de K, de modo que su polinomio minimal es $f(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$. Como α es primitivo, entonces $(1, \alpha, \ldots, \alpha^{n-1})$ es una base ordenada de K como k-espacio vectorial, de modo que la matriz de la transformación lineal m_α en dicha base es

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

De modo que el polinomio característico es el determinante de

$$\begin{bmatrix} t & 0 & \cdots & 0 & a_0 \\ -1 & t & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t+a_{n-1} \end{bmatrix},$$

el cual es de hecho el polinomio minimal $f(t)$ (¿por qué?).

Sea $\alpha \in K$ un elemento genérico. Definamos $L := K(\alpha)$, luego se tiene que podemos elegir una base $(y_1, \ldots, y_p)$ de L/k y una base $(z_1, \ldots, z_q)$ de K/L, de modo que $(y_i z_j)_{ij}$ es una base de K/k con el orden lexicográfico. Sea $M := [a_{ij}]_{ij}$ la matriz de m_α en la base $(y_j)_j$, es decir, $\alpha y_i = \sum_{h=1}^{p} a_{ih} y_h$. Luego vemos que

$$\alpha(y_i z_j) = (\alpha y_i) z_j = \sum_{h=1}^{n} a_{ih} y_h z_j.$$

Así pues, la representación matricial de m_α es

$$\begin{bmatrix} M & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & M & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & M \end{bmatrix} \in \mathrm{Mat}_{pq}(k).$$

De ésto se sigue que si $\psi_{\alpha,L/k}$ es el polinomio minimal, entonces $\psi_{\alpha,K/k}(t) = \big(\psi_{\alpha,L/k}(t)\big)^q$. Ésto concluye el teorema. □

Ejemplo. En la extensión $\mathbb{C}/\mathbb{R}$, la norma y traza son:

$$\mathrm{Nm}_{\mathbb{R}}^{\mathbb{C}}(z) = z \cdot \overline{z} = |z|^2, \qquad \mathrm{Tr}_{\mathbb{R}}^{\mathbb{C}}(z) = z + \overline{z} = 2\,\mathrm{Re}(z).$$

Teorema 4.66 (transitividad de la norma y de la traza): Sean $L/K/k$ extensiones finitas, entonces:

$$\mathrm{Nm}_{L/k} = \mathrm{Nm}_{L/K} \circ \mathrm{Nm}_{K/k}, \qquad \mathrm{Tr}_{L/k} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{K/k}\,.$$

§4.5.2 Raíces de la unidad y extensiones ciclotómicas. Recordemos que un elemento de un cuerpo ω se dice una n-ésima raíz de la unidad si $\omega^n = 1$. Ésto lo habíamos estudiado en el caso complejo, pero la teoría de cuerpos admite mayor diámetro. Comenzaremos con un teorema curioso que prueba ser útil en teoría de números y teoría de la representación.

Teorema 4.67: $\sum_{d|n} \phi(d) = n.$

Pista: Estudie el orden de los elementos del grupo $\mathbb{Z}/n\mathbb{Z}$. Si no, cf. **[57,** Prop. 3.5]. □

Lema 4.68: Sea G un grupo finito de orden g y denotemos por $S_d := \{x \in G : x^d = 1\}$. Entonces G es cíclico syss para todo $d \mid g$ se cumple que $|S_d| \leq d$, o equivalentemente, si para todo $d \in \mathbb{N}_{\neq 0}$ se cumple que $|S_d| \leq d$.

Demostración: $\Longleftarrow$. Denotemos por T_d a los elementos de orden d. Si $x \in T_d$, entonces $\langle x \rangle \subseteq S_d$ y como $|\langle x \rangle| = d \geq |S_d|$ se concluye que $\langle x \rangle = S_d$. Luego, $x^r \in T_d$ syss $(d; r) = 1$, de modo que $|T_d| = \phi(d)$. Como todo $x \in G$ tiene un orden d con $d \mid n$, entonces

$$\sum_{T_d \neq \varnothing} \phi(d) = |G| = \sum_{d|n} \phi(d),$$

pero, por lo tanto, debe cumplirse que todos los T_d's con $d \mid n$ son no vacíos y, en particular, $T_n \neq \varnothing$.

$\Longrightarrow$. Aplíquese el teorema y el razonamiento anterior para comprobar que $|S_d| = d$. □

Con ésto probamos que:

Teorema 4.69: Si k es un cuerpo finito, entonces $k^\times$ es cíclico.

Teorema 4.70: Sea $\operatorname{car} k = p$ y L/k el cuerpo de escisión de $f(x) := x^n - 1$. El conjunto de las n-ésimas raíces de la unidad Z con la multiplicación conforma un grupo cíclico. Más aún:

(a) Si $p \nmid n$ (incluyendo $p = 0$), entonces $|Z| = n$.

(b) Si $n = p^r m$ con $p \nmid m$, entonces $|Z| = m$.

En el caso (a), los generadores de Z se dicen n-ésimas raíces ***primitivas*** de la unidad.

Demostración: En el caso (a): Como $f(x)$ es separable, puesto que su derivada nx^{n-1} tiene solo raíces nulas, se concluye que efectivamente hay n raíces distintas de la unidad. En el caso (b): Vemos que, por el sueño del

aprendiz, $f(x) = (x^m)^{p^r} - 1 = (x^m - 1)^{p^r}$, de modo que Z se corresponde con las m-ésimas raíces de la unidad y nos reducimos al caso (a). Para comprobar que es cíclico basta aplicar el lema 4.68. □

Por ejemplo: claramente el 1 no es una raíz n-ésima de la unidad primitiva, excepto para $n = 1$.

Definición 4.71: Sea k un cuerpo, el cuerpo de escisión L_n del polinomio $x^n - 1$ se llama la n-ésima ***extensión ciclotómica***. Más generalmente, K se dice una ***extensión ciclotómica*** si existe n tal que $L_n/K/k$ son extensiones de cuerpos.

En teoría algebraica de números, los cuerpos ciclotómicos se asumen como extensiones ciclotómicas de $\mathbb{Q}$.

Definición 4.72: Sea K/k una extensión de Galois. K se dice una ***extensión cíclica*** (resp. ***abeliana***) si $\mathrm{Gal}(K/k)$ es cíclico (resp. abeliano).

Teorema 4.73: Sea k un cuerpo. Entonces:

1. La n-ésima extensión ciclótomica es una extensión cíclica.

2. Toda extensión ciclotómica K/k es abeliana.

Demostración: Basta ver que si L_n es la n-ésima extensión ciclotómica, entonces ésta es abeliana (pues las subextensiones también). Podemos suponer que $\mathrm{car}\, k \nmid n$ de modo que L_n es separable y por ende admite una raíz primitiva ζ tal que $L = k(\zeta)$. Luego todo $\sigma \in \mathrm{Gal}(L/k)$ está determinado por adónde manda ζ y sus conjugados son de la forma ζ^j y es fácil notar que si $\sigma\zeta = \zeta^a$ y $\tau\zeta = \zeta^b$, entonces $\sigma\tau\zeta = \sigma\zeta^b = \zeta^{ab} = \tau\sigma\zeta$. □

De ésta demostración se desprenden fácilmente dos consecuencias:

Teorema 4.74: Si k es un cuerpo finito y K/k es una extensión finita, entonces K/k es una extensión cíclica.

Demostración: Por el teorema 4.35 vemos que todas las extensiones $K/\mathbb{F}_p$ son ciclotómicas y, por tanto, cíclicas. Luego, basta notar que todo cociente de un grupo cíclico es también cíclico para concluir. □

Teorema 4.75: Sea ζ_n una n-ésima raíz primitiva de la unidad en $\mathbb{C}$, y sea $K_n := \mathbb{Q}(\zeta_n)$. La extensión $K_n/\mathbb{Q}$ es de Galois y $\mathrm{Gal}(K_n/K)$ es isomorfo a $U_n := (\mathbb{Z}/n\mathbb{Z})^\times$.

Desde aquí nos dedicamos a estudiar las extensiones ciclótomicas de $\mathbb{Q}$. En particular ya vimos que todas las raíces n-ésimas de la unidad pueden ser generadas a partir de la siguiente:

$$\zeta_n := \mathrm{cis}\left(\frac{2\pi}{n}\right)$$

vale decir, ζ_n^j son todas las raíces n-ésimas de la unidad. En particular ζ_n^j es primitiva syss j y n son coprimos.

Definición 4.76: Se define el n-ésimo ***polinomio ciclotómico*** como

$$\Phi_n(x) := \prod_{\substack{j=1 \\ (j;n)=1}}^{n} (x - \zeta_n^j) \in \mathbb{C}[x].$$

De momento sabemos poco del polinomio ciclotómico exceptuando por tres detalles triviales: El primero es que todas las raíces de Φ_n son exactamente las raíces n-ésimas primitivas de la unidad, el segundo es que $\Phi_n \mid (x^n - 1)$ y el tercero es que Φ_p concuerda con nuestra antigua definición de «Φ_p». La segunda observación se puede mejorar a:

Proposición 4.77: Sea $n > 0$, entonces

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Reordenando la ecuación anterior se obtiene que

$$\Phi_n(x) = \frac{x^n - 1}{\displaystyle\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)}.$$

Ésto puede parecer trivial, pero es de hecho lo que nos permite calcular los

polinomios ciclotómicos:

n	$\Phi_n(x)$
1	$x-1$
2	$x+1$
3	x^2+x+1
4	x^2+1
5	$x^4+x^3+x^2+x+1$
6	x^2-x+1
7	$x^6+x^5+x^4+x^3+x^2+x+1$
8	x^4+1

Una curiosidad de la teoría de números es que los factores pequeños parecen solo constar de coeficientes «± 1», sin embargo, es sabido que el polinomio ciclotómico $\Phi_{105}(x)$ posee un «-2» y es la primera vez que sucede. Se puede demostrar que los coeficientes son arbitrariamente grandes para un índice arbitrariamente grande.

Teorema 4.78: Para todo $n > 0$ se cumplen:

1. $\Phi_n(x)$ es mónico, tiene grado $\phi(n)$ y está en $\mathbb{Z}[x]$.
2. Φ_n es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$, de modo que Φ_n es el polinomio minimal de ζ_n sobre $\mathbb{Q}$.
3. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es un cuerpo de Galois de grado $\phi(n)$ que es, de hecho, el cuerpo de escisión de $x^n - 1$.

Demostración: Para la primera todas son triviales excepto que $\Phi_n \in \mathbb{Z}[x]$, lo cual se demuestra por inducción fuerte empleando nuestro conocimiento sobre el caso primo. Y la tercera es equivalente a la segunda, que es la que vamos a probar.

Para ello, veremos lo siguiente: Si ω es una raíz n-ésima de la unidad primitiva cualquiera, $f(x) \in \mathbb{Q}[x]$ es su polinomio minimal y $p \nmid n$, entonces ω^p también es raíz de $f(x)$. Como todo número coprimo a n se obtiene multiplicando primos que no dividen a n, entonces al comprobar ésto veremos que necesariamente f tiene por raíces a todas las raíces n-ésimas primitivas de la unidad, por lo que $f = \Phi_n$.

Definamos $h(x)$ tal que $x^n - 1 = f(x)h(x)$, y supongamos, por contradicción, que ω^p no es raíz de $f(x)$. Entonces ω^p es raíz de $h(x)$, es decir, ω es raíz de $h(x^p)$ y como f es el polinomio minimal de ω se cumple que existe

$g \in \mathbb{Q}[x]$ tal que

$$h(x^p) = f(x)g(x).$$

Y como h, f tienen coeficientes enteros, entonces g también. Luego, podemos llevar la igualdad anterior a $\mathbb{F}_p$ y notar que $h(x^p) \equiv h(x)^p$ (mód p), por lo que $[\omega]$ es raíz común de f y h, por lo que f, h no son coprimos. Pero $x^n - 1 = f(x)h(x)$ también en $\mathbb{F}_p[x]$, y la derivada es nx^{n-1} el cual no es cero puesto que $p \nmid n$; por lo que no tiene raíces repetidas, pero acabamos de ver que $[\omega]$ está repetida, lo cual es absurdo. □

Teorema 4.79: Sea $\operatorname{car} k = p$ y sea K/k una extensión cíclica de grado n donde o bien $p = 0$ o bien n y p son coprimos. Si k contiene a todas las raíces n-ésimas de la unidad, entonces $L = k(\gamma)$, donde γ es raíz de $x^n - a$ para algún $a \in k$.

Demostración: Como K es cíclica, entonces sea $\langle\sigma\rangle = \operatorname{Gal}(K/k)$ y para todos $x, t \in k$ definamos

$$u(x,t) := \sum_{i=0}^{n-1} \left(\prod_{j=0}^{i-1} \sigma^j(x) \right) \sigma^i(t),$$

en particular, si $x \cdot \sigma(x) \cdots \sigma^{n-1}(x) = 1$, entonces $x \cdot \sigma\big(u(x,t)\big) = u(x,t)$. Sea ζ una n-ésima raíz primitiva de la unidad, entonces como $\zeta \in k$, entonces $\sigma\zeta = \zeta$ y por lo tanto,

$$\zeta \cdot \sigma(\zeta) \cdots \sigma^{n-1}(\zeta) = \zeta^n = 1,$$

El lema de independencia de Dededekind nos dice que existe un t tal que $\gamma := u(\zeta, t) \neq 0$, luego $\zeta\sigma(\gamma) = \gamma$ y en general $\sigma^i(\gamma) = \zeta^{-i}\gamma$. Es decir, todos los k-conjugados de γ son $\gamma, \zeta\gamma, \ldots, \zeta^{n-1}\gamma$, por lo que, $L = k(\gamma)$ y su producto es $\pm\gamma^n \in k$ como se quería probar. □

Teorema 4.80: Sea $\operatorname{car} k = p \neq 0$, y sea $f_a(x) := x^p - x - a \in k[x]$.

1. Si $f_a(x)$ no tiene raíces en k y γ es una raíz, entonces $k(\gamma)$ es cíclica de grado p.
2. Si K/k es una extensión cíclica de grado p, entonces $K = k(\gamma)$ donde γ es raíz de $f_a(x)$ para algún $a \in k$.

Demostración:

1. Basta notar que si γ es raíz y $b \in \mathbb{F}_p$, entonces $\gamma + b$ es raíz de $f_a(x)$ (por el sueño del aprendiz y el pequeño teorema de Fermat); ésto nos otorga todas las p raíces del polinomio.

2. Como K es cíclica, sea $\langle\sigma\rangle = \mathrm{Gal}(K/k)$. Por el lema de independencia de Dedekind existe $\beta \in K$ tal que $\sum_{i=1}^{p} \sigma^i(\beta) \neq 0$. Definamos

$$\delta := \sigma\beta + 2\sigma^2\beta + \cdots + (p-1)\sigma^{p-1}\beta.$$

Luego se tiene que $\delta - \sigma\delta = \sigma\beta + \sigma^2\beta + \cdots + \sigma^{p-1}\beta - (p-1)\beta = \sum_{i=1}^{p} \sigma^i(\beta) \neq 0$, de modo que $\delta \notin k$ y necesariamente $K = k(\delta)$ (puesto que un grupo de orden p es simple). Es fácil notar que $\sigma^i\delta - \sigma^{i+1}\delta = \delta - \sigma\delta =: f$, por lo que, los conjugados de δ son $\delta, \delta+f, \ldots, \delta+(p-1)f$. Definamos $\gamma := \delta/f$ y nótese que sus conjugados son $\gamma, \gamma+1, \ldots, \gamma+(p-1)$. Más aún

$$a := \gamma \cdot (\gamma-1) \cdots \big(\gamma-(p-1)\big) = \mathrm{Nm}_{K/k}(\gamma) \in k.$$

Nótese que $b \in \mathbb{F}_p$ syss es raíz de $x^p - x = \prod_{b\in\mathbb{F}_p}(x-b)$, de lo que se sigue que $\gamma^p - \gamma = a$, o equivalentemente, que γ es raíz de $f_a(x) \in k[x]$. □

§4.5.3 La insolubilidad de la quíntica. Éste es tal vez uno de los temas más conocidos y una de las motivaciones para el estudio de la teoría de Galois. Aquí le dejamos al final para ser la «cereza sobre el pastel» de todo el trabajo de éste capítulo y es obligatoria la lectura de la sección §1.5.2.

Definición 4.81: Se dice que una extensión $k(\alpha)/k$ es ***pura*** si $\alpha^m \in k$ para algún α. Se dice que una extensión finita K/k es ***radical*** si existe una cadena de extensiones de cuerpos:

$$K =: K_0 \supseteq K_1 \supseteq \cdots \supseteq K_n = k$$

tales que K_i/K_{i+1} es una extensión pura.

La definición de extensión radical ya debería hacer eco de los grupos resolubles, pero además debería tener sentido ésta definición. De hecho, la fórmula cuadrática ya nos otorga una demostración constructiva de que toda extensión de grado 2 de $\mathbb{Q}$ es radical.

Sin embargo, una observación vital es que ésta definición puede parecer no ser tan general, dado que no necesariamente se cumpliría que toda subextensión de una radical sea también radical, por ello se define lo siguiente:

Definición 4.82: Una extensión es ***resoluble (por radicales)*** si está contenida en otra extensión radical.

Proposición 4.83: Se cumplen:

1. $\mathrm{Gal}(k(\zeta_n)/k)$ es abeliano.
2. Sea α raíz del polinomio irreducible $x^n - \beta \in k[x]$ y supongamos que $\zeta_n \in k$. Entonces $\mathrm{Gal}(k(\alpha)/k)$ es abeliano.
3. Toda extensión normal radical tiene grupo de Galois resoluble.
4. Toda extensión normal resoluble tiene grupo de Galois resoluble.

Demostración:

1. Nótese que como todas las raíces primitivas n-ésimas de la unidad son potencias de ζ_n, un $\mathbb{Q}$-automorfismo σ está completamente determinado por su valor en ζ_n, en particular denotemos $\sigma_j(\zeta_n) = \zeta_n^j$. Nótese que σ_j determina un automorfismo syss $(j;n) = 1$. Luego $(\sigma_j \circ \sigma_k)(\zeta_n) = \sigma_k(\zeta_n^j) = (\zeta_n^j)^k = (\zeta_n^k)^j = (\sigma_k \circ \sigma_j)(\zeta_n)$, lo que basta para comprobar que el grupo es abeliano.
2. γ es otra raíz de $x^n - \beta$ syss $(\gamma/\alpha)^n = \beta/\beta = 1$, vale decir, si γ/α es una raíz n-ésima de la unidad. Pero por hipótesis k posee a todas las raíces n-ésimas de la unidad, luego $k(\alpha)/k$ es una extensión normal. Más aún, es claro que el grupo de automorfismos es abeliano puesto que todos son de la forma $\sigma_j(\alpha) = \alpha\zeta_m^j$.
3. Supongamos que $K := k(\alpha_1, \ldots, \alpha_n)$ es radical, de modo que $\alpha_{i+1}^{m_{i+1}} \in k(\alpha_1, \ldots, \alpha_i)$ para todo i. Luego consideremos a la clausura normal N de K, la cual ha de ser de la forma

$$N = k(\zeta_{m_1}, \ldots, \zeta_{m_n}, \alpha_1, \ldots, \alpha_n).$$

Finalmente definamos $N_j := k(\zeta_{m_1}, \ldots, \zeta_{m_j})$ para $j \leq n$ y $N_j := k(\zeta_{m_1}, \ldots, \zeta_{m_n}, \alpha_1, \ldots, \alpha_{n-j})$ para $j > n$. Entonces claramente N_{i+1} es una extensión normal de N_i, por lo que se obtiene la siguiente serie normal de $\mathrm{Gal}(N/k)$:

$$\mathrm{Gal}(N/k) = \mathrm{Gal}(N/N_0) \trianglerighteq \mathrm{Gal}(N/N_1) \trianglerighteq \cdots \trianglerighteq \mathrm{Gal}(N/N_{2n}) = \{1\}.$$

Pero aún mejor, $\mathrm{Gal}(N/N_i)/\mathrm{Gal}(N/N_{i+1}) \cong \mathrm{Gal}(N_{i+1}/N_i)$ (por el teorema fundamental de la teoría de Galois) el cual es abeliano por los

incisos anteriores. Finalmente, hemos construido una serie abeliana de $\mathrm{Gal}(N/k)$, por lo que $\mathrm{Gal}(N/k)$ es un grupo resoluble.

Además, $\mathrm{Gal}(N/k)/\mathrm{Gal}(N/K) \cong \mathrm{Gal}(K/k)$, por el teorema fundamental de la teoría de Galois, y sabemos que todo cociente de un grupo resoluble es también resoluble. □

Lema 4.84: Toda extensión separable radical está contenida en una extensión de Galois radical.

Demostración: Sea K/k una extensión separable radical, en particular es una extensión finita y por el teorema del elemento primitivo se cumple que $K = k(\alpha)$ y consideremos la clausura normal L de K que está generada por el resto de raíces del polinomio minimal de α. Como K es radical sea una cadena de extensiones puras:

$$K = k(\beta_1, \ldots, \beta_n) \supseteq \cdots \supseteq k(\beta_1) \supseteq k$$

donde $\beta_i^{n_i} = r_i$. Entonces elijamos a un conjugado de α, éste ha de ser de la forma $\sigma(\alpha)$ donde $\sigma \in \mathrm{Gal}(L/k)$. Luego podemos construir la siguiente cadena de extensiones puras:

$$K = k(\gamma_1, \ldots, \gamma_n) \supseteq \cdots \supseteq k(\gamma_1) \supseteq k$$

donde $\gamma_i := \sigma(\beta_i)$ y es pura pues $\gamma_i^{n_i} = \sigma(r_i)$. Luego $\sigma(\alpha)$ se obtiene con la misma combinación para α sustituyendo β_i por γ_i. Haciendo lo mismo para el resto de raíces se obtiene que L es radical y claramente es de Galois. □

Finalmente bastaría encontrar un cuerpo de Galois cuyo grupo no fuese resoluble (e.g., S_n con $n \geq 5$) para poder concluir.

Lema 4.85: Sea p un número primo y $G \leq S_p$ un subgrupo. Si G contiene un elemento de orden p y alguna trasposición, entonces $G = S_p$.

Demostración: Si $p = 2$, entonces $|S_2| = 2! = 2$ por lo que es claro. Supondremos que $p \neq 2$. En primer lugar, nótese que si $\sigma \in G$ es el elemento de orden p, entonces podemos escribirlo como ciclos disjuntos $\sigma = \sigma_1 \cdots \sigma_n$, y que, como son disjuntos, conmutan y es fácil notar que

$$p = \mathrm{ord}(\sigma_1 \cdots \sigma_n) = \mathrm{mcm}(\mathrm{ord}(\sigma_1), \ldots, \mathrm{ord}(\sigma_n)),$$

de lo que se sigue que necesariamente σ sea un ciclo.

Sea $\sigma := (a_1, \ldots, a_p) \in G$ y sea $\tau := (b, c) \in G$ una trasposición, entonces $\sigma^{-1}\tau\sigma = (\sigma(b), \sigma(c)) \in G$ el cual es necesariamente una trasposición distinta puesto que σ no fija a ningún elemento y tiene orden > 2. Así proseguimos construyendo $(\sigma^j(b), \sigma^j(c))$ para todo $j \in \{0, 1, \ldots, p-1\}$, las cuales son trasposiciones que pasan por todos los elementos de $\{1, 2, \ldots, p\}$. En particular hay alguna trasposición de la forma $(1, d_1)$ y hay una cadena $(d_1, d_2), (d_2, d_3), \ldots, (d_m, 2)$ de trasposiciones en G de modo que

$$(2, d_m)(d_m, d_{m-1}) \cdots (d_2, d_1)(1, d_1)(d_1, d_2) \cdots (d_m, 2) = (1, 2),$$

y así podemos comprobar que G contiene a todas las trasposiciones y, por lo tanto, es todo S_p. □

Teorema 4.86: Sea $f(x) \in \mathbb{Q}[x]$ un polinomio irreducible de grado p que, en $\mathbb{C}$, posee exactamente dos raíces no reales. Sea K el cuerpo de escisión de $f(x)$, entonces $\mathrm{Gal}(K/\mathbb{Q}) = S_p$.

Demostración: Sean $\alpha_1, \ldots, \alpha_p$ las raíces de $f(x)$, de modo que $f(x) = \prod_{i=1}^{p}(x - \alpha_i) \in \mathbb{C}[x]$ y llamemos $G := \mathrm{Gal}(K/\mathbb{Q})$. Nótese que $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ es una extensión de $\mathbb{Q}(\alpha_1)$ el cual satisface $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = p$, por lo que $p \mid [K : \mathbb{Q}] = |G|$. Luego, por el teorema de Cauchy, G contiene un elemento de orden p. Además, como K está generado por los α_i's y éstos son conjugados, entonces todo $\mathbb{Q}$-automorfismo de K está determinado por adónde lleva cada α_i y necesariamente los permuta, lo que comprueba que $G \leq S_p$. Finalmente, como K posee exactamente dos raíces no-reales y como $\overline{f(z)} = f(\bar{z})$, donde $\overline{()}$ denota conjugación compleja, entonces es claro que las dos raíces no-reales β_1, β_2 son conjugadas complejas la una de la otra. Además, la conjugación compleja τ es claramente un K-automorfismo. Como G contiene a σ (de orden p) y a τ (de orden 2), entonces concluimos que $G = S_p$ como se quería probar. □

Ejemplo. Considere el polinomio $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ (ver fig. 4.1). $f(x)$ es irreducible por el criterio de Eisenstein y veremos que posee exactamente dos raíces no-reales: ésto debido a que $\lim_{x \to \pm\infty} f(x) = \pm\infty$, a que $f(0) = 2$ y $f(1) = -1$, y que $f'(x) = 5x^4 - 4$ tiene por únicas raíces $\pm\sqrt[4]{4/5} \approx \pm 0{,}94574$. Por el teorema anterior, concluimos que el grupo de Galois de su cuerpo de escisión es S_5, el cual no es resoluble, luego $f(x)$ no es resoluble por radicales.

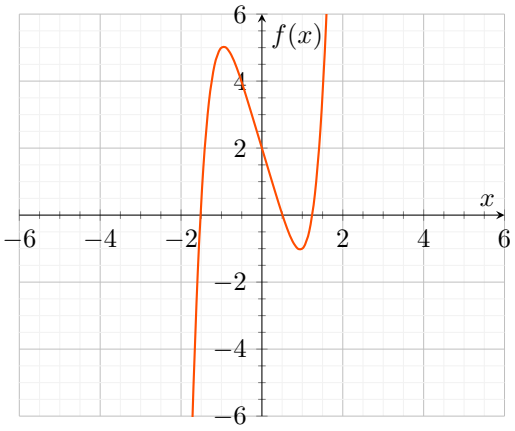


Figura 4.1

4.6 Trascendencia

A lo largo del capítulo nos hemos enfocado en el estudio de extensiones algebraicas, pero también hemos definido la noción de «elemento trascendente» pese a no hacer uso de él. En ésta sección veremos qué clase de teoría se puede construir si las extensiones de cuerpo consideradas no son algebraicas.

§4.6.1 Grado de trascendencia.

Definición 4.87: Sea K/k una extensión de cuerpos y sean $\alpha_1, \ldots, \alpha_n$ elementos de K, éstos se dicen ***algebraicamente dependientes*** si existe un polinomio $f \in k[x_1, \ldots, x_n]$ no constante tal que $f(\alpha_1, \ldots, \alpha_n) = 0$; de lo contrario, se dice que dichos elementos son ***algebraicamente independientes***.

Una extensión de cuerpos K/k se dice ***puramente trascendente*** si existe un conjunto $B \subseteq K$ algebraicamente independiente tal que $K = k(B)$.

Es claro que la independencia algebraica hace eco de la independencia lineal, de modo que los paralelismos entre ambos son inevitables. Intuitivamente, un conjunto algebraicamente independiente es aquel que «no posee relaciones algebraicas entre sí», por ejemplo, π y π^2 son elementos trascendentes (ésto lo probaremos más adelante), pero claramente sí poseen una relación entre ambos.

Proposición 4.88: Sean K/k y K'/k extensiones de cuerpo, sean $S \subseteq K$ y $S' \subseteq K'$ conjuntos algebraicamente independientes y sea $f\colon S \to S'$ una biyección. Entonces existe un único k-isomorfismo $\bar{f}\colon k(S) \to k(S')$ tal que $\bar{f}|_S = f$.

Demostración: Nótese que la biyección f puede considerarse como una función $f\colon S \to k(S')$ de modo que, como $k(S')$ es un dominio, entonces podemos extenderlo de manera única al homomorfismo de evaluación $\tilde{f}\colon k[S] \to k(S')$ (teo. 2.68). Como S es algebraicamente independiente, entonces se concluye que $\tilde{f}$ tiene núcleo nulo, luego es un k-monomorfismo. Como $k[S]$ es un dominio íntegro, cuyo cuerpo de fracciones es $k(S)$ y $\tilde{f}$ es un monomorfismo, entonces admite una única extensión $\bar{f}\colon k(S) \to k(S')$ (teo. 2.61). Finalmente como $\bar{f}$ es un k-monomorfismo y $S' \subseteq \operatorname{Img} \bar{f}$, entonces $\bar{f}$ es un k-isomorfismo. □

Corolario 4.89: Sea K/k una extensión de cuerpos, $S \subseteq K$ un conjunto algebraicamente independiente y $K = k(S)$. Si X es un conjunto de indeterminadas con $|X| = |S|$, entonces K es k-isomorfo al cuerpo de fracciones $k(X)$.

Proposición 4.90: Sea K/k una extensión de cuerpos y $S \subseteq K$ un conjunto algebraicamente independiente. Un elemento $\beta \in K/k(S)$ es trascendente syss $S \cup \{\beta\}$ es algebraicamente independiente.

Demostración: $\Longrightarrow$. Sea $f \in k[x_1, \ldots, x_n, y]$ tal que $f(s_1, \ldots, s_n, \beta) = 0$ para algunos $s_i \in S$. Podemos escribir

$$f(x_1, \ldots, x_n, y) = \sum_{j=0}^{m} g_j(x_1, \ldots, x_n) y^j,$$

y definir $a_j := g_j(s_1, \ldots, s_n) \in k(S)$, de modo que $h(y) := \sum_{j=0}^{m} a_j y^j \in k(S)[y]$ es tal que

$$h(\beta) = f(s_1, \ldots, s_n, \beta) = 0.$$

Como β es trascendente, ésto implica que $h = 0 \in k(S)[y]$, y luego $a_j = 0$ para todo j. Pero S es algebraicamente independiente, luego $g_j = 0 \in k[x_1, \ldots, x_n]$, de lo que se sigue que f es el polinomio nulo.

$\Longleftarrow$. Ejercicio para el lector. □

Definición 4.91: Sea K/k una extensión de cuerpos, se dice que $S \subseteq K$

es una ***base de trascendencia*** de K/k si es un conjunto algebraicamente independiente $\subseteq$-maximal.

Teorema 4.92: Sea K/k una extensión de cuerpos y sea $S \subseteq K$ un conjunto algebraicamente independiente. Entonces S es una base de trascendencia syss $K/k(S)$ es una extensión algebraica.

Teorema (AE) 4.93: Sea K/k una extensión de cuerpos y sea $S \subseteq K$. Si $K/k(S)$ es una extensión algebraica, entonces S contiene alguna base de trascendencia.

Demostración: Por el lema de Zorn, sea $T \subseteq S$ un subconjunto algebraicamente independiente $\subseteq$-maximal. Entonces, por la proposición 4.90 se cumple que los elementos de $S \setminus T$ son $k(T)$-algebraicos. Luego $k(S)/k(T)$ es algebraico y luego $K/k(T)$ también lo es. Finalmente, por el teorema anterior, T es una base de trascendencia de K/k. □

Teorema (AE) 4.94: Sea K/k una extensión de cuerpos y sean S, T bases de trascendencia de K/k. Luego $|S| = |T|$.

Demostración:

(a) Si $S = \{s_1, \ldots, s_n\}$ es finito: entonces T es algebraico sobre $k(s_1, \ldots, s_n)$, pero no todo elemento de T es algebraico sobre $k(s_2, \ldots, s_n)$ puesto que de lo contrario $K/k(T)/k(s_2, \ldots, s_n)$ serían extensiones algebraicas y s_1 sería algebraico respecto a $k(s_2, \ldots, s_n)$. Así pues, sea $t_1 \in T$ tal que t_1 es trascendente sobre $k(s_2, \ldots, s_n)$ y notemos que, por la proposición 4.90, se cumple que el conjunto $T' := \{t_1, s_2, \ldots, s_n\}$ es algebraicamente independiente. Además, por maximalidad de S, debe cumplirse que s_1 es algebraico respecto a $k(T')$, de modo que T' es una base de trascendencia. Repitiendo el proceso llegamos a que $T = \{t_1, \ldots, t_n\}$.

(b) Si S fuese infinito: entonces por la parte anterior se sigue que T también lo es. Sea $s \in S$ arbitrario, luego es algebraico respecto a $k(T)$ y, por lo tanto, existe un subconjunto $T_s \subseteq T$ finito y $\subseteq$-minimal, tal que s es algebraico respecto a $k(T_s)$. Luego S es algebraico respecto a $k\left(\bigcup_{s\in S} T_s\right)$, de modo que $\bigcup_{s\in S} T_s$ es una base de trascendencia y, por definición, $T = \bigcup_{s\in S} T_s$ y procedemos análogamente a la demostración de equipotencia de bases (teo. 3.29). □

Definición 4.95: Sea K/k una extensión de cuerpos. Se define el ***grado de trascendencia*** de K/k, denotado $\mathrm{trdeg}(K/k)$, a la cardinalidad de cualquiera de sus bases de trascendencia.

Proposición 4.96: Sea k un cuerpo. Entonces:

1. Una extensión K/k es algebraica syss $\mathrm{trdeg}(K/k) = 0$.
2. Sea $K := k(x_1, \ldots, x_n)$ el cuerpo de polinomios en n variables, entonces $\mathrm{trdeg}(K/k) = n$.

Teorema (AE) 4.97: Sean K, L cuerpos algebraicamente cerrados de igual característica, de modo que tienen el mismo cuerpo primo k, y supongamos que $\mathrm{trdeg}(K/k) = \mathrm{trdeg}(L/k)$. Entonces $K \cong L$.

Demostración: Sean S y T las bases de trascendencia de K y L sobre k resp. Por hipótesis existe una biyección $f\colon S \to T$ que luego se extiende de manera única a un isomorfismo $\bar{f}\colon k(S) \to k(T)$, de modo que $k(S) \cong k(T)$. Finalmente K es la clausura algebraica de $k(S)$ y L la de $k(T)$, y las clausuras algebraicas de un mismo cuerpo son isomorfas. □

Corolario (AE) 4.98: Sea K un cuerpo no numerable cuyo cuerpo primo es k, entonces $\mathrm{trdeg}(K/k) = |K|$. En consecuencia, dos cuerpos no numerables algebraicamente cerrados de igual característica son isomorfos syss tienen la misma cardinalidad.

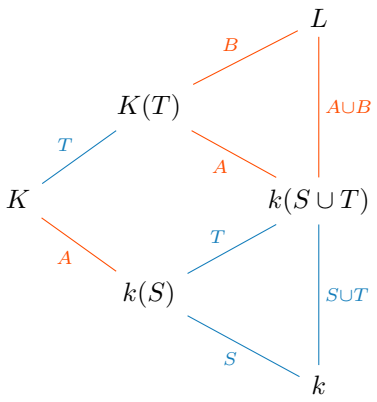
Ejemplo. Por el corolario anterior, $\mathbb{C}$ y $\mathbb{C}(z)^{\mathrm{alg}}$ son isomorfos como cuerpos, aunque claramente no son $\mathbb{C}$-isomorfos.

Teorema 4.99: Sean $L/K/k$ extensiones de cuerpo, entonces

$$\mathrm{trdeg}(L/k) = \mathrm{trdeg}(L/K) + \mathrm{trdeg}(K/k).$$

Demostración: Probaremos algo ligeramente más fuerte: Si S es una base de trascendencia de K/k y T una base de trascendencia de L/K, entonces $S \cup T$ es una base de trascendencia de L/k (con $S \cap T = \varnothing$).

Es fácil ver que $S \cap T = \varnothing$. Definamos $A := K \setminus k(S)$ y $B := L \setminus K(T)$. Luego, podemos ver que se tiene el siguiente diagrama de extensiones (donde las líneas rojas son extensiones algebraicas y las azules son puramente trascendentes):



De modo que $k(S \cup T)(A \cup B) = L$ donde $A \cup B$ son algebraicos sobre $k(S \cup T)$, luego se sigue que $S \cup T$ es una base de trascendencia de L/k. $\square$

§4.6.2 Teorema de Lüroth.

Definición 4.100: Una extensión de cuerpos K/k se dice ***trascendente simple*** si $K = k(x)$, donde x es trascendente en K/k.

Sea $f \in k(x)$ una función racional, y sea $f = g(x)/h(x)$ con $g(x), h(x) \in k[x]$ coprimos. Entonces se define su ***altura*** como

$$\text{alt } f := \text{máx}\{\deg g(x), \deg h(x)\}.$$

Una función racional $f \in k(x)$ se dice una ***transformación lineal fraccionaria*** si es de la forma

$$f(x) = \frac{ax + b}{cx + d},$$

donde $a, b, c, d \in k$ y $ad - bc \neq 0$. Se denota por $\text{LF}(k)$ al conjunto de las transformaciones lineales fraccionarias.

Proposición 4.101: Sea k un cuerpo. Entonces, en $k(x)$:

1. Las constantes son exactamente los elementos de altura 0.
2. $\text{LF}(k)$ son exactamente los elementos de altura 1.
3. $(\text{LF}(k), \circ)$, donde $\circ$ es la composición formal, es un grupo.

Demostración: Para la última, sean

$$\varphi := \frac{ax+b}{cx+d}, \qquad \psi := \frac{ex+f}{gx+h}$$
$$\varphi \circ \psi = \frac{(ae+cf)x+(be+df)}{(ag+ch)x+(bg+dh)}.$$

De aquí es fácil notar que conforma un grupo. □

El lector atento debería reconocer una forma matricial en la última forma. En efecto, $\mathrm{LF}(k)$ es *casi* el grupo de matrices invertibles, pero con la restricción de que $\frac{2x}{2} = \frac{x}{1}$.

Proposición 4.102: Sea $\varphi = g(x)/h(x) \in k(x)$ no constante con $g(x), h(x)$ coprimos. Entonces:

1. φ es k-trascendente.
2. $k(x)/k(\varphi)$ es una extensión finita de cuerpos.
3. El polinomio minimal de x sobre $k(\varphi)$ es

$$\theta(y) := g(y) - \varphi \cdot h(y) \in k(\varphi)[y],$$

de modo que $[k(x) : k(\varphi)] = \operatorname{alt} \varphi$.

Demostración: Es claro que x es una raíz de $\theta(y) \in k(\varphi)[y]$ y que, de probar la 3, el resto se sigue trivialmente. Hay dos cosas que probar: la primera es que $\theta(y)$ no sea el polinomio nulo y la segunda es que $\theta(y)$ sea irreducible en $k(\varphi)[y]$. Denotemos $g(y) = \sum_{i=0}^{n} a_i y^i$ y $h(y) = \sum_{i=0}^{n} b_i y^i$, donde podemos agregar coeficientes nulos para exigir que $n = \operatorname{alt} \varphi$. Luego

$$\theta(y) = g(y) - \varphi h(y) = \sum_{i=0}^{n} (a_i - \varphi b_i) x^i.$$

Como $h(y)$ no es el polinomio nulo, entonces $b_j \neq 0$ para algún j, y vemos que $\theta(y)$ no es el polinomio nulo, pues $a_j/b_j \in k$ pero $\varphi \notin k$. Además, es claro notar que $\deg \theta = \operatorname{alt} \varphi$.

Finalmente, por el criterio de irreducibilidad de Gauss $\theta(y)$ es irreducible en $k(\varphi)[y]$ syss lo es en $k[\varphi][y]$, y efectivamente lo es en el último, debido al corolario 2.88. □

Corolario 4.103: Sea $\varphi \in k(x)$, entonces $k(x) = k(\varphi)$ syss $\varphi \in \mathrm{LF}(k)$.

Teorema 4.104 – *Teorema de Lüroth*: Sea $k(x)/k$ una extensión trascendente simple y sea $k(x)/L/k$ una extensión intermedia estricta, vale decir, tal que $k(x) \neq L \neq k$. Entonces L es trascendente simple relativo a k.

DEMOSTRACIÓN: Sea L una extensión intermedia. Es fácil ver que $k(x)/L$ es una extensión finita de cuerpos (¿por qué?) de grado n, de modo que podemos elegir el polinomio minimal de x en L:

$$I(x,y) = y^n + \frac{g_{n-1}(x)}{h_{n-1}(x)}y^{n-1} + \cdots + \frac{g_0(x)}{h_0(x)} \in L[y],$$

donde $g_i(x), h_i(x) \in k[x]$ de modo que $g_i/h_i \in k(x) \supseteq L$. Como x no es k-algebraico, entonces necesariamente debe haber algún coeficiente de I que no pertenece a k, digamos que $g_j(x)/h_j(x) \notin k$. Definamos $g(x) := g_j(x), h(x) := h_j(x) \in k[x]$, $\varphi := g(x)/h(x) \in L \setminus k$ y

$$\theta(x,y) := g(y) - \varphi \cdot h(y) \in k(\varphi)[y].$$

Por la proposición anterior, sea $m := \deg_y(\theta) = \operatorname{alt}(\varphi) = [k(x) : k(\varphi)]$. Luego

$$m = [k(x) : L][L : k(\varphi)] = n \cdot [L : k(\varphi)],$$

y así, bastaría ver que $m = n$ para concluir que $L = k(\varphi)$.

Así pues, x es raíz del polinomio $I(x,y) \in k(x)[y]$ irreducible en $L[y]$ y también es raíz de $\theta(x,y) \in L[y] \subseteq k(x)[y]$, luego $I(x,y) \mid \theta(x,y)$ en $k(x)[y]$ y existe $a(x,y) \in k(x)[y]$ tal que

$$\theta(x,y) = a(x,y)I(x,y).$$

Por el lema de primitividad de Gauss podemos factorizar el contenido de los polinomios, y es notorio que $c(\theta) = 1/h(x)$, de modo que

$$\theta^*(x,y) = h(x)g(y) - g(x)h(y) \in k[x][y],$$

además es claro que $m = \deg_x(\theta^*) = \deg_y(\theta^*) = \deg_y(\theta)$.

Ahora, nótese que $\deg_x(\theta^*) = \operatorname{alt}(g_j/h_j) \leq \max_i\{\operatorname{alt}(g_i/h_i)\} \leq \deg_x(I^*)$ (por la propoción 2.90), de modo que $\deg_x(a^*) + m \leq m$ y necesariamente $\deg_x(a^*) = 0$, es decir, $a^* \in k[y]$. Pero como $\theta^*(y,x) = -\theta^*(x,y)$, entonces necesariamente $\deg_y(a^*) = 0$ también y, por ende, $a^* \in k$. Finalmente notamos que

$$m = \deg_x(\theta^*) = \deg_x(a^*) + \deg_x(I^*) = 0 + n,$$

lo que concluye el teorema. □

Notas históricas

Ésta sección está principalmente basada en el artículo Kiernan **[52].**

Tal como señalamos en el capítulo 2, el estudio de las extensiones simples algebraicas comienza con la llamada *teoría de divisores* de **Leopold Kronecker [44],** quién si bien comparte sus aportes con varios de sus colegas mediante correspondencia, no publica su teoría sino hasta en 1882; de ahí también que describamos nuestro primer teorema como *teorema de extensión de Kronecker* (poco común por cierto).

Los trabajos de Kronecker están fuertemente inspirados en los trabajos de **Ernst Eduard Kummer**, quién principalmente estudia a los enteros algebraicos ciclotómicos. La primera figura relevante en las matemáticas en estudiar extensiones de cuerpos (al principio, exclusivamente de $\mathbb{Q}$ y de $\mathbb{R}$) fue Gauss, mediante los llamados enteros gaussianos y los números complejos; seguido de **Leonhard Euler** quién asume erróneamente que extensiones de $\mathbb{Z}$ como $\mathbb{Z}[\sqrt{-5}]$ admiten factorización única (éste es un conocido contraejemplo). Kummer fue el primero en ir un tanto más allá, y prueba que $\mathbb{Z}[\zeta_{23}]$ (donde ζ_{23} es una raíz 23-ésima primitiva de la unidad) no es un DFU (cf. Kummer **[46]** (1844)), pero al parecer casos de la forma $\mathbb{Z}[\zeta_p]$ con $p < 23$ primo sí funcionan. Tras percatarse de ésta característica fundamental de las extensiones de $\mathbb{Z}$, Kummer se adentra en un estudio profundo de los enteros ciclotómicos y en una busqueda de una sustitución de la factorización única. El caso general de enteros ciclotómicos para exponentes no necesariamente primos lo estudia en Kummer **[47]** (1856).

El desarrollo de la teoría de Galois nace del antiquísimo problema algebraico de buscar soluciones mediante métodos algebraicos a polinomios irreducibles. Uno de los intereses que llevó a esta pregunta fue el de los polígonos regulares constructibles con regla y compás. Las ecuaciones de grado 5 y superior fueron intentadas de resolver por grandes nombres como los de Euler, Vandermonde y Lagrange, pero ninguno tuvo éxito. Gauss **[40]** (1801) fue el primero en trabajar con la ecuación $x^p - 1 = 0$ y notar que sus soluciones coinceden con los vértices de un p-gono regular. En su texto, Gauss demuestra que los n-gonos regulares, donde $n = 2^\ell \cdot p_1 \cdots p_n$ con p_i's primos de Fermat distintos, son constructibles.

Inspirado en el trabajo de Gauss, el matemático holandés **Niels Henrik Abel** comenzó a investigar la (in)solubilidad de la quíntica. Primero, creía haber encontrado una demostración de la solubilidad en su adolescencia, pero revisando su propia demostración se convenció de que debía darse el caso contrario. Finalmente, publicó su demostración en un panfleto **[30]** (1824)

que envió a Gauss. La carta de Abel fue encontrada en el lecho de muerte de Gauss en 1855 en medio de una montaña de papeles, aún sin abrir. Uno de los pasos en el artículo de Abel involucraba la clasificación de ciertas expresiones algebraicas; años más tarde, **William Rowan Hamilton** se percató de que había un error en ésta parte, pero que no afectaba la conclusión del artículo; éste paso es reminiscente al teorema de Jordan-Hölder que vimos en el primer capítulo. Abel reescribió y clarificó sus descubrimientos más tarde en el artículo **[31]** (1826).

Tras probar que, en general, la quíntica no es soluble, Abel comienza a investigar qué clase de polinomios sí admiten soluciones por radicales. En Abel **[32]** (1829) demuestra que, en lenguaje moderno, aquellos polinomios cuyo grupo de Galois (de su cuerpo de escisión) es abeliano sí son resolubles; años más tarde, Kronecker llamaría *abelianos* a ésta clase de polinomios y se les llama *grupos abelianos* a los grupos conmutativos debido a éste aporte de Abel.

Finalmente, la teoría de Galois fue naturalmente desarrollada por **Évariste Galois**, aunque no hasta el punto en que nosotros lo hemos visto. En **[39]** y **[38],** escritos en 1830 cuando Galois tenía dieciocho años y publicados póstumos en 1846, Galois introduce la noción de *grupo* como un conjunto de permutaciones cerrado bajo composición y Galois estudia el hoy llamado en su honor *grupo de Galois* de una ecuación (el grupo de Galois del cuerpo de escisión) y llega a que la ecuación es resoluble por radicales si el grupo de Galois es resoluble. Galois trabajó en éstos *memoirs* hasta el día de su muerte, haciendo correcciones hasta 1832. Para aquél entonces varios matemáticos sabían de la obra de Galois, pero es paradójico el que hayan tenido que esperar hasta 1846 para poder tener referencias explícitas.

Sobre Galois, Grothendieck escribe **[51,** pág. 46] (en un pie de página):

> Estoy convencido de que un Galois hubiera ido todavía mucho más lejos que yo. Por una parte a causa de sus dones totalmente excepcionales (que a mí no me han tocado en suerte). Por otra porque probablemente no hubiera dedicado, como yo, la mayor parte de su energía a interminables y minuciosas tareas de puesta a punto de lo que ya estaba más o menos conseguido...[2]

[2] *Je suis persuadé d'ailleurs qu'un Galois serait allé bien plus loin encore que je n'ai été. D'une part à cause de ses dons tout à fait exceptionnels (que je n'ai pas reçus en partage, quant à moi). D'autre part parce qu'il est probable qu'il n'aurait pas, comme moi, laissé se distraire la majeure part de son énergie, pour d'interminables tâches de mise en forme minutieuse, au fur et à mesure, de ce qui est déjà plus ou moins acquis...*

5

Módulos, otra vez

En el capítulo 3 ya introducimos la noción de módulos, principalmente para poder hablar de módulos libres y el caso particular de espacios vectoriales. El capítulo culminó notando que la teoría de espacios vectoriales se reduce al estudio de un sólo número (cardinal): la dimensión, y que las propiedades de ser «libre» permiten una completa identificación de los homomorfismos de espacios vectoriales (o aplicaciones lineales) con las matrices, que englobaban toda la información en una tabla finita.

En éste capítulo abandonamos toda la facilidad de los espacios vectoriales para estudiar a los módulos dentro de su parte «no libre», y también sirve como excusa para introducir nociones avanzadas del álgebra como sucesiones exactas y homologías.

5.1 La categoría de módulos

Definición 5.1: Sean M, N un par de A-módulos, se define $M \times N$ con

$$(\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{z}, \boldsymbol{w}) := (\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{y} + \boldsymbol{w}), \quad \lambda(\boldsymbol{x}, \boldsymbol{y}) := (\lambda\boldsymbol{x}, \lambda\boldsymbol{y}).$$

para todo $\boldsymbol{x}, \boldsymbol{z} \in M$, $\boldsymbol{y}, \boldsymbol{w} \in N$ y $\lambda \in A$.

El producto directo se puede generalizar a una familia $\{M_i\}_{i\in I}$ de A-módulos, cuyos elementos son:

$$(\boldsymbol{m}_i)_{i\in I} \in \prod_{i\in I} M_i \iff \forall i \in I\ \boldsymbol{m}_i \in M_i$$

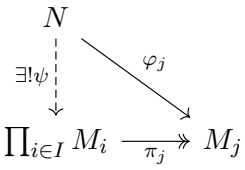
y cuyas operaciones son:

$$(\boldsymbol{m}_i)_{i\in I} + (\boldsymbol{n}_i)_{i\in I} := (\boldsymbol{m}_i + \boldsymbol{n}_i)_{i\in I}, \qquad \lambda \cdot (\boldsymbol{m}_i)_{i\in I} := (\lambda \boldsymbol{m}_i)_{i\in I}.$$

Proposición 5.2: Sea $\{M_i\}_{i\in I}$ una familia de A-módulos, entonces:

1. Las proyecciones $\pi_j \colon \prod_{i\in I} M_i \to M_j$ son morfismos de A-módulos para todo $j \in I$.

2. Si $\{\varphi_i \colon T \to M_i\}$ es una familia de morfismos de A-módulos, entonces $\psi := \Delta_{i\in I}\, \varphi_i \colon T \to \prod_{i\in I} M_i$ es el único morfismo de A-módulos tal que el siguiente diagrama: $\psi := \Delta_{i\in I}\, \varphi_i \colon T \to \prod_{i\in I} M_i$ es el único morfismo de A-módulos tal que el siguiente diagrama:



   conmuta para todo $j \in I$.

En resumen, el producto de A-módulos es un producto categorial. El resultado también aplica para k-espacios vectoriales.

Definición 5.3: Sea $\{M_i\}_{i\in I}$ una familia de A-módulos, entonces su suma directa se define como:

$$\bigoplus_{i\in I} M_i := \left\{ (\boldsymbol{m}_i)_i \in \prod_{i\in I} M_i : \boldsymbol{m}_i = \vec{0} \text{ salvo finitos } i\text{'s} \right\}.$$

En el caso de una familia finita de A-módulos el producto y la suma directa coinciden. En el caso infinito disciernen, dado que un elemento en $\bigoplus_{i\in I} M_i$ puede verse como una suma de finitos vectores no nulos de los M_i's, en cambio en $\prod_{i\in I} M_i$ pueden ser todos no nulos.

Un ejemplo:

$$k[x] \cong \bigoplus_{n\in\mathbb{N}} \langle x^n \rangle.$$

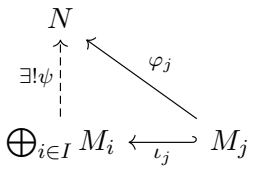
Proposición 5.4: Sea $\{M_i\}_{i\in I}$ una familia de A-módulos, entonces:

1. Las inclusiones canónicas $\iota_j \colon M_j \to \bigoplus_{i\in I} M_i$ son morfismos de A-módulos para todo $j \in I$.

2. Si $\{\varphi_i \colon M_i \to N\}$ es una familia de morfismos de A-módulos, entonces

$$\begin{aligned}\psi := \left(\textstyle\sum_{i\in I} \varphi_i\right) \colon \bigoplus_{i\in I} M_i &\longrightarrow N \\ \sum_{i\in I} \boldsymbol{m}_i &\longmapsto \sum_{i\in I} \varphi_i(\boldsymbol{m}_i)\end{aligned}$$

es el único morfismo de A-módulos tal que el siguiente diagrama:



conmuta para todo $j \in I$.

(Nótese que ψ está bien definido ya que sólo finitos de los $\boldsymbol{m}_i$'s son no nulos.)

En resumen, la suma directa de A-módulos es un coproducto categorial. El resultado también aplica para k-espacios vectoriales.

Proposición 5.5: Sean $\{M_i\}_{i\in I}$ una familia de A-módulos. Entonces para todo A-módulo N se satisface que

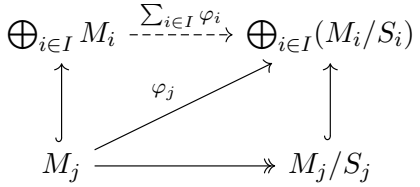
$$\begin{aligned}\operatorname{Hom}_A\left(N, \prod_{i\in I} M_i\right) &\cong \prod_{i\in I} \operatorname{Hom}_A(N, M_i) \\ \operatorname{Hom}_A\left(\bigoplus_{i\in I} M_i, N\right) &\cong \prod_{i\in I} \operatorname{Hom}_A(M_i, N)\end{aligned}$$

(en Mod_A).

Proposición 5.6: Sea A un anillo, y sean $\{(S_i, M_i)\}_{i\in I}$ una familia tal que M_i es un A-módulo y $S_i \subseteq M_i$ es un submódulo. Entonces:

$$\bigoplus_{i\in I}\left(\frac{M_i}{S_i}\right) \cong \frac{\bigoplus_{i\in I} M_i}{\bigoplus_{i\in I} S_i}.$$

Demostración: Considere el siguiente diagrama conmutativo:



Donde la flecha punteada existe por propiedad universal del coproducto. Finalmente, es claro que $\psi := \sum_{i\in I}\varphi_i$ es suprayectiva, así que basta notar que $\ker\psi = \coprod_{i\in I} S_i$ para concluir el teorema. □

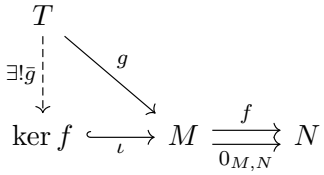
Proposición 5.7: $A^n \times A^m \cong A^n \oplus A^m \cong A^{n+m}$.

Una ventaja del lenguaje categórico es una mejor descripción del (co)núcleo:

Proposición 5.8: Sea $f\colon M \to N$ un morfismo de A-módulos. Entonces:

1. $\iota\colon \ker f \to M$ es un morfismo de A-módulos tal que $\iota \circ f = \iota \circ 0_{M,N}$, donde $0_{M,N}\colon M \to N$ es el morfismo nulo.

2. Si existe otro morfismo $g\colon T \to M$ tal que $g \circ f = g \circ 0_{M,N}$, entonces existe un único morfismo $\bar{g}\colon T \to \ker f$ tal que el siguiente diagrama conmuta:



En resumen, $\ker f$ es un núcleo categorial.

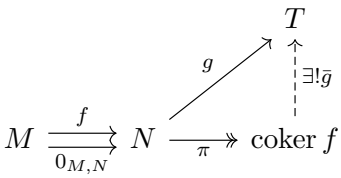
Definición 5.9: Sea $f\colon M \to N$ un morfismo de A-módulos. Puesto que $\operatorname{Img} f$ es submódulo de N se define $\operatorname{coker} f := N/\operatorname{Img} f$.

Ésto nos permite construir el siguiente objeto:

Proposición 5.10: Sea $f\colon M \to N$ un morfismo de A-módulos. Entonces:

1. $\pi\colon N \to \operatorname{coker} f$ es un morfismo de A-módulos tal que $f \circ \pi = 0_{M,N} \circ \pi$.

2. Si existe otro morfismo $g\colon N \to T$ tal que $f \circ g = 0_{M,N} \circ g$, entonces existe un único morfismo $\bar{g}\colon \operatorname{coker} f \to T$ tal que el siguiente diagrama conmuta:



En resumen, $\operatorname{coker} f$ es un conúcleo categorial.

El conúcleo no solo dualiza la propiedad universal del núcleo sino que también dualiza una caracterización usual de módulos:

Proposición 5.11: Sea $f\colon M \to N$ un morfismo de A-módulos. Entonces f es suprayectiva syss $\operatorname{coker} f$ es nulo.

Al igual que en Grp, es útil trabajar con las herramientas de sucesiones exactas:

Proposición 5.12: Sean M, N un par de A-módulos y $f\colon M \to N$ un morfismo de A-módulos. Entonces:

1. f es inyectiva syss $0 \longrightarrow M \xrightarrow{f} N$ es una sucesión exacta.

2. f es suprayectiva syss $M \xrightarrow{f} N \longrightarrow 0$ es una sucesión exacta.

3. f es isomorfismo syss $0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$ es una sucesión exacta.

4. Para todo $T \leq M$ submódulo se cumple que

$$0 \longrightarrow T \xrightarrow{\iota} M \xrightarrow{\pi} M/T \longrightarrow 0$$

es una sucesión exacta.

Podemos reescribir los teoremas de isomorfismos en lenguaje de sucesiones exactas:

Teorema 5.13: Se cumplen:

1. Si $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ es una sucesión exacta, entonces

$$M \cong \operatorname{Img} f = \ker g, \qquad T \cong N/\operatorname{Img} f = \operatorname{coker} f.$$

2. Sean S, T submódulos de M, entonces el siguiente diagrama conmuta y las filas son exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S \cap T & \longrightarrow & S & \longrightarrow & \dfrac{S}{S \cap T} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} & & \wr & & \\ 0 & \longrightarrow & T & \longrightarrow & S+T & \longrightarrow & \dfrac{S+T}{T} & \longrightarrow & 0 \end{array}$$

3. Si $S \leq T \leq M$, entonces existe una sucesión exacta:

$$0 \longrightarrow S/T \longrightarrow M/T \longrightarrow M/S \longrightarrow 0$$

Definición 5.14: Se dice que una sucesión exacta

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

se escinde si existe un $h\colon T \to N$ tal que $h \circ g = \mathrm{Id}_T$. A veces se emplea como una flecha punteada en el mismo diagrama de la sucesión exacta.

Proposición 5.15: Si una sucesión exacta

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

se escinde, entonces $N \cong M \oplus T = \ker g \oplus \operatorname{coker} f$.

Demostración: Sea $h\colon T \to N$ tal que $h \circ g = \mathrm{Id}_T$, veremos que $N = \operatorname{Img} f \oplus \operatorname{Img} h$.

Sea $\boldsymbol{n} \in N$, luego $g(\boldsymbol{n}) \in C$ y además se cumple que $\boldsymbol{n} - h(g(\boldsymbol{n})) \in \ker g$. Luego como $\ker g = \operatorname{Img} f$, existe $\boldsymbol{m} \in M$ tal que $f(\boldsymbol{m}) = \boldsymbol{n} - h(g(\boldsymbol{n}))$, así que claramente $N = \operatorname{Img} f + \operatorname{Img} h$. Más aún, sea $\boldsymbol{n} := f(\boldsymbol{m}) = h(\boldsymbol{t})$, luego $g(\boldsymbol{n}) = g(f(\boldsymbol{m})) = \boldsymbol{t} = \vec{0}$ dado que $f \circ g = 0$, pero entonces $\boldsymbol{n} = h(\vec{0}) = \vec{0}$, así que $\operatorname{Img} f \cap \operatorname{Img} h = \{\vec{0}\}$ como se quería probar. □

Ya vimos que $\mathrm{Hom}_A(X,Y)$ es un A-módulo, así pues podemos establecer el siguiente resultado:

Proposición 5.16: Sea M un A-módulo y $f\colon X \to Y$ un morfismo de A-módulos, entonces:

$$\begin{aligned} h^f\colon \mathrm{Hom}_A(M,X) &\longrightarrow \mathrm{Hom}_A(M,Y) \\ g &\longmapsto g\circ f \end{aligned}$$

y

$$\begin{aligned} h_f\colon \mathrm{Hom}_A(Y,M) &\longrightarrow \mathrm{Hom}_A(X,M) \\ g &\longmapsto f\circ g \end{aligned}$$

son también morfismos de A-módulos.

Demostración: Sea $\boldsymbol{m}\in M$, entonces:

$$\begin{aligned} \big((g+h)\circ f\big)(\boldsymbol{m}) &= f\big((g+h)(\boldsymbol{m})\big) = f\big(g(\boldsymbol{m})+h(\boldsymbol{m})\big) \\ &= f\big(g(\boldsymbol{m})\big)+f\big(h(\boldsymbol{m})\big) = (g\circ f)(\boldsymbol{m})+(h\circ f)(\boldsymbol{m}). \end{aligned}$$

Y el producto escalar se demuestra análogamente. El resto de resultados queda al lector. □

Corolario 5.17: Para todo A-módulo M se satisface que el siguiente

$$\begin{array}{ccc} X & & \mathrm{Hom}_A(M,X) \\ {\scriptstyle f}\big\downarrow & \xRightarrow{\mathrm{Hom}_A(M,-)} & \big\downarrow{\scriptstyle h^f} \\ Y & & \mathrm{Hom}_A(M,Y) \end{array}$$

es un funtor covariante en Mod_A; y el siguiente:

$$\begin{array}{ccc} X & & \mathrm{Hom}_A(X,M) \\ {\scriptstyle f}\big\downarrow & \xRightarrow{\mathrm{Hom}_A(-,M)} & \big\uparrow{\scriptstyle h_f} \\ Y & & \mathrm{Hom}_A(Y,M) \end{array}$$

es un funtor contravariante en Mod_A. Éstos funtores se llaman ***funtores de representación***.

En la teoría de conjuntos se demuestra que los funtores de representación siempre existen y están bien definidos; la sorpresa radica en que, en general, los conjuntos Hom's no suelen ser elementos de la categoría y los funtores de representación tampoco suelen traducirse en flechas de la categoría; ésto indica que la categoría Mod_A es bastante especial.

Definición 5.18: Sea $F\colon \mathscr{A} \subseteq A\text{-}\mathsf{Mod} \to \mathscr{B} \subseteq B\text{-}\mathsf{Mod}$ un funtor (covariante). Entonces F se dice:

Aditivo Si para todo $M, N \in \mathscr{A}$ se satisface que la aplicación

$$\begin{aligned} \mathrm{Hom}_A(M,N) &\longrightarrow \mathrm{Hom}_B(FM, FN) \\ g &\longmapsto F(g) \end{aligned}$$

es un homomorfismo de grupos.

Exacto por la izquierda Si para toda sucesión exacta

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$$

se satisface que la siguiente sucesión

$$0 \longrightarrow FM' \xrightarrow{F(f)} FM \xrightarrow{F(g)} FM''$$

también es exacta.

Exacto por la derecha Si para toda sucesión exacta

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

se satisface que la siguiente sucesión

$$FM' \xrightarrow{F(f)} FM \xrightarrow{F(g)} FM'' \longrightarrow 0$$

también es exacta.

Exacto Si es exacto por la izquierda y por la derecha. En general, si preserva toda clase de exactitud.

Si el funtor es contravariante las mismas definiciones aplican sobre $F\colon \mathscr{A}^{\mathrm{op}} \to \mathscr{B}$.

En general, que un funtor sea exacto es una condición increiblemente fuerte, y la condición de exactitud por un lado u otro es suficiente.

Teorema 5.19: Sea M un A-módulo, entonces $\mathrm{Hom}(M,-)$ es un funtor covariante exacto por la izquierda y $\mathrm{Hom}(-,M)$ es un funtor contravariante exacto por la derecha.

Proposición 5.20: Sean X, Y, Z un trío de A-módulos. Son equivalentes:

1. La siguiente sucesión es exacta:

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

2. La siguiente sucesión es exacta para todo M:

$$\mathrm{Hom}_A(M,X) \xrightarrow{h^f} \mathrm{Hom}_A(M,Y) \xrightarrow{h^g} \mathrm{Hom}_A(M,Z)$$

3. La siguiente sucesión es exacta para todo M:

$$\mathrm{Hom}_A(X,M) \xleftarrow{h_f} \mathrm{Hom}_A(Y,M) \xleftarrow{h_g} \mathrm{Hom}_A(Z,M)$$

Demostración: $1 \implies 2$. Sea $j \in \mathrm{Hom}_A(M,Y)$, se cumple que $j \in \ker(h^g)$ syss $j \circ g = 0$, es decir para todo $\boldsymbol{m} \in M$ se cumple que $g(j(\boldsymbol{m})) = \vec{0}$, o lo que es equivalente, $\mathrm{Img}\, j \subseteq \ker g$. Por otro lado $j \in \mathrm{Img}(h^f)$ syss $j = k \circ f$, luego $j(\boldsymbol{m}) = f(k(\boldsymbol{m}))$, por lo que $\mathrm{Img}\, j \subseteq \mathrm{Img}\, f = \ker g$, es decir, $\mathrm{Img}(h^f) = \ker(h^g)$ como se quería probar.

$2 \implies 1$. Fijemos $M = X$, entonces $h^f(\mathrm{Id}_X) = f \in \ker(h^g)$, es decir, $f \circ g = 0$ y $\mathrm{Img}\, f \subseteq \ker g$. Ahora fijemos $M = \ker g$, entonces como $\ker g \subseteq Y$ existe $\iota \in \mathrm{Hom}_A(\ker g, Y)$ y claramente $\iota \circ g = 0$ por lo que $\iota \in \ker(h^g) = \mathrm{Img}(h^f)$, luego $\iota = j \circ f$, es decir, para todo $\boldsymbol{y} \in \ker g$ se cumple que $\boldsymbol{y} \in \mathrm{Img}\, f$.

El resto son análogas. □

5.2 Cadenas de submódulos

§5.2.1 Módulos noetherianos y artinianos.

Lema 5.21: Sea A un anillo y M un A-módulo. Son equivalentes:

1. Todo submódulo de M está finitamente generado.
2. Para toda cadena ascendente de submódulos
$$N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots$$
existe un n tal que para todo $m \geq n$ se cumple que $N_n = N_m$.
3. Toda familia no vacía de submódulos admite un elemento $\subseteq$-maximal.

Pista: Es análogo a la demostración para anillos. □

Definición 5.22: Se dice que un A-módulo M es ***noetheriano*** si satisface las condiciones del lema anterior.

La siguiente definición permite un elegante paralelo con la noción de noetheriano:

Definición 5.23: Se dice que un A-módulo M es ***artiniano*** si para toda cadena descendiente de submódulos
$$N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots$$
existe un n tal que para todo $m \geq n$ se cumple que $N_n = N_m$. Se dice que el anillo A es ***artiniano*** si es un A-módulo artiniano.

Ejemplo. Todo cuerpo es noetheriano y artiniano. Ya vimos también que todo DIP es noetheriano.

Ejemplo. $\mathbb{Z}$ es un dominio euclídeo, luego es un DIP y luego es noetheriano. Sin embargo, no es artiniano puesto que
$$\mathbb{Z} \supseteq (2) \supseteq (2^2) \supseteq (2^3) \supseteq \cdots$$
es una cadena $\subseteq$-descendiente de ideales sin $\subseteq$-minimal.

Ejemplo. Ya vimos que $k[x_1, x_2, x_3, \dots]$ no es noetheriano, pero tampoco es artiniano:

$$(x_1, x_2, x_3, \dots) \supset (x_2, x_3, \dots) \supset (x_3, \dots) \supset \cdots$$

Ahora, procedemos a dar varias propiedades de los módulos noetherianos que tendrán demostraciones análogas para los módulos artinianos que, en consecuencia, vamos a obviar.

Proposición 5.24: Sea M un A-módulo noetheriano (resp. artiniano). Entonces todo submódulo N y todo módulo cociente M/N es noetheriano (resp. artiniano).

Demostración: Como todo submódulo T de N es un submódulo de M, entonces está finitamente generado. Más aún, por el teorema de la correspondencia, todo submódulo de M/N es de la forma $(T+N)/N$ con $T \leq M$; luego como T es finitamente generado, se sigue que $(T+N)/N$ también lo es. □

Corolario 5.25: Sea A un anillo noetheriano (resp. artiniano) y sea $\mathfrak{a}$ un ideal de A. Entonces $A/\mathfrak{a}$ también es noetheriano (resp. artiniano).

Corolario 5.26: Si $\varphi\colon M \to N$ es un morfismo de A-módulos suprayectivo y M es noetheriano (resp. artiniano), entonces N también.

§5.2.2 Módulos (semi)simples y el teorema de Jordan-Hölder.

Definición 5.27: Un A-módulo M no trivial se dice ***simple***[1] si sus únicos submódulos son $\{\vec{0}\}$ y M. M se dice ***semisimple*** si es la suma directa de (posiblemente infinitos) A-módulos simples.

Lema 5.28 (Schur): Si M es un A-módulo simple, entonces:

1. Todo homomorfismo de A-módulos $M \to N$ es o bien nulo o bien un monomorfismo.

2. Todo homomorfismo de A-módulos $N \to M$ es o bien nulo o bien un epimorfismo.

[1] Jacobson [**6**] emplea el término *irreducible*. A sugerencia de Matsumura [**19,** pág. 40] reservamos la palabra para la definición 6.71.

3. Todo endomorfismo de A-módulos $M \to M$ es o bien nulo o bien un automorfismo.

Demostración: Basta notar que el núcleo y la imagen de un homomorfismo es un submódulo. □

Corolario 5.29: Sea M un A-módulo simple. Entonces $(\mathrm{End}_A(M), +, \circ)$ es un anillo de división.

Algo relativamente sencillo de probar es lo siguiente:

Proposición 5.30: Un A-módulo M es simple syss existe un ideal $\mathfrak{m} \lhd A$ maximal tal que $M \cong A/\mathfrak{m}$.

Demostración: $\Longrightarrow$. Sea $\boldsymbol{u} \in M$ no nulo, entonces $\mathrm{Span}_A\{\boldsymbol{u}\}$ es un submódulo no trivial, luego es todo M. Por ende, sea $f\colon A \to M$ definido por $f(a) := a\boldsymbol{u}$, ésta función es suprayectiva por lo anterior, luego induce un isomorfismo $\bar{f}\colon A/\ker f \to M$ y $A/\ker f$ no posee submódulos impropios, luego $\ker f$ ha de ser un ideal maximal.
$\Longleftarrow$. Es claro. □

Por ende, parece más interesante analizar el caso de los módulos semisimples:

Definición 5.31: Se dice que un A-módulo M es un ***sumando directo*** de N si existe M' tal que $N = M \oplus M'$.

Proposición (AE) 5.32: Un A-módulo M es semisimple syss todo submódulo $T \leq M$ es un sumando directo de M.

Demostración: $\Longrightarrow$. Sea $M = \bigoplus_{i\in I} S_i$, donde los S_i's son simples. Para cada $J \subseteq I$ definamos

$$S_J := \bigoplus_{i\in J} S_i,$$

entonces, por lema de Zorn, podemos conseguir J maximal tal que $S_J \cap T = \{\vec{0}\}$ y es fácil comprobar que $S_J + T = M$ (ejercicio).
$\Longleftarrow$. Ésto lo haremos en dos pasos:

(i) Todo submódulo B impropio de M contiene un sumando directo simple:
Sea $\boldsymbol{u} \in B$ no nulo y, por el lema de Zorn, sea $C \leq B$ maximal tal que

$\boldsymbol{u} \notin C$. Como $C \leq M$, entonces $C \oplus S = M$ e, intersectando con B, se obtiene que $B = C \oplus D$ donde $D := S \cap M \leq M$. Probaremos que D es un módulo simple.

Si D no fuese simple, entonces, por el argumento anterior, $D = E \oplus F$ con E, F no nulos. Luego $B = C \oplus E \oplus F$. Veamos que $\boldsymbol{u}$ no puede estar en ambos $C \oplus E$ y $C \oplus F$: de lo contrario, $\boldsymbol{u} = \boldsymbol{c}_1 + \boldsymbol{e} = \boldsymbol{c}_2 + \boldsymbol{f}$ con $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C$, $\boldsymbol{e} \in E$ y $\boldsymbol{f} \in F$. Pero $\boldsymbol{c}_2 - \boldsymbol{c}_1 = \boldsymbol{e} - \boldsymbol{f} \in C \cap D = \{\vec{0}\}$, luego $\boldsymbol{e} = \boldsymbol{f} \in E \cap F = \{\vec{0}\}$ y por ende $\boldsymbol{u} = \boldsymbol{c}_1 \in C$ lo cual es absurdo. Finalmente, si $\boldsymbol{u} \notin C \oplus E$, entonces $C \oplus E$ contradice la maximalidad de C.

(ii) M es semisimple: Por el lema de Zorn, sea $U \leq M$ el submódulo maximal semisimple de M y sea V tal que $U \oplus V = M$. Si V no fuese trivial, entonces V no es simple y posee la propiedad de que todos sus submódulos son sumandos directos suyos, por lo que, $V = U' \oplus V'$ donde U' es semisimple y, por el paso (i), no es trivial, lo que contradice la maximalidad de U. □

Corolario (AE) 5.33: Todo submódulo y todo cociente de un módulo semisimple es también semisimple.

Definición 5.34: Un ideal $\mathfrak{a} \trianglelefteq A$ no nulo se dice ***minimal*** si es un A-módulo simple, i.e., si no existe otro ideal $\mathfrak{b} \neq (0)$ tal que $\mathfrak{b} \lhd \mathfrak{a}$. Un dominio A se dice ***semisimple*** si es la suma directa de ideales minimales.

Lema 5.35: Si un dominio A y $\mathfrak{a}_i \trianglelefteq A$ para todo $i \in I$ son tales que $A = \bigoplus_{i \in I} \mathfrak{a}_i$, entonces para todos salvo finitos i's se cumple que $\mathfrak{a}_i$ es nulo.

Demostración: Basta notar que $1 \in A = \bigoplus_{i \in I} \mathfrak{a}_i$ y, por definición de suma directa, se cumple que $1 = a_1 + \cdots + a_n$, donde $a_i \in \mathfrak{a}_i$, de modo que $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n = A$ y el resto son ideales nulos. □

Corolario 5.36: El producto directo de finitos anillos semisimples es semisimple. En particular, el producto directo de finitos cuerpos es un dominio semisimple.

Definición 5.37: Sea G un grupo y k un cuerpo. Definimos $k[G]$ como

el anillo dado por los objetos formales:

$$\sum_{i=1}^{n} a_i g_i \in k[G], \qquad \forall i\ a_i \in k, g_i \in G.$$

Donde se definen la suma y multiplicación por:

$$\alpha := \sum_{g\in G} a_g g, \qquad \beta := \sum_{g\in G} b_g g,$$

$$\alpha + \beta := \sum_{g\in G} (a_g + b_g) g, \qquad \alpha \cdot \beta := \sum_{g\in G} \left(\sum_{fh=g} a_f b_h \right) g.$$

Teorema 5.38 – *Teorema de Maschke*: Sea G un grupo finito y k un cuerpo de característica p (posiblemente cero) tal que p no divide a $|G|$. Entonces $k[G]$ es un anillo semisimple izquierdo.[a]

[a] Tecnicamente hasta el momento nos hemos ocupado del caso conmutativo, pero relajando dicha restricción nuestros teoremas son igualmente válidos imponiendo que «simple izquierdo» aplica para ideales izquierdos y *verbatim*.

Demostración: En primer lugar, nótese que $k[G]$ es un k-espacio vectorial y que todo ideal izquierdo $\mathfrak{a}$ de $k[G]$ es un subespacio. Sabemos que todo subespacio de un espacio vectorial es un sumando directo, es decir, existe V tal que $\mathfrak{a} \oplus_k V = k[G]$; luego existe un función k-lineal $d\colon k[G] \to \mathfrak{a}$ tal que $d|_{\mathfrak{a}} = \mathrm{Id}_{\mathfrak{a}}$.

Si probásemos que d es $k[G]$-lineal, entonces habríamos probado el teorema, pero en su lugar, construiremos una función D «promediando» la función d para forzar la $k[G]$-linealidad:

$$\begin{aligned} D\colon k[G] &\longrightarrow k[G] \\ x &\longmapsto \frac{1}{|G|} \sum_{g\in G} g d(g^{-1}x). \end{aligned}$$

Nótese que la condición de que $p \nmid |G|$ es para que $|G| \neq 0$ luego sea inversible.

Así, es fácil comprobar que D es k-lineal, y recordando que $\mathfrak{a}$ es un ideal izquierdo (luego $g \cdot \mathfrak{a} \subseteq \mathfrak{a}$) vemos que $\operatorname{Img} D \subseteq \mathfrak{a}$ y de que D fija a $\mathfrak{a}$.

Aún queda ver que D es $k[G]$-lineal: nótese que basta probar que si $x \in k[G]$ y $g \in G$ entonces $D(gx) = gD(x)$. Para ello:

$$gD(x) = \frac{1}{|G|} \sum_{h\in G} ghd(h^{-1}x) = \frac{1}{|G|} \sum_{h\in G} ghd(h^{-1}g^{-1}gx)$$

$$= \frac{1}{|G|} \sum_{\substack{j=gh\in G \\ h}} jd(j^{-1}gx) = D(gx),$$

donde la última igualdad sale del hecho de que $h \mapsto gh$ es una mera permutación sobre G. □

Desde aquí en adelante podemos hacer una discusión análoga a la de grupos resolubles y las series normales (véase §1.5.2).

Lema 5.39 (de Zassenhaus): Sean $B \leq B^*$ y $C \leq C^*$ submódulos de M. Entonces:

1. $B + (B^* \cap C)$ es submódulo de $B + (B^* \cap C^*)$.
2. $C + (C^* \cap B)$ es submódulo de $C + (C^* \cap B^*)$.
3. $\dfrac{B + (B^* \cap C^*)}{B + (B^* \cap C)} \cong \dfrac{C + (C^* \cap B^*)}{C + (C^* \cap B)}$.

Definición 5.40: Una serie de un A-módulo M es una cadena de submódulos:

$$M \geq M_1 \geq \cdots \geq M_n = \{\vec{0}\}.$$

Los cocientes M_i/M_{i+1} se llaman ***factores*** de la serie. Una serie se dice ***estricta*** si $M_i \neq M_{i+1}$ para todo i. Una serie de submódulos se dice ***de composición*** si es estricta y los factores son módulos simples.

Un par de series se dicen equivalentes si tienen la misma longitud y sus factores son isomorfos bajo permutación.

Proposición 5.41: Un A-módulo posee una serie de composición syss es noetheriano y artiniano.

Teorema 5.42 (de refinamiento de Schreier): Dos series de un mismo A-módulo poseen al menos un refinamiento equivalente.

Teorema 5.43 – *Teorema de Jordan-Hölder*: Todas las series de composición de un A-módulo (si existen) son equivalentes.

Definición 5.44: Si un A-módulo M posee una serie de composición, entonces por el teorema anterior todas sus series de composición tendrán la

misma longitud. Definimos $\ell(M)$, llamada la ***longitud*** de M, a la longitud de cualquier serie de composición.

Proposición (AEN) 5.45: Para un k-espacio vectorial V, las siguientes condiciones son equivalentes:

1. V tiene dimensión finita.
2. V tiene longitud finita.
3. V es noetheriano.
4. V es artiniano.

Más aún, si ese es el caso, entonces $\ell(V) = \dim_k(V)$.

Demostración: Es claro que $1 \implies 2$, y $2 \implies 3$ y $2 \implies 4$. Para ver que $3 \implies 1$, veamos la contrarrecíproca: Si V tiene dimensión infinita, entonces sea $\{\boldsymbol{x}_n : n \in \mathbb{N}\}$ un conjunto linealmente independiente, luego la cadena ascendente:

$$\mathrm{Span}_k\{\boldsymbol{x}_1\} \subset \mathrm{Span}_k\{\boldsymbol{x}_1, \boldsymbol{x}_2\} \subset \mathrm{Span}_k\{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3\} \subset \cdots$$

no posee $\subseteq$-maximal, por lo que V no es noetheriano.

La implicancia $4 \implies 1$ es análoga. □

Proposición 5.46: Dada la siguiente sucesión exacta de A-módulos noetherianos y artinianos:

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

se satisface que $\ell(M) = \ell(M') + \ell(M'')$.

Definición 5.47: Se dice que un A-módulo M es ***indecomposible*** si no existen $M_1, M_2 \leq M$ no nulos, tales que $M = M_1 \oplus M_2$.

Proposición 5.48: Un A-módulo M no trivial es indecomposible syss existe $\varphi \in \mathrm{End}(M) \setminus \{0, \mathrm{Id}\}$ idempotente.

Demostración: Ambas implicancias las haremos por contrarrecíproca.

$\Longleftarrow$. Si $M = M_1 \oplus M_2$, entonces la proyección π_1 que fija a M_1 y anula a M_2 es idempotente.

$\Longrightarrow$. Sea $\varphi \in \mathrm{End}(M) \setminus \{0, \mathrm{Id}\}$ idempotente. Definamos $e_1 := \varphi$ y $e_2 := \mathrm{Id} - \varphi$, nótese que

$$e_2^2 = 1 - 2e_1 + e_1^2 = 1 - 2e_1 + e_1 = 1 - e_1 = e_2,$$

y $e_1 e_2 = e_1(1 - e_1) = 0 = e_2 e_1$ (¿por qué?). Finalmente $M_i := e_i[M]$ satisface lo exigido. □

Definición 5.49: Un A-módulo M se dice ***fuertemente indecomposible*** si $M \neq 0$ y $\mathrm{End}(M)$ es un anillo local.

Lema 5.50: Sean M, N un par de A-módulos, con $M \neq 0$ y N indecomposible. Si $f\colon M \to N$ y $g\colon N \to M$ son homomorfismos de A-módulos y $f \circ g$ es un automorfismo, entonces f, g son isomorfismos.

Demostración: Basta probar que f lo es. Sea $\phi := f \circ g\colon M \to N$, $\psi := \phi^{-1}\colon N \to M$ y $h := g \circ \psi\colon N \to M$. Claramente $f \circ h = \mathrm{Id}_M$ y

$$(hf)^2 = h\underline{fh}f = hf,$$

por lo que hf es idempotente sobre N, y por inyectividad de f es claramente no nula, luego $hf = \mathrm{Id}$. □

Teorema 5.51: Sean:

$$M = M_1 \oplus \cdots \oplus M_n, \quad N = N_1 \oplus \cdots N_m,$$

donde $M \cong N$ y para todo i, j se cumple que M_i es fuertemente indecomposible y N_j es indecomposible. Entonces $n = m$ y tras una permutación $M_i \cong N_i$.

Demostración: Sean e_i las proyecciones en M hacia M_i, y f_j las proyecciones en N hacia N_j. Sea g un isomorfismo, entonces definamos $h_j := e_1 \circ g \circ f_j$ y $\ell_j := f_j \circ g^{-1} \circ e_1$, entonces observe el siguiente diagrama conmutativo:

$$\begin{array}{ccccc}
M & \xleftarrow{e_1} & M & & \\
{\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h_j} & & \\
N & \xrightarrow{f_j} & N & \xrightarrow{f_j} & N \\
 & & \downarrow{\scriptstyle \ell_j} & & \downarrow{\scriptstyle g^{-1}} \\
 & & M & \xleftarrow[e_1]{} & M
\end{array}$$

luego $h_j\ell_j = e_1 g f_j g^{-1} e_1$ y de hecho

$$\sum_{j=1}^{m} h_j\ell_j = \sum_{j=1}^{m} e_1 g f_j g^{-1} e_1 = e_1 g \left(\textstyle\sum_{j=1}^{m} f_j\right) g^{-1} e_1 = e_1.$$

Como e_1 fija a M_1, en particular podemos considerar las restricciones $e_1' \colon M_1 \to M_1$ y $(h_j\ell_j)' \colon M_1 \to M_1$; por la ecuación anterior se concluye que $\sum_{j=1}^{m} (h_j\ell_j)' = \mathrm{Id}_{M_1}$, pero como $\mathrm{End}(M_1)$ es un anillo local, entonces no todos los $h_j\ell_j$'s pueden estar en el maximal, vale decir, alguno es inversible. Reordenemos de modo que $(h_j\ell_j)'$ es inversible, es decir, es un automorfismo, luego por el lema anterior se satisface que $h_1' \colon M_1 \to N_1$ y $\ell_1' \colon N_1 \to M_1$ son isomorfismos. Para finalizar sólo basta probar que

$$M = g^{-1}[N_1] \oplus (M_2 + \cdots + M_n).$$

Sea $\boldsymbol{x} \in g^{-1}[N_1] \cap (M_2 + \cdots + M_n)$, luego sea $\boldsymbol{y} := g(\boldsymbol{x}) \in N_1$, como $\boldsymbol{x} \in M_2 + \cdots + M_n$, entonces

$$\vec{0} = e_1(\boldsymbol{x}) = (g^{-1} \circ e_1)(\boldsymbol{y}) = (f_1 \circ g^{-1} \circ e_1)(\boldsymbol{y}) = \ell_j'(\boldsymbol{y}),$$

por lo que $\boldsymbol{y} = \vec{0}$ y $\boldsymbol{x}$ también. Por otro lado sea $\boldsymbol{x} \in M' := g^{-1}[N_1] + M_2 + \cdots + M_n$; luego $\boldsymbol{x}, e_2\boldsymbol{x}, \ldots, e_n\boldsymbol{x} \in M'$ por lo que $e_1\boldsymbol{x} \in M'$ y por ende $M' \supseteq e_1[g^{-1}[N_1]] = (g^{-1}e_1)[N_1] = \ell_1[N_1] = M_1$, de lo que se concluye que $M' = M$.

Finalmente, el enunciado se concluye por inducción sobre n. □

Definición 5.52: Sea M un A-módulo y $f \in \mathrm{End}(M)$, entonces se definen:

$$f^{\infty}M := \bigcap_{n\in\mathbb{N}} f^n[M], \qquad f^{-\infty}0 := \bigcup_{n\in\mathbb{N}} \ker(f^n).$$

Nótese que ambos son submódulos de M.

Lema 5.53 (Fitting): Sea M un A-módulo noetheriano y artiniano, y $f \in \mathrm{End}(M)$. Entonces:

$$M = f^{\infty}M \oplus f^{-\infty}0,$$

y más aún, f se restringe a un automorfismo en $f^{\infty}M$ y es nilpotente en $f^{-\infty}0$.

Demostración: Nótese que se tienen las siguientes cadenas de submódulos:

$$M \subseteq f[M] \subseteq f^2[M] \cdots \to f^\infty M, \quad \ker f \supseteq \ker(f^2) \supseteq \cdots \to f^{-\infty}0.$$

Como M es artiniano y noetheriano, existe n suficientemente grande tal que $f^n[M] = f^\infty M$ y $\ker(f^n) = f^{-\infty}0$.

Sea $\boldsymbol{z} \in f^\infty M \cap f^{-\infty}0$, entonces $\boldsymbol{z} = f^n(\boldsymbol{y})$ y $f^n(\boldsymbol{z}) = \vec{0}$, pero como $\ker(f^n) = \ker(f^{2n})$, entonces $f^{2n}(\boldsymbol{y}) = \vec{0}$, y $\boldsymbol{y} \in \ker(f^{2n}) = \ker(f^n)$, por lo que $\boldsymbol{z} = f^n(\boldsymbol{y}) = \vec{0}$. y en sintesis $f^n(\boldsymbol{z} - f^n(\boldsymbol{y})) = \vec{0}$.

Sea $\boldsymbol{x} \in M$, luego, $f^n(\boldsymbol{x}) \in f^n[M] = f^{2n}[M]$, por lo que $f^n(\boldsymbol{x}) = f^{2n}(\boldsymbol{y})$, luego $f^n(\boldsymbol{x} - f^n(\boldsymbol{y})) = \vec{0}$ y, por ende,

$$\boldsymbol{x} = f^n(\boldsymbol{y}) + (\boldsymbol{x} - f^n(\boldsymbol{y})) \in f^\infty M + f^{-\infty}0. \qquad \square$$

Corolario 5.54: Sea M un A-módulo noetheriano y artiniano. Si M es indecomposible, entonces todo endomorfismo de M es un automorfismo o es nilpotente. En particular, M es fuertemente indecomposible.

Finalmente, y aplicando lo visto en el teorema de Jordan-Hölder se obtiene que:

Teorema 5.55 (Krull-Schmidt): Sea $M \neq 0$ un A-módulo noetheriano y artiniano, entonces existen M_i's indecomposibles tales que

$$M = M_1 \oplus \cdots \oplus M_n,$$

y toda otra factorización de éste estilo es tal que los términos son isomorfos salvo permutación.

5.3 Productos tensoriales

Definición 5.56: Sean M, N, T un trío de A-módulos. Una aplicación $\varphi\colon M \times N \to T$ es ***A*-bilineal** si es un morfismo en cada coordenada, formalmente:

BL1. Si para todo $\boldsymbol{n}_0 \in N$ se cumple que la aplicación $\boldsymbol{m} \mapsto \varphi(\boldsymbol{m}, \boldsymbol{n}_0)$ es un morfismo de A-módulos.

BL2. Si para todo $\boldsymbol{m}_0 \in M$ se cumple que la aplicación $\boldsymbol{n} \mapsto \varphi(\boldsymbol{m}_0, \boldsymbol{n})$ es un morfismo de A-módulos.

Se denota por $\mathrm{Bil}_A(M \times N, T)$ al conjunto de aplicaciones A-bilineales desde $M \times N$ hasta T.

Ejemplo. En el capítulo sobre módulos ya vimos un primer ejemplo clásico: el determinante. La aplicación $\det\colon k^2 \times k^2 \to k$ es claramente k-bilineal (por definición, de hecho), pero no es k-lineal en sí misma, de hecho, si $\operatorname{car} k \neq 2$, entonces

$$\det\big((2,0),(0,2)\big) = 4 \neq 2 = 2\det\big((1,0),(0,1)\big).$$

En general las aplicaciones bilineales no suelen ser lineales y ejemplos análogos al anterior aplican.

En ésta sección pretendemos definir el producto tensorial, sin embargo hay dos posibilidades: una es comenzar definiéndolo de manera concreta y concluir la propiedad universal categórica que le define, o la otra es comenzar por definir la propiedad categórica y concluir por otorgar una construcción concreta. En éste libro hemos en general optado por la primera, pero ahora lo haremos de manera inversa.

Comencemos con la siguiente observación:

Proposición 5.57: Fijemos un par de A-módulos M, N.

1. Para todo A-módulo T, se cumple que $\mathrm{Bil}_A(M \times N, T)$ es un A-módulo.
2. Dado un homomorfismo de A-módulos $f\colon T_1 \to T_2$ se cumple que la poscomposición:
$$\begin{aligned} h^f\colon \mathrm{Bil}_A(M \times N, T_1) &\longrightarrow \mathrm{Bil}_A(M \times N, T_2) \\ \varphi &\longmapsto \varphi \circ f \end{aligned}$$
es también un homomorfismo de A-módulos.
3. Dado $\mathrm{Id}_T\colon T \to T$ se cumple que $h^T = \mathrm{Id}\colon \mathrm{Bil}_A(M \times N, T) \to \mathrm{Bil}_A(M \times N, T)$.
4. Dados $f\colon T_1 \to T_2, g\colon T_2 \to T_3$ homomorfismos de A-módulos, se cumple que $h^{f\circ g} = h^f \circ h^g$.

En resumen, $\mathrm{Bil}_A(M \times N, -)\colon \mathsf{Mod}_A \to \mathsf{Mod}_A$ es un funtor:

$$\begin{array}{ccc} T_1 & & \mathrm{Bil}_A(M \times N, T_1) \\ {\scriptstyle f}\big\downarrow & \xRightarrow{\mathrm{Bil}_A(M\times N,-)} & \big\downarrow{\scriptstyle h^f} \\ T_2 & & \mathrm{Bil}_A(M \times N, T_2) \end{array}$$

Hay una serie de teoremas que expresaremos en ésta estructura a lo largo del libro. Nótese que uno podría simplemente especificar la definición de h^f y poner el diagrama y eso expresa tanto como los cuatro incisos juntos.

Definición 5.58: Un par $(M \otimes_A N, \otimes)$ es un producto tensorial de M, N si:

PT1. $\otimes\colon M \times N \to M \otimes_A N$ es una aplicación A-bilineal.

PT2. Para toda aplicación A-bilineal $\varphi\colon M \times N \to T$ existe un único homomorfismo de A-módulos $\bar{\varphi}\colon M \otimes_A N \to T$ tal que $\varphi = \otimes \circ \bar{\varphi}$. Es decir, el siguiente diagrama conmuta (en Set):

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_A N \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \exists!\bar{\varphi}} \\ & & T \end{array}$$

Equivalentemente, $M \otimes_A N$ es un objeto representado por el funtor $\mathrm{Bil}_A(M \times N, -)$.

Cuando no haya ambigüedad sobre los signos podemos obviar el subíndice «A».

Teorema 5.59: Los productos tensoriales existen.

Demostración: Sean M, N un par de A-módulos. Entonces comencemos por definir $F(M \times N) := A^{\oplus(M\times N)}$, es decir, el A-módulo libre que tiene por base a $M \times N$, queremos que la función $j\colon M \times N \to F(M \times N)$ que manda cada objeto en sí mismo sea bilineal. Sea K el submódulo generado por todos los elementos de la forma

$$j(\alpha \boldsymbol{m}_1 + \beta \boldsymbol{m}_2, \boldsymbol{n}) - \alpha j(\boldsymbol{m}_1, \boldsymbol{n}) - \beta j(\boldsymbol{m}_2, \boldsymbol{n})$$

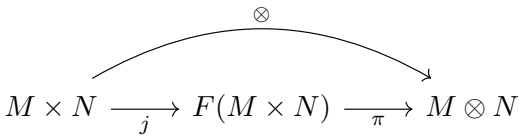
con $\alpha, \beta \in A$, $\boldsymbol{m}_1, \boldsymbol{m}_2 \in M$ y $\boldsymbol{n} \in N$; y los elementos de la forma

$$j(\boldsymbol{m}, \alpha \boldsymbol{n}_1 + \beta \boldsymbol{n}_2) - \alpha j(\boldsymbol{m}, \boldsymbol{n}_1) - \beta j(\boldsymbol{m}, \boldsymbol{n}_2)$$

con $\alpha, \beta \in A$, $\boldsymbol{m} \in M$ y $\boldsymbol{n}_1, \boldsymbol{n}_2 \in N$. Finalmente definamos

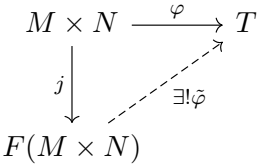
$$M \otimes N := \frac{F(M \times N)}{K},$$

junto a la aplicación:



Nótese de que por construcción de K se cumple que $\otimes$ resulte bilineal.

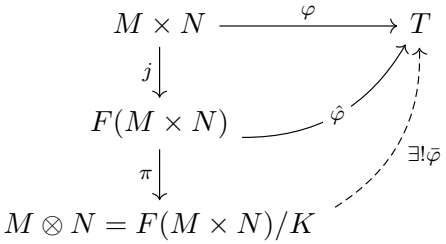
Luego hay que verificar que se satisfaga la propiedad universal. Sea $\varphi\colon M \times N \to T$ bilineal, entonces por definición de módulo libre se cumple que existe:



tal que el diagrama conmuta, donde $\hat{\varphi}$ es un morfismo de A-módulos. Basta probar que $\hat{\varphi}$ se anula en K:

$$\begin{aligned}
&\hat{\varphi}\big(j(\alpha\boldsymbol{m}_1 + \beta\boldsymbol{m}_2, \boldsymbol{n}) - \alpha j(\boldsymbol{m}_1, \boldsymbol{n}) - \beta j(\boldsymbol{m}_2, \boldsymbol{n})\big)\\
&\quad = \hat{\varphi}\big(j(\alpha\boldsymbol{m}_1 + \beta\boldsymbol{m}_2, \boldsymbol{n})\big) - \alpha\hat{\varphi}\big(j(\boldsymbol{m}_1, \boldsymbol{n})\big) - \beta\hat{\varphi}\big(j(\boldsymbol{m}_2, \boldsymbol{n})\big)\\
&\quad = \varphi(\alpha\boldsymbol{m}_1 + \beta\boldsymbol{m}_2, \boldsymbol{n}) - \alpha\varphi(\boldsymbol{m}_1, \boldsymbol{n}) - \beta\varphi(\boldsymbol{m}_2, \boldsymbol{n})\\
&\quad = \vec{0}.
\end{aligned}$$

De lo cual se sigue que el siguiente diagrama necesariamente conmuta:



□

Definición 5.60: Los objetos de $M \otimes_A N$ se le llaman ***tensores***. Nótese que como $M \times N$ es base de $F(M \times N)$, entonces es un sistema generador de $M \otimes N$, es decir, todo tensor es de la forma

$$\boldsymbol{m}_1 \otimes \boldsymbol{n}_1 + \boldsymbol{m}_2 \otimes \boldsymbol{n}_2 + \cdots + \boldsymbol{m}_s \otimes \boldsymbol{n}_s,$$

con $s > 0$, $\boldsymbol{m}_i \in M$ y $\boldsymbol{n}_i \in N$ (aquí suprimimos los coeficientes dados que por bilinealidad se pueden «meter» dentro del producto y dado que los objetos de los módulos son cerrados bajo producto escalar).

A los tensores de la forma $\boldsymbol{m} \otimes \boldsymbol{n}$ se le dicen ***tensores puros***. Nótese que los tensores puros generan al resto de tensores, pero ellos no constituyen necesariamente todos los tensores.

Proposición 5.61: Si $M = \mathrm{Span}_A(B)$ y $N = \mathrm{Span}_A(C)$, entonces

$$M \otimes_A N = \mathrm{Span}_A(\{\boldsymbol{b} \otimes \boldsymbol{c} : \boldsymbol{b} \in B, \boldsymbol{c} \in C\}).$$

Demostración: Basta notar que si

$$\boldsymbol{m} = \lambda_1 \boldsymbol{b}_1 + \cdots + \lambda_s \boldsymbol{b}_s$$

entonces $\boldsymbol{m} \otimes \boldsymbol{n} = \sum_{i=1}^{s} \lambda_i (\boldsymbol{b}_i \otimes \boldsymbol{n}_i)$. □

En consecuencia diríamos que si V, W son k-espacios vectoriales, entonces $\dim_k(V \otimes_k W) \leq \dim_k(V) \cdot \dim_k(W)$. Pero ésta afirmación se puede mejorar.

Primero comenzaremos con la siguiente observación:

Teorema 5.62: Sean M, N, T un trío de A-módulos, entonces

$$\mathrm{Hom}_A(M \otimes_A N, T) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, T))$$

(como A-módulos).

Demostración: Sea $\alpha \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, T))$, eso quiere decir que $\alpha(\boldsymbol{m}) \in \mathrm{Hom}_A(N, T)$. Luego la siguiente aplicación:

$$\begin{aligned} \varphi\colon M \times N &\longrightarrow T \\ (\boldsymbol{m}, \boldsymbol{n}) &\longmapsto \alpha(\boldsymbol{m})(\boldsymbol{n}) \end{aligned}$$

es A-bilineal, y por ende admite una única factorización $\overline{\alpha}\colon M \otimes_A N \to T$ (que es un morfismo de A-módulos) tal que $\otimes \circ \overline{\alpha} = \alpha$. Queda al lector comprobar que la aplicación $\alpha \mapsto \overline{\alpha}$ es el isomorfismo de A-módulos deseado. □

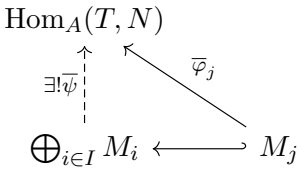
Ésto puede parecer un resultado parcialmente inofensivo, pero demuestra una intrínseca dualidad especial entre los tensores y los conjuntos Hom's.

Proposición 5.63: Sean M, N, T un trío de A-módulos, entonces:

1. $M \otimes_A N \cong N \otimes_A M$.
2. $(M \oplus N) \otimes_A T \cong (M \oplus T) \otimes_A (N \oplus T)$.

3. En general, si $\{M_i\}_{i\in I}$ es una familia de A-módulos, entonces
$$\left(\bigoplus_{i\in I} M_i\right) \otimes_A T \cong \bigoplus_{i\in I}(M_i \otimes_A T).$$
4. En particular, $A^{\oplus X} \otimes_A A^{\oplus Y} \cong A^{\oplus(X\times Y)}$.
5. Más en particular, si k es cuerpo, entonces $k^n \otimes_k k^m = k^{nm}$.
6. $A \otimes_A M \cong M$ y $0 \otimes_A M \cong 0$.
7. $- \otimes_A N$ es un funtor exacto por la derecha.
8. Sea $\mathfrak{a}$ un ideal de A, entonces
$$\frac{A}{\mathfrak{a}} \otimes_A M \cong \frac{M}{\mathfrak{a}M}.$$
9. Sean $\mathfrak{a}, \mathfrak{b}$ ideales de A, entonces
$$\frac{A}{\mathfrak{a}} \otimes_A \frac{A}{\mathfrak{b}} \cong \frac{A}{\mathfrak{a}+\mathfrak{b}}.$$

Demostración: La primera es clara. Las propiedades 2 a 5 salen todas con tal de probar la 3, lo cual haremos por propiedad universal: Sea $\{\varphi_i \colon M_i \otimes T \to N\}_{i\in I}$ una familia de morfismos de A-módulos. Vale decir,
$$\varphi_i \in \mathrm{Hom}_A(M_i \otimes_A T, N) \iff \overline{\varphi}_i \in \mathrm{Hom}_A(M_i, \mathrm{Hom}_A(T,N));$$
luego existe una única extensión tal que el siguiente diagrama conmuta:



finalmente consideramos que $\overline{\psi} \in \mathrm{Hom}\left(\bigoplus_{i\in I} M_i, \mathrm{Hom}_A(T,N)\right)$ lo devolvemos a $\psi \in \mathrm{Hom}\left(\left(\bigoplus_{i\in I} M_i\right) \otimes_A T, N\right)$. Queda al lector comprobar que ψ es una extensión única.

Para la sexta emplee $\otimes \colon (a, \boldsymbol{m}) \mapsto a\boldsymbol{m}$ y note que toda aplicación bilineal desde $0\times M$ es necesariamente el morfismo nulo. Para la séptima basta aplicar el mismo truco anterior y recordar que Hom preservaba sucesiones exactas.

Para la octava considere la sucesión exacta

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0$$

la cual se traduce en

$$\mathfrak{a} \otimes_A M \longrightarrow A \otimes_A M \cong M \longrightarrow A/\mathfrak{a} \otimes_A M \longrightarrow 0 \otimes_A M \cong 0$$

Nótese además que $\mathfrak{a} \otimes_A M \cong \mathfrak{a}M$. Luego existe una transformación canónica que completa el que $A/\mathfrak{a} \otimes_A M \cong M/\mathfrak{a}M$. □

Ejemplo. Consideraremos los siguientes productos tensoriales en $\mathbb{Z}$. Considere la siguiente sucesión exacta

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$$

donde $f(n) = 2n$ y tensoricemos los factores por $\mathbb{Z}/2\mathbb{Z}$: luego considere

$$\bar{f} := f \otimes \mathbb{Z}/2\mathbb{Z} \colon \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

que nótese que manda el [0] en el cero y el [1] en el cero. De modo que $\bar{f} = 0$, por lo que la sucesión

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\bar{f}} \mathbb{Z}/2\mathbb{Z}$$

no es exacta.

Proposición 5.64 (cambio de base): Sea M un A-módulo, N un B-módulo y P un A-B-bimódulo (i.e., un A-módulo izquierdo que es B-módulo derecho y tal que $(ax)b = a(xb)$ para todo $a \in A, b \in B, x \in P$). Entonces:

1. $\mathrm{Hom}_A(M, \mathrm{Hom}_B(P, N)) \cong \mathrm{Hom}_B(M \otimes_A P, N)$.
2. $(M \otimes_A P) \otimes_B N \cong M \otimes_A (P \otimes_B N)$.

Demostración: En la primera, interpretamos que $\mathrm{Hom}_B(P, N)$ es un A-módulo con el producto escalar $\varphi \in \mathrm{Hom}_B(P, N)$ dado por $a\varphi(x) = \varphi(ax)$. Dado un homomorfismo de B-módulos $\psi \colon M \otimes_A P \to N$, entonces podemos definir

$$\begin{aligned} f(\psi) \colon M &\longrightarrow \mathrm{Hom}_B(P, N) \\ m &\longmapsto \big(p \mapsto \psi(m \otimes p)\big). \end{aligned}$$

Recíprocamente, dado $\phi \colon M \to \mathrm{Hom}_B(P, N)$ podemos definir $\bar{\phi} := g(\phi) \colon M \otimes_A P \to N$ que toma valores $\bar{\phi}(m \otimes p) = \phi(m)(p)$ sobre los tensores puros.

Es fácil comprobar que f, g establecen isomorfismos, una siendo la inversa de la otra.

Para la propiedad 2, recordamos el teorema 5.62 y aplicamos para un B-módulo T:

$$\begin{aligned}\mathrm{Hom}_B\left((M \otimes_A P) \otimes_B N, T\right) &\cong \mathrm{Hom}_B\left(M \otimes_A P, \mathrm{Hom}_B(N,T)\right)\\ &\cong \mathrm{Hom}_A\left(M, \mathrm{Hom}_B(P, \mathrm{Hom}_B(N,T))\right)\\ &\cong \mathrm{Hom}_A\left(M, \mathrm{Hom}_B(P \otimes_B N, T)\right)\\ &\cong \mathrm{Hom}_B\left(M \otimes_A (P \otimes_B N), T\right).\end{aligned}$$ □

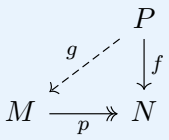
Definición 5.65: Se dice que el A-módulo N es ***plano*** si $- \otimes_A N$ es un funtor exacto. El A-módulo N se dice ***fielmente plano*** si el funtor $- \otimes_A N$ preserva y refleja exactitud.

Proposición 5.66: Un A-módulo $M = \bigoplus_{i \in I} M_i$ es (fielmente) plano syss cada M_i es (fielmente) plano.

De momento no le podremos sacar tanto provecho a los módulos planos, pero veremos varias propiedades más en el capítulo de álgebra conmutativa.

5.4 Módulos proyectivos e inyectivos

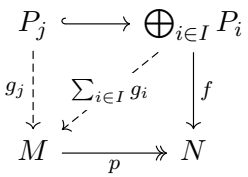
Definición 5.67: Sea P un A-módulo. P se dice un ***módulo proyectivo*** si para todo par de A-módulos M, N, y todo $f\colon P \to N$ y $p\colon M \to N$ homomorfismos de A-módulos, con p suprayectivo, existe un $g\colon P \to M$ tal que el siguiente diagrama:



conmuta.

Proposición 5.68: La suma directa de módulos proyectivos es proyectiva.

Demostración: Basta considerar el siguiente diagrama conmutativo:



□

Como ejercicio, note que la demostración anterior emplea un uso de elección y encuéntrelo. No obstante, dicho uso puede erradicarse empleando la siguiente proposición:

Proposición 5.69: Un A-módulo P es proyectivo syss el funtor $\mathrm{Hom}_A(P,-)$ es exacto.

Demostración: Ya sabemos que $\mathrm{Hom}_A(P,-)$ es exacto por la izquierda, luego basta comprobar que si

$$M \xrightarrow{\ p\ } N \longrightarrow 0$$

es exacto (i.e., si p es suprayectivo), entonces

$$\mathrm{Hom}_A(P,M) \xrightarrow{\ h^p\ } \mathrm{Hom}(P,N) \longrightarrow 0$$

también es exacto, pero ésto es la definición de ser proyectivo. □

Corolario 5.70: El producto tensorial de finitos módulos proyectivos es proyectivo.

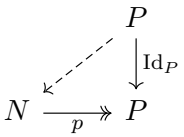
Proposición (AE) 5.71: Sea P un A-módulo. Son equivalentes:

1. P es proyectivo.
2. Toda sucesión exacta corta

$$0 \longrightarrow M \longrightarrow N \xrightarrow{\ p\ } P \longrightarrow 0$$

   se escinde.
3. P es un sumando directo de un A-módulo libre. Más aún, si P es finitamente generado, entonces es el sumando directo de un A-módulo libre de dimensión finita.

Demostración: 1 $\implies$ 2. En la sucesión, p es suprayectivo, luego basta considerar el siguiente diagrama conmutativo:



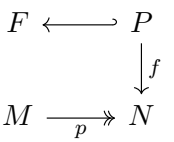
para concluir.

2 $\implies$ 3. Sea S un sistema generador de P, y sea $F := A^{\oplus S}$, es decir, el A-módulo libre que posee a S como base, de modo que $\iota\colon S \to P$ induce trivialmente un epimorfismo $p\colon F \to P$. Luego sea $P' := \ker p$ y así se obtiene la siguiente sucesión exacta:

$$0 \longrightarrow P' \longrightarrow F \xrightarrow{\ p\ } P \longrightarrow 0$$

la cual se escinde, luego $F = P \oplus P'$.

3 $\implies$ 1. Dado el siguiente diagrama conmutativo:



como $F = P \oplus P'$ podemos definir $\hat{f}\colon F \to N$ tal que se anule en P' y coincida con f en P. Sea $X = \{\boldsymbol{x}_i + \boldsymbol{y}_i\}_{i\in I}$ una base de F, donde $\boldsymbol{x}_i \in P$ e $\boldsymbol{y}_i \in P'$ para todo $i \in I$. Podemos definir una función $h^*\colon X \to M$ donde a cada $\boldsymbol{x}_i + \boldsymbol{y}_i$ le asigne un elemento de $p^{-1}\big[\{\hat{f}(\boldsymbol{x}_i)\}\big]$ (el cuál existe porque p es suprayectivo), que luego, por definición de módulo libre, se extiende a un homomorfismo de A-módulos $h\colon F \to M$. Finalmente, queda al lector comprobar que efectivamente $g := \iota \circ h \circ p\colon P \to N$ hace conmutar el diagrama. □

Y otro corolario particularmente útil es el siguiente:

Teorema (AE) 5.72: Los A-módulos proyectivos son planos.

Proposición (AE) 5.73 (lema de las bases duales): Sea P un A-módulo. Son equivalentes:

1. P es proyectivo.
2. Existe $\{\boldsymbol{x}_i\}_{i\in I}$ en P y $\{f_i\}_{i\in I}$ en $\mathrm{Hom}_A(P, A)$ tales que para todo $\boldsymbol{x} \in P$ se cumple que $f_i(\boldsymbol{x}) = 0$ para todos salvo finitos $i \in I$, y tal que

$$\boldsymbol{x} = \sum_{i\in I} f_i(\boldsymbol{x})\boldsymbol{x}_i.$$

En cuyo caso $\{\boldsymbol{x}_i\}_{i\in I}$ es un sistema generador de P. Más aún, si P es finitamente generado podemos exigir que I sea finito.

Demostración: $\Longrightarrow$. Sea $S := \{\boldsymbol{x}_i\}_{i\in I}$ un sistema de generadores de P. Luego sea F un A-módulo libre con base $\{\boldsymbol{y}_i\}_{i\in I}$, luego el morfismo $p\colon F \to P$ que manda $p(\boldsymbol{y}_i) = \boldsymbol{x}_i$ es suprayectivo, por lo que se factoriza en $q\colon P \to F$ tal que $q \circ p = \mathrm{Id}_P$. Como F es libre, la aplicación $\pi_j\colon F \to A$ dada por

$$\pi_j\left(\sum_{i\in I} a_i\boldsymbol{y}_i\right) = a_j$$

está bien definida y es un homomorfismo; más aún, para un $\boldsymbol{y} \in F$ fijo, $\pi_j(\boldsymbol{y})$ es nulo para todos salvo finitos $i \in I$. Luego definimos $f_i := q \circ \pi_i$ y comprobamos que cumple lo exigido.

$\Longleftarrow$. Nuevamente, sea F un A-módulo libre con base $\{\boldsymbol{y}_i\}_{i\in I}$ y considere el epimorfismo $p\colon F \to P$ que manda $p(\boldsymbol{y}_i) = \boldsymbol{x}_i$. Nótese que trivialmente $\tau_j\colon \boldsymbol{x} \mapsto f_j(\boldsymbol{x})\boldsymbol{y}_j$ es un homomorfismo de módulos, que induce el siguiente homomorfismo

$$\begin{aligned} s := \sum_{i\in I} \tau_i\colon P &\longrightarrow F \\ \boldsymbol{x} &\longmapsto \sum_{i\in I} f_i(\boldsymbol{x})\boldsymbol{y}_i \end{aligned}$$

que satisface que $s \circ p = \mathrm{Id}_P$. Finalmente la sucesión:

$$0 \longrightarrow \ker p \longrightarrow F \xrightarrow{\ p\ } P \longrightarrow 0$$

es exacta y se escinde. □

Pese al nombre no se confunda, ni $\{\boldsymbol{x}_i\}_{i\in I}$ ni $\{f_i\}_{i\in I}$ tienen por que ser bases.

Dualizar el concepto de módulo proyectivo da la noción de módulo inyectivo. Éstos conceptos se estudian en mayor profundidad en el cuarto capítulo de mi libro de categorías y álgebra homológica **[55],** por lo que no los veremos en tanta profundidad aquí, exceptuando por un par de resultados de álgebra conmutativa.

5.5 Módulos sobre DIPs

El primer resultado que querremos ver que sobre un DIP todo submódulo de un módulo libre es libre. Para ello volveremos un poco al tema de grupos abelianos:

Proposición 5.74: Sea G un grupo abeliano, entonces para todo $n > 0$ natural:

$$nG := \{ng : g \in G\}$$

es un subgrupo de G. Más aún, si p es un número primo, entonces G/pG es un $\mathbb{F}_p$-espacio vectorial.

Demostración: Sea $[r] \in \mathbb{F}_p$ y sea $g \in G$, luego definamos

$$[r] \cdot (a + pG) := ra + pG.$$

Nótese que está bien definido dado que si $r' = r + pm$, entonces

$$r'a + pG = ra + pma + pG = ra + pG,$$

dado que $p(ma) \in pG$. También es fácil probar el resto de axiomas de un espacio vectorial. □

Corolario 5.75: Se cumplen:

1. Todo grupo abeliano libre finitamente generado es isomorfo a $\mathbb{Z}^n$ para algún n. Más generalmente, definiendo $\mathbb{Z}^{\oplus\kappa} := \bigoplus_{\alpha=1}^{\kappa} \mathbb{Z}$, se cumple que todo grupo abeliano libre es isomorfo a $\mathbb{Z}^{\oplus\kappa}$ para algún número cardinal κ.

2. Más aún, $\mathbb{Z}^n \cong \mathbb{Z}^m$ syss $n = m$. De modo que todo par de bases de un grupo abeliano libre finitamente generado son de igual cardinalidad.

3. (AE) $\mathbb{Z}^{\oplus\kappa} \cong \mathbb{Z}^{\oplus\mu}$ syss $\kappa = \mu$. De modo que todo par de bases de un grupo abeliano libre son de igual cardinalidad.

Demostración: Para probar la segunda y la tercera basta tomar un grupo abeliano libre G y considerar a $G/2G$ como $\mathbb{F}_2$-espacio vectorial. Luego la unicidad de cardinalidad de bases de un espacio vectorial induce la unicidad de cardinalidad de bases como grupo abeliano libre. □

Definición 5.76: Dado un grupo abeliano libre G, se denota por $\operatorname{rang} G$ a la cardinalidad de cualquiera de sus bases.

Proposición 5.77: Sea G un grupo abeliano con un conjunto X tal que satisface lo siguiente: Para todo grupo abeliano H y toda aplicación $f\colon X \to H$, existe una única extensión $f^*\colon G \to H$ que es un homomorfismo de grupos. Entonces G es un grupo abeliano libre de base X.

Demostración: Sea H un grupo abeliano libre de base Y tal que existe una biyección $q\colon X \to Y$ de inversa $p\colon Y \to X$. Luego, por ser libres, ambas funciones se extienden a $f\colon G \to H$ y $g\colon H \to G$, homomorfismos de grupos. Nótese que además $p \circ q = \mathrm{Id}_X\colon X \to X \subseteq G$ es una aplicación que posee una extensión $\mathrm{Id}_G\colon G \to G$ que es única, y lo mismo vale para Id_H como extensión única de $q \circ p$. Finalmente, $p \circ q$ también se extiende a $f \circ g$ y $q \circ p$ se extiende a $g \circ f$, luego se comprueba que f, g son homomorfismos de grupos y además son una la inversa de la otra. □

Proposición (AE) 5.78: Sea M un A-módulo y $N \leq M$ tal que M/N es un módulo libre. Entonces existe $F \leq M$ tal que $M/N \cong F$ y $M = N \oplus F$.

Demostración: Si N es un submódulo de M, entonces la siguiente sucesión:

$$0 \longrightarrow N \longrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$$

es exacta. Como M/N es libre entonces posee una base $X = \{[x_i]\}_{i\in I}$, por tanto, la aplicación $g\colon X \to M$ dada por $g([x_i]) := x_i$ admite una extensión única $g\colon M/N \to M$, tal que $g \circ \pi$ fija a la base, luego por unicidad, se cumple que $g \circ \pi = \mathrm{Id}_{M/N}$. Es decir, la sucesión exacta se escinde y por la proposición 5.15 se cumple el enunciado. □

Como ejercicio en la demostración anterior ubique el uso de elección.

Teorema (AE) 5.79: Sea A un DIP, entonces todo A-submódulo M de un módulo libre F es también libre; y de hecho $\operatorname{rang} M \leq \operatorname{rang} F$.

Demostración: Como F es libre, entonces posee una base, que por el teorema del buen orden (AE) admite un buen orden $X = \{x_\alpha : \alpha < \kappa\}$ (aquí los subíndices son ordinales). Luego definamos

$$F'_\beta := \langle\{x_\alpha : \alpha < \beta\}\rangle, \qquad F_\beta := F'_\beta \oplus \langle x_\beta\rangle.$$

Y definamos $M'_\beta := M \cap F'_\beta$ y $M_\beta := M \cap F_\beta$. Nótese que

$$\frac{M_\beta}{M'_\beta} = \frac{M_\beta}{M_\beta \cap F'_\beta} \cong \frac{M_\beta + F'_\beta}{M_\beta} \subseteq \frac{F'_\beta}{F_\beta} \cong A,$$

donde hemos empleado el tercer teorema de isomorfismos (para módulos). Así que M_β/M'_β es isomorfo a un ideal de A, pero todos los ideales de A son principales, luego o son el ideal nulo o son isomorfos (como A-módulos) a

A. Si el ideal no es nulo, entonces por la proposición anterior se cumple que $M_\beta \cong M'_\beta \oplus \langle \boldsymbol{m}_\beta \rangle$ para algún $\boldsymbol{m}_\beta \in M_\beta$ tal que $\langle \boldsymbol{m}_\beta \rangle \cong A$; si el ideal es nulo entonces $\boldsymbol{m}_\beta := \vec{0}$. Claramente, eliminando los $\boldsymbol{m}_\beta$'s nulos se tiene que éstos elementos son linealmente independientes (por construcción, de hecho), de modo que simplemente bastaría probar que generan a M para concluir el enunciado.

Para ello, definamos $M^* := \text{Span}\{\boldsymbol{m}_\beta\}_{\beta<\kappa}$ y definamos:

$$\mu(\boldsymbol{m}) := \text{mín}\{\alpha : \boldsymbol{m} \in F_\alpha\}.$$

Supongamos que $M^* < M$, entonces definamos γ como el mínimo índice tal que $\gamma = \mu(\boldsymbol{m})$ para algún $\boldsymbol{m} \in M \setminus M^*$ y sea $\tilde{\boldsymbol{m}}$ un elemento que cumpla lo anterior, luego se cumple que

$$\tilde{\boldsymbol{m}} = \boldsymbol{a} + \lambda \boldsymbol{m}_\gamma \in M_\gamma$$

para unos únicos $\boldsymbol{a} \in M'_\gamma$ y $\lambda \in A$. Luego como $\boldsymbol{m}_\gamma \in M^*$ y $\tilde{\boldsymbol{m}} \notin M^*$ necesariamente se tiene que $\boldsymbol{a} \notin M^*$. Pero $\boldsymbol{a} \in F'_\gamma$, luego $\mu(\boldsymbol{a}) < \gamma$ contradiciendo la minimalidad de γ. □

Nótese que si F es finitamente generado, entonces no hay uso de elección.

Corolario (AE) 5.80: En un DIP todo módulo proyectivo es libre.

Éste teorema se puede mejorar, pero requiere más trabajo (ver teo. 6.50).

Corolario (AE) 5.81: En un DIP todo submódulo de un módulo proyectivo es también proyectivo.

Notas históricas

Los productos tensoriales fueron surgiendo progresivamente en varias partes de las matemáticas. Se cree que el primer registro fue en el caso de espacios vectoriales y, en particular, el caso de espacios tangente en geometría diferencial. El primero en trabajar con tensores en contexto de grupos abelianos fue Whitney [**49**] (1938)). La construcción fue generalizada por Bourbaki [**34**] (1942) quién realizó la construcción en módulos sobre anillos no conmutativos con la distinción de módulo izquierdo y derecho; ésto también fue hecho independientemente por E. Artin *y col.* [**33**] (1946).

6

Introducción al álgebra conmutativa

6.1 Anillos locales y radicales

§6.1.1 Localización. Ésta es una de las técnicas más importantes para el álgebra conmutativa. El nombre proviene de la interpretación de la geometría algebraica.

Definición 6.1: Se dice que un anillo unitario A es un ***anillo local*** si posee un único ideal maximal. Decimos que $(A, \mathfrak{m})$ es local, si A es local y $\mathfrak{m}$ es el único ideal maximal de A; y decimos que $(A, \mathfrak{m}, k)$ es local si $(A, \mathfrak{m})$ es local y $k = A/\mathfrak{m}$. A k le decimos el ***cuerpo de residuos*** de A.

Nótese que por el teorema de Krull se tiene que todo anillo posee al menos un ideal maximal, así que la definición está justificada.

Otras consecuencia del teorema de Krull es la siguiente:

Proposición (AE) 6.2: Todo elemento no inversible está contenido en un ideal maximal.

Demostración: Basta notar que $(a) \neq (1)$ si a no es inversible. □

Proposición 6.3: Se cumplen:

1. Un dominio es un anillo local syss el conjunto de los elementos no inversibles constituye un ideal, en cuyo caso, corresponde al único ideal maximal.

2. Sea A un anillo con un ideal maximal $\mathfrak{m}$ tal que para todo $x \in \mathfrak{m}$ se cumpla que $1 + x$ es inversible. Entonces A es un anillo local.

Demostración: La primera es consecuencia de la proposición anterior.

Para la segunda sea $x \notin \mathfrak{m}$, luego por maximalidad $(x, \mathfrak{m}) = A$, es decir, $ax + y = 1$ para algún $a \in A, y \in \mathfrak{m}$. Luego $ax = 1 - y \in 1 + \mathfrak{m}$, por lo que es inversible y luego $(ax)^{-1}a = x^{-1}$. □

Ejemplo. Considere el siguiente anillo

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b \right\},$$

es fácil notar que es local y que su ideal maximal es $p \cdot \mathbb{Z}_{(p)}$. Más aún, su cuerpo de residuos es $\mathbb{F}_p$.

Definición 6.4: Sea A un dominio. Un ***sistema multiplicativo*** S, es un subconjunto tal que $(S, \cdot)$ es un monoide, esto es, tal que:

1. Si $a, b \in S$, entonces $ab \in S$ (clausura).

2. Si $a, b, c \in S$, entonces $(ab)c = a(bc)$ (asociatividad).

3. $1 \in S$ (elemento neutro).

(Nótese que la condición de asociatividad es redundante pues se hereda de la asociatividad en A.)

Lema 6.5: Sea S un sistema multiplicativo, entonces la relación $\sim$ sobre $A \times S$ dada por

$$(a, s) \sim (b, t) \iff \exists r \in S \quad r(at - bs) = 0$$

es de equivalencia.

Demostración: La reflexividad y simetría son triviales. Veamos la transitividad: sean $(a, s) \sim (b, t)$ y $(b, t) \sim (c, u)$. Por definición sean $r_1, r_2 \in S$ tales que

$$r_1(at - bs) = r_2(bu - ct) = 0$$

luego, nótese que $r_2, t, s \in S$ de modo que

$$r_1 r_2(uat - ubs) = r_1 r_2(sbu - sct) = 0$$

sumando ambas ecuaciones se obtiene que

$$r_1 r_2(uat - sct) = r_1 r_2 t(au - cs) = 0$$

con $r_1 r_2 t \in S$ como se quería probar. □

Definición 6.6: Se denota por $S^{-1}A := A \times S/\sim$, donde $\sim$ es la relación del lema anterior. Se denota $a/s := [a, s] \in S^{-1}A$

Es inmediato que la construcción anterior generaliza el cuerpo de fracciones, así que es natural que surja el siguiente teorema:

Teorema 6.7: $(S^{-1}A, +, \cdot)$ es un dominio de neutro aditivo $0/1$, neutro multiplicativo $1/1$, donde

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

La función $\lambda_S \colon A \to S^{-1}A$ dada por $\lambda_S(a) = a/1$ es un morfismo de anillos. Más aún, $S^{-1}A$ es un A-módulo, λ_S un morfismo de módulos y todo elemento de S es inversible en $S^{-1}A$.

Demostración: Hay que ver primero que las operaciones están bien definidas: Para ello sean $a_1/s_1 = a_2/s_2$ tales que $r(a_1 s_2 - a_2 s_1) = 0$ con $r \in S$. Nótese que basta ver que

$$\frac{a_1 t + b s_1}{s_1 t} = \frac{a_2 t + b s_2}{s_2 t}, \quad \frac{a_1 b}{s_1 t} = \frac{a_2 b}{s_2 t}.$$

Para ello nótese que

$$r\big((a_1 t + \cancel{b s_1}) s_2 t - (a_2 t + \cancel{b s_2}) s_1 t\big) = t^2 \cdot r(a_1 s_2 - a_2 s_1) = 0,$$
$$r\big(a_1 b s_2 t - a_2 b s_1 t\big) = bt \cdot r(a_1 s_2 - a_2 s_1) = 0.$$

Probar que es un anillo es análogo a las demostraciones de que $\mathrm{Frac}(A)$ lo es. Lo mismo para notar que λ_S es morfismo. □

Teorema 6.8: Sea A un dominio y S un sistema multiplicativo de A.

1. Todos los ideales de $S^{-1}A$ son de la forma $S^{-1}\mathfrak{a}$ con $\mathfrak{a} \trianglelefteq A$.

2. Todos los ideales primos de $S^{-1}A$ son de la forma $S^{-1}\mathfrak{p}$ con $\mathfrak{p} \trianglelefteq A$ primo disjunto de S.

Demostración:

1. Sea $\mathfrak{b} \trianglelefteq S^{-1}A$ y definamos $\mathfrak{a} := \mathfrak{b} \cap A$. Sea $x = a/s \in \mathfrak{b}$, entonces $sx = a \in \mathfrak{b} \cap A = \mathfrak{a}$, de modo que $\mathfrak{b} = S^{-1}\mathfrak{a}$.

2. Sea $\mathfrak{q} \trianglelefteq S^{-1}A$ un ideal primo, entonces por el enunciado anterior $\mathfrak{p} := \mathfrak{q} \cap A \trianglelefteq A$ es un ideal primo (¿por qué?). Como $1 \notin \mathfrak{q}$ se sigue que $\mathfrak{p} \cap S = \varnothing$.

   Conversamente sea $\mathfrak{p} \trianglelefteq A$ disjunto de S, y sea $\mathfrak{q} := S^{-1}\mathfrak{p}$, veamos que ha de ser un ideal primo: Supongamos que $\frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{q}$, de modo que como $s, t \in S$, existe $r \in S$ tal que $rab \in \mathfrak{p}$. Como $\mathfrak{p}$ es primo y $r \notin \mathfrak{p}$, entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, de lo que se sigue que $a/s \in \mathfrak{q}$ o $b/t \in \mathfrak{q}$. □

Proposición 6.9: Si A es noetheriano y S es un sistema multiplicativo de A, entonces $S^{-1}A$ también es noetheriano.

Proposición 6.10: Sea $\mathfrak{p} \lhd A$ primo. Luego $S := A \setminus \mathfrak{p}$ es un sistema multiplicativo tal que $(S^{-1}A, S^{-1}\mathfrak{p}, \mathrm{Frac}(A/\mathfrak{p}))$ es un anillo local. En éste caso, denotamos por $A_{\mathfrak{p}}$ a dicho anillo y le llamamos la ***localización en*** $\mathfrak{p}$.

Demostración: Sea

$$I := \{a/s \in S^{-1}A : a \in \mathfrak{p},\ s \in S\}.$$

Basta comprobar que I es efectivamente un ideal de A (¿por qué?) y que todo elemento no inversible esté en I. Para la segundo, si a/s no es inversible, entonces $s/a \notin S^{-1}A$, lo que equivale a que $a \notin S$, lo que equivale a que $a \in \mathfrak{p}$, luego $a/s \in I$ como se quería probar. □

La construcción anterior justifica la notación de $\mathbb{Z}_{(p)}$ e ilustra por qué es local. La localización es una de las principales técnicas del álgebra conmutativa, junto con los cocientes $A/\mathfrak{p}$ (ya vistos en el capítulo 2) y junto con las compleciones (que veremos en el capítulo 12).

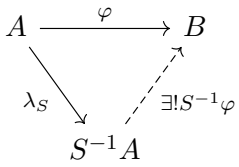
Lema 6.11: El morfismo λ_S es inyectivo syss S no posee divisores de cero.

Demostración: $\Longrightarrow$. Por contrarrecíproca: si $a \in S$ es divisor de cero, es decir, si $ab = 0$ con $b \neq 0$, entonces $\lambda_S(b) = \lambda_S(0)$.

$\Longleftarrow$. Sean $a, b \in A$ tales que $\lambda_S(a) = \lambda_S(b)$ lo que se traduce en que existe $r \in S$ tal que $r(a-b) = 0$; pero como r no es divisor de cero, entonces necesariamente $a - b = 0$ y $a = b$. □

Teorema 6.12: Sean A, B dominios y S un sistema multiplicativo de A. Sea $\varphi\colon A \to B$ un morfismo tal que $\varphi[S] \subseteq B^\times$, entonces el siguiente diagrama conmuta:

$$\begin{aligned} S^{-1}\varphi\colon S^{-1}A &\longrightarrow B \\ a/s &\longmapsto \varphi(a)/s \end{aligned}$$



Demostración:

i) Veamos que dicho morfismo está bien definido: En primer lugar $\varphi(s)$ es inversible pues $\varphi[S] \subseteq B^\times$ y además si $a/s = b/t$ existe $r \in S$ tal que $r(at - bs) = 0$ y

$$0 = \varphi(r)\big(\varphi(at) - \varphi(bs)\big) = \varphi(a)\varphi(t) - \varphi(b)\varphi(s)$$

donde cancelamos a $\varphi(r)$ pues es inversible. Y así nos queda que $\bar{\varphi}(a/s) = \bar{\varphi}(b/t)$.

Ver que es morfismo de anillos y que el diagrama conmuta queda al lector.

ii) Veamos que es único: Supongamos que α, β hacen conmutar al diagrama y sea $a/s \in S^{-1}A$, entonces

$$\alpha(a/s) = \alpha(a/1)\alpha(1/s) = \varphi(a)\varphi(s)^{-1} = \beta(a/1)\beta(1/s) = \beta(a/s).$$

□

Definición 6.13: Dado un anillo A, llamamos su ***anillo de fracciones totales*** K al anillo $S^{-1}A$ donde S es el conjunto de los elementos de A que no son divisores de cero.

Si A es un dominio íntegro, entonces su anillo de fracciones totales coincide con su cuerpo de fracciones.

Antes de seguir, nótese la siguiente observación:

Proposición 6.14: Sea A un dominio. Entonces si consideramos a A como A-módulo, sus submódulos son, efectivamente, los ideales de A.

Así pues, queremos extender las construcciones anteriores para A-módulos, así que similarmente establecemos los siguientes resultados análogos:

Lema 6.15: Sea S un sistema multiplicativo de A y sea M un A-módulo, entonces la relación $\sim$ sobre $M \times S$ dada por

$$(\boldsymbol{u}, s) \sim (\boldsymbol{v}, t) \iff \exists r \in S \quad r(\boldsymbol{u}t - \boldsymbol{v}s) = \vec{0}$$

es de equivalencia.

Proposición 6.16: $S^{-1}M$ es un A-módulo (y un $S^{-1}A$-módulo también) y la función $\lambda_S \colon M \to S^{-1}M$ dada por $\lambda_S(\boldsymbol{m}) = \boldsymbol{m}/1$ es un morfismo de módulos. Más aún, λ_S es inyectiva syss S no contiene divisores de cero.

Proposición 6.17: Sea S un sistema multiplicativo de A. Entonces determina un funtor covariante exacto entre los A-módulos:

$$\begin{aligned} S^{-1}f \colon S^{-1}M_1 &\longrightarrow S^{-1}M_2 \\ \boldsymbol{m}/s &\longmapsto f(\boldsymbol{m})/s \end{aligned} \qquad \begin{array}{ccc} M_1 & & S^{-1}M_1 \\ {\scriptstyle f}\downarrow & \overset{S^{-1}-}{\Longrightarrow} & \downarrow{\scriptstyle S^{-1}f} \\ M_2 & & S^{-1}M_2 \end{array}$$

Proposición 6.18: 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.

Demostración: Claramente 1 $\implies$ 2 $\implies$ 3. Veamos 3 $\implies$ 1 por contrarrecíproca: Si $M \neq 0$ sea $\boldsymbol{m} \neq \vec{0} \in M$. Luego sea $\mathfrak{a} := \operatorname{Ann}(\boldsymbol{m}) \neq (1)$.[1] Por el teorema de Krull, se cumple que $\mathfrak{a} \subseteq \mathfrak{m}$ maximal. Luego $\boldsymbol{m}/1 \in M_{\mathfrak{m}}$ y $\boldsymbol{m}/1 \neq \vec{0}$, puesto que si lo fuera entonces $s\boldsymbol{m} = \vec{0}$ con $s \in A \setminus \mathfrak{m} \subseteq A \setminus \mathfrak{a}$, lo que es absurdo. □

[1] Véase def. 6.34.

Ésto es un sumo útil, pues permite reducir varios problemas al caso de anillos locales. También motiva la siguiente definición:

Definición 6.19: Dado un A-módulo M se le llama su ***soporte*** al conjunto $\mathrm{Supp}(M)$ de todos los ideales primos $\mathfrak{p} \lhd A$ tales que $M_\mathfrak{p} \neq 0$.

La proposición anterior ahora se traduce en que M es no nulo syss su soporte no es vacío.

Corolario 6.20: Sea $\varphi\colon M \to N$ un homomorfismo de A-módulos. Entonces φ es inyectiva (resp. suprayectiva, isomorfismo) syss para todo $\mathfrak{m} \lhd A$ maximal se cumple que $\varphi_\mathfrak{m}\colon M_\mathfrak{m} \to N_\mathfrak{m}$ lo es.

Proposición 6.21: Sea M un A-módulo y S un sistema multiplicativo de A. Entonces, para todo par N, T de submódulos de M se cumplen:

1. $S^{-1}N$ es un submódulo de $S^{-1}M$.
2. $S^{-1}(N+T) = S^{-1}N + S^{-1}T$.
3. $S^{-1}(N \cap T) = S^{-1}N \cap S^{-1}T$.
4. $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.
5. Si $\mathfrak{a}, \mathfrak{b}$ son ideales de A, entonces $S^{-1}(\mathfrak{a}\cdot\mathfrak{b}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$.

Proposición 6.22: Sea M un A-módulo. Entonces

$$\begin{aligned} f\colon S^{-1}A \otimes_A M &\longrightarrow S^{-1}M \\ \sum_{k=1}^{n}(a_k/s_k)\otimes \boldsymbol{m}_k &\longmapsto \sum_{k=1}^{n} a_k\boldsymbol{m}_k/s_k. \end{aligned}$$

es un isomorfismo, y más aún es el único entre dichos dominios.

Demostración: Consideremos la aplicación

$$\begin{aligned} \varphi\colon S^{-1}A \times M &\longrightarrow S^{-1}M \\ (a/s, \boldsymbol{m}) &\longmapsto a\boldsymbol{m}/s. \end{aligned}$$

Claramente φ es A-bilineal y por definición de producto tensorial se cumple que existe una única $\bar\varphi\colon S^{-1}A \otimes M \to S^{-1}M$ tal que $\varphi = \otimes \circ \bar\varphi$. Luego definimos $f := \bar\varphi$ que concuerda con el enunciado.

Claramente f es suprayectiva y para ver que es inyectiva. Primero veamos que todo tensor en $S^{-1}A \otimes M$ es puro: Para ello, definamos $s := \prod_{k=1}^{n} s_k$ y $t_i := \prod_{\substack{k=1 \\ k\neq i}}^{n} s_k$, luego:

$$\sum_{k=1}^{n} \frac{a_k}{s_k} \otimes \boldsymbol{m}_k = \sum_{k=1}^{n} \frac{a_k t_k}{s} \otimes \boldsymbol{m}_k = \sum_{k=1}^{n} \frac{1}{s} \otimes a_k t_k \boldsymbol{m} = \frac{1}{s} \otimes \left(\sum_{k=1}^{n} a_k t_k \boldsymbol{m} \right).$$

Luego, como $1/s$ es inversible, se cumple que $f(1/s \otimes \boldsymbol{m}) = \boldsymbol{m}/s = 0$ syss $\boldsymbol{m} = \vec{0}$. □

Corolario 6.23: $S^{-1}A$ es un A-módulo plano.

§6.1.2 Radicales.

Definición 6.24: Sea A un dominio, entonces un elemento $a \in A$ es ***nilpotente*** si existe $n \geq 1$ tal que $x^n = 0$.

Proposición (AE) 6.25: Si S es un sistema multiplicativo que no contiene al 0, entonces existe el conjunto de los ideales contenidos en S^c posee un $\subseteq$-maximal que es de hecho un ideal primo del anillo.

Demostración: Sea $\mathcal{F} := \{\mathfrak{a} : \mathfrak{a} \trianglelefteq A, \mathfrak{a} \subseteq S^c\}$, y sea $\{\mathfrak{a}_i\}_{i\in I}$ una $\subseteq$-cadena de $\mathcal{F}$; ya sabemos que $\mathfrak{b} := \bigcup_{i\in I} \mathfrak{a}_i$ es también un ideal y claramente está también contenido en S^c. Luego por lema de Zorn $\mathcal{F}$ posee un elemento $\subseteq$-maximal $\mathfrak{p}$.

Probaremos que $\mathfrak{p}$ es primo por contradicción: Sea $ab \in \mathfrak{p}$ tales que $a, b \notin \mathfrak{p}$, entonces como $(a, \mathfrak{p}) \supset \mathfrak{p}$ se ha de cumplir que $(a, \mathfrak{p})$ y $(b, \mathfrak{p})$ poseen elementos de S, digamos:

$$s = r_1 a + p, \qquad s' = r_2 b + p'$$

con $s, s' \in S$, $r_1, r_2 \in A$ y $p, p' \in \mathfrak{p}$. Luego

$$s \cdot s' = r_1 r_2 ab + p'(r_1 a) + ps'$$

pero $s \cdot s' \in S$ y $ab, p, p' \in \mathfrak{p}$ lo que es absurdo puesto que $\mathfrak{p}$ no posee elementos de S. □

Corolario 6.26: Se cumplen:

1. Un elemento nilpotente pertenece a todos los ideales primos de A.
2. (AE) Si un elemento pertenece a todos los ideales primos de A, entonces es nilpotente.

Definición 6.27: Dado un ideal $\mathfrak{a}$ se define su radical como

$$\mathrm{Rad}(\mathfrak{a}) = \{a \in A : \exists n\ a^n \in \mathfrak{a}\}.$$

Se dice que $\mathfrak{a}$ es ***radical*** si $\mathfrak{a} = \mathrm{Rad}(\mathfrak{a})$.

Se le llama el ***nilradical*** de A a $\mathfrak{N}(A) := \mathrm{Rad}(0)$, es decir, al conjunto de los elementos nilpotentes. Un dominio está ***reducido*** si $\mathfrak{N}(A) = (0)$.

El corolario anterior entonces se puede reescribir así:

$$\mathfrak{N}(A) = \bigcap\{\mathfrak{p} : \mathfrak{p} \trianglelefteq A \text{ primo}\}.$$

El lector creerá que es un caso particular del radical, pero engloba a todo el resto haciendo la siguiente observación: Sea $\mathfrak{a}$ un ideal arbitrario de A, entonces el nilradical de $A/\mathfrak{a}$, bajo el teorema de la correspondencia, nos otorga el siguiente teorema:

Teorema (AE) 6.28: 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.

Corolario 6.29: Todo ideal primo es radical.

Una demostración es trivial, pero intente hacerlo sin emplear AE y por lo tanto sin emplear el teorema anterior.

Proposición 6.30: Para todo sistema multiplicativo S de A se cumple que $S^{-1}\,\mathfrak{N}(A) = \mathfrak{N}(S^{-1}A)$.

Demostración: Sea $a \in A, s \in S$ tales que $a/s \in \mathfrak{N}(S^{-1}A)$, luego $(a/s)^n = 0$ syss $ta^n = 0 = (ta)^n$ con $ta \in \mathfrak{N}(A)$. Luego $\frac{a}{s} = \frac{ta}{ts} \in S^{-1}\,\mathfrak{N}(A)$. □

Corolario 6.31: A es reducido syss $A_{\mathfrak{m}}$ es reducido para todo $\mathfrak{m} \lhd A$ maximal.

Proposición 6.32: 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 $\mathrm{Rad}(\mathfrak{a}) + \mathrm{Rad}(\mathfrak{b}) = (1)$.

Demostración: Probaremos las primeras dos:

1. Definamos $\mathfrak{r} := \mathrm{Rad}(\mathfrak{a})$. Claramente se cumple que $\mathfrak{a} \subseteq \mathrm{Rad}(\mathfrak{a})$, así que veamos que es un ideal. Para ello consideremos $a, b \in \mathfrak{r}$, de modo que $a^n, b^m \in \mathfrak{a}$ para algunos n, m:
   i) Para todo $\lambda \in A$ se da que $(\lambda a)^n = \lambda^n a^n \in \mathfrak{a}$, dado que $\mathfrak{a}$ es ideal.
   ii) Se cumple que $a + b \in \mathfrak{r}$: En efecto, basta notar que
   $$\begin{aligned}(a+b)^{n+m} &= \sum_{j=0}^{n+m} \binom{n+m}{j} a^j b^{n+m-j} \\ &= b^m \sum_{j=0}^{n} \binom{n+m}{j} a^j b^{n-j} + a^n \sum_{j=0}^{m} \binom{n+m}{n+j} a^j b^{m-j}.\end{aligned}$$
   iii) Claramente $a \cdot b \in \mathfrak{r}$ puesto que si $N := \min\{n, m\}$, entonces $(ab)^N = a^N b^N$, donde alguno de los dos factores está en $\mathfrak{a}$, luego el producto también.
2. Por la proposición anterior claramente se da que $\mathrm{Rad}(\mathfrak{a}) \subseteq \mathrm{Rad}(\mathrm{Rad}(\mathfrak{a}))$. Sea $a \in \mathrm{Rad}(\mathrm{Rad}(\mathfrak{a}))$, entonces $a^n \in \mathrm{Rad}(\mathfrak{a})$ y entonces $(a^n)^m \in \mathfrak{a}$ para algunos n, m. Pero entonces $(a^n)^m = a^{nm} \in \mathfrak{a}$, luego $a \in \mathrm{Rad}(\mathfrak{a})$. □

Proposición 6.33: Sea $\mathfrak{m} \lhd A$ un ideal maximal, y sea $\mathfrak{n} := \mathfrak{m}A_{\mathfrak{m}}$ el cual es maximal. Para todo $n \in \mathbb{N}$, el morfismo

$$\phi_n \colon A/\mathfrak{m}^n \longrightarrow A_{\mathfrak{m}}/\mathfrak{n}^n$$

$$a + \mathfrak{m}^n \longmapsto a + \mathfrak{n}^n$$

es un isomorfismo y, de hecho comprueba que $\mathfrak{m}^r/\mathfrak{m}^n \cong \mathfrak{n}^r/\mathfrak{n}^n$ para todo $r < n$.

Demostración: Nótese que $\mathfrak{n}^n = (\mathfrak{m}^n)^e$, de modo que

$$\ker(A/\mathfrak{m}^n \to A_\mathfrak{m}/\mathfrak{n}^n) = (\mathfrak{m}^n)^{ec}/\mathfrak{m}^n.$$

Sea $a \in (\mathfrak{m}^n)^{ec}$, es decir, $a/1 = b/s$ para $b \in \mathfrak{m}^n, s \in S$ donde $S = A \setminus \mathfrak{m}$. Luego existe $t \in S$ tal que $tsa \equiv 0 \pmod{\mathfrak{m}^n}$. Pero $t, s \in S$ son inversibles en $A_\mathfrak{m}$, por lo tanto, $a \equiv 0 \pmod{\mathfrak{m}^n}$. Esto comprueba que $(\mathfrak{m}^n)^{ec} \subseteq \mathfrak{m}^n$ y ϕ_n es inyectiva.

Falta ver que ϕ_n es suprayectiva: para ello sea $a/s \in A_\mathfrak{m}$ con $a \in A, s \in S$. Todo ideal maximal que contiene a $\mathfrak{m}^n$ contiene a $\mathrm{Rad}(\mathfrak{m}^n) = \mathfrak{m}$, luego $(s) + \mathfrak{m}^n$ no está contenido en ningún ideal maximal y es, por lo tanto, todo A. Ergo, $sb + q = 1$ para algún $b \in A, q \in \mathfrak{m}^n$ de lo que se sigue:

$$\begin{aligned} sb = 1 - q &\iff s(ab) = a(1-q) \\ &\iff \frac{ab}{1} = \frac{a}{s} - \frac{aq}{s}, \end{aligned}$$

como $aq/s \in \mathfrak{n}^n$ se sigue que $ab/1 = a/s \pmod{\mathfrak{n}^n}$ de lo que se concluye la suprayectividad. □

Definición 6.34: 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 6.35: Sean $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ideales de A. Entonces:

1. $(\mathfrak{a} : \mathfrak{b})$ es un ideal.
2. Más generalmente, si S, T son submódulos de un A-módulo M, entonces $(S : T)$ es un ideal de A.
3. $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.
4. $\big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big) = (\mathfrak{a} : \mathfrak{bc}) = \big(\mathfrak{a} : \mathfrak{c} : \mathfrak{b}\big)$.

5. $\left(\bigcap_{i\in I}\mathfrak{a}_i : \mathfrak{b}\right) = \bigcap_{i\in I}(\mathfrak{a}_i : \mathfrak{b})$.
6. $\left(\mathfrak{a} : \sum_{i\in I}\mathfrak{b}_i\right) = \bigcap_{i\in I}(\mathfrak{a} : \mathfrak{b}_i)$.

Demostración: Haremos un par:

3. Para todo $x \in \mathfrak{a}$ se cumple que $\mathfrak{a} \supseteq xA \supseteq x\mathfrak{b}$.

6. Lo haremos probando las dos inclusiones: Sea $x \in \left(\mathfrak{a} : \sum_{i\in I}\mathfrak{b}_i\right)$, luego, nótese que como $0 \in \mathfrak{b}_i$ para todo ideal en general, se tiene que para todo $y \in \mathfrak{b}_i$ se cumple que $xy \in \mathfrak{a}$, luego $x \in (\mathfrak{a} : \mathfrak{b}_i)$ para todo $i \in I$. En particular x está en la intersección.

   La otra inclusión viene dada por que si $x \in \bigcap_{i\in I}(\mathfrak{a} : \mathfrak{b}_i)$, entonces para todo $y_i \in \mathfrak{b}_i$ se cumple que $xy_i \in \mathfrak{a}$, luego $x\sum_{i\in I} y_i \in \mathfrak{a}$. □

Proposición 6.36: Denotemos D el conjunto de los divisores de cero de A. Entonces

$$D = \bigcup_{x\neq 0} \mathrm{Rad}(\mathrm{Ann}(x)) = \bigcup_{x\neq 0} \mathrm{Ann}(x).$$

§6.1.3 Extensión y contracción de ideales. Es muy usual en álgebra conmutativa reducir desde un anillo a otro. Un método sencillo de aprovechar esta correspondencia es mediante la extensión y contracción de ideales.

Definición 6.37: Sea $\varphi\colon A \to B$ un morfismo de anillos, y sean $\mathfrak{a}, \mathfrak{b}$ ideales de A y B resp. Entonces se define la ***contracción*** de $\mathfrak{b}$ y la ***extensión*** de $\mathfrak{a}$ como:

$$\mathfrak{b}^c := \varphi^{-1}[\mathfrak{b}], \qquad \mathfrak{a}^e := \big(\varphi[\mathfrak{a}]\big).$$

Nótese que si $A \subseteq B$, entonces $\mathfrak{b}^c = \mathfrak{b} \cap A$.

La idea de éstas definiciones está en forzar de manera natural una correspondencia entre ideales bajo el morfismo. Así pues, ya hemos visto que la contracción de ideales primos es primo, pero la extensión no necesariamente.

Ejemplo. Sea $\iota\colon \mathbb{Z} \to \mathbb{Q}$, entonces $(p)^e = \mathbb{Q}$ para todo p primo; de modo que la extensión de todo ideal primo no nulo es no primo. Reemplazando $\mathbb{Z}$ por cualquier dominio íntegro y $\mathbb{Q}$ por su cuerpo de fracciones vemos que esta misma situación siempre se replica.

La siguiente proposición justifica la terminología:

Proposición 6.38: Sea $\varphi\colon A \to B$ un morfismo de anillos y sean $\mathfrak{a}, \mathfrak{b}$ ideales de A y B resp. Entonces:

1. Si $\mathfrak{a} \subseteq \mathfrak{a}' \trianglelefteq A$, entonces $\mathfrak{a}^e \subseteq \mathfrak{a}'^e$. Si $\mathfrak{b} \subseteq \mathfrak{b}' \trianglelefteq B$, entonces $\mathfrak{b}^c \subseteq \mathfrak{b}'^c$.
2. $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ y $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$.
3. $\mathfrak{a}^e = \mathfrak{a}^{ece}$ y $\mathfrak{b}^c = \mathfrak{b}^{cec}$.
4. Las siguientes aplicaciones:

$$\{\mathfrak{a} \trianglelefteq A : \mathfrak{a}^{ec} = \mathfrak{a}\} \underset{()^c}{\overset{()^e}{\rightleftarrows}} \{\mathfrak{b} \trianglelefteq B : \mathfrak{b}^{ce} = \mathfrak{b}\}$$

   son biyecciones y son la una la inversa de la otra.

Proposición 6.39: Sea S un sistema multiplicativo de A, $\mathfrak{a} \trianglelefteq A$ y consideremos el morfismo $\lambda_S\colon A \to S^{-1}A$. Entonces:

1. Todo ideal de $S^{-1}A$ es una extensión de un ideal en A.
2. $\mathfrak{a}^{ec} = \bigcup_{s\in S}(\mathfrak{a} : s)$. En consecuencia, $\mathfrak{a}^e = (1)$ syss $\mathfrak{a} \cap S \neq \varnothing$.
3. $\mathfrak{a}$ es una contracción syss ningún elemento de S es divisor de cero en $A/\mathfrak{a}$.
4. Las siguientes aplicaciones:

$$\{\mathfrak{p} \lhd A : \mathfrak{p} \text{ primo}, \mathfrak{p} \cap S \neq \varnothing\} \underset{()^c}{\overset{S^{-1}-}{\rightleftarrows}} \{\mathfrak{q} \lhd S^{-1}A : \mathfrak{q} \text{ primo}\}$$

   son biyecciones y son la una la inversa de la otra.

Demostración:

1. Sea $\mathfrak{b} \trianglelefteq S^{-1}A$, hay que probar que $\mathfrak{b}^{ce} = \mathfrak{b}$. Para ello, sea $x/s \in \mathfrak{b}$, entonces $x/1 \in \mathfrak{b}$, por ende $x \in \mathfrak{b}^c$ y luego $x/s \in \mathfrak{b}^{ce}$; es decir, hemos probado que $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$ y se concluye por doble contención.
2. Siga la siguiente cadena de equivalencias:

$$\begin{aligned} x \in \mathfrak{a}^{ec} = (S^{-1}\mathfrak{a})^c &\iff \exists a \in \mathfrak{a}, s \in S \quad x/1 = a/s \\ &\iff \exists a \in \mathfrak{a}, s \in S, t \in S \quad (xs - a)t = 0 \\ &\iff \exists s \in S, t \in S \quad xst \in \mathfrak{a} \\ &\iff \exists s \in S \quad x \in (\mathfrak{a} : s). \end{aligned}$$

3. $\mathfrak{a}$ es contracción syss $\mathfrak{a}^{ec} \subseteq \mathfrak{a}$ y luego emplee el inciso anterior.

4. Ejercicio para el lector. □

Proposición 6.40: 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.

Demostración: $\Longrightarrow$. Trivial.

$\Longleftarrow$. Sea $S := \varphi[A \setminus \mathfrak{p}] \subseteq B$. Entonces $\mathfrak{p}^e$ no corta a S y, por tanto, su extensión en $S^{-1}B$ es propia, de modo que está contenido en un ideal maximal $\mathfrak{m} \lhd S^{-1}B$. Sea $\mathfrak{q}$ la contracción de $\mathfrak{m}$ en B, entonces $\mathfrak{q}$ es primo (por ser la contracción de un primo) y $\mathfrak{q} \supseteq \mathfrak{p}^e$ y $\mathfrak{q} \cap S = \varnothing$. Finalmente $\mathfrak{q}^c = \mathfrak{p}$. □

§6.1.4 El lema de Nakayama y sus consecuencias.

Definición 6.41: Dado un anillo A, se define su ***radical de Jacobson*** como

$$\mathfrak{J}(A) := \bigcap \{\mathfrak{m} : \mathfrak{m} \lhd A,\ \mathfrak{m} \text{ maximal}\}.$$

Proposición 6.42: Se cumplen:

1. El radical de Jacobson es un ideal radical.

2. Si A es un anillo local, $\mathfrak{J}(A)$ es su único ideal maximal.

3. $y \in \mathfrak{J}(A)$ syss para todo $x \in A$ se cumple que $1 - xy \in A^\times$.

Demostración: La primera y segunda quedan al lector. La tercera: $y \in \mathfrak{J}(A)$ syss $y \in \mathfrak{m}$ para todo $\mathfrak{m} \lhd A$ maximal. Como $1 \notin \mathfrak{m}$, entonces $1 - xy \notin \mathfrak{m}$ para todo $x \in A$. Pero todo elemento no inversible está contenido en algún ideal maximal (por teorema de Krull), de modo que $1 - xy$ es inversible. □

Teorema 6.43 – *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 $a_i \in \mathfrak{a}$.

Demostración: En primer lugar, si M es finitamente generado sea $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ un sistema generador finito y luego se ha de cumplir que $\varphi(\boldsymbol{x}_i) = \sum_{j=1}^{n} c_{ij}\boldsymbol{x}_j$ con $c_{ij} \in \mathfrak{a}$, o equivalentemente

$$\sum_{j=1}^{n}(\delta_{ij}\varphi - c_{ij})\boldsymbol{x}_j = \vec{0}$$

para todo i. Luego formando la matriz $B := [\delta_{ij}\varphi - c_{ij}]_{ij}$, nos damos cuenta de que B aplicado sobre todo $\boldsymbol{x}_i$ se anula, por lo que, multiplicando por $\operatorname{adj} B$ también los anula y se comprueba que $\det(B) = 0$. Expandiendo el determinante se obtiene un polinomio como el del enunciado; en el caso de elegir una base para un k-espacio vectorial ésto no es más que el polinomio característico de la matriz. □

Ésta proposición será empleada para el siguiente resultado y más adelante en la sección de dependencia íntegra.

Ahora procedemos a probar un famoso resultado de álgebra conmutativa. El lema de Nakayama posee varias versiones y aquí enlisté todas las que encontré. El mismo Nakayama sugiere que se le llame «teorema de Krull-Azumaya», pero el nombre de «lema de Nakayama» es mucho más estándar.

Teorema 6.44 – *Lema de Nakayama*: Sea M un A-módulo finitamente generado. Se cumplen:

1. Si $\mathfrak{a} \trianglelefteq A$ tal que $\mathfrak{a}M = M$, entonces existe $x \equiv 1 \pmod{\mathfrak{a}}$ tal que $xM = \{\vec{0}\}$.
2. Si $\mathfrak{a} \trianglelefteq A$ tal que $\mathfrak{a} \subseteq \mathfrak{J}(A)$. Si $\mathfrak{a}M = M$ entonces $M = \{\vec{0}\}$.
3. Si N es un submódulo de M tal que $N + \mathfrak{J}(A)M = M$, entonces $N = M$.
4. Si $M/\mathfrak{J}(A)M = \operatorname{Span}_A\{[\boldsymbol{x}_1], \ldots, [\boldsymbol{x}_n]\}$, entonces $M = \operatorname{Span}_A\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$.

Demostración:

1. Considere el lema anterior con $\varphi = \mathrm{Id}$ y sea $x := 1 + a_{n-1} + \cdots + a_1 + a_0$.
2. Sea x como en el inciso 1, entonces $x - 1 = y \in \mathfrak{J}(A)$, pero $1 - y = x$ es inversible, luego $xM = M = \{\vec{0}\}$.
3. Basta aplicar el inciso anterior con M/N.

4. Basta aplicar el inciso anterior con $N = \mathrm{Span}_A\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$. □

Ejemplo. Considere a $\mathbb{Q}$, el cual es un $\mathbb{Z}_{(p)}$-módulo, pero *no* es finitamente generado. Nótese que $p \cdot \mathbb{Q} = \mathbb{Q}$, pero $\mathbb{Q} \neq \{0\}$.

Definición 6.45: Se dice que un conjunto $S \subseteq M$ es una ***base minimal*** si es un sistema generador y es minimal, vale decir, si todo subconjunto propio de S no genera a M.

Observe que, pese al nombre, una base minimal *no* necesariamente es una base; ésto sólo se daría en módulos libres. Por ejemplo, $\{1\}$ es una base minimal de $\mathbb{Z}/2\mathbb{Z}$ (como $\mathbb{Z}$-módulo) que claramente no es base.

En particular, el lema de Nakayama induce lo siguiente para dominios locales:

Proposición 6.46: Sea $(A, \mathfrak{m}, k)$ un dominio local, sea M un A-módulo finitamente generado y sea $\overline{M} := M/\mathfrak{m}M$. Entonces:

1. $\overline{M}$ es un k-espacio vectorial de dimensión finita n.
2. Si elegimos una base $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ para $\overline{M}$, y para cada $\boldsymbol{v}_i$ consideramos una preimagen $\boldsymbol{u}_i \in M$, entonces $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ es una base minimal de M.
3. Conversamente, toda base minimal se proyecta en una base para $\overline{M}$.
4. Sean $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ y $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ dos bases minimales de M, tales que

$$\forall i \in \{1, \ldots, n\} \quad \boldsymbol{u}_i = \sum_{j=1}^{n} a_{ij}\boldsymbol{v}_j,$$

y sea $B := [a_{ij}]_{ij} \in \mathrm{Mat}_n(A)$. Entonces $\det(B) \in A^\times$ y B es inversible.

Teorema 6.47: Sea A un dominio y M un A-módulo finitamente generado. Si $f\colon M \to M$ es un homomorfismo de A-módulos suprayectivo, entonces también es inyectivo y, por ende, es un automorfismo.

Demostración: Fijemos a $f \in \mathrm{Hom}_A(M, M)$. En particular, podemos ver a M como un $A[x]$-módulo con la operación:

$$\left(\sum_{i=0}^{n} c_i x^i\right) \cdot \boldsymbol{m} = \sum_{i=0}^{n} c_i f^i(\boldsymbol{m}),$$

donde aquí f^i representa la composición i veces, y $f^0 := \mathrm{Id}$. Por hipótesis $(x) \cdot M = M$ y existe $p(x) = 1 + xq(x) \in A[x]$ tal que $(1 + x \cdot q(x))M = \{\vec{0}\}$. Sea $\boldsymbol{m} \in \ker f$, luego se tiene que

$$\vec{0} = \left(1 + \sum_{i=1}^{N} c_i x^i\right) \cdot \boldsymbol{m} = \boldsymbol{m} + \sum_{i=1}^{N} c_i f^i(\boldsymbol{m}) = \boldsymbol{m}. \qquad \square$$

Lema 6.48: Sea F un A-módulo que es una suma directa de módulos numerablemente generados. Si M es un sumando directo de F, entonces es también la suma directa de submódulos numerablemente generados.

Demostración: Sea $F = M \oplus N = \bigoplus_{\gamma<\kappa} E_\gamma$, donde cada E_γ es numerablemente generado. Queremos construir una familia $\{F_\alpha\}_{\alpha<\mu}$ con las siguientes propiedades:

1. Si $\alpha < \beta$, entonces $F_\alpha \subset F_\beta$.
2. $F = \bigcup_{\alpha<\mu} F_\alpha$.
3. $F_{\alpha+1}/F_\alpha$ es numerablemente generado.
4. $F_\alpha = M_\alpha \oplus N_\alpha$, donde $M_\alpha = M \cap F_\alpha$ y $N_\alpha = N \cap F_\alpha$.
5. Cada F_α es una suma directa de E_γ's.

La construcción es por recursión transfinita: Definimos $F_0 := (0)$ y si λ es un ordinal límite, entonces $F_\lambda = \bigcup_{\delta<\lambda} F_\delta$. Para el caso del sucesor, sea $E_\gamma \not\subseteq F_{\alpha+1}$ y $Q_1 := E_\gamma$. Sea $\{\boldsymbol{x}_{11}, \boldsymbol{x}_{12}, \boldsymbol{x}_{13}, \dots\}$ un sistema generador de Q_1. Tómese a $\boldsymbol{x}_{11} = \boldsymbol{m}_{11} + \boldsymbol{n}_{11}$ con $\boldsymbol{m}_{11} \in M$ y $\boldsymbol{n}_{11} \in N$, y definamos Q_2 como la mínima unión de E_γ's (que son finitos) tales que $\boldsymbol{m}_{11}, \boldsymbol{n}_{11} \in Q_2$. Sea $\{\boldsymbol{x}_{21}, \boldsymbol{x}_{22}, \dots\}$ un sistema generador de Q_2 y siga el mismo procedimiento, construyendo $\boldsymbol{x}_{ij}$. Finalmente definimos $F_{\alpha+1} := F_\alpha + \mathrm{Span}_A\{\boldsymbol{x}_{ij}\}$.

Nótese que

$$M = \bigcup_{\alpha<\mu} M_\alpha,$$

donde M_α es un sumando directo de $M_{\alpha+1}$. Más aún,

$$\frac{F_{\alpha+1}}{F_\alpha} = \frac{M_{\alpha+1}}{M_\alpha} \oplus \frac{N_{\alpha+1}}{N_\alpha},$$

donde $M_{\alpha+1}/M_\alpha$ es numerablemente generado. Luego $M_{\alpha+1} = M_\alpha \oplus \tilde{M}_\alpha$, donde $\tilde{M}_\alpha$ es numerablemente generado. Definiendo $M_\lambda = 0$ para λ ordinal límite, finalmente se cumple que

$$M = \bigcup_{\alpha<\mu} \tilde{M}_\alpha. \qquad \square$$

Lema 6.49: Sea A un dominio local, P un A-módulo proyectivo y $\boldsymbol{x} \in P$. Entonces existe un sumando directo de P que es libre y contiene a $\boldsymbol{x}$.

Demostración: Sea $F = P \oplus P'$ con F libre. Elijamos una base $\{\boldsymbol{y}_i\}_{i\in I}$ de F tal que la representación de $\boldsymbol{x}$ en la base posea la cantidad minimal de coeficientes no nulos. Sea $\boldsymbol{x} = a_1\boldsymbol{y}_1 + \cdots + a_n\boldsymbol{y}_n$ con $0 \neq a_i \in A$, entonces se cumple que

$$a_i \notin \sum_{\substack{j\in I\\ j\neq i}} Aa_j$$

(¿por qué?). Sea $\boldsymbol{y}_i = \boldsymbol{p}_i + \boldsymbol{q}_i$ con $\boldsymbol{p}_i \in P$ y $\boldsymbol{q}_i \in P'$, luego $\boldsymbol{x} = \sum_{i=1}^n a_i\boldsymbol{p}_i$. Cada $\boldsymbol{p}_i = \sum_{j=1}^n c_{ij}\boldsymbol{y}_j + \boldsymbol{s}_i$, donde $\boldsymbol{s}_i$ son sumas de otros elementos de la base, de modo que se tiene que

$$\boldsymbol{x} = \sum_{i=1}^n a_i\boldsymbol{y}_i = \sum_{i=1}^n a_i\boldsymbol{p}_i = \sum_{i=1}^n \left(\sum_{j=1}^n c_{ij}\boldsymbol{y}_j + \boldsymbol{s}_i\right).$$

Por lo que se concluye que necesariamente

$$a_i = \sum_{j=1}^n a_j c_{ji},$$

como no se pueden simplificar los a_i's (por construcción de la base), debe darse que $1 - c_{ii} \in \mathfrak{m}$ para todo $i = 1, \ldots, n$ y que $c_{ij} \in \mathfrak{m}$ para $i \neq j$. Luego sea $C := [c_{ij}]_{ij} \in \mathrm{Mat}_n(A)$. Nótese que $\det(C) \equiv 1 \pmod{\mathfrak{m}}$, luego $\det(C) \in A^\times$ y luego podemos reemplazar $\boldsymbol{y}_i$ con $\boldsymbol{p}_i$, para todo $i = 1, \ldots, n$. Luego $\boldsymbol{x} \in \sum_{i=1}^n A\boldsymbol{p}_i$ el cual es un sumando directo libre de P. □

Teorema 6.50: Sea $(A, \mathfrak{m})$ un dominio local. Entonces todo A-módulo proyectivo es libre.

Demostración: Sea M un A-módulo proyectivo. Lo veremos por casos:

(a) M es finitamente generado: Sea $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ una base minimal de M y sea F el A-módulo libre generado por $\{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n\}$. Sea $\varphi\colon F \to M$ que manda $\varphi(\boldsymbol{y}_i) = \boldsymbol{x}_i$, de modo que es un epimorfismo. Sea $K := \ker\varphi$. Por definición de base minimal, debe cumplirse que en K:

$$\varphi\left(\sum_{i=1}^n a_i\boldsymbol{x}_i\right) = \sum_{i=1}^n a_i\boldsymbol{x}_i = \vec{0},$$

con $a_i \in \mathfrak{m}$; por lo que $K \subseteq \mathfrak{m}F$. Como M es proyectivo, entonces existe $\psi\colon M \to F$ tal que $\psi \circ \varphi = \mathrm{Id}_M$ y, por lo tanto, $F = \psi[M] \oplus K$; luego $K = \mathfrak{m}K$, pero por el lema de Nakayama, $K = 0$, por lo que $M \cong F$.

(b) M es numerablemente generado: Sea $M = \mathrm{Span}_A\{\boldsymbol{m}_1, \boldsymbol{m}_2, \dots\}$. Luego por el lema anterior sea $\boldsymbol{m}_1 \in F_1$, donde $M = F_1 \oplus M_1$, F_1 es libre y M_1 es proyectivo numerablemente generado. Sea $\boldsymbol{m}_2'$ la componente de $\boldsymbol{m}_2$ en M_1 y sea $\boldsymbol{m}_2' \in F_2$, donde $M_1 = F_2 \oplus M_2$, F_2 es libre y M_2 es proyectivo numerablemente generado. Y así sucesivamente, finalmente se comprueba que

$$M = \bigoplus_{n=1}^{\infty} F_n.$$

(c) Caso general: Un A-módulo libre F es una suma directa de A's y un módulo proyectivo P es un sumando directo de un módulo libre, en consecuencia, es suma directa de submódulos numerablemente generados. Es claro que cada sumando directo de P es proyectivo, luego ellos son libres y la suma directa de módulos libres es libre. □

§6.1.5 Planitud. Para exponer mejor los resultados necesitamos del concepto de *álgebra*:

Definición 6.51: Dados A, B anillos, se dice que un homomorfismo de anillos $f\colon A \to B$ es una A-álgebra, o cuando no hay ambigüedad, que B es una A-álgebra.

En el capítulo 10 veremos éste concepto en más profundidad, pero ésto nos es suficiente. Naturalmente una A-álgebra B puede verse como un A-módulo con el producto escalar $a \cdot b := f(a)b$.

Proposición 6.52: 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 $N \otimes_B (B \otimes_A M) = N \otimes_A M$. □

Definición 6.53: 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 6.54: 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: □

Teorema 6.55: 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. 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 $a = 0$.

¿Por qué? Cf. **[18,** págs. 21-22].

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. □

6.2 Ideales asociados y descomposición primaria

Definición 6.56: Dado un A-módulo M, se dice que un ideal primo $\mathfrak{p} \lhd A$ está ***asociado*** a M, si existe $\boldsymbol{m} \in M_{\neq 0}$ tal que $\mathfrak{p} = \operatorname{Ann} \boldsymbol{m}$. El conjunto de los ideales asociados a M se denota $\operatorname{As}_A(M)$; obviamos el subíndice A de no haber ambigüedad sobre los signos. Dado un ideal $\mathfrak{a} \lhd A$, definimos $\operatorname{As}(\mathfrak{a}) := \operatorname{As}(A/\mathfrak{a})$. Decimos que $a \in A$ es un ***divisor de cero*** de M si existe $\boldsymbol{m} \in M_{\neq 0}$ tal que $a\boldsymbol{m} = \vec{0}$. Se dice que M es un ***módulo fiel*** si no posee divisores de cero además de $0 \in A$.

Proposición 6.57: Sea A un dominio noetheriano y M un A-módulo no nulo.

1. Todo $\operatorname{Ann}(\boldsymbol{x})$ con $\boldsymbol{x} \in M_{\neq 0}$ está contenido en algún ideal asociado a M.
2. Los divisores de cero de M son $\bigcup \operatorname{As}(M)$.

Demostración:

1. Definamos $\mathcal{F} := \{\operatorname{Ann}(\boldsymbol{x}) : \boldsymbol{x} \in M_{\neq 0}\}$. Nótese que toda cadena ascendente se estabiliza porque A es noetheriano, así que sólo basta ver que algún elemento $\subseteq$-maximal $\mathfrak{p} = \operatorname{Ann}(\boldsymbol{y})$ es un ideal primo. Para ello, sean $ab \in \mathfrak{p}$ con $b \notin \mathfrak{p}$, es decir, $ab\boldsymbol{y} = 0$, pero $b\boldsymbol{y} \neq 0$. Claramente $\operatorname{Ann}(\boldsymbol{y}) \subseteq \operatorname{Ann}(b\boldsymbol{y})$, luego se tiene igualdad por maximalidad, y luego $a \in \mathfrak{p}$.

2. Ejercicio para el lector. □

Teorema 6.58: Sea S un sistema multiplicativo de A sin divisores de cero y fijemos el monomorfismo $\iota\colon A \to S^{-1}A$.

1. Sea N un $S^{-1}A$-módulo (luego, también un A-módulo), entonces $\mathfrak{q} \in \mathrm{As}_{S^{-1}A}(N)$ syss $\mathfrak{q}^c = \mathfrak{q} \cap A \in \mathrm{As}_A(N)$.

2. Si A es noetheriano y M es un A-módulo, entonces $\mathfrak{p} \in \mathrm{As}_A(S^{-1}M)$ syss $\mathfrak{p} \in \mathrm{As}_A(M)$ y $\mathfrak{p} \cap S = \varnothing$.

Demostración:

1. Es claro que si $\mathfrak{q} \in \mathrm{As}_{S^{-1}A}(N)$ entonces $\mathfrak{q}^c = \mathfrak{q} \cap A \in \mathrm{As}_A(N)$. Recíprocamente si $\mathfrak{p} \in \mathrm{As}_A(N)$ con $\mathfrak{p} \cap S = \varnothing$ y $\mathfrak{p} = \mathrm{Ann}_A(\boldsymbol{x})$, entonces $\mathfrak{p}^e = \mathrm{Ann}_{S^{-1}A}(\boldsymbol{x})$ es un ideal primo.

2. Sea $\mathfrak{p} = \mathrm{Ann}(\boldsymbol{x})$ con $\mathfrak{p} \cap S = \varnothing$. $(a/s)x = 0$ con $\boldsymbol{x}/s \in S^{-1}M$ y $a \in A$ syss $t(a\boldsymbol{x} - s0) = ta\boldsymbol{x} = \vec{0}$ para algún $t \in S$. Como $t \notin \mathfrak{p}$, entonces necesariamente $a \in \mathfrak{p}$ y luego vemos que $\mathfrak{p}^e = \mathrm{Ann}_{S^{-1}A}(\boldsymbol{x}) \in \mathrm{As}_{S^{-1}A}(S^{-1}M)$ con lo que $\mathfrak{p} \in \mathrm{As}_A(S^{-1}M)$.

   Recíprocamente si $\mathfrak{q} = \mathrm{Ann}(\boldsymbol{x}/s) \in \mathrm{As}_{S^{-1}A}(S^{-1}M)$ y definimos $\mathfrak{p} := \mathfrak{q}^c$ (que satisface $\mathfrak{q} = \mathfrak{p}^e$). Como A es noetheriano, $\mathfrak{p}$ es finitamente generado, digamos $\mathfrak{p} = (a_1, \ldots, a_r)$, de modo que $t_i a_i \boldsymbol{x} = \vec{0}$ para ciertos $t_i \in S$, luego tomando el producto $t = t_1 \cdots t_r \in S$ vemos que $\mathfrak{p} = \mathrm{Ann}(t\boldsymbol{x}) \in \mathrm{As}_A(M)$. □

Corolario 6.59: Sea A un dominio noetheriano y M un A-módulo, entonces $\mathfrak{p} \in \mathrm{As}_A(M)$ syss $\mathfrak{p}^e = \mathfrak{p}A_{\mathfrak{p}} \in \mathrm{As}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$.

Teorema 6.60: Sean M_1, M_2, M_3 un trío de A-módulos.

1. Dada la sucesión exacta $0 \to M_1 \to M_2 \to M_3 \to 0$ se cumple que $\mathrm{As}(M_1) \subseteq \mathrm{As}(M_2) \subseteq \mathrm{As}(M_1) \cup \mathrm{As}(M_3)$.

2. En particular, si $M_2 = M_1 \oplus M_3$, entonces $\mathrm{As}(M_2) = \mathrm{As}(M_1) \cup \mathrm{As}(M_3)$.

Demostración:

1. Dado $\mathfrak{p} \in \mathrm{As}(M_2)$, entonces $\mathfrak{p} = \mathrm{Ann}(\boldsymbol{x})$ para algún $\boldsymbol{x} \in M_2$, luego es fácil notar que $N := \mathrm{Span}\{\boldsymbol{x}\} \cong A/\mathfrak{p}$ y, más aún, para todo $\boldsymbol{y} \in N_{\neq 0}$ podemos ver que $\mathrm{Ann}(\boldsymbol{y}) = \mathfrak{p}$. Mirando a $M_1 \subseteq M_3$, si $N \cap M_1 \neq \{\vec{0}\}$,

entonces tendríamos que $\mathfrak{p} \in \mathrm{As}(M_1)$. Por el contrario si $N \cap M_1 = \{\vec{0}\}$, entonces la imagen de N en M_3 es isomorfa a $N \cong A/\mathfrak{p}$ de modo que $\mathfrak{p} \in \mathrm{As}(M_3)$.

2. Basta aplicar el inciso anterior para concluir que $\mathrm{As}(M_1) \subseteq \mathrm{As}(M_2)$ y $\mathrm{As}(M_3) \subseteq \mathrm{As}(M_2)$. □

Corolario 6.61: Sea A un dominio noetheriano, M un A-módulo finitamente generado, entonces existe una cadena de submódulos $\{\vec{0}\} = M_0 \subset M_1 \subset \cdots \subset M_n = M$ tal que $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ donde cada $\mathfrak{p}_i \lhd A$ es un ideal primo.

Demostración: Definamos $M_0 = \{\vec{0}\}$ y dado $\mathfrak{p}_1 \in \mathrm{As}(M)$ elegimos M_1 tal que $M_1 = M_1/M_0 \cong A/\mathfrak{p}_1$. Luego dado $\mathfrak{p}_2 \in \mathrm{As}(M/M_1)$ elegimos M_2 tal que $M_2/M_1 \cong A/\mathfrak{p}_2$ y así procedemos recursivamente construyendo una cadena ascendente de submódulos, la cual se estabiliza pues M es un A-módulo noetheriano. □

Teorema 6.62: 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.

Demostración:

1. Basta emplear el corolario anterior para construir la cadena

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

y notar que induce la siguiente sucesión exacta de A-módulos:

$$0 \longrightarrow M_{n-1} \longrightarrow M \longrightarrow M/M_{n-1} = A/\mathfrak{p}_n \longrightarrow 0$$

de modo que $\mathrm{As}(M) \subseteq \mathrm{As}(M_{n-1}) \cup \mathrm{As}(A/\mathfrak{p}_n)$ donde $\mathrm{As}(A/\mathfrak{p}_n) = \{\mathfrak{p}_n\}$.

2. Si $\mathfrak{p} \in \mathrm{As}(M)$ entonces $0 \to A/\mathfrak{p} \to M$ es una sucesión exacta que induce la sucesión exacta $0 \to A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \to M_{\mathfrak{p}}$ es exacta y, por tanto, $M_{\mathfrak{p}} \neq 0$.

3. Por el inciso anterior basta probar que todo $\subseteq$-minimal de $\operatorname{Supp}(M)$ está en $\operatorname{As}(M)$. Sea $\mathfrak{p} \in \operatorname{Supp}(M)$ minimal, luego $M_{\mathfrak{p}} \neq 0$ y sabemos que $\operatorname{As}(M_{\mathfrak{p}}) \neq \varnothing$. Dado $\mathfrak{q} \in \operatorname{As}(M_{\mathfrak{p}})$ notamos que $\mathfrak{q} \setminus \mathfrak{p} = \varnothing$ (luego $\mathfrak{q} \subseteq \mathfrak{p}$) y $\mathfrak{q} \in \operatorname{As}(M)$, pero además $\mathfrak{q} \in \operatorname{Supp}(M)$ por lo que $\mathfrak{q} = \mathfrak{p}$. □

Definición 6.63: Dado un A-módulo M decimos que un submódulo $N \leq M$ es ***primario*** si para todo $a \in A$ y $\boldsymbol{m} \in M \setminus N$ con $a\boldsymbol{m} \in N$ se cumple que $a^n M \subseteq N$ para algún n. Equivalentemente, N es primario syss todo divisor de cero a de M/N es tal que $a \in \operatorname{Rad}\operatorname{Ann}(M/N)$. Un ideal $\mathfrak{q}$ se dice ***primario*** syss lo es como submódulo de A.

Se dice que un A-módulo M es ***coprimario*** si el submódulo 0 es primario, equivalentemente, M es coprimario syss los divisores de cero son $\operatorname{Rad}\operatorname{Ann}(M)$.

Así pues, N es un submódulo primario de M syss M/N es coprimario.

Teorema 6.64: Sea A un dominio noetheriano y M un A-módulo finitamente generado. Un submódulo $N \leq M$ es primario syss $\operatorname{As}(M/N)$ sólo posee un elemento $\mathfrak{p}$; en cuyo caso, el ideal $\mathfrak{a} := \operatorname{Ann}(M/N)$ es primario y $\operatorname{Rad}\mathfrak{a} = \mathfrak{p}$.

Demostración: $\Longleftarrow$. Si $\operatorname{As}(M/N) = \{\mathfrak{p}\}$, entonces los divisores de cero son exactamente los elementos de $\mathfrak{p}$. Es claro que $\operatorname{Rad}\operatorname{Ann}(M/N) \subseteq \mathfrak{p}$, bastaría ver la otra inclusión. Como M es finitamente generado, entonces M/N también y está generado digamos por $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r\}$ y luego, podemos notar que

$$\begin{aligned}\mathfrak{q} \in \operatorname{Supp}(M/N) &\iff (M/N)_{\mathfrak{q}} \neq 0 \iff \exists i : \boldsymbol{u}_i \neq 0 \in (M/N)_{\mathfrak{q}} \\ &\iff \exists i : \operatorname{Ann}(\boldsymbol{u}_i) \subseteq \mathfrak{q} \iff \operatorname{Ann}(M/N) = \bigcap_{i=1}^{r} \operatorname{Ann}(\boldsymbol{u}_i) \subseteq \mathfrak{q}.\end{aligned}$$

Y ahora recuerde que, por el inciso 3 del teorema anterior, que $\mathfrak{p} \in \operatorname{Supp}(M/N)$.

$\Longrightarrow$. Si N es primario y $\mathfrak{p} \in \operatorname{As}(M/N)$, entonces por la proposición 6.57 se tiene que si $a \in \mathfrak{p}$ entonces a es un divisor de cero de M/N, luego $a \in \operatorname{Rad}(\operatorname{Ann}(M/N)) = \operatorname{Rad}\mathfrak{a}$ (puesto que N es primario). De modo que $\mathfrak{p} \subseteq \operatorname{Rad}\mathfrak{a}$, pero además,

$$\operatorname{Rad}\mathfrak{a} = \bigcap \operatorname{As}(M/N) \subseteq \mathfrak{p},$$

de lo que se concluye la igualdad. □

Definición 6.65: Si $N \leq M$ es tal que $\mathfrak{p} = \operatorname{Rad}\operatorname{Ann}(M/N)$ es primo, entonces N se dice un submódulo $\mathfrak{p}$-***primario***. Similarmente, M se dice $\mathfrak{p}$-coprimario si 0 es $\mathfrak{p}$-primario.

Proposición 6.66: Si $\operatorname{Rad}\operatorname{Ann}(M)$ es maximal, entonces M es coprimario. En particular, las potencias de un ideal maximal $\mathfrak{m}$ son ideales $\mathfrak{m}$-primarios.

Proposición 6.67: En un anillo noetheriano, todo ideal contiene a alguna potencia de su radical.

Demostración: Sea $\mathfrak{a} \trianglelefteq A$ un ideal. Como A es noetheriano, su radical es finitamente generado, ergo $\operatorname{Rad}\mathfrak{a} = (x_1, \ldots, x_r)$ y por definición del radical, para todo $1 \leq i \leq r$ existe n_i tal que $x_i^{n_i} \in \mathfrak{a}$. Definamos:

$$m := 1 + \sum_{i=1}^{r}(n_i - 1),$$

luego nótese que $(\operatorname{Rad}\mathfrak{a})^m$ está generado por los productos $x_1^{\alpha_1} \cdots x_r^{\alpha_r}$ donde $\alpha_1 + \cdots + \alpha_r = m$; pero entonces debe haber algún $\alpha_i \geq n_i$, por lo que los generadores están en $\mathfrak{a}$ y en consecuencia $(\operatorname{Rad}\mathfrak{a})^m \subseteq \mathfrak{a}$. □

Corolario 6.68: En un anillo noetheriano el nilradical es nilpotente.

Corolario 6.69: 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 $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$.

Demostración: 1 $\iff$ 2. Proposición 6.66.
2 $\implies$ 3. Por la proposición anterior.
3 $\implies$ 2. Basta aplicar radicales a la desigualdad. □

Lema 6.70: Sean $N_1, \ldots, N_r$ submódulos $\mathfrak{p}$-primarios de M, entonces $\bigcap_{i=1}^{r} N_i$ es $\mathfrak{p}$-primario.

Demostración: Por inducción basta probarlo para $r = 2$. Por hipótesis, $M/N_1, M/N_2$ son $\mathfrak{p}$-coprimarios, luego $M/N_1 \oplus M/N_2$ también. Ahora bien, $M/(N_1 \cap N_2)$ está contenido en $M/N_1 \oplus M/N_2$, luego debe ser $\mathfrak{p}$-coprimario puesto que $\mathrm{As}(M/N_1 \oplus M/N_2) = \{\mathfrak{p}\}$. □

Definición 6.71: 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***.

Definición 6.72: Sea M un A-módulo y $M' \leq M$. Una ***descomposición*** de M' es una expresión:

$$M' = \bigcap_{i=1}^{r} N_i.$$

Dicha descomposición se dice ***irredundante*** si no podemos omitir ningún N_i. Una decomposición se dice ***irreducible*** (resp. ***primaria***) si todos los N_i's son submódulos irreducibles (resp. primarios) en M. Una descomposición primaria es ***minimal*** si todos los $\operatorname{Rad}\operatorname{Ann}(M/N_i)$'s son distintos.

Dada una descomposición primaria minimal de M':

$$M' = \bigcap_{i=1}^{r} N_i, \qquad \operatorname{Rad}\operatorname{Ann}(M/N_i) = \mathfrak{p}_i,$$

entonces N_i se dice la $\mathfrak{p}_i$***-componente primaria*** de M'. M' se dice ***descomposible*** si posee alguna descomposición primaria.

Es claro que toda descomposición de un módulo puede simplificarse a una descomposición irredundante. Por el lema anterior toda descomposición primaria se puede reducir a una descomposición minimal, de ahí dicho concepto.

Teorema 6.73: 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 $\operatorname{As}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

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.

Demostración:

1. Por contrarrecíproca sea N un submódulo que no es primario. Sustituyendo M por M/N podemos suponer que $N = 0$ y probar que es reducible. Por el teorema 6.64 se cumple que $\operatorname{As}(M)$ posee al menos dos elementos $\mathfrak{p}_1, \mathfrak{p}_2$, de modo que M posee dos submódulos K_1, K_2 isomorfos a $A/\mathfrak{p}_1, A/\mathfrak{p}_2$ resp., y claramente $K_1 \cap K_2 = 0$.

2. Como M es un módulo noetheriano, entonces es fácil ver que todo submódulo suyo se escribe como intersección de finitos submódulos irreducibles, los cuales son primarios y luego podemos simplificarla a una descomposición primaria minimal.

3. Nuevamente nos reducimos al caso $N = 0$. Como $N_1 \cap \cdots \cap N_r = 0$, podemos ver a M contenido en $(M/N_1) \oplus \cdots \oplus (M/N_r)$ y

$$\operatorname{As} M \subseteq \operatorname{As}\left(\bigoplus_{i=1}^{r} M/N_i\right) = \bigcup_{i=1}^{r} \operatorname{As}(M/N_i) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}.$$

Como la descomposición es irredundante tenemos que $N_2 \cap \cdots \cap N_r \neq 0$ y luego existe $\boldsymbol{x} \in N_2 \cap \cdots \cap N_r$ no nulo. Luego $\operatorname{Ann} \boldsymbol{x} = (0 : \boldsymbol{x}) = (N_1 : \boldsymbol{x})$ y $(N_1 : M)$ es un ideal primario contenido en $\mathfrak{p}_1$, de modo que $\mathfrak{p}_1^n M \subseteq N_1$ para algún n y luego $\mathfrak{p}_1^n \boldsymbol{x} = 0$ para algún n. Elijamos dicho n tal que $\mathfrak{p}_1^n \boldsymbol{x} \neq 0$ y $\mathfrak{p}_1^{n+1} \boldsymbol{x} = 0$, y elijamos algún $\boldsymbol{y} \in \mathfrak{p}_1^n \boldsymbol{x}$ no nulo, de modo que $\mathfrak{p}_1 \boldsymbol{y} = 0$. Nótese que $\boldsymbol{y} \in N_2 \cup \cdots \cup N_r$ de modo que $\boldsymbol{y} \notin N_1$ y $\operatorname{Ann} \boldsymbol{y} \subseteq \mathfrak{p}_1$, por lo que $\operatorname{Ann} \boldsymbol{y} = \mathfrak{p}_1$ y se concluye que $\mathfrak{p}_1 \in \operatorname{As} M$. Así concluimos que $\operatorname{As} M = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

4. Sea $N = N_1 \cap \cdots \cap N_r$ una descomposición primaria minimal y sea $\mathfrak{p} := \operatorname{Rad} \operatorname{Ann}(M/N_1)$. Es fácil comprobar que

$$N_{\mathfrak{p}} = (N_1)_{\mathfrak{p}} \cap \cdots \cap (N_r)_{\mathfrak{p}}.$$

Ahora bien, como para todo i existe un $m > 0$ tal que $\mathfrak{p}_i^m \subseteq \operatorname{Ann}(M/N_i)$ y como $\mathfrak{p}_i \not\subseteq \mathfrak{p}$ para $i \neq 1$, vemos que $(M/N_i)_{\mathfrak{p}} = 0$, o equivalentemente, $(N_i)_{\mathfrak{p}} = M_{\mathfrak{p}}$ por lo que $N_{\mathfrak{p}} = (N_1)_{\mathfrak{p}}$ y de aquí es fácil concluir. □

Corolario 6.74: Un anillo noetheriano reducido A es tal que su anillo de fracciones totales K es un producto directo de finitos cuerpos.

Demostración: Sea D el conjunto de divisores de cero de A, entonces $K = S^{-1}A$ donde $S := A \setminus D$. Por la proposición 6.57, se cumple que $D = \bigcup \mathrm{As}(A)$ y $\mathrm{As}(A) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ es finito por el teorema 6.62. □

Probar que noetheriano reducido es producto de cuerpos.

Definición 6.75: Una familia $\mathcal{F}$ de ideales primos asociados a $\mathfrak{a}$ se dice ***aislada*** si para todo $\mathfrak{q}$ primo asociado a $\mathfrak{a}$ tal que $\mathfrak{q} \subseteq \mathfrak{p}$ para algún $\mathfrak{p} \in \mathcal{F}$ se cumple que $\mathfrak{q} \in \mathcal{F}$.

Teorema 6.76: 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.

Demostración: Definamos $S := A \setminus \bigcup_{j=1}^{m} \mathfrak{p}_{i_j}$ y nótese que es un sistema multiplicativo. Más aún, sea $\mathfrak{p}$ un ideal primo asociado a $\mathfrak{a}$: Si $\mathfrak{p} \in \mathcal{F}$, entonces por definición se cumple que $\mathfrak{p} \cap S = \varnothing$. Si $\mathfrak{p} \notin \mathcal{F}$, entonces $\mathfrak{p} \not\subseteq \bigcup_{j=1}^{m} \mathfrak{p}_{i_j}$ por la proposición 2.58, por lo que $\mathfrak{p} \cap S \neq \varnothing$.

Finalmente basta aplicar el resultado anterior para obtener el enunciado. □

6.3 Módulos noetherianos y artinianos, de nuevo

Teorema 6.77: 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).

Demostración: Falta probar $\Longrightarrow$: En primer lugar construyamos la siguiente aplicación:

$$\begin{aligned} \Phi\colon \{T : T \leq M\} &\longrightarrow \{L : L \neq N\} \times \{S : S \leq M/N\} \\ T &\longmapsto \left(T \cap N, \frac{T+N}{N}\right) \end{aligned}$$

Sean $E \leq T \leq M$ tales que $\Phi(E) = \Phi(T)$, queremos probar que si eso ocurre entonces $E = T$: Basta notar que si $\boldsymbol{x} \in T \setminus E$, entonces como $E \cap N = T \cap N$ se ha de cumplir que $\boldsymbol{x} \notin N$ y luego $[\boldsymbol{x}] \neq [\boldsymbol{y}]$ para todo $\boldsymbol{y} \in E$, puesto que de lo contrario $\boldsymbol{x} - \boldsymbol{y} = \boldsymbol{n} \in N$, pero entonces $\boldsymbol{n} \in T \cap N = E \cap N$, por lo que $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{n} \in E$; lo que es absurdo.

Luego sea

$$E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots$$

una cadena de submódulos de M. Nótese que $E_i \cap N$ es una cadena de submódulos de N y que $(E_i + N)/N$ es una cadena de submódulos de M/N, luego ambas se estabilizan digamos en un n suficientemente grande. Pero empleando la proposición 6.9, ésto implica que los E_i's también se estabilizan desde dicho n; luego M es noetheriano. □

Corolario 6.78: La suma directa de A-módulos noetherianos (resp. artinianos) es también noetheriano (resp. artiniano).

Reescribiendo el último teorema en lenguaje de sucesiones exactas:

Proposición 6.79: Si $0 \longrightarrow N \longrightarrow M \longrightarrow T \longrightarrow 0$ es una sucesión exacta de A-módulos, entonces M es noetheriano (resp. artiniano) syss N, T lo son.

Corolario 6.80: Sea $M = \bigoplus_{i=1}^{n} M_i$ un A-módulo. Entonces M es noetheriano (resp. artiniano) syss cada M_i lo es.

Demostración: Basta considerar la siguiente sucesión exacta y aplicar inducción:

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0 \qquad \square$$

Teorema 6.81: Sea M un A-módulo noetheriano. Entonces $\bar{A} := A/\operatorname{Ann}(M)$ es un anillo noetheriano. En particular, si M es fiel, entonces A es noetheriano.

Demostración: Basta probar el caso en que $\operatorname{Ann}(M) = 0$ (¿por qué?). Como M es noetheriano, entonces es finitamente generado y podemos escribir $M = A \cdot \boldsymbol{m}_1 + \cdots + A \cdot \boldsymbol{m}_n$. Luego podemos considerar el morfismo $a \mapsto (a\boldsymbol{m}_1, \ldots, a\boldsymbol{m}_n)$ desde A hasta M^n, y notar que su imagen es un submódulo de M^n. Pero $M^n = \bigoplus_{i=1}^{n} M$ es noetheriano, luego A lo es. □

Uno de los resultados más importantes que vimos era el teorema de las bases de Hilbert, el cual dice que $A[x_1, \ldots, x_n]$ es noetheriano si A lo es. Podemos sacar la siguiente consecuencia:

Proposición 6.82: Se cumplen:

1. Si A es noetheriano y B es una A-álgebra de tipo finito, entonces B es noetheriano.
2. Si A es noetheriano (resp. artiniano), entonces todo A-módulo finitamente generado también es noetheriano (resp. artiniano).

Teorema (AE) 6.83 (Formanek): Sea A un dominio y M un A-módulo fiel finitamente generado. Si todos los submódulos de M de la forma $\mathfrak{a}M$, con $\mathfrak{a} \trianglelefteq A$, satisfacen la condición de la cadena ascendente; entonces A es noetheriano.

Demostración: Por el teorema anterior, basta notar que M es noetheriano. Procedemos por contradicción: si M no lo fuese, entonces considere la familia de submódulos:

$$\mathcal{F} := \{\mathfrak{a}M : \mathfrak{a} \triangleleft A,\ M/\mathfrak{a}M \text{ no es noetheriano}\}$$

luego $\{\vec{0}\} \in \mathcal{F}$, así que no es vacío y por hipótesis posee un elemento maximal $\mathfrak{a}M$. Sustituyendo M por $M/\mathfrak{a}M$ y A por $A/\operatorname{Ann}(M/\mathfrak{a}M)$, podemos asumir que M no es noetheriano, pero que todos los módulos de la forma $M/\mathfrak{a}M$ con $\mathfrak{a} \neq (0)$ si lo son.

Sea

$$\mathcal{G} := \{N : N < M, M/N \text{ es fiel sobre } A\},$$

nótese que $\{\vec{0}\} \in \mathcal{G}$, y que se satisface que si $M = \operatorname{Span}_A\{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_n\}$

$$N \in \mathcal{G} \iff \forall a \in A_{\neq 0}\{a\boldsymbol{m}_1, \ldots, a\boldsymbol{m}_n\} \not\subseteq N.$$

Luego, aplicando el lema de Zorn, $\mathcal{G}$ posee un elemento maximal N_0. Si M/N_0 fuese noetheriano, entonces A lo sería y en consecuente M también, lo que es absurdo. Así pues $\bar{M} := M/N_0$ posee las siguientes propiedades:

1. $\bar{M}$ no es noetheriano.
2. Para todo $\mathfrak{a} \neq (0)$ ideal de A se cumple que $\bar{M}/\mathfrak{a}\bar{M}$ sí es noetheriano.
3. Para todo $N \neq (0)$ submódulo, $\bar{M}/N$ no es fiel.

Sea N un submódulo arbitrario de $\bar{M}$. Como $\bar{M}/N$ no es fiel, existe $a \in A_{\neq 0}$ tal que $a \cdot \bar{M}/N = 0$, es decir, $a\bar{M} \subseteq N$. Por la propiedad 2, $\bar{M}/(a)\bar{M}$ es noetheriano, luego $N/(a)\bar{M}$ es finitamente generado. Como $\bar{M}$ es finitamente generado y $(a)\bar{M}$ también, entonces N es finitamente generado; luego $\bar{M}$ es noetheriano, lo que es absurdo. □

Como corolario:

Teorema (AE) 6.84 (Eakin-Nagata): Sea B un dominio noetheriano y A un subanillo de B, tal que B es un A-módulo finitamente generado. Entonces A es noetheriano.

Proposición 6.85: Un dominio artiniano A sólo posee finitos ideales maximales.

Demostración: Considere la familia de las intersecciones finitas de los ideales maximales de A. Como A es artiniano, hay un elemento $\subseteq$-minimal $\mathfrak{a} := \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. Sea $\mathfrak{m}$ otro ideal maximal de A, si $\mathfrak{m} \neq \mathfrak{m}_i$ para todo i es porque existe $a_i \in \mathfrak{m}_i \setminus \mathfrak{m}$ y luego se cumple que $a_1 \cdots a_n \in \mathfrak{a} \setminus \mathfrak{m}$ (pues $\mathfrak{m}$ es primo), luego $\mathfrak{a} \cap \mathfrak{m} \subset \mathfrak{a}$ lo cual es absurdo. □

Proposición 6.86: Todo dominio íntegro artiniano es un cuerpo.

Demostración: Sea $x \in D$ y no es inversible, entonces la siguiente cadena de ideales no posee $\subseteq$-minimal:

$$(x) \supset (x^2) \supset (x^3) \supset \cdots$$ □

Corolario 6.87: En un anillo artiniano, todo ideal primo es maximal.

Corolario 6.88: En un anillo artiniano, el nilradical es igual al radical de Jacobson.

Teorema 6.89 – *Teorema de Akizuki*: Todo dominio noetheriano es artiniano.

Demostración: Procedemos por contradicción: Supongamos que existe un dominio artiniano A que no sea noetheriano. Necesariamente A debe ser infinito y debe poseer ideales infinitamente generados, luego podemos elegir $\mathfrak{a}$ un ideal $\subseteq$-minimal entre la familia de los infinitamente generados (puesto que A es artiniano). Nótese que $\mathfrak{a}$ satisface que todo ideal propio contenido en $\mathfrak{a}$ es finitamente generado.

Luego, veamos que para todo $r \in A$ se cumple que $r\mathfrak{a} = 0$ ó $r\mathfrak{a} = \mathfrak{a}$: Si $r\mathfrak{a} \neq \mathfrak{a}$, entonces consideremos el epimorfismo $\varphi\colon x \mapsto rx$, del cual concluimos

que como $r\mathfrak{a}$ es finitamente generado y

$$\frac{\mathfrak{a}}{\ker\varphi} \cong r\mathfrak{a},$$

entonces $\ker\varphi \subseteq \mathfrak{a}$ es un ideal infinitamente generado y, en consecuencia, $\ker\varphi = \mathfrak{a}$.

Sea $\mathfrak{p} := \operatorname{Ann}(\mathfrak{a})$. Nótese que si $r, s \notin \mathfrak{p}$, ha de ser porque $r\mathfrak{a} = s\mathfrak{a} = \mathfrak{a}$; luego $rs\mathfrak{a} = \mathfrak{a}$ y $rs \notin \mathfrak{p}$; en consecuencia, $\mathfrak{p}$ es un ideal primo. Por lo tanto, $k := A/\mathfrak{p}$ es un dominio íntegro artiniano, y por la proposición anterior, es un cuerpo.

Nótese que $\mathfrak{a}$ es un k-espacio vectorial con el producto escalar $[r]\cdot x = rx$ el cual está bien definido. Como $\mathfrak{a}$ no está finitamente generado en A, y todos sus ideales propios sí, entonces $\mathfrak{a}$ es un k-espacio vectorial artiniano de dimensión infinita; lo cual es absurdo. □

Ejemplo 8: Sea $p \in \mathbb{Z}$ primo, y definamos $C(p^\infty) := \{\mathbb{Z} + \frac{a}{p^n} : a \in \mathbb{Z}, n \in \mathbb{N}\}$. Claramente $C(p^\infty)$ es un grupo abeliano, pero lo convertiremos en un anillo conmutativo definiendo que $xy = 0$ para todo $x, y \in C(p^\infty)$; nótese que de éste modo no es un anillo unitario y todos sus elementos son divisores de cero. Más aún, de éste modo todo subanillo es simplemente un subgrupo, y también es un ideal.

Nótese que todo ideal propio de $C(p^\infty)$ es simplemente un subgrupo finito, de modo que es un anillo artiniano. Pero no es noetheriano puesto que la siguiente cadena no posee $\subseteq$-maximal:

$$\langle p^{-1}\rangle \subset \langle p^{-2}\rangle \subset \langle p^{-3}\rangle \subset \cdots$$

Nótese que el ejemplo anterior es válido puesto que $C(p^\infty)$ no es unitario, luego no es un dominio. El caso no conmutativo aparece bajo el nombre del teorema de Hopkins-Levitzki.

Definición 6.90: En un dominio noetheriano A, se denota por $n := k.\dim A$ al supremo n tal que

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n \subset A$$

es una cadena de ideales primos. A $k.\dim A$ se le dice la ***dimensión de Krull*** del anillo.

Ejemplo. La dimensión de Krull puede pensarse como una medida de complejidad del anillo.

- Un anillo A tiene dimensión 0 syss todo ideal primo es maximal.
- Si A es un cuerpo, entonces $k.\dim A = 0$.
- Si A es un DIP, entonces $k.\dim A = 1$ si A es íntegro y $k.\dim A = 0$ si no (demuéstrelo empleando que todo DIP es un DFU).
- En particular, si $A = k[x]$, un anillo de polinomios, se cumple que $k.\dim A = 1$. También $k.\dim \mathbb{Z} = 1$.
- Es fácil notar que $k.\dim(k[x_1, \ldots, x_n]) \geq n$, pero no es tan fácil establecer igualdad.

Proposición (AEN) 6.91: 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.

Demostración: Definamos por recursión $\mathfrak{a}_0 := A$ y $\mathfrak{a}_{i+1} := \mathfrak{a}_i \cdot \mathfrak{m}_i$, entonces se tiene la siguiente cadena de ideales:

$$\mathfrak{a}_0 = A \supset \mathfrak{a}_1 = \mathfrak{m}_1 \supseteq \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n = (0).$$

Además $\mathfrak{a}_i/\mathfrak{a}_{i+1} = \mathfrak{a}_i/(\mathfrak{a}_i \cdot \mathfrak{m}_i)$ es un $A/\mathfrak{m}_i$-espacio vectorial (¿por qué?), luego los cocientes son noetherianos syss son artinianos. Luego empleando inducción, recordando que $\mathfrak{a}_{n-1}/\mathfrak{a}_n = \mathfrak{a}_{n-1}$ y empleando el teorema 6.77 se concluye el enunciado. □

Ahora podemos mejorar el teorema de Akizuki:

Teorema 6.92: Un dominio A es artiniano syss es noetheriano y tiene dimensión 0.

Demostración: $\Longrightarrow$. Por el teorema de Akizuki, A es noetheriano y como todo ideal primo es maximal, entonces $k.\dim A = 0$.

$\Longleftarrow$. Como el ideal nulo es decomposible, entonces A posee finitos ideales primos, los cuales son maximales. Luego $\mathfrak{N}(A) = \mathfrak{m}_1 \cdots \mathfrak{m}_k$ y ya vimos que en un anillo noetheriano, el nilradical es nilpotente, por lo que $\mathfrak{N}(A)^n = \mathfrak{m}_1^n \cdots \mathfrak{m}_k^n = (0)$, por lo que concluimos por el corolario 6.91. □

Corolario 6.93: Sea $(A, \mathfrak{m})$ un dominio noetheriano local, entonces sólo una de las siguientes se cumple:

1. Para todo $n \in \mathbb{N}$ se da que $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$.

2. $\mathfrak{m}$ es nilpotente, en cuyo caso A es artiniano.

Demostración: Si no se cumple 1, entonces como $\mathfrak{J}(A) = \mathfrak{m}$ aplicamos el lema de Nakayama para concluir que $\mathfrak{m}$ es nilpotente, y por el teorema anterior, se concluye que A es artiniano. □

Teorema 6.94: Todo dominio artiniano se escribe de forma única (salvo isomorfismo) como producto directo de finitos anillos artinianos locales.

Demostración: En todo dominio artiniano A se puede escribir $(0) = \prod_{i=1}^{k} \mathfrak{m}_i^{n_i}$, donde cada $\mathfrak{m}_i$ es maximal y distinto. Como todos los factores son coprimos (puesto que sus radicales lo son, por la proposición 6.32), entonces por el teorema chino del resto se cumple que $\bigcap_{i=1}^{k} \mathfrak{m}_i^{n_i} = \prod_{i=1}^{k} \mathfrak{m}_i^{n_i}$ y por ende $A \to \prod_{i=1}^{k} (A/\mathfrak{m}_i^{n_i})$ es un isomorfismo.

Ahora veamos la unicidad, supongamos que existe $\psi \colon A \to \prod_{i=1}^{n} A_i$ un isomorfismo, entonces definamos $\phi_i := \psi \circ \pi_j \colon A \to A_j$, y sea $\mathfrak{a}_i := \ker(\phi_i)$. Por el teorema chino del resto, los $\mathfrak{a}_i$'s son coprimos dos a dos y $\bigcap_{i=1}^{n} \mathfrak{a}_i = (0)$. Sea $\mathfrak{q}_i$ el único ideal maximal de A_i, luego sea $\mathfrak{p}_i$ su contracción, el cual es un ideal primo y por ende maximal. Como $\mathfrak{q}_i$ es nilpotente (por ser el radical de Jacobson en un artiniano), entonces $\mathfrak{a}_i$ es $\mathfrak{p}_i$-primario. Como los $\mathfrak{a}_i$'s son coprimos, entonces los $\mathfrak{p}_i$'s lo son, luego los $\mathfrak{a}_i$'s son únicos por el teorema 6.76, por lo que los $A_i \cong A/\mathfrak{a}_i$'s también lo son. □

Corolario 6.95: Todo dominio artiniano reducido se escribe de forma única como producto directo de finitos cuerpos.

Proposición 6.96: Sea $(A, \mathfrak{m}, k)$ un dominio artiniano local. Son equivalentes:

1. A es un DIP.

2. $\mathfrak{m}$ es principal.

3. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

Demostración: $1 \implies 2 \implies 3$. Trivial.

$3 \implies 1$. Si $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$, entonces $\mathfrak{m} = \mathfrak{m}^2$ y por el lema de Nakayama se concluye que $\mathfrak{m} = (0)$.

Si $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, entonces $\mathfrak{m}$ es principal, también por el lema de Nakayama. Sea $\mathfrak{a} \trianglelefteq A$ un ideal impropio, luego como $\mathfrak{m}$ es maximal y nilpotente, entonces existe n tal que $\mathfrak{a} \subseteq \mathfrak{m}^n$ y $\mathfrak{a} \nsubseteq \mathfrak{m}^{n+1}$, luego podemos elegir $y \in \mathfrak{a} \setminus \mathfrak{m}^{n+1}$ tal que $y = ax^n$ con $a \notin \mathfrak{m}$, es decir, a es inversible, luego $x^n \in \mathfrak{a}$ y $(x^n) = \mathfrak{m}^n \subseteq \mathfrak{a}$. Finalmente $\mathfrak{a} = (x^n)$. □

En la demostración anterior hemos visto algo mucho más fuerte, en un dominio artiniano local todo ideal es una potencia del maximal.

Notas históricas

Los anillos locales tomaron un lugar protagónico en el álgebra conmutativa tras la publicación de Krull [**45**] (1938). La tecnica de *localización* fue introducida por Grell [**41**] (1927), un estudiante de E. Noether, y fue generalizado para dominios (anillos conmutativos unitarios) por Chevalley [**35**] (1944). El nombre *anillo local* nace de la *localización* en geometría algebraica, en donde dado un anillo $\mathcal{O}(X)$, cuyos elementos se conocen como «secciones globales», estudiamos la naturaleza de las secciones localmente en torno a un punto P, lo que resulta en el anillo $\mathcal{O}_{P,X}$ que efectivamente es un anillo local. Los elementos de $\mathcal{O}_{P,X}$ se dicen «secciones (o gérmenes) locales» y, de hecho, todas las localizaciones de $\mathcal{O}(X)$ coinciden con los $\mathcal{O}_{P,X}$ cuando P recorre todos los puntos de X.

La técnica de descomposición primaria fue originalmente descubierta por Lasker [**0**] (1905) para cierto tipo de anillos (afínes y de series de potencias) empleando teoría de la eliminación. La teoría fue reescrita por Noether [**48**] (1921), artículo en el cual lo demuestra en el caso general de anillos noetherianos siguiendo las mismas técnicas que nosotros empleamos.

7

Cuerpos formalmente reales y cuadrados

Comenzamos el capítulo con la observación de que la prueba del teorema fundamental del álgebra dada en 4.62 sólo requiere de un par de condiciones básicas sobre la existencia de un orden en el cuerpo. El objetivo del capítulo es llevar las cosas más lejos: no sólo buscamos caracterizar a $\mathbb{R}$ algebraicamente, sino que, en el proceso, buscamos también contestar a uno de los problemas de Hilbert y entender la estrecha relación entre positividad y la suma de cuadrados.

7.1 Cuerpos formalmente reales

Definición 7.1: Sea R un cuerpo. Se dice que $(R, \leq)$ es *ordenado* si:

CO1. Si $a \leq c$ y $b \leq d$, entonces $a + b \leq c + d$.

CO2. Si $a \leq b$, entonces $-a \geq -b$.

CO3. Si $a, b > 0$, entonces $a \cdot b > 0$.

En cuyo caso, los elementos de P se dicen *estrictamente positivos*. Si existe un conjunto $P \subseteq R$ con éstas características, entonces decimos que R es ordenable.

Un cuerpo R se dice *formalmente real* si el -1 no puede escribirse

como suma de cuadrados, i.e., si no existen $a_1, \ldots, a_n \in R$ tales que

$$-1 = a_1^2 + \cdots + a_n^2.$$

Inmediatamente se confirman las dos siguientes:

Teorema 7.2: Los cuerpos ordenados tienen característica 0.

Proposición 7.3: Todo cuerpo ordenado es formalmente real.

Más adelante veremos el recíproco a la última.

Ahora, cabe destacar que la noción de cuerpo ordenado es *frágil* en el sentido de que pueden existir múltiples ordenes válidos con los axiomas. Por ejemplo, considera a $R := \mathbb{Q}(\sqrt{2})$: R puede considerarse como ordenado si lo es con el orden usual como subcuerpo de $\mathbb{R}$, pero también podemos definir $a \leq * b$ como $\sigma(a) \leq \sigma(b)$, donde σ es la conjugación, y notamos que éste también es un orden válido en el cual $\sqrt{2} <^* 0$.

Definición 7.4: Sea R un cuerpo arbitrario. Un *cono positivo* P es un subconjunto $P \subseteq R$ que satisface:

CP1. Si $a, b \in P$, entonces $a + b, ab \in P$.

CP2. Si $N := \{-a : a \in P\}$, entonces $P \cup N = \mathbb{R}$ y $P \cap N = \{0\}$.

Por otro lado, un *precono positivo* P es un subconjunto $P \subseteq R$ que satisface:

PCP1. Si $a, b \in P$, entonces $a + b, ab \in P$.

PCP2. Si $a \in R$, entonces $a^2 \in P$.

PCP3. $-1 \notin P$.

Proposición 7.5: Sea R un cuerpo.

1. R es ordenado syss posee un cono positivo.

2. Todo cono positivo es un precono positivo.

Teorema (AE) 7.6: Si R es un cuerpo, entonces todo precono positivo puede extenderse a un cono positivo.

Demostración: Sea P_0 un precono positivo, entonces por el lema de Zorn podemos definir P como el precono positivo $\subseteq$-maximal que contiene a P_0 y veamos que es efectivamente un cono positivo. La propiedad CP1 se hereda de la propiedad PCP1.

Sea $x \in R$, veamos que $xP \cap (1+P) = \varnothing$ o $(-x)P \cap (1+P) = \varnothing$: De lo contrario, existirían $a, b, c, d \in P$ tales que

$$ax = 1 + b, \qquad -cx = 1 + d,$$
$$-acx^2 = 1 + b + d + bd,$$

de modo que reordenando $-1 = acx^2 + b + d + bd \in P$ lo que es absurdo.

Así pues, supongamos sin perdida de generalidad que $xP \cap (1+P) = \varnothing$ y definamos

$$Q := P - xP = \{a - bx : a, b \in P\}.$$

Nótese que para todo $a \in P$ se cumple que $a - 0x = a \in Q$. Veamos también que Q satisface los axiomas de un precono positivo: sean $\alpha = a - bx$ y $\beta = c - dx$ elementos de Q, entonces:

1. $\alpha + \beta = (a + c) - (b + d)x \in Q$ y $\alpha\beta = (ac + bdx^2) - (bc + ad)x \in Q$.
2. Si $a \in R$, entonces $a^2 \in P \subseteq Q$.
3. Si $-1 = \alpha$, entonces $bx = 1 + a \in xP \cap (1+P) = \varnothing$, lo que sería absurdo.

Luego, como P es maximal, entonces $P = Q$, y entonces $-x = 0 - 1x \in P$.

Análogamente si $(-x)P \cap (1+P) = \varnothing$ se obtiene que necesariamente $x \in P$. Con lo que hemos probado que $P \cup (-P) = R$.

Finalmente, supongamos que $a \in P \cap (-P)$ es no nulo. Entonces $a, -a \in P$. Por la propiedad anterior $1/a \in P \cup (-P)$, luego $\pm 1/a \in P$, pero entonces $-1 = (\mp a) \cdot (\pm 1/a) \in P$ lo que sería absurdo. □

Definición 7.7: Sea k un cuerpo arbitrario, entonces definamos S_k como el conjunto de todas las posibles sumas de cuadrados en k.

Nótese que S_k es potencialmente un precono positivo, pero puede fallar en satisfacer la propiedad PCP3. Más aún, de existir un precono positivo, entonces contiene a S_k.

Proposición 7.8: Sea k un cuerpo arbitrario. Entonces:

1. Todo precono positivo contiene a S_k.
2. S_k es cerrado bajo adición.
3. $S_k \setminus \{0\}$ es un subgrupo multiplicativo de $k^\times$.

Demostración: Es fácil notar que $S_k \setminus \{0\}$ es cerrado bajo productos, por lo que sólo basta comprobar que hay inversos. Sean $a_1, \ldots, a_n \in k$ no todos nulos. Entonces:

$$\frac{1}{a_1^2 + \cdots + a_m^2} = \frac{a_1^2 + \cdots + a_m^2}{(a_1^2 + \cdots + a_m^2)^2} = \sum_{i=1}^{m} \left(\frac{a_i}{a_1^2 + \cdots + a_m^2} \right)^2. \qquad \square$$

Teorema (AE) 7.9: Sea R un cuerpo. Son equivalentes:

1. R es ordenado.
2. R es formalmente real.
3. No todo elemento es suma de cuadrados y $\operatorname{car} R \neq 2$.
4. $a_1^2 + \cdots + a_n^2 = 0$ syss $a_j = 0$ para todo j.

Demostración: Claramente hemos visto que $1 \implies 2 \implies 3$, y es fácil comprobar $4 \implies 2$.

$2 \implies 1$. Basta aplicar el teorema anterior.

$3 \implies 2$. Lo probaremos por contrarrecíproca: Si $-1 \in S_R$ y $a \in R$ es arbitrario, entonces $4a = (1+a)^2 + (-1) \cdot (1-a)^2 \in S_R$, y claramente $1/4 = (1/2)^2 \in S_R$, de modo que $a \in S_R$ como se quería probar.

$2 \implies 4$. Sean a_j todos no nulos tales que $a_1^2 + \cdots + a_n^2 = 0$. Luego $n \geq 2$ y podemos notar que $-a_n^2 \in S_R \setminus \{0\}$ y empleando que $S_R \setminus \{0\}$ es subgrupo multiplicativo se concluye que $-1 \in S_R \setminus \{0\}$. $\square$

Definición 7.10: Un cuerpo R se dice *realmente cerrado* si toda extensión algebraica K/R con $K \neq R$ no es formalmente real.

Teorema (AE) 7.11: Si R es formalmente real, entonces posee una extensión algebraica K que es realmente cerrada.

Aquí estaríamos tentados a decir que esta clase de extensiones se llaman *clausuras reales* pero aún falta probar unicidad.

Teorema 7.12: Sea R un cuerpo realmente cerrado. Entonces:

1. Para todo $a \in R$ existe $b \in R$ tal que $a = \pm b^2$.
2. R sólo posee un ordenamiento posible, o equivalentemente, sólo posee un cono positivo.
3. Todos los automorfismos de R son aplicaciones crecientes.[1]

Demostración:

1. Supongamos que existe $a \in R$ tal que a no es un cuadrado. Entonces $K := R(\sqrt{a})$ es una extensión algebraica propia de R, de modo que no es formalmente real. Luego $-1 = \gamma_1^2 + \cdots + \gamma_n^2$ con $\gamma_j = b_j + c_j\sqrt{a} \in K$. Expandiendo nos queda que

$$-1 = \sum_{j=1}^{n} b_j^2 + a\left(\sum_{j=1}^{n} c_j^2\right) + 2\left(\sum_{i=1}^{n} b_j c_j\right)\sqrt{a}.$$

   Analizando las coordenadas de K como R-espacio vectorial, y reordenando, nos queda que

$$1 + \sum_{j=1}^{n} b_j^2 + a\left(\sum_{j=1}^{n} c_j^2\right) = 0 \iff -a = \frac{1 + \sum_{j=1}^{n} b_j^2}{\sum_{j=1}^{n} c_j^2}.$$

   De la última igualdad nos queda que $-a \in S_R$ (por ser grupo con la multiplicación).

   Si $-a$ tampoco fuese un cuadrado, entonces, repitiendo el argumento, obtendríamos que $a \in S_R$ lo que es absurdo. Luego $-a$ sí debe ser un cuadrado, que es lo que se quería probar.

2. Basta probar que S_R es un cono positivo, para lo cual basta notar que el inciso anterior demuestra CP2.

3. Como todo automorfismo de R manda cuadrados en cuadrados, entonces, por la anterior, preserva positividad. Más aún, si $a \leq b$, entonces $b - a \geq 0$ y $b - a = c^2$, de modo que $\sigma(b) = \sigma(a) + \sigma(c)^2 \geq \sigma(a)$. □

Ahora nos proponemos a clasificar a los cuerpos realmente cerrados.

[1] Se suele emplear el término «orden-isomorfismo», pero creo que «creciente» es más visual fuera del contexto de conjuntos ordenados.

Teorema 7.13: Sea k un cuerpo de característica cero y K/k una extensión de cuerpos de grado impar. Dados $a_1, \ldots, a_n \in k$ no nulos tales que $a_1x_1^2 + \cdots + a_nx_n^2 = 0$ tiene solución no trivial en K, entonces posee solución no trivial en k también.

Demostración: Como k es de característica cero, entonces K/k es separable y, por el teorema del elemento primitivo, $K = k(\alpha)$ donde α es raíz de un polinomio minimal $g(x) \in k[x]$ de grado $2m+1$. Por extensión de Kronecker sabemos que $K \cong k[x]/\big(g(x)\big)$, de modo que una solución no trivial a la ecuación se traduce a que existen $f_1, \ldots, f_n \in k[x]$ no todos nulos tales que

$$a_1f_1(x)^2 + \cdots + a_nf_n(x)^2 = h(x)g(x)$$

para algún $h(x) \in k[x]$. Más aún, como $k[\alpha]$ corresponde a evaluar polinomios de grado $< 2m+1$, entonces podemos exigir que $\deg(f_i) \leq 2m$ y que sean coprimos. Luego, el lado izquierdo corresponde a un polinomio de grado par $\leq 4m$, de modo que $h(x)$ debe tener grado impar $\leq 2m-1$.

Luego $h(x) = h_1(x)h_2(x)$, donde h_1 es irreducible, de grado impar $\leq 2m-1 < 2m+1$. Por lo tanto, si β es una raíz de h_1, entonces definimos $L := k(\beta)$. Como los f_i's son coprimos tenemos que las clases $[f_i] \in k[x]/(h_1(x)) \cong L$ no son todas nulas y, por lo tanto, determinan una solución no trivial en L. Luego procedemos recursivamente obteniendo soluciones en cuerpos de grado impar cada vez menor de modo que en un máximo de m pasos obtenemos una solución no trivial en k. □

Teorema (AE) 7.14: Sea $(R, \leq)$ un cuerpo ordenado y K/R una extensión finita de cuerpos tal que se da alguno de los casos:

(a) $K = R(\sqrt{a})$ con $a > 0$.

(b) $[K : R]$ es impar.

Entonces K es formalmente real y posee un orden que extiende al de R.

Demostración: Probaremos que el conjunto:

$$P := \left\{ \sum_{j=1}^{n} c_j\alpha_j^2 : c_j \in R, \alpha_j \in K, c_j > 0 \right\}$$

es un precono positivo. Claramente P satisface PCP2, y un cálculo directo demuestra que satisface PCP1. Basta probar PCP3, para ello supongamos,

por contradicción, que

$$-1 = \sum_{j=1}^{n} c_j \alpha_j^2 \iff 0 = 1 \cdot 1^2 + c_1\alpha_1^2 + \cdots + c_n\alpha_n^2.$$

En el caso (b), basta aplicar el teorema anterior, lo que nos da una solución no trivial en R, lo que es absurdo. En el caso (a), escribamos $\alpha_i = b_i + d_i\sqrt{a}$ y notemos que $\alpha_i^2 = b_i^2 + ad_i^2 + 2b_id_i\sqrt{a}$, de modo que, estudiando la primera coordenada se tiene que

$$0 = 1^2 + \sum_{i=1}^{n} \left(c_ib_i^2 + ac_id_i^2\right),$$

donde todos los coeficientes yacen en R. Pero ésto es absurdo puesto que claramente el lado derecho es positivo. □

Teorema (AE) 7.15: Sea R un cuerpo, entonces son equivalentes:

1. R es realmente cerrado.
2. Todo polinomio de grado impar en $R[x]$ posee raíz, y existe un ordenamiento bajo el cual todos los positivos son exactamente los cuadrados de R.
3. R no es algebraicamente cerrado y $R(\mathrm{i})$ (donde $\mathrm{i} = \sqrt{-1}$) es su clausura algebraica.

Demostración: 1 $\implies$ 2. Ya vimos la afirmación de los cuadrados. Si $p(x) \in R[x]$ es de grado impar, entonces podemos construir una extensión de cuerpo de grado impar K/R en donde sí tenga raíces. Por el teorema anterior, K es formalmente real, pero como R es realmente cerrado, entonces $K = R$.

2 $\implies$ 3. Como R posee un orden, entonces es formalmente real, luego $\sqrt{-1} \notin R$. Comprobar que $R[\mathrm{i}]$ es algebraicamente cerrado se reduce al teorema 4.62.

3 $\implies$ 1. Probaremos que la suma de cuadrados es también un cuadrado en R: Sean $a, b \in R$. Como $R(\mathrm{i})$ es algebraicamente cerrado, entonces $a + \mathrm{i}b$ posee raíz:

$$a + b\mathrm{i} = (c + d\mathrm{i})^2 = c^2 - d^2 + 2cd\mathrm{i},$$

con $c, d \in R$. Luego

$$a^2 + b^2 = (c^2 - d^2)^2 + 4c^2d^2 = (c^2 + d^2)^2.$$

Por inducción sobre los sumandos concluimos que toda suma de cuadrados es un cuadrado. Como -1 no es un cuadrado, se concluye que R es formalmente real.

Sea K/R una extensión algebraica de R. Entonces $K(\mathrm{i})/R(\mathrm{i})$ es algebraica, pero como $R(\mathrm{i})$ es algebraicamente cerrado, entonces $K(\mathrm{i}) = R(\mathrm{i})$. Luego $R(\mathrm{i})/K/R$ son extensiones de cuerpo y como $[R(\mathrm{i}) : R] = 2$, entonces suceden dos cosas: o bien $K = R$, o bien $K = R(\mathrm{i})$. En el segundo caso, $R(\mathrm{i})$ no es formalmente real, lo que comprueba que R es realmente cerrado. □

Lema 7.16: Sea k un cuerpo de característica $p \neq 0$ con una extensión finita de cuerpos de grado p. Entonces para todo $n \in \mathbb{N}_{\neq 0}$ existe una cadena de extensiones

$$k = K_0 \subset K_1 \subset \cdots \subset K_n$$

tal que K_{i+1}/K_i es de grado p.

Demostración: Sea $a \in k$, definimos $\phi(a) := a^p - a$. Entonces, nótese que posee las siguientes propiedades:

1. $\phi(a) + \phi(b) = \phi(a + b)$.
2. Si $a \in k$ y $b \in \mathbb{F}_p$, entonces $\phi(ab) = b\phi(a)$.
3. $a \in \mathbb{F}_p$ syss $\phi(a) = 0$.
4. Si $a \notin \phi[k]$, entonces $f_a(x) = x^p - x - a$ es irreducible en $k[x]$

La 1 es el sueño del aprendiz, la 2 es corolario de la 1, la 3 es el pequeño teorema de Fermat y la 4 es parte del teorema 4.80.

Sea β raíz de $f_a(x)$, probaremos que $a\beta^{p-1} \notin \phi[k(\beta)]$: De lo contrario, para algún

$$\gamma = c_0 + c_1\beta + \cdots + c_{p-1}\beta^{p-1} \in k(\beta)$$

con $c_i \in k$, se tiene que $\gamma^p - \gamma = \phi\gamma = a\beta^{p-1}$. Como $\beta^p = \beta + a$ se tiene que

$$a\beta^{p-1} = \sum_{i=0}^{p-1} c_i^p(\beta^p)^i - \sum_{i=0}^{p-1} c_i\beta^i = \sum_{i=0}^{p-1} c_i^p(\beta + a)^i - \sum_{i=0}^{p-1} c_i\beta^i.$$

Como $1, \beta, \ldots, \beta^{p-1}$ son linealmente independientes sobre k, podemos mirar los coeficientes de β^{p-1} y obtener la relación $a = c_{p-1}^{p-1} - c_{p-1} = \phi(c_{p-1})$; pero $a \notin \phi[k]$ lo que es absurdo. □

Teorema (AE) 7.17: Sea K un cuerpo no algebraicamente cerrado, pero cuya clausura algebraica K^{alg}/K es una extensión finita. Entonces K es realmente cerrado y $K^{\text{alg}} = K(\sqrt{-1})$.

Demostración: Si $K^{\text{alg}} = K(\sqrt{-1})$, entonces basta aplicar el teorema 7.15, así que supondremos que $K(\sqrt{-1}) \subset K^{\text{alg}}$.

Si K no es un cuerpo perfecto, entonces tiene característica $p \neq 0$ y Frob_K no es un automorfismo (en particular, no es suprayectivo), de modo que existe $a \in K$ tal que para todo $b \in K$ se cumple que $x^p - a \in K[x]$ no posee raíces y así construimos una extensión de cuerpos $K \subset K\left[\sqrt[p]{a}\right]$ de grado p, y aplicamos el lema anterior.

Por el párrafo anterior, K debe ser perfecto y K^{alg} debe ser una extensión de Galois. Sea $G := \text{Gal}(K^{\text{alg}}/K(\sqrt{-1}))$ y, por el teorema de Cauchy, sea $H \leq G$ cíclico de orden primo q (luego es un grupo simple), y sea L su cuerpo fijado. Nótese que $q \neq p$ pues de lo contrario volvemos a aplicar el lema anterior para probar que la extensión es infinita. Sea ζ_n una q^n-ésima raíz primitiva de la unidad en K^{alg}. Si $\zeta_1 \notin L$, entonces $1 < [L(\zeta_1) : L] < q$ lo que contradice que H no posee subgrupos impropios (por ser simple). Luego $\zeta_1 \in L$ y $K^{\text{alg}} = L(\sqrt[q]{a})$ para algún $a \in L$ por el teorema 4.80. Sea γ una raíz de $x^{q^2} - a$, de modo que $x^{q^2} - a = \prod_{i=1}^{q^2}(x - \zeta_2^i\gamma)$. Como $[K^{\text{alg}} : L] = q$, entonces $x^{q^2} - a$ es reducible sobre L, así pues posee algún factor irreducible mónico $h(x)$ de grado q. El coeficiente libre de $h(x)$ es de la forma $\gamma^q\zeta_2^j$. Como γ^q es raíz de $x^q - a$, entonces $\gamma^q \notin L$ y luego $K^{\text{alg}} = L(\zeta_2)$.

Sea k el cuerpo primo de K. Consideremos el cuerpo $k(\zeta_2)$ y sea r el mínimo natural tal que $\zeta_r \in k(\zeta_2)$ pero $\zeta_{r+1} \notin k(\zeta_2)$. Nótese que $\zeta_{r+1} \notin L$, de modo que su polinomio minimal $g(x) \in L[x]$ tiene grado q y es un factor de $\prod_{i=1}^{q^{r+1}}(x - \zeta_{r+1}^i)$, el cual tiene coeficientes en $k(\zeta_{r+1})$. Ergo,

$$g(x) \in \big(k(\zeta_{r+1}) \cap L\big)[x] \quad \text{y} \quad \big[k(\zeta_{r+1}) : \big(k(\zeta_{r+1}) \cap L\big)\big] = q.$$

Nótese que $[k(\zeta_{r+1}) : k(\zeta_r)] = q$ y que como $\zeta_r \notin L$, entonces $k(\zeta_r) \neq k(\zeta_{r+1}) \cap L$. Ésto demuestra que $G^* := \text{Gal}(k(\zeta_{r+1})/k)$ posee al menos dos subgrupos de orden q, de modo que G^* no es cíclico. En consecuencia, por el teorema 4.74, se cumple que $k = \mathbb{Q}$. Como G^* no es cíclico, entonces $q = 2$, de modo que $\zeta_2 = \pm\sqrt{-1}$, pero por definición de L se cumple que $\zeta_2 \in L$ lo que es absurdo. □

Probar que si un grupo no es cíclico y posee dos subgrupos de orden 2, entonces

7.2 Teoremas de Pfister

Definición 7.18: Sea k un cuerpo arbitrario. Se le llama el *nivel*[2] del cuerpo, denotado $s(k)$, al mínimo n tal que

$$-1 = a_1^2 + \cdots + a_n^2,$$

donde $a_i \in k$. Si k es formalmente real, denotamos $s(k) := \infty$.

El objetivo de ésta sección es entender qué clase de valores puede tomar $s(k)$ (además de ∞).

Ejemplo.
- Por la ley de reciprocidad cuadrática, si $p = 2$ o $p \equiv 1$ (mód 4) entonces $s(\mathbb{F}_p) = 1$.
- $s\big(\mathbb{Q}(\sqrt{-2})\big) = 2$, puesto que $-1 = \sqrt{-2}^2 + 1^2$ y -1 no es cuadrado (¿por qué?).
- $s\big(\mathbb{Q}(\sqrt{-3})\big) \leq 3$ puesto que $-1 = \sqrt{-3}^2 + 1^2 + 1^2$. Por el mismo razonamiento $s\big(\mathbb{Q}(\sqrt{-11})\big) \leq 3$
- $s\big(\mathbb{Q}(\sqrt{-d})\big) \leq 5$ con $d \in \mathbb{Z}_{>0}$, puesto que $d^2 - 1 \in \mathbb{Z}_{>0}$ siempre se puede escribir como suma de cuatro cuadrados por el teorema de Lagrange.

Estaría bien saber si los dos últimos ejemplos se pueden refinar.

Teorema 7.19: Sea k un cuerpo arbitrario y sea $n = 2^m$. Entonces existen identidades de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \tag{7.1}$$

donde:

$$z_j = \sum_{i=1}^{n} t_{ij} y_j, \qquad t_{ij} \in k(x_1, \ldots, x_n).$$

Demostración: Lo haremos por inducción sobre m. El caso base $m = 1$ sale del hecho de que $|\alpha\beta|^2 = |\alpha|^2 |\beta|^2$ para $\alpha, \beta \in \mathbb{C}$. Supongamos que aplica para m, y por tanto la identidad (7.1) es válida para $n = 2^m$. Denotando

[2] de. *Stufe*.

$T := [t_{ij}]_{ij}$, entonces se reescribe como

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = T \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Empleando productos internos podemos reescribir la identidad como

$$\begin{aligned}(x_1^2 + \cdots + x_n^2)(y_1, \ldots, y_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} &= (z_1, \ldots, z_n) \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \\ &= (y_1, \ldots, y_n) t^t t \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.\end{aligned}$$

Reordenando los términos equivale a que

$$\begin{aligned}(y_1, \ldots, y_n)\big((x_1^2 + \cdots + x_n^2) I_n - T^t T\big) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = 0, \\ (x_1^2 + \cdots + x_n^2) I_n = T^t T.\end{aligned}$$

Ahora, queremos ver que éste es el caso para $m+1$ y, por ende, para $2n$. Sea

$$\big((x_1, \ldots, x_n), (x_{n+1}, \ldots, x_{2n})\big) = (\boldsymbol{X}_1, \boldsymbol{X}_n).$$

Por hipótesis inductiva existen T_1, T_2 tales que:

$$\begin{aligned}(x_1^2 + \cdots + x_n^2) I_n = \boldsymbol{X}_1 \boldsymbol{X}_1^t I_n = T_1 T_1^t = T_1^t T_1, \\ (x_{n+1}^2 + \cdots + x_{2n}^2) I_n = \boldsymbol{X}_2 \boldsymbol{X}_2^t I_n = T_2 T_2^t = T_2^t T_2.\end{aligned}$$

Queremos encontrar un T que funcione para ambas matrices en simultáneo. Sea $T := \left(\begin{smallmatrix} T_1 & T_2 \\ T_2 & M \end{smallmatrix}\right)$, entonces se tiene que

$$\begin{aligned}T^t T &= \begin{bmatrix} T_1^t T_1 + T_2^t T_2 & T_1^t T_2 + T_2^t M \\ T_2^t T_1 + M^t T_2 & T_2^t T_2 + M^t X \end{bmatrix} \\ &= \begin{bmatrix} (x_1^2 + \cdots + x_{2n}^2) I_n & A \\ B & C \end{bmatrix}.\end{aligned}$$

Y queremos elegir a M de modo que $A = B = 0$ y $C = (x_1^2 + \cdots + x_{2n}^2)I_n$. Para forzar las primeras dos condiciones elegimos $M = -(T_2^t)^{-1}T_1^{-1}T_2$ (¿por qué?), pero milagrosamente también satisface la tercera condición:

$$\begin{aligned} C = T_2^tT_2 + M^tM &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + T_2^tT_1T_2^{-1}(T_2^t)^{-1}T_1^tT_2 \\ &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + (x_{n+1}^2 + \cdots + x_{2n}^2)^{-1}T_2^tT_1T_1^tT_2 \\ &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + (x_1^2 + \cdots + x_n^2)I_n. \end{aligned}$$

Ésto completa la demostración. □

Lema 7.20 (Cassels): Sea $f(x) \in k[x] \subseteq k(x)$. Si $f(x)$ es una suma de n cuadrados en $k(x)$, entonces también es una suma de n cuadrados en $k[x]$.

Demostración: Veamos un par de casos aislados:

(a) Si $n = 1$, entonces es trivial.

(b) Si $\operatorname{car} k = 2$, entonces como $a^2 + b^2 = (a + b)^2$ se nota que se reduce al caso $n = 1$.

(c) Si $\operatorname{car} k \neq 2$ y $s(k) < n$, entonces digamos que $-1 = b_1^2 + \cdots + b_{n-1}^2$ con $b_i \in k$. Luego, nótese que

$$\begin{aligned} f(x) &= \left(\frac{f+1}{2}\right)^2 - \left(\frac{f-1}{2}\right)^2 \\ &= \left(\frac{f+1}{2}\right)^2 + \left(b_1 \cdot \frac{f-1}{2}\right)^2 + \cdots + \left(b_{n-1} \cdot \frac{f-1}{2}\right)^2. \end{aligned}$$

Si ninguno de los casos previos se da, entonces sea

$$f(x) = (p_1/q_1)^2 + \cdots + (p_n/q_n)^2 \in k(x),$$

luego, limpiando denominadores tenemos la ecuación

$$f \cdot h^2 = g_1^2 + \cdots + g_n^2, \qquad g_1, \ldots, g_n, h \in k[x], h \neq 0.$$

Es decir, la ecuación $f \cdot Z^2 = Y_1^2 + \cdots + Y_n^2$ tiene alguna solución no trivial $Z \neq 0$ en $k[x]$, queremos ver que posee alguna solución no trivial en k y para ello, elegiremos $(\zeta, \eta_1, \ldots, \eta_n)$ una solución con $\deg \zeta$ minimal.

Por contradicción supongamos que $\deg \zeta > 0$. Por algoritmo de la división (sobre $k[x]$) sea $\eta_j = \lambda_j\zeta + \gamma_j$ para todo j, donde γ_j es o bien nulo, o bien

$\deg \gamma_j < \deg \zeta$. Nótese que, por minimalidad de ζ, existe algún j tal que $\gamma_j \neq 0$. Definamos

$$\alpha := \sum_{i=1}^{n} \lambda_i^2 - f, \qquad \beta := \sum_{i=1}^{n} \lambda_i \eta_i - f\zeta,$$
$$\bar{\zeta} := \alpha\zeta - 2\beta, \qquad \bar{\eta}_j := \alpha\eta_j - 2\beta\lambda_j.$$

Es claro que ambos son polinomios en $k[x]$.

(I) $(\bar{\zeta}, \bar{\eta}_1, \ldots, \bar{\eta}_n)$ es solución: Ésto es un cálculo. Puede reducirse a probar que $\sum_{j=1}^{n} \bar{\eta}_j^2 = f\bar{\zeta}^2$, ésto nos queda como

$$\sum_{j=1}^{n} (\alpha^2\eta_j^2 - 4\alpha\beta\eta_j\lambda_j + 4\beta^2\lambda_j^2) = (\alpha^2\zeta^2 - 4\alpha\beta\zeta + 4\beta^2)f.$$

Reordenando términos, factorizando el 4β común y expandiendo la definición de α, β se reduce a probar que

$$4\beta \cdot \left(\left(\sum_{i=1}^{n} \lambda_i\eta_i - f\zeta \right) \sum_{j=1}^{n} \lambda_j^2 - \left(\sum_{i=1}^{n} \lambda_i^2 - f \right) \sum_{j=1}^{n} \eta_j\lambda_j \right.$$
$$\left. - \left(\sum_{j=1}^{n} \lambda_j\eta_j - f\zeta \right) f + \left(\sum_{i=1}^{n} \lambda_i^2 - f \right) f\zeta \right) = 0.$$

(II) $\bar{\zeta} \neq 0$: Comenzamos por definir $\Lambda_j := \gamma_j/\zeta = \eta_j/\zeta - \lambda_j \in k(x)$. Luego tenemos que

$$\bar{\zeta} = \left(\sum_{j=1}^{n} \left(\frac{\eta_j^2}{\zeta^2} - \frac{2\eta_j\Lambda_j}{\zeta} + \Lambda_j^2 \right) - f \right) \zeta - 2 \left(\sum_{j=1}^{n} \left(\frac{\eta_j}{\zeta} - \Lambda_j \right) \eta_j - f\zeta \right)$$
$$= (\Lambda_1^2 + \cdots + \Lambda_n^2)\zeta = \frac{1}{\zeta} \sum_{j=1}^{n} \gamma_j^2.$$

Como $s(k) \geq n$, mirando el mayor coeficiente de γ_j^2 concluimos que la suma es no nula.

(III) $\deg(\bar{\zeta}) < \deg \zeta$: Por la última igualdad tenemos que $\zeta \cdot \bar{\zeta} = \sum_{j=1}^{n} \gamma_j^2$, de modo que $\deg \zeta + \deg \bar{\zeta} = 2 \max_j(\gamma_j) < 2 \deg \zeta$ (puesto que $\deg \gamma_j < \deg \zeta$ para todo j), de modo que $\deg(\bar{\zeta}) < \deg \zeta$.

Ésto contradice la minimalidad del grado de ζ lo que es absurdo. □

Varios corolarios:

Corolario 7.21: Sea $\operatorname{car} k \neq 2$ y sea $f(x_1, \ldots, x_m) \in k(x_1, \ldots, x_m)$ una suma de n cuadrados. Sean $a_1, \ldots, a_m \in k$ tales que $f(a_1, \ldots, a_m)$ está bien definido (el denominador no es cero), entonces $f(a_1, \ldots, a_m)$ es una suma de n cuadrados.

Corolario 7.22: Sea k un cuerpo arbitrario. Denotemos por $G_n(k)$ a los elementos no nulos que se pueden escribir con n cuadrados, donde n es una potencia de 2. Entonces $G_n(k)$ es un grupo con la multiplicación.

Demostración: Ésto sale del teorema 7.19. □

Corolario 7.23: Sea $\operatorname{car} k \neq 2$ y sea $d \in k$. El polinomio $x^2 + d \in k[x]$ es una suma de n cuadrados en $k(x)$ (y por lema de Cassels en $k[x]$) syss -1 o d son sumas de $n-1$ cuadrados en k.

Demostración: $\Longleftarrow$ es claro. Veamos $\Longrightarrow$: Sea $x^2 + d = p_1(x)^2 + \cdots + p_n(x)^2$ con $p_i(x) \in k[x]$ de grado ≤ 1. Luego $p_i = a_i x + b_i$ y tenemos

$$x^2 + d = (a_1 x + b_1)^2 + \cdots + (a_n x + b_n)^2,$$

nótese que si $\operatorname{car} k \neq 2$, entonces para algún j se cumple que la ecuación $C = \pm(a_j C + b_j)$ posee solución (separar por casos si $a_j = 1$ o no). Luego podemos reordenar los términos de modo que $C = \pm p_n(C)$ y evaluando en $x = C$ se obtiene

$$\cancel{C^2} + d = (a_1 C + b_1)^2 + \cdots + (a_{n-1} C + b_{n-1})^2 + \cancel{C^2},$$

con lo que comprobamos que d se escribe como suma de $n-1$ cuadrados. □

Corolario 7.24: Considere $\mathbb{R}(x_1, \ldots, x_n)$, aquí $x_1^2 + \cdots + x_n^2$ no es una suma de $n-1$ cuadrados.

Pista: Aplicar inducción y definir $k := \mathbb{R}(x_1, \ldots, x_n)$ de modo que $k(x_{n+1}) = \mathbb{R}(x_1, \ldots, x_{n+1})$. □

Teorema 7.25: Sea k un cuerpo no formalmente real. Entonces $s(k)$ es una potencia de 2. Recíprocamente, dada la potencia 2^m existe un cuerpo k tal que $s(k) = 2^m$.

Demostración:

(i) Los niveles son potencias de 2: Nótese que siempre existe m tal que

$$n := 2^m \leq s(k) < 2^{m+1} = 2n.$$

Así pues, sea $a_1^2 + \cdots + a_n^2 + a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1 = 0$ para algunos $a_i \in k$ (posiblemente nulos). Sean

$$A := a_1^2 + \cdots + a_n^2, \qquad B := a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1,$$

Como $s(k) \geq n$ entonces podemos elegir los a_i's de modo que $A \neq 0 \neq B$ y la condición se traduce en que $A+B = 0$, o equivalentemente, $A = -B$. Por definición $A, B \in G_n(k)$, de modo que $A/B = -1 \in G_n(k)$, por ser grupo multiplicativo, luego -1 se escribe como una suma de n cuadrados y $s(k) \leq n$. Por antisimetría del $\leq$, $s(k) = n$ como se quería probar.

(ii) Las potencias de 2 son niveles: El caso $n = 1$ es conocido (e.g., $s(\mathbb{C}) = 1$). Sea $n = 2^m > 1$ y sean $k := \mathbb{R}(x_1, \ldots, x_{n+1})$ y $L := k(\gamma)$, donde los x_i's son indeterminadas (elementos trascendentes algebraicamente independientes) y γ es raíz del polinomio:

$$\gamma^2 + x_1^2 + \cdots + x_{n+1}^2 = 0,$$

dividiendo por γ^2 se concluye que $s(L) \leq n + 1$ y por ende $s(L) \leq n$ puesto que tiene que ser una potencia de 2.

Si $s(L) < n$, entonces existen $t_1, \ldots, t_n \in L$ tales que

$$t_1^2 + \cdots + t_n^2 = 0.$$

Como L/k es una extensión de grado 2, entonces cada $t_i = \alpha_i\gamma + \beta_i$. Luego, la igualdad superior se reescribe como

$$\left(\gamma^2 \cdot \sum_{i=1}^{n} \alpha_i^2 + \sum_{i=1}^{n} \beta_i^2\right) + 2\gamma \sum_{i=1}^{n} \alpha_i\beta_i = 0.$$

Como k es formalmente real, entonces algún α_i es no nulo, y análogamente se puede ver que algún β_i es no nulo. Enfocándonos en el primer paréntesis, nos queda que

$$-\gamma^2 = x_1^2 + \cdots + x_{n+1}^2 = \frac{\sum_{i=1}^n \beta_i^2}{\sum_{i=1}^n \alpha_i^2} \in G_n(k),$$

puesto que $G_n(k)$ es un grupo bajo multiplicación. Pero ésto contradice el corolario anterior. En conclusión, se cumple que $n = s(L)$ como se quería probar. □

¿Los cuerpos de nivel arbitrariamente grande siempre tienen alto grado de trascendencia sobre $\mathbb{Q}$?

Ahora también podemos probar un recíproco del teorema 7.19:

Teorema 7.26: Sea n un número que no es potencia de 2. Entonces existe un cuerpo k en donde no se satisface una identidad de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2,$$

donde:

$$z_j = \sum_{i=1}^n t_{ij} y_j, \qquad t_{ij} \in k(x_1, \ldots, x_n).$$

Demostración: Sea m tal que $2^{m-1} < n < 2^m$ y sea k un cuerpo tal que $s(k) = 2^m$. Luego podemos elegir $a_i \in k$ tales que

$$a_1^2 + \cdots + a_n^2 + a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1 = 0,$$

puesto que $2n > s(k)$ y definir $A := a_1^2 + \cdots + a_n^2$ y $B := a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1$ notando que son no nulos. Si existiese una identidad de ese estilo, entonces se comprobaría que $G_n(k)$ es un grupo con la multiplicación y así $-1 = A/B \in G_n(k)$, pero ésto es absurdo puesto que $n < s(k)$. □

§7.2.1 Calculando el nivel. Ahora veremos cómo calcular el nivel de ciertos cuerpos. Comencemos sencillo con los finitos:

Proposición 7.27: Sea $q = p^\alpha$. Entonces:

$$s(\mathbb{F}_q) = \begin{cases} 1, & p = 2 \vee p \equiv 1 \pmod 4 \vee \alpha \text{ par}, \\ 2, & p \equiv 3 \pmod 4 \wedge \alpha \text{ impar}. \end{cases}$$

En particular, el nivel es fácil de determinar en característica $\neq 0$. El siguiente es el caso de los cuerpos cuadráticos. Primero necesitaremos el siguiente resultado:

Lema 7.28 (Davenport-Cassels): Supongamos que $n \in \mathbb{Z}$ puede escribirse como suma de tres cuadrados racionales, entonces también puede escribirse como suma de tres cuadrados enteros.

Demostración: Sea $n = \lambda_1^2 + \lambda_2^2 + \lambda_3^2 \in \mathbb{Q}$. Limpiando denominadores se obtiene que

$$t^2 n = \mu_1^2 + \mu_2^2 + \mu_3^2, \qquad t, \mu_1, \mu_2, \mu_3 \in \mathbb{Z},$$

donde elegimos que t sea minimal.

Desde aquí seguimos de forma muy análoga la demostración del lema de Cassels. Sea $\mu_i/t = q_i + r_i$ con $q_j \in \mathbb{Z}$ y $|r_i| \leq 1/2$. Por minimalidad de t podemos suponer que algún r_i es no nulo y definamos:

$$a := q_1^2 + q_2^2 + q_3^2 - n, \qquad b := 2\big(nt - (\mu_1 q_1 + \mu_2 q_2 + \mu_3 q_3)\big),$$
$$\bar{t} := at + b, \qquad \bar{\mu}_i := a\mu_i + bq_i.$$

Luego notamos que

$$\begin{aligned}\sum_{i=1}^{3} \bar{\mu}_i^2 &= a^2 \sum_{i=1}^{3} \mu_i^2 + b^2 \sum_{i=1}^{3} q_i^2 + 2ab \sum_{i=1}^{3} \mu_i q_i \\ &= a^2(t^2 n) + b^2(a+n) + ab(2nt - b) \\ &= n(at+b)^2 = n\bar{t}^2.\end{aligned}$$

Así, nos queda ver que $\bar{t}$ es no nulo:

$$\begin{aligned}t \cdot \bar{t} &= at^2 + bt \\ &= t^2 \left(\sum_{i=1}^{3} q_i^2 - n \right) + t \left(2nt - 2 \sum_{i=1}^{3} \mu_i q_i \right) \\ &= t^2 \sum_{i=1}^{3} q_i^2 - 2t \sum_{i=1}^{3} \mu_i q_i + \sum_{i=1}^{3} \mu_i^2 \\ &= \sum_{i=1}^{3} (tq_i - \mu_i)^2 = t^2(r_1^2 + r_2^2 + r_3^2).\end{aligned}$$

Y que es menor que t:

$$\bar{t} = t(r_1^2 + r_2^2 + r_3^2) \leq t \left(\frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^2} \right) = \frac{3}{4} t. \qquad \square$$

Teorema 7.29: Sea $d > 0$ un entero libre de cuadrados. Entonces:

$$s\big(\mathbb{Q}(\sqrt{-d})\big) = \begin{cases} 1, & d = 1 \\ 2, & d \not\equiv 7 \pmod 8 \\ 4, & d \equiv 7 \pmod 8 \end{cases}$$

Más aún, $s\big(\mathbb{Q}(\sqrt{-d})\big) = 2$ syss d puede escribirse como suma de tres cuadrados.

Demostración: Fijemos $d > 0$ libre de cuadrados y $k := \mathbb{Q}(\sqrt{-d})$ Ya hemos visto que $s(k) \leq 5$ en un ejemplo y de ahí que las posibilidades se reducen a 1, 2 y 4. Es claro también que $s(k) = 1$ syss $d = 1$.

Si $d \not\equiv 7 \pmod 8$, entonces d se puede escribir como suma de tres cuadrados y se obtiene que $0 = (\sqrt{-d})^2 + a^2 + b^2 + c^2$ y reordenando términos obtenemos que $-1 = \alpha^2 + \beta^2 + \gamma^2$ y $s(k) \leq 3$. De aquí ya podemos concluir que necesariamente $s(k) = 2$, pero constructivamente:

$$-1 = \left(\frac{\alpha\gamma + \beta}{\alpha^2 + \beta^2}\right)^2 + \left(\frac{\beta\gamma - \alpha}{\alpha^2 + \beta^2}\right)^2.$$

Si $d \equiv 7 \pmod 8$ y $s(k) = 2$, entonces

$$\begin{aligned} -1 &= (a_1 + b_1\sqrt{-d})^2 + (a_2 + b_2\sqrt{-d})^2 \\ &= \big(a_1^2 + a_2^2 - d(b_1^2 + b_2^2)\big) + 2(a_1b_1 + a_2b_2)\sqrt{-d}, \end{aligned}$$

definiendo $\gamma := b_1^2 + b_2^2$ podemos notar que

$$b_1^2(a_1^2 + a_2^2) = (a_1b_1)^2 + a_2^2b_1^2 = (-a_2b_2)^2 + a_2^2b_1^2 = a_2^2\gamma,$$

de modo que, reordenando obtenemos que

$$d = \frac{1}{\gamma}(a_1^2 + a_2^2 + 1) = \frac{a_1^2 + a_2^2}{\gamma} + \frac{\gamma}{\gamma^2} = \frac{a_2^2}{b_1^2} + \frac{b_1^2}{\gamma^2} + \frac{b_2^2}{\gamma^2}.$$

Lo cual es absurdo, puesto que d no puede escribirse como suma de tres cuadrados. □

8

Álgebra lineal avanzada

8.1 Grupos abelianos libres, y de torsión

Ya vimos en el capítulo de módulos como todo k-espacio vectorial es un módulo libre que induce un grupo aditivo que es *casi* libre, con la excepción de que la cualidad de ser «abeliano» es en sí mismo una restricción.

Definición 8.1: Sea $\{G_i\}_{i\in I}$ una familia de grupos, entonces definimos su producto como

$$\prod_{i\in I} G_i := \{(g_i)_{i\in I} : \forall i \in I \; g_i \in G_i\}$$

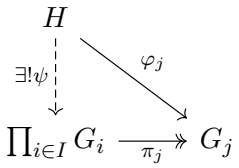
con la operación

$$(g_i)_{i\in I} \cdot (h_i)_{i\in I} := (g_i \cdot h_i)_{i\in I}.$$

Proposición 8.2: Sea $\{G_i\}_{i\in I}$ una familia de grupos, entonces:

1. $\prod_{i\in I} G_i$ es también un grupo, y las proyecciones $\pi_j \colon \prod_{i\in I} G_i \to G_j$ son homomorfismos de grupos.

2. Si H es un grupo y $\{\varphi_i \colon H \to G_i\}_{i\in I}$ es una familia de homomorfismos de grupos, entonces existe un único homomorfismo $\psi := \Delta_{i\in I}\, \varphi_i \colon H \to \prod_{i\in I} G_i$ tal que el siguiente entonces existe un único homomorfismo $\psi := \Delta_{i\in I}\, \varphi_i \colon H \to \prod_{i\in I} G_i$ tal que el siguiente diagrama:



conmuta. En consecuencia, $\prod_{i\in I} G_i$ es un producto categorial en Grp.

3. $\prod_{i\in I} G_i$ es abeliano syss todos los G_i's lo son.

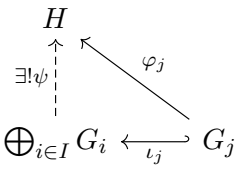
Definición 8.3: Dada una familia de grupos $\{G_i\}_{i\in I}$ se denota:

$$\bigoplus_{i\in I} G_i := \{(g_i)_{i\in I} : \{i : g_i \neq 1\} \text{ es finito}\} \subseteq \prod_{i\in I} G_i.$$

Proposición 8.4: Sea $\{G_i\}_{i\in I}$ una familia de grupos, entonces:

1. $\bigoplus_{i\in I} G_i$ es un subgrupo de $\prod_{i\in I} G_i$, y las inclusiones $\iota_j \colon G_j \to \bigoplus_{i\in I} G_i$ son homomorfismos de grupos.

2. Si H es un grupo y $\{\varphi_i \colon G_i \to H\}_{i\in I}$ es una familia de homomorfismos de grupos, entonces existe un único homomorfismo $\psi := \sum_{i\in I} \varphi_i \colon \bigoplus_{i\in I} G_i \to H$ tal que el siguiente diagrama:



conmuta. En consecuencia, $\bigoplus_{i\in I} G_i$ es un coproducto categorial en Grp.

3. $\bigoplus_{i\in I} G_i$ es abeliano syss todos los G_i's lo son.

Reiteramos que éstas propiedades no deben de sorprender a nadie, puesto que son absolutamente análogas al caso de módulos. En ésta sección hicimos énfasis en el hecho de que los (co)productos existen en Ab, ésto permite definir lo siguiente:

Definición 8.5: Se dice que un grupo G es *abeliano libre* (en conjunto) si existe $\{x_i\}_{i\in I} \subseteq G$ tal que

$$G \cong \bigoplus_{i\in I} \langle x_i \rangle,$$

donde cada $\langle x_i \rangle$ es un grupo cíclico infinito. En cuyo caso, al conjunto $\{x_i\}_{i\in I}$ se le dice una *base* de G.

En general, desde aquí en adelante emplearemos notación aditiva para los grupos abelianos, es decir, la operación entre x e y se denota «$x+y$», «0» es el neutro y la n-ésima potencia de x se denota «nx».

Proposición 8.6: Sea G un grupo abeliano, entonces para todo $n > 0$ natural:

$$nG := \{ng : g \in G\}$$

es un subgrupo de G. Más aún, si p es un número primo, entonces G/pG es un $\mathbb{F}_p$-espacio vectorial.

Demostración: Sea $[r] \in \mathbb{F}_p$ y sea $g \in G$, luego definamos

$$[r] \cdot (a + pG) := ra + pG.$$

Nótese que está bien definido dado que si $r' = r + pm$, entonces

$$r'a + pG = ra + pma + pG = ra + pG,$$

dado que $p(ma) \in pG$. También es fácil probar el resto de axiomas de un espacio vectorial. □

Corolario 8.7: Se cumplen:

1. Todo grupo abeliano libre finitamente generado es isomorfo a $\mathbb{Z}^n$ para algún n. Más generalmente, definiendo $\mathbb{Z}^{\oplus\kappa} := \bigoplus_{\alpha=1}^{\kappa} \mathbb{Z}$, se cumple que todo grupo abeliano libre es isomorfo a $\mathbb{Z}^{\oplus\kappa}$ para algún número cardinal κ.

2. Más aún, $\mathbb{Z}^n \cong \mathbb{Z}^m$ syss $n = m$. De modo que todo par de bases de un grupo abeliano libre finitamente generado son de igual cardinalidad.

3. (AE) $\mathbb{Z}^{\oplus\kappa} \cong \mathbb{Z}^{\oplus\mu}$ syss $\kappa = \mu$. De modo que todo par de bases de un grupo abeliano libre son de igual cardinalidad.

Demostración: Para probar la segunda y la tercera basta tomar un grupo abeliano libre G y considerar a $G/2G$ como $\mathbb{F}_2$-espacio vectorial. Luego la unicidad de cardinalidad de bases de un espacio vectorial induce la unicidad de cardinalidad de bases como grupo abeliano libre. □

Definición 8.8: Dado un grupo abeliano libre G, se denota por $\operatorname{rank} G$ a la cardinalidad de cualquiera de sus bases.

Proposición 8.9: Sea G un grupo abeliano con un conjunto X tal que satisface lo siguiente: Para todo grupo abeliano H y toda aplicación $f\colon X \to H$, existe una única extensión $f^*\colon G \to H$ que es un homomorfismo de grupos. Entonces G es un grupo abeliano libre de base X.

Demostración: Sea H un grupo abeliano libre de base Y tal que existe una biyección $q\colon X \to Y$ de inversa $p\colon Y \to X$. Luego, por ser libres, ambas funciones se extienden a $f\colon G \to H$ y $g\colon H \to G$, homomorfismos de grupos. Nótese que además $p \circ q = \mathrm{Id}_X\colon X \to X \subseteq G$ es una aplicación que posee una extensión $\mathrm{Id}_G\colon G \to G$ que es única, y lo mismo vale para Id_H como extensión única de $q \circ p$. Finalmente, $p \circ q$ también se extiende a $f \circ g$ y $q \circ p$ se extiende a $g \circ f$, luego se comprueba que f, g son homomorfismos de grupos y además son una la inversa de la otra. □

Proposición (AE) 8.10: Sea M un A-módulo y $N \leq M$ tal que M/N es un módulo libre. Entonces existe $F \leq M$ tal que $M/N \cong F$ y $M = N \oplus F$.

Demostración: Si N es un submódulo de M, entonces la siguiente sucesión:

$$0 \longrightarrow N \longrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$$

es exacta. Como M/N es libre entonces posee una base $X = \{[x_i]\}_{i \in I}$, por tanto, la aplicación $g\colon X \to M$ dada por $g([x_i]) := x_i$ admite una extensión única $g\colon M/N \to M$, tal que $g \circ \pi$ fija a la base, luego por unicidad, se cumple que $g \circ \pi = \mathrm{Id}_{M/N}$. Es decir, la sucesión exacta se escinde y por la proposición 5.15 se cumple el enunciado. □

Como ejercicio en la demostración anterior ubique el uso de elección.

Teorema (AE) 8.11: Sea A un DIP, entonces todo A-submódulo M de un módulo libre F es también libre; y de hecho $\operatorname{rank} M \leq \operatorname{rank} F$.

Demostración: Como F es libre, entonces posee una base, que por el teorema del buen orden (AE) admite un buen orden $X = \{x_\alpha : \alpha < \kappa\}$ (aquí los subíndices son ordinales). Luego definamos

$$F'_\beta := \langle \{x_\alpha : \alpha < \beta\} \rangle, \qquad F_\beta := F'_\beta \oplus \langle x_\beta \rangle.$$

Y definamos $M'_\beta := M \cap F'_\beta$ y $M_\beta := M \cap F_\beta$. Nótese que

$$\frac{M_\beta}{M'_\beta} = \frac{M_\beta}{M_\beta \cap F'_\beta} \cong \frac{M_\beta + F'_\beta}{M_\beta} \subseteq \frac{F'_\beta}{F_\beta} \cong A,$$

donde hemos empleado el tercer teorema de isomorfismos (para módulos). Así que M_β/M'_β es isomorfo a un ideal de A, pero todos los ideales de A son principales, luego o son el ideal nulo o son isomorfos (como A-módulos) a A. Si el ideal no es nulo, entonces por la proposición anterior se cumple que $M_\beta \cong M'_\beta \oplus \langle \boldsymbol{m}_\beta \rangle$ para algún $\boldsymbol{m}_\beta \in M_\beta$ tal que $\langle \boldsymbol{m}_\beta \rangle \cong A$; si el ideal es nulo entonces $\boldsymbol{m}_\beta := \vec{0}$. Claramente, eliminando los $\boldsymbol{m}_\beta$'s nulos se tiene que éstos elementos son linealmente independientes (por construcción, de hecho), de modo que simplemente bastaría probar que generan a M para concluir el enunciado.

Para ello, definamos $M^* := \mathrm{Span}\{\boldsymbol{m}_\beta\}_{\beta<\kappa}$ y definamos:

$$\mu(\boldsymbol{m}) := \text{mín}\{\alpha : \boldsymbol{m} \in F_\alpha\}.$$

Supongamos que $M^* < M$, entonces definamos γ como el mínimo índice tal que $\gamma = \mu(\boldsymbol{m})$ para algún $\boldsymbol{m} \in M \setminus M^*$ y sea $\tilde{\boldsymbol{m}}$ un elemento que cumpla lo anterior, luego se cumple que

$$\tilde{\boldsymbol{m}} = \boldsymbol{a} + \lambda \boldsymbol{m}_\gamma \in M_\gamma$$

para unos únicos $\boldsymbol{a} \in M'_\gamma$ y $\lambda \in A$. Luego como $\boldsymbol{m}_\gamma \in M^*$ y $\tilde{\boldsymbol{m}} \notin M^*$ necesariamente se tiene que $\boldsymbol{a} \notin M^*$. Pero $\boldsymbol{a} \in F'_\gamma$, luego $\mu(\boldsymbol{a}) < \gamma$ contradiciendo la minimalidad de γ. □

Nótese que su F es finitamente generado, entonces no hay uso de elección.

Proposición 8.12: Sea A un anillo, F un A-módulo libre de base X y M otro A-módulo. Toda aplicación $f\colon X \to M$ admite una única extensión $f^*\colon F \to M$ en un morfismo de A-módulos.

Definición 8.13: Sea G un grupo abeliano, definimos su *subgrupo de torsión* como

$$\mathsf{T}(G) := \{x \in G : \operatorname{ord} x \neq 0\},$$

o equivalentemente es el subgrupo de los x tales que alguna potencia no nula sea el neutro. G se dice un *grupo de torsión* si $\mathsf{T}(G) = G$; y se dice *libre de torsión* si $\mathsf{T}(G) = \{1\}$.

Ejemplo. Todo grupo abeliano finito es un grupo de torsión. $(\mathbb{Z}, +)$ es libre de torsión. $(\mathbb{R}^\times, \cdot)$ es tal que $\mathsf{T}(\mathbb{R}^\times) = \{\pm 1\}$, así que ni es de torsión ni es libre de torsión.

Proposición 8.14: Para todo G, H abelianos, se cumplen:

1. $G/\mathsf{T}(G)$ es libre de torsión.
2. Si $G \cong H$, entonces $\mathsf{T}(G) \cong \mathsf{T}(H)$ y $G/\mathsf{T}(G) \cong H/\mathsf{T}(H)$.

Teorema 8.15: Se cumplen las siguientes:

1. Todo grupo abeliano finitamente generado y libre de torsión es un grupo abeliano libre. En consecuencia dicho grupo será isomorfo a $\mathbb{Z}^n$ para algún n.
2. Todo subgrupo H de un grupo abeliano libre finitamente generado G es también abeliano libre y además $\operatorname{rank} H \leq \operatorname{rank} G$.
3. (AE) Todo subgrupo H de un grupo abeliano libre G es también abeliano libre y además $\operatorname{rank} H \leq \operatorname{rank} G$.

Demostración:

1. La demostración es por inducción sobre la cantidad de generadores $\langle x_1, \ldots, x_n\rangle$ del grupo G. Claramente se satisface el caso base $n = 1$.

   Para el caso inductivo, sea $G := \langle x_1, \ldots, x_n, x_{n+1}\rangle$ y sea

   $$H := \{g \in G : \exists m \in \mathbb{Z}_{\neq 0}\ mg \in \langle x_{n+1}\rangle\}.$$

   Claramente $H \leq G$, y G/H es un grupo abeliano, libre de torsión (¿por qué?) que está generado por $\{[x_1], \ldots, [x_n]\}$, por lo que, por hipótesis inductiva, es un grupo abeliano libre. En consecuencia, basta probar que H sea también abeliano libre.

Sea $g \in H$, y sea $m \in \mathbb{Z}_{\neq 0}$ tal que $mg \in \langle x_{n+1} \rangle$, de modo que existe $r \in \mathbb{Z}$ tal que $rx_{n+1} = mg$; definamos $\varphi\colon H \to \mathbb{Q}$ dado por $\varphi(g) := r/m$. Nótese que φ está bien definido: En efecto, si $r'x_{n+1} = m'g$ con r', m' distintos, entonces $r'rx_{n+1} = m'mg$, pero x_{n+1}, g tienen orden 0, así que necesariamente $r'r = m'm$ y $r'/m' = r/m$. Además φ es un homomorfismo de grupos inyectivo (¿por qué?), así que basta probar que todo subgrupo finitamente generado F de $\mathbb{Q}$ sea abeliano libre para poder concluir éste inciso.

Sea $F := \langle a_1/b_1, \ldots, a_r/b_r \rangle \leq \mathbb{Q}$. Y sea $d := \prod_{i=1}^{n} b_i$, entonces $f\colon D \to \mathbb{Z}$ dado por $f(x) := dx$ es un homomorfismo de grupos bien definido, dado que d «limpia todos los denominadores», pero más aún, como D es libre de torsión, entonces $\ker f$ es trivial y, por lo tanto, f es inyectivo; luego f es un encaje, i.e., un isomorfismo con un subgrupo de $\mathbb{Z}$. Pero todos los subgrupos de $\mathbb{Z}$ son ideales de $\mathbb{Z}$ que son además principales, por lo que $U \cong \{0\}$ o $U \cong n\mathbb{Z} \cong \mathbb{Z}$.

2. Basta notar que todo grupo abeliano libre puede verse como un $\mathbb{Z}$-módulo libre y que $\mathbb{Z}$ es un DIP para aplicar el teorema 8.11. □

Corolario 8.16: Se cumplen:

1. Todo grupo abeliano finitamente generado G puede escribirse como
$$G = \mathsf{T}(G) \oplus F$$
donde F es un grupo abeliano libre finitamente generado.

2. Dados G, H abelianos y finitamente generados. Entonces $G \cong H$ syss $\mathsf{T}(G) \cong \mathsf{T}(H)$ y $\operatorname{rank}(G/\mathsf{T}(G)) \cong \operatorname{rank}(H/\mathsf{T}(H))$.

8.2 Formas canónicas

En ésta sección trabajaremos exclusivamente con espacios vectoriales de dimensión finita.

Daremos varias definiciones para endomorfismos lineales, y nos daremos la libertad de asumir que las definiciones también aplicar singularmente a matrices mediante el endomorfismo $\boldsymbol{v} \mapsto \boldsymbol{v} \cdot B$.

Definición 8.17: Sea $T\colon V \to V$ una función lineal, si existe $\boldsymbol{v} \in V_{\neq \vec{0}}$ tal que $T(\boldsymbol{v}) = \lambda \boldsymbol{v}$ para algún $\lambda \in k$, entonces se dice que $\boldsymbol{v}$ es un *autovector* y λ es su *autovalor* asociado.

Denotamos por $\sigma(T)$ al conjunto de los autovalores de T.

Teorema 8.18: Dado $A \in \mathrm{Mat}_n(k)$, se cumple que λ es autovalor de A syss $\det(\lambda I_n - A) = 0$.

Demostración: Sea λ el autovalor asociado a $\boldsymbol{v} \in V_{\neq \vec{0}}$, es decir, $\boldsymbol{v}A = \lambda \boldsymbol{v}$. Luego $\boldsymbol{v} \cdot (\lambda I_n - A) = \vec{0}$, por lo que $\lambda I_n - A$ no es inversible y $\det(\lambda I_n - A) = 0$. El recíproco es análogo. □

Definición 8.19: Dado $A \in \mathrm{Mat}_n(k)$, se define

$$\psi_A(x) := \det(xI_n - A) \in k[x]$$

llamado el *polinomio característico* de A.

Ahora el teorema anterior se reescribe como que λ es autovalor de A syss λ es raíz de ψ_A.

Corolario 8.20: Toda matriz de $n \times n$ posee a lo más n autovalores.

Teorema 8.21: Son equivalentes:

1. k es algebraicamente cerrado.
2. Toda matriz cuadrada con coeficientes en k tiene un autovector.

Demostración: Claramente $1 \implies 2$, veremos la recíproca: Para ello basta probar por inducción que todo polinomio está asociado al polinomio característico de una matriz. En particular el polinomio característico de

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

es

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$ □

Lema 8.22: Sea $A \in \mathrm{Mat}_n(k)$, entonces $\psi_A(x)$ es un polinomio mónico y el coeficiente que acompaña al monomio x^{n-1} es $-(a_{11} + a_{22} + \cdots + a_{nn}) = -\operatorname{tr}(A)$.

Proposición 8.23: Sea $A \in \mathrm{Mat}_n(\overline{k})$, tal que sus autovalores son $\alpha_1, \ldots, \alpha_n$ (contando multiplicidades), entonces

$$\mathrm{tr}(A) = -\sum_{i=1}^{n} \alpha_i, \qquad \det(A) = \prod_{i=1}^{n} \alpha_i.$$

Definición 8.24: Se dice que dos matrices $A, B \in \mathrm{Mat}_n(k)$ son *similares* si existe $C \in \mathrm{GL}(n,k)$ tal que $A = C^{-1}BC$.

Proposición 8.25: Dadas dos matrices $A, B \in \mathrm{Mat}_n(k)$ que son similares se cumple que $\psi_A = \psi_B$.

Demostración: Sea $C \in \mathrm{GL}(n,k)$ tal que $A = C^{-1}BC$, luego $\det(xI - A) = \det(xC^{-1}IC - C^{-1}BC) = \det(C^{-1})\det(xI - B)\det(C)$. □

Definición 8.26: Se dice que una matriz $A \in \mathrm{Mat}_n(k)$ es *diagonalizable* si es similar a una matriz diagonal. Equivalentemente, un endomorfismo es diagonalizable si su representación matricial en alguna base es diagonal.

Teorema 8.27: Una matriz A es diagonalizable syss el conjunto de sus autovectores genera el espacio. En cuyo caso, A es similar a $\mathrm{diag}(\alpha_1, \ldots, \alpha_n)$, donde los α_i's son los autovalores (contando multiplicidad) de la matriz.

Demostración: $\Longleftarrow$. Sean S los autovectores de A. Si $\mathrm{Span}\, S = V$, entonces existe $B \subseteq S$ base y claramente $\mathrm{M}_B^B(A) = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$.

$\Longrightarrow$. Sea $B := C^{-1}AC = \mathrm{diag}(\beta_1, \ldots, \beta_n)$, entonces $\boldsymbol{e}_1 B = \beta_1 \boldsymbol{e}_1$, $\boldsymbol{e}_2 B = \beta_2 \boldsymbol{e}_2$ y así. Por lo que, definiendo $\boldsymbol{v}_i := \boldsymbol{e}_i C^{-1}$ se obtiene que $\boldsymbol{v}_i$ son autovectores de A que generan el espacio y que los β_i's eran efectivamente los autovalores de A. □

8.3 Formas bilineales

Volvemos al contexto general de módulos. Recordemos lo siguiente:

Definición 8.28: Sea A un dominio. Una forma bilineal sobre un A-módulo M es una aplicación

$$\beta \colon M \times M \longrightarrow A$$

tal que β es lineal en cada coordenada.

Se dice que una forma bilineal β es *no degenerada* si para todo homomorfismo de R-módulos $\varphi\colon M \to R$ se cumple que existe un único $\boldsymbol{x}_0$ tal que $\varphi(\boldsymbol{y}) = \beta(\boldsymbol{x}_0, \boldsymbol{y})$; y que existe un único $\boldsymbol{y}_0$ tal que $\varphi(\boldsymbol{x}) = \beta(\boldsymbol{x}, \boldsymbol{y}_0)$. En cuyo caso, se dice que la forma bilineal es un *producto interno* y se suele denotar $\beta(\boldsymbol{x}, \boldsymbol{y}) =: \boldsymbol{x} \cdot \boldsymbol{y}$.

Si β es una forma bilineal (resp. producto interno) sobre M, decimos que el par (M, β) es un *A-módulo de forma bilineal* (resp. *A-módulo de producto interno*). De no haber ambigüedad sobre los signos omitiremos el β.

Un homomorfismo $f\colon (M, \beta) \to (M', \beta')$ de A-módulos de forma bilineal es un homomorfismo de A-módulos $f\colon M \to M'$ tal que

$$\beta'(f(x), f(y)) = \beta(x, y).$$

Proposición 8.29: Los A-módulos de forma bilineal (como objetos) y los homomorfismos entre ellos (como flechas) conforman una categoría, denotada Bil_A.

Ésto permite una definición natural de isomorfismo de A-módulos de forma bilineal. Además existe un claro funtor olvidadizo a la categoría de A-módulos, pero no haremos mucho uso de ambos hechos.

Definición 8.30: Un A-módulo de producto interno (M, β) se dice un *espacio de producto interno* si M es un A-módulo finitamente generado y proyectivo.

§8.3.1 Módulos libres de forma bilineal.

Definición 8.31: Sea (M, β) un A-módulo libre de forma bilineal de rango finito. Sea $X = (x_1, \ldots, x_n)$ una base ordenada de M, entonces llamamos *representación matricial de β* a la matriz

$$\mathrm{M}_X(\beta) := [\beta(x_i, x_j)]_{ij}.$$

Proposición 8.32: Sea (M, β) un A-módulo libre de forma bilineal de rango finito y sea B su representación matricial en alguna base ordenada. Entonces β es una forma bilineal (anti)simétrica syss B es una matriz (anti)simétrica.

Proposición 8.33: Sea (M, β) un A-módulo libre de forma bilineal de rango finito. Sean X, Y dos bases ordenadas de M y sea $A := \mathrm{M}_X^Y(\mathrm{Id})$ la matriz de cambio de base, entonces

$$\mathrm{M}_Y(\beta) = A \cdot \mathrm{M}_X(\beta) \cdot A^t.$$

Demostración: Sea $A = [a_{ij}]_{ij}$, de modo que $y_i = \sum_{j=1}^n a_{ij}x_j$. Luego nótese que

$$\begin{aligned}\big(\mathrm{M}_Y(\beta)\big)_{ij} = \beta(y_i, y_j) = \beta\left(\sum_{k=1}^n a_{ik}x_k, y_j\right) &= \sum_{k=1}^n a_{ik}\beta(x_k, y_j) \\ &= \sum_{k=1}^n a_{ik} \cdot \left(\sum_{\ell=1}^n a_{j\ell}\beta(x_k, x_\ell)\right) \\ &= \sum_{k=1}^n a_{ik} \cdot \left(\sum_{\ell=1}^n \beta(x_k, x_\ell)(A^t)_{\ell j}\right) = \big(A \cdot \mathrm{M}_X(\beta) \cdot A^t\big)_{ij}. \qquad \square\end{aligned}$$

Nótese que como, desgraciadamente, aparece la matriz multiplicada por su traspuesta y no por su inversa, inicialmente no tenemos un invariante matricial, salvo por el siguiente:

Lema 8.34: Sea (M, β) un A-módulo libre de forma bilineal de rango finito. β es un producto interno syss su representación matricial en una base (y, por tanto, en todas) es invertible.

Con la proposición anterior, también hemos probado algo más fuerte:

Lema 8.35: Sean (A^n, β) y (A^n, γ) dos A-módulos de formas bilineales. Entonces son isomorfos syss dada una base ordenada X de A^n (e.g., la base canónica) existe una matriz invertible B tal que

$$M_X(\beta) = B \cdot M_X(\gamma) \cdot B^t.$$

Definición 8.36: Sea (M, β) un A-módulo libre de forma bilineal de rango finito. Llamamos *determinante* del producto β, denotado $\det(\beta)$, al elemento $[\det(B)] \in A/(A^\times)^2$, donde B es la representación matricial de β en alguna base ordenada.

Nótese que la necesidad del cociente es para asegurar unicidad. En el capítulo de cuerpos formalmente reales veremos que éste cociente es parti-

cularmente interesante si A es un cuerpo formalmente real, lo que explica la necesidad de elaborar otra teoría para anillos como $\mathbb{C}$.

Definición 8.37: Sea $(e_1, \ldots, e_n)$ la base ordenada de un A-espacio de producto interno. Entonces se le llama base dual $(f_1, \ldots, f_n)$ a la tupla tal que $\beta(e_i, f_j) = \delta_{ij}$.

Proposición 8.38: A toda base ordenada de un A-espacio de producto interno le corresponde una única base dual.

Definición 8.39: Sean $(M_1, \beta_1), \ldots, (M_n, \beta_n)$ un conjunto de A-módulos de forma bilineal. Entonces se define su *suma ortogonal* como el A-módulo $\bigoplus_{i=1}^n M_i$ tal que

$$\beta\big((u_1, \ldots, u_n), (v_1, \ldots, v_n)\big) = \sum_{i=1}^n \beta_i(u_i, v_i).$$

Proposición 8.40: Sean $M_1, \ldots, M_n$ un conjunto de A-módulos de forma bilineal. $\bigoplus_{i=1}^n M_i$ es un espacio de producto interno (de rango finito) syss M_i lo es para todo i (de rango finito). Si son de rango finito, entonces

$$\operatorname{rang}\left(\bigoplus_{i=1}^n M_i\right) = \sum_{i=1}^n \operatorname{rang}(M_i), \quad \det\left(\bigoplus_{i=1}^n M_i\right) = \prod_{i=1}^n \det(M_i).$$

Definición 8.41: Sea M un A-módulo de forma bilineal (anti)simétrica. Sea $N \subseteq M$, entonces llamamos su *complemento ortogonal*, denotado $N^\perp$, al conjunto de los $x \in M$ tales que $\beta(x, y) = 0$ para todo $y \in N$.

Lema 8.42 (de descomposición ortogonal): Sea M un A-módulo de forma bilineal (anti)simétrica. Supongamos que $N \leq M$ es tal que $\beta \restriction N \times N$ es un producto interno, entonces $M \cong N \oplus N^\perp$.

Demostración: Sea $x \in N \cap N^\perp$, entonces $\beta(x, y) = 0$ para todo $y \in N$, de modo que $x = 0$ por ser no degenerada.

Sea $x \in M$, entonces $n \mapsto \beta(x, n)$ es una endomorfismo de A-módulos sobre N y, por lo tanto, existe un único $y \in N$ tal que $\beta(x, n) = \beta(y, n)$ para todo $n \in N$. Sea $z := x - y$, entonces nótese que $\beta(z, n) = 0$ para todo $n \in N$, de modo que $z \in N^\perp$. Finalmente $x = y + z \in N + N^\perp$ como se quería probar. □

Nótese que no se le exige a β ser producto interno en todo M, sino sólo en N.

Teorema 8.43: Sea M un A-módulo de forma bilineal (anti)simétrica. Sean $x_1, \ldots, x_k \in M$ tales que la matriz $[\beta(x_i, x_j)]_{ij} \in \mathrm{Mat}_k(A)$ es invertible, entonces $x_1, \ldots, x_k$ son linealmente independientes y denotando $N := \mathrm{Span}_A(x_1, \ldots, x_k)$ se cumple que

$$M \cong N \oplus N^\perp.$$

Corolario 8.44: Sea M un A-módulo finitamente generado de forma bilineal simétrica. Entonces existe un submódulo $N \leq M$ y existen $a_1, \ldots, a_k \in A^\times$ tales que

$$M \cong \langle a_1 \rangle \oplus \cdots \oplus \langle a_k \rangle \oplus N,$$

donde $\beta(x, x) \notin A^\times$ para todo $x \in N$.

Demostración: Si $\beta(x, x) \notin A^\times$ para todo $x \in M$ entonces estamos listos. Si no, sea $x_1 \in M$ tal que $\beta(x_1, x_1) = a_1$, luego por el lema de descomposición ortogonal

$$M \cong (Ax_1) \oplus (Ax_1)^\perp,$$

y es claro que $Ax_1 \cong \langle a_1 \rangle$ (como espacios de producto interno). Luego procedemos inductivamente y aplicamos el teorema anterior. □

Definición 8.45: Sea M un A-módulo libre de forma bilineal (anti)simétrica. Se dice que $X \subseteq M$ es una *base ortogonal* si es una base y para todo $x, y \in X$ distintos se cumple que $\beta(x, y) = 0$.

Corolario 8.46: Sea A un dominio local en donde $2 \in A^\times$, entonces todo A-espacio de producto interno simétrico posee una base ortogonal.

Demostración: Por el corolario anterior podemos anotar

$$M \cong \langle a_1 \rangle \oplus \cdots \oplus \langle a_k \rangle \oplus N.$$

Luego N es un A-módulo proyectivo sobre un dominio local, ergo es libre (teo. 6.50) y posee una base X, de la que podemos extraer un conjunto finito $e_1, \ldots, e_n$ que posee una base dual $f_1, \ldots, f_n$ y vemos que

$$2 = 2e_1 \cdot f_1 = (e_1 + f_1) \cdot (e_1 + f_1) - e_1 \cdot e_1 - f_1 \cdot f_1,$$

lo que es absurdo pues $2 \in A^\times$. □

§8.3.2 El teorema de Witt.

Definición 8.47: Sea M un A-módulo de forma bilineal simétrica y sea $M \cong N_1 \oplus N_2$. Una *reflexión* de M en torno a (N_1, N_2) es un endomorfismo $r\colon M \to M$ tal que $r(x) = x$ para $x \in N_1$ y $r(y) = -y$ para $y \in N_2$.

En particular, las reflexiones son involuciones, i.e., $r \circ r = \mathrm{Id}_M$. Además, las reflexiones son endomorfismos de Bil, i.e., preservan la forma bilineal:

$$\beta(r(x), r(y)) = \beta(x, y).$$

Lema 8.48: Sea A un dominio local con $2 \in A^\times$, y sea M un A-módulo de forma bilineal simétrica. Entonces:

1. Toda involución que preserva la forma bilineal es una reflexión.
2. Supongamos que $x, y \in M$ satisfacen que

$$\beta(x, x) = \beta(y, y) \in A^\times,$$

entonces existe una reflexión que lleva x a y.

Demostración:

Revisar bien el ejercicio.

1. Ejercicio para el lector.
2. Definamos $u := \frac{x+y}{2}$ y $v := \frac{x-y}{2}$. Nótese que $\beta(u, v) = 0$, de modo que

$$\beta(x, x) = \beta(u, u) + \beta(v, v),$$

luego como A es local, entonces alguno debe ser inversible (¿por qué?). Sin perdida de generalidad, si $\beta(u, u)$ es inversible, entonces $M = (Au) \oplus (Au)^\perp$ y construimos la reflexión apropiada. □

Corolario 8.49: Sea A un dominio local con $2 \in A^\times$, y sea M un A-espacio de producto interno simétrico de rango n. Entonces todo automorfismo $f\colon M \to M$ es la composición de n reflexiones.

Demostración: Basta notar que un automorfismo transforma bases en bases y aplicar inducción. □

Teorema 8.50 – *Teorema de Witt*: Sea A un dominio local con $2 \in A^\times$. Supongamos que M, N, P son A-espacios de producto interno simétrico tales que $M \oplus P \cong N \oplus P$ (en Bil_A), entonces $M \cong N$ (en Bil_A).

Demostración: Podemos escribir P como la suma ortogonal de espacios libres de rango 1, así que, aplicando inducción basta considerar $P = \mathrm{Span}_A(e)$. Sea $f\colon M \oplus P \to N \oplus P$ un isomorfismo arbitrario, luego $f(\vec{0}_M, e)$ y $(\vec{0}_N, e)$ en $N \oplus P$ satisfacen las hipótesis del lema 8.48, de modo que existe una reflexión $r\colon N \oplus P \to N \oplus P$ tal que $r(f(\vec{0}_M, e)) = (\vec{0}_N, e)$. Luego

$$f \circ r\colon M \oplus P \longrightarrow N \oplus P$$

es un isomorfismo que manda el subespacio $P_M := \mathrm{Span}_A\{(\vec{0}_M, e)\}$ en el subespacio $P_N := \mathrm{Span}_A\{(\vec{0}_N, e)\}$ y, por lo tanto, manda los complementos ortogonales $M = P_M^\perp$ en $N = P_N^\perp$. □

§8.3.3 El anillo de Witt.

Lema 8.51: Sean $(M_1, \beta_1), \ldots, (M_n, \beta_n)$ un conjunto de A-módulos de forma bilineal. Existe una única forma bilineal β sobre $N := M_1 \otimes \cdots \otimes M_n$ que satisface que

$$\beta(x_1 \otimes \cdots \otimes x_n, y_1 \otimes \cdots \otimes y_n) = \prod_{i=1}^{n} \beta_i(x_i, y_i)$$

para todos $x_i, y_i \in M_i$.

Demostración: Consideremos que la aplicación

$$\begin{aligned} \phi\colon M_1 \times \cdots \times M_n \times M_1 \times \cdots \times M_n &\longrightarrow A \\ (x_1, \ldots, x_n, y_1, \ldots, y_n) &\longmapsto \prod_{i=1}^{n} \beta_i(x_i, y_i) \end{aligned}$$

es $2n$-multilineal, de modo que induce un homomorfismo de A-módulos

$$M_1 \otimes \cdots \otimes M_n \otimes M_1 \otimes \cdots \otimes M_n = N \otimes N \longrightarrow A$$

el cual es único. Nótese que ϕ también se extiende a una aplicación $N \times N \to A$ bilineal que coincide con β cuya extensión es la misma aplicación superior. Ésto comprueba el enunciado. □

Lema 8.52: Si $M_1, \ldots, M_n$ son A-espacios de producto interno, entonces $M_1 \otimes \cdots \otimes M_n$ también lo es.

Demostración: Nótese que el producto tensorial de finitos módulos finitamente generados proyectivos es finitamente generado y también es proyectivo (por el corolario 5.70). Denotemos por $M^* := \mathrm{Hom}_A(M, A)$. Luego cada producto interno β_i da lugar a un isomorfismo:

$$\begin{aligned} \bar{\beta}_i \colon M_i &\longrightarrow M_i^* \\ x &\longmapsto (y \overset{\bar{\beta}_i(x)}{\mapsto} \beta_i(x, y)) \end{aligned}$$

Luego, si $\eta \colon M_1^* \otimes \cdots \otimes M_n^* \to (M_1 \otimes \cdots \otimes M_n)^*$ es el isomorfismo canónico, entonces podemos definir el siguiente homomorfismo de A-módulos:

$$\bar{\beta} := (\bar{\beta}_1 \otimes \cdots \bar{\beta}_n) \circ \eta \colon M_1 \otimes \cdots \otimes M_n \longrightarrow (M_1 \otimes \cdots \otimes M_n)^*,$$

de modo que se comprueba el enunciado. □

Definición 8.53: Se dice que un A-espacio de producto interno simétrico M es un *A-espacio metabólico*[1] si existe $N \leq M$ tal que $N = N^\perp$ y N es un sumando directo de M.

Lema 8.54: Sean M, M' dos A-espacios metabólicos y (N, β) un A-espacio de producto interno arbitrario. Entonces:

1. $M \oplus M$ es metabólico.
2. $M \otimes_A N$ es metabólico.
3. $(N, \beta) \oplus (N, -\beta)$ es metabólico.

Demostración: Para la última sólo basta notar que $M := \langle 1 \rangle \oplus \langle -1 \rangle$ es metabólico y que

$$M \otimes_A N = (N, \beta) \oplus (N, -\beta).$$ □

Lema 8.55: Sea A un anillo en donde todo A-módulo finitamente generado proyectivo es libre (e.g., un cuerpo, un DIP o un dominio local). Un

[1] Knebusch [**0,** pág. 122] emplea «metabólico», mientras que Milnor [**15,** pág. 12] emplea «se escinde» (eng. *split*).

A-espacio de producto interno es metabólico syss la representación de su producto interno es de la forma

$$\begin{bmatrix} \mathbf{0} & I \\ I & B \end{bmatrix}$$

para alguna base. Más aún, si $2 \in A^\times$, entonces podemos elegir la base de modo que $B = \mathbf{0}$.

Demostración: Sea M un A-espacio metabólico que, por hipótesis, es un A-módulo libre de rango finito. Sea $N \leq M$ un sumando directo, el cual es libre, y sea $e_1, \ldots, e_n$ una base para N, la cual podemos extender a una base $e_1, \ldots, e_m$ para M, y sea $f_1, \ldots, f_m$ su base dual.

Claramente, podemos restringir la base dual a $f_{n+1}, \ldots, f_{2n}$ que es base para $N^\perp = N$, de modo que podemos sustituir los elementos y obtener la siguiente base de M:

$$X := (e_1, \ldots, e_n, f_1, \ldots, f_n).$$

Un mero cálculo comprueba que $\mathrm{M}_X(\beta) = \left[\begin{smallmatrix} \mathbf{0} & I \\ I & B \end{smallmatrix}\right]$ y el recíproco es claro.

Supongamos que $2 \in A^\times$ y definamos la matriz $C := -\frac{1}{2}B$ de modo que

$$\begin{bmatrix} I & \mathbf{0} \\ C & I \end{bmatrix} \begin{bmatrix} \mathbf{0} & I \\ I & B \end{bmatrix} \begin{bmatrix} I & \mathbf{0} \\ C & I \end{bmatrix}^t = \begin{bmatrix} \mathbf{0} & I \\ I & \mathbf{0} \end{bmatrix}. \qquad \square$$

Definición 8.56: Dos A-espacios de producto interno simétrico N_1, N_2 se dice que pertenecen a la misma clase de Witt, denotado $N_1 \sim N_2$, si existen dos espacios metabólicos M_1, M_2 tales que $N_1 \oplus M_1 \cong N_2 \oplus M_2$. Se denota por $W(A)$ el conjunto de todas las clases de Witt.

Lema 8.57: Sean $M \sim M'$ y $N \sim N'$, entonces $M \oplus N \sim M' \oplus N'$ y $M \otimes_A N \sim M' \otimes_A N'$.

Recordemos que $(M, \beta) \oplus (M, -\beta) \sim 0$ y $M \otimes_A \langle 1 \rangle \sim M$, ésto, combinado con el trabajo anterior nos comprueba lo siguiente:

Teorema 8.58: $W(A)$ es un dominio (i.e., anillo unitario conmutativo) donde $1 = [\langle 1 \rangle]$, $[M] + [N] = [M \oplus N]$ y $[M] \cdot [N] = [M \otimes_A N]$.

Por ello, a $W(A)$, se le llama el *anillo de Witt* de A.

9

Teoría espectral

9.1 Diagonalización

En esta sección se desarrollan varios resultados para endomorfismos sobre espacios vectoriales de dimensión finita, nótese que toda B puede verse como el endomorfismo $x \mapsto Bx$, así que obviaremos mencionar cosas como "ésta definición se aplica para matrices así...".

Definición 9.1 – *Subespacio f-invariante*: Dado un módulo M, $f \in \mathrm{End}(M)$ y un subespacio S de M, se dice que S es f-invariante si $f[S] \subseteq S$.

Proposición 9.2: Para todo $f \in \mathrm{End}(M)$ se cumple que son subespacios f-invariantes:

1. El subespacio nulo $\{\mathbf{0}\}$.
2. Todo subespacio de $\ker f$.
3. Todo subespacio que contenga a $\mathrm{Img}\, f$.

Lema 9.3: Si $f \in \mathrm{End}(\Bbbk^n)$ y X, Y son bases ordenadas cualesquiera de $\Bbbk^n$, entonces para todo $x \in \Bbbk$

$$\det(xI_n - \mathrm{M}_X^X(f)) = \det(xI_n - \mathrm{M}_Y^Y(f))$$

Demostración: Como hemos visto

$$\mathrm{M}_Y^Y(f) = \mathrm{M}_Y^X(\mathrm{Id})\,\mathrm{M}_X^X(f)\,\mathrm{M}_X^Y(\mathrm{Id}),$$

luego si llamamos $B := \mathrm{M}_X^Y(\mathrm{Id})$ (que es invertible), cumple que

$$\mathrm{M}_Y^Y(f) = B^{-1}\,\mathrm{M}_X^X(f)B,$$

luego

$$\begin{aligned}\det(xI_n - \mathrm{M}_Y^Y(f)) &= \det(xI_n - B^{-1}\,\mathrm{M}_X^X(f)B)\\ &= \det(B^{-1}(xI_n - \mathrm{M}_X^X(f))B) = \det(xI_n - \mathrm{M}_X^X(f)).\end{aligned}$$

□

Definición 9.4 – *Polinomio característico*: Si $f \in \mathrm{End}(\Bbbk^n)$, entonces dada una base X cualquiera se define

$$p_f(x) := \det(xI_n - \mathrm{M}_X^X(f))$$

conocido como el *polinomio característico* de f.

Definición 9.5: Si M es un A-módulo y $f \in \mathrm{End}(M)$, entonces $v \in M_{\neq 0}$ se dice un *autovector* de f si $\mathrm{Span}\{v\}$ es f-invariante, o tradicionalmente, si existe $\alpha \in M$ tal que $f(v) = \alpha v$, en cuyo caso se dice que α es el *autovalor* asociado a v de f. Si $M = A^n$ y $B \in \mathrm{Mat}_n(A)$, entonces se definen los autovalores y autovectores de B a aquellos correspondientes a la función $f(v) := Bv$.
Una transformación lineal f se dice *diagonalizable* si existe una base ordenada X tal que $\mathrm{M}_X^X(f)$ es una matriz diagonal.
Se le llama *espectro* de f, denotado por $\sigma(f)$ al conjunto de sus autovalores.

Teorema 9.6: Un escalar $\lambda \in \sigma(f)$ syss $p_f(\lambda) = 0$.

Definición 9.7: Sea $f \in \mathrm{End}(V)$. Si $\alpha \in \Bbbk$, entonces se les llaman *autoespacio* y *autoespacio generalizado* generado por α de f a:

$$V_\alpha^f := \{v \in V : f(v) = \alpha v\}, N_\alpha^f := \{v \in V : \exists r \geq 0\ (f - \alpha\,\mathrm{Id})^r v = 0\};$$

de no haber ambigüedad se obvia el "f".

Para un $\alpha \in \Bbbk$ se le dice *multiplicidad geométrica* y *algebraíca* resp., a $\dim V_\alpha$ y $\dim N_\alpha$.

Proposición 9.8: Para todo $f \in \mathrm{End}(\Bbbk^n)$ y todo $\alpha \in \Bbbk$ se cumple:

1. V_α y N_α son submódulos o subespacios vectoriales de $\Bbbk^n$.
2. $V_\alpha \leq N_\alpha$.
3. V_α y N_α son f-invariantes.
4. La multiplicidad geométrica de α siempre es menor o igual a su multiplicidad algebraíca.
5. α es autovalor syss tiene multiplicidad geométrica no nula syss tiene multiplicidad algebraíca no nula.

Definición 9.9 – *Endomorfismo nilpotente*: Se dice que $f \in \mathrm{End}(V)$ es *nilpotente de grado* n si $f^{n-1} \neq 0$ y $f^n = 0$. Análogo para matrices cuadradas.

El estudio de endomorfismos nilpotentes es relevante pues si λ es autovalor de f, entonces $f - \lambda \,\mathrm{Id}$ restringido al autoespacio N_λ es nilpotente.

Proposición 9.10: Sea $f \in \mathrm{End}(V)$:

1. Si f es nilpotente y su campo escalar es un dominio íntegro, entonces todos sus autovalores son nulos.
2. Si $\lambda \in \sigma(f)$, entonces $(f - \lambda \,\mathrm{Id})$ es nilpotente en N_λ.

Proposición 9.11: Sea V un módulo sobre un dominio íntegro y $f \in \mathrm{End}(V)$. Si $\alpha \neq \beta$, entonces $f - \alpha \,\mathrm{Id}$ es inyectiva en N_β. Y si el último es de dimensión finita, entonces $f - \alpha \,\mathrm{Id}$ es biyección.

Demostración: Sea $v \in N_\beta$ tal que $(f - \alpha \,\mathrm{Id})v = 0$, luego se cumple que

$$(f - \beta \,\mathrm{Id})v = (\alpha - \beta)v.$$

Si $v = 0$ entonces $f - \alpha \,\mathrm{Id}$ es inyectiva, como se quería probar. Si $v \neq 0$, entonces v es autovector de $(f - \beta \,\mathrm{Id})$ con autovalor $\alpha - \beta \neq 0$. Pero $(f - \beta \,\mathrm{Id})$ es nilpotente en N_β, luego sólo posee autovalores nulos, contradicción. □

Teorema 9.12: Sea V un módulo sobre un dominio íntegro y $f \in \mathrm{End}(V)$. Si $\alpha_1, \ldots, \alpha_n$ son escalares distintos, entonces sus autoespacios generalizados son independientes. En consecuencia, sus autoespacios comúnes también lo son.

DEMOSTRACIÓN: La demostración es por inducción sobre n. El caso base $n = 1$ es trivial. Sean $v_i \in N_{\alpha_i}$ tales que

$$v_1 + \cdots + v_n + v_{n+1} = 0,$$

por definición existe $r > 0$ tal que

$$(f - \alpha_{n+1} \operatorname{Id})^r v_{n+1} = 0,$$

luego aplicando la función al resto de v_is se obtiene que

$$(f - \alpha_{n+1} \operatorname{Id})^r v_1 + \cdots + (f - \alpha_{n+1} \operatorname{Id})^r v_n = 0,$$

que corresponde al paso inductivo, puesto que N_{α_i} son invariantes; por lo tanto para todo $i \in \{1, \ldots, n\}$:

$$(f - \alpha_{n+1} \operatorname{Id})^r v_i = 0.$$

Finalmente aplicamos la proposición anterior que dice que $(f - \alpha_{n+1} \operatorname{Id})^r$ es biyección en N_{α_i} para deducir que $v_i = 0$. □

Corolario 9.13: Sea $f \in \mathrm{End}(\Bbbk^n)$. Si f posee n autovalores distintos, entonces es diagonalizable.

Teorema 9.14: Un endomorfismo es diagonalizable syss existe una base formada por sus autovectores.

Teorema 9.15: Son equivalentes:

1. $\Bbbk$ es algebraicamente cerrado.

2. Toda matriz cuadrada con coeficientes en $\Bbbk$ tiene un autovector.

DEMOSTRACIÓN: Claramente 1 $\implies$ 2, veremos la recíproca: Para ello basta probar por inducción que todo polinomio está asociado al polinomio

característico de una matriz. En particular el polinomio característico de

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

es

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

□

Definición 9.16: Se dice que un endomorfismo $f \in L(\mathbb{k}^n)$ es *triangularizable* syss existe una base ordenada X tal que su representación matricial es triangular. En el caso de matrices cuadradas, si existe $C \in \mathrm{Mat}_n(\mathbb{k})$ tal que $C^{-1}BC$ es triangular.

Teorema 9.17: Para un endomorfismo sobre V, son equivalentes:

1. f es triangularizable.
2. Existe una cadena maximal de subespacios f-invariantes:

$$0 =: V_0 \subset V_1 \subset \cdots \subset V_n := V$$

Demostración: 1) $\implies$ 2). Si f es triangularizable, entonces sea $X := (x_1, \ldots, x_n)$ la base para la que f es triangular. Luego la cadena viene dada por $V_k := \langle x_1, \ldots, x_k \rangle$.
2) $\implies$ 1). Basta ir formando la base a partir de puntos en los V_k, tomamos un vector no nulo en V_1, luego $x_2 \in V_2 \setminus V_1$ y así. □

Ejemplo (matriz triangular no diagonalizable). Consideremos

$$B = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$$

para que B sea diagonalizable ha de existir C invertible tal que $C^{-1}BC$ sea diagonal, es decir:

$$C^{-1}BC = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{\det C}\begin{bmatrix} ad+dc-bc & d^2 \\ -c^2 & ad-bc-cd \end{bmatrix}.$$

luego $c = d = 0$, pero en éste caso $\det C = 0$ lo que es una contradicción.

§9.1.1 El teorema fundamental del álgebra II. Ésta demostración hace uso de cierta noción muy básica de análisis. Aquí aplicaremos una inducción extraña para la cual admitimos la siguiente definición:

> $P(\Bbbk, d, r)$: Todo conjunto $A_1, \ldots, A_r$ de matrices cuyo producto conmuta sobre $\Bbbk^n$ con $d \nmid n$ posee un autovector en común.

Lema 9.18: Si $P(\Bbbk, d, 1)$, entonces para todo $r \geq 1$ se cumple que $P(\Bbbk, d, r)$.

Demostración: Probaremos la propiedad $P(\Bbbk, d, r+1)$ por inducción fuerte sobre la dimensión n del espacio vectorial: El caso $n = 1$ es trivial. Sean $A_1, \ldots, A_r, A_{r+1}$ matrices conmutativas en $\Bbbk^{n+1}$ con $d \nmid n+1$. Como $P(\Bbbk, d, 1)$ se cumple, entonces A_{r+1} tiene un autovalor λ, luego se define $B := A_{r+1} - \lambda I$ y se definen

$$U := \ker(B), \qquad W := \operatorname{Img}(B),$$

que por conmutatividad de los endomorfismos son invariantes para todo A_i (¿por qué?).

Si $U = V$, entonces $A_{r+1} = \lambda v$ para todo $v \in V$, luego todos son autovectores de V, así que cualqueir autovector común de $A_1, \ldots, A_r$ lo es con A_{r+1}.

Si $U \neq V$, entonces como $\dim W + \dim Z = \dim V$ hay alguno que tiene dimensión no divisible por d, sin perdida de generalidad supongamos que es U. Luego, por inducción, $A_1, \ldots, A_{r+1}$ tienen un autovector común en $W \subseteq V$. □

Proposición 9.19: Se cumple que $P(\mathbb{R}, 2, r)$ para todo $r \in \mathbb{N}_{\neq 0}$

Demostración: Para ésto basta ver que $P(\mathbb{R}, 2, 1)$, lo que equivale a ver que toda matriz $B \in \operatorname{Mat}_n(\mathbb{R})$ tiene autovectores para n impar. En este caso, el polinomio característico de B es de grado impar, y todo polinomio de grado impar sobre $\mathbb{R}$ tiene raíces. □

Definición 9.20 – *Matriz hermitiana*: Dada $B \in \operatorname{Mat}_n(\mathbb{C})$, se denota por $B^* := \overline{B}^t$. Se dice que B es *hermitiana* (o *auto-adjunta* en algunos libros) si $B = B^*$.

Corolario 9.21: El conjunto de las matrices hermitianas de $n \times n$ es un $\mathbb{R}$-espacio vectorial de dimensión n^2.

Pista: Recuerde que en la diagonal de una matriz hermitiana sólo pueden ir números reales. □

Lema 9.22: Se cumple que $P(\mathbb{C}, 2, 1)$.

Demostración: Sea $A \in \mathrm{Mat}_n(\mathbb{C})$ con n impar. Sea V el $\mathbb{R}$-espacio vectorial de las matrices hermitianas de $\mathrm{Mat}_n(\mathbb{C})$. Se definen los endomorfismos sobre V:

$$L_1(B) := \frac{AB + BA^*}{2}, \quad L_2(B) := \frac{AB - BA^*}{2i}.$$

Ésta elección deriva de que

$$AB = \frac{AB + B^*A^*}{2} + \mathrm{i} \cdot \frac{AB - B^*A^*}{2i},$$

aplicando el hecho de que B es hermitiana.
Como V tiene dimensión n^2 impar, y L_1, L_2 son operadores que conmutan (¿por qué?), entonces comparten un autovector $B \in V$ en común, con lo que luego

$$AB = L_1(B) + \mathrm{i}L_2(B) = (\mu + \mathrm{i}\lambda)B,$$

osea B es autovector de A que es lo que se quería probar. □

Teorema 9.23: Para todo $k > 0$ se cumple que $P(\mathbb{C}, 2^k, 1)$. En consecuencia, toda matriz tiene autovalores en $\mathbb{C}$, y $\mathbb{C}$ resulta ser algebraícamente cerrado.

Demostración: Lo probaremos por inducción fuerte sobre k, habiendo ya probado el caso base. Sea $A \in \mathrm{Mat}_n(\mathbb{C})$ con $2^{k-1} \mid n$ y $2^k \nmid n$. Sea V el conjunto de matrices anti-simétricas complejas de orden $n \times n$ (i.e., $B \in V$ syss $B^t = -B$). Se definen los endomorfismos sobre V:

$$L_1(B) := AB - BA^t, \quad L_2(B) := ABA^t$$

que conmutan (¡demuéstrelo!). Nótese que $\dim V = \frac{n(n-1)}{2}$ y cumple que $2^{k-1} \nmid \dim V$, luego por hipótesis inductiva existe B autovector común, de modo que

$$L_2(B) = \mu B = A(BA^t) = A(AB - L_1(B)) = A(AB - \lambda B)$$

luego despejando B se obtiene que

$$(A^2 - \lambda A + \mu I)B = 0,$$

tomando alguna columna no nula $\boldsymbol{v}$ de B se tiene que

$$(A^2 - \lambda A + \mu I)\boldsymbol{v} = 0.$$

Como en $\mathbb{C}$ todo polinomio cuadrático se escinde se tiene que existen $\alpha, \beta \in \mathbb{C}$ tales que $x^2 - \lambda x - \mu = (x - \alpha)(x - \beta)$. Por lo que, en conclusión:

$$(A - \alpha I)(A - \beta I)\boldsymbol{v} = 0$$

Luego o $(A - \beta I)v = 0$ con lo que v es autovector de A, o $(A - \beta I)v$ es autovector de A. □

§9.1.2 Teorema de Cayley-Hamilton. Si A es un dominio, entonces hemos probado que $A[x]$ también lo es. Usando ésto realizaremos comparaciones entre dos tipos de espacios cursiosos: $\mathrm{Mat}_n(A[x])$, es decir, el conjunto de matrices del anillo $A[x]$ de los polinomios de A; y $(\mathrm{Mat}_n A)[x]$, es decir, el conjunto de polinomios con coeficientes matrices de A.

Por ejemplo, un elemento de $\mathrm{Mat}_2(\mathbb{Z}[x])$ podría ser

$$\begin{bmatrix} x^2 + 1 & 3x \\ x^3 - 2x & 0 \end{bmatrix}$$

y un elemento de $(\mathrm{Mat}_2 \mathbb{Z})[x]$ podría ser

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 3 \\ -2 & 0 \end{bmatrix} X + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} X^2 + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} X^3.$$

Queremos probar que son isomorfos. Para ello admitimos el convenio de que $r_p(f)$ es el coeficiente que acompaña a la x, o que si f es de grado n, entonces $f(x) = \sum_{p=0}^{n} r_p(f)x^p$. Si $F \in \mathrm{Mat}_n(A[x])$ entonces convenimos que $[r_p(F)]_{i,j} := r_p(F_{i,j})$ (en general denotaremos elementos de $\mathrm{Mat}_n(A[x])$ con letras mayúsculas).

Proposición 9.24: Sean $F, G \in \mathrm{Mat}_n(A[x])$, entonces para todo k:

1. $r_p(F + G) = r_p(F) + r_p(G)$.
2. $r_p(F \cdot G) = \sum_{\ell=0}^{p} r_\ell(F) r_{p-\ell}(G)$

Demostración: La primera es trivial, la segunda tiene la misma forma que los coeficientes del producto de polinomios y es el resultado de una manipulación algebraíca:

$$(r_p(F \cdot G))_{ij} = r_p((F \cdot G)_{ij}) = r_p\left(\sum_{k=1}^{n} F_{ik} G_{kj}\right)$$

$$= \sum_{k=1}^{n} r_p(F_{ik}G_{kj}) = \sum_{k=1}^{n}\sum_{\ell=0}^{p} r_\ell(F_{ik})r_{p-\ell}(G_{kj})$$
$$= \sum_{\ell=0}^{p}\sum_{k=1}^{n}[r_\ell(F)]_{ik}[r_{p-\ell}(G)]_{kj} = \sum_{\ell=0}^{p} r_\ell(F)r_{p-\ell}(G).$$

□

Teorema 9.25:

$$\mathrm{Mat}_n(A[x]) \cong (\mathrm{Mat}_n\, A)[x]$$

Teorema 9.26 – *Teorema de Cayley-Hamilton*: Si B es una matriz cuadrada de polinomio característico $p_B(x) = a_0 + a_1x + \cdots + a_nx^n$, entonces

$$p_B(B) = a_0I + a_1B + \cdots + a_nB^n = 0.$$

Demostración: Sea $\varphi : \mathrm{Mat}_n(A[x]) \to (\mathrm{Mat}_n\, A)[x]$ el isomorfismo canónico. Sabemos que se define

$$p_B(x) := \det(xI - B),$$

y que

$$(\mathrm{adj}\, B)B = \det(B)I$$

de modo que

$$\mathrm{adj}(xI - B)(xI - B) = p_B(x)I$$

notemos que ésta es una relación sobre $\mathrm{Mat}_n(A[x])$ (pues la matriz a la derecha tiene por coordenadas polinomios), luego por el teorema anterior se cumple que se traduce a $(\mathrm{Mat}_n\, A)[X]$:

$$\mathrm{adj}(X - B)(X - B) = p_B(X),$$

finalmente por regla de Ruffini como $X - B$ divide a $p_B(X)$ se cumple que $X = B$ es raíz de $p_B(X)$. □

9.2 Espacios duales

Dado un $\Bbbk$-espacio vectorial V, entonces $V^* := L(V, \Bbbk)$ es el espacio formado por funcionales lineales desde V.

Ésta demostración es de **[25].**

Proposición 9.27: Se cumple:

1. Si $\dim V < \infty$ entonces $\dim V = \dim V^*$.
2. Existe un monomorfismo canónico $\iota : V \to V^*$ tal que establece un isomorfismo entre V y $\iota[V]$.
3. (AEN) Si $\dim V$ es infinito, entonces $\dim V < \dim V^*$.

Demostración: La primera es trivial, probaremos la segunda: Consideremos que $\{\boldsymbol{e}_i\}_{i\in I}$ es base de V, de modo que $\dim V = |I|$. Para construir el monomorfismo, definimos $\iota(\boldsymbol{e}_i)$ como el funcional tal que $[\iota(\boldsymbol{e}_i)](\boldsymbol{e}_j) = \delta_{ij}$. Luego al extender linealmente a ι le definimos sobre todo V y vemos que la imágen sobre la base genera un conjunto linealmente independiente en V^*. Claramente ι es inyectiva y prueba que $\dim V \leq \dim V^*$ en todo caso.

Para probar la tercera probaremos varios pasos:

1. **Si $\Bbbk \leq \aleph_0$, entonces $|V| = |I|$:**
   Claramente $|V| \geq |I|$, así que veremos la otra implicancia. Veamos que V puede ser visto como un subconjunto de S, donde S es la familia de subconjuntos finitos de $\Bbbk \times I$, por lo que,
   $$|V| \leq |S| = \left|[\Bbbk \times I]^{<\aleph_0}\right| = |\aleph_0| \cdot |\Bbbk \times I| = |I|.$$
2. **Si $\Bbbk \leq \aleph_0$, entonces $\dim V < \dim V^*$:**
   Simple: como toda función lineal viene determinada exclusivamente por los valores en la base, se cumple que
   $$|V| = |\operatorname{Func}(I;\Bbbk)| = |\Bbbk|^{|I|} \geq 2^{|I|} > |I| = |V|$$
   donde la última desigualdad es el teorema de cardinalidad de Cantor.
3. **Caso arbitrario:**
   Notemos que $\Bbbk$, por ser un cuerpo, siempre contiene a otro cuerpo
   $$F := \begin{cases} \mathbb{Q}, & \operatorname{car}\Bbbk = 0 \\ \mathbb{F}_p, & \operatorname{car}\Bbbk = p \end{cases}$$
   Luego si $W := \operatorname{Span}_F(\boldsymbol{e}_i)_{i\in I}$ vemos que $\dim_F W = \dim_\Bbbk V$, y sabemos que $\dim_F W < \dim_k W^*$, así que basta probar que $\dim_F W^* \leq \dim_\Bbbk V^*$.

   Sea $G \in L_F(W^*, V^*)$ definida así: Sea $\varphi \in W^*$, es decir, $\varphi : W \to F$ es F-lineal y queremos que $G(\varphi) : V \to \Bbbk$ sea $\Bbbk$-lineal. Sea $\boldsymbol{v} \in V$, existe

$(\lambda_i)_{i\in I} \in \Bbbk$ tal que es nula excepto en finitos índices y $\boldsymbol{v} = \sum_{i\in I} \lambda_i \boldsymbol{e}_i$. Luego se define

$$[G(\varphi)](\boldsymbol{v}) = \sum_{i\in I} \lambda_i \varphi(\boldsymbol{e}_i)$$

el cual está bien definido y veamos que todo cumple las condiciones esperadas, dados

$$\boldsymbol{u} = \sum_{i\in I} \alpha_i \boldsymbol{e}_i, \quad \boldsymbol{v} = \sum_{i\in I} \beta_i \boldsymbol{e}_i$$

y dados $\lambda \in \Bbbk$ se cumple

a) Fijada $\varphi \in W^*$ vemos que

$$\begin{aligned}[G(\varphi)](\boldsymbol{u}+\boldsymbol{v}) &= \sum_{i\in I} (\alpha_i + \beta_i)\varphi(\boldsymbol{e}_i) \\ &= \sum_{i\in I} \alpha_i \varphi(\boldsymbol{e}_i) + \sum_{i\in I} \beta_i \varphi(\boldsymbol{e}_i) = [G(\varphi)](\boldsymbol{u}) + [G(\varphi)](\boldsymbol{v}).\end{aligned}$$

Y claramente $[G(\varphi)](\lambda \boldsymbol{v}) = \lambda [G(\varphi)](\boldsymbol{v})$ de modo que $G(\varphi)$ efectivamente es un elemento de V^*.

b) G es efectivamente una aplicación F-lineal (¿por qué?).

c) Si $\boldsymbol{u} \in W$, entonces $\alpha_i \in F$ y se cumple que

$$\varphi(\boldsymbol{u}) = \varphi\left(\sum_{i\in I} \alpha_i \boldsymbol{e}_i\right) = \sum_{i\in I} \alpha_i \varphi(\boldsymbol{e}_i) = [G(\varphi)](\boldsymbol{u})$$

De ésto se deduce que G es inyectiva.

Por ende G comprueba que $\dim_F W^* \leq \dim_F V^*$, pero queremos ver algo más fuerte ...

□

9.3 Formas bilineales

Cuando definimos el determinante nos topamos con la noción de forma multilineal, en este capítulo la retomamos pero sólo admitiendo dos coordenadas.

§9.3.1 Formas bilineales.

Definición 9.28 – *Forma bilineal*: Una forma bilineal $F \in L(V, V; \Bbbk)$ es una forma multilineal de $V \times V$ a $\Bbbk$, donde V es un $\Bbbk$-espacio vectorial. En general también exigiremos que F sea simétrica, es decir, que $F(\boldsymbol{u}, \boldsymbol{v}) = F(\boldsymbol{v}, \boldsymbol{u})$ para todo $\boldsymbol{u}, \boldsymbol{v} \in V$.
Si $\boldsymbol{u}, \boldsymbol{v}$ cumplen que $F(\boldsymbol{u}, \boldsymbol{v}) = 0$ para una forma bilineal simétrica, entonces diremos que son *ortogonales* respecto a F, lo que denotaremos por $\boldsymbol{u} \perp \boldsymbol{v}$.

Sea $B := (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ una base de V, entonces se le llama representación matricial de la forma bilineal F según B a

$$\mathrm{M}_B(F) := [F(\boldsymbol{x}_i, \boldsymbol{x}_j)]_{ij}$$

Si F es una forma bilineal simétrica, decimos que $q : V \to \Bbbk$ definido por $q(\boldsymbol{v}) := F(\boldsymbol{v}, \boldsymbol{v})$ es su *forma cuadrática* asociada.

Proposición 9.29: Dada una forma bilineal F sobre $\Bbbk^n$ con base ordenada B, se cumple que una matriz $M = \mathrm{M}_B(F)$ syss para todo $\boldsymbol{u}, \boldsymbol{v} \in \Bbbk^n$ se cumple que

$$F(\boldsymbol{u}, \boldsymbol{v}) = \pi_B(\boldsymbol{u}) M \pi_B(\boldsymbol{v})^t.$$

Luego si denotamos $(\boldsymbol{u}, \boldsymbol{v}) := \pi_B(\boldsymbol{u})\pi_B(\boldsymbol{v})^t$ para alguna base fijada, como la canónica, entonces toda forma bilineal F corresponde a

$$F(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}A, \boldsymbol{v}) = (\boldsymbol{u}, \boldsymbol{v}A^t)$$

con una matriz A.

Proposición 9.30: Si F es una forma bilineal simétrica, entonces su representación matricial bajo cualquier base también lo es.

Teorema 9.31: Si V es un $\Bbbk$-espacio vectorial con $\operatorname{car} \Bbbk \neq 2$ y $\dim V < \infty$, entonces si F es una forma bilineal simétrica sobre V, V posee una base ortogonal respecto a F.

Demostración: La demostración es por inducción sobre n, la dimensión de V. El caso base es trivial.
Si F es nula, entonces toda base es ortogonal. De lo contrario, sean $\boldsymbol{u}, \boldsymbol{v}$ tales que $F(\boldsymbol{u}, \boldsymbol{v}) \neq 0$, luego si q es su forma cuadrática, entonces

$$q(\boldsymbol{u} + \boldsymbol{v}) = q(\boldsymbol{u}) + 2F(\boldsymbol{u}, \boldsymbol{v}) + q(\boldsymbol{v})$$

de modo que q es no nulo para al menos alguno entre $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u}+\boldsymbol{v}$; sea $\boldsymbol{e}_1$ alguno de ellos. Sea

$$W := \{\boldsymbol{x} \in V : \boldsymbol{x} \perp \boldsymbol{e}_1\}.$$

Vamos a probar que $V = \operatorname{Span}(\boldsymbol{e}_1) \oplus W$: Sea $\boldsymbol{x} \in \operatorname{Span}(\boldsymbol{e}_1) \cap W$, entonces $\boldsymbol{x} = \alpha \boldsymbol{e}_1 \perp \boldsymbol{e}_1$ satisface que $F(\boldsymbol{x}, \boldsymbol{e}_1) = 0 = \alpha F(\boldsymbol{e}_1, \boldsymbol{e}_1)$ de modo que $\alpha = 0$ y $\boldsymbol{x} = \vec{0}$.
Notemos que $\boldsymbol{x} \mapsto F(\boldsymbol{x}, \boldsymbol{e}_1)$ es un funcional lineal (por definición de forma bilineal) suprayectivo y cuyo kernel es W, de modo que por fórmula de dimensiones se cumple que $\dim W = n - 1$, de modo que $\dim(\operatorname{Span}(\boldsymbol{e}_1) \oplus W) = n$ y se comprueba nuestra hipótesis.

Finalmente como W tiene dimensión menor, por hipótesis inductiva, posee base ortogonal $\boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ y añadirle $\boldsymbol{e}_1$ genera una base ortogonal para V. □

Supongamos que sea $(\boldsymbol{e}_i)_i$ una base ortogonal de V según una forma bilineal simétrica F de representación matricial A, entonces si M es la matriz cambio de base a ella, entonces se cumple que

$$F(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}A, \boldsymbol{v}) = ((\boldsymbol{u}M)B, \boldsymbol{v}M) = (\boldsymbol{u}(MBM^t), \boldsymbol{v})$$

De modo que $A = MBM^t$.

Definición 9.32: Se dice que dos matrices A, B son *congruentes* si existe M invertible tal que $A = MBM^t$.

Por ende hemos probado:

Teorema 9.33: Toda matriz simétrica sobre un campo escalar de característica distinta de 2 es congruente a una matriz diagonal.

Sea F una forma bilineal simétrica con base ortonormal $(\boldsymbol{x}_i)_i$, entonces si B es la representación diagonal de F por el teorema anterior, B tiene por diagonal $\alpha_i^2 \lambda_i$ donde $\lambda_i := F(\boldsymbol{x}_i, \boldsymbol{x}_i)$ y α_i es un escalar que multiplicamos por $\boldsymbol{x}_i$ a conveniencia, luego es claro que:

Teorema 9.34: Si $\operatorname{car} \Bbbk \neq 2$ y todo elemento de $\Bbbk$ posee raíz cuadrada, entonces toda matriz simétrica es congruente a una única matriz $[\underbrace{1, \ldots, 1}_{r}, 0, \ldots, 0]$.

En $\mathbb{C}$ ésto es claro, pero en $\mathbb{R}$ no sucede. Lo mejor que tenemos en $\mathbb{R}$ es una matriz diagonal con 1s, (-1)s y 0s.

Proposición 9.35: Si $\operatorname{car}\mathbb{k} \neq 2$, entonces si F es una forma bilineal simétrica sobre V con forma cuadrática asociada q, entonces F está completamente determinada por

$$F(u,v) = \frac{q(u+v) - q(u) - q(v)}{2}.$$

De éste modo podemos definir una forma cuadrática de tal modo que la función descrita cumpla ser una forma bilineal simétrica.

Definición 9.36: Dada una forma cuadrática q sobre V, se dice que posee alguna de las siguientes propiedades si para todo $\boldsymbol{v} \in V$:

Definida positiva Si $\boldsymbol{x} \neq 0$ implica $q(\boldsymbol{x}) > 0$.

Semidefinida positiva Si $q(\boldsymbol{x}) \geq 0$.

Definida negativa Si $\boldsymbol{x} \neq 0$ implica $q(\boldsymbol{x}) < 0$.

Semidefinida negativa Si $q(\boldsymbol{x}) \leq 0$.

§9.3.2 Formas sesquilineales, producto interno y "geometría euclídea".

Definición 9.37 – *Forma sesquilineal*: Sea H un $\mathbb{K}$-espacio vectorial, se dice que $F : H^2 \to \mathbb{K}$ es una forma sesquilineal si para todo $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in H$ y $\alpha \in \mathbb{K}$ se cumple:

1. $F(\boldsymbol{u}, \boldsymbol{v}) = \overline{F(\boldsymbol{v}, \boldsymbol{u})}$ (simetría hermitiana).
2. $F(\boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w}) = F(\boldsymbol{u}, \boldsymbol{w}) + F(\boldsymbol{v}, \boldsymbol{w})$ (linealidad).
3. $F(\alpha\boldsymbol{u}, \boldsymbol{v}) = \alpha F(\boldsymbol{u}, \boldsymbol{v})$.

Las mismas nociones de representación matricial y formas cuadráticas (ahora llamadas *hermitianas*) aplica.

Proposición 9.38: Si F es una forma sesquilineal, entonces para todo $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^n$ y todo $\alpha \in \mathbb{K}$ se cumple:

1. $F(\boldsymbol{u}, \alpha\boldsymbol{v}) = \bar{\alpha} F(\boldsymbol{u}, \boldsymbol{v})$.
2. $F(\boldsymbol{u}, \boldsymbol{u}) \in \mathbb{R}$.

El resultado anterior permite conservar las definiciones para forma cuadrática en $\mathbb{R}$ y nos permite ver un análogo para la representación matricial:

Teorema 9.39: Dada una forma sesquilineal F sobre $\mathbb{K}^n$ con base ordenada B, se cumple que una matriz $A := \mathrm{M}_B(F)$ syss para todo $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^n$ se cumple que

$$F(\boldsymbol{u}, \boldsymbol{v}) = \pi_B(\boldsymbol{u}) A \pi_B(\boldsymbol{v})^*$$

Luego si denotamos $(\boldsymbol{u}, \boldsymbol{v}) := \pi_B(\boldsymbol{u})\pi_B(\boldsymbol{v})^*$, entonces toda forma sesquilineal corresponde a

$$F(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}A, \boldsymbol{v}) = (\boldsymbol{u}, \boldsymbol{v}A^*).$$

Definición 9.40 – *Producto interno*: Se dice que una forma sesquilineal $(,) : H^2 \to \mathbb{K}$ es un *producto interno* si su forma cuadrática asociada es definida positiva. Un par $(H, (,))$ se dice un *espacio vectorial con producto interno* o un *espacio prehilbertiano*. En éste capítulo, H siempre representará un espacio prehilbertiano.

Denotamos $\| \| : H \to [0, \infty)$ a la aplicación

$$\|\boldsymbol{x}\| := \sqrt{(\boldsymbol{x}, \boldsymbol{x})},$$

que ésta bien definida y sólo toma 0 en el $\vec{0}$.

§9.3.3 Formas hermitianas y espacios de producto interno.

Definición 9.41 – *Forma hermitiana*: Sea H un $\mathbb{K}$-espacio vectorial, se dice que $f : H^2 \to \mathbb{K}$ es una forma hermitiana si para todo $u, v, w \in H$ y $\alpha \in \mathbb{K}$ se cumple:

1. $f(u, v) = \overline{f(v, u)}$ (simetría hermitiana).
2. $f(u + v, w) = f(u, w) + f(v, w)$ (linealidad).
3. $f(\alpha u, v) = \alpha f(u, v)$.

Se dice que $\langle , \rangle : H^2 \to \mathbb{K}$ es un *producto interno* si es una forma hermitiana que satisface que $f(u, u) = 0$ syss $u = \mathbf{0}$, y que $f(u, u) \geq 0$. Un par $(H, \langle , \rangle)$ se dice un *espacio prehilbertiano*.

Si H es prehilbertiano, entonces se define

$$\|x\| := \sqrt{\langle x, x\rangle}.$$

En este capítulo, H siempre denotara un espacio prehilbertiano.

Proposición 9.42: Si f es una forma hermitiana sobre H, entonces, para todo $u, v \in H$ y $\alpha \in \mathbb{K}$:

1. $f(u, \alpha v) = \overline{\alpha} f(u, v)$.
2. $f(u, u) \in \mathbb{R}$.

DEMOSTRACIÓN: Para probar el segundo veamos primero que por simetría hermitiana $f(u, u)$ ha de ser real. □

Lema 9.43: Sea $x \in H$. Se cumple que $x = \mathbf{0}$ syss para todo $y \in H$ se cumple que $\langle x, y\rangle = 0$.

Corolario 9.44: Sean $x, y \in H$. Se cumple que $x = y$ syss para todo $z \in H$ se cumple que $\langle x, z\rangle = \langle y, z\rangle$.

Corolario 9.45: Sean $A, B \in \mathrm{End}(H)$. Se cumple que $A = B$ syss para todo $x, y \in H$ se cumple que $\langle Ax, y\rangle = \langle Bx, y\rangle$.

DEMOSTRACIÓN: Basta fijar un x cualquiera para que variar el y concluya que $Ax = Bx$ para dicho x. Luego variando todo x se cumple que $Ax = Bx$ para todo $x \in H$, i.e., $A = B$. □

Teorema 9.46 – *Desigualdad de Cauchy-Schwarz*: Para todo $x, y \in H$ se cumple:

$$|\langle x, y\rangle| \leq \|x\| \, \|y\|$$

DEMOSTRACIÓN: Supongamos que $y \neq 0$ (pues $y = 0$ es trivial), entonces notemos que

$$\begin{aligned} 0 \leq \langle x - \alpha y, x - \alpha y\rangle &= \langle x, x\rangle - \alpha \langle y, x\rangle - \overline{\alpha} \langle x, y\rangle + |\alpha|^2 \langle y, y\rangle \\ &= \|x\|^2 - 2\,\mathrm{Re}(\alpha \langle y, x\rangle) + |\alpha|^2 \|y\|^2. \end{aligned}$$

para todo $\alpha \in \mathbb{k}$, luego sea $\alpha := \frac{\langle x,y\rangle}{\|y\|^2}$ y despejemos un poco:

$$0 \leq \|x\|^2 - 2\frac{\langle x,y\rangle\,\langle y,x\rangle}{\|y\|^2} + \frac{|\,\langle x,y\rangle\,|^2}{\|y\|^2} = \|x\|^2 - \frac{|\,\langle x,y\rangle\,|^2}{\|y\|^2},$$

de lo que se concluye el resultado. □

Teorema 9.47 (Desigualdad traingular): Para todo $x, y \in H$ se cumple que

$$\|x+y\| \leq \|x\| + \|y\|,$$

luego, $\|\,\| : H^2 \to \mathbb{R}$ es una norma.

Demostración: Basta aplicar el siguiente procedimiento:

$$\begin{aligned}
\|x+y\|^2 &= \langle x+y, x+y\rangle \\
&= \langle x,x\rangle + \langle x,y\rangle + \langle y,x\rangle + \langle y,y\rangle \\
&= \|x\|^2 + 2\,\mathrm{Re}(\langle x,y\rangle) + \|y\|^2 \\
&\leq \|x\|^2 + 2|\,\langle x,y\rangle\,| + \|y\|^2 \\
&\leq \|x\|^2 + 2\|x\|\cdot\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2.
\end{aligned}$$

□

Llamaremos *unitarios* a los vectores de norma 1.

Definición 9.48 – *Ortogonalidad*: Un par $x, y \in H$ se dicen *ortogonales* si $\langle x,y\rangle = 0$, en cuyo caso se escribe $x \perp y$. Más aún, dado un subconjunto $A \subseteq H$, le llamamos *complemento ortogonal* a

$$A^\perp := \{x \in H : \forall a \in A\ (x \perp a)\}.$$

Diremos que una sucesión (finita o infinita) de vectores es *ortogonal*, si los vectores lo son dos a dos. Diremos que una sucesión es *ortonormal*, si los vectores son unitarios y la sucesión es ortogonal.

Teorema 9.49: Se cumple:

1. $\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2$ (ley del paralelogramo).
2. $x \perp y$ syss $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ (teorema de Pitágoras I).
3. Si $\{x_i\}_{i=1}^n$ es una sucesión ortonormal, entonces para todo $i \leq n$ se cumple $x_i \perp \sum_{j\neq i} x_j$.

4. Si $\{x_i\}_{i=1}^n$ es una sucesión ortonormal, entonces para todo $x \in H$ se cumple
$$\|x\|^2 = \sum_{i=1}^n |\alpha_i|^2 + \left\| x - \sum_{i=1}^n \alpha_i x_i \right\|^2,$$
donde $\alpha_i := \langle x, x_i \rangle$ (teorema de Pitágoras II).

Demostración:

4. Obsérvese que
$$x = \sum_{i=1}^n \alpha_i x_i + \left(x - \sum_{i=1}^n \alpha_i x_i \right).$$
Donde hay $n+1$ vectores, hemos de probar que todos son ortogonales entre sí para aplicar el teorema de Pitágoras. Es claro que $x_i \perp x_j$ con $i \neq j$, por ende, basta notar que
$$\begin{aligned} \left\langle x_k, x - \sum_{i=1}^n \alpha_i x_i \right\rangle &= \langle x_k, x \rangle - \sum_{i=1}^n \langle x_k, \alpha_i x_i \rangle \\ &= \langle x_k, x \rangle - \overline{\alpha_k} \cancelto{1}{\langle x_k, x_k \rangle} = 0. \end{aligned}$$

□

Teorema 9.50 – *Ortogonalización de Gram-Schmidt*: Si $\dim H \leq \aleph_0$ tiene una base $\{x_i\}_i$, entonces posee una base ortonormal $\{z_i\}_i$ que satisface que para todo $k > 0$:
$$\operatorname{Span}\{x_1, \ldots, x_k\} = \operatorname{Span}\{y_1, \ldots, y_k\}$$

Demostración: Sea $\{x_i\}$ una base cualquiera de H. Para el proceso de Gram-Schmidt primero definiremos $y_1 := x_1$. Luego queremos que $y_2 \perp y_1$ y que $\operatorname{Span}(x_1, x_2) = \operatorname{Span}(y_1, y_2)$, para lo cual
$$y_2 := x_2 - \frac{\langle x_2, y_1 \rangle}{\|y_1\|^2} y_1$$
que comprueba cumplir nuestras condiciones (¿por qué?). Así se define por recursión
$$y_{n+1} := x_{n+1} - \sum_{k=1}^n \frac{\langle x_{n+1}, y_k \rangle}{\|y_k\|^2} y_k$$
Finalmente se normaliza $\{y_i\}$ en $\{z_i\}$ y ya está. □

Proposición 9.51: Se cumple:

1. Si $S \subseteq H$, entonces $S^\perp \leq H$.
2. Para todo $S \subseteq H$ se cumple que $S \subseteq (S^\perp)^\perp$.

Si exigimos que $\dim H \leq \aleph_0$, entonces para todo $E \leq H$ se cumple que:

3. Existe una única transformación lineal $\pi_E : H \to E$ tal que $\pi_E(v) = v$ si $v \in E$ y $\pi_E(v) = 0$ si $v \notin E$, a la que llamamos *proyección ortogonal* sobre E.
4. $E \oplus E^\perp = H$.
5. $(E^\perp)^\perp = E$.

Demostración: Se elige $\{x_i\}_i$ base ortonormal de H que contiene una subsucesión $\{y_i\}_i$ que es base (también ortonormal) de E. Finalmente π_E lo que hace es anular los coeficientes de $\{x_i\}_i$ que no están en $\{y_i\}_i$. □

¿Y cómo se ve el producto interno? Sea $\{x_i\}$ una base ortonormal de H y sean $\boldsymbol{u}, \boldsymbol{v} \in H$. Por definición de base existen unas sucesiones de escalares $(\alpha_i)_i$ y $(\beta_i)_i$ tales que

$$\boldsymbol{u} = \sum_{i=1} \alpha_i x_i, \quad \boldsymbol{v} = \sum_{i=1} \beta_i x_i$$

luego

$$\begin{aligned}\langle \boldsymbol{u}, \boldsymbol{v} \rangle &= \left\langle \sum_{i=1} \alpha_i x_i, \boldsymbol{v} \right\rangle = \sum_{i=1} \alpha_i \langle x_i, \boldsymbol{v} \rangle \\ &= \sum_{i=1} \alpha_i \left\langle x_i, \sum_{j=1} \beta_j x_j \right\rangle = \sum_{i=1} \alpha_i \sum_{j=1} \bar{\beta}_j \langle x_i, x_j \rangle \\ &= \sum_{i=1} \alpha_i \sum_{j=1} \bar{\beta}_j \delta_{ij} = \sum_{i=1} \alpha_i \bar{\beta}_i.\end{aligned}$$

Luego, todo el producto interno queda completamente determinado por una base ortonormal. Si exigimos que la base canónica sea ortonormal por definición, entonces se tiene que

$$\langle (u_1, \ldots, u_n), (v_1, \ldots, v_n) \rangle = \sum_{i=1}^{n} u_i \bar{v}_i.$$

Es más, si identificamos $H := \mathrm{Mat}_{n\times 1}(\mathbb{C})$, entonces tenemos que para todo $\boldsymbol{u}, \boldsymbol{v} \in H$ se cumple que

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \overline{\boldsymbol{v}}^t \boldsymbol{u}.$$

Corolario 9.52 (Desigualdad de Bessel): Sea $\{x_i\}$ una sucesión[1] ortonormal, entonces para todo $x \in H$ se cumple

$$\sum_i |\alpha_i|^2 \leq \|x\|^2,$$

donde $\alpha_i := \langle x, x_i \rangle$.

Pista: Para probar el caso de un conjunto ortonormal infinito, basta notar que para todo n se cumple por el teorema de Pitágoras, por ende, la sucesión dada por las sumas parciales es creciente y acotada, ergo, converge. □

Teorema 9.53: Sea $\{x_i\}_{i=0}^n$ una sucesión finita ortonormal y $x \in H$. Entonces, los escalares $\lambda_i \in \Bbbk$ que minimizan el valor de

$$\left\| x - \sum_{i=0}^{n} \lambda_i x_i \right\|$$

son únicos y son $\lambda_i = \langle x, x_i \rangle$.

Demostración: Observe que

$$\begin{aligned}
\left\| x - \sum_{i=0}^{n} \lambda_i x_i \right\|^2 &= \|x\|^2 - \sum_{i=0}^{n} (\overline{\lambda_i} \langle x, x_i \rangle + \lambda_i \overline{\langle x, x_i \rangle}) + \left\| \sum_{i=0}^{n} \lambda_i x_i \right\|^2 \\
&= \|x\|^2 + \sum_{i=0}^{n} |\lambda_i|^2 - \sum_{i=0}^{n} (\overline{\lambda_i} \langle x, x_i \rangle + \lambda_i \overline{\langle x, x_i \rangle}) \\
&\quad + \sum_{i=0}^{n} |\langle x, x_i \rangle|^2 - \sum_{i=0}^{n} |\langle x, x_i \rangle|^2 \\
&= \|x\|^2 + \sum_{i=0}^{n} |\lambda - \langle x, x_i \rangle|^2 - \sum_{i=0}^{n} |\langle x, x_i \rangle|^2,
\end{aligned}$$

de aquí es fácil deducir el enunciado. □

[1] Aquí se obvian los límites de los índices pues el resultado es válido tanto para sucesiones finitas como infinitas.

Corolario 9.54: Si una sucesión ortonormal $\{x_i\}$ genera un subespacio V de H, entonces todo $x \in V$ se escribe de forma única como combinación lineal con

$$x = \sum_i \langle x, x_i \rangle \, x_i.$$

Proposición 9.55 (Identidad de Parseval): Una sucesión ortonormal $\{x_i\}$ es base de H syss para todo $x \in H$ se cumple

$$\|x\|^2 = \sum_i |\langle x, x_i \rangle \, x_i|^2.$$

§9.3.4 Formas cuadráticas.

Definición 9.56 – *Formas bilineales y cuadráticas*: Sea V un $\Bbbk$-espacio vectorial. Se dice que $F : V^2 \to \Bbbk$ es una *forma bilineal* si para todo $u, v, w \in V$ y todo $\alpha, \beta \in \Bbbk$ se cumple:

1. $F(\alpha u + \beta v, w) = \alpha F(u, w) + \beta F(v, w)$.
2. $F(u, \alpha v + \beta w) = \alpha F(u, v) + \beta F(u, w)$.

y se dice que una forma bilineal es *simétrica* si $F(u, v) = F(v, u)$.
Dada una forma bilineal F, se le dice la *forma cuadrática* asociada a F a $q : V \to \Bbbk$ es $q(v) := F(v, v)$.

Proposición 9.57: Si el campo escalar de V es de característica distinta de 2, entonces: Si F es una forma bilineal simétrica sobre V con forma cuadrática asociada q, entonces F está completamente determinada por

$$F(u, v) = \frac{q(u + v) - q(u) - q(v)}{2}.$$

De éste modo podemos definir una forma cuadrática de tal modo que la función descrita cumpla ser una forma bilineal simétrica.

10

Álgebras

10.1 Definiciones elementales

Definición 10.1: Sea A un dominio. Una A-***álgebra*** B es un A-(bi)módulo con una forma bilineal $\beta\colon B \times B \to B$, al que llamamos *multiplicación* o *producto* y denotamos $\beta(a,b) =: a\cdot b$. Se le exige también a B que existe un 1 tal que $1\cdot b = b\cdot 1 = b$ para todo $b \in B$.[a] Se dice que B es una A-***álgebra asociativa*** (resp. ***conmutativa***) si el producto es asociativo (resp. conmutativo).

Un homomorfismo de A-álgebras es un homomorfismo de A-bimódulos $\varphi\colon B \to C$ de modo que $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$ y que $\varphi(1_B) = 1_C$.

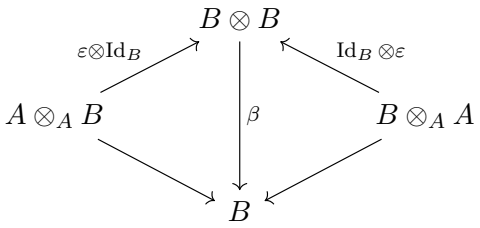
[a] Algunos libros le llaman a ésta clase de estructuras *álgebras unitarias*. En éste texto *no* estudiaremos álgebras no-unitarias.

Varios libros no suelen tratar el tema de álgebras asociativas. Nosotros no enfatizaremos las álgebras no asociativas, con la excepción de las álgebras de Lie y de Jordan.

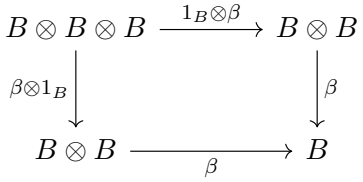
Proposición 10.2: Las A-álgebras asociativas (como objetos) y los homomorfismos de A-álgebras (como flechas) conforman una categoría denotada Alg_A. La subcategoría de A-álgebras conmutativas se denota CAlg_A.

Nótese que las A-álgebras asociatativas pueden verse como anillos que en

cierta forma incluyen a A. En particular, el producto escalar $A \times B \to B$ es una aplicación bilineal y, por ende, induce un homomorfismo de A-módulos $A \otimes_A B \to B$. Luego, la condición de ser un A-bimódulo puede entenderse como exigir que el siguiente diagrama conmute:



Mientras que la asociatividad puede entenderse como exigir que el siguiente diagrama conmute:



Ejemplo. Sea A un dominio.

1. Sea $G = \{g_1, \ldots, g_n\}$ un grupo finito. Denotemos $A[G]$ al conjunto de sumas formales $\sum_{i=1}^{n} a_i g_i$, donde la suma es coordenada a coordenada, el producto por escalar es sobre los coeficientes de la suma y la forma bilineal es la siguiente:

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{g \in G} b_g g\right) = \sum_{g \in G}\left(\sum_{hk=g} a_h b_k\right) g.$$

   Es claro que $A[G]$ es una A-álgebra asociativa y es conmutativa syss G es un grupo abeliano. Llamamos a $A[G]$ la A-álgebra asociada al grupo G.

2. De hecho no es necesario que sea un grupo ni que sea finito. Si G es un monoide arbitrario,[1] entonces también podemos definir $A[G]$ exactamente del mismo modo, exigiendo que las sumas formales sean finitas,

[1] Si trabajaramos con álgebras no-unitarias, entonces también podriamos admitir que G sea un semigrupo.

y notamos que la multiplicación está bien definida puesto que sólo habrán finitas combinaciones que sumar. En cualquier caso $A[G]$ también es una A-álgebra asociativa.

Es fácil notar que $A[G]$ es un A-módulo libre y que G es la base.

3. Sea $S = \{x_i\}_{i\in I}$ un conjunto de indeterminadas, entonces $A[S]$, el anillo de polinomios, es una A-álgebra asociativa conmutativa. De hecho, es un caso especial de una A-álgebra inducida por el monoide G dado por los monomios $x_{i_1}^{\alpha_1}\cdots x_{i_n}^{\alpha_n}$ con la operación dada por factorizar los respectivos términos.

4. Si retomamos el ejemplo anterior, pero consideramos G como el monoide libre cuya base es $S = \{x_i\}_{i\in I}$ (aquí, por ejemplo, $xy \neq yx$), entonces obtenemos $A\langle S\rangle$ el cual es una A-álgebra asociativa, pero si S tiene más de una indeterminada, entonces es no conmutativa.

5. Es claro que si B es un anillo que contiene a A, entonces B es una A-álgebra asociativa. En particular, las extensiones de cuerpo son álgebras conmutativas. Más en particular, $\mathbb{C}$ es una $\mathbb{R}$-álgebra asociativa conmutativa.

6. Considere el grupo finito Q_4 de cuaterniones. Se denota por $\mathbb{H} := \mathbb{R}[Q_4]$, el cual es una $\mathbb{R}$-álgebra asociativa no-conmutativa y sus elementos son de la forma $a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$, donde

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1, \qquad \mathrm{ij} = \mathrm{k},\ \mathrm{ik} = -\mathrm{j},\ \mathrm{jk} = \mathrm{i}.$$

Algunas definiciones típicas:

Definición 10.3: Sea B una A-álgebra. Un subconjunto $C \subseteq B$ se dice que es una ***subálgebra*** si es un A-submódulo, contiene al 1 y es cerrado bajo la multiplicación de B.

Un ***ideal*** es una subálgebra $\mathfrak{b} \subseteq B$ tal que $B\mathfrak{b} = \mathfrak{b}B = \mathfrak{b}$ y en particular, si B es una álgebra asociativa, entonces un ideal (como álgebra) es un ideal izquierdo y derecho (como anillo) que es también una subálgebra. Es fácil comprobar que el anillo cociente $B/\mathfrak{b}$ es también una A-álgebra, de modo que le llamamos una A-álgebra cociente.

Lema 10.4: La intersección arbitraria de subálgebras (resp. ideales) es también una subálgebra (resp. un ideal).

Definición 10.5: Sea B una A-álgebra. Dado un subconjunto $S \subseteq B$, denotamos por $A[S]$ a la mínima subálgebra de B que contiene a S. Si B es una álgebra asociativa, entonces denotamos por $A + (S)$ al mínimo ideal de B que contiene a S.

Proposición 10.6: Sea B una A-álgebra y sea $S \subseteq B$ un subconjunto. Entonces:

$$A[S] = \left\{ \sum_{i=1}^{n} s_i t_i : s_i, t_i \in S \cup A \right\},$$
$$A + (S) = \left\{ \sum_{i=1}^{n} b_i s_i c_i : b_i, c_i \in B, s_i \in S \cup A \right\}.$$

Proposición 10.7: La unión de una cadena de subálgebras (resp. ideales) es también una subálgebra (resp. un ideal).

Proposición 10.8: Sean B, C un par de A-álgebras y $\varphi\colon B \to C$ un homomorfismo de A-álgebras. Entonces $\ker\varphi$ es un ideal de B e $\operatorname{Img}\varphi$ es una subálgebra de C.

Definición 10.9: Un subconjunto $S \subseteq B$ es un ***sistema generador*** si $A[S] = B$. Se dice que B es una A-álgebra ***de tipo finito*** si posee un sistema generador finito.

Otros textos emplean la expresión «álgebra finitamente generada» o «álgebra finita», pero creo que ésto ocasiona confusiones con ser finitamente generado como módulo o ser finito en cardinalidad. Es claro que hay álgebras de tipo finito que no tienen cardinalidad finita, pero más aún:

Ejemplo. Considere el álgebra polinomial $A[x]$. Ésta álgebra es de tipo finito (está generada por $\{x\}$), pero no es un A-módulo finitamente generado, pues su base es $\{1, x, x^2, \dots\}$.

En general, reservaré las letras x y similares para las indeterminadas, de modo que $A[x]$ siempre será el álgebra polinomial y $A[a]$ representa el subálgebra generada por a.

Definición 10.10: Sea B una A-álgebra asociativa. Un subconjunto $X \subseteq$

B es un ***conjunto libre*** si el conjunto de todos los posibles productos (finitos) de elementos de X es linealmente independiente.

Un subconjunto $X \subseteq B$ es una ***base*** si para toda A-álgebra asociativa C toda función $f\colon X \to C$ posee una única extensión $\bar{f}\colon B \to C$ tal que $\bar{f}|_X = f$.

Teorema 10.11: Dado un conjunto X, existe una álgebra asociativa $A\langle X\rangle$ en donde X es un sistema generador libre.

Teorema 10.12: Sea B una A-álgebra asociativa. El conjunto $X \subseteq B$ es una base syss es un sistema generador libre.

Demostración: $\Longleftarrow$. Sea X un sistema generador libre y P el conjunto de todos los productos finitos con elementos en X. Entonces P es linealmente independiente y, como está cerrado bajo multiplicación, es también un sistema generador de B como A-módulo, de modo que es una base de B como A-módulo. Dada una función $f\colon X \to C$ es fácil ver que se extiende a una única función $f^*\colon P \to C$ por multiplicación, la cual a su vez se extiende a un único homomorfismo $\bar{f}\colon B \to C$ de A-módulos. Ahora, con una comprobación rutinaria, es fácil comprobar que $\bar{f}$ sí respeta productos (en particular respeta las unidades), de modo que sí resulta un homomorfismo de A-álgebras. La unicidad deriva de que deben coincidir en los productos finitos de elementos de X, los que constituyen una base para B.

Denotaremos por $A\langle X\rangle$ al álgebra generada por los monomios ordenados.

$\Longrightarrow$. Denotemos por $F := A\langle X\rangle$ al álgebra construida en la parte anterior de la demotración, la cual hemos probado que es libre. Considere la inclusión $\iota_B\colon X \to F$, por hipótesis se extiende a un único homomorfismo de A-álgebras $f\colon B \to F$. Así mismo, la inclusión $\iota_F\colon X \to B$ se extiende a un único homomorfismo de A-álgebras $g\colon F \to B$. Luego $f \circ g\colon B \to B$ es un endomorfismo de A-álgebras que fija a la base, por lo que debe ser la identidad y análogamente con $g \circ f$. □

Corolario 10.13: Dos álgebra libres $A\langle X\rangle, A\langle Y\rangle$ son isomorfas si $|X| = |Y|$.

El recíproco parecería sencillo pero, ¡inténtelo! En esencia, el problema resulta difícil, incluso si A es un cuerpo, porque los elementos de la base son algebraicamente independientes; se asimila a probar la unicidad del grado de trascendencia, pero con la problemática de la falta de conmutatividad. No

obstante, nótese que, por un argumento de cardinalidad, si las bases tienen mayor cardinalidad que $\aleph_0 + |A|$, entonces el recíproco es trivial.

Definición 10.14: Sea B una A-álgebra asociativa conmutativa. Un subconjunto $X \subseteq B$ es una ***base*** si para toda A-álgebra asociativa conmutativa C toda función $f\colon X \to C$ posee una única extensión $\bar{f}\colon B \to C$ tal que $\bar{f}|_X = f$.

La noción de sistema generador libre también vale aquí, pero con la restricción de que el conjunto P de los productos no posea dos productos cuyos factores sean los mismos salvo permutación.

Así pues, se llegan a las siguientes conclusiones:

Teorema 10.15: Sea A un dominio y S un conjunto arbitrario.

1. La álgebra polinomial $A[S]$ es una álgebra asociativa conmutativa libre que tiene a S por base.
2. Si S, T son dos conjuntos de indeterminadas con la misma cardinalidad, entonces $A[S] \cong A[T]$.
3. Recíprocamente, si F_1, F_2 son álgebras conmutativas libres, entonces son álgebras polinomiales con la misma cantidad de indeterminadas.

Como señalé anteriormente, la última parte la podemos concluir por los argumentos desarrollados en la teoría de trascendencia (cf. §4.6).

Teorema 10.16 (lema de Zariski): Sea L/k una extensión de cuerpos tal que L es una k-álgebra de tipo finito, entonces L es una extensión finita.

Aluffi [**1,** p. 405] le llama a éste resultado el «Nullstellensatz fuerte»; sin embargo, dicho nombre lo reservamos para el teorema **??**. Daremos tres demostraciones:

Demostración (Rabinowitsch): En esta demostración supondremos que k no es numerable.

Si L es un k-álgebra de tipo finito, entonces viene generado por una m-tupla finita $\boldsymbol{a}$. Para ver que L es una extensión finita, basta ver que cada uno de los elementos es algebraico. Para ello sea $\mathrm{ev}_{\boldsymbol{a}}\colon k[x_1, \ldots, x_m] \to L$ el morfismo suprayectiva, entonces viene generado, como k-espacio vectorial, por todos los monomios de $k[x_1, \ldots, x_m]$ evaluados en $\boldsymbol{a}$ que son numerables.

Sea $\alpha \in L \setminus k$, para ver que es algebraica entonces nótese que el conjunto

$$\left\{ \frac{1}{\alpha - \beta} : \beta \in k \right\}$$

es no numerable, luego no puede ser base así que ha de ser linealmente dependiente y existe

$$\frac{\lambda_1}{\alpha - \beta_1} + \cdots + \frac{\lambda_n}{\alpha - \beta_n} = \frac{p(\alpha)}{q(\alpha)} = 0$$

para algunos λ_i no nulos. Sustituyendo α por una variable x arbitraria se obtienen los polinomios $p(x), q(x) \in k[x]$, donde $q(x) = (x - \beta_1) \cdots (x - \beta_n)$ es no nulo en α, así que $p(\alpha) = 0$.

Ésto prueba que L es algebraico, y como viene generado por finitos elementos, es una extensión finita. □

Damos otra demostración en la proposición 10.68 y el corolario 11.56.

Ya hemos visto que la k-álgebra polinomial $k[x]$ es de tipo finito y claramente la indeterminada $x \in k[x]$ es k-trascendente, pero $k[x]/k$ no es una extensión de cuerpos; para que lo fuese tenemos que empezar a incluir fracciones y éstas son las que, por el lema de Zariski, constituirán un sistema generador infinito.

Teorema 10.17 – *Teorema débil de ceros de Hilbert*: Si k es algebraicamente cerrado, entonces un ideal $\mathfrak{a} \lhd k[x_1, \ldots, x_n]$ es maximal syss $\mathfrak{a} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ con $\alpha_i \in k$.

Demostración: Nótese que $k[x_1, \ldots, x_n]/(x_1 - \alpha_1, \ldots, x_n - \alpha_n) \cong k$ que es un cuerpo, así que $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ es un ideal maximal.

Conversamente sea $\mathfrak{m} \trianglelefteq k[x_1, \ldots, x_n]$ un ideal maximal, luego se induce un monomorfismo natural $k \to k[x_1, \ldots, x_n]/\mathfrak{m} =: L$, donde L/k es una extensión de cuerpos que es de tipo-finito como k-álgebra, así por la versión fuerte se da que L es una extensión algebraica, ergo $L = K$. Luego la proyección natural $\pi\colon k[x_1, \ldots, x_n] \to k$ es un epimorfismo de anillos con $\mathfrak{m} = \ker \pi$. Definiendo $\alpha_i := \pi(x_i)$ se cumple que

$$(x_1 - \alpha_1, \ldots, x_n - \alpha_n) \subseteq \mathfrak{m} \neq k[x_1, \ldots, x_n]$$

y por maximalidad del conjunto de la izquierda se da la igualdad buscada. □

Una historia curiosa es que, cuando Rabinowitsch emigró a los Estados Unidos simplificó su nombre a Rainich. Fue catedrático en la Universidad de Michigan en donde expuso una vez una lectura en donde dijo emplear un famoso truco que había descubierto. Un alumno entonces se paró de su pupitre y acusó al profesor de haber tomado crédito por el famoso truco de Rabinowitsch, tras lo cual, Rainich se dio vuelta hacia el pizarron y anoto en mayúsculas el nombre de RABINOWITSCH y comenzó a borrar una por una letras hasta quedar RA IN I CH.

10.2 Álgebras asociativas

Definición 10.18: Una A-álgebra B se dice ***graduada*** por $B = \bigoplus_{d\in\mathbb{N}} B_d$ si:

AG1. Cada B_i es un A-módulo.

AG2. Para cada $d, e \geq 0$ se satisface que $B_d \cdot B_e \subseteq B_{d+e}$.

En consecuencia de AG2., se satisface que B_0 es un anillo (y veremos que es unitario), y que cada B_d es un B_0-módulo y B también. Dicha descomposición se dice una ***graduación***, y cada $f \in A_d$ se dice un elemento ***homogéneo de grado*** d. Un ***anillo graduado*** es una $\mathbb{Z}$-álgebra graduada.

Una subálgebra $C \subseteq B$ se dice ***homogéneo*** si $C = \bigoplus_{d\in\mathbb{N}}(C \cap B_d)$. Un ideal se dice ***homogéneo*** si es una subálgebra homogénea. El conjunto $B^+ := \bigoplus_{d>0} B_d$ es un ideal homogéneo llamado el ***ideal irrelevante***.

El principal ejemplo de un anillo graduado es el siguiente:

Ejemplo. Sea A un dominio, y sea $S = \{x_i\}_{i\in I}$ un conjunto de indeterminadas:

- El álgebra polinomial $P := A[S]$ es una A-álgebra graduada, donde los elementos homogéneos de grado d son los polinomios que se escriben como suma de monomios de grado d (incluyendo al cero).

- Similarmente, el álgebra libre $A\langle S\rangle$ es una A-álgebra graduada, donde los elementos homogéneos de grado d son los monomios que resultan palabras (del semigrupo libre) de longitud d, y las combinaciones lineales de ellos.

Lema 10.19: Sea A un anillo graduado. El 1 es un elemento homogéneo de grado 0.

Demostración: Nótese que si $1 = e_0 + \cdots + e_n$, donde e_i es su componente homogénea de grado i, entonces

$$e_0 = e_0 \cdot 1 = e_0^2 + e_0 e_1 + \cdots + e_0 e_n,$$

de modo que $e_0 e_i = 0$ si $i \neq 0$. Luego para $i \neq 0$:

$$e_i = 1 \cdot e_i = e_0 e_i + e_1 e_i + \cdots + e_n e_i,$$

como e_i tiene todas sus componentes homogéneas nulas, exceptuando (tal vez) la i-ésima, entonces $e_j e_i = 0$ si $j \neq 0$, de modo que $e_i = e_0 e_i = 0$ por lo anterior. Por ende, $1 = e_0$. □

Teorema 10.20: Sea A un anillo graduado. Una subálgebra $S \subseteq A$ es homogénea syss está generada por un conjunto de elementos homogéneos.

Demostración: $\Longrightarrow$. Si S es homogénea entonces está generada por $\bigcup_{d\in\mathbb{N}} S \cap A_d$.

$\Longleftarrow$. Sea T tal que $\mathfrak{a} = (T)$ y tal que los elementos de T son homogéneos. Luego, sea $f \in \mathfrak{a}$, por definición

$$f = g_1 f_1 + \cdots g_n f_n$$

donde $f_i \in T$ y $g_i \in A$. Como A es graduado, y los g_i's son finitos, podemos encontrar suficientes h_j's homogéneos tales que

$$g_i = \lambda_{1i} h_1 + \cdots + \lambda_{mi} h_m,$$

donde $\lambda_{ji} \in A_0$. Por lo tanto,

$$f = \lambda_{11} h_1 f_1 + \lambda_{21} h_2 f_1 + \cdots \lambda_{mn} h_m f_n.$$

donde cada $h_j f_i$ es homogéneo. Es decir, $f \in \bigoplus_{d\in\mathbb{N}} (\mathfrak{a} \cap A_d)$. La otra inclusión es trivial. □

Definición 10.21: Sean B, C un par de A-álgebras graduadas Se dice que $\varphi\colon B \to C$ es una ***función lineal homogénea*** de grado g si es un homomorfismo de A-álgebras tal que $\varphi[B_d] \subseteq C_{d+g}$ para todo d.

Lema 10.22: Sean B, C un par de A-álgebras graduadas. Supongamos que $\{\lambda_g \colon B \to C\}_{g\in\mathbb{N}}$ es una familia de funciones lineales homogéneas que tiene las siguientes propiedades:

1. Cada λ_g es homogénea de grado g.
2. Para todo $b \in B$ se cumple que $\lambda_g(b) = 0$ para todos salvo finitos g's.
3. $\sum_{g\in\mathbb{N}} \lambda_g = 0$.

Entonces todas las λ_g's son identicamente nulas.

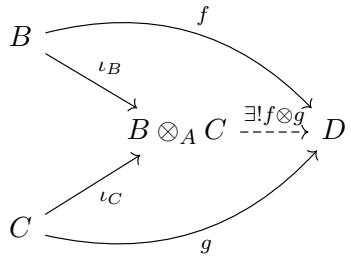
Definición 10.23: Sean B, C un par de A-álgebras. Considere $T := B \otimes_A C$ como A-módulos y definamos un producto en T que, en los tensores puros, corresponde a

$$(b_1 \otimes c_1) \cdot (b_2 \otimes c_2) = b_1 b_2 \otimes c_1 c_2,$$

entonces $(T, +, \cdot)$ es un anillo con unidad $1 = 1 \otimes 1$. Y es fácil notar que T es una A-álgebra mediante el morfismo $a \mapsto a \cdot 1 = a \otimes 1 = 1 \otimes a$.

Veamos una caracterización de los productos tensoriales de álgebras:

Proposición 10.24: Sean B, C, D un trío de A-álgebras, y sean $f \colon B \to D$ y $g \colon C \to D$ dos homomorfismos de A-álgebras tales que para todo $b \in B, c \in C$ se cumple que $[f(b), g(c)] = 0$ (el conmutador). Entonces, existe un único homomorfismo de A-álgebras $(f \otimes g) \colon B \otimes_A C \to D$ tal que el siguiente diagrama conmuta (en Alg_A):



Teorema 10.25: Sean B, C un par de A-álgebras conmutativas. Entonces $B \otimes_A C$ corresponde con el coproducto en la categoría CAlg_A.

Proposición 10.26: Sean $\{x_i\}_{i\in I}, \{y_j\}_{j\in J}$ dos conjuntos disjuntos de indeterminadas, entonces

$$A[\{x_i\}_{i\in I}] \otimes_A A[\{y_j\}_{j\in J}] = A[\{x_i, y_j : i \in I, j \in J\}].$$

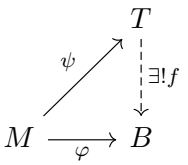
Ejemplo. Nótese que $A[x] \otimes_A A[y] = A[x, y]$ y que $A[x] = A\langle x\rangle$, pero que el coproducto en Alg_A es

$$A[x] \amalg A[y] = A\langle x\rangle \amalg A\langle y\rangle = A\langle x, y\rangle \ncong A[x, y].$$

Definición 10.27: Sea M un A-módulo. Un par (T, ψ) se dice una ***álgebra tensorial*** sobre M si:

AT1. T es una A-álgebra y $\psi\colon M \to T$ es un homomorfismo de A-módulos.

AT2. Si $\varphi\colon M \to B$ es un homomorfismo de A-módulos, donde B es una A-álgebra, entonces existe un único homomorfismo de A-álgebras $f\colon T \to B$ tal que el siguiente diagrama conmuta:



Teorema 10.28: Dado un A-módulo M existe una álgebra tensorial sobre M, denotada $T(M)$. Más aún, todas las álgebras tensoriales sobre M son isomorfas.

Demostración: La unicidad de las álgebras es un típico ejercicio de categorías.

Para construir a $T(M)$ considere a M como un conjunto de variables y considere $F := A\langle M\rangle$ el álgebra libre con base en M. Para distinguir las operaciones en F de las operaciones en M diremos que para todo $\alpha \in A$, los símbolos $x + y, x - y, \alpha x$ denotan operaciones en M y $x \dot{+} y, x \dot{-} y, \alpha \cdot x$ las operaciones en F. Luego, al igual que con los tensores, construimos el ideal $\mathfrak{a}$ generado por elementos de la forma:

$$x \dot{+} y \dot{-} (x + y), \qquad \alpha \cdot x \dot{-} (\alpha x).$$

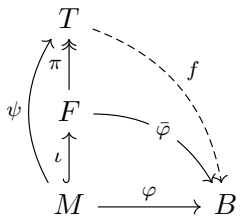
Y definimos $T(M) := F/\mathfrak{a}$. Construimos el morfismo $\psi\colon M \to T$ dado por composición de inclusión de los elementos en F y la proyección.

Sea $\varphi\colon M \to B$ un homomorfismo de A-módulos, donde B es una A-álgebra. Por definición de base, se extiende a un único homomorfismo de A-álgebras $\bar{\varphi}\colon F \to B$. Luego, nótese que $\bar{\varphi}$ se anula en $\mathfrak{a}$, en particular lo hace sobre sus generadores:

$$\bar{\varphi}\big(x \dot{+} y \dot{-} (x + y)\big) = \bar{\varphi}(x) + \bar{\varphi}(y) - \bar{\varphi}(x + y)$$

$$= \varphi(x) + \varphi(y) - \varphi(x+y) = 0,$$

donde empleamos el hecho de que φ es lineal; y es análogo con los otros generadores. Finalmente podemos proyectar $\bar{\varphi}$ en $F/\mathfrak{a}$ y nos dará una aplicación f. Visualmente:



□

Ejemplo. Sea A un dominio. Luego A mismo es un A-módulo libre con base $\{1\}$, afirmamos que $T(A) = A[x]$. Hay una manera más larga de proceder, pero con las caracterizaciones categoriales es sencillo: sea B una A-álgebra arbitraria, entonces queremos C tal que

$$\mathrm{Hom}_{\mathsf{Alg}}(C, B) \approx \mathrm{Hom}_{\mathsf{Mod}}(A, B) \approx \mathrm{Func}(\{1\}, B),$$

donde $\approx$ denota equipotencia. Pero $\mathrm{Func}(\{1\}, B) \approx \mathrm{Hom}_{\mathsf{Alg}}(A[x], B)$ pues $A[x]$ es la A-álgebra libre con un generador.

Extrapolando el mismo ejercicio se obtiene:

Proposición 10.29: Sea A un dominio. Sea S un conjunto arbitrario y denotemos por $A^{\oplus S}$ el A-módulo libre con base S, se cumple que $T(A^{\oplus S}) = A\langle S\rangle$.

Otra propiedad de las álgebras tensoriales (en particular de su construcción) es que son álgebras graduadas: En efecto, nótese que $A\langle M\rangle$ es un álgebra graduada por ser libre, y que las combinaciones lineales formales de elementos en M son los elementos homogéneos de grado 1. Luego el ideal construido está generado por elementos homogéneos y luego es un ideal homogéneo, de modo que el cociente es una álgebra graduada.

Teorema 10.30: Sea M, N un par de A-módulos, y sea $\beta\colon M^d = \prod_{i=1}^{d} M \to N$ un aplicación d-multilineal. Entonces existe un homorfismo de A-módulos $\varphi\colon T_d(M) \to N$ tal que

$$\varphi(m_1 \cdots m_d) = \beta(m_1, \ldots, m_d),$$

donde a la izquierda tenemos un producto formal (el cuál es válido en $T(M)$) y a la derecha

Demostración: Volvemos a la construcción de $T(M)$: F es el álgebra libre $A\langle M\rangle$ y $\mathfrak{a}$ es el ideal tal que $F/\mathfrak{a} = T(M)$, S es el conjunto de generadores para $\mathfrak{a}$ descrito en la demostración, y el símbolo «$\boxdot$» denota multiplicación en F. Luego, los elementos de $\mathfrak{a}$ son sumas de elementos de la forma $a \boxdot s \boxdot b$ donde $a, b \in F$ y $s \in S$.

Sea $u \in F_d \cap \mathfrak{a}$, luego $u = \sum_{i=1}^{n} a_i \boxdot s_i \boxdot b_i$, donde $s_i \in S$ es homogéneo de grado 1 y donde

$$a_i = \sum_{k=0}^{m} a_{ik}, \qquad b_i = \sum_{\ell=0}^{m} b_{i\ell},$$

donde a_{ik}, b_{ik} son las componentes homogéneas de grado k de a_i, b_i resp. (y donde elegimos a m suficientemente grande). Luego

$$u = \sum_{i=1}^{n} \sum_{k,\ell}^{m} a_{ik} \boxdot s_i \boxdot b_{i\ell},$$

nótese que cada término $a_{ik} \boxdot s_i \boxdot b_{i\ell}$ es homogéneo de grado $k + 1 + \ell$, luego como u es homogéneo de grado d tenemos la igualdad

$$u = \sum_{i=1}^{n} \sum_{k+\ell+1=d} a_{ik} \boxdot s_i \boxdot b_{i\ell}.$$

Los elementos de $F_d(M)$ son combinaciones lineales de productos (libres) de d elementos en M. Luego, u es una combinación lineal de elementos de la forma:

$$x_1 \boxdot \cdots \boxdot x_k \boxdot s \boxdot y_1 \boxdot \cdots \boxdot y_\ell, \tag{10.1}$$

donde $x_i, y_j \in M$ para todo i, j, $s \in S$ y $k + \ell + 1 = d$.

Nótese que el conjunto $\{z_1 \boxdot \cdots \boxdot z_h : z_i \in M\}$ es una base de F_h, de modo que dada una aplicación h-multilineal $\beta\colon M^d \to N$ se extiende a un único homomorfismo de A-módulos $\psi\colon F_d \to N$. Es fácil ver que ψ se anula en $F_d \cap \mathfrak{a}$ puesto que sus elementos son de la forma descrita en (10.1), luego desciende al cociente $F_d/(F_d \cap \mathfrak{a}) = T_d(M)$ como se quería ver. □

Corolario 10.31: Para todo $d \geq 1$ se cumple que $T_d(M) \cong M^{\otimes d}$ (como A-módulos).

Definición 10.32: Sea B una A-álgebra graduada. Se dice que B es una ***álgebra anticonmutativa*** si

AAC1. Para todo b, c elementos homogéneos de grados d, e resp., se cumple que $b \cdot c = (-1)^{de} c \cdot b$.

AAC2. Si b es homogéneo de grado impar, entonces $b^2 = 0$.

Nótese que si 2 no es divisor de cero en A (e.g., si A es un cuerpo de característica $\neq 2$) entonces AAC1 implica AAC2.

Proposición 10.33: Sea B una A-álgebra graduada. Supongamos que B está generada por un sistema $S = \{x_1, \ldots, x_n\}$ tal que:

1. Cada $x_i \in S$ es homogéneo de grado impar.
2. $x_i x_j + x_j x_i = 0$ para todo i, j.
3. $x_i^2 = 0$ para todo i.

Entonces B es una álgebra anticonmutativa.

Teorema 10.34: Toda subálgebra y todo cociente de una álgebra anticonmutativa es también una álgebra anticonmutativa.

Teorema 10.35: Sean $B_1, \ldots, B_r$ un conjunto de A-álgebras anticonmutativas, entonces $B_1 \otimes_A \cdots \otimes_A B_r$ es una álgebra anticonmutativa.

Teoremas pendientes.

Teorema 10.36: Sean B, C un par de A-álgebras graduadas y sea D una A-álgebra anticonmutativa. Supongamos que existen $\varphi\colon B \to D$ y $\psi\colon C \to D$ homomorfismos homogéneos de grado 0. Entonces existe un único homomorfismo de A-álgebras $\theta\colon B \otimes_A C \to D$ tal que $\theta(b \otimes c) = \varphi(b)\psi(c)$.

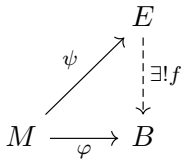
§10.2.1 Álgebra exterior y determinantes.

Definición 10.37: Sea M un A-módulo. Un par (E, ψ) se dice una ***álgebra exterior*** sobre M si:

AE1. E es una A-álgebra y $\psi\colon M \to E$ es un homomorfismo de A-módulos.

AE2. Para todo $\boldsymbol{m} \in M$ se cumple que $\psi(\boldsymbol{m})^2 = 0$.

AE3. Si $\varphi\colon M \to B$ es un homomorfismo de A-módulos, donde B es una A-álgebra, tal que $\varphi(\boldsymbol{m})^2 = 0$ para todo $\boldsymbol{m} \in M$, entonces existe un único homomorfismo de A-álgebras $f\colon E \to B$ tal que el siguiente diagrama conmuta:



Lema 10.38: Sea M un A-módulo. Supongamos que E_1, E_2 son A-álgebras exteriores sobre M, entonces $E_1 \cong E_2$.

Teorema (AE) 10.39: Dado un A-módulo libre M existe una álgebra exterior sobre M, denotada $E(M)$.

Demostración: Sea $X = \{\boldsymbol{u}_\alpha\}_{\alpha<\kappa}$ una base de M la cual está indexada por ordinales por AE; construiremos E como prosigue. Diremos que para todos $\boldsymbol{u}, \boldsymbol{v} \in X$ distintos, entonces $\boldsymbol{u}^2 = 0$ y $\boldsymbol{uv} = -\boldsymbol{vu}$. Para ello consideramos los conjuntos finitos S de X y en particular podemos verlo como los índices y denotaremos $\bar{u}_\alpha$ en lugar de $\boldsymbol{u}_\alpha$ para enfatizar que estamos en E y no en M. Luego, dado un determinado producto $\bar{u}_{\alpha_1} \cdots \bar{u}_{\alpha_n}$ lo definimos como 0 si tiene algún índice repetido, si no

$$\bar{u}_{\alpha_1} \cdots \bar{u}_{\alpha_n} = (\operatorname{sgn}\sigma) \cdot \bar{u}_{\alpha_{\sigma(1)}} \cdots \bar{u}_{\alpha_{\sigma(n)}},$$

donde $\sigma \in S_n$. En particular lo reordenamos hasta obtener los índices en orden creciente. Así pues, definimos E como el A-módulo libre con base $\mathcal{P}_{<\infty}(X)$ (incluyendo el vacío, el producto del conjunto vacío de vectores corresponde al 1 del álgebra) con el producto de «monomios» definido como arriba.

Construiremos $\psi\colon M \to E$ así: dado un $\boldsymbol{m} = \sum_{\alpha=0}^{\kappa} c_\alpha \boldsymbol{u}_\alpha$, entonces $\psi(\boldsymbol{m}) = \sum_{\alpha=0}^{\kappa} c_\alpha \bar{u}_\alpha$. Luego notamos que

$$\begin{aligned}\left(\sum_\alpha c_\alpha \bar{u}_\alpha\right)^2 &= \sum_{\alpha<\beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta + \cancelto{0}{\sum_\alpha c_\alpha^2 \bar{u}_\alpha^2} + \sum_{\alpha>\beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta \\ &= \sum_{\alpha<\beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta + \sum_{\beta>\alpha} c_\beta c_\alpha \bar{u}_\beta \bar{u}_\alpha \\ &= \sum_{\alpha<\beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta - \sum_{\beta>\alpha} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta = 0.\end{aligned}$$

Ahora bien, sea $\varphi\colon M \to A$ tal que $\varphi(\boldsymbol{m})^2 = 0$, en particular, $\varphi(\boldsymbol{u}_\alpha)\cdot\varphi(\boldsymbol{u}_\alpha) = 0$. Nótese que

$$0 = \varphi(\boldsymbol{u}_\alpha + \boldsymbol{u}_\beta)^2 = \cancel{\varphi(\boldsymbol{u}_\alpha)^2} + \cancel{\varphi(\boldsymbol{u}_\beta)^2} + \varphi(\boldsymbol{u}_\alpha)\varphi(\boldsymbol{u}_\beta) + \varphi(\boldsymbol{u}_\beta)\varphi(\boldsymbol{u}_\alpha).$$

Luego, podemos definir $f(\bar{u}_{\alpha_1}\cdots\bar{u}_{\alpha_n}) = \varphi(\boldsymbol{u}_{\alpha_1})\cdots\varphi(\boldsymbol{u}_{\alpha_n})$ que está bien definida por la observación anterior. □

Nótese que el uso de elección sólo se emplea si la base no viene con un buen orden canónico. En particular no es necesario si tiene rango numerable. De la demostración se concluye lo siguiente:

Corolario (AE) 10.40: Si M es un A-módulo libre de rango κ, entonces $\operatorname{rang}(E(M)) = 2^\kappa$.

Otra conclusión de la demostración es que $E(M)$ es de hecho un cociente sobre $T(M)$ y es fácil notar que el ideal empleado está generado por elementos homogéneos, de modo que $E(M)$ es también una álgebra graduada. Los elementos homogéneos de grado d son de la forma $\bar{m}_1\cdots\bar{m}_d$. Luego, si M es libre de rango n, entonces $E_d(M)$ es un A-módulo libre de rango $\binom{n}{d}$.

Corolario 10.41: Sea M un A-módulo con una álgebra exterior $E(M)$. Dado un endomorfismo de A-módulos $L\colon M \to M$, se puede construir un endomorfismo de A-álgebras $\eta(L)\colon E(M) \to E(M)$ dado por el siguiente diagrama conmutativo:

$$\begin{array}{ccc} M & \xrightarrow{\psi} & E(M) \\ {\scriptstyle L}\downarrow & & \vdots\,{\scriptstyle \exists!\eta(L)} \\ M & \xrightarrow[\psi]{} & E(M) \end{array}$$

Si $L_1, L_2 \in \operatorname{End}_{\mathsf{Mod}}(M)$ entonces:

$$\eta(1_M) = 1_{E(M)}, \qquad \eta(L_1 \circ L_2) = \eta(L_1) \circ \eta(L_2).$$

Además, $\eta(L)$ es un automorfismo de A-álgebras syss L es automorfismo de A-módulos.

El lector atento debería inmediatamente reconocer que la construcción $(E, \eta)\colon \mathsf{FMod}_A \to \mathsf{Alg}_A$ es un funtor.

Ahora veamos una conexión entre la álgebra exterior y los determinantes: Sea $L\colon M \to M$ un endomorfismo de M y sea $B := (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ una base ordenada de M. Definamos $L(\boldsymbol{u}_i) = \sum_{j=1}^n a_{ij}\boldsymbol{u}_j$, de modo que claramente $[a_{ij}]_{ij} = \mathrm{M}_B^B(L)$. Luego

$$\begin{aligned}\eta(L)(\bar{u}_1 \cdots \bar{u}_n) = L(\boldsymbol{u}_1)\cdots L(\boldsymbol{u}_n) &= \sum_{j_1=1}^n a_{1j_1}\bar{u}_{j_1} L(\boldsymbol{u}_2)\cdots L(\boldsymbol{u}_n)\\ &= \sum_{j_1=1}^n \cdots \sum_{j_n=1}^n a_{1j_1}\cdots a_{nj_n}\bar{u}_{j_1}\cdots\bar{u}_{j_n}.\end{aligned}$$

Ahora recordamos que $\bar{u}_{j_1}\cdots\bar{u}_{j_n}$ se anulará si hay indices repetidos, de modo que la única manera de que no se anule es que $j_k = \sigma(k)$ donde $\sigma \in S_n$ y obtenemos que

$$\begin{aligned}\eta(L)(\bar{u}_1 \cdots \bar{u}_n) &= \sum_{\sigma\in S_n} a_{1,\sigma(1)}\cdots a_{n,\sigma(n)}\bar{u}_{\sigma(1)}\cdots\bar{u}_{\sigma(n)}\\ &= \sum_{\sigma\in S_n} (\operatorname{sgn}\sigma) a_{1,\sigma(1)}\cdots a_{n,\sigma(n)}\bar{u}_1\cdots\bar{u}_n = (\det L)\bar{u}_1\cdots\bar{u}_n.\end{aligned}$$

Ésto nos otorga otra prueba, más directa aún, de que

$$\det(L_1 \circ L_2) = \det(L_1)\det(L_2).$$

Teorema 10.42: Sea k un cuerpo y sea $k[\{x_{ij} : 1 \le i, j \le n\}]$ el anillo de polinomios. Considere $X = [x_{ij}]_{ij} \in \mathrm{Mat}_n(k[x_{ij}]_{ij})$, luego $\det X \in k[x_{ij}]_{ij}$ es un polinomio irreducible.

Demostración: Procedemos por inducción sobre n, donde el caso base $n = 1$ es trivial. Por la proposición 3.54 sabemos que

$$\det X = \sum_{i=1}^n (-1)^{1+i} x_{1i} M_{i1}(X),$$

donde $M_{i1}(X)$ son los menores complementos de X. Sea $D \subseteq k[x_{ij}]_{ij}$ correspondiente al subanillo de polinomios sobre las indeterminadas x_{ij} con $(i,j) \neq (1,1)$. Luego $\det X = x_{11}X_{11} + Y$ con $X_{11} = M_{11}(X), Y \in D$. Por hipótesis inductiva, X_{11} es irreducible en D. Nótese que el grado de $\det X$ en D (i.e., respecto a x_{11}) es 1, luego, sus factorizaciones son de la forma $(Px_{11} + Q)R$ con $P, Q, R \in D$. $PR = X_{11}$, y como D es un anillo de polinomios, entonces es un DFU, luego (salvo asociados) $P \in \{1, X_{11}\}$. Si $P = X_{11}$ y $R = 1$ entonces corresponde a la factorización trivial.

Si $\det X$ fuese reducible, entonces su factorización sería $P = 1$ y $R = X_{11}$, entonces tenemos que $X_{11} \mid \det X$ en $k[x_{ij}]_{ij}$. Análogamente podemos concluir que $X_{ii} \mid \det X$ para todo $i \in \{1, 2, \ldots, n\}$. Luego

$$X_{11}X_{22}\cdots X_{nn} \mid \det X$$

en $k[x_{ij}]_{ij}$, donde el primer término tiene grado $\frac{n(n-1)}{2}$ el cual es mayor que n para todo $n > 2$ y es por tanto absurdo. Para $n = 2$ se tiene que $x_{11}x_{22} \mid (x_{11}x_{22} - x_{12}x_{21})$ lo cual también es absurdo. □

Teorema 10.43: Sea k un cuerpo infinito y sea $k[\{x_{ij} : 1 \leq i, j \leq n\}]$ el cual podemos ver como un anillo de polinomios con indeterminadas en $\mathrm{Mat}_n(k)$. Supongamos que $Q(X) \in k[x_{ij}]_{ij}$ es un polinomio homogéneo de grado q tal que:

1. $Q(I_n) = 1$.
2. $Q(A \cdot B) = Q(A)Q(B)$ para todos $A, B \in \mathrm{Mat}_n(k)$.

Entonces $Q(X)$ es una potencia de $\det X$.

Demostración: En primer lugar, nótese que para todo $A \in \mathrm{Mat}_n(k)$ se tiene que

$$Q(A)Q(\operatorname{adj} A) = Q(A \cdot \operatorname{adj} A) = Q((\det A)I_n) = (\det A)^q.$$

Sabemos que la coordenada $(\operatorname{adj} X)_{ij} = (-1)^{i+j}M_{ji}(X)$ la cual es un polinomio en $k[x_{ij}]_{ij}$, de modo que $Q(\operatorname{adj} X)$ es también un polinomio en $k[x_{ij}]_{ij}$.

Luego $P(X) := Q(X)Q(\operatorname{adj} X) - (\det X)^q \in k[x_{ij}]_{ij}$ es un polinomio que evaluado en todas las matrices $A \in \mathrm{Mat}_n(k)$ se anula, y como k es infinito, eso implica que $P(X) = 0 \in k[x_{ij}]_{ij}$, de modo que $Q(X) \cdot Q(\operatorname{adj} X) = (\det X)^q$, o lo que es equivalente, $Q(X) \mid (\det X)^q$. Como $\det X \in k[x_{ij}]_{ij}$ es irreducible y $k[x_{ij}]_{ij}$ es un DFU se concluye que $Q(X)$ es una potencia de $\det X$ como se quería probar. □

De hecho, con ello se demuestra que $q = n^r$ y por igualdad de grados nos queda que $Q(X) = (\det X)^r$.

§10.2.2 Representaciones.

Definición 10.44: Sea M un A-módulo, entonces podemos ver a $\mathrm{End}_{\mathsf{Mod}}(M)$ como una A-álgebra: donde $1 \in \mathrm{End}(M)$ es $1 = \mathrm{Id}_M$, $L_1 + L_2$ y $\alpha \cdot L$ son las operaciones coordenada a coordenada y $L_1 \cdot L_2 := L_1 \circ L_2 \in \mathrm{End}(M)$.

El álgebra de endomorfismos nos otorga de hecho un teorema similar al de Cayley para grupos:

Teorema 10.45: Sea B un A-álgebra, entonces B es isomorfo a una subálgebra de $\mathrm{End}_{\mathsf{Mod}}(B)$.

Demostración: Para todo $b \in B$ definimos $\mu_b(c) := c \cdot b$ el cual es una función sobre B y es fácil notar que μ_b es un endomorfismo de A-módulos. Luego la aplicación $b \mapsto \mu_b$ es un monomorfismo de A-álgebras (¡demuéstrelo!) cuya imagen es una subálgebra de $\mathrm{End}_{\mathsf{Mod}}(B)$. □

Supongamos que B es un A-módulo libre de rango n, luego $\mathrm{End}_{\mathsf{Mod}}(B) = \mathrm{End}_{\mathsf{Mod}}(A^n) = \mathrm{Mat}_n(A)$. Así pues, a todos los elementos de B les asignamos un enfomorfismo de A-módulos, el cual llamamos ***una representación*** del elemento y, en particular, el endomorfismo dado por la multiplicación derecha es llamado ***la representación regular***. En particular, para todo $b \in B$ podemos asignarle una traza, norma y polinomio característico:

$$\mathrm{Tr}_{B/A}(b) := \mathrm{tr}(\mu_b), \quad \mathrm{Nm}_{B/A}(b) := \det(\mu_b), \quad \psi_{b,B/A}(x) := \psi_{\mu_b}(x) \in k[x].$$

Nótese que éstos son los mismos invariantes introducidos en el capítulo de teoría de Galois (cf. §4.5.1).

10.3* El problema de Hurwitz

§10.3.1 El problema aritmético de Hurwitz. Comencemos con un problema, más relacionado a la aritmética que al álgebra, basado en sumas de cuadrados. En general, es conocida la identidad:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{10.2}$$

que tiene la ventaja de corresponder con la compacta $|\alpha\beta|^2 = |\alpha|^2|\beta|^2$ para $\alpha, \beta \in \mathbb{C}$. Ésta famosa identidad era conocida desde los griegos, y Euler encontró otra parecida para cuatro términos:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2, \tag{10.3}$$

donde

$$\begin{aligned} z_1 &= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, \\ z_2 &= x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3, \end{aligned}$$

$$z_3 = x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2,$$
$$z_4 = x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1.$$

Una de las particularidades es que éstas identidades son *puramente* algebraicas, en el sentido de que son válidas sobre cualquier cuerpo. Naturalmente que uno puede ser tramposo y trabajar en $\mathbb{F}_2$ en donde el sueño del aprendiz nos otorga identidades para todo n, por ello se imponen éstas restricciones. Para continuar el patrón en 1822 C. F. Degan encontró otra identidad para $n = 8$ cuadrados. Ésto establece la curiosa insinuación de que éstas identidades sólo aparecen en potencias de dos y, siguiendo un olfato matemático, uno se vería tentado a buscar una identidad para $n = 16$.

En 1898, Hurwitz ahondó en ésta pregunta, lo que nos devuelve al contexto de álgebras: ya mencionamos que para la identidad (10.2) tenemos una intuición asociada a los complejos $\mathbb{C}$, pero para (10.3) podemos encontrar una fórmula asociada al álgebra de los cuaterniones $\mathbb{H}$ propuesta por Hamilton y para la identidad de 8 términos de Degan podemos asociar otra álgebra, cuyos elementos se conocen como los ***octoniones*** de Cayley (1845). Así pues, la pregunta tiene un estrecho vínculo con el estudio de álgebras.

Formalizando, la pregunta es la siguiente: dado $n > 0$ existe una identidad de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \tag{10.4}$$

donde cada z_ℓ es una función bilineal sobre x_i e y_j. Para arruinar la sorpresa ésto sólo funciona para $n \in \{1, 2, 4, 8\}$, ésto lo iremos probando progresivamente.

Comencemos por reformular el problema (10.4): buscamos que $z_i = \sum_{j=1}^n a_{ij}y_j$, donde cada a_{ij} es una función lineal sobre $\{x_1, \ldots, x_n\}$. Definiendo $A = [a_{ij}]_{ij}$, vemos que buscamos una fórmula del estilo:

$$\boldsymbol{Z} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = A\boldsymbol{Y}.$$

que satisfaga que

$$(x_1^2 + \cdots + x_n^2) \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} I_n = (x_1^2 + \cdots + x_n^2)\boldsymbol{Y}^t\boldsymbol{Y} I_n$$
$$= \boldsymbol{Z}^t\boldsymbol{Z} = \boldsymbol{Y}^t A^t A\boldsymbol{Y}.$$

Reordenando se obtiene que

$$(x_1^2 + \cdots + x_n^2)I_n - A^tA = \mathbf{0}.$$

Como cada a_{ij} es una función lineal de los $\{x_1, \ldots, x_n\}$, entonces tenemos que

$$a_{ij} = b_{ij}^1 x_1 + b_{ij}^2 x_2 + \cdots + b_{ij}^n x_n,$$

donde en b_{ij}^ℓ el ℓ es un superíndice, no un exponente. Definiendo $B_\ell := [b_{ij}^\ell]_{ij}$, se tiene que

$$A = B_1 x_1 + \cdots + B_n x_n.$$

De modo que buscamos que

$$(x_1^2 + \cdots + x_n^2)I_n = (B_1^t x_1 + \cdots + B_n^t x_n)(B_1 x_1 + \cdots + B_n x_n).$$

Como aplica para todo $x_i \in k$, entonces podemos elegir $x_j = \delta_{ij}$ para algún i fijo (es decir, todos los x_j's nulos exceptuando el $x_i = 1$) de modo que obtenemos que:

- $B_i^t B_i = I_n$ para todo i.
- $B_i^t B_j + B_j^t B_i = \mathbf{0}$ para $i \neq j$.

Podemos definir $C_i := B_n^t C_i$ y un cálculo comprueba:

1. $C_i^t C_i = I_n$. En consecuencia, $\det(C_i) \neq 0$.
2. $C_i^t + C_i = \mathbf{0}$ o $C_i^t = -C_i$.
3. $C_i^t C_j + C_j^t C_i = \mathbf{0}$ con $i \neq j$.
4. $C_i^2 = -I_n$ para $i \neq n$ (por 1 y 2).
5. $C_i C_j = -C_j C_i$ para $i \neq j$ (por 3 y 2).

Sabemos que $\det(C_i) = \det(C_i^t) = \det(-C_i) = (-1)^n \det(C_i)$ luego n es necesariamente par y hemos probado:

Proposición 10.46: No existe una identidad (10.4) si n es impar.

Considere el conjunto $\mathcal{G}$ de los elementos de la forma $G = C_{i_1} \cdots C_{i_r}$ con $i_1 < i_2 < \cdots < i_r < n$, junto con la identidad. Así pues, los elementos de $\mathcal{G}$ están en correspondencia con los subconjuntos de $\{1, 2, \ldots, n-1\}$ por lo que contiene $\leq 2^{n-1}$ elementos (puesto que tal vez se repitan).

(I) G es simétrica syss $r \equiv 0$ o $3 \pmod 4$, en caso contrario es antisimétrica: Basta notar que

$$\begin{aligned} G^t &= C_{i_r}^t \cdots C_{i_1}^t = (-1)^r C_{i_r} \cdots C_{i_1} \\ &= (-1)^r (-1)^{r-1} C_{i_1} (C_{i_r} \cdots C_{i_2}) \\ &= (-1)^r (-1)^{r-1} \cdots (-1)^1 C_{i_1} \cdots C_{i_r} = (-1)^{1+2+\cdots+r} G = (-1)^{\frac{r(r-1)}{2}} G. \end{aligned}$$

(II) Si $M \in \mathcal{G}$ entonces $M\mathcal{G}$ es una permutación de $\mathcal{G}$ quizas alternando algunos signos: Si $M = C_1$ entonces es claro, puesto que si $MG \in \mathcal{G}$ si G no contiene a C_1 y $-MG \in \mathcal{G}$ si G sí contiene a C_1.

Por simetría, vemos que si $C_1C_2H = C_2C_1H$, de modo que podemos readaptar el caso anterior si $M = C_2$. Análogamente si $M = C_i$ para cualquier C_i con $i < n$. Empleando recursivamente éstos hechos, se concluye en el caso general.

Una *relación* R es una combinación lineal

$$R: \quad \lambda_1 G_1 + \cdots + \lambda_n G_n = 0,$$

válida para las matrices $G_i \in \mathcal{G}$. Se dice que la relación es *irreducible* si no se puede escribir de forma $R = R_1 + R_2$ con $R_1 = 0 = R_2$, donde R_1, R_2 no tienen matrices en común.

(III) Una relación irreducible $R = 0$ no puede involucrar tanto matrices simétricas y antisimétricas: Sea M_1 la subrelación de R que sólo involucra matrices simétricas y M_2 la subrelación que involucra antisimétricas. Si $R = M_1 + M_2 = 0$, entonces $M_1 = -M_2$. Pero $M_1 = M_1^t = -M_2^t = M_2$ (donde aquí, $()^t$ significa trasponer todas las matrices en la relación, lo cual es aditivo). Por ende, $M_1 = M_2 = 0$ y por irreducibilidad se tiene que $R = 0$.

Prosigamos: sea $R = 0$ una relación irreducible no-trivial sobre $\mathcal{G}$. Podemos tomar una matriz M involucrada en R y multiplicar todo por G^{-1} y por un escalar para obtener otra relación T también no-trivial e irreducible (¿por qué?) que involucre a la matriz identidad I_n, de modo que, reordenando nos queda que

$$I_n = \sum_{i_1 < n} \alpha_{i_1} C_{i_1} + \sum_{i_1 < i_2 < n} \alpha_{i_1, i_2} C_{i_1} C_{i_2} + \cdots, \tag{10.5}$$

por la propiedad (III) se cumple que los productos C_{i_1}, $C_{i_1}C_{i_2}$ y demáses, deben ser matrices simétricas, por lo que, por la propiedad (I) se cumple que no hay productos de uno o dos términos.

§10.3.2 Álgebras de composición y su clasificación.

Definición 10.47: Se dice que un par (B, Q) es una ***A-álgebra de composición*** si:

1. B es una A-álgebra (posiblemente no asociativa) y $Q\colon B \to A$ es una forma cuadrática no degenerada.
2. Para todo $b, c \in B$ se cumple $Q(bc) = Q(b)Q(c)$.

Se denota por

$$\beta(x, y) := Q(x + y) - Q(x) - Q(y)$$

a la forma bilineal simétrica asociada a Q.

Nótese que $Q(x + y)Q(z) = Q(x)Q(z) + Q(y)Q(z) = Q(xz + yz)$, de modo que como $Q(x) + \beta(x, y) + Q(y) = Q(x + y)$ se obtiene que:

$$\begin{aligned} Q(x)Q(z) + \beta(x, y)Q(z) + Q(y)Q(z) &= Q(x + y)Q(z) = Q(xz + yz) \\ &= Q(xz) + \beta(xz, yz) + Q(yz). \end{aligned}$$

Con lo que hemos probado que

$$\beta(x, y)Q(z) = \beta(xz, yz), \qquad Q(x)\beta(y, z) = \beta(xy, xz).$$

Con un cálculo es fácil comprobar que

$$\beta(x, y)\beta(z, w) = \beta(xz, yw) + \beta(yz, xw) = \beta(zx, wy) + \beta(zy, wx), \quad (10.6)$$

donde para la última igualdad recordamos que el anillo base A es conmutativo, de modo que conmutamos los primeros factores.

Definimos la siguiente aplicación:

$$\begin{aligned} \overline{()}\colon \beta &\longrightarrow \beta \\ x &\longmapsto \beta(x, 1)1_B - x. \end{aligned}$$

Aquí el 1_B enfatiza el hecho de que es la unidad de B. Nótese que $\overline{()}$ es un endomorfismo de A-módulos.

Lema 10.48: Sea (B, Q) una A-álgebra de composición. Para todo $x, y \in B$ se tiene lo siguiente:

1. $\overline{()}$ es una involución (i.e., $\bar{\bar{x}} = x$) y $Q(\bar{x}) = Q(x)$.

2. $\bar{x}x = x\bar{x} = Q(x)1$.

3. $\bar{x}(xy) = (\bar{x}x)y = Q(x)y$.

4. $(yx)\bar{x} = y(x\bar{x}) = Q(x)y$.

5. $\overline{xy} = \bar{y}\bar{x}$.

Recuerde que las identidades son destacables porque B puede no ser asociativa en general.

Demostración:

1. Ejercicio.

2. Primero, nótese que

$$\begin{aligned}\beta(x, \bar{y}z) &= \beta\big(x, \beta(y,1)z - yz\big) = \beta(y,1)\beta(x,z) - \beta(x,yz) \\ &= \beta(yx,z) + \cancel{\beta(yz,x)} - \cancel{\beta(x,yz)} = \beta(yx,z),\end{aligned}$$

donde empleamos la identidad (10.6). Con un razonamiento análogo concluimos que

$$\beta(x,\bar{y}z) = \beta(yx,z), \qquad \beta(xy,z) = \beta(x,z\bar{y}), \tag{10.7}$$

luego, nótese que

$$Q(x)\beta(1,y) = \beta(x,xy) = \beta(x,\bar{\bar{x}}y) = \beta(\bar{x}x,y),$$

o lo que es equivalente, $\beta(Q(x)1 - \bar{x}x, y) = 0$ para todo y. Como β es una forma bilineal no degenerada, se concluye que necesariamente $Q(x)1 = \bar{x}x$. Para la otra igualdad, sustituimos x por $\bar{x}$:

$$x\bar{x} = \bar{\bar{x}}\bar{x} = Q(\bar{x})1 = Q(x)1.$$

3. Siga el siguiente procedimiento:

$$\begin{aligned}\beta(\bar{x}(xy),z) &= \beta\big((\beta(x,1)1 - x)(xy), z\big) \\ &= \beta(x,1)\beta(xy,z) - \beta(x(xy),z) \\ &= \cancel{\beta(x(xy),z)} + \beta(xz,xy) - \cancel{\beta(x(xy),z)} \\ &= Q(x)\beta(z,y) = Q(x)\beta(y,z) = \beta(Q(x)y,z).\end{aligned}$$

4. Ejercicio.

5. Nótese que por la identidad (10.7)

$$\beta\big((\overline{xy})1, z\big) = \beta(1, \overline{\overline{xy}}z) = \beta(1, (xy)z).$$

Veremos lo mismo para la otra:

$$\begin{aligned}\beta(\bar{y}\bar{x}, z) &= \beta\big((\beta(y,1)1 - y)(\beta(x,1)1 - x), z\big)\\ &= \beta(y,1)\beta(x,1)\beta(1,z) - \beta(y,1)\beta(x,z) - \beta(x,1)\beta(y,z) - \beta(yx,z).\end{aligned}$$

Desarrollemos algunos términos por separado:

$$\begin{aligned}\beta(y,1)\beta(x,z) &= \beta(yx,z) + \beta(yz,x)\\ \beta(y,1)\beta(x,1) &= \beta(x,1)\beta(y,x) = \beta(xy,1) + \beta(x,y)\\ \beta(xy,1)\beta(1,z) &= \beta(xy,z) + \beta((xy)z,1)\\ \beta(x,1)\beta(y,z) &= \beta(xy,z) + \beta(xz,y)\end{aligned}$$

Cancelando los términos apropiadamente obtenemos que

$$\begin{aligned}\beta(\bar{y}\bar{x}, z) &= \beta((xy)z,1) + \beta(x,y)\beta(1,z) - \beta(yz,x) - \beta(xz,y)\\ &= \beta((xy)z,1).\end{aligned}$$

□

Definición 10.49: Sea B una A-álgebra. Para $x, y, z \in B$ se define el ***asociador***:

$$[x, y, z] := (xy)z - x(yz).$$

Nótese que el asociador es una forma trilineal y que es idénticamente nulo syss B es una álgebra asociativa. La álgebra B se dice ***alternativa*** si para todo $x, y \in B$ se cumple que

$$[x, x, y] = 0 = [y, x, x].$$

Corolario 10.50: Toda álgebra de composición es alternativa.

Demostración: Basta emplear el hecho de que $\overline{x} = \beta(x,1)1 - x$ y las propiedades 3 y 4 del lema anterior. □

El nombre de álgebra alternativa deriva de un hecho muy simple: una álgebra es alternativa syss el asociador es una forma multilineal alternada, y ya hemos visto que toda forma multilineal alternada es antisimétrica. En particular, $[x, y, x] = -[x, x, y] = 0$, de modo que podemos definir $xyx := (xy)x$ en una álgebra alternativa.

Proposición 10.51: Sea B una A-álgebra alternativa. Entonces para todo $x, y, z \in B$ se cumple que

$$(ux)(yu) = u(xy)u, \tag{10.8}$$

la que se conoce como ***identidad de Moufang***.

Demostración: Nótese que como el asociador es alternante, $[u, x, y] = [x, y, u]$, lo que equivale a que

$$(ux)y + x(yu) = u(xy) + (xy)u.$$

Luego siga el siguiente procedimiento:

$$\begin{aligned}(u^2x)y + 2(ux)(yu) + x(yu^2) &= u((ux)y) + u(x(yu)) + ((ux)y)u + (x(yu))u \\ &= u\big((ux)y + x(yu)\big) + \big((ux)y + x(yu)\big)u \\ &= u\big(u(xy) + (xy)u\big) + \big(u(xy) + (xy)u\big)u \\ &= u^2(xy) + 2u(xy)u + (xy)u^2,\end{aligned}$$

con lo que aplicamos la igualdad inicial y concluimos que $2((ux)(yu) - u(xy)u) = 0$. □

Probar caso característica = 2.

Teorema 10.52: Sea B una A-álgebra. Son equivalentes:

1. B es una álgebra alternada con una involución $\overline{()}\colon B \to B$ tal que $\overline{x}x = Q(x)$, donde $Q\colon B \to A$ es una forma cuadrática no degenerada.
2. (B, Q) es una álgebra de composición.

Demostración: Ya tenemos probado que $2 \implies 1$. Veamos el recíproco: En primer lugar nótese que

$$\begin{aligned}(\cancel{Q(x)} + \beta(x, y) + \cancel{Q(y)})1 &= Q(x + y)1 \\ &= \overline{(x + y)}(x + y) = \cancel{\bar{x}x} + \bar{y}x + \bar{x}y + \cancel{\bar{y}y}, \end{aligned} \tag{10.9}$$

Aplicando $y = 1$ se obtiene que $\bar{x} + x = \beta(x, 1)1 =: T(x)1$ lo que sumado a la asociatividad de $[x, x, y] = 0$ nos da que $\bar{x}(xy) = (\bar{x}x)y = Q(x)1$. Recuerde que la propiedad $\overline{xy} = \bar{y}\bar{x}$ se demostraba únicamente empleando las proposiciones anteriores, de modo que también es válido aquí. Luego:

$$\begin{aligned}Q(xy)1 = \overline{xy}(xy) = (\bar{y}\bar{x})(xy) &= \big((T(y)1 - y)\bar{x}\big)(xy) \\ &= T(y)\bar{x}(xy) - (y\bar{x})(xy) = T(y)Q(x)y - y(\bar{x}x)y \\ &= Q(x)(T(y) - y)y = Q(x)\bar{y}y = Q(x)Q(y)1.\end{aligned}$$

□

Definición 10.53: Sea B una A-álgebra con una involución $\overline{()}\colon B \to B$ tal que $\bar{x}x = Q(x)1$, donde Q es una forma cuadrática no degenerada; y sea $c \in A_{\neq 0}$. Definimos el ***c*-duplicado** de B como el A-módulo $C := B \times B$ dotado del producto:

$$(u, v) \cdot (x, y) := (ux + c\bar{y}v, yu + v\bar{x}).$$

Veamos algunas propiedades del c-duplicado:

- Es claro que $\cdot$ es una forma bilineal de modo que el c-duplicado es una A-álgebra.
- $(1, 0)$ es el neutro de $\cdot$. En consecuencia, denotamos $1 := (1, 0)$
- $(u, 0)(x, 0) = (ux, 0)$ y $(0, v)(0, y) = (c\bar{y}v, 0)$.
- La aplicación $\overline{(x, y)} := (\bar{x}, -y)$ es una involución.
- $$\overline{(x, y)} \cdot (x, y) = (\bar{x}, -y)(x, y) = (\bar{x}x - c\bar{y}y, y\bar{x} - y\bar{x}) = \big(Q(x) - cQ(y)\big)1.$$
- Definiendo $Q_C(x, y) := Q(x) - cQ(y)$ notamos que es de hecho una forma cuadrática y que su forma bilineal asociada:
$$\beta_C\big((u, v), (x, y)\big) = \beta(u, x) - c\beta(v, y)$$
es no degenerada.

Teorema 10.54: Sea B una A-álgebra y C su c-duplicado. Entonces:

1. C es conmutativo y asociativo syss B lo es y $\bar{x} = x$.
2. C es asociativo syss B es conmutativo y asociativo.
3. C es alternativo syss B es asociativo.

Demostración: Recordemos que el conmutador es $[\alpha, \beta] := \beta\alpha - \alpha\beta$. Como B es una subálgebra de C, entonces hereda todas sus propiedades. Sean $X := (x, y), U := (u, v), Z := (z, w) \in C$, luego:

$$[U, X] = \big([x, u] + c(\bar{y}v - \bar{v}y), [u, y] + v\bar{x} - x\bar{v}\big) \tag{10.10}$$

aplicando $u = 0 = x$ y $v = 1$ se obtiene que la conmutatividad implicar que $\bar{y} = y$ para todo $y \in B$. El recíproco es claro, de modo que hemos probado 1.

El asociador es más complicado:

$$[U, X, Z] = \big([u, v, x] + c(\bar{w}(yu) - u(\bar{w}y) + \bar{w}(v\bar{x}) - (\bar{x}\bar{w})v + (\bar{y}v)z - (z\bar{y})v, \\ w(ux) - (wx)u + (yu)\bar{z} - (y\bar{z})u + (v\bar{x})\bar{z} - (v\bar{z})\bar{x} + c(w(\bar{y}v) - v(\bar{y}w)))\big). \tag{10.11}$$

Si C es asociativo, entonces B lo es y empleando (10.11) con $v = x = z = 0$ y $t = 1$ se obtiene que $yu = uy$ lo que comprueba la conmutatividad de B. Si B es conmutativo y asociativo, entonces es claro que el asociador siempre se anula, de modo que hemos probado 2.

Para la 3, veamos $\Longleftarrow$: queremos probar que $[X, X, Z] = 0$, pero nótese que como $X + \bar{X} = T(X)1$, donde $T(X) = \beta(x, 1)$, vemos que equivale a probar que $[\bar{X}, X, Z] = 0$. Aplicando la involución se obtiene

$$\overline{[X, Y, Z]} = \overline{(XY)Z - X(YZ)} = \bar{Z}(\bar{Y}\bar{X}) - (\bar{Z}\bar{Y})\bar{X} = -[\bar{Z}, \bar{Y}, \bar{X}].$$

De modo que también concluye el caso restante. Si B es alternativo, entonces empleando $U = \bar{X}$ en (10.11) y recordando que $[\bar{x}, y, x] = 0$ y que $w(\bar{y}y) = y(\bar{y}w)$ y análogos, se obtiene que

$$[\bar{X}, X, Z] = \big(c[\bar{x}, \bar{w}, y], -[y, \bar{z}, \bar{x}]\big),$$

lo que es claramente cero si B es asociativa, y recíprocamente si C es alternante entonces la fórmula de arriba permite concluir asociatividad en B. □

Por éste teorema, los duplicados permiten la siguiente jerarquía de álgebras de composición: Sea A un anillo base que es conmutativo (y asociativo), luego duplicándolo (como álgebra) mediante la involución identidad obtenemos las ***álgebras cuadráticas***, que tienen rango 2 y son conmutativas. Duplicando otra vez con una involución que no es la identidad obtenemos las ***álgebras cuaterniónicas*** que tienen rango 4 y no son conmutativas, pero sí son asociativas. Duplicando otra vez obtenemos las ***álgebras octoniónicas*** que tienen rango 8 y no son asociativas.

Lema 10.55: Sea (B, Q) una A-álgebra de composición y sea C una subálgebra propia de B que es invariante por $\overline{()}$ y tal que Q es no degenerada en C. Entonces C está encajado en una subálgebra de B que es también de composición y que es isomorfa a un c-duplicado de C.

Demostración: En primer lugar, nótese que como $Q|_C$ es no degenerada, entonces induce un producto interno y por descomposición ortogonal $B = C \oplus C^\perp$. Sea $t \in C^\perp$ tal que $c := -Q(t) \neq 0$. Como C es una subálgebra, entonces $1 \in C$ y luego $\beta(1,t) = 0$ de modo que $\bar{t} = -t$ y $t^2 = -\bar{t}t = -Q(t)1 = c1$. Por la ec. (10.9) se tiene que para todo $x \in C$ se cumple

$$\bar{x}t + \bar{t}x = \beta(x,t) = 0 \iff \bar{x}t = tx.$$

Sean $x, y \in C$ arbitrarios. Luego, por (10.7), se tiene que $\beta(x, yt) = \beta(\bar{y}x, t) = 0$ puesto que $\bar{y}x \in C$; de modo que $C \cdot t \subseteq C^\perp$ y $D := C \oplus C \cdot t$.

Como B es de composición se tiene que $\bar{x}(xy) = Q(x)y$, de lo que se deduce que

$$\bar{x}(zy) + \bar{z}(xy) = \beta(x,z)y,$$

empleando $z = t$ se obtiene que $\bar{x}(ty) = t(xy) = (\bar{y}\bar{x})t$ lo que, sustituyendo por sus conjugados nos da que

$$x(yt) = (yx)t.$$

Luego aplique $\overline{()}$ y nótese que

$$\bar{t}(\bar{x}\bar{y}) = (\bar{t}\bar{y})\bar{x} \iff \overline{(\bar{x}\bar{y})}t = (yx)t = (yt)\bar{x},$$

sustituyendo x por $\bar{x}$ se obtiene que $(yt)x = (y\bar{x})t$. Por último,

$$(xt)(yt) = (t\bar{x})(yt) = t(\bar{x}y)t = (\bar{y}x)t^2 = c\bar{y}x.$$

Empleando todo ésto, se tiene que el producto en D está determinado por

$$(u + vt)(x + yt) = ux + c\bar{y}v + (v\bar{x} + yu)t,$$

que es claramente isomorfo al c-duplicado de C. □

Teorema 10.56 – *Teorema de Hurwitz*: Sea A un dominio con $\operatorname{car} A \neq 2$. Las álgebras de composición son las siguientes:

(a) A.

(b) Las álgebras cuadráticas.

(c) Las álgebras cuaterniónicas.

(d) Las álgebras octoniónicas.

Demostración: Sea (B, Q) una A-álgebra de composición. Si $B = A$ entonces estamos en el caso (a), y si no $A \subset B$ en cuyo caso, por el lema anterior, B contiene una A-álgebra cuadrática B_1 no degenerada e invariante salvo $\overline{()}$; si $B_1 = B$ estamos en el caso (b). De lo contrario, B_1 está contenido en una subálgebra cuaterniónica B_2 y si ésta no es toda el álgebra, entonces B_2 está contenida en un álgebra octoniónica. En cada paso fuimos perdiendo propiedades de modo que que las álgebras octoniónicas no son asociativas y, por ende, no podemos duplicar la construcción. □

§10.3.3 Aplicación: álgebras de división. Veamos ahora cómo se emplea la clasificación de Hurwitz sobre tres casos particulares:

Teorema 10.57: Sea k un cuerpo algebraicamente cerrado. Entonces k no posee álgebras de división finitamente generadas impropias.

Demostración: Sea A una k-álgebra finitamente generada, entonces se trata de un k-espacio vectorial de dimensión finita digamos n, y, por ende, para todo $\beta \in k$ se cumple que $\{1, \beta, \beta^2, \ldots, \beta^n\}$ es un conjunto linealmente dependiente, luego, podemos reorganizar la dependencia lineal y obtener que β es raíz de algún polinomio $p(x) \in k[x]$, de modo que β es k-algebraico. Más aún, $k(\beta)$ tiene que ser claramente un cuerpo (la conmutatividad se sigue trivial de la conmutatividad de las potencias de β, y los inversos del hecho de que A es de división), luego es una extensión algebraica, pero entonces $k(\beta) = k$ y $\beta \in k$. □

Teorema 10.58 – *Teorema de Frobenius*: Las $\mathbb{R}$-álgebras de división alternativas finitamente generadas son: $\mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$.

Demostración: Sea A una $\mathbb{R}$-álgebra de división finitamente generada, $\mathbb{R} \cdot 1 \subseteq A$ es una subálgebra que identificaremos como $\mathbb{R}$ mismo. Sea A' el conjunto de elementos $u \in A$ tales que $u^2 \in \mathbb{R}$ y $u^2 \leq 0$.

A' es un subespacio vectorial de A: Claramente si $u \in A'$ entonces $\lambda u \in A'$ para todo $\lambda \in \mathbb{R}$. Sean $u, v \in A'$, queremos ver que $u + v \in A'$ y basta comprobar el caso en que son linealmente independientes (¿por qué?) y, en particular, no nulos. Nótese que no se puede dar que $u = \alpha v + \beta$ con $\alpha, \beta \in \mathbb{R}$ de lo contrario:

$$\alpha^2 v^2 + \beta^2 + 2\alpha\beta v = (\alpha v + \beta)^2 = u^2 \in \mathbb{R},$$

y como $v \notin \mathbb{R}$ se cumple que $\alpha\beta = 0$ lo cual sería absurdo. En consecuencia, $\{1, u, v\}$ son linealmente independientes. Por construcción, u, v son raíces de

polinomios cuadráticos, luego también lo son $u+v, u-v$ y, por lo tanto, existen $p, q, r, s \in \mathbb{R}$ tales que

$$(u+v)^2 = p(u+v) + q, \qquad (u-v)^2 = r(u-v) + s.$$

Como $(u \pm v)^2 = u^2 \pm (uv+vu) + v^2$, $u^2 = c < 0$ y $v^2 = d < 0$ se obtiene que

$$\begin{aligned} c + d + (uv+vu) &= p(u+v) + q, \\ c + d - (uv+vu) &= r(u-v) + s. \end{aligned}$$

Sumando ambas ecuaciones se obtiene que $(p+r)u + (p-r)v + (q+s-2c-2d) = 0$ y por independencia lineal se concluye que $p = r = 0$ y $q + s < 0$. Luego alguno de los dos $u+v$ o $u-v$ están en A'.

Empleando el mismo truco de la demostración anterior, vemos que todo $\beta \in A \setminus \mathbb{R}$ es raíz de algún polinomio irreducible en $\mathbb{R}[x]$ no lineal, los cuales son polinomios cuadráticos, digamos raíz de $p(x) = x^2 - 2ax + b$, con discriminante negativo, es decir, $a^2 < b$. Apliquemos

$$p(\beta + a) = \beta^2 + 2a\beta + a^2 - 2a(\beta - a) + b = b - a^2 < 0,$$

de modo que $\beta + a = \gamma \in A'$ y se comprueba que $A = \mathbb{R} \oplus A'$ (como $\mathbb{R}$-espacio vectorial).

Sea $u \in A'$ definamos $Q(u) := -u^2 \in \mathbb{R}$ y nótese que $Q(u) \geq 0$, donde $Q(u) = 0$ syss $u = 0$. Podemos notar que $\beta(u,v) := -(u+v)^2 + u^2 + v^2 = -(uv+vu)$ es una forma bilineal simétrica y que Q es su forma cuadrática asociada, la cual es positiva definida.

Ahora por fin podemos completar la demostración: Si $A = \mathbb{R}$ entonces estamos listos. Si no, buscamos $\mathrm{i} \in A'$ tal que $Q(\mathrm{i}) = 1$ y notamos que $\mathrm{i} = -1$, luego $\mathbb{R}[\mathrm{i}] = \mathbb{R} \oplus \mathbb{R} \cdot \mathrm{i}$ es una subálgebra conmutativa de A. Si $A \supset \mathbb{R}[\mathrm{i}]$, entonces existe $\mathrm{j} \perp \mathbb{R}\mathrm{i}$ tal que $Q(\mathrm{j}) = 1$, luego $\mathrm{j}^2 = -1$ y $-\beta(\mathrm{i},\mathrm{j}) = \mathrm{ij} + \mathrm{ji} = 0$ de modo que $\mathrm{ij} = -\mathrm{ji}$. Definiendo $\mathrm{k} := \mathrm{ij}$, vemos que

$$\mathrm{k} = -\mathrm{ji},\ \mathrm{k}^2 = -1,\ \mathrm{ik} + \mathrm{ki} = 0 = \mathrm{jk} + \mathrm{kj},$$

por lo que $R[\mathrm{i},\mathrm{j}] = \mathbb{R} \oplus \mathbb{R}\mathrm{i} \oplus \mathbb{R}\mathrm{j} \oplus \mathbb{R}\mathrm{k}$ es una subálgebra asociativa isomorfa a $\mathbb{H}$ de A. Si $A \subset \mathbb{H}$, entonces también podemos proceder a encontrar otro elemento con el que dubplicar a $\mathbb{H}$ y obtener a $\mathbb{O}$, y por el teorema de Hurwitz no podemos seguir extendiendo las álgebras. $\square$

Teorema 10.59 – *Teorema de Wedderburn*: Todo anillo de división finito es un cuerpo.

Demostración: Sea A un anillo de división finito de centro F, el cual es necesariamente un cuerpo. Definamos $q := |F|$ y $n := [A : F]$, de modo que $|A| = q^n$. $A^\times = A_{\neq 0}$ es un grupo multiplicativo y $F^\times$ actúa sobre él, de modo que, por la ecuación de clases se obtiene

$$|A^\times| = q^n - 1 = \sum_a [A^\times : \mathrm{Stab}_a] = q - 1 + \sum_{a \notin F} [A^\times : \mathrm{Stab}_a],$$

donde a recorre representantes en las clases de equivalencia de la conjugación. Si $x_i \notin F$, entonces Stab_{x_i} es un subgrupo multiplicativo y, más aún, $F_i := \mathrm{Stab}_{x_i} \cup \{0\}$ es un subanillo de división de A y claramente $F \subset F_i$ de modo que $|F_i| = q^{d_i}$ con $d_i < n$ luego

$$[A^\times : F_i^\times] = \frac{q^n - 1}{q^{d_i} - 1},$$

por lo que

$$q^n - 1 = q - 1 + \sum_i \frac{q^n - 1}{q^{d_i} - 1}. \tag{10.12}$$

Nótese además que A es claramente un F_i-módulo para todo i, de modo que $d_i \mid n$.

Ahora procedemos por contradicción: si $n > 1$, entonces podemos considerar un análogo de la fórmula (10.12) entre polinomios. Recordemos que $x^n - 1 = \prod_{d|n} \Phi_d(x)$, donde $\Phi_d(x) \in \mathbb{Z}[x]$ es el d-ésimo polinomio ciclotómico; luego

$$\frac{x^n - 1}{x^{d_i} - 1} = \frac{\prod_{d|n} \Phi_d(x)}{\prod_{d|d_i} \Phi_d(x)} = \prod_{\substack{d|n \\ d \nmid d_i}} \Phi_d(x),$$

el cual es un polinomio no constante en $\mathbb{Z}[x]$, en particular, es divisible por $\Phi_n(x)$. Claramente $\Phi_n(x) \mid x^n - 1$ también. Las divisibilidades descienden a $\mathbb{Z}$ y se obtiene que $\Phi_n(q) \mid q^n - 1$ y a los sumandos, de modo que $\Phi_n(q) \mid q - 1$. Ahora bien, $\Phi_n(q) = \prod_\zeta (q - \zeta)$ donde $\zeta \in \mathbb{C}$ recorre todas las raíces n-ésimas primitivas de la unidad, pero por desigualdad triangular $q \leq |q - \zeta| + 1$ donde la igualdad sólo se alcanza para la raíz de la unidad $\zeta = 1$ la que no está en Φ_n cuando $n > 1$, por lo que $|q - 1| < \prod_\zeta |q - \zeta| = |\Phi_n(\zeta)|$ lo cual es absurdo. □

10.4 Dependencia íntegra

En ésta sección 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 10.60: 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 $\boldsymbol{m}_1, \ldots, \boldsymbol{m}_n$. 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 10.61: 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 2.81 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 10.62: 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 10.63: 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 10.64: 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 10.65: Sean $C/B/A$ extensiones de anillos. Entonces C/A es una extensión entera syss C/B y B/A son extensiones enteras.

Proposición 10.66: 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 10.67: 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 $C = A[\alpha_1, \ldots, \alpha_n] = \text{Span}_B\{\beta_1, \ldots, \beta_m\}$, 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 $C = \text{Span}_{B_0}\{\beta_1, \ldots, \beta_m\}$, 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 10.68 (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 10.69: 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 10.70: 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 $A[\alpha] = \operatorname{Span}_A S$ y $A[\alpha, \beta] = \operatorname{Span}_{A[\alpha]} T$. Sea

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

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

Definición 10.71: 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 $\operatorname{Frac}(A)$.

Proposición 10.72: 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 10.73: 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 10.74: 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 10.75: Sea A un dominio íntegramente cerrado con $k := \operatorname{Frac} A$, 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 10.76: 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 10.77: 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 10.78: Sea A un dominio íntegramente cerrado, entonces $A[x]$ es íntegramente cerrado.

Demostración: Sea $k := \operatorname{Frac} A$. Si $f(x) \in k(x) = \operatorname{Frac}(A[x])$ 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 10.79: 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 10.80: 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 10.81: 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 $\mathfrak{n} \lhd B_{\mathfrak{p}}$ 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 10.82: Sea A un dominio y $\mathfrak{a} \lhd A$ 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 $\mathfrak{p}_i \lhd A$ es un ideal primo.

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

Teorema 10.83 (del ascenso): 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:

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

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

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

Proposición 10.84: 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 10.85: 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 10.86: 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 10.87 (del descenso): Sea B/A una extensión entera de anillos, y sean

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

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

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

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 6.40 se reduce a ver que $\mathfrak{p}_2^{ec} = B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A \subseteq \mathfrak{p}_2$.

Sea $x \in B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$, entonces es de la forma y/s con $y \in B\mathfrak{p}_2$ y $s \in B \setminus \mathfrak{q}_1$. Nótese que $y \in B\mathfrak{p}_2 \subseteq \operatorname{Rad}(B\mathfrak{p}_2)$ 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. □

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

Teorema 10.88: 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 10.89: 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 10.90: 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 $L = \operatorname{Frac}(B)$, 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. □

§10.4.1 Anillos de Jacobson.

Definición 10.91: Se dice que un anillo A es ***de Jacobson***[2] si todo ideal primo es una intersección de ideales maximales.

Proposición 10.92: 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.

[2]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: $1 \implies 2$. 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 10.93 (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 $A/\mathfrak{m}$.

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

$$d_0b^m + \cdots + d_m = 0,$$

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_mb^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 $A[1/(c_nd_m)]$. Finalmente concluimos por la proposición 10.74 que $A[(c_nd_m)^{-1}]$ es cuerpo y luego A también. Empleando nuevamente 10.74 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 10.94: Sea A un dominio. Son equivalentes:

1. A es de Jacobson.

2. Para todo $\mathfrak{a} \lhd A$ se cumple que $\mathrm{Rad}\,\mathfrak{a}$ es la intersección de los ideales maximales que le contienen.

3. Para todo $\mathfrak{a} \lhd A$ se cumple que $\mathfrak{N}(A/\mathfrak{a}) = \mathfrak{J}(A/\mathfrak{a})$.

Corolario 10.95: Un anillo noetheriano local es de Jacobson syss es artiniano.

§10.4.2 Teoremas de normalización.

Lema 10.96: 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 10.97: 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 10.89 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 10.98 – *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:

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

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 10.99: 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 10.74) 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 10.96 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 $K[\boldsymbol{y}]/y_1 K[\boldsymbol{y}] \cong K[y_2, \ldots, y_n]$ 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.

Corolario 10.100: 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. Toda cadena maximal

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

de ideales primos tiene longitud $r = \operatorname{alt} \mathfrak{p}$.

§10.4.3 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 10.101: 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. [**58,** 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

$$\begin{aligned}(p-1)!N_p e^x &= \sum_{j=p-1}^{r} j! b_j e^x \\ &= p! g_p(x) + \sum_{j=b-1}^{r} \left(\frac{j!}{(j-p+1)!} b_j x^{j-p+1} + \cdots + j b_j x^{j-1} \right) \\ &\quad + \sum_{j=p-1}^{r} b_j x^j \left(1 + \frac{x}{j+1} + \frac{x^2}{(j+1)(j+2)} + \cdots \right),\end{aligned}$$

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 10.102: 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

$$(v_1 u_1') \cdot (v_2 u_2') = v_1 v_2 (u_1 + u_2)'.$$

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

$$v_0 + v_1 T'(u_1) + \cdots + v_n T'(u_n) = 0, \tag{10.13}$$

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 (10.13), 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

$$\begin{aligned}\left| N_p C^p v_0 + C^p \sum_{i=1}^{n} v_i \sum_{\eta \in G} p g_p(\eta(u_i)) \right| &= \Bigg| (N_p C^p v_0 - N_p C^p v_0) \\ &\quad + C^p \sum_{i=1}^{n} v_i \sum_{\eta \in G} \left(p g_p(\eta(u_i)) - N_p e^{\eta(u_i)} \right) \Bigg| \\ &< \frac{2 M^p C^p m}{(p-1)!} \sum_{i=1}^{n} |v_i|.\end{aligned}$$

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

$$\left| N_p C^p v_0 + C^p \sum_{i=1}^{n} v_i \sum_{\eta \in G} p g_p(\eta(u_i)) \right| < \frac{2(MC)^p m L}{(p-1)!},$$

donde los términos a la izquierda son enteros y eligiendo que $p > |N_p v_0|$ vemos que han de ser no nulos; pero eso es absurdo pues el término de la derecha converge a 0. □

Teorema 10.103 – *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 $\sum_{i=1}^{n} k_i u_i$ y $\sum_{i=1}^{n} l_i u_i$ son números algebraicos distintos, y luego por el teorema anterior se cumple que $(e^{u_1})^{k_1} \cdots (e^{u_n})^{k_n} = e^{\sum_{i=1}^{n} k_i u_i}$ y $e^{\sum_{i=1}^{n} l_i u_i}$ 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 10.104: e y π son números trascendentes.

Parte III.

Geometría Algebraica

11

Teoría de valuación

11.1 Valores absolutos y cuerpos métricos

Definición 11.1: Sea k un cuerpo, una función $|\,|\colon k \to \mathbb{R}$ se dice una aplicación ***valor absoluto*** si:

VA1. $|x| > 0$ para todo $x \neq 0$ y $|0| = 0$.

VA2. $|xy| = |x|\,|y|$.

VA3. $|x + y| \leq |x| + |y|$ (desigualdad triangular).

Si además, satisface que $|x+y| \leq \max\{|x|, |y|\}$, llamada la ***desigualdad ultramétrica***, entonces $|\,|$ se dice un ***valor absoluto no-arquimediano*** y, de lo contrario se dice ***arquimediano***.

Todo valor absoluto induce una métrica $d(x, y) := |x - y|$ sobre k, y por ende, una topología. Por ello, se dice que el par $(k, |\,|)$ es un ***cuerpo métrico*** si $|\,|$ es un valor absoluto sobre k, se le añade elsufijo «arquimediano» o «no-arquimediano» según si el valor absoluto lo es. De no haber ambigüedad sobre los signos obviaremos el valor absoluto. Se dice que dos valores absolutos son ***equivalentes*** si inducen la misma topología sobre k.

Ejemplo. • Sea k un cuerpo arbitrario. Entonces $|\,|\colon k \to \mathbb{R}$ dado por

$$|x| = \chi_{k^\times}(x) = \begin{cases} 0, & x = 0 \\ 1, & x \neq 0 \end{cases}$$

es un valor absoluto no-aquimediano, llamado el valor absoluto ***trivial***. Nótese que el valor absoluto induce la topología discreta. *Ojo*, la expresión «cuerpo métrico discreto» la emplearemos con otros fines.

- Los valores absoluto estándar sobre $\mathbb{R}$ y $\mathbb{C}$ son, efectivamente, funciones «valor absoluto» e inducen las topologías usuales resp.; les denotaremos $|\,|_\infty$ para diferenciarles de otros valores absoluto.

Corolario 11.2: Sea k un cuerpo métrico. Entonces:

1. $|1| = 1$.
2. $|a^n| = |a|^n$ para todo $n \in \mathbb{Z}$.
3. $|-1| = 1$, por ende, $|-a| = |a|$.
4. Para todo $n \in \mathbb{N}$ se cumple que $|n| \leq n$.
5. Si k es finito, entonces $|\,|$ es trivial.

Será necesario comprobar lo siguiente:

Teorema 11.3: Sea k un cuerpo métrico. Las funciones:

$$+\colon k \times k \to k, \quad \cdot\colon k \times k \to k, \quad ()^{-1}\colon k^\times \to k^\times$$

son continuas. Equivalentemente, k es un cuerpo topológico. Además, como es un espacio métrico, la función $|\,|\colon k \to \mathbb{R}$ es continua.

Demostración: En el enunciado y la demostración $k \times k$ denota el producto como espacios topológicos. Es sabida que dicha topología es la misma que aquella inducida por la métrica L^2 (y cualquier métrica L^p con $p \in [1, \infty]$). En particular fijaremos la métrica L^∞, en donde:

$$d\big((a_1, b_1), (a_2, b_2)\big) = \text{máx}\{|a_1 - a_2|, |b_1 - b_2|\} < \delta$$

Sean $a, b \in k$, demostrar que $+$ es continua equivale a ver que para todo $\epsilon > 0$ existe $\delta > 0$ tal que

$$d\big((a_1, b_1), (a_2, b_2)\big) < \delta \implies |(a_1 + b_1) - (a_2 + b_2)| < \epsilon.$$

Así pues, basta elegir $\delta = \epsilon/2$.

Para el producto, sea $(a_1, b_1) \in k$ un punto arbitrario y sea $M := \text{máx}\{|a_1|, |b_1|, 1\} > 0$. Luego elegimos $\delta := \text{mín}\{\frac{\epsilon}{2M+1}, 1\}$, y vemos que

$$\begin{aligned} |a_1b_1 - a_2b_2| &= |a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2| \leq |a_1 - a_2|\,|b_1| + |a_2|\,|b_1 - b_2| \\ &< \delta(|b_1| + |a_2|) \leq \delta(|b_1| + |a_2| + \delta) \\ &< \frac{\epsilon}{2M+1}(M + M + 1) = \epsilon. \end{aligned}$$

Finalmente, para la inversa, sea $a \in k^\times$, luego $|a| > 0$. Elegimos $\delta := \text{mín}\{\frac{|a|^2}{2}\epsilon, \frac{|a|}{2}\} > 0$ y notamos que si $|a-b| < \delta$, entonces $|b| > |a| - \delta \geq |a|/2$ y

$$\left|\frac{1}{a} - \frac{1}{b}\right| = \frac{|a-b|}{|a|\,|b|} < \frac{\delta}{|a|\,|a|/2} \leq \epsilon. \qquad \square$$

Proposición 11.4: Sean $|\,|_1$, $|\,|_2$ dos valores absolutos no triviales sobre k. Entonces las siguientes afirmaciones son equivalentes:

1. $|\,|_1$ y $|\,|_2$ son valores absolutos equivalentes.
2. $|x|_1 < 1$ implica $|x|_2 < 1$ para todo $x \in k$.
3. Existe un $\lambda > 0$ real tal que $|x|_1 = |x|_2^\lambda$ para todo $x \in k$.

Demostración: 1 $\implies$ 2. Si $|x|_1 < 1$, entonces $\lim_n |x|_1^n = 0$, por lo que $\lim_n x = 0$. Como las topologías son la misma, la convergencia se da para ambos valores absolutos, luego $\lim_n |x|_2^n = 0$, por lo que $|x|_2 < 1$.

2 $\implies$ 3. Nótese que si $|x|_1 < 1$ implica $|x|_2 < 1$, luego si $|x|_1 > 1$ elijamos x^{-1} luego $|x^{-1}|_1 < 1$ implica $|x^{-1}|_2 < 1$. Como $|\,|_1$ y $|\,|_2$ son no triviales, elijamos x_0 tal que $a := |x_0|_1 > 1$ y $b := |x_0|_2 > 1$. Sea

$$\lambda := \frac{\ln b}{\ln a} > 0,$$

y claramente se satisface que $|x_0|_1 = |x_0|_2^\lambda$. Sea $x \in k^\times$, entonces sea $\alpha > 0$ tal que $|x|_1 = |x_0|_1^\alpha$. Luego sean m, n enteros tales que $m/n > \alpha$, luego

$$|x|_1 < |x_0|_1^{m/n} \iff |x^n/x_0^m|_1 < 1 \iff |x^n/x_0^m|_2 < 1 \iff |x|_2 < |x_0|_2^{m/n}$$

como ello aplica para todo racional, entonces $|x|_2 \leq |x_0|_2^\alpha$. De manera análoga se comprueba que $|x|_2 \geq |x_0|_2^\alpha$. Finalmente se estable que $|x|_1 = |x_0|_1^\alpha = |x_0|_2^{\lambda\alpha} = |x|_2^\lambda$.

3 $\implies$ 1. Trivial. $\square$

Proposición 11.5: Un cuerpo métrico k es no-arquimediano syss para todo $n \in \mathbb{Z}$ se cumple que $|n| \leq 1$.

Demostración: $\Longrightarrow$. Basta notar que

$$|n| = |\underbrace{1+1+\cdots+1}_{n}| \leq \text{máx}\{|1|, \ldots, |1|\} = 1$$

para $n \geq 0$, y emplear que $|-n| = |n|$ para $n < 0$.

$\Longleftarrow$. Sean $a, b \in k$ arbitrarios, entonces

$$\begin{aligned}|(a+b)^n| &= |a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n| \\ &\leq |a|^n + |a|^{n-1}|b| + \cdots + |b|^n \leq (n+1)\,\text{máx}\{|a|^n, |b|^n\}.\end{aligned}$$

Luego aplicando raíces (reales) a los valores absolutos se obtiene que $|a+b| \leq \sqrt[n]{n+1}\,\text{máx}\{|a|, |b|\}$ para todo $n \in \mathbb{N}_{\neq 0}$, pero $\lim_n \sqrt[n]{n+1} = 1$, lo que comprueba que $|a+b| \leq \text{máx}\{|a|, |b|\}$. □

Corolario 11.6: Todo cuerpo métrico de característica no nula es no-arquimediano.

Corolario 11.7: Si un valor absoluto $|\,|$ sobre k es no-arquimediano sobre algún subcuerpo (e.g., es trivial), entonces es no-arquimediano en todo k.

Ejemplo 9: Sea $p \in \mathbb{Z}$ primo. Se define $\nu_p(a)$, la ***valuación p-ádica*** de $a \in \mathbb{Z}$, como el máximo $n \in \mathbb{N}$ tal que $p^n \mid a$; se extiende a que $\nu_p(0) := \infty$. Ésto lo podemos extender a $\mathbb{Q}$ definiendo que $\nu_p(a/b) := \nu_p(a) - \nu_p(b)$ (¿por qué está bien definido?). Finalmente, eligiendo un real $\lambda \in (0,1)$ podemos definir:

$$\left|\frac{a}{b}\right|_p := \lambda^{\nu_p(a/b)},$$

y verificamos que efectivamente sea un valor absoluto no-arquimediano.

La condición VA1 es clara. Además, para enteros se verifica que $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ de lo que se concluye VA2. Nótese lo siguiente, $n = \nu_p(a/b)$ syss $\frac{a}{b} = p^n \frac{u}{v}$ donde $p \nmid uv$, de éste modo si $n := \nu_p(a/b) \leq \nu_p(c/d) =: m$

$$\frac{a}{b} + \frac{c}{d} = p^n \frac{u}{v} + p^m \frac{w}{z} = p^n \frac{uz + p^{m-n}wv}{vz},$$

donde claramente $p \nmid uz + p^{m-n}wv$ y $p \nmid vz$. Con ésto se comprueba que $\nu_p(a/b + u/v) = \text{mín}\{\nu_p(a/b), \nu_p(c/d)\}$, ésto se traduce en la desigualdad ultramétrica.

La observación de cierre es que la elección de λ para el valor absoluto no afecta en nada, en el sentido de que otorga valores absolutos equivalentes. Por ello, el estándar es escoger $\lambda = 1/p$ de modo que $|a/b|_p = p^{-\nu_p(a/b)}$.

Con éste ejemplo se puede probar:

Proposición 11.8: Para todo $x \in \mathbb{Q}^\times$ se satisface que

$$|x|_\infty \cdot |x|_2 \cdot |x|_3 \cdots = |x|_\infty \cdot \prod_p |x|_p = 1,$$

donde p recorre todos los primos de $\mathbb{Z}$. (Nótese que el producto converge pues $|x|_p = 1$ para todos salvo finitos p's.)

Definición 11.9: 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 $b/a \in \mathbb{Z}_{(p)}$.

El último ejemplo es parte de algo más general:

Proposición 11.10: Sea k un cuerpo métrico no-arquimediano. Definamos:

$$\mathfrak{o} := \{a \in k : |a| \leq 1\}, \qquad \mathfrak{m} := \{a \in k : |a| < 1\},$$

entonces $(\mathfrak{o}, \mathfrak{m})$ es un anillo local de valuación, y su cuerpo de residuos $\mathfrak{o}/\mathfrak{m}$ se le dice el ***cuerpo de restos (de clases)*** de k.

Demostración: El que $\mathfrak{o}$ sea un dominio íntegro deriva de que $1 \in \mathfrak{o}$, no posee divisores de cero por estar contenido en k, es cerrado bajo multiplicación por VA2 y es cerrado bajo adición por la desigualdad ultramétrica.

El hecho de que $\mathfrak{m}$ sea su ideal maximal se deriva de que, las razones anteriores demuestran que $\mathfrak{m}$ es ideal de $\mathfrak{o}$ y si $a \in \mathfrak{m}$, entonces $a^{-1} \in k$ tiene valor absoluto $|a|^{-1} > 1$, luego $a^{-1} \notin \mathfrak{o}$. □

Teorema 11.11 – *Teorema de Ostrowski*: Todo valor absoluto no-trivial sobre $\mathbb{Q}$ es (salvo equivalencia):

1. $|\,|_\infty$ si $|\,|$ es arquimediano.
2. Un valor p-ádico $|\,|_p$ si es no-arquimediano.

Demostración:

1. Sea $n > 1$ entero. Entonces nótese que todo m posee una única expansión en base n:

$$m = m_t n^t + \cdots + m_1 n + m_0, \qquad 0 \leq m_i \leq n-1, m_t \neq 0$$

donde $n^t \leq m < n^{t+1}$. Luego por desigualdad triangular, empleando que $|m_i| \leq n-1$, se concluye que $|m| \leq (t+1)(n-1)r^t$. Como $m^j < n^{j(t+1)}$, luego

$$|m|^j = |m^j| \leq j(t+1)(n-1)r^{jt} \implies r > \frac{\sqrt[t]{m}}{\sqrt[jt]{j(t+1)(n-1)}},$$

aplicando límites se concluye que $r \geq \sqrt[t]{|m|}$; como algún m tiene valor absoluto $|m| > 1$ (por ser arquimediano), entonces $r > 1$ y como $t = \lfloor \log_n(m) \rfloor = \log_n(m)$ se concluye que

$$|m| \leq r^t \leq r^{\log_n(m)}.$$

Cambiando m entero a x racional, vemos que la misma cota aplica, luego si $|x|_\infty < 1$, entonces $\log_n(x) < 0$ y $|x| < 1$ lo que prueba que los valores absolutos son equivalentes.

2. Supongamos que $|\,|$ es un valor absoluto no trivial sobre $\mathbb{Q}$. Por la proposición anterior, sea $(\mathfrak{o}, \mathfrak{m})$ el anillo de valuación asociado a $|\,|$. Nótese que, como $|n| \leq 1$ para todo $n \in \mathbb{Z}$, concluimos que $\mathbb{Z} \subseteq \mathfrak{o}$. Luego $\mathbb{Z} \cap \mathfrak{m}$ es un ideal primo de $\mathbb{Z}$, digamos (p); luego $A \supseteq \mathbb{Z}_{(p)}$. Como $|\,|$ es no trivial, entonces $\mathfrak{o} \neq \mathbb{Q}$ y $\mathbb{Z}_{(p)} \neq \mathbb{Q}$ por lo que $p \neq 0$. Si $a \in \mathbb{Z}$ es tal que $p \nmid a$, entonces $a \notin \mathfrak{m}$ y necesariamente $|a| = 1$. Luego si $p \nmid ab$, entonces $|p^n \frac{a}{b}| = |p|^n$ y de ahí se concluye que $|\,|$ es equivalente a $|\,|_p$. □

Si k es un cuerpo métrico, entonces podemos importar las siguientes definiciones de la topología/análisis:

Definición 11.12: Sea k un cuerpo métrico. Sea $(a_n)_{n\in\mathbb{N}} \subseteq k$ una sucesión. Se dice que $(a_n)_n$ converge a un límite $L \in k$, denotado $\lim_n a_n = L$, si para todo

$$\forall \epsilon > 0 \exists N \in \mathbb{N} \forall n > N \quad |a_n - L| < \epsilon.$$

Se dice que $(a_n)_n$ es una ***sucesión fundamental*** si es una sucesión de Cauchy, i.e., si para todo $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que

$$\forall n, m > N \quad |a_n - a_m| < \epsilon.$$

Un cuerpo con valor absoluto se dice ***completo*** si toda sucesión fundamental es convergente.

Se dice que un cuerpo K con un valor absoluto $\| \ \|$ es una ***compleción*** de k si:

1. K es completo.
2. K/k es una extensión de cuerpos y $\|x\| = |x|$ para todo $x \in k$.
3. k es (topológicamente) denso en K, i.e., para todo $x \in K$ y todo $\epsilon > 0$ existe $y \in k$ tal que $\|x - y\| < \epsilon$.

Luego veremos otra definición categorial de *compleción* que nos servirá para fines del álgebra conmutativa, pero ésta definición es suficiente por el momento.

Teorema 11.13: Todo cuerpo métrico k posee una compleción. Más aún, sus compleciones son isométricamente isomorfas.[1]

Demostración: Como k es un espacio métrico, entonces posee una compleción K (como espacio) y podemos definir $\|\alpha\| := d(\alpha, 0)$ para $\alpha \in K$, donde d es la métrica en K que extiende a la métrica de k.

Los elementos de K son límites de sucesiones fundamentales en k, así pues definimos $\alpha := \lim_n a_n$ y $\beta := \lim_n b_n$. Luego $\alpha + \beta := \lim_n (a_n + b_n)$, $\alpha \cdot \beta := \lim_n (a_n \cdot b_n)$ y si $\alpha \neq 0$ y $(a_n)_n$ no se anula, entonces se comprueba que $\alpha^{-1} = \lim_n a_n^{-1}$ (esta última es una igualdad, no una definición). Todo

[1] Es decir, existe un isomorfismo de cuerpos que además preserva distancias o, en este caso, que respeta el valor absoluto; en particular, es también un homeomorfismo.

ésto se puede comprobar a partir de que la suma, el producto y la inversa es continua en un cuerpo topológico y, en particular, lo es en un cuerpo métrico.

Finalmente, si $(K_1, |\,|_1)$ y $(K_2, |\,|_2)$ son compleciones de k, con los encajes de cuerpos topológicos $f\colon k \to K_1$ y $g\colon k \to K_2$ (que son encajes topológicos y monomorfismos de cuerpos), entonces todos los elementos de K_1 son de la forma $\lim_n f(a_n)$ para alguna sucesión fundamental $(a_n)_n \in k$. Luego definimos:

$$\begin{aligned} \varphi\colon K_1 &\longrightarrow K_2 \\ \lim_n f(a_n) &\longmapsto \lim_n g(a_n), \end{aligned}$$

el cual está bien definido y es un homeomorfismo.[2] Para ver que además es un homomorfismo de cuerpos, basta recordar que f y g lo son, y que la suma, producto e inverso son continuas. □

Corolario 11.14: Sea $\varphi\colon k \to L$ un encaje de cuerpos topológicos, donde k es métrico y L es métrico completo. Entonces, $\overline{\varphi[k]}$ (la clausura topológica) es una compleción de k.

Corolario 11.15: $\mathbb{R}$ sólo posee un valor absoluto arquimediano salvo equivalencia, $|\,|_\infty$.

Demostración: Basta notar que $\mathbb{R}$ es la compleción de $(\mathbb{Q}, |\,|_\infty)$ y de que todo valor absoluto en $\mathbb{R}$ se restringe a $\mathbb{Q}$. □

Lema 11.16: Sean $|\,|_1, \ldots, |\,|_n$ valores absoluto sobre k tales que ningún par es equivalente. Existe $a \in k$ tal que

$$|a|_1 > 1, \quad \forall i \neq 1\ |a|_i < 1.$$

Demostración: Lo probaremos por inducción sobre n. El caso base $n = 2$ esta dado puesto que, por la proposición 11.4, podemos encontrar $b, c \in k$ tales que

$$|b|_1 < 1,\ |b|_2 \geq 1, \quad |c|_1 \geq 1,\ |c|_2 < 1.$$

Luego elegimos $a = bc^{-1}$ y notamos que $|a|_1 < 1$ y $|a|_2 > 1$ como se quería.

Para el caso $n + 1$, por hipótesis inductiva y por lo anterior podemos encontrar $b, c \in k$ tales que

$$|b|_1 > 1, \quad |b|_2 < 1,\ \cdots,\ |b|_n < 1$$

[2] De hecho, ésta misma función es la que se emplea para probar que la compleción de un espacio métrico es única salvo homeomorfismo.

$$|c|_1 > 1, \qquad |c|_{n+1} < 1.$$

(a) Si $|b|_{n+1} \leq 1$: Entonces elegimos $a := b^r c$ donde $r \in \mathbb{N}$ no está fijo. Nótese que $|a|_1 > 1$ y $|a|_i = |b|_i^r |c|$ para $1 < i \leq n$, luego como $|b|_i^r \to 0$ podemos elegir r suficientemente grande de modo que $|a|_i < 1$ para $1 < i \leq n$ y es claro que $|a|_{n+1} < 1$.

(b) Si $|b|_{n+1} > 1$: Entonces elegimos

$$a := \frac{b^r}{1+b^r} c,$$

con $r \in \mathbb{N}$ sin fijar. Como $|b|_i^r \to 0$, entonces se comprueba que $|a|_i < 1$ para todo $1 < i \leq n$ si r es suficientemente grande. Para $j = 1$ o $j = n+1$, nótese que $|b|_j > 1$ luego nótese que

$$|b|_j^r - 1 \leq |1 + b^r|_j \leq 1 + |b|_j^r$$

por desigualdad triangular, luego

$$1 = \lim_r \frac{|b|_j^r}{|b|_j^r - 1} \geq \lim_r \frac{|b|_j^r}{|1+b^r|_j} \geq \lim_r \frac{|b|_j^r}{|b|_j^r + 1} = 1,$$

con lo cual, por teorema del sandwich, el límite de al medio converge a 1, luego para un r suficientemente grande se cumple que $|a|_j$ está «cerca» de $|c|_j$ y luego $|a|_1 > 1$ y $|a|_n < 1$ como se quería probar. □

Teorema 11.17 (de aproximación): Sean $|\,|_1, \ldots, |\,|_n$ valores absoluto sobre k tales que ningún par es equivalente. Sean $a_1, \ldots, a_n \in k$ y sea $\epsilon > 0$, entonces existe $a \in k$ tal que

$$\forall 1 \leq i \leq n \quad |a - a_i|_i < \epsilon.$$

Demostración: Empleando el lema, podemos obtener $b_i \in k$ tal que $|b_i|_i > 1$ y $|b_i|_j < 1$ para $j \neq i$. Luego nótese que

$$\lim_r \left| \frac{b_i^r}{1+b_i^r} \right|_i = 1, \qquad \lim_r \left| \frac{b_i^r}{1+b_i^r} \right|_j = 0, \ j \neq i.$$

Luego $a_i b_i^r/(1+b_i^r)$ tendrá valor absoluto en $|\,|_i$ cercano a $|a_i|_i$ y valor absoluto en $|\,|_j$ cercano a 0. Definimos

$$a := \sum_{i=1}^n \frac{a_i b_i^r}{1+b_i^r},$$

el cual, con r suficientemente grande, satisface las hipótesis requeridas. □

Nótese que hay un paralelo entre el teorema chino del resto y el teorema de aproximación: En efecto, podemos considerar a los valores absolutos como los p-ádicos y los a_i's como residuos mód p_i, luego el $a \in \mathbb{Q}$ dado satisface que $|a - a_i|_i < p^{-n_i}$, o equivalentemente, satisface que $\nu_{p_i}(a - a_i) \geq n_i$

§11.1.1 Teorema de Ostrowski II. El teorema de Ostrowski I nos clasifica los valores absolutos sobre $\mathbb{Q}$, pero hay una segunda versión, también atribuida a Ostrowski **[0,** Teo. 1.1, pág. 33**]** que nos clasifica, más generalmente, los valores absolutos arquimedianos. En cierta manera, éste teorema nos dará otro indicio de unicidad para $\mathbb{R}$.

Lema 11.18: El único valor absoluto arquimediano $|\,|$ sobre $\mathbb{C}$ es (salvo equivalencia) $|\,|_\infty$.

Demostración: Sea $\zeta = a + b\mathrm{i}$ con $a, b \in \mathbb{R}$. Como $\mathrm{i}^4 = 1$, entonces $|\mathrm{i}| = 1$. Además, sabemos que $|\,|$ en $\mathbb{R}$ es equivalente a $|\,|_\infty$, luego $|a| = |a|_\infty^\lambda$ para algún $\lambda > 0$ real. Luego:

$$|\zeta| = |a + b\mathrm{i}| \leq |a| + |b| = |a|_\infty^\lambda + |b|_\infty^\lambda \leq 2|\zeta|_\infty^\lambda.$$

Luego elijamos α, β y por el teorema de aproximación existe γ tal que $|\alpha - \gamma|, |\beta - \gamma|_\infty < \epsilon$, pero nótese que

$$|\alpha - \gamma|_\infty \geq \left(\frac{|\alpha - \gamma|}{2}\right)^{1/\lambda} \geq \left(\frac{|\alpha - \beta| - \epsilon}{2}\right)^{1/\lambda},$$

lo cual, eligiendo $|\alpha - \beta|$ y ϵ apropiadamente, conlleva a una contradicción. □

Lema 11.19: Sea k un cuerpo métrico completo. Supongamos que $t^2 + 1$ es irreducible en $k[t]$, entonces existe $\Delta > 0$ real tal que

$$\forall a, b \in k \quad |a^2 + b^2| \geq \Delta \,\mathrm{máx}\{|a|^2, |b|^2\}.$$

Demostración: Definamos

$$\Delta := \frac{|4|}{1 + |4|}.$$

Probaremos la contrarrecíproca: supongamos que existe $c_1 \in k$ tal que

$$\delta_1 := |c_1^2 + 1| < \Delta < 1,$$

entonces construiremos una sucesión fundamental que converja a una solución del polinomio. Para ello definamos $c_2 := c_1 + h_1$, luego

$$c_2^2 + 1 = c_1^2 + 1 + 2c_1h_1 + h_1^2,$$

por lo que elegimos

$$h_1 := -\frac{(c_1^2+1)}{2c_1},$$

con lo que se comprueba que

$$\delta_2 := |c_2^2 + 1| = |h_1|^2 = \frac{|c_1^2+1|^2}{|4|\,|c_1|^2} \leq \delta_1\theta,$$

donde

$$\theta := \frac{\delta_1}{|4|(1-\delta_1)} < 1,$$

donde empleamos que $|c_1| \geq 1 - \delta_1 > 0$ por desigualdad triangular; nótese que $\delta_2 < \delta_1$. Definiendo por recursión c_n y h_n del mismo modo, vemos que, por inducción sobre n se cumple

$$\delta_{n+1} = |c_{n+1}^2 + 1| = |h_n|^2 \leq \delta_n\theta \leq \delta_1\theta^n.$$

Finalmente, basta notar que $(c_n)_n$ es una sucesión fundamental:

$$|c_{n+1} - c_n|^2 = |h_n|^2 \leq \delta_1\theta^n.$$

Y así, $c^* := \lim_n c_n$ existe y satisface que $|c^{*2} + 1| = \lim_n |c_n^2 + 1| = 0$. □

Lema 11.20: Sea k un cuerpo métrico completo. Supongamos que t^2+1 es irreducible en $k[t]$, entonces $|\,|$ posee una extensión a un valor absoluto en $k(\sqrt{-1})$.

Demostración: Sea $\mathrm{i} := \sqrt{-1}$ y definamos en $k(\mathrm{i})$:

$$\|a + \mathrm{i}b\| := \sqrt{|a^2 + b^2|}.$$

Es fácil notar que $\|\ \|$ extiende a k. Y es fácil también comprobar que satisface VA1 y VA2. Vamos a comprobar la desigualdad triangular: sean $\alpha, \beta \in k(\mathrm{i})$, la desigualdad es trivial si alguno fuese nulo, así que en caso contrario, elijamos $0 \neq \|\alpha\| \geq \|\beta\|$, entonces vemos que

$$\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\| \iff \left\|1 + \frac{\beta}{\alpha}\right\| \leq 1 + \left\|\frac{\beta}{\alpha}\right\|,$$

donde $\gamma := \beta/\alpha$ satisface que $\|\gamma\| \leq 1$. Así, supongamos que $\|a + \mathrm{i}b\|^2 \leq 1$, entonces, por el lema anterior, se cumple que $|a|, |b| \leq \Delta^{-1/2}$. Luego vemos que

$$\begin{aligned}\|1 + (a + \mathrm{i}b)\|^2 = |(1 + a)^2 + b^2| &\leq 1 + |2|\,|a| + |a|^2 + |b|^2 \\ &\leq 1 + |2|\Delta^{-1/2} + 2\Delta^{-1} =: C^2.\end{aligned}$$

Revisar conclusión, **[0,** pág. 37].

Con lo que se cumple lo pedido. □

Teorema 11.21 – *Teorema de Ostrowski*: Sea k un cuerpo métrico arquimediano. Entonces existe un monomorfismo de cuerpos $f\colon k \to \mathbb{C}$ y una constante real $\lambda > 0$ tales que $|x| = |f(x)|^\lambda$. Más aún, si k es completo (como espacio métrico), entonces k es isomorfo a $\mathbb{R}$ o a $\mathbb{C}$.

Demostración: En particular, probaremos lo siguiente:

> Si k es un cuerpo métrico arquimediano completo e $\mathrm{i} = \sqrt{-1} \in k$, entonces k es isométricamente isomorfo a $\mathbb{C}$.

Como k es arquimediano, entonces $\operatorname{car} k = 0$ y contiene a $\mathbb{Q}$. Como es completo, entonces contiene a $\mathbb{R}$ y como contiene a i, entonces contiene a $\mathbb{C}$. Es claro que la restricción de $|\,|$ en $\mathbb{C}$ es equivalente al valor absoluto usual $|\,|_\infty$.

Sea $\alpha \in k$ arbitrario. Luego $z \mapsto |\alpha - z|$ es una función continua de dominio $\mathbb{C}$ y codominio $\mathbb{R}$ que, veremos, alcanza un mínimo. Nótese que $|\alpha - z| \geq |z|_\infty^\lambda - |\alpha|$, de modo que para un radio $R > 0$ suficientemente grande se cumple que si $|z| > R$ entonces $|\alpha - z| \geq |\alpha|$, luego, por compacidad de la bola de radio R, el mínimo se alcanza en su interior, digamos en el complejo $b \in \mathbb{C}$ y definimos $\beta := \alpha - b$. Si $\alpha \notin \mathbb{C}$, entonces $\beta \neq 0$ y $|\beta| > 0$. Nótese que

$$0 < |\beta| = \inf_{z \in \mathbb{C}} |\alpha - z|.$$

Sea $c \in \mathbb{C}$ tal que $0 < |c| < |\beta|$. Por la propiedad superior se cumple que $|\beta - c| \geq |\beta|$. Notemos que

$$\frac{\beta^n - c^n}{\beta - c} = \prod_{\substack{\zeta^n = 1 \\ \zeta \neq 1}} (\beta - \zeta c),$$

como $\mathbb{C}$ contiene a todas las raíces de la unidad, entonces $\zeta c \in \mathbb{C}$ y $|\beta - \zeta c| \geq |\beta|$. Aplicando $|\,|$ a ambos lados se obtiene que:

$$\frac{|\beta - c|}{|\beta|} \leq \frac{|\beta^n - c^n|}{|\beta|^n} = |1 - (c/\beta)^n| = 1 + |c/\beta|^n,$$

el cual converge a 1 para n suficientemente grande. Luego $|\beta - c| \leq |\beta|$ y por antisimetría de $\leq$ se concluye igualdad, es decir, en el complejo $b - c$ también se alcanza el mínimo.

Sustituyendo β por $\beta - c$ y repitiendo el proceso notamos que el mínimo siempre se alcanza en $b - nc$ para todo $n \in \mathbb{N}$, pero

$$|n|\,|c| \leq |\beta| + |\beta - nc| = 2|\beta|.$$

Luego, como $|n| > 1$ para algún n y claramente también para sus potencias, se concluye que $|c| = 0$ lo cual es absurdo por elección de $|c|$. En conclusión, necesariamente $\alpha \in \mathbb{C}$. □

11.2 Valuaciones

Ya en la sección anterior vimos la definición de anillo de valuación, pero ahora queremos sacarle más provecho.

Proposición 11.22: 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.[3]

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]Un dominio que satisface ésto se le dice un *anillo de Bézout* en literatura especializada.

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 11.23: 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 $0 \geq -a$.

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 11.24: 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 *va-*

luaciones a los valores absoluto. lang:algebra emplea «valor absoluto / valuación», mientras que jacobson:basic emplea «valuación / valuación exponencial» y nagata:fields 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 11.25: Sea A un dominio íntegro.

1. Si 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 11.26: 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 $b/a \in A$. $\square$

Corolario 11.27: Sea A un anillo de valuación y sea $\mathfrak{p} \lhd A$ primo, entonces $\mathfrak{p} = \mathfrak{p} \cdot A_{\mathfrak{p}}$, y el cociente $A/\mathfrak{p}$ es de valuación.

Demostración: Claramente $\mathfrak{p} \subseteq \mathfrak{p} \cdot A_{\mathfrak{p}}$. Sea $a \in \mathfrak{p} \cdot A_{\mathfrak{p}}$, entonces $a \notin A_{\mathfrak{p}}^{\times}$ y $a^{-1} \notin A$, luego $a \in A$ y $\mathfrak{p} \cdot A_{\mathfrak{p}} \cap A = \mathfrak{p}$.

Para notar que el cociente es de valuación, basta notar que los ideales principales también están linealmente ordenados por inclusión. □

Teorema 11.28: Sea K un cuerpo, $(A, \mathfrak{m})$ un anillo de valuación de K y A^* un anillo de valuación de $A/\mathfrak{m}$. Definamos

$$B := \{a \in A : [a]_{\mathfrak{m}} \in A^*\},$$

entonces B es de valuación en K.

Demostración: Sea $a \in K$ tal que $a \notin S$. Si $a \notin A$, entonces $a^{-1} \in \mathfrak{m} \subseteq B$. Si $a \in A$, entonces $a \mod \mathfrak{m} \notin A^*$ y $a^{-1} \mod \mathfrak{m} \in A^*$ (por ser de valuación), con lo que $a^{-1} \in B$. □

Definición 11.29: Sea k un cuerpo, $v\colon k \to G \cup \{\infty\}$ una G-valuación y $\mathfrak{o} := \{x \in k : v(x) \geq 0\}$. Le decimos el ***rango*** de la valuación v a $k.\dim(\mathfrak{o})$.

Vamos a necesitar el siguiente hecho que queda como ejercicio al lector: si A es un dominio íntegro de $k.\dim A = 1$, entonces todo ideal maximal es principal.

Teorema 11.30: Sea k un cuerpo.

1. Si $|\,|$ es un valor absoluto no-arquimediano sobre k, entonces para todo $r \in (0,1)$ real se cumple que $v(a) := \log_r |a|$ es una $\mathbb{R}$-valuación de rango 1.

2. Recíprocamente, si v es una valuación de rango 1 sobre k con grupo de valuación G, entonces existe un monomorfismo creciente de grupos $\varphi\colon G \to \mathbb{R}$ tal que para todo $r \in (0,1)$ real se cumple que $|a| := r^{\phi(v(a))}$ es un valor absoluto no-arquimediano.

En ambos casos, el anillo de valuación del valor absoluto $|\,|$ y de la valuación v coinciden.

Demostración: La primera ya la probamos.

Para la segunda, nótese primero que $\mathfrak{m} = (\pi)$ por la observación anterior y así, para todo $a \in k$ existe un único $e = e(n,a) \in \mathbb{Z}$ tal que $a^n \notin \pi^e\mathfrak{o}$ y $a^n \in \pi^{e-1}\mathfrak{o}$, o equivalentemente, $(e-1)v(\pi) \leq nv(a) < ev(\pi)$. Luego, para $m > n$ se cumple que

$$\left|\frac{e(n,a)}{n} - \frac{e(m,a)}{m}\right| \leq \frac{1}{n}$$

de modo que el límite $u(a) := \lim_n e(n,a)/n$ existe.

Definimos $\varphi\colon G \to \mathbb{R}$ dado por $\varphi(v(a)) := u(a)$ y hay que verificar que es un monomorfismo creciente de grupos. Sean $\alpha = v(a), \beta = v(b) \in G$, sabemos que $\alpha + \beta = v(ab)$. Por definición $a^n \notin \pi^{e(n,a)}\mathfrak{o}$, $a^n \in \pi^{e(n,a)-1}\mathfrak{o}$ y $b^n \notin \pi^{e(n,b)}\mathfrak{o}$, $b^n \in \pi^{e(n,b)-1}\mathfrak{o}$ de modo que podemos concluir que $e(n,a) + e(n,b) - e(n,ab)$ es 0 o 1. Luego en el límite se obtiene que $\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta)$ y se trata de un homomorfismo de grupos.

Supongamos que $\alpha = v(a) > 0$, entonces $a \in \mathfrak{m} = \pi\mathfrak{o}$ y $e(1,a) > 1$. Nótese que la sucesión $(e(n,a)-1)/n$ es creciente para $n = 2, 2^2, 2^3, \ldots$, de modo que

$$\lim_n \frac{e(n,a)}{n} = \lim_r \frac{e(2^r,a)-1}{2^r} \geq \frac{e(2,a)-1}{2} > 0$$

lo que comprueba que es creciente e inyectiva. □

§11.2.1 Dominios de valuación discreta.

Definición 11.31: Sea k un cuerpo métrico. Decimos que un valor absoluto es ***discreto***, cuando el grupo multiplicativo $\{|a| : a \in k^\times\} \subseteq \mathbb{R}^\times$ es discreto como subespacio (con la topología usual).

Como el grupo multiplicativo de un cuerpo métrico es claramente un grupo topológico, entonces basta notar que el neutro 1 está aislado, vale decir, que existe un $\delta > 0$ tal que

$$1 - \delta < |a| < 1 + \delta \implies |a| = 1.$$

Proposición 11.32: El valor absoluto de un cuerpo es discreto syss en su anillo de valuación $(\mathfrak{o}, \mathfrak{m})$ se cumple que $\mathfrak{m}$ es principal.

DEMOSTRACIÓN: $\Longleftarrow$. Si $\mathfrak{m} = (\pi)$ es principal, entonces

$$|a| < 1 \implies a \in \mathfrak{m} \implies \exists b \in \mathfrak{o} : a = \pi b \implies |a| \leq |\pi|.$$

Por otro lado, si $|a| > 1$, entonces $|a^{-1}| < 1$ y $|a| \geq |\pi|^{-1}$. Concluimos pues $|\pi| < 1$ (por estar en $\mathfrak{m}$).

$\Longrightarrow$. Si $||$ es discreto, entonces el conjunto

$$\{|a| : |a| < 1\}$$

alcanza su máximo, digamos en $\pi \in \mathfrak{m}$. Luego si $|a| < 1$, entonces $|\pi^{-1}a| \leq 1$ así que $b = \pi^{-1}a \in \mathfrak{o}$ y luego $a = b\pi$ con lo que comprobamos que $\mathfrak{m} = (\pi)$. □

Como $(\mathfrak{o}, \mathfrak{m})$ es un DIP, entonces $k.\dim A = 1$; así pues, podemos hablar equivalentemente de o valores absolutos discretos o valuaciones discretas.

Definición 11.33: Se dice que un anillo de valuación $(A, \mathfrak{m})$ es un ***dominio de valuación discreta*** si existe una valuación discreta v sobre $K := \operatorname{Frac} A$ tal que $A = \{a \in K : v(a) \geq 0\}$.

En una valuación discreta v se cumple que $v(1) = 0$, y en su anillo de valuación, $v(x) = 0$ syss x es inversible. Con ésto se puede concluir lo siguiente:

Corolario 11.34: Sea A un dominio de valuación discreta v. Entonces:

1. Todos los ideales impropios de A son de la forma:

$$\mathfrak{a}_n = \{x \in A : v(x) \geq n\}.$$

2. A es noetheriano.

3. A es local y su único ideal maximal es $\mathfrak{a}_1$.

Demostración: Es claro que de la primera se sigue el resto. Supongamos que $v(x) = v(y)$, entonces supongamos que $xy^{-1} \in A$ (por ser anillo de valuación), luego $v(xy^{-1}) = 0$, por lo que es inversible y luego $(x) = (y)$. Si $\mathfrak{b} \lhd A$ es un ideal impropio, entonces $v[\mathfrak{b}] \subseteq \mathbb{N}$, por lo que posee un mínimo n y un $x \in \mathfrak{b}$ con $v(x) = n$, luego es fácil concluir que $\mathfrak{b} = (x) = \mathfrak{a}_n$. □

Teorema 11.35: 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 íntegramente cerrado.

3. $\mathfrak{m}$ es un ideal principal.

4. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.
5. Todo ideal impropio es una potencia de $\mathfrak{m}$.
6. Existe un $x \in A$ tal que todo ideal impropio es de la forma (x^n).

DEMOSTRACIÓN: 1 $\implies$ 2. Puesto que

dominio de valuación discreta
$\Downarrow$
anillo de valuación
$\Downarrow$
íntegramente cerrado

2 $\implies$ 3. Sea $a \in \mathfrak{m}$ no nulo, entonces (a) es un ideal impropio. 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 impropio, 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 11.36: Si $(A, \mathfrak{m})$ es un dominio de valuación discreta y $\mathfrak{m} = (\pi)$, entonces decimos que π es un ***uniformizador*** de A.

Proposición 11.37: 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.

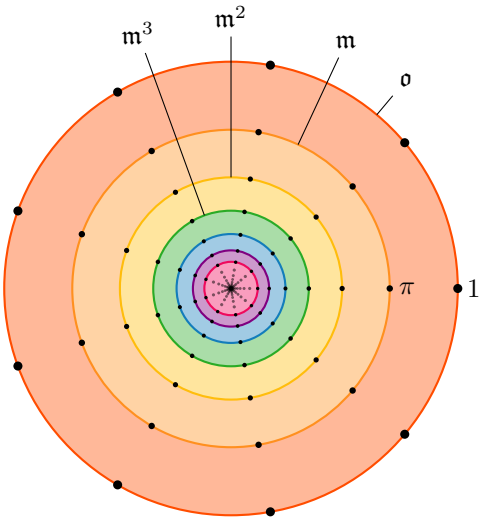


Figura 11.1. Cuerpo métrico discreto.

Demostración: Sea $\mathfrak{a} \lhd A$ un ideal impropio, por el teorema 6.73 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 6.76). □

Definición 11.38: Sea k un cuerpo métrico y sea $(a_n)_{n\in\mathbb{N}} \subseteq k$ una sucesión. Decimos que la suma formal $\sum_{n\in\mathbb{N}} a_n$ converge a un valor S, si la sucesión de las sumas parciales:

$$S_n := \sum_{i=0}^{n} a_n$$

converge a S; en cuyo caso anotaremos que $S = \sum_{n=0}^{\infty} a_n$.

Proposición 11.39: Sea k un cuerpo métrico no-arquimediano completo.

La serie $\sum_{n\in\mathbb{N}} a_n$ converge syss $\lim_n a_n = 0$.

DEMOSTRACIÓN: $\Longrightarrow$. Basta notar que

$$\lim_n a_n = \lim_n (s_n - s_{n-1}) = (\lim_n S_n) - (\lim_n S_{n-1}) = S - S = 0.$$

$\Longleftarrow$. Basta notar que, por desigualdad ultramétrica, se cumple que para $m > n$

$$|S_m - S_n| = |a_{n+1} + a_{n+2} + \cdots + a_m| \leq \text{máx}\{|a_j| : n < j \leq m\},$$

el cual, eligiendo n suficientemente grande, podemos acotar por un $\epsilon > 0$ arbitrario, y así, la sucesión $(S_n)_n$ es fundamental y converge. □

Ésto genera un símil con las series de $\mathbb{C}$, pero demuestra por qué la propiedad de ser *no-arquimediano* es mucho más potente (¡y útil!) en éstos casos.

Definición 11.40: Sea k un cuerpo métrico no-arquimediano. Un subconjunto $S \subseteq k$ se dice un ***conjunto de representantes de restos*** si para toda clase de equivalencia C de su cuerpo de restos de clases $\mathfrak{o}/\mathfrak{m}$ se cumple que existe exactamente un elemento de C en S.

Proposición 11.41: Sea k un cuerpo métrico no-arquimediano completo discreto. Sea $(\mathfrak{o}, \mathfrak{m})$ su anillo de valuación y sea $(\pi) = \mathfrak{m}$. Si S es un conjunto de representantes de restos, entonces todo elemento $a \in \mathfrak{o}$ se escribe de forma única como

$$a = \sum_{n=0}^{\infty} a_n \pi^n, \qquad a_i \in S.$$

DEMOSTRACIÓN: Como acotación, nótese que las series de esa forma siempre convergen por la proposición anterior, de modo que hay una correspondencia biunívoca.

Sea $a \in \mathfrak{o}$, entonces considere la clase de equivalencia $[a] \in \mathfrak{o}/(\pi)$, nótese que, por definición de S, existe un único $a_0 \in S$ tal que $a_0 \equiv a \pmod{\pi}$, vale decir, tal que $a - a_0 = \pi b_0$ para un único $b_0 \in \mathfrak{o}$. Análogamente existe un único $a_1 \in S$ tal que $a_1 \equiv b_0 \pmod{\pi}$, vale decir, tal que $b_0 - a_1 = \pi b_1$ para un único $b_1 \in \mathfrak{o}$; luego notamos que $a = a_0 + a_1\pi + b_1\pi^2$. Así procedemos definiendo por recursión $(a_n)_n \subseteq S$ y $(b_n)_n \in \mathfrak{o}$. Luego, comprobamos que

$$\left| a - \sum_{n=0}^{N} a_n \pi^n \right| = |b_N \pi^N| \leq |\pi|^N,$$

donde como $|\pi| < 1$, vemos que para $N \to \infty$ el valor absoluto converge a 0, o equivalentemente, $a = \sum_{n=0}^{\infty} a_n \pi^n$.

Para comprobar unicidad empleamos un método similar. Si $\sum_{n=0}^{\infty} c_n \pi^n = \sum_{n=0}^{\infty} a_n \pi^n$, entonces vemos que $c_0 \equiv a_0 \pmod{\pi}$ con lo que $c_0 = a_0$ por definición de conjunto de representantes de restos, y así vamos inductivamente comprobando. □

Teorema 11.42: Sea k un cuerpo métrico discreto y supongamos que su cuerpo de restos de clases es finito. Entonces $\mathfrak{o}$ es (topológicamente) compacto.

Demostración: Para espacios métricos, ser compacto equivale a ser secuencialmente compacto (cf. [**58,** Teo. 3.55]). Así pues, debemos comprobar que dada una sucesión $(a_j)_{j\in\mathbb{N}} \subseteq \mathfrak{o}$, entonces posee una subsucesión convergente. Sea S un conjunto de representantes de restos, el cual es finito por hipótesis; por la proposición anterior se cumple que

$$a_j = \sum_{n=0}^{\infty} a_{jn} \pi^n, \qquad a_{j,n} \in S.$$

Nótese que para cada n hay una sucesión $(a_{j,n})_j$ de puntos en S, luego necesariamente hay un valor que se repite infinitamente, para $j = 0$ escogemos una subsucesión $\sigma(j, 0)$ tal que $a_{\sigma(j,0),0}$ es constante. Similarmente, para $j = 1$ podemos extraer una subsucesión $\sigma(j, 1)$ de $\sigma(j, 0)$ tal que $a_{\sigma(j,0),0}$ y $a_{\sigma(j,1),1}$ son ambas constantes. Y esto lo podemos hacer para todo j, y finalmente definimos $\eta(j) := \sigma(j, j)$, la cual fija a la coordenada n-ésima para todo $j \geq n$, luego notamos que claramente converge. □

Corolario 11.43: Sea k un cuerpo métrico no-arquimediano. Son equivalentes:

1. k es localmente compacto.
2. k es completo, discreto y su cuerpo de restos de clases es finito.

Note que si uno quiere extender el corolario a cuerpos métricos arquimedianos, entoces ser localmente compacto equivale a ser completo por el teorema de Ostrowski.

§11.2.2 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 11.44: 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 11.45 – *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 $\mathfrak{o}$?). □

Veamos algunas aplicaciones del lema de Hensel:

Teorema 11.46: Sea $p \in \mathbb{Z}$ primo:

- Si $p \neq 2$: Sea $b \in \mathbb{Z}_p$ tal que $|b| = 1$ (i.e., $p \nmid b$). Supongamos que b es un residuo cuadrático módulo p, entonces b es un cuadrado en $\mathbb{Z}_p$.
- Si $p = 2$: Sea $b \in \mathbb{Z}_2$ tal que $b \equiv 1 \pmod 8$, entonces existe algún $a \in \mathbb{Z}_p$ tal que $b = a^2$.

Demostración: En ambos casos se emplea el lema con $f(x) := x^2 - b$. Nótese que $f'(x) = 2x$. El ser residuo cuadrático equivale a que existe a_0 con $a_0^2 \equiv b \pmod p$, de modo que $|f(a_0)| < 1 = |2a_0|^2 = |f'(a_0)|^2$ (pues $|2| = 1$). Para el segundo caso evaluamos en $a_0 = 1$ y se tiene que $|f(1)| \leq 2^{-3} < 2^{-2} = |2|^2$. □

Nótese que la condición de que $b \equiv 1 \pmod 8$ nos dice que b es un residuo cuadrático módulo 2^n para todo $n > 0$.

Corolario 11.47: Sea $p \in \mathbb{Z}$ primo:

- Si $p \neq 2$: El grupo $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, y representantes de las clases laterales son $1, p, c, cp$ con c un residuo no-cuadrático módulo p. En consecuencia, $\mathbb{Q}_p$ tiene exactamente 3 extensiones cuadráticas.
- Si $p = 2$: El grupo $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$, y representantes de las clases laterales son los generados por $-1, 5, 2$. En consecuencia, $\mathbb{Q}_2$ tiene exactamente 7 extensiones cuadráticas.

DEMOSTRACIÓN: Sea x un número no nulo libre de cuadrados en $\mathbb{Z}_p$ con $p \neq 2$. Aplicamos reducción módulo p: si $x \not\equiv 0 \pmod{p}$, entonces x es una unidad y existe $y \in \mathbb{Z}_p$ tal que $xy = c$, luego $y = c/x$ es un residuo cuadrático no nulo módulo p (pues es división de dos residuos no cuadradáticos) y por lo tanto $[c] = [x] \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. Si $x \equiv 0 \pmod{p}$, entonces como $p^2 \nmid x$ se tiene que $x/p \not\equiv 0 \pmod{p}$ luego, o bien x/p es un cuadrado o no, i.e., o bien $[x] = [p]$ o bien $[x] = [cp] \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

Para $p = 2$ siga un procedimiento similar. Otra manera de verlo es que $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ es un grupo abeliano de ocho elementos y tal que $[x^2] = 1$ para todo elemento del grupo. □

Proposición 11.48: Sea $p \in \mathbb{Z}$ primo:

- Si $p \neq 3$: Sea $b \in \mathbb{Z}_p$ con $|b| = 1$. Supongamos que b un residuo cúbico módulo p, entonces b es un cubo en $\mathbb{Z}_p$.
- Si $p = 3$: Sea $b \in \mathbb{Z}_3$ con $|b| = 1$. Se cumple que $b \equiv \pm 1 \pmod{9}$ syss b es un cubo en $\mathbb{Z}_3$.

DEMOSTRACIÓN: En éste caso empleamos el lema de Hensel con $f(x) := x^3 - b$. Veamos el caso de $p = 3$. La condición de que $b \equiv \pm 1$ (9) se traduce en que existe $e \in \{0, \pm 1\}$ tal que $b \equiv \pm(1 + 3e)^3 \pmod{27}$. Luego con $a_0 := \pm(1+3e)^3$ vemos que $|f(a_0)| \leq 3^{-3}$ y que $|f'(a_0)| = |3|\,|a_0^2| = 3^{-1}$. □

Aquí vemos un ejemplo del «comportamiento local» de los p-ádicos. Para hablar de ecuaciones diofantinas conviene admitir la siguiente terminología:

Definición 11.49: Se dice que $\mathbb{Q}$ es un ***cuerpo global*** y que sus completiones $\mathbb{R}, \mathbb{Q}_p$ son ***cuerpos locales***.

Como los cuerpos locales contienen al cuerpo global, vemos la siguiente observación a modo de eslógan:

> *La existencia de soluciones globales implica la existencia de soluciones locales.*

Una pregunta interesante sería tener una especie de recíproco, vale decir, ¿existen soluciones globales si existen soluciones locales en todas partes? La respuesta en general es que no:

Ejercicio 11.50: La ecuación diofántica:

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$$

tiene soluciones locales en todas partes, pero no soluciones globales.

Demostración: Es claro que la ecuación no posee soluciones globales. Por otro lado, sabemos que 2 es un cuadrado en $\mathbb{Q}_{17}$ y que 17 es un cuadrado en $\mathbb{Q}_2$ pues $17 \equiv 1 \pmod 8$. Finalmente, nótese que en $\mathbb{Z}_p$ con $p \notin \{2, 17\}$ siempre se cumple que $2, 17, 34$ son inversibles (tienen $|\,| = 1$) y siempre alguno es un cuadrado módulo p (basta expresarlos como potencias de una raíz primitiva). □

Lema 11.51: 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

$$\begin{aligned} u_0 + u_1\alpha + \cdots + u_n\alpha^n &= 1 \\ v_0 + v_1\alpha^{-1} + \cdots + v_m\alpha^{-m} &= 1 \end{aligned} \tag{11.1}$$

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 (11.1) se obtiene una expresión con grado menor, lo que contradice la minimalidad de n. □

Lema (AE) 11.52: 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) 11.53: 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:

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & L \\ & \searrow \quad \nearrow_{f^*} & \\ & k & \end{array}$$

así mismo, como k'/k es finita y L es normal, entonces:

$$\begin{array}{ccc} k' & \xrightarrow{\ \bar{f}\ } & L \\ \uparrow & & \| \\ k & \xrightarrow{\ f^*\ } & L \end{array} \quad \mathrm{Id}$$

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) 11.54: 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:

$$\begin{array}{ccccccc} & & & \overset{\varphi}{\frown} & & & \\ A & \hookrightarrow & A' & \twoheadrightarrow & k & \hookrightarrow & L \end{array}$$

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 $\alpha \notin V$. □

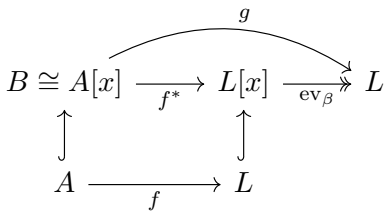
Proposición (AE) 11.55: Sea B/A una extensión de dominios íntegros con B una A-álgebra de tipo finito. Sea $v \in B_{\neq 0}$ existe un $u \in A_{\neq 0}$ tal que todo homomorfismo de anillos $f\colon A \to L$ con L un cuerpo algebraicamente cerrado y con $f(u) \neq 0$ se puede extender a $g\colon B \to L$ 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) <u>α es trascendente:</u> 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 10.63 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) 11.56: Sea L/k una extensión de cuerpos con L una k-álgebra de tipo finito. Entonces L/k es una extensión finita.

11.3 Dominios de valuación discreta y de Dedekind

Lema 11.57: 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 11.22.

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 11.58: 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 11.59: En un dominio de valuación discreta, todo ideal puede escribirse de manera única como producto de ideales primos.

Definición 11.60: 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 11.61: 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 10.80 se satisface que es no vacío en $\mathbb{Z}$, luego su contracción es maximal, así que por el colorario 10.79 se cumple que $\mathfrak{p}$ es maximal. □

Definición 11.62: 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 $MN = A$.

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 11.63: Sea A un dominio íntegro, $K := \operatorname{Frac} A$ y $M \subseteq K$ un A-submódulo. Entonces son equivalentes:

1. M es inversible.
2. M es finitamente generado y para todo $\mathfrak{p} \lhd A$ primo, $M_{\mathfrak{p}}$ es inversible.
3. M es finitamente generado y para todo $\mathfrak{m} \lhd A$ maximal, $M_{\mathfrak{m}}$ es inversible.

Demostración: $1 \implies 2$. Basta notar que $A_{\mathfrak{p}} = (M \cdot (A : M))_{\mathfrak{p}} = M_{\mathfrak{p}} \cdot (A : M)_{\mathfrak{p}}$.

$2 \implies 3$. Trivial.

$3 \implies 1$. Definamos $\mathfrak{a} := M \cdot (A : M)$ el cual es un ideal entero sobre A. Como $M_{\mathfrak{m}}$ es inversible, entonces

$$\mathfrak{a}_{\mathfrak{m}} = \big(M \cdot (A : M)\big)_{\mathfrak{m}} = M_{\mathfrak{m}} \cdot (A : M)_{\mathfrak{m}} = M_{\mathfrak{m}} \cdot (A_{\mathfrak{m}} : M_{\mathfrak{m}}) = A_{\mathfrak{m}},$$

por lo que $\mathfrak{a} \not\subseteq \mathfrak{m}$ y ésto aplica para todo ideal maximal, por lo que $\mathfrak{a} = A$. $\square$

Proposición 11.64: Sea A un dominio íntegro local. Entonces A es un dominio de valuación discreta syss todo ideal fraccionario no nulo es inversible.

Demostración: $\implies$. 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 $M = (x^{r-s})$.

$\impliedby$. 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 11.65: 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 11.66: Sea A un dominio de Dedekind. Entonces los ideales fraccionarios no nulos de A forman un grupo.

12

Compleciones y teoría de la dimensión

12.1 Series de potencias

Definición 12.1 (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 12.2: 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 12.3: 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 12.4: $f(x) \in A[[x]]$ 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 12.5: 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.

12.2 Compleciones

Definición 12.6: 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 12.7: 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 12.8: 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 12.9: 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. [**55,** 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. [**55,** Prop. 2.21]) y es fácil describir los límites inversos de Set (cf. [**55,** 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. [**58,** Def. 2.30, p. 43]).

Definición 12.10: 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 12.11: 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 12.12: 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 12.13: 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 12.14: 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 12.15: $\hat{G}/\hat{G}_n \cong G/G_n$ y de hecho $\hat{\hat{G}} = G$.

Definición 12.16: 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 12.17: 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 12.18: 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 12.19: La topología sobre $\hat{M}$ tal que $\hat{M} \cong \varprojlim_n M/\mathfrak{a}^n M$ se dice la ***topología*** $\mathfrak{a}$***-ádica***.

12.3 Anillos y módulos graduados

Definición 12.20: Un ***anillo graduado*** es una $\mathbb{Z}$-álgebra graduada.

Proposición 12.21: Sea A un anillo graduado y sean $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$ homogéneos. Entonces:

1. $A/\mathfrak{a} = \bigoplus_{d\in\mathbb{N}} A_d/\mathfrak{a}$. En consecuente, $A/\mathfrak{a}$ es un anillo graduado.
2. $\mathfrak{a}$ es primo syss para todos $f, g \in A$ homogéneos tales que $fg \in \mathfrak{a}$ se cumple que $f \in \mathfrak{a}$ o $g \in \mathfrak{a}$.
3. $\mathfrak{a} + \mathfrak{b}, \mathfrak{a} \cdot \mathfrak{b}, \mathfrak{a} \cap \mathfrak{b}$ son homogéneos.
4. $\mathrm{Rad}(\mathfrak{a})$ es homogéneo.

Demostración:

1. Es claro ver que $A/\mathfrak{a} = \sum_{d\in\mathbb{N}} A_d/\mathfrak{a}$ en general (vale incluso si $\mathfrak{a}$ no es homogéneo). Así que queda probar que están en suma directa, para ello sean $f \in A_d/\mathfrak{a} \cap A_e/\mathfrak{a}$ con $d \neq e$. Es decir, $f = f_d + g_d = f_e + g_e \in A$, donde $f_d \in A_d, f_e \in A_e$ y $g_d, g_e \in \mathfrak{a}$. Nótese que como su representación por coordenadas es única se obtiene que, mirando la d-ésima coordenada, se tiene que $f_d + c_d h_{dd} = c'_d h_{de}$, donde h_{ij} son

generadores homogéneos de $\mathfrak{a}$ y $c_d, c'_d \in R_0$. Pero por clausura de $\mathfrak{a}$ como ideal se concluye de $f_d = c_d h_{dd} - c'_d h_{de} \in \mathfrak{a}$, por lo que $f = 0 \in A/\mathfrak{a}$ como se quería probar.

2. Claramente se cumple « $\Longrightarrow$ », veamos la otra implicancia: En primer lugar, como $f', g' \in A$ se ha de cumplir que

$$f' = \sum_{i=0}^{n} f_i, \quad g' = \sum_{j=0}^{m} g_j$$

con f_d, g_d homogéneos de grado d (posiblemente nulos). Luego sea $f'g' = \sum_{d=0}^{n+m} \sum_{i+j=d} f_i g_j \in \mathfrak{a}$. Por construcción, se debe cumplir que cada término homogéneo $h_d := \sum_{i+j=d} f_i g_j \in \mathfrak{a}$. Luego haremos la demostración por inducción sobre la cantidad de términos homogéneos de $f'g'$:

El caso base: un solo término, es trivial ya que $f' = f_i$ y $g' = g_j$, donde cada término es homogéneo. Y el caso inductivo se ve así:

$$f'g' = h_0 + h_1 + \cdots + h_{n+m}.$$

Donde $h_{n+m} \neq 0$. Como $\mathfrak{a}$ es un ideal homogéneo ha de cumplirse que cada $h_d \in \mathfrak{a}$. Además, $h_{n+m} = f_n g_m \in \mathfrak{a}$ necesariamente. Luego, $f_n \in \mathfrak{a}$ o $g_m \in \mathfrak{a}$, sin perdida de generalidad supongamos la primera. Luego

$$(f' - f_n)g' = h_0 + \cdots + h_{n-1} + h'_n + \cdots + h'_{n+m-1}$$

donde cada $h'_{n+i} = f_{n-1}g_{i+1} + \cdots = h_{n+i} - f_n g_i$. Sin embargo, como $f_n \in \mathfrak{a}$ se cumple que $h'_{n+i} \in \mathfrak{a}$, por lo que $(f' - f_n)g' \in \mathfrak{a}$ y tiene menos términos que el original, así que, por hipótesis inductiva, se cumple que $(f' - f_n) \in \mathfrak{a}$ o $g' \in \mathfrak{a}$; lo que concluye el caso inductivo.

3. La intersección es trivial. Sean T_a, T_b son generadores por homogéneos de $\mathfrak{a}, \mathfrak{b}$ resp. Para la suma, basta notar que $T_a \cup T_b$ es un generador por homogéneos de $\mathfrak{a} + \mathfrak{b}$, y para el producto basta notar que $T_a \cdot T_b = \{fg : f \in T_a, g \in T_b\}$ es generador por homogéneos de $\mathfrak{a} \cdot \mathfrak{b}$.

4. Emplearemos la caracterización del radical como intersección de ideales primos, notando que si $\mathfrak{a} \subseteq \mathfrak{p}$, con $\mathfrak{p} \trianglelefteq R$ primo, entonces existe $\mathfrak{a} \subseteq \mathfrak{p}_h \subseteq \mathfrak{p}$, donde $\mathfrak{p}_h$ es primo y homogéneo. Para ello definamos

$$\mathfrak{p}_h := \big(\{f \in \mathfrak{p} : f \text{ homogéneo}\}\big),$$

por el inciso anterior se concluye que $\mathfrak{p}_h$ es primo y claramente $\mathfrak{a} \subseteq \mathfrak{p}_h$. Luego, hemos probado que

$$\mathrm{Rad}(\mathfrak{a}) = \bigcap \{\mathfrak{p} : \mathfrak{a} \subseteq \mathfrak{p} \trianglelefteq R \text{ primo y homogéneo}\}$$

de modo que $\mathrm{Rad}(\mathfrak{a})$ es homogéneo por el inciso anterior. □

Hay otra demostración de que $\mathrm{Rad}(\mathfrak{a})$ que no emplea AE (y por ende, no emplea el teorema 6.28), queda al lector proponerla.

Proposición 12.22: Sea A un dominio graduado. Entonces son equivalentes:

1. A es noetheriano.

2. A_0 es noetheriano y A es una A_0-álgebra de tipo finito.

Demostración: $1 \implies 2$. Primero, se tiene que $A_0 \cong A/A^+$ es noetheriano.

Como $A^+ \lhd A$, entonces $A^+ = (\alpha_1, \ldots, \alpha_s)$ con α_i homogéneo de grado $k_i > 0$ y sea $A' := A_0[\alpha_1, \ldots, \alpha_s]$. Hemos de probar inductivamente que $A_n \subseteq A'$ para todo n. El caso base $A_0 \subseteq A'$ es trivial. Sea $y \in A_n$ con $n > 0$, luego $y \in A^+$ y por ende $y = \sum_{i=1}^{s} \lambda_i \alpha_i$, donde podemos elegir a λ_i tal que sea homogéneo de grado $n - k_i < n$. Por hipótesis inductiva $\lambda_i \in A'$, luego $y \in A'$ como se quería ver.

$2 \implies 1$. Ver teorema de bases de Hilbert. □

Definición 12.23: Dado un anillo graduado A como ántes, se dice que M es un *A-módulo graduado* si existe una familia $(M_n)_{n\in\mathbb{N}}$ de subgrupos de M tales que:

MG1. $M = \bigoplus_{n\in\mathbb{N}} M_n$.

MG2. $A_n \cdot M_m \subseteq M_{n+m}$ para todo $n, m \in \mathbb{N}$.

Dado un par M, N de A-módulos graduados, se dice que $\varphi\colon M \to N$ es un *homomorfismo de A-módulos graduados* si es un homomorfismo de A-módulos y $\varphi[M_n] \subseteq N_n$.

Definición 12.24: Sea A un dominio y sea $\mathfrak{a} \trianglelefteq A$. Se define la ***álgebra***

de Rees de $\mathfrak{a}$ como:[2]

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

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 12.25: 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 equivalentes:

1. $\mathrm{Bl}_{\mathcal{J}}(M)$ es un $\mathrm{Bl}_{\mathfrak{a}}(A)$-módulo finitamente generado.

2. La filtración $\mathcal{J}$ es $\mathfrak{a}$-estable.

Demostración: Sea $Q_n := \bigoplus_{n=0}^{r} M_n$ 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 $\mathrm{Bl}_{\mathfrak{a}}(A)$-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 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 12.26 (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'.

[2] Atiyah y McDonald [**16**] 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.

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 12.27: 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 12.28: 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 12.29: 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 12.30: Sea A un dominio y M un A-módulo finitamente generado. Sea

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

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

Demostración: Por la proposición anterior se induce:

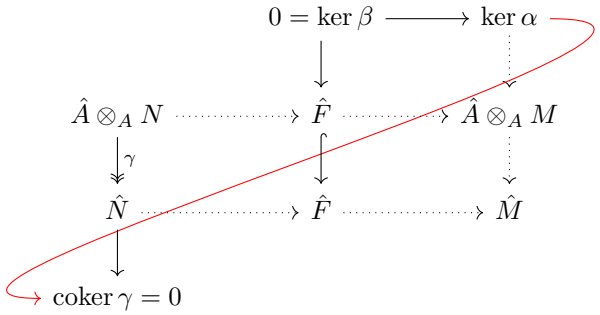
$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & M \otimes N & \longrightarrow & N & \longrightarrow & 0 \\ & & & & \Downarrow & & & & \\ 0 & \longrightarrow & \hat{M} & \longrightarrow & \widehat{M \otimes N} & \longrightarrow & \hat{N} & \longrightarrow & 0 \end{array}$$

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 12.31: 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 12.32: 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 12.33: 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 12.34: Sea A es un dominio noetheriano íntegro y $\mathfrak{a} \lhd A$. Entonces

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

Teorema 12.35 (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 12.36: 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 12.37: 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. □

Definición 12.38: 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:

$$\mathrm{in}\colon A \longrightarrow \mathrm{gr}_\mathfrak{a}(A)$$

$$a \longmapsto (a \mod \mathfrak{a}^n)_{n\in\mathbb{N}}.$$

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 $\operatorname{in} a = 0$ syss $a = 0$, pero como in no es un homomorfismo, entonces ésto no implica inyectividad.

Proposición 12.39: Sea A un dominio noetheriano local y $\mathfrak{a} \lhd A$. Si $\operatorname{gr}_{\mathfrak{a}}(A)$ es un dominio íntegro, entonces A también.

Demostración: Sean $a, b \in A$ tales que $ab = 0$. Luego, claramente $\operatorname{in}(a)\operatorname{in}(b) = 0$ y como $\operatorname{gr}(A)$ 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 12.40: Sea A un dominio noetheriano, $\mathfrak{a}$ un ideal propio de A. Entonces:

1. $\operatorname{gr}_{\mathfrak{a}}(A)$ es noetheriano.
2. $\operatorname{gr}_{\mathfrak{a}}(A) \cong \operatorname{gr}_{\hat{\mathfrak{a}}}(\hat{A})$ (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 $\operatorname{gr}_{\mathcal{J}}(M)$ es un $\operatorname{gr}_{\mathfrak{a}}(A)$-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 $\operatorname{gr}_{\mathfrak{a}}(A) = (A/\mathfrak{a})[\overline{\alpha}_1, \ldots, \overline{\alpha}_s]$. $A/\mathfrak{a}$ es noetheriano y $\operatorname{gr}_{\mathfrak{a}}(A)$ 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 $\operatorname{gr}_n(M)$ 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 $\operatorname{gr}_{n_0+r}(M) = 0$ en $(A/\mathfrak{a})$. Por lo que, $\operatorname{gr}(M) = \bigoplus_{n=0}^{n_0} \operatorname{gr}_n(M)$, el cual es una suma directa finita de módulos finitamente generados, luego es también finitamente generada como $\operatorname{gr}_{\mathfrak{a}}(A)$-módulo. □

Lema 12.41: 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:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \ker(\mathrm{gr}_n(\phi)) & \longrightarrow & \ker(f_{n+1}) & \longrightarrow & \ker(f_n) \\ & \searrow & & & & & \\ & & \mathrm{coker}(\mathrm{gr}_n(\phi)) & \longrightarrow & \mathrm{coker}(f_{n+1}) & \longrightarrow & \mathrm{coker}(f_n) \longrightarrow 0 \end{array}$$

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 12.13. □

Proposición 12.42: 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:

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

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 12.43: 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 $\operatorname{gr}(M)$ es un $\operatorname{gr}(A)$-módulo noetheriano, entonces M es noetheriano.

Teorema 12.44: 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 $\operatorname{gr}_{\mathfrak{a}}(A) \cong \operatorname{gr}_{\hat{\mathfrak{a}}}(\hat{A})$ y que $\operatorname{gr}_{\mathfrak{a}}(A)$ es noetheriano. Luego basta aplicar el corolario anterior. □

Teorema 12.45: 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 12.46: 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

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

   tal que $x_i \mapsto f_i$.

2. Si el A-homomorfismo inducido $A \to B/\mathfrak{n}$ es un epimorfismo, entonces $\operatorname{ev}_{(f_1,\ldots,f_n)}$ 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 $x_i \mapsto f_i \mod \mathfrak{n}^m$. 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:

$$\begin{array}{ccc} \frac{A[[\boldsymbol{x}]]}{(x_1,\ldots,x_n)^m} & \xrightarrow{\alpha_m} & \frac{B}{\mathfrak{n}^m} \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow \\ \frac{A[[\boldsymbol{x}]]}{(x_1,\ldots,x_n)^{m-1}} & \xrightarrow{\alpha_{m-1}} & \frac{B}{\mathfrak{n}^{m-1}} \end{array} \tag{12.1}$$

luego pasando límites inversos tenemos el homomorfismo deseado.

2. Basta notar que en el diagrama 12.1 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 $\mathrm{in}\, g$ 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 $\ker \mathrm{gr}\,\varphi = (0)$, luego $\mathrm{gr}\,\varphi(\mathrm{in}\, g) \neq 0$ y, en particular, como $\mathrm{gr}\,\varphi$ es un homomorfismo entre álgebras graduadas, $\mathrm{gr}\,\varphi(\mathrm{in}\, g)$ tiene parte homogénea de grado d no nula. Ahora bien, como $g \equiv \mathrm{in}(g)$ mód $(x_1,\ldots,x_n)^{d+1}$, tenemos que $\varphi(g) \equiv \mathrm{gr}\,\varphi(\mathrm{in}(g)) \mod \mathfrak{n}^{d+1}$ por lo que $\varphi(g) \neq 0$ como se quería ver. □

12.4 Teoría de la dimensión

Definición 12.47: 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 $\operatorname{rank}\colon C \to \mathbb{Z}$ 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 5.46 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 12.48: 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 12.49 (Hilbert-Serre): Sea A un anillo graduado noetheriano, tal que $A = A_0[\alpha_1, \ldots, \alpha_s]$ 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 12.50: 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 12.51: 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 $\operatorname{Poin}(M,t)$, 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 10: 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 12.52: 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 12.53: Sea $(A, \mathfrak{m})$ un dominio noetheriano local, $\mathfrak{q}$ un ideal $\mathfrak{m}$-primario, M un A-módulo finitamente generado y $(M_n)_{n\in\mathbb{N}}$ 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 $G(A) := \bigoplus_{n\in\mathbb{N}} \mathfrak{q}^n/\mathfrak{q}^{n+1}$ y $G(M) := \bigoplus_{n\in\mathbb{N}} M_n/M_{n+1}$. Como A es noetheriano, $G(A)$ también y luego $G(M)$ es un $G(A)$-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 12.54: 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 12.55: 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 $\ell(M/M_n)$ para n suficientemente grande. Si $M = A$, entonces obviamos el superíndice, i.e., $\chi_{\mathfrak{q}}(n) := \chi_{\mathfrak{q}}^A(n)$.

Proposición 12.56: 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 12.57: 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 12.58: $\delta(A) \geq d(A)$.

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

Proposición 12.59: 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 12.60: 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 12.61: $d(A) \geq k.\dim(A)$.

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 $d > 0$: Si $k.\dim(A) = 0$, entonces claramente vale el enunciado, sino sea

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

una cadena de ideales primos en A, luego 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 12.62: Si A es un dominio noetheriano local, entonces posee dimensión de Krull finita.

Definición 12.63: Sea $\mathfrak{p} \lhd A$ primo, entonces definimos su *altura*, denotada $n := \operatorname{alt}\mathfrak{p} \geq 0$, como el máximo natural tal que existe una cadena

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$

de ideales primos de A. La dimensión de Krull de A corresponde entonces al supremo de las alturas de sus ideales primos.

Además por correspondencia se puede ver que $\operatorname{alt}\mathfrak{p} = k.\dim(A_{\mathfrak{p}})$.

Corolario 12.64: En un dominio noetheriano local todo ideal primo posee altura finita. Luego toda cadena descendiente de ideales primos posee minimal.

Proposición 12.65: 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 2.58, 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 12.66 – *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 12.67: 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 12.68: 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 12.69: 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 $\operatorname{alt} \mathfrak{p} = k.\dim(A_{\mathfrak{p}}) \leq r$. □

Teorema 12.70 (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 $\operatorname{alt}\mathfrak{p} = 1$. □

Teorema 12.71: 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 2.45 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. □

Corolario 12.72: 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: Sea $d := k.\dim(A/(\beta))$, por el corolario 12.60 se satisface que $d \leq k.\dim(A) - 1$. Por otro lado, sean $\overline{\alpha}_1, \ldots, \overline{\alpha}_d$ un sistema de parámetros de $A/(x)$, luego $(\alpha_1, \ldots, \alpha_d, \beta)$ es un ideal $\mathfrak{m}$-primario en A y luego $d + 1 \geq k.\dim(A)$. □

Corolario 12.73: 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 $\chi_{\mathfrak{m}}(n) = \chi_{\hat{\mathfrak{m}}}(n)$. □

Proposición 12.74: 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 10. Pero $d(\mathrm{gr}_{\mathfrak{q}}(A)) = d$, por lo que el último resultado es absurdo. □

Corolario 12.75: 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. □

Teorema 12.76: 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 12.77: Un dominio noetheriano local A se dice *regular* si satisface cualquiera de las condiciones del teorema anterior.

Lema 12.78: Sea A un dominio, $\mathfrak{a}$ un ideal de A tal que $\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = (0)$. Si $\mathrm{gr}_{\mathfrak{a}}(A)$ es un dominio íntegro, entonces A también lo es.

Demostración: Sean α, β no nulos. Como $\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n$, entonces existen m, r naturales tales que $\alpha \in \mathfrak{a}^m \setminus \mathfrak{a}^{m+1}$ y $\beta \in \mathfrak{a}^r \setminus \mathfrak{a}^{r+1}$, luego sus proyecciones $\overline{\alpha}, \overline{\beta}$ tienen componentes homogéneas no nulas en $\mathrm{gr}_m(A), \mathrm{gr}_r(A)$ resp., por lo que $\overline{\alpha} \cdot \overline{\beta} \neq 0$ y luego $\alpha \cdot \beta \neq 0$ en A. □

Corolario 12.79: Un dominio regular de dimensión 1 es un dominio de valuación discreta.

Proposición 12.80: 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. □

Notas históricas

El teorema de las intersecciones de Krull fue demostrado originalmente en Krull **[45]** (1938).

13

Derivaciones

13.1 Módulo de diferenciales de Kähler

Definición 13.1 – *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 13.2: 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 13.3: $\mathrm{Der}_k(A, -) \colon \mathsf{Mod}_A \to \mathsf{Set}$ 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 13.4: Sea $f \colon k \to A$ una k-álgebra y M un A-módulo. Entonces $A * M := A \oplus M$ con la multiplicación

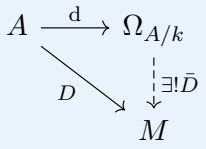
$$(a, \boldsymbol{m}) \cdot (b, \boldsymbol{n}) := (ab, a\boldsymbol{n} + b\boldsymbol{m})$$

es una k-álgebra; con $\lambda \mapsto (f(\lambda), \vec{0})$.

Proposición 13.5: 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 13.6: 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):

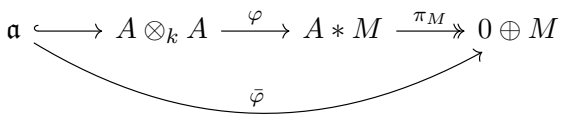
$$0 \longrightarrow \Omega_{A/k} \xrightarrow{\iota} B \xrightarrow{\bar{\mu}} A \longrightarrow 0$$

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 13.7: 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 13.8: $\Omega_{A/k}$ 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 13.9: 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:

$$\begin{array}{ccc} A & \xrightarrow{u} & B/\mathfrak{n} \\ \uparrow & \overset{v}{\swarrow} & \uparrow\!\uparrow \\ k & \dashrightarrow & B \end{array} \tag{13.1}$$

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 (13.1) conmuta. Una k-álgebra A se dice 0-***étale*** sobre k si es 0-suave y 0-no ramificada.

Proposición 13.10: A es 0-no ramificada sobre k syss $\Omega_{A/k} = 0$.

DEMOSTRACIÓN: $\Longrightarrow$. Por la proposición 13.5 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 13.11: Dados $f\colon k \to A, g\colon A \to B$ homomorfismos de anillos, se tiene la siguiente sucesión exacta (en Mod_B):

$$\Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \longrightarrow 0 \tag{13.2}$$

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

$$0 \longrightarrow \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \longrightarrow 0 \tag{13.3}$$

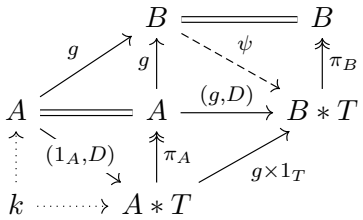
es exacta y se escinde.

Demostración: Por la proposición 5.20, 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 13.5 extraemos el siguiente diagrama conmutativo:



donde la existencia de ψ viene de la definición de 0-suave. Nuevamente la correspondencia 13.5 nos da una derivación lo que demuestra que h_α es epimorfismo. □

Teorema 13.12: 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):

$$\begin{aligned} \mathfrak{m}/\mathfrak{m}^2 &\xrightarrow{\delta} \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \longrightarrow 0 \\ x \text{ mód } \mathfrak{m}^2 &\longmapsto \mathrm{d}_{A/k}x \otimes 1. \end{aligned} \tag{13.4}$$

Además, si B es 0-suave sobre k, entonces la siguiente sucesión

$$0 \longrightarrow \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\delta} \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \longrightarrow 0 \qquad (13.5)$$

es exacta y se escinde.

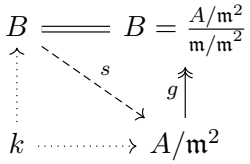
En primer lugar, nótese que en éste caso la proyección $g\colon A \to A/\mathfrak{m} = B$ es un epimorfismo, de modo que es fácil comprobar que el homomorfismo de B-módulos α de (13.2) es un epimorfismo; luego por exactitud $\Omega_{B/A} = 0$.

Demostración: La exactitud de (13.4) equivale, por la proposición 5.20, 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 13.3. 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 (13.5) se escinde. □

Teorema 13.13: 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 (13.3). □

En particular, el último teorema aplica siempre que $\operatorname{car} K = 0$.

Teorema 13.14: 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

$$D^n = c_{n-1}D^{n-1} + \cdots + c_1 D + c_0. \tag{13.6}$$

   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 (13.6) 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. □

13.2 Separabilidad

Definición 13.15: 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 13.16: 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 13.17: 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

$$\Delta(B) := \det\left([\mathrm{Tr}_{A/k}(\alpha_i \alpha_j)]_{ij}\right).$$

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 13.18: 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 $L := k^{\text{alg}}$, 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 $0 = \text{trdeg}_k(A) = k.\dim(A)$ por lo que A es un dominio artiniano reducido y por el corolario 6.95 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 13.19: 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 13.20: 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

$$(A^t \cdot A)_{ij} = \sum_{\ell=1}^{n} \sigma_\ell(\gamma^{i-1})\sigma_\ell(\gamma^{j-1}) = \sum_{\ell=1}^{n} \sigma_\ell(\gamma^{i-1}\gamma^{j-1}) = \text{Tr}_{K'/k}(\gamma^{i-1}\gamma^{j-1}).$$

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. 3.58)

$$\det(A) = \prod_{i<j}(\sigma_j(\gamma) - \sigma_i(\gamma)),$$

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

$$k(\Gamma) \otimes_k L \leq \text{Frac}(k[\Gamma] \otimes_k L) = \text{Frac}(L[\Gamma]) = L(\Gamma),$$

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 13.21: 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 13.22: 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 $F(x_1, \ldots, x_r, y) \in k[\boldsymbol{x}, y]$ tal que $F(\alpha_1, \ldots, \alpha_r; \beta^p) = 0$.

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:

$$k(\alpha_1, \ldots, \alpha_r; \beta) \otimes_k k^{1/p} = \frac{k[\boldsymbol{x}, y]}{(F(\boldsymbol{x}, y))} \otimes_k k^{1/p} = \frac{k^{1/p}[\boldsymbol{x}, y]}{(G(\boldsymbol{x}, y)^{1/p})},$$

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 $k(\alpha_2, \ldots, \alpha_r; \beta)$. Intercambiando α_1, β tenemos que $\alpha_{r+1}, \ldots, \alpha_{q+1}$ es separable algebraico sobre k' y, por inducción, vemos que $\alpha_{r+1}, \ldots, \alpha_n$ lo es. □

Teorema 13.23: 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 4.34 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 6.74, 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 13.24: Dada una extensión L/k con K, K' extensiones intermedias, son equivalentes:

1. Si $\alpha_1, \ldots, \alpha_r \in K$ son k-linealmente independientes, entonces son K'-linealmente independientes.
2. Si $\beta_1, \ldots, \beta_r \in K'$ 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 $\alpha_1, \ldots, \alpha_r$ sean k-linealmente independientes y $\alpha_{r+1}, \ldots, \alpha_m$ 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 13.25: Dada una extensión L/k con K, K' extensiones intermedias, se dice que K, K' son ***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 13.26: 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 5.64) da:

Teorema 13.27: Sea Ω/k una extensión de cuerpos con $M/L/k$ y K/k extensiones intermedias. Luego M y K son linealmente disjuntos sobre k syss L y K son linealmente disjuntos sobre k, y $K \vee L$ y M son linealmente disjuntos sobre L (ver fig. 13.1).

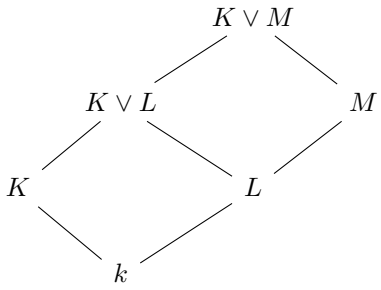


Figura 13.1

Teorema 13.28 (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. □

§13.2.1 Bases diferenciales.

Teorema 13.29: 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 13.30: 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 13.31: 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 13.32: 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:

$$\phi \colon \operatorname{Der}_k(K) \longrightarrow \operatorname{Func}(S; K)$$

   tal que para todo $s \in S$ y toda derivación $D \in \operatorname{Der}_k(K)$ se cumple que $Ds = \phi(D)(s)$.

4. En particular, $\dim_K(\operatorname{Der}_k(K)) = |S|$.

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 13.30, 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 13.30 para concluir. □

Definición 13.33: 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 13.34: 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 base de trascendencia.

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 13.30 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 13.32. □

Lema 13.35: Sea L/K una extensión de cuerpos. Son equivalentes:

1. L y K^{alg} (vistos dentro de L^{alg}) son 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 [8, pág. 95].

$3 \implies 1$. Trivial. □

Definición 13.36: 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 $\mathrm{Frac}(R)/K$ es una extensión regular de cuerpos.

Teorema 13.37: 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 linealmente disjuntas sobre k y K/k es regular, entonces $K \vee L/L$ es regular.
4. Si L, K son extensiones intermedias linealmente disjuntas sobre k, y K/k y L/k son regulares, entonces $K \vee L/k$ es regular.

Demostración:

1. Claramente $K \otimes_k k^{\text{alg}} \leq L \otimes_k k^{\text{alg}}$.
2. Por cambio de base, $L \otimes_k k^{\text{alg}} = L \otimes_K (K \otimes_k k^{\text{alg}}) \cong L \otimes_K (K \vee k^{\text{alg}})$. Como $K \vee k^{\text{alg}}/K$ es una extensión de cuerpos, entonces $L \otimes_k k^{\text{alg}}$ 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. □

Índice de notación

$\vee, \wedge$	Disyuntor, "o lógico" y conjuntor, "y lógico" respectivamente.
$\Longrightarrow$	Implica, entonces.
$\Longleftrightarrow$	Si y sólo si.
$\forall, \exists$	Para todo, existe respectivamente.
$\in$	Pertenencia.
$\subseteq, \subset$	Subconjunto, subconjunto propio resp.
$\cup, \cap$	Unión e intersección binaria respectivamente.
$A \setminus B$	Resta conjuntista, A menos B.
A^c	Complemento de A (respecto a un universo relativo).
$A \times B$	Producto cartesiano de A por B.
$A_{\neq x}$	Abreviación de $A \setminus \{x\}$.
$f : A \to B$	Función f de dominio A y codominio B.
$f \circ g$	Composición de f con g. $(f \circ g)(x) = g(f(x))$.
$\mathcal{P}(A)$	Conjunto potencia de A.
resp.	Respectivamente.

syss	Si y sólo si.
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$	Conjuntos de números naturales, enteros y racionales resp.
$\aleph_0$	Cardinal numerable, cardinalidad de $\mathbb{N}$.
AE	Axioma de elección.
DE, AEN	Axioma de elecciones dependientes, y de elecciones numerables resp.
ZF(C)	Teoría de Zermelo-Fraenkel. La C representa el axioma de elección.
a^{-1}	Inversa de un elemento invertible en un grupo, p. 4.
$S \leq G$	S es subgrupo (anillo o espacio) de G, p. 6.
$\langle S \rangle$	Subgrupo, cuerpo o espacio generado por S, p. 6.
$\operatorname{ord} x$	Orden de un elemento x, p. 7.
$G \cong H$	G y H son estructuras isomorfas, p. 9.
$\mathbb{Z}_n^\times$	Grupo multiplicativo o de las unidades de n, aquél formado por los coprimos de n, p. 11.
$\phi(n)$	Función indicatriz de Euler de n, esto es, la cantidad de coprimos positivos menores a n, p. 11.
S_n	Grupo simétrico sobre $\{1, 2, \ldots, n\}$, p. 13.
$\operatorname{sgn} \sigma$	Signo de la permutación σ, p. 15.
A_n	Grupo alternante en S_n, p. 16.
D_{2n}	Grupo diedral de cardinal $2n$, p. 17.
$N \trianglelefteq G$	N es subgrupo de G, p. 18.
$Z(S), Z(G)$	Centralizador de S, centro de G resp., p. 18.
$\mathrm{N}_G(S)$	Normalizador de S, p. 19.
$C_G(S)$	Clase de conjugación de S, p. 19.
K_4	Grupo de Klein de 4 elementos, $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, p. 26.

$N \rtimes_\alpha A$	Producto semidirecto de N con A, donde A actúa sobre N, p. 28.
Orb_a	Órbita de a, osea, los $\alpha_g(a)$ para todo $g \in G$, p. 29.
Stab_a	Estabilizador de a, osea, los $g \in G$ que dejan a a fijo, p. 29.
$\mathrm{Fix}_g(S)$	Puntos fijos de la acción α_g sobre S, p. 32.
$\mathrm{Fix}_G(S)$	Puntos fijos de todas las acciones sobre S, p. 32.
$\mathrm{Syl}_p(G)$	El conjunto de p-subgrupos de Sylow de G, p. 33.
$A^\times$	El conjunto de elementos invertibles de un anillo unitario A, p. 50.
$\Bbbk$	Un cuerpo general, p. 51.
$\mathrm{Frac}(A)$	Cuerpo de fracciones de un dominio íntegro A, p. 67.
$A[S]$	Conjunto de polinomios con coeficientes en A y con indeterminadas de S, p. 69.
$\deg f$	Grado del polinomio f, p. 69.
$\mathrm{ev}_{\alpha_1,\ldots,\alpha_n}$	Homomorfismo de evaluación de un anillo de polinomios $A[x_1,\ldots,x_n]$ sustituyendo $x_i = \alpha_i$, p. 72.
$c(f)$	Contenido del polinomio f, p. 78.
$\mathbb{C}$	Conjunto de números complejos, p. 86.
$\mathrm{Re}\, z, \mathrm{Im}\, z$	Parte real e imaginaria de z resp., p. 86.
ζ_n	$= \mathrm{cis}(2\pi/n)$, raíz primitiva canónica n-ésima de la unidad, p. 88.
$\mathrm{Hom}_A(M,N)$	Espacio de morfismos de A-módulos desde M a N, p. 94.
$\det B$	Determinante de la matriz B, p. 111.
$\mathrm{adj}\, B$	Matriz adjunta de B, p. 112.
$\mathrm{tr}\, B$	$= \sum_{k=1}^n b_{kk}$, traza de una matriz, p. 115.
$\psi_B(x)$	$= \det(x \cdot I_n - B)$, polinomio característico de una matriz, p. 115.

$\operatorname{rang}(A)$	Rango de una matriz o de una transformación lineal, p. 117.
$[K : k]$	$= \dim_k(K)$, grado de la extensión K de k, p. 121.
$\operatorname{Gal}(K/k)$	Grupo de Galois de los k-automorfismos de K, p. 129.
$\operatorname{Frob}_k(a)$	$= a^p$, endomorfismo de Frobenius sobre un cuerpo k de característica $p \neq 0$, p. 134.
k^{alg}	La clausura algebraica de k, p. 149.
$\mathbb{A}$	$= \mathbb{Q}^{\mathrm{alg}}$, el cuerpo de números algebraicos, p. 149.
$\operatorname{Tr}_{K/k}(\alpha)$	$= \operatorname{tr}(m_\alpha)$, traza de $\alpha \in K$, p. 151.
$\operatorname{Nm}_{K/k}(\alpha)$	$= \det(m_\alpha)$, norma de $\alpha \in K$, p. 151.
$\psi_{\alpha,K/k}(t)$	$= \psi_{m_\alpha}(t) \in k[t]$, polinomio característico de $\alpha \in K$, p. 151.
$\operatorname{alt} f$	Altura de una función racional en $k(x)$, p. 166.
$A_{\mathfrak{p}}$	Localización del anillo A en su ideal primo $\mathfrak{p}$, p. 206.
$\operatorname{Supp}(M)$	Soporte de un A-módulo M, p. 209.
$\mathfrak{N}(A)$	Nilradical de A, p. 211.
$(S : T)$	$= \{a \in A : aT \subseteq S\}$, donde S, T son submódulos de un A-módulo M, p. 213.
$\operatorname{Ann}(T)$	$= (0 : T)$, p. 213.
$\mathfrak{a}^e$	$= \big(\varphi[\mathfrak{a}]\big)$, la extensión del ideal $\mathfrak{a}$, p. 214.
$\mathfrak{b}^c$	$= \varphi^{-1}[\mathfrak{b}]$, la contracción del ideal $\mathfrak{b}$, p. 214.
$\operatorname{As}_A(M)$	Ideales asociados al A-módulo M, p. 223.
$k.\dim A$	Dimensión de Krull de un anillo A, p. 234.
$\psi_A(x)$	$= \det(xI_n - A)$, el polinomio característico de A, p. 264.
Bil_A	Categoría de A-módulos de forma bilineal, p. 266.
$p_f(x), p_B(x)$	Polinomio característico de un endomorfismo o una matriz, p. 276.

$\sigma(f)$	Espectro de un endomorfismo lineal, o de una matriz cuadrada, p. 276.
B^*	$= \overline{B}^t$, p. 280.
$x \perp y$	x e y son ortogonales, p. 291.
$A^\perp$	Complemento ortogonal de A, p. 291.
$T(M)$	Álgebra tensorial sobre un A-módulo libre M, p. 307.
$E(M)$	Álgebra exterior sobre un A-módulo libre M, p. 311.
$[x, y, z]$	$= (xy)z - x(yz)$, el asociador de x, y, z, p. 321.
$\operatorname{alt} \mathfrak{a}$	Altura del ideal $\mathfrak{a}$, p. 335.
$A[[S]]$	Anillo de series formales de potencias con coeficientes en A e indeterminadas en S, p. 388.
$\operatorname{ord} f$	$= \operatorname{mín}\{m : a_m \neq 0\}$, orden de una serie formal de potencias, p. 388.
$\operatorname{gr}_{\mathfrak{a}}(A)$	$= \bigoplus_{n\in\mathbb{N}} \mathfrak{a}^n/\mathfrak{a}^{n+1}$, p. 402.
$\operatorname{gr}_{\mathcal{J}}(M)$	$= \bigoplus_{n\in\mathbb{N}} M_n/M_{n+1}$, p. 402.
$\operatorname{Poin}(M, t)$	$= \sum_{n\in\mathbb{N}} \lambda(M_n)t^n$, serie de Poincaré-Hilbert de un A-módulo graduado finitamente generado, p. 407.
$\chi_{\mathfrak{q}}^M$	Polinomio de Hilbert-Samuel, el polinomio tal que $\chi_{\mathfrak{q}}^M(n) = \ell(M/\mathfrak{q}^n M)$ para n suficientemente grande, p. 410.
$\Omega_{A/k}$	Módulo de diferenciales de Kähler de A sobre k, p. 420.
$k^{p^{-n}}, k^{p^{-\infty}}$	$= \{\alpha \in k^{\mathrm{alg}} : \alpha^{p^n} \in k\}$ y $= \bigcup_{n\in\mathbb{N}} k^{p^{-n}}$, resp., p. 428.

Bibliografía

Las fechas empleadas son aquellas de la primera publicación o del primer registro de Copyright.

Álgebra abstracta

1. Aluffi, P. *Algebra. Chapter 0* (American Mathematical Society, 1960).
2. Castillo, C. I. *Álgebra* `https://www.uv.es/ivorra/Libros/Al.pdf` (2020).
3. Chevalley, C. *The Construction and Study of Certain Important Algebras* (The Mathematical Society of Japan, 1955).
4. Chevalley, C. *Fundamental Concepts of Algebra* (Academic Press, 1956).
5. Fine, B. y Rosenberger, G. *The Fundamental Theorem of Algebra* (Springer-Verlag New York, 1997).
6. Jacobson, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
7. Lang, S. *Algebra* (Springer-Verlag New York, 2002).
8. Nagata, M. *Theory of Commutative Fields Translations in Mathematical Monographies* **125** (American Mathematical Society, 1967).
9. Prestel, A. *Lectures on Formally Real Fields Lecture Notes in Mathematics* **1093** (American Mathematical Society, 1975).
10. Rajwade, A. R. *Squares* (Cambridge University Press, 1993).
11. Rotman, J. J. *Advanced Modern Algebra* 3.ª ed. 2 vols. *Graduate Studies in Mathematics* 165, 180 (American Mathematical Society, 2015).

Álgebra lineal

12. CURTIS, M. L. *Abstract Linear Algebra* (Springer-Verlag New York Inc., 1990).

13. IBORT, A. y RODRÍGUEZ, M. A. *Notas de Álgebra Lineal* `http://mimosa.pntic.mec.es/jgomez53/matema/docums/ibort-algebra_lineal.pdf` (2014).

14. KATZNELSON, Y. y KATZNELSON, Y. R. *A (Terse) Introduction to Linear Algebra* (American Mathematical Society, 2008).

15. MILNOR, J. y HUSEMOLLER, D. *Symmetric Bilinear Forms* (Springer-Verlag Berlin Heidelberg, 1973).

Álgebra conmutativa

16. ATIYAH, M. F. y MCDONALD, I. G. *Introduction to Commutative Algebra* (Addison-Wesley, 1969).

17. EISENBUD, D. *Commutative Algebra with a View Toward Algebraic Geometry* (Springer Science+Business Media, 1994).

18. MATSUMURA, H. *Commutative Algebra* (W.A. Benjamin, Inc., 1969).

19. MATSUMURA, H. *Commutative Ring Theory* trad. por REID, M. *Cambridge Studies in Advanced Mathematics* **8** (Cambridge University Press, 1986).

20. MILNE, J. S. *A Primer of Commutative Algebra* `https://www.jmilne.org/math/xnotes/CA.pdf` (2020).

21. NAGATA, M. *Local Rings* (Interscience, 1962).

22. ZARISKI, O. y SAMUEL, P. *Commutative Algebra* 2 vols. (D. Van Nostrand, 1958).

Artículos

23. BANASCHEWSKI, B. A New Proof that "Krull implies Zorn". *Mathematical Logic Quarterly.* doi:`10.1002/malq.19940400405` (1994).

24. BLASS, A. Existence of Basis implies the Axiom of Choice. *Contemporary Mathematics* **31.** `http://www.math.lsa.umich.edu/~ablass/bases-AC.pdf` (1984).

25. CONRAD, K. Infinite-dimensional Dual Spaces. https://kconrad.math.uconn.edu/blurbs/linmultialg/dualspaceinfinite.pdf (2018).

26. CONRAD, K. Simplicity of A_n. https://kconrad.math.uconn.edu/blurbs/grouptheory/Ansimple.pdf (2018).

27. CONRAD, K. The Sylow Theorems. https://kconrad.math.uconn.edu/blurbs/grouptheory/sylowpf.pdf (2018).

28. CONRAD, K. Zorn's Lemma and some applications. https://kconrad.math.uconn.edu/blurbs/zorn1.pdf (2018).

29. DERKSEN, H. The Fundamental Theorem of Algebra and Linear Algebra. *The American Mathematical Monthly.* doi:10.2307/3647746 (2003).

Documentos históricos

30. 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.

31. 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.

32. ABEL, N. H. Mémoire sur une classe particulière d'équations résolubles algébriquement. *Journal für die reine und angewandte Mathematik.* doi:10.1515/crll.1829.4.131 (1829).

33. ARTIN, E., NESBITT, C. J. y THRALL, R. M. *Rings with minimum condition* (University of Michigan Press, 1946).

34. BOURBAKI, N. *Éléments de Mathématique.* 2.1: *Algèbre. Chapitres 1-3* (Hermann, 1942).

35. CHEVALLEY, C. On the Theory of Local Rings. *Annals of Mathematics.* doi:10.2307/1969105 (1944).

36. DEDEKIND, R. Sur la théorie des nombres entiers algébriques. *Bulletin des Sciences Mathématiques et Astronomiques.* doi:10.1007/978-3-322-98606-1_3 (1876).

37. DIRICHLET, P. G. L. *Vorlesungen über Zahlentheorie* (ed. DEDEKIND, R.) (Braunschweig, 1863).

38. 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.

39. 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.

40. 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).

41. GRELL, H. Beziehungen zwischen den Idealen verschiedener Ringe. *Mathematische Annalen.* doi:`10.1007/BF01447879` (1927).

42. HILBERT, D. Ueber die Theorie der algebraischen Formen. *Mathematische Annalen.* doi:`10.1007/BF01208503` (1890).

43. HILBERT, D. Ueber die vollen Invariantensysteme. *Mathematische Annalen.* doi:`10.1007/978-3-642-52012-9_19` (1893).

44. KRONECKER, L. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die reine und angewandte Mathematik.* doi:`10.1515/crll.1882.92.1` (1882).

45. KRULL, W. Dimensionstheorie in Stellenringen. *Journal für die reine und angewandte Mathematik.* doi:`10.1515/crll.1938.179.204` (1938).

46. KUMMER, E. E. *De Numeris Complexis, Qui Radicibus Unitatis Et Numeris Integris Realibus Constant* (Kessinger Publishing, 1844).

47. 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).

48. NOETHER, E. Idealtheorie in Ringbereichen. *Mathematische Annalen.* doi:`10.1007/978-3-642-39990-9_19` (1921).

49. WHITNEY, H. Tensor products of abelian groups. *Duke Mathematical Journal.* doi:`10.1215/S0012-7094-38-00442-9` (1938).

Historia

50. EDWARDS, H. M. The Genesis of Ideal Theory. *Archive for History of Exact Sciences.* doi:`10.1007/bf00327914` (1980).

51. GROTHENDIECK, A. *Cosechas y Siembras* trad. por NAVARRO, J. A. http://matematicas.unex.es/~navarro/res/ (1986).

52. KIERNAN, B. M. The development of Galois theory from Lagrange to Artin. *Archive for History of Exact Sciences*. doi:10.1007/BF00327219 (1971).

53. KLINE, M. *Mathematical Thought from Ancient to Modern Times* 3 vols. (Oxford University Press, 1972).

Libros de autoría propia

54. CUEVAS, J. *Geometría algebraica* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/geo-alg/geometria-algebraica.pdf (2022).

55. CUEVAS, J. *Teoría de categorías y álgebra homológica* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/cats/teoria-categorias.pdf (2022).

56. CUEVAS, J. *Teoría de Conjuntos* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/conjuntos/conjuntos.pdf (2022).

57. CUEVAS, J. *Teoría de Números* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/teo-numeros/main.pdf (2022).

58. 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