

# Álgebra

José Cuevas Barrientos

30 de mayo de 2024



---

## Índice general

---

	INTRODUCCIÓN . . . . .	VII
<b>I</b>	<b>Álgebra Abstracta Elemental</b>	<b>1</b>
1	TEORÍA DE GRUPOS . . . . .	3
	1.1 Estructuras algebraicas . . . . .	3
	1.2 Ejemplos de grupos . . . . .	12
	1.2.1 Grupos simétrico y alternante . . . . .	12
	1.2.2 Grupo diedral . . . . .	16
	1.3 Representaciones de grupos finitos . . . . .	17
	1.3.1 Teoremas de isomorfismos . . . . .	17
	1.3.2 Productos directos y semidirectos de grupos . . . . .	24
	1.4 Teoremas de Sylow . . . . .	27
	1.4.1 Acciones y producto semidirecto . . . . .	27
	1.4.2 Teoremas de Sylow . . . . .	33
	1.5 Otros tópicos de grupos . . . . .	38
	1.5.1 Grupos libres y presentación . . . . .	38
	1.5.2 Grupos solubles . . . . .	42
2	ANILLOS Y CUERPOS . . . . .	51
	2.1 Definiciones elementales . . . . .	51
	2.1.1 Teorema del binomio . . . . .	59
	2.1.2 Característica . . . . .	60
	2.2 Divisibilidad en anillos . . . . .	61
	2.3 Polinomios . . . . .	70
	2.4 Divisibilidad de polinomios . . . . .	80
	2.4.1 Raíces básicas . . . . .	87

2.5	Números complejos . . . . .	87
2.5.1	El teorema fundamental del álgebra I . . . . .	90
3	MÓDULOS Y VECTORES . . . . .	95
3.1	Módulos . . . . .	95
3.2	Módulos libres y bases . . . . .	100
3.2.1	Finitamente generados . . . . .	100
3.2.2	Espacios de dimensión infinita . . . . .	103
3.2.3	Fórmulas con la dimensión . . . . .	105
3.3	Matrices y transformaciones lineales . . . . .	106
3.4	Determinante . . . . .	111
3.4.1	Invariantes: traza y polinomio característico . . . . .	116
3.4.2	Rango de matrices . . . . .	118
3.5	Los grupos de matrices . . . . .	120
<b>II</b>	<b>Teoría de Anillos y Módulos</b>	<b>123</b>
4	EXTENSIONES DE CUERPO . . . . .	125
4.1	Extensiones algebraicas . . . . .	125
4.2	Extensiones normales y separables . . . . .	134
4.2.1	Cuerpos de escisión . . . . .	134
4.2.2	Extensiones separables . . . . .	137
4.3	Teoría y extensiones de Galois . . . . .	140
4.4	Cuerpos algebraicamente cerrados . . . . .	150
4.4.1	Aplicación: El teorema fundamental del álgebra II . . . . .	155
4.5	Otras aplicaciones . . . . .	156
4.5.1	Norma y traza . . . . .	156
4.5.2	Raíces de la unidad y extensiones ciclotómicas . . . . .	158
4.5.3	La insolubilidad de la quintica . . . . .	163
4.6	Trascendencia . . . . .	167
4.6.1	Grado de trascendencia . . . . .	167
4.6.2	Teorema de Lüroth . . . . .	171
5	MÓDULOS, OTRA VEZ . . . . .	177
5.1	La categoría de módulos . . . . .	177
5.2	Cadenas de submódulos . . . . .	186
5.2.1	Módulos noetherianos y artinianos . . . . .	186
5.2.2	Módulos (semi)simples y el teorema de Jordan-Hölder . . . . .	187
5.3	Productos tensoriales . . . . .	195
5.4	Módulos proyectivos e inyectivos . . . . .	203
5.5	Módulos sobre DIPs . . . . .	210

6	INTRODUCCIÓN AL ÁLGEBRA CONMUTATIVA . . . . .	217
	6.1 Anillos locales y radicales . . . . .	217
	6.1.1 Localización . . . . .	217
	6.1.2 Radicales . . . . .	224
	6.1.3 Extensión y contracción de ideales . . . . .	228
	6.1.4 El lema de Nakayama y sus consecuencias . . . . .	230
	6.2 Ideales asociados y descomposición primaria . . . . .	235
	6.3 Módulos noetherianos y artinianos, de nuevo . . . . .	242
7	CUERPOS FORMALMENTE REALES Y CUADRADOS . . . . .	253
	7.1 Cuerpos formalmente reales . . . . .	253
	7.2 Teoremas de Pfister . . . . .	262
	7.2.1 Calculando el nivel . . . . .	269
8	ÁLGEBRA LINEAL AVANZADA . . . . .	273
	8.1 Grupos abelianos libres, y de torsión . . . . .	273
	8.2 Formas canónicas . . . . .	279
	8.3 Formas bilineales . . . . .	281
	8.3.1 Módulos libres de forma bilineal . . . . .	282
	8.3.2 El teorema de Witt . . . . .	286
	8.3.3 El anillo de Witt . . . . .	287
9	TEORÍA ESPECTRAL . . . . .	291
	9.1 Diagonalización . . . . .	291
	9.1.1 El teorema fundamental del álgebra II . . . . .	296
	9.1.2 Teorema de Cayley-Hamilton . . . . .	298
	9.2 Espacios duales . . . . .	299
	9.3 Formas bilineales . . . . .	301
	9.3.1 Formas bilineales . . . . .	301
	9.3.2 Formas sesquilineales, producto interno y “geometría euclídea” . . . . .	304
	9.3.3 Formas hermitianas y espacios de producto interno . . . . .	305
	9.3.4 Formas cuadráticas . . . . .	311
10	ÁLGEBRAS . . . . .	313
	10.1 Definiciones elementales . . . . .	313
	10.2 Álgebras asociativas . . . . .	319
	10.2.1 Anillos, módulos y álgebras graduadas . . . . .	319
	10.2.2 Productos tensoriales y ejemplos de álgebras . . . . .	324
	10.2.3 Álgebra exterior y determinantes . . . . .	329
	10.2.4 Representaciones . . . . .	334

*10.3 El problema de Hurwitz . . . . .	335
10.3.1 El problema aritmético de Hurwitz . . . . .	335
10.3.2 Álgebras de composición y su clasificación . . . . .	338
10.3.3 Aplicación: álgebras de división . . . . .	345
10.4 Introducción a las álgebras centrales simples . . . . .	348
10.5 Álgebras cuaterniónicas II . . . . .	353
10.5.1 Allegro: interpretación geométrica . . . . .	357
10.5.2 Álgebras bicuaterniónicas . . . . .	360
<b>III Métodos (co)homológicos y Álgebra no conmutativa</b>	
<b>361</b>	
11 (Co)HOMOLOGÍA DE MÓDULOS . . . . .	363
11.1 La categoría de módulos . . . . .	363
11.1.1 Módulos proyectivos . . . . .	365
11.1.2 Módulos inyectivos . . . . .	369
11.1.3 Módulos y anillos (semi)simples . . . . .	372
11.2 Extensiones y el funtor Ext . . . . .	377
11.3 Tensores y el funtor Tor . . . . .	388
11.3.1 Tensores (caso no conmutativo) . . . . .	388
11.3.2 El teorema de Eilenberg-Watts y equivalencia de Morita	391
11.3.3 El funtor Tor . . . . .	399
11.3.4 El teorema de coeficientes universales . . . . .	403
12 COHOMOLOGÍA Y REPRESENTACIONES DE GRUPOS . . . . .	415
12.1 Cohomología de grupos . . . . .	415
12.1.1 Interpretación del $H^1$ . . . . .	419
12.1.2 (Co)homología entre subgrupos . . . . .	420
12.1.3 Cohomología modificada de Tate . . . . .	423
13 GRUPOS TOPOLÓGICOS Y PROFINITOS . . . . .	429
13.1 Grupos topológicos . . . . .	429
*13.2 Uniformidades y métricas . . . . .	437
13.3 Dualidad de Pontryagin-van Kampen . . . . .	439
13.4 Grupos profinitos . . . . .	440
13.4.1 Teoría de Galois infinita . . . . .	448
13.5 Cohomología de Galois . . . . .	453
ÍNDICE ALFABÉTICO . . . . .	457

---

## 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,  $\pi$  o  $\sqrt{2}$ . ¿Y qué hay de  $\emptyset$ ? No, ésto es un conjunto. Sin embargo, von Neumann propone construir el conjunto de los naturales usando al conjunto vacío  $\emptyset$  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  $\{\text{cero},$

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



## Escritura técnica

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

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



Parte I.

---

# ÁLGEBRA ABSTRACTA ELEMENTAL

---

En el álgebra suelen haber tres clases de *categorías* predominantes: las de los grupos, las de los anillos y las de los módulos.<sup>1</sup> En esto, éste texto pretende dar un vistazo relativamente clásico a la teoría, aunque también pasando por un par de enunciados de cierta novedad.

---

<sup>1</sup>Tradicionalmente también se incluía las categorías de los retículos y las álgebras booleanas. Hoy, por convenio, se suelen agrupar con tópicos de *lógica matemática* como la teoría de conjuntos.



# 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:** Una función  $\cdot : G^2 \rightarrow G$  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.

Se dice que un grupo es *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*.
- $(\mathbb{Z}, +)$ ,  $(C_n := \mathbb{Z}/n\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$  y  $(\mathbb{R}, +)$ .
- $(\mathbb{Q}_{\neq 0}, \cdot)$  y  $(\mathbb{R}_{\neq 0}, \cdot)$ .
- Si  $p$  es primo, entonces  $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \cdot)$ .
- Si  $X \neq \emptyset$ , entonces el conjunto de las biyecciones de  $X$  con la composición  $(\text{Sym}(X), \circ)$  es un grupo.

De estos, 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  $\Sigma$  en lugar de  $\Pi$ .

**Proposición 1.4 (asociatividad generalizada):** Si  $g_1, \dots, g_n \in G$  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 demuestra 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:** Sea  $G$  un grupo. Se dice que  $S \subseteq G$  es subgrupo si  $(S, \cdot \upharpoonright S^2)$  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:** Sea  $G$  un grupo y  $S \subseteq G$  un subconjunto. Se satisface que  $S \leq G$  syss es  $S$  no es vacío y para todo  $x, y \in S$  se cumple que  $xy^{-1} \in S$ .

**Corolario 1.7.1:** La intersección arbitraria de subgrupos es un subgrupo. Además nunca es vacía pues 1 siempre pertenece a la intersección de subgrupos.

**Definición 1.8:** 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  $S = \{x_1, \dots, x_n\}$  denotaremos  $\langle x_1, \dots, x_n \rangle := \langle S \rangle$ .

**Corolario 1.8.1:** Sea  $G$  un grupo y  $S \subseteq G$ . El conjunto  $S$  es un subgrupo syss  $\langle S \rangle = S$ .

**Proposición 1.9:** 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 1.10:** 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 pérdida 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  $b \in A$ .  $\square$



**Proposición 1.11:** Si  $\{H_i : i \in I\}$  es una  $\subseteq$ -cadena<sup>1</sup> 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.  $\square$

**Definición 1.12:** 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 un **sistema generador** si  $\langle B \rangle = G$ . Un grupo  $G$  se dice **finitamente generado** si posee un sistema generador finito. Un grupo se dice **cíclico** si posee un sistema generador de un solo elemento. Se define el orden de un elemento  $x$ , denotado por  $\text{ord } x$ , 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 1.12.1:** Se cumplen:

1. Los grupos cíclicos son abelianos.
2. Todo subgrupo de un grupo cíclico es también cíclico.
3. Si  $\text{ord } x \neq 0$ , entonces  $\text{ord } x = |\langle x \rangle|$ .

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

•  $(C_n, +)$  es un grupo cíclico, cuyo generador es el 1 y de orden  $n$ .

**Ejemplo** Un grupo que no es finitamente generado. Considere el grupo  $(\mathbb{Q}, +)$  y veamos que no es finitamente generado. Sea  $H \subseteq \mathbb{Q}$  finito,

<sup>1</sup>Es decir, tal que para todo  $i, j \in I$  se cumple que  $H_i \subseteq H_j$  o  $H_j \subseteq H_i$ .

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

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

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 esto es absurdo por construcción.

**Proposición 1.13:** Dado  $a \in G$  y  $n \in \mathbb{Z}_{\neq 0}$ , se cumple que

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

**Proposición 1.14:** Si  $a, b \in G$  conmutan, entonces

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

**Proposición 1.15:** 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

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

**Teorema (AE) 1.16:** Si  $G$  es finitamente generado, entonces todo subgrupo propio está contenido en un subgrupo maximal.

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

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

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

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

entonces  $\mathcal{F}$  es un conjunto parcialmente ordenado por la inclusión, y toda cadena tiene supremo por la proposición anterior (1.11), 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.  $\square$

**Definición 1.17:** Decimos que una aplicación  $\varphi: (G, \cdot) \rightarrow (H, \star)$  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  $G \cong H$ .

Si  $\varphi: G \rightarrow G$  se le añade el prefijo *endo-* y si además resulta ser biyectiva, entonces se le añade el prefijo *auto-*.

Visualmente denotamos los monomorfismos por  $\hookrightarrow$ , los epimorfismos por  $\twoheadrightarrow$  y los isomorfismos por  $\xrightarrow{\sim}$ .

Se le llama el **núcleo**<sup>2</sup> de un homomorfismo  $\varphi: G \rightarrow H$  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 inyectivo pero no sobreyectivo, pues 1 no tendría preimagen.

**Proposición 1.18:** Si  $\varphi: G \rightarrow H$  es un isomorfismo, entonces:

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

**Teorema 1.19:** Sea  $G = \langle g \rangle$ , entonces:

1. Si es finito y  $|G| = m$ , entonces  $G = \{1, g, g^2, \dots, g^{m-1}\}$  y  $g^n = e$  syss  $m \mid n$ .

---

<sup>2</sup>De. *kernel*, fr. *noyau*.

2. Si  $G$  es infinito, entonces  $(G, \cdot) \cong (\mathbb{Z}, +)$ .
3. Si  $G$  es finito, entonces  $G \cong C_m$ .

**Definición 1.20:** Dados dos subconjuntos  $A, B$  de un grupo  $G$ , se define

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

Si alguno es un conjunto de un solo elemento  $A = \{a\}$ , omitiremos las llaves, de modo que  $aB := \{a\} \cdot B$  y  $Ab := A \cdot \{b\}$ . Cuando uno consta de un solo elemento y el otro es un subgrupo, usualmente se les llaman **clases laterales**.

**Lema 1.21.A:** Sea  $H \leq G$  un subgrupo de  $G$  y  $a, b \in G$ , entonces

1.  $a \in aH$ .
2.  $aH = bH$  o  $aH \cap bH = \emptyset$ .
3.  $a \equiv b$  (mód  $H_-$ ) dado por  $a^{-1}b \in H$  y  $a \equiv b$  (mód  $H_+$ ) 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.  $\square$

**Definición 1.21:** Sea  $G$  un grupo y  $H \leq G$  un 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), llamado el **índice** de  $H$  en  $G$ .

**Teorema 1.22 – Teorema de Lagrange:** Sea  $H \leq G$  un subgrupo de un grupo  $G$  finito, entonces

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

**Corolario 1.22.1:** El orden de todo elemento de un grupo finito es un divisor de su cardinal.

**Corolario 1.22.2:** Todo grupo de cardinal  $p$  primo es cíclico y, en consecuencia, isomorfo a  $C_p$ .

**Definición 1.23:** Denotamos por  $U_n := (\mathbb{Z}/n\mathbb{Z})^\times$  (léase «grupo multiplicativo» o «unidades de  $n$ ») al conjunto de todos los elementos coprimos a  $n$  de  $\mathbb{Z}/n\mathbb{Z}$ . Queda al lector demostrar que  $(U_n, \cdot)$  es un grupo abeliano de neutro 1.

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

$$\phi(n) := |U_n| = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Así, como corolario al teorema de Lagrange tenemos lo siguiente:

**Teorema 1.24 (Euler-Fermat):** Si  $a$  coprimo a  $n$ , entonces

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

**Corolario 1.24.1 (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 1.25 – Teorema chino del resto:** Si  $(n, m) = 1$ , entonces

$$C_n \times C_m \cong C_{nm},$$

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

$$f(a, b) \equiv f(c, d)$$

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

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.  $\square$

**Corolario 1.25.1:** Si  $(n; m) = 1$ , entonces

$$U_n \times U_m \cong U_{nm},$$

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

**Proposición 1.26:** 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  $(\text{Func}(S), \circ)$  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  $\text{Sym}(S)$ .

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

**Proposición 1.27:** 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 1.28 – Teorema de Cayley:** Para todo grupo finito  $G$  de cardinal  $n$  se cumple que

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

DEMOSTRACIÓN: Vamos a definir  $\varphi_a : G \rightarrow G$  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.  $\square$

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 1.29:** Dado  $\sigma \in \text{Sym}(S)$  y  $a \in S$ , diremos que la **órbita** de  $a$  es la tupla ordenada

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

En particular, como  $\text{Sym}(S)$  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

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

se denotará como  $(2, 3, 5)$ ,  $(3, 5, 2)$  o  $(5, 2, 3)$ . Los ciclos de orden 2 se denominarán **trasposiciones**.

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



Nótese que los ciclos están ordenados, no es lo mismo  $(2, 3, 5)$  que  $(5, 3, 2)$ .

**Teorema 1.30:** Se cumplen:

1. El orden de los ciclos es el cardinal de su órbita no trivial.
2. La inversa de un ciclo  $(a_1, a_2, \dots, a_{n-1}, a_n)$  es  $(a_n, a_{n-1}, \dots, a_2, a_1)$ .

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  $(a_1, \dots, a_n)$  es un ciclo, entonces

$$\sigma^{-1}(a_1, \dots, a_n)\sigma = (\sigma(a_1), \dots, \sigma(a_n)).$$

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

$$(a_1, a_2, \dots, a_n) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_n). \quad \square$$

### Signo de una permutación.

**Lema 1.31:** 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  $n$ .  $\square$

**Definición 1.32:** Si una permutación  $\sigma$  se puede escribir como un producto de  $n$  trasposiciones, entonces  $\text{sgn } \sigma := (-1)^n$ . 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 1.33:** Se cumple que  $\text{sgn} : S_n \rightarrow (\{\pm 1\}, \cdot)$  es un homomorfismo, es decir,  $\text{sgn}(\sigma\tau) = \text{sgn } \sigma \cdot \text{sgn } \tau$ .

**Corolario 1.33.1:** El signo se conserva entre inversas y conjugados.

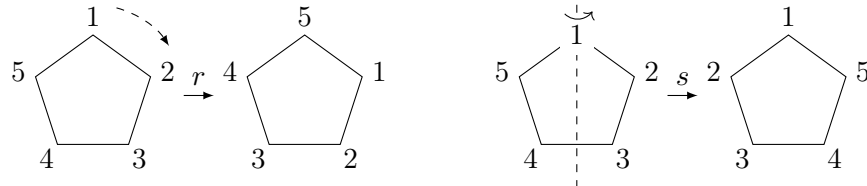
Como vimos, el signo es un morfismo de grupos, esto es importante porque significa que el kernel del signo, es decir el conjunto de permutaciones pares, es un subgrupo normal del simétrico. Luego denotamos

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

**Proposición 1.34:** 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 1.35:** Fijado un  $n > 2$ , se definen  $r := (1, 2, \dots, n)$  (el

cual se identifica con una *rotación*) y

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

(el cual se identifica con una *reflexión*). Luego  $D_{2n} := \langle r, s \rangle$  se denomina el **grupo diedral** (o *diédrico*) de orden  $2n$ .

**Proposición 1.36:** Para todo grupo diedral se cumple:

1. En  $D_{2n}$  se cumple que  $\text{ord } r = n$  y  $\text{ord } s = 2$ .
2.  $rs = sr^{-1}$  y más generalmente  $r^k s = sr^{-k}$ . Esto equivale a que  $srs^{-1} = r^{-1}$  y que  $\text{ord}(r^k s) = 2$ .
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 1.37:** 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  $N \subseteq xNx^{-1}$ .  $\square$

**Definición 1.38:** 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  $N \trianglelefteq G$ , si para todo  $x \in G$  se cumple que  $xN = Nx$ .

**Proposición 1.39:** Si  $\varphi: G \rightarrow H$  es un homomorfismo, entonces

$$\ker \varphi \trianglelefteq G.$$

**Teorema 1.40:** 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  $\pi: G \rightarrow G/N$  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  $\pi$  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  $x \in \ker \pi$ .  $\square$

**Proposición 1.41:** Un homomorfismo de grupos  $\varphi: G \rightarrow H$  es inyectivo si  $\ker \varphi = \{1\}$ .

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  $x = y$ .  $\square$

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

**Definición 1.42:** 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**  $N_G(S)$  de un conjunto  $S$  a los elementos que fijan al conjunto bajo

conjugación, i.e.,

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

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

**Proposición 1.43:** Se cumple:

1.  $N \trianglelefteq G$  syss  $N_G(N) = G$  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  $Z(S) \leq N_G(S) \leq G$ .
6. Si  $H \leq G$  entonces  $H \trianglelefteq N_G(H) \leq G$ . Más aún si  $N \leq G$  es tal que  $H \trianglelefteq N$ , entonces  $N \subseteq N_G(H)$ .
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 1.44:** 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  $xN = G \setminus N = Nx$ .  $\square$

**Proposición 1.45:** Se cumple:

1. Para todo  $S \subseteq G$  se cumple que  $|C_G(S)| = [G : N_G(S)]$ .
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  $b^k = c^{-1}a^k c$ , por lo que si  $n := \text{ord } a$ , entonces  $b^n = c^{-1}a^n c = c^{-1}ec = e$ . Por lo que  $\text{ord } b \leq \text{ord } a$ . Pero notemos que  $a = (c^{-1})^{-1}bc^{-1}$ , por lo que  $\text{ord } a \leq \text{ord } b$ . En conclusión,  $\text{ord } a = \text{ord } b$ .  $\square$

**Proposición 1.46:** 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  $Z(D_{2n}) = \langle r^{n/2} \rangle$  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.  $\square$

**Teorema 1.47 – Primer teorema de isomorfismos:** Sea  $\varphi: G \rightarrow H$  un morfismo de grupos con  $N := \ker \varphi \trianglelefteq G$ , entonces  $\bar{\varphi}: G/N \rightarrow \text{Img } \varphi$  dado por  $\bar{\varphi}(x) := \varphi(xN)$  resulta ser un isomorfismo.

En figura de diagrama conmutativo:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \pi \downarrow & & \uparrow \iota \\ G/\ker \varphi & \xrightarrow[\bar{\varphi}]{\sim} & \text{Img } \varphi \end{array}$$

**Corolario 1.47.1:** Si  $\varphi: G \rightarrow H$  es epimorfismo, entonces  $G/\ker \varphi \cong H$ .

**Teorema 1.48 – 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  $\varphi : H \rightarrow HK/K$  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  $\varphi$ . 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.  $\square$

**Teorema 1.49 – Tercer teorema de isomorfismos:** Sean  $K \leq H \leq G$  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  $\varphi : G \rightarrow (G/K)/(H/K)$  dado por  $\varphi(g) := (gK)(H/K)$  es un epimorfismo de grupos, donde el  $x \in G$  pertenece al kernel si  $gK \in H/K$ , i.e,  $g \in H$ .  $\square$

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

**Definición 1.50 (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  $\text{Im} \varphi_i = \ker \varphi_{i+1}$  para todo  $i \in \mathbb{Z}$  (para el cuál estén definidos). Una sucesión exacta se dice **corta** si es finita.

**Proposición 1.51:** Se cumple:

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

3. Si  $H \trianglelefteq G$ , entonces

$$H \xhookrightarrow{\iota} G \xrightarrow{\pi} G/H$$

es una sucesión exacta corta.

4. Dados  $f: H \rightarrow G$  y  $g: G \rightarrow J$  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

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

conmuta.

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

**Teorema 1.52:** Sean,  $H, K \leq G$  finito, entonces

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

DEMOSTRACIÓN: Sea  $f: H \times K \rightarrow HK$  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

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

**Proposición 1.53:** 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:

$$\begin{array}{ccccc} & & \pi_1 & & \\ & \searrow & & \searrow & \\ G_1 \times G_2 & \longrightarrow & G_1 & \twoheadrightarrow & \frac{G_1}{H_1} \end{array}$$

y análogamente con  $\pi_2 : G_1 \times G_2 \rightarrow G_2/H_2$ . 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.  $\square$

**Teorema 1.54 – Teorema de la correspondencia:** Si  $\varphi : G \twoheadrightarrow H$ , entonces

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

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

1.  $\Phi$  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)  $\Phi$  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)  $\Phi$  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  $\Phi$  es biyectiva, podemos usar  $\Phi^{-1}$  para probar el converso.  $\square$

### §1.3.2 Productos directos y semidirectos de grupos.

**Teorema 1.55:** 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.  $\implies$ . 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.  
 $\Leftarrow$ . 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 pérdida 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  $x^{-1}h k x = (x^{-1}h x)(x^{-1}k x)$ .  $\square$

**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 1.56:** Sea  $G$  un grupo. Dados  $x, y \in G$ , definamos su **conmutador** como  $[x, y] := x^{-1}y^{-1}xy \in G$ , el cual satisface que  $xy = yx[x, y]$ .

**Corolario 1.56.1:** Dados dos elementos  $x, y$  de un grupo  $G$ , se cumple que  $xy = yx$  si y sólo si  $[x, y] = 1$ .

**Proposición 1.57:** 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.  $\square$

**Definición 1.58:** 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 1.59:** 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  $\alpha: K \rightarrow G$  y  $\beta: K \rightarrow H$  son homomorfismos de grupos, entonces la diagonal  $\gamma := (\alpha, \beta): K \rightarrow G \times H$  es el único homomorfismo de grupos que hace que el siguiente diagrama:

$$\begin{array}{ccc}
 & \xrightarrow{\alpha} & G \\
 K & \xrightarrow{\exists! \gamma} G \times H & \nearrow \pi_1 \\
 & \searrow \pi_2 & \\
 & \xrightarrow{\beta} & H
 \end{array}$$

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.

**Proposición 1.60:** 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  $\varphi : H \times K \rightarrow G$  dado por  $\varphi(h, k) := hk$  es un isomorfismo.

**Proposición 1.61:** El producto directo de dos grupos abelianos es abeliano.

**Teorema 1.62 – Teorema fundamental de los grupos abelianos:** Si  $G$  es abeliano finitamente generado, entonces existen primos  $p_1, \dots, p_n$  (posiblemente iguales) y naturales no nulos  $\alpha_1, \dots, \alpha_n, \beta$  tales que

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

En particular, se cumple para grupos abelianos finitos.

DEMOSTRACIÓN: Sea  $\langle g_1, \dots, g_k \rangle$  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  $N_i \cong C_m$ . Podemos agrupar todos los  $\mathbb{Z}$ s que encontremos, y si  $N_i \cong C_m$  entonces  $m = q_1^{\gamma_1} \cdots q_j^{\gamma_j}$  donde los  $q_i$ 's son primos distintos y los  $\gamma_i$ s son naturales no nulos, luego por teorema chino del resto:

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

Finalmente agrupando todo nos da el enunciado.  $\square$

**Corolario 1.62.1:** Todo grupo abeliano posee subgrupos de todos los divisores de su cardinal.

Veamos dos aplicaciones de esto:

**Proposición 1.63:** Todo grupo de cardinalidad 4 es o bien  $C_4$  o bien  $K_4 := C_2 \times C_2$ . 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  $C_4$ . Si todos tienen orden 2, entonces el grupo es abeliano (por la proposición 1.15) y, por ende, se escribe como producto de grupos cíclicos y luego es fácil ver que es  $K_4$ .  $\square$

**Proposición 1.64:** Todo grupo de cardinalidad 6 es  $C_6$  (si es abeliano) o  $D_6$  (si no lo es). En consecuencia,  $S_3 \cong D_6$ .

DEMOSTRACIÓN: Nuevamente por Lagrange cada elemento puede tener orden 1, 2, 3 o 6. Si es abeliano luego es  $C_2 \times C_3$  o  $C_6$ , pero por el teorema chino del resto  $C_2 \times C_3 \cong C_6$ .

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,  $xy = y^2x$  y  $xyx = y^{-1}$ . Pero entonces  $\varphi: G \rightarrow D_6$  dado por  $\varphi(x) = s$  y  $\varphi(y) = r$  demuestra ser isomorfismo.  $\square$

## 1.4 Teoremas de Sylow

### §1.4.1 Acciones y producto semidirecto.

**Definición 1.65:** Una **acción derecha** de un grupo  $G$  sobre un conjunto  $S$  no vacío arbitrario es un homomorfismo  $\alpha: G \rightarrow \text{Sym}(S)$ , y denotaremos a un grupo con acción como  $\alpha: G \curvearrowright S$ . Es decir, cada  $\alpha_g$  con  $g \in G$  es una permutación de  $S$ , y éstas cumplen que

$$\forall g, h \in G \quad \alpha_{gh} = \alpha_g \circ \alpha_h, \quad \alpha_{g^{-1}} = \alpha_g^{-1}.$$

Para  $x \in S$  denotaremos ocasionalmente  $x^g := \alpha_g(x)$  (*notación exponencial*) o  $x \cdot g := \alpha_g(x)$  (*notación multiplicativa*); la condición anterior se traduce en que para todo  $x \in S$  y todo  $g, h \in G$  se cumpla que

$$x^1 = x, \quad (x^g)^h = x^{gh}. \quad (1.1)$$

El núcleo de la acción es  $\ker \alpha := \{g \in G : \alpha_g = \text{Id}_S\}$ ; vale decir,  $g \in \ker \alpha$  si y sólo si  $x^g = x$  para todo  $x \in S$ . Diremos que una acción es **fiel** si  $\alpha$  es inyectiva, lo que equivale a ver que  $\ker \alpha = \{1\}$ .

Dada una acción  $\alpha: G \curvearrowright S$ , entonces definimos los siguientes con-

juntos:

$$\text{Orb}_a := \{a^g : g \in G\}, \quad \text{Stab}_a := \{g \in G : a^g = a\}$$

a los que llamamos **órbita** y **estabilizador** de  $a$  resp. Diremos que una acción es **transitiva** si para todo  $a \in S$  se cumple que  $\text{Orb}_a = S$ .

Si en lugar de las condiciones 1.1, exigimos que

$$1 \cdot x = x, \quad g \cdot (h \cdot x) = gh \cdot x,$$

obtenemos la definición de una *acción izquierda* que suele ser más común en otros textos.

**Ejemplo.** Son acciones:

- Para todo conjunto  $S$  y grupo  $G$ , tenemos la **acción trivial**  $\alpha: G \curvearrowright S$  dada por  $x^g := x$ . Nótese que, a menos que  $G = 1$ , no es fiel y que las órbitas de cada elemento son el mismo punto.
- Un grupo  $G$  actúa sobre sí mismo  $\mu: G \curvearrowright G$  mediante  $\mu_g(x) := x \cdot g$ , llamada la **acción por traslación** o *por multiplicación derecha*. Ésta acción es fiel y transitiva, y de hecho, ésta es la que se emplea para probar el teorema de Cayley.
- Un grupo  $G$  actúa sobre sí mismo  $\kappa: G \curvearrowright G$  mediante  $x^g := g^{-1}xg$ , llamada la **acción por conjugación**. Se cumple que  $\ker \alpha = Z(G)$ .
- Dado un conjunto  $S$  no vacío, el homomorfismo de grupos  $\text{Id}: \text{Sym}(S) \rightarrow \text{Sym}(S)$  induce la acción  $\text{Sym } S \curvearrowright S$  dada por  $x^\sigma := \sigma(x)$ , la cual es una acción fiel y transitiva.

**Ejemplo 1.66:** Dado un grupo  $G$ , el grupo cíclico actúa sobre él  $\epsilon: C_2 \curvearrowright G$ , donde si escribimos a  $C_2 = (\{1, -1\}, \cdot)$  en notación multiplicativa, tenemos que  $\epsilon_1(x) = x$  y  $\epsilon_{-1}(x) = x^{-1}$ . Nótese que  $\epsilon$  no es fiel syss todo elemento  $g \in G \setminus \{1\}$  tiene orden 2.  $\lrcorner$

**Lema 1.67.A:** Sean  $N, A$  un par de grupos y sea  $\alpha: H \rightarrow \text{Aut}_{\text{Grp}}(N)$  un homomorfismo de grupos, donde veremos al último como una acción. Entonces el conjunto  $G := N \times A$  con la operación  $\cdot$  definida por

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

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

**Definición 1.67:** Sean  $N, A$  un par de grupos con un homomorfismo de grupos  $\alpha: A \rightarrow \text{Aut}_{\text{Grp}}(N)$ . Llamamos al grupo construido en el lema anterior como el **producto semidirecto** de  $N, A$  y le denotamos por  $N \rtimes_{\alpha} A$ .

**Proposición 1.68:** Si  $N, H$  son grupos y  $\alpha: H \curvearrowright N$  es la acción trivial, entonces  $N \rtimes_{\alpha} A = N \times A$ .

En consecuencia, el producto directo es un caso particular del producto semidirecto.

La acción descrita ahora en el ejemplo 1.66 induce un producto semidirecto bastante interesante:

**Ejercicio 1.69:** Sea  $n > 2$  y considere la acción  $\epsilon: C_2 \curvearrowright C_n$  del ejemplo 1.66. Entonces  $C_n \rtimes_{\epsilon} C_2 \cong D_{2n}$ .

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  $r^k = (k \bmod n, 0)$ , de modo que  $\text{ord } r = n$ . Y  $s^2 = (0, 1)(0, 1) = (0 + \alpha_1(0), 1 + 1) = (0, 0)$ , por lo que  $\text{ord } s = 2$ .

Finalmente, veamos que

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

Así, podemos notar que el producto semidirecto de grupos abelianos puede ser no abeliano.

A veces al siguiente resultado se le conoce como el «teorema de la órbita-estabilizador»:

**Teorema 1.70:** Si un grupo  $G$  actúa sobre el conjunto  $S$ , entonces:

1.  $\text{Stab}_a \leq G$ .
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

$$\text{Stab}_{\alpha_g(a)} = g^{-1}\text{Stab}_a g.$$

Ergo, los estabilizadores son conjugados.

4. Existe una biyección entre  $G/\text{Stab}_a$  y  $\text{Orb}_a$ , en particular si  $G$  es finito, entonces

$$|G| = |\text{Orb}_a| |\text{Stab}_a|.$$

DEMOSTRACIÓN:

1. Ejercicio para el lector.
2. Basta ver que si dos órbitas no son disjuntas entonces son iguales, para ello, dados  $a, b \in S$  basta probar la inclusión  $\text{Orb}_a \subseteq \text{Orb}_b$ . Sea  $c \in \text{Orb}_a \cap \text{Orb}_b$ , 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  $d \in \text{Orb}_b$ .

3. Ejercicio para el lector.



4. Prefijado un  $a \in S$ , vamos a definir  $H := \text{Stab}_a$ ,  $K := \text{Orb}_a$  y  $\varphi : G/H \rightarrow K$  como  $\varphi(gH) = \alpha_g(a)$ . En primer lugar, veamos que está bien definida, si  $x \equiv y$  (mód  $H$ ), 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  $\varphi$  es una biyección.  $\square$

**Corolario 1.70.1:** Si  $G$  actúa sobre  $S$ , donde  $S$  es finito, entonces existen  $x_1, \dots, x_n$  tales que

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

**Ejemplo.** Sea  $H \leq G$  un subgrupo. Entonces  $G$  tiene una acción derecha sobre la familia de clases laterales derechas  $\mathcal{S} := \{Ha : a \in G\}$  de  $H$ , dada por  $Ha \cdot g := H(ag)$ . Es claro que esta acción es transitiva y que el estabilizador de toda clase es precisamente  $H$ , por lo que el teorema de órbita-estabilizador recupera el teorema de Lagrange.

**Definición 1.71:** Si consideramos la acción por conjugación de un grupo  $G$  sobre sí mismo denotamos por  $C_G(x)$  y  $Z(x)$  a la órbita y al estabilizador de un elemento  $x \in G$ , los cuales se llaman *conjugador* y *centralizador* de  $x$  resp.

**Lema 1.72.A:** Dos clases de conjugación o son iguales o son disjuntas.

DEMOSTRACIÓN: Se sigue de que las clases de conjugación son órbitas de la acción por conjugación.  $\square$

Aplicado a la acción por conjugación, el corolario 1.70.1 toma la siguiente forma:

**Teorema 1.72 – Ecuación de clases:** Para todo grupo finito  $G$ , existen  $g_1, \dots, g_k \in G \setminus Z(G)$  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.  $\square$

**Definición 1.73:** Se dice que  $G$  es un  *$p$ -grupo* si posee su cardinalidad es alguna potencia del número primo  $p$ . También se dice que  $H$  es un  *$p$ -subgrupo* de  $G$  si  $H \leq G$  y  $H$  es un  $p$ -grupo.

**Corolario 1.73.1:** Todo  $p$ -grupo posee centro no trivial.

**Proposición 1.74:** Si  $G/Z(G)$  es cíclico, entonces  $G$  es abeliano. En particular,  $|G/Z(G)|$  nunca es primo.

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

**Corolario 1.74.1:** Para un grupo  $G$ , se cumplen:

1. Si  $G$  tiene cardinalidad  $p^2$  con  $p$  primo, entonces  $G$  es abeliano y es isomorfo a  $C_{p^2}$  o  $C_p \times C_p$ .
2. Si  $G$  tiene cardinalidad  $pq$  con  $p, q$  primos y tiene centro no trivial, entonces es cíclico.

**Definición 1.75:** Sea  $\alpha: G \curvearrowright S$  una acción de un grupo  $G$  en un conjunto  $S$ . Se denota por  $\text{Fix}_g(S)$  al conjunto de *puntos fijos* de la permutación  $\alpha_g$ , es decir

$$\text{Fix}_g(S) := \{x \in S : \forall g \in G \quad x^g = x\}.$$

Denotamos  $\text{Fix}_G(S)$  al conjunto de puntos fijos bajo cualquier permutación de la acción, vale decir,  $\text{Fix}_G(S) := \bigcap_{g \in G} \text{Fix}_g(S)$ .

**Teorema 1.76:** Si  $G$  es un  $p$ -grupo que actúa sobre  $S$  finito, entonces

$$|S| \equiv |\text{Fix}_G(S)| \pmod{p}.$$

DEMOSTRACIÓN: Por la ecuación de órbitas se cumple que

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

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

**Corolario 1.76.1:** 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<sup>3</sup> 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.

**Teorema 1.77 – 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.  $\square$

**Corolario 1.77.1:** Si todos los elementos no neutros de un grupo finito  $G$  tienen orden  $p$ , entonces  $G$  es un  $p$ -grupo.

<sup>3</sup>A veces el cuarto se considera una variación del tercero.

**Definición 1.78:** 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  $\text{Syl}_p(G)$  al conjunto de  $p$ -subgrupos de Sylow de  $G$ .

**Teorema 1.79 – Primer teorema de Sylow:** Todo grupo finito  $G$  contiene un  $p$ -subgrupo de Sylow para todo  $p$  primo. Osea,  $\text{Syl}_p(G) \neq \emptyset$ .

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  $\varphi : P \rightarrow \bar{P}$  tal que  $\varphi(g) = gN$ , como  $\varphi$  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  $G$ .  $\square$

**Teorema 1.80:** 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

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

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  $D_{2p}$ .  $\square$

**Teorema 1.81 – 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

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

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  $\mathrm{Fix}_Q(G/P)$  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.  $\square$

**Corolario 1.81.1:**  $G$  posee un único  $p$ -subgrupo de Sylow si y sólo si éste es normal.

**Definición 1.82 – 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 1.82.1:** Un grupo de cardinal  $mp$  con  $p$  primo y  $p \nmid m$  no es simple.

**Teorema 1.83 – 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  $n_p := |\mathrm{Syl}_p(G)|$ .

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

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

Probaremos ahora, por contradicción, que  $P$  es el único punto fijo de su acción. Sea  $Q \in \mathrm{Syl}_p(G)$  distinto de  $P$  tal que es punto fijo. Por definición,

para todo  $g \in P$  se cumple que  $g^{-1}Qg = Q$ , luego  $P \leq N_G(Q) \leq G$ . Luego, podemos ver que  $Q$  y  $P$  son  $p$ -subgrupos de Sylow de  $N_G(Q)$ , y  $Q$  es normal, luego por el corolario anterior  $P = Q$ . En conclusión  $|\text{Fix}_P(\text{Syl}_p(G))| = 1$ .

Consideremos la acción de  $G$  sobre  $\text{Syl}_p(G)$  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,  $n_p \mid m$ .  $\square$

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

**Teorema 1.84 – Cuarto teorema de Sylow:** Se cumple que  $n_p := |G/N_G(P)|$  donde  $P \in \text{Syl}_p(G)$ .

PISTA: Relea el último paso en la demostración anterior.  $\square$

Veamos un par de aplicaciones:

**Proposición 1.85:** Sea  $G$  un grupo finito. Entonces  $G$  es el producto directo de todos sus subgrupos de Sylow syss todos ellos son subgrupos normales.

DEMOSTRACIÓN: La implicancia «  $\implies$  » es obvia, así que probaremos «  $\impliedby$  »: escribamos  $|G| = p_1^{e_1} \cdots p_r^{e_r}$  y sea  $S_j$  el único  $p_j$ -subgrupo de Sylow de  $G$ . Procedemos por inducción sobre  $r$ . Claramente el subgrupo generado  $S_1 \cdots S_r = G$  y dado  $x \in S_i$  se cumple que tiene orden  $p_i^\alpha$  para algún  $0 \leq \alpha \leq e_i$ . Por hipótesis inductiva, todo  $y \in \prod_{j \neq i} S_j$  se escribe como  $y = \prod_{j \neq i} s_j$ , para algunos  $s_j \in S_j$ ; luego como el producto es directo vemos que

$$y^{p_i^\alpha} = \prod_{j \neq i} s_j^{p_i^\alpha} \neq 1,$$

pues cada  $s_j^{p_i^\alpha} \neq 1$ , probando así la proposición.  $\square$

**Teorema 1.86:** Sean  $p < q$  un par de números primos distintos.

- (a) Si  $p \nmid q - 1$ , entonces el grupo cíclico  $C_{pq}$  es el único grupo de cardinalidad  $pq$  (salvo isomorfismo).
- (b) Si  $p \mid q - 1$ , entonces hay exactamente dos grupos de cardinalidad  $pq$  (salvo isomorfismo).

DEMOSTRACIÓN: Sea  $G$  un grupo de cardinalidad  $pq$  y sea, por el teorema de Cauchy,  $P \leq G$  un subgrupo de cardinalidad  $p$  y  $Q \leq G$  de cardinalidad  $q$ ; es claro que  $PQ = G$ . Por el tercer teorema de Sylow, se sigue que  $Q$  es normal. Además, los elementos de  $Q$  son o bien el neutro 1 o tienen orden  $q$ , y análogamente con  $P$ , de modo que  $P \cap Q = \{1\}$ . Así pues, se sigue que  $G = Q \rtimes_{\alpha} P$ , para algún homomorfismo de grupos  $\alpha: P \rightarrow \text{Aut}_{\text{Grp}}(Q)$ .

Ahora bien,  $\text{Aut}(Q)$  tiene cardinalidad  $q - 1$  y, como  $P$  tiene cardinalidad prima, sabemos que  $P$  solo posee dos subgrupos. Luego, si  $p \nmid q - 1$  necesariamente  $\alpha$  es el homomorfismo trivial, dando lugar al caso (a). Si  $p \mid q - 1$ , entonces hay dos posibles opciones para  $\alpha$ : o bien el homomorfismo trivial, dando el producto directo  $G = C_q \times C_p = C_{pq}$ , o bien  $\alpha$  es un monomorfismo, lo que da al menos un producto semidirecto no abeliano. Pero si  $\alpha, \beta: P \rightarrow \text{Aut}(Q)$  son dos monomorfismos, siempre existe un automorfismo  $\gamma: P \rightarrow P$  de modo que  $\alpha = \gamma \circ \beta$ , por lo que todos los productos semidirectos no abelianos dan el mismo grupo.  $\square$

**Lema 1.87:** Sea  $G$  un grupo finito. Si existe un número primo  $p$  tal que  $p \mid |G|$  y  $n_p! < |G|$ , entonces  $G$  no es simple.

DEMOSTRACIÓN: Supongamos que se da aquello, luego consideremos la acción  $\alpha: G \rightarrow \text{Sym}(\text{Syl}_p(G)) \cong S_{n_p}$  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.  $\square$

**Proposición 1.88:** No hay grupos de cardinalidad  $< 60$  que sean simples y no abelianos.

DEMOSTRACIÓN: En primer lugar, todo grupo de cardinalidad prima  $p$  es abeliano; y todo grupo de cardinalidad  $pq$  con  $p < q$  primos distintos posee un  $q$ -subgrupo de Sylow, el cual será normal. Si su cardinalidad es  $p^n$ , entonces su centro es siempre 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)  $30 = 2 \cdot 3 \cdot 5$ : 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)  $56 = 2^3 \cdot 7$ : 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 2-subgrupo de Sylow  $K$ , 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.  $\square$

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

Un subconjunto  $X \subseteq G$  se dice **libre** si para toda sucesión finita  $x_1, \dots, x_n \in X$  donde  $x_i \neq x_{i+1}$ , y toda sucesión  $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$  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:

$$\text{Hom}(G, H) \approx \text{Func}(X, H), \quad (1.2)$$

donde  $\approx$  significa equipotencia de conjuntos.

**Teorema 1.90:** 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  $()^{-1}: \bar{S} \rightarrow \bar{S}$  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  $w := x_1 x_2 \cdots x_n$ , o formalmente una tupla ordenada finita de  $\bar{S}$ , donde su longitud viene dada por la de tupla ordenada, denotada  $|w| = n$ . El gran problema es que las palabras no reducidas pueden tener partes redundantes pues en el ejemplo anterior:

$$x_1 x_2 x_3^{-1} x_4^{-1} x_5 x_6^{-1} = x_1 x_2 x_3^{-1} x_4^{-1}$$



Así, definimos una reducción elemental<sup>4</sup>  $R_e: \bar{S}^{<\omega} \rightarrow \bar{S}^{<\omega}$  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  $R: \bar{S}^{<\omega} \rightarrow \bar{S}^{<\omega}$  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 consideramos palabras irreducibles, 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 irreducible).  $\square$

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

**Teorema 1.91:** 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  $\alpha$ '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  $\alpha_i = \beta_i$ .

---

<sup>4</sup>Recordar que  $\bar{S}^{<\omega}$  es el conjunto de todas las tuplas ordenadas finitas (incluyendo la tupla vacía) de  $\bar{S}$ .

$\Leftarrow$ . Sea  $X$  un sistema generador libre y sea  $f : X \rightarrow H$  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.

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

Más aún, sea  $\text{Id} : X \rightarrow X \subseteq F(X)$  una biyección, donde  $F(X)$  es un grupo donde  $X$  es libre, entonces se extiende a un único homomorfismo  $f^* : G \rightarrow F[X]$ . 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 1.92:** 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  $f: X \rightarrow Y$  biyección, luego se extiende a un homomorfismo  $f^*: G \rightarrow H$  y lo mismo con  $(f^{-1})^*: H \rightarrow G$ . Luego  $f^* \circ (f^{-1})^*: G \rightarrow G$  es un endomorfismo que fija a  $X$ , pero notemos que la identidad también lo es y por unicidad se cumple que  $f^* \circ (f^{-1})^* = \text{Id}_G$  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  $\varphi: G \rightarrow H$  un isomorfismo de grupos, y sea  $f \in \text{Hom}(H, \mathbb{Z}_2)$ , luego se cumple  $\varphi \circ f \in \text{Hom}(G, \mathbb{Z}_2)$  y es fácil ver que  $f \mapsto \varphi \circ f$  es un isomorfismo entre los grupos  $\text{Hom}(H, \mathbb{Z}_2) \cong \text{Hom}(G, \mathbb{Z}_2)$ , ergo

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

lo que comprueba el caso finito.

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

**Definición 1.93:** Por el teorema anterior llamamos *rango* de un grupo libre al cardinal de cualquiera de sus bases. En general si  $\kappa$  es un número cardinal denotamos  $F(\kappa)$  al grupo libre de rango  $\kappa$ , que es único salvo isomorfismos.

Una aplicación de los grupos libres como tal son las demostraciones de la paradoja de Banach-Tarski (véase [0, §A.1.2.]).

**Teorema 1.94:** Todo grupo es isomorfo a un cociente de un grupo libre.

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

**Definición 1.95:** 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  $f: X \rightarrow Y$  cuya extensión  $f^*: F(X) \rightarrow G$  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 1.96 (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  $f : G \rightarrow H$ .

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

$$\begin{array}{ccc} G = \frac{F(X)}{N} & \dashrightarrow & H \\ \pi \downarrow & & \uparrow \wr \\ \frac{F(X)/N}{\ker f^*/N} & \xrightarrow{\sim} & \frac{F(X)}{\ker f^*} \end{array}$$

conmuta, del que se deriva el epimorfismo deseado.  $\square$

### §1.5.2 Grupos solubles.

**Definición 1.97:** Dado un grupo  $G$  se le dice **serie normal** de subgrupos a una cadena de inclusiones estrictas

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

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 1.98:** 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

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

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  $G \triangleright G_1 \triangleright \cdots \triangleright G_m = N$  cuyos factores son simples, ergo, pegando las dos series se obtiene una serie de composición para  $G$ .

□

**Definición 1.99:** Llamaremos **subgrupo derivado**  $G'$  al subgrupo generado por todos los conmutadores de  $G$ . El subgrupo derivado



El conjunto de los conmutadores de un grupo no suele ser un subgrupo. La siguiente es la «propiedad universal» del conmutador:

**Proposición 1.100:** Se cumplen:

1.  $G' \trianglelefteq G$  y  $G/G'$  es abeliano. Al grupo  $G^{\text{ab}} := G/G'$  le llamamos la **abelianización** de  $G$ .
2. Si  $N \trianglelefteq G$ , entonces  $G/N$  es abeliano syss  $G' \leq N$ .
3. Para todo homomorfismo de grupos  $\varphi: G \rightarrow A$  con  $A$  abeliano, existe

un homomorfismo  $\bar{\varphi}: G^{\text{ab}} \rightarrow A$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A \\ \pi \searrow & & \nearrow \exists! \bar{\varphi} \\ & G^{\text{ab}} & \end{array}$$

DEMOSTRACIÓN: Probaremos el inciso 2, dejando el resto como ejercicios.

$\implies$ . 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  $G' \leq N$ .

$\Leftarrow$ . 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.  $\square$

**Lema 1.101.A:** 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)  $\implies$  (2)  $\implies$  (3).

(3)  $\implies$  (1). Por el corolario, si  $G$  posee una serie abeliana

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

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

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

por lo que los factores siguen siendo abelianos. Iterando el proceso se llega a una serie de composición abeliana.

(4)  $\implies$  (3). Entonces se cumpliría que

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

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

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

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

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  $G^{(n)} = \{e\}$ .  $\square$

**Definición 1.101:** Un grupo se dice *soluble* si satisface las condiciones del lema anterior.

**Corolario 1.101.1:** Un grupo simple y no abeliano no es soluble.

Veamos un ejemplo:

**Corolario 1.101.2:** Todo  $p$ -grupo es soluble.

DEMOSTRACIÓN: En efecto, o bien un  $p$ -grupo  $G$  es abeliano, en cuyo caso es trivialmente soluble; o bien no es abeliano y su centro  $Z(G)$  es normal y no trivial. Por inducción sobre la potencia de primo, se comprueba que el  $p$ -grupo  $G/Z(G)$  es soluble y  $Z(G)$  es abeliano, por lo que también es soluble.  $\square$

**Teorema 1.102:** Se cumple:

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

DEMOSTRACIÓN:

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

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

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

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

es una serie abeliana pues

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

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

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

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

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  $HK \supseteq H$ , donde  $H$  es soluble y  $HK/H \cong K/(H \cap K)$  es soluble por ser cociente de  $K$  que es soluble.  $\square$

**Lema 1.103:** Sea  $G$  un grupo finito y sea  $p$  el mínimo número primo tal que  $p \mid |G|$ . Todo subgrupo  $H \leq G$  de índice  $p$  es normal.

DEMOSTRACIÓN: Nótese que  $G$  actúa, por multiplicación izquierda, sobre el conjunto de clases laterales izquierdas de  $H$ . Esto determina un homomorfismo de grupos

$$\alpha: G \longrightarrow \text{Aut}_{\text{Set}}(\{aH : a \in G\}) = S_p,$$

donde  $\text{Aut}_{\text{Set}}$  denota las permutaciones del conjunto, el cual posee  $p$  elementos, por lo que es el grupo simétrico  $S_p$ .

Sea  $K := \ker \alpha \leq G$  el núcleo, el cual es un subgrupo normal, y nótese que  $K \supseteq H$ . Ahora  $G/K$  es isomorfo a un subgrupo de  $S_p$ . Nótese que  $S_p$  tiene orden  $p!$  y  $|G/K|$  divide a  $|G|$ , pero  $\text{mcd}(|G|, p!) = p$ , por lo que  $|G/K|$



es o bien 1 o  $p$ . Nótese que  $|G/K| \neq 1$  ya que la acción  $\alpha$  es transitiva), por lo que  $|G/K| = p$  y  $p = [G : H] = [G : K][K : H] = p[K : H]$  y, por tanto,  $[K : H] = 1$ ; es decir,  $H = K$  es normal.  $\square$

Como consecuencia:

**Proposición 1.104:** Sean  $p \neq q$  un par de números primos distintos. Todo grupo de cardinalidad  $pq$  es soluble.

DEMOSTRACIÓN: Por el teorema de Cauchy, si  $G$  tiene cardinalidad  $pq$ , entonces tiene un subgrupo  $Q \leq G$  de cardinalidad  $q$ , el cual es un subgrupo normal cíclico y tal que  $G/Q$  es cíclico.  $\square$

**Definición 1.105:** Dos series de composición para un grupo  $G$ :

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

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

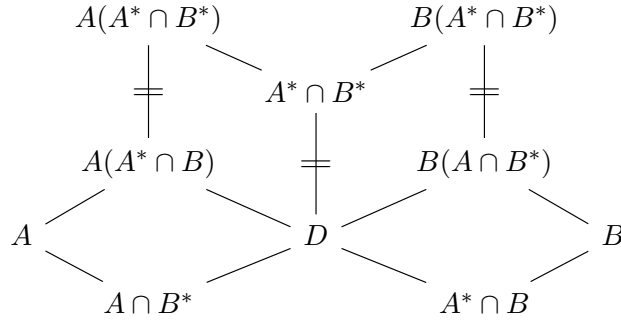
1.  $A(A^* \cap B) \trianglelefteq A(A^* \cap B^*)$ .
2.  $B(B^* \cap A) \trianglelefteq B(B^* \cap A^*)$ .
3.  $\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}$ .

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:<sup>5</sup>



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

**Definición 1.107:** Dada una serie normal  $G \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$ , se le llama un **refinamiento** a otra serie normal  $G \triangleright G'_1 \triangleright \cdots \triangleright G'_m = \{1\}$  tal que la primera es un subconjunto de la segunda.

**Teorema 1.108 (de refinamiento de Schreier):** Dos series normales de un mismo grupo poseen al menos un refinamiento equivalente.

DEMOSTRACIÓN: Sean

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

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

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

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

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

<sup>5</sup>Éste diagrama fue introducido por Lang en [0] y fue la razón de que él le nombrara el «lema de la mariposa».

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.  $\square$

**Teorema 1.109 – 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 1.110:** 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  $(a, b)(c, d) = (a, b, c)(c, a, d)$ .  $\square$

**Lema 1.111:** Si  $n \geq 5$ , y  $N \trianglelefteq A_n$  contiene un ciclo de longitud 3, entonces  $N = A_n$ .

DEMOSTRACIÓN: Sea  $\tau$  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  $N = A_n$ .  $\square$

**Teorema 1.112:** Si  $n \geq 5$ , entonces  $A_n$  es simple.

DEMOSTRACIÓN:

- 1)  $A_5$  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  $N \triangleleft A_{n+1}$ , entonces  $N \cap A_n \triangleleft A_n$ . 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  $\sigma$  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  $A_{n+1}$ .  $\square$

**Corolario 1.112.1:** Si  $n \geq 5$ , entonces  $A_n$  no soluble y, en consecuencia,  $S_n$  tampoco lo es.

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

**Proposición 1.113:**  $A_5$  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.  $\square$

## 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 [0] definen anillo con neutro multiplicativo y «anillo» (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 2.3.1:** Todo cuerpo es un dominio íntegro.

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

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

**Proposición 2.4:** 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 2.5:** 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 2.6:** 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 2.7 – Subanillo, ideal:** Se dice que  $\emptyset \neq B \subseteq A$  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 2.8:** Si  $1 \in B \leq A$  (como anillo), entonces  $B^\times \leq A^\times$  (como grupos).

**Proposición 2.9 (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 2.10:** La intersección arbitraria de subanillos (resp. ideales) es un subanillo (resp. ideal).

**Definición 2.11:** 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 2.12:** 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  $y \in S_y \in \mathcal{F}$ , 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.  $\square$

**Proposición 2.13:** Si  $\emptyset \neq S \subseteq A$  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, sobretudo, 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 2.14:** Todo ideal  $\mathfrak{a}$  de un anillo unitario  $A$  es propio syss no contiene elementos invertibles.

**Corolario 2.14.1:** 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 2.15 – Morfismos:** Una aplicación  $\varphi: A \rightarrow B$  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 2.16:** Sean  $A, B, C$  anillos. Entonces:

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

En consecuencia, los anillos y los homomorfismos de anillos constituyen una categoría denotada  $\mathbf{Rng}$ .

**Proposición 2.17:** Si  $\varphi: A \rightarrow B$  es un homomorfismo de anillos. Entonces:

1.  $\varphi(0_A) = 0_B$ .
2. Si  $\varphi$  es suprayectiva y  $A$  es unitario, entonces  $B$  también y  $\varphi(1_A) = 1_B$ .
3. Se cumple que  $\text{Im} \varphi \leq B$  y  $\ker \varphi \leq A$ .
4. Si  $A$  es un cuerpo, entonces  $\varphi$  es o inyectiva o es nula. Si  $B$  es unitario, entonces  $\varphi$  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 2.18:** Dado  $\mathfrak{a} \leq A$  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 2.19:** Dado  $\mathfrak{a} \leq A$  propio, entonces  $(A/\mathfrak{a}, +, \cdot)$  es también un anillo.

**Lema 2.20:** Si  $\mathfrak{a} \leq A$  y  $\mathfrak{b} \leq A$ , entonces  $\mathfrak{a} + \mathfrak{b} \leq A$ .

**Teorema 2.21 – Teoremas de isomorfismos:** Sean  $A, B$  anillos y  $\varphi : A \rightarrow B$  un morfismo, luego:

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

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  $\pi : A \rightarrow A/\mathfrak{a}$  induce una biyección

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

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

**Corolario 2.21.1:** Si  $\varphi : A \rightarrow B$  es morfismo, entonces:

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

**Definición 2.22 – Dominio euclídeo:** Sea  $A$  un dominio íntegro ordenado es un **dominio euclídeo** syss existe una función  $d : A_{\neq 0} \rightarrow \mathbb{N}$ , 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 2.23:** 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  $I = (a)$ .  $\square$

**Teorema 2.24:** 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  $\mathfrak{a}_m = \mathfrak{a}_n$ .

- (3) Toda familia no-vacía de ideales de  $A$  admite un  $\subseteq$ -maximal.<sup>1</sup>

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  $a_0 \in \mathfrak{a}$  y ver que  $(a_0) \subset \mathfrak{a}$ , luego, podríamos extraer  $a_1 \in \mathfrak{a} \setminus (a_0)$  tal que  $(a_0, a_1) \subset \mathfrak{a}$  y así sucesivamente para obtener una cadena infinita sin un elemento maximal.  $\square$

**Definición 2.25 – Anillo noetheriano:** Un dominio íntegro es un *anillo noetheriano* si cumple con las condiciones del teorema 2.24.

**Corolario 2.25.1:** Todo DIP es noetheriano.

<sup>1</sup>Véase [0, Def. 2.3]

## §2.1.1 Teorema del binomio.

**Definición 2.26:** 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 2.27:** Se cumple:

1.

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

2.

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{1} = n.$$

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.  $\square$

**Teorema 2.28 – 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.  $\square$

### §2.1.2 Característica.

**Lema 2.29:** Si  $A$  es unitario, entonces existe un único homomorfismo  $\varphi: \mathbb{Z} \rightarrow A$ .

PISTA: Basta construir  $\varphi$  por recursión empleando que  $\varphi(1) = 1$ .  $\square$

**Definición 2.30:** Si  $A$  es unitario le llamamos su *característica*, denotado por  $\text{car } A$ , al  $n \in \mathbb{N}$  tal que  $\ker \varphi = n\mathbb{Z}$ , donde  $\varphi$  es el morfismo del lema anterior.

En particular, los anillos unitarios de característica  $n$  conforman su propia subcategoría, denotada  $\text{Ring}_n$ .

**Corolario 2.30.1:** La característica de un dominio íntegro es o 0 o un número  $p$  primo.

**Proposición 2.31:** Si  $A, B$  son unitarios y existe un  $\phi: A \rightarrow B$  morfismo de anillos, entonces  $\text{car } B \mid \text{car } A$ .

**Teorema 2.32:** Si  $\mathbb{k}$  es un cuerpo, entonces:

1. Si  $\text{car } \mathbb{k} = p$ , entonces existe un único morfismo  $\phi: \mathbb{F}_p \rightarrow \mathbb{k}$ .
2. Si  $\text{car } \mathbb{k} = 0$ , entonces existe un único morfismo  $\phi: \mathbb{Q} \rightarrow \mathbb{k}$ .

En consecuencia,  $\mathbb{Q}$  es el objeto inicial de  $\text{Fld}_0$  y  $\mathbb{F}_p$  el de  $\text{Fld}_p$ .

**Definición 2.33:** 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 2.34 (Sueño del aprendiz):** Si  $\text{car } \mathbb{k} = p \neq 0$ , entonces para todo  $x, y \in \mathbb{k}$  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  $p$ .  $\square$

## 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 2.35 – 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 si 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 sí mismo; y *propios*.

**Definición 2.36 – Irreducibles y primos:** Sea  $A$  un dominio. Diremos que un elemento es *irreducible* si 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* si  $p \mid ab$  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 irreducible concuerdan (cf. lema de Euclides), pero ese no es siempre el caso.

**Teorema 2.37:** 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.  $\square$

**Definición 2.38:** 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 irreducibles 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 2.39:** En un DFU un elemento es primo si y sólo si es irreducible.

**Teorema 2.40:** 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  $y_0, \dots, y_k$  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  $i = 0, \dots, k$ . Construyamos la permutación  $\sigma$  tal que  $p_0 \mid q_{\sigma(0)}$ , pero como ambos son irreducibles, 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.  $\square$

**Definición 2.41:** 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) 2.42 (Cohen):** Un dominio  $A$  es noetheriano syss todo ideal primo de  $A$  es finitamente generado.

DEMOSTRACIÓN:  $\implies$ . Trivial.

$\impliedby$ . 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:

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

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  $\mathfrak{m} = (m_1, \dots, m_n) + \mathfrak{n}a$ : Es claro que  $(m_1, \dots, m_n) \subseteq \mathfrak{m}$  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  $(m_1, \dots, m_n)$  por definición, y el segundo sumando está en  $\mathfrak{m}$ , de modo que el factor que acompaña a  $a$  está, efectivamente, en  $\mathfrak{n}$ .  $\square$

**Proposición 2.43:** Sea  $\varphi: A \rightarrow B$  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 2.44:** Un ideal  $\mathfrak{p}$  en un dominio  $A$  es primo syss  $A/\mathfrak{p}$  es un dominio íntegro.

DEMOSTRACIÓN:  $\implies$ . 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.

$\Leftarrow$ . Es análogo.  $\square$

**Teorema 2.45:** Un ideal  $\mathfrak{m}$  en un dominio  $A$  es maximal syss  $A/\mathfrak{m}$  es un cuerpo.

DEMOSTRACIÓN:  $\implies$ . Como  $\mathfrak{m} \neq A$ ,  $A/\mathfrak{m}$  es un dominio. Supongamos que  $\mathfrak{a}$  es un ideal de  $A/\mathfrak{m}$  y  $\pi: A \rightarrow A/\mathfrak{m}$  es un homomorfismo de anillos, entonces  $\mathfrak{b} := \pi^{-1}(\mathfrak{a})$  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 2.14.1 es un cuerpo.

$\Leftarrow$ . Es análogo.  $\square$

**Corolario 2.45.1:** 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 2.69).

**Lema 2.46:** 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 irreducible es primo. Lo que sumado al teorema 2.40 nos da:

**Teorema 2.47:** Todo DIP es un DFU.

**Definición 2.48:** 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 2.49 (Identidad de Bézout):** Sea  $A$  un DIP con  $a_0, \dots, a_n \in A$ ; luego sea  $m$  un mcd, entonces

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

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

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

DEMOSTRACIÓN: Definamos que  $(m) = \sum_{i=0}^n (a_i)$ , probaremos que  $m$  es un mcd de dicha secuencia. Evidentemente  $m \mid a_i$  para  $i = 0, \dots, n$  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.  $\square$

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 2.50:** 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 2.51:** 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 2.52:** Se cumplen:

1. Sean  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  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  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  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  $\mathfrak{p} = \mathfrak{a}_j$ .  $\square$

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

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

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

DEMOSTRACIÓN: Ver que  $\varphi$  es un homomorfismo de anillos es trivial y

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

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  $db_1 + db_2 = d(b_1 + b_2) = d \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$ .  $\square$

**Corolario 2.53.1:** Si  $A$  es un dominio y  $\mathfrak{a}_1, \dots, \mathfrak{a}_n \trianglelefteq A$ , entonces el homomorfismo  $\varphi$  del teorema anterior se restringe a un homomorfismo de grupos

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

**Teorema 2.54:** 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:

$$\begin{array}{ccc} A & \xhookrightarrow{\varphi} & K \\ & \searrow \iota & \nearrow \exists! \bar{\varphi} \\ & k & \end{array}$$

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

Sea  $\varphi : A \rightarrow K$ ; 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.  $\square$

**Corolario 2.54.1:** 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 2.55:** Por el corolario anterior se denota por  $\text{Frac}(A)$  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  $\text{Frac}(A)$  es exactamente la misma que de  $\mathbb{Q}$  desde  $\mathbb{Z}$ , es decir, podríamos

definir  $\mathbb{Q} := \text{Frac}(\mathbb{Z})$ . 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 difícil 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  $\mathbb{F}_i := \{a + ib : a, b \in \mathbb{F}_p\}$  donde  $i^2 = -1$  y para tomar un ejemplo en concreto, sea  $p = 3$ ; luego  $f(i) = i^9 - i^3 = i - (-i) = 2i \neq 0$ . 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  $\eta: S \rightarrow \mathbb{N}$  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  $\epsilon_x$  es la función que da 1 cuando la indeterminada del argumento y del índice 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 2.56 – Polinomio:** Finalmente, dado un anillo  $A$  y un conjunto de indeterminadas  $S$ , denotaremos  $A[S]$  al conjunto de todas las aplicaciones  $f: M \rightarrow A$  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 líder**. Si el coeficiente líder 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 2.57:** 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 probarla manualmente. Si  $A$  es unitario, entonces  $1(x) := 1 \in A[x]$  que es, asimismo, una unidad. La conmutatividad es trivial.  $\square$

Podemos afirmar sencillamente que  $\deg(f + g) \leq \max(\deg f, \deg g)$  y  $\deg(fg) \leq \deg f + \deg g$ .

**Teorema 2.58:** 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,  $\deg(fg) = \deg f + \deg g$ .  $\square$

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,  $A[x_1, \dots, x_n, x_{n+1}] = A[x_1, \dots, x_n][x_{n+1}]$ .

**Teorema 2.59:** Si  $A$  es un dominio íntegro y  $S$  un conjunto de indeterminadas, entonces  $A[S]^\times = A^\times$ .

DEMOSTRACIÓN: Por el teorema 2.58 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  $A$ .  $\square$

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 2.60:** Sean  $A, B$  dominios, sea  $\phi: A \rightarrow B$  un homomorfismo de anillos tal que  $\phi(1) = 1$ ,  $S$  un conjunto de indeterminadas y  $v: S \rightarrow B$  una función arbitraria. Entonces existe un único homomorfismo de anillos  $\Phi: A[S] \rightarrow B$  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:

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

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:

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

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.  $\square$

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

$$\text{ev}_{\alpha_1, \dots, \alpha_n} : A[x_1, \dots, x_n] \longrightarrow A.$$

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

**Teorema 2.61 – 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  $\beta(x) = b_0 + \cdots + b_mx^m$  y  $\alpha(x) = a_0 + \cdots + a_nx^n$ , luego  $\alpha a_n^{-1}b_mx^{m-n} = \sum_{i=0}^n a_i a_n^{-1}b_mx^{m-n+i}$  posee mismo término director, por ende, existen  $q, r \in A[x]$  tales que:

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

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

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

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.  $\square$

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

**Teorema 2.62:** Si  $A$  es un dominio íntegro, entonces  $A[x]$  es un DIP syss  $A$  es un cuerpo.

DEMOSTRACIÓN: El corolario anterior prueba  $\Leftarrow$ , 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.  $\square$

**Teorema 2.63 – 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 2.64:** Sea  $A$  un anillo con  $p(x) \in A[x]$  de grado  $n$ , entonces  $p$  tiene, a lo sumo,  $n$  raíces.

**Teorema 2.65 (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  $\pm 1$ . En conclusión:

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

□

**Teorema 2.66 (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

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

□

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

Podemos ver que es correcto, pues

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

$$\begin{array}{r|rrr}
& 3 & 2 & 1 \\
-1 & & 3 \cdot -1 = -3 & -1 \cdot -1 = 1 \\
\hline
& 3 & 2 + (-3) = -1 & 1 + 1 = 2
\end{array}$$

**Figura 2.1.** Aplicación del algoritmo de Horner-Ruffini.

**Teorema 2.67 – Polinomio de interpolación de Lagrange:** Sea  $A$  un cuerpo con  $a_1, \dots, a_n, b_1, \dots, b_n \in A$ . Existe un único polinomio  $f \in A[x]$  de grado menor a  $n$  tal que  $f(a_i) = b_i$  para todo  $i = 1, \dots, n$ ; y está dado por la fórmula<sup>a</sup>

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

<sup>a</sup>En análisis matemático, la expresión  $P_i(a_i)$  estaría indeterminada por ser del tipo «0/0», no obstante, aquí se realiza la división 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 cumpliera 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 2.64.  $\square$

**Teorema 2.68 – Teorema de bases de Hilbert:** Si  $A$  es un anillo noetheriano, entonces  $A[x_1, \dots, x_n]$  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  $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$  (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  $\mathfrak{a}_i = (a_{i0}, \dots, a_{im})$  (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  $\mathfrak{c} := (p_{ij} : i = 0, \dots, n; j = 0, \dots, m)$ . 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  $x^{k-n}p_{n0}, \dots, x^{k-n}p_{nm}$  son  $a_{n0}, \dots, a_{nm}$  que definen  $\mathfrak{a}_k = \mathfrak{a}_n$ , luego, existen  $b_0, \dots, b_m \in A$  tales que

$$q := b_0x^{k-n}a_{n0} + \dots + b_mx^{k-n}a_{nm}$$

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.  $\square$

**Ejemplo Un anillo de polinomios, con campo de coeficientes noetheriano, que no es noetheriano.** Tomemos a  $\mathbb{R}$  que es cuerpo y por ende noetheriano. Luego si  $S := \{x_1, x_2, x_3, \dots\}$  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  $\geq 1$ ), pero no es finitamente generado.

Veamos una aplicación de los anillos de polinomios:

**Teorema 2.69:** 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 2.12) 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  $R \cdot U^{-1} \leq \text{Frac}(R)$ , 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  $\lambda$  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.  $\square$

## 2.4 Divisibilidad de polinomios

**Definición 2.70 (Contenido):** Sea  $A$  un DFU, definimos la aplicación  $c: A[x] \rightarrow \mathcal{P}(A)$ , 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** si  $c(f) = (1)$ , es decir, si sus coeficientes no nulos son coprimos. En particular, todo polinomio mónico es primitivo.

**Teorema 2.71 – Teorema de las raíces racionales:** Sea  $A$  un DFU,  $K := \text{Frac}(A)$  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:

$$\begin{aligned} a^n c_n &= -b \sum_{i=0}^{n-1} a^i b^{n-1-i} c_i \\ b^n c_0 &= -a \sum_{i=1}^{n-1} a^{i-1} b^{n-i} c_i, \end{aligned}$$

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.  $\square$

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 2.71.1:** Si  $p(x) \in \mathbb{Q}[x]$  es mónico, entonces sus raíces (si las tiene) son enteras.

**Lema 2.72 (de primitividad de Gauss):** Sea  $A$  un DFU con  $f, g \in A[x]$  primitivos, entonces  $f \cdot g$  es primitivo.

DEMOSTRACIÓN: Sean  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  y  $g(x) = b_0 + \cdots + b_mx^m$ , 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

$$p \mid c_{u+v} - a_ub_v = \sum_{i=0}^{u-1} \textcolor{red}{b}_i c_{u+v-i} + \sum_{i=0}^{v-1} b_{u+v-i} \textcolor{red}{c}_i$$

debido a que  $p$  divide los términos en rojo. Pero como  $p \nmid a_u, b_v$  concluimos que  $p \nmid c_{u+v}$ .  $\square$

**Teorema 2.73:** 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.  $\square$

**Lema 2.74:** Sea  $A$  un DFU con  $K$  su cuerpo de cocientes y  $f, g \in A[x]$  polinomios primitivos no-constantos.  $f$  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  $A[x]$ .  $\square$

**Teorema 2.75:** Si  $f \in \mathbb{k}[x]$  es de grado 2 o 3, entonces es irreducible syss no posee raíces.

DEMOSTRACIÓN: Por regla de Ruffini es claro que si es irreducible no posee raíces. Para el caso recíproco basta considerar que toda posible factorización incluye un término de grado 1.  $\square$

**Teorema 2.76 – Criterio de Irreducibilidad de Gauss:** Sea  $A$  un DFU,  $K := \text{Frac}(A)$  y  $f \in A[x]$  un polinomio primitivo no constante.  $f$  es irreducible en  $A[x]$  syss lo es en  $K[x]$ .

DEMOSTRACIÓN:  $\Leftarrow$ . Éste caso es trivial.

$\Rightarrow$ . 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  $g_1(x) = \sum_{i=0}^n a_i \tilde{b}_i x^i$  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  $A[x]$ .  $\square$

**Proposición 2.77:** Sea  $k$  un cuerpo,  $p(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$  un polinomio y  $A := k[x_1, \dots, x_{n-1}]$ . Escribamos  $p$  como un polinomio  $p(x_n) \in A[x_n]$ :

$$p(x_n) = a_0(x_1, \dots, x_{n-1}) + \dots + a_m(x_1, \dots, x_{n-1})x_n^m,$$

donde cada  $a_i(x_1, \dots, x_{n-1}) \in A$ . Si  $p(x_n)$  es primitivo y no puede factorizarse en polinomios de grado menor, entonces  $p(x_1, \dots, x_n)$  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 consecuencia,  $p(x_1, \dots, x_n)$  es irreducible en  $A[x_n] = A[x_1, \dots, x_n]$ .  $\square$

**Corolario 2.77.1:** Sea  $k$  un cuerpo,  $g, h \in k[x_1, \dots, x_n]$  polinomios coprimos, y sea

$$f(x_1, \dots, x_n, y) = yg(x_1, \dots, x_n) + h(x_1, \dots, x_n) \in k[x_1, \dots, x_n, y],$$

entonces  $f$  es irreducible en  $k[x_1, \dots, x_n, y]$ .

DEMOSTRACIÓN: Basta notar que  $f$  es lineal en  $A[y]$  con  $A = k[x_1, \dots, x_n]$ , de modo que no puede factorizarse en polinomios de grado menor y como  $g, h$  son coprimos, entonces  $f$  es primitivo.  $\square$

**Lema 2.78:** 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

$$f(x) = \frac{a_n}{b_n}x^n + \dots + \frac{a_0}{b_0} \in k[x],$$

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.  $\square$

**Proposición 2.79:** Sea  $k$  un cuerpo y sea

$$f(x, y) = y^n + \frac{g_{n-1}(x)}{h_{n-1}(x)}y^{n-1} + \dots + \frac{g_0(x)}{h_0(x)} \in k(x)[y],$$

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

$$\max\{g_i(x), h_i(x) : i \in \{0, 1, \dots, n-1\}\} \leq \deg_x(f^*).$$

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  $h_0, \dots, h_n$ ; de modo que  $c(f) = u_i h_i$  con  $u_i \in k[x]$  para todo  $i$ . Así pues, nos queda que

$$f^*(x, y) = c(f)f(x, y) = c(f)y^n + u_{n-1}(x)g_{n-1}(x)y^{n-1} + \dots + u_0(x)g_0(x) \in k[x][y],$$

de modo que si  $m := \deg_x(f^*)$ , entonces

$$m = \max\{\deg_x(c(f)), \deg_x(u_i) + \deg_x(g_i)\}.$$

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  $i$ .  $\square$

**Teorema 2.80:** 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.  $\square$

**Teorema 2.81 – 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  $i = 0, 1, \dots, n-1$ .
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.  $\square$

**Teorema 2.82:** Sea  $A$  un dominio con  $a \in A$  invertible y  $b \in A$  cualquiera, entonces  $p(x)$  es irreducible syss  $p(ax + b)$  lo es.

DEMOSTRACIÓN: Para demostrarlo veremos que  $f : A[x] \rightarrow A[x]$  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.  $\square$

**Ejemplo 2.83** (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 irreducibles 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  $p \mid \binom{p}{n}$ .  $\lrcorner$

Usualmente se suelen aplicar en conjunto el criterio de Eisenstein con el teorema anterior para demostrar la irreducibilidad 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 irreducible 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 irreducible por criterio de Eisenstein. Recuerde que 3 es una unidad de  $\mathbb{Q}$  y como el polinomio original es primitivo, entonces es irreducible también en  $\mathbb{Z}$ .

**Teorema 2.84 (criterio de irreducibilidad por reducción):** Sea  $\sigma: A \rightarrow B$  un homomorfismo entre dominios íntegros. Sean  $K := \text{Frac}(A)$  y  $L := \text{Frac}(B)$ . 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  $\deg \sigma(f) = \deg f$ , 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.  $\square$

**Ejemplo.** Veamos que el polinomio  $p(x) := x^3 + x + 1 \in \mathbb{Z}[x]$  es irreducible. Consideremos  $\pi: \mathbb{Z} \rightarrow \mathbb{F}_2$  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 2.85:** Un polinomio que es irreducible en  $\mathbb{Z}[x]$ , pero reducible en  $\mathbb{F}_p[x]$  para todo  $p$  primo. 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 2.85.1:** Sea  $A$  un DFU,  $K := \text{Frac}(A)$  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 2.86:** Dado  $\alpha \in \mathbb{k}$ , decimos que  $\beta$  es una  $n$ -ésima raíz de  $\alpha$  si  $\beta^n = \alpha$  o alternativamente si  $\beta$  es raíz del polinomio  $x^n - \alpha$ .

**Lema 2.87:** Si  $\beta$  es una raíz cuadrada de  $\alpha$ , entonces  $-\beta$  y  $\beta$  son todas las raíces cuadradas de  $\alpha$ .

**Teorema 2.88 (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  $\alpha$  raíz cuadrada de  $\Delta$ , 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  $\alpha$  es raíz de  $\Delta$ , entonces  $\pm\alpha/2 = x - r/2$  y así se deduce el enunciado.  $\square$

**Corolario 2.88.1:** Un polinomio de grado 2 es irreducible 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 irreducible  $x^2 + 1$ . Aquí haremos una definición alternativa de los números complejos que permitirá al lector acostumbrarse a ellos.

**Definición 2.89 – 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  $(a, b) = a + ib$ . Pues  $(1, 0)$  se comporta como el neutro multiplicativo,  $(0, 0)$  como el neutro aditivo e  $i^2 = (0, 1)^2 = (-1, 0) = -1$ . También se definen las funciones  $\text{Re}, \text{Im} : \mathbb{C} \rightarrow \mathbb{R}$  como

$$\text{Re}(a + ib) = a, \quad \text{Im}(a + ib) = b,$$

las que se llaman **parte real** e **imaginaria**, resp.

También, denotamos

$$|a + ib| := \sqrt{a^2 + b^2}, \quad \overline{a + ib} := a - ib,$$

donde a  $|z|$  se le dice el **valor absoluto** de  $z$  y a  $\bar{z}$  su **conjugado** de  $z$ .

**Proposición 2.90:** Para todo  $z, w \in \mathbb{C}$  se cumple:

1.  $|z| = 0$  syss  $z = 0$ .
2.  $\bar{\bar{z}} = z$ .
3.  $|\bar{z}| = |z|$ .
4.  $z + \bar{z} = 2 \text{Re } z$  y  $z - \bar{z} = 2i \text{Im } z$ .
5.  $\overline{z + w} = \bar{z} + \bar{w}$  y  $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$ . En otras palabras,  $\bar{\cdot}$  es un automorfismo de cuerpos.
6.  $x \in \mathbb{R}$  syss  $\bar{x} = x$  syss  $i\bar{x} = -x$ .
7.  $z \cdot \bar{z} = |z|^2$ .
8.  $|zw| = |z| |w|$ .

**Teorema 2.91:**  $(\mathbb{C}, +, \cdot)$  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  $z^{-1} = \bar{z}/|z|^2$  mediante las propiedades anteriores.  $\square$

**Teorema 2.92:** 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 2.93:** Todo complejo tiene raíz cuadrada. En consecuencia, todo polinomio cuadrático es reducible en los complejos.

**Proposición 2.94:** Si  $P, Q \in \mathbb{C}[x]$ , entonces:

1. Para todo  $z \in \mathbb{C}$  que  $\overline{P}(\bar{z}) = \overline{P(z)}$ .
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  $\bar{z}$  también es raíz.
5.  $P \cdot \overline{P} \in \mathbb{R}[x]$ .

**Definición 2.95:** Se define la función  $\text{cis} : \mathbb{R} \rightarrow \mathbb{C}$  tal que

$$\text{cis } \theta := \cos \theta + i \sin \theta.$$

Y se define  $\arg : \mathbb{C}_{\neq 0} \rightarrow (-\pi, \pi]$  así:

$$\arg(x + iy) = \begin{cases} \arctan(y/x), & x > 0 \\ \arctan(y/x) + \pi, & x < 0 \wedge y \geq 0 \\ \arctan(y/x) - \pi, & x < 0 \wedge y < 0 \\ \pi/2, & x = 0 \wedge y > 0 \\ -\pi/2, & x = 0 \wedge y < 0 \end{cases}$$

**Proposición 2.96:** Si  $z \in \mathbb{C}_{\neq 0}$ , entonces  $z = |z| \text{cis}(\arg z)$ .

**Teorema 2.97 – Teorema de De Moivre:** Si  $u = r \text{cis } \alpha$  y  $v = s \text{cis } \beta$ , entonces

$$u \cdot v = rs \text{cis}(\alpha + \beta). \quad (2.2)$$

En particular

$$u^n = r^n \text{cis}(n\alpha). \quad (2.3)$$

DEMOSTRACIÓN: Basta notar que

$$\begin{aligned} u \cdot v &= rs(\operatorname{cis} \alpha \cdot \operatorname{cis} \beta) \\ &= rs(\cos \alpha \cos \beta - \sin \alpha \sin \beta + i(\sin \alpha \cos \beta + \cos \alpha \sin \beta)) \\ &= rs(\cos(\alpha + \beta) + i \sin(\alpha + \beta)) = rs \operatorname{cis}(\alpha + \beta) \end{aligned}$$

como se quería probar.  $\square$

**Corolario 2.97.1:** 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 2.98:** 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

$$\zeta_n := \operatorname{cis}(2\pi/n) = \cos(2\pi/n) + i \sin(2\pi/n),$$

de modo que todas las raíces  $n$ -ésimas de la unidad son simplemente las potencias de  $\zeta_n$ .

**§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 2.99:** Si  $f \in \mathbb{C}[x]$  es no constante, entonces  $|f(z)| \rightarrow \infty$  si  $|z| \rightarrow \infty$ . 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

$$\lim_{|z| \rightarrow \infty} \frac{|f(z)|}{|z|^n} = |c_n|$$

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.  $\square$

**Lema 2.100:** 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.  $\square$

**Teorema 2.101 – 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  $\alpha$  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  $g(0) = 1$ .  $\square$

## 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 [0], 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 [0] (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,<sup>2</sup> 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

<sup>2</sup>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 [0] (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  $k[x_1, \dots, x_n]$  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 [0] (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  $+: M^2 \rightarrow M$  y  $\cdot: A \times M \rightarrow M$  tales que  $(M, +)$  es un grupo abeliano (de neutro  $\vec{0}$ ) y para todo  $\mathbf{u}, \mathbf{v} \in M$  y  $\alpha, \beta \in A$  se cumple:

1.  $\alpha(\beta\mathbf{u}) = (\alpha\beta)\mathbf{u}$ .
2.  $1\mathbf{u} = \mathbf{u}$ .
3.  $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$ .
4.  $(\alpha + \beta)\mathbf{u} = \alpha\mathbf{u} + \beta\mathbf{u}$ .

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  $v \in M$  se cumple que  $0 \cdot v = \vec{0}$ .
3. Para todo  $v \in M$  se cumple que  $(-1)v = -v$ .

**Ejemplo 3.3:** Son  $A$ -módulos:

- $A^n$  con la suma y el producto por escalar coordenada a coordenada.
- $\text{Func}(S; A)$  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  $\text{Func}(S; A)$ .
- $I$  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 3.4:** Todo grupo abeliano es un  $\mathbb{Z}$ -módulo: Sea  $G$  abeliano, entonces consideramos  $u + v := u * v$  (donde  $*$  es la operación de grupo de  $G$ ) y  $nu := (u)^n$ . La notación engorrosa es solamente para ilustrar el sentido de ésta afirmación. Claramente  $\langle(G, +)\rangle$  es un grupo abeliano de neutro  $\langle\vec{0}\rangle$  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 3.5 – Morfismos de módulos:** Una aplicación  $f: M \rightarrow N$  se dice un morfismo de  $A$ -módulos si para todo  $u, v \in M$  y  $\lambda \in A$  se comprueba

$$f(u + v) = f(u) + f(v), \quad f(\lambda u) = \lambda f(u).$$

Nuevamente la nomenclatura categórica se extiende a morfismos de módulos. El conjunto de morfismos de  $A$ -módulos desde  $M$  a  $N$  se denota por  $\text{Hom}_A(M, N)$ .

Un morfismo entre espacios vectoriales se dice una *función lineal*.

**Proposición 3.6:** Sea  $M$  un  $A$ -módulo. Entonces:

1.  $\text{Id}_M: M \rightarrow M$  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  $\mathbf{Mod}_A$ . Ésto también aplica para  $k$ -espacios vectoriales, cuya categoría se denota  $\mathbf{Vect}_k$ .

**Ejemplo.** Sean  $M, N$  un par de  $A$ -módulos. Entonces  $\text{Hom}_A(M, N)$  es un  $A$ -módulo. La construcción es similar a la de  $\text{Func}(S; A)$ .

**Proposición 3.7:** Dados  $X, Y$  no vacíos se cumple que  $\text{Func}(X; A) \cong \text{Func}(Y; A)$  syss  $|X| = |Y|$ . Luego, dado un cardinal  $\kappa$  denotamos  $A^\kappa$  a un  $A$ -módulo  $\text{Func}(S; A)$  genérico<sup>1</sup> con  $|S| = \kappa$ .

**Definición 3.8 – 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 *irreducible*) si no admite submódulos propios.

**Teorema 3.9 (Criterio del submódulo):**  $N$  es submódulo del  $A$ -módulo  $M$  syss  $N$  es no vacío y para todo  $u, v \in N$  y todo  $\lambda \in A$  se cumpla que  $\lambda u + v \in N$ .

**Lema 3.10:** La intersección de submódulos es un submódulo.

**Definición 3.11:** 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  $\langle S \rangle = M$ .

<sup>1</sup>En particular consideramos la representación ordinal-conjuntista de  $\kappa$ .

**Proposición 3.12:** Se cumple que

$$\langle S \rangle = \left\{ \sum_{i=1}^n \lambda_i x_i : \forall i (\lambda_i \in A \wedge x_i \in S) \right\}.$$

**Proposición 3.13:** Si  $N$  es un submódulo del  $A$ -módulo  $M$ , entonces  $x \equiv y \pmod{N}$  definido porque  $x - y \in N$  es una relación de equivalencia, bajo la cuál se denota por  $M/N$  al conjunto cociente que también resulta ser un  $A$ -módulo.

**Teorema 3.14 – Teoremas de isomorfismos:** Se cumple:

I Si  $M, N$  son  $A$ -módulos y  $\varphi: M \rightarrow N$  un morfismo, entonces

$$\frac{M}{\ker \varphi} \cong \text{Img } \varphi.$$

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,  $S \subseteq T$  si y sólo si  $\frac{S+N}{N} \subseteq \frac{T+N}{N}$ .

**Definición 3.15 (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 3.16:** 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  $\sum_{i \in I} \mathbf{m}_i = \vec{0}$  con  $\mathbf{m}_i \in N_i$  para todo  $i \in I$ , entonces  $\mathbf{m}_i = \vec{0}$ .
- c) Para todo  $\mathbf{m} \in M$  existen unos únicos  $\mathbf{m}_i \in N_i$  para cada  $i \in I$  tales que

$$\mathbf{m} = \sum_{i \in I} \mathbf{m}_i.$$

DEMOSTRACIÓN: a)  $\implies$  b). Procedemos a demostrarlo por contradicción, supongamos que existe un subconjunto  $J \subseteq I$  tal que

$$\sum_{j \in J} \mathbf{m}_j = \vec{0}$$

con  $\mathbf{m}_j \neq \vec{0}$  para todo  $j \in J$ . Tomemos un  $j_0 \in J$  tal que  $\mathbf{m}_{j_0} \neq \vec{0}$ , evidentemente  $\mathbf{m}_{j_0} = \sum_{j \in J \setminus \{j_0\}} -\mathbf{m}_j$ . Luego

$$\mathbf{m}_{j_0} \in N_{j_0} \cap \sum_{j \in J \setminus \{j_0\}} N_j \subseteq N_{j_0} \cap \sum_{i \in I \setminus \{j_0\}} N_i.$$

b)  $\implies$  c). Consideraremos el siguiente homomorfismo

$$\begin{aligned} f: \prod_{i \in I} N_i &\longrightarrow M \\ (\mathbf{m}_i)_{i \in I} &\longmapsto \sum_{i \in I} \mathbf{m}_i, \end{aligned}$$

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  $\mathbf{m} \in M$  con dos descomposiciones

$$\mathbf{m} = \sum_{i \in I} \mathbf{m}_i = \sum_{i \in I} \mathbf{n}_i.$$

Luego para algún  $i \in I$  ha de darse que  $\mathbf{m}_i \neq \mathbf{n}_i$ , luego

$$\vec{0} \neq \mathbf{m}_i - \mathbf{n}_i = \sum_{j \neq i} \mathbf{n}_j - \mathbf{m}_j$$

luego  $\mathbf{m}_i - \mathbf{n}_i \in N_i \cap \sum_{j \neq i} N_j$  que es absurdo.  $\square$

## 3.2 Módulos libres y bases

**Definición 3.17:** Sea  $M$  un  $A$ -módulo con  $X \subseteq M$ . Diremos que  $X$  es *libre* o que sus elementos son *linealmente independientes* si se da la ecuación

$$\lambda_0 \mathbf{x}_0 + \cdots + \lambda_n \mathbf{x}_n = \vec{0}$$

se da con  $\mathbf{x}_i \in X$  distintos dos a dos y  $\lambda_i \in A$  siempre que  $\lambda_i = 0$  para todo  $i = 0, \dots, n$ . 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 3.18:** Un módulo que no es libre Es fácil notar que con la suma y producto normal  $\mathbb{Q}$  es un  $\mathbb{Z}$ -módulo, sin embargo, no es libre (¿por qué?).  $\lrcorner$

### §3.2.1 Finitamente generados.

**Definición 3.19:** 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  $(\mathbf{x}_1, \dots, \mathbf{x}_n)$  tal que el morfismo de módulos

$$\begin{aligned} \varphi: A^n &\longrightarrow M \\ (\lambda_1, \dots, \lambda_n) &\longmapsto \lambda_1 \mathbf{x}_1 + \cdots + \lambda_n \mathbf{x}_n \end{aligned}$$

es suprayectivo.

**Ejemplo Un módulo que no es finitamente generado.** 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  $\{p_1(x), \dots, p_n(x)\}$  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 3.20:** 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

$$M = \bigoplus_{\mathbf{x} \in X} \langle \mathbf{x} \rangle;$$

luego es isomorfo a  $\prod_{\mathbf{x} \in X} \langle \mathbf{x} \rangle$  y  $\langle \mathbf{x} \rangle \cong A$  trivialmente para todo  $\mathbf{x} \in X$ .  $\square$

Desde aquí en adelante veremos resultados casi exclusivamente para espacios vectoriales:

**Lema 3.21:** Si  $S$  es ligado en un espacio vectorial, entonces existe un  $\mathbf{v} \in S$  que es generado por el resto, es decir, tal que  $\mathbf{v} \in \langle S \setminus \{\mathbf{v}\} \rangle$ .

**Teorema 3.22:** Si  $G$  es un sistema generador ligado, entonces  $\mathbf{v} \in G$  está generado por el resto de  $G$  syss  $G \setminus \{\mathbf{v}\}$  es un sistema generador. Si  $S$  es libre en un espacio vectorial y  $\mathbf{v}$  no es generado por  $S$ , entonces  $S \cup \{\mathbf{v}\}$  es libre.

**Corolario 3.22.1:** Todo sistema generador finito en un espacio vectorial contiene una base. En consecuencia, todo espacio vectorial finitamente generado es libre.

**Teorema 3.23:** Todo par de bases de un espacio vectorial finitamente generado posee el mismo cardinal.

DEMOSTRACIÓN: Sean  $X := \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$  e  $Y$  bases tal que  $|X| \leq |Y|$  (en principio,  $Y$  podría ser infinito). Sea  $\mathbf{y}_1 \in Y$  cualquiera, como  $\mathbf{y}_1 \in V = \langle X \rangle$ , entonces existen  $\alpha_{1,i} \in \mathbb{k}$  tales que

$$\mathbf{y}_1 = \sum_{i=1}^n \alpha_{1,i} \mathbf{x}_i$$

como  $\mathbf{y}_1 \neq 0$  algún  $\alpha_{1,i}$  ha de ser no nulo y reordenando supongamos que  $\alpha_{1,1} \neq 0$ , luego

$$\mathbf{x}_1 = \frac{1}{\alpha_{1,1}} \mathbf{y}_1 - \sum_{i=2}^n \frac{\alpha_{1,i}}{\alpha_{1,1}} \mathbf{x}_i,$$

llamando  $B_0 := X$  y  $B_1 := B_0 \setminus \{\mathbf{x}_1\} \cup \{\mathbf{y}_1\}$ , como  $X \subseteq \langle B_1 \rangle$ , entonces  $B_1$  es base y posee  $n$  elementos.

Análogamente se escoge  $\mathbf{y}_2 \in Y \subseteq V = \langle B_1 \rangle$ , luego existen  $\alpha_{2,i} \in \mathbb{k}$  tales que

$$\mathbf{y}_2 = \alpha_{2,1} \mathbf{y}_1 + \sum_{i=2}^n \alpha_{2,i} \mathbf{x}_i$$

notamos que algún  $\alpha_{2,i}$  con  $i > 1$  ha de ser no nulo y reordenamos para que  $\alpha_{2,2} \neq 0$ , luego

$$\mathbf{x}_2 = \frac{1}{\alpha_{2,2}} - \left( \frac{\alpha_{2,1}}{\alpha_{2,2}} \mathbf{y}_1 + \sum_{i=3}^n \frac{\alpha_{2,i}}{\alpha_{2,2}} \mathbf{x}_i \right),$$

de modo que si  $B_2 := B_1 \setminus \{\mathbf{x}_2\} \cup \{\mathbf{y}_2\}$  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.  $\square$

**Corolario 3.23.1:** Todo conjunto libre en un espacio vectorial finitamente generado se puede extender a una base.

**Definición 3.24 – Dimensión:** Si  $V$  es un  $\mathbb{k}$ -espacio vectorial y sus bases son equipotentes, entonces denotamos por  $\dim_{\mathbb{k}} V$  al cardinal de cualquiera de ellas.

**Corolario 3.24.1:** 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  $\mathbb{k}$ -espacios vectoriales que comparten dimensión finita, entonces son isomorfos. En consecuencia si  $n := \dim_{\mathbb{k}} V$ , entonces  $V \cong \mathbb{k}^n$ .



**Definición 3.26 – Base canónica:** Se le llama *base canónica* de  $\mathbb{k}^n$  como  $\mathbb{k}$ -espacio vectorial a la base ordenada  $(\mathbf{e}_1, \dots, \mathbf{e}_n)$  donde

$$\mathbf{e}_i := (0, \dots, \underset{(i)}{1}, \dots, 0).$$

Por ejemplo, la base canónica de  $\mathbb{k}^2$  es

$$\mathbf{e}_1 := (1, 0), \quad \mathbf{e}_2 := (0, 1).$$

La base canónica será útil ya que en lugar de hablar de espacios vectoriales abstractos de dimensión finita podemos simplemente usar a  $\mathbb{k}^n$  con la base canónica.

**§3.2.2 Espacios de dimensión infinita.** Es sencillo notar que para todo cuerpo  $\mathbb{k}$  se cumple que  $\mathbb{k}[x]$  es un  $\mathbb{k}$ -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 contenera 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  $F_i$  son finitos. Definamos  $X := \bigcup_{i \in I} X_i$ , si  $\mathbb{k}$  es un cuerpo arbitrario, entonces  $\mathbb{k}(X)$  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  $f \in \mathbb{k}(X)$  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  $\mathbb{k}(X)$  conformado por las funciones racionales  $i$ -homogéneas de grado 0 para todo  $i \in I$ ;  $K$  resulta ser un subcuerpo estricto de  $\mathbb{k}(X)$  (¿por qué?), luego  $\mathbb{k}(X)$  es un  $K$ -espacio vectorial. Finalmente denotamos por  $V$  al  $K$ -subespacio de  $\mathbb{k}(X)$  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  $v \in B_i$ .  $\square$

**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.  $\square$

**Ejemplo 3.29** (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.  $\lrcorner$

**Teorema (AE) 3.30:** 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  $f: Y \rightarrow X \times \mathbb{N}$  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  $g: X \times \mathbb{N} \rightarrow X$ , luego  $f \circ g: Y \rightarrow X$  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.  $\square$

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 3.31:** 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  $B := \{[v] : v \in B_V \setminus B_W\}$  conserva el cardinal deseado y que es base de  $V/W$ . Sean  $u, v \in B_V \setminus B_W$ , si  $[u] = [v]$  entonces  $u - v \in W$ , 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  $[v] \in V/W$  se escribe como

$$v = \sum_{i=1}^n \lambda_i e_i$$

donde  $e_i \in B_V$ , luego

$$[v] = \sum_{i=1}^n \lambda_i [e_i],$$

donde  $[e_i]$  o pertenece a  $B$ , o es nulo, en cuyo caso podemos omitirlo. 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  $V = \langle B \rangle = W$ .  $\square$

**Teorema 3.32 – 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 3.33:** Si  $f : V \rightarrow W$  es lineal, entonces

$$\dim V = \dim(\ker f) + \dim(\operatorname{Im} f).$$

### 3.3 Matrices y transformaciones lineales

**Teorema 3.34:** Sea  $f : X \rightarrow N$  donde  $X$  es base de un  $A$ -módulo  $M$  y  $N$  es otro  $A$ -módulo. Entonces existe un único homomorfismo de módulos  $\tilde{f} : M \rightarrow N$  tal que  $\tilde{f}|_X = f$ .

**Teorema 3.35:** 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  $\dim \operatorname{Im} f = n$ .

**Corolario 3.35.1:** 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  $\pi_i^B : M \rightarrow A$  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  $\pi_i^B$  están bien definidas. Se define  $\pi^B : M \rightarrow A^I$  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  $X := (x_1, \dots, x_n)$  es base ordenada de  $M$ , entonces

1. Para todo  $i$  se cumple que  $\pi_i^X$  es un funcional.
2. Para todo  $i, j$  se cumple que  $\pi_i^X(x_j) = \delta_{ij}$ .
3.  $\pi^X$  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  $f : M \rightarrow N$  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 síntesis, 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  $M : \{1, \dots, n\} \times \{1, \dots, m\} \rightarrow A$ , 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  $\text{Mat}_{n \times m}(A)$ . El conjunto  $\text{Mat}_{n \times m}(A)$  es un  $A$ -módulo, en donde:

1.  $(B + C)_{ij} := B_{ij} + C_{ij}$  para todo  $B, C \in \text{Mat}_{n \times m}(A)$ .
2.  $(\lambda B)_{ij} := \lambda B_{ij}$  para todo  $B \in \text{Mat}_{n \times m}(A)$  y  $\lambda \in A$ .

La diagonal de una matriz se le llama al conjunto de coeficientes de

coordenadas  $(i, i)$ .

Si  $B \in \text{Mat}_{n \times m}(A)$  y  $C \in \text{Mat}_{m \times p}(A)$ , se define su producto interno como:

$$(B \cdot C)_{ij} := \sum_{k=1}^m B_{ik} C_{kj}$$

Dado  $B \in \text{Mat}_{n \times m}(A)$  se define su **matriz traspuesta** como  $B^t \in \text{Mat}_{m \times n}(A)$  tal que  $(B^t)_{i,j} := B_{j,i}$ .

Se les llama matrices:

**Cuadradas** A las de orden  $n \times n$ . Se denota  $\text{Mat}_n(A) := \text{Mat}_{n \times n}(A)$ .

**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

$$M := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \in \text{Mat}_{2 \times 3}(\mathbb{Q})$$

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  $\text{Mat}_{1 \times n}(A)$ , de modo que  $\pi^X(v) \in \text{Mat}_{1 \times n}(A)$ .

**Proposición 3.39:**  $\text{Mat}_{n \times m}(A)$  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.  $\text{Mat}_n(A)$  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  $f \in L(\mathbb{k}^n, \mathbb{k}^m)$ , y  $X := (\mathbf{x}_1, \dots, \mathbf{x}_n)$ ,  $Y := (\mathbf{y}_1, \dots, \mathbf{y}_m)$  son bases ordenadas de  $\mathbb{k}^n$  y  $\mathbb{k}^m$  resp., entonces denotamos  $M_X^Y(f)$  a la matriz de orden  $n \times m$  a aquella tal que sus columnas son las imágenes ordenadas de la base  $X$ , dicho de otro modo que  $M_X^Y(f) := [\pi_j^Y(f(\mathbf{x}_i))]_{ij}$ .

**Teorema 3.43:** Sean  $f \in L(\mathbb{k}^n, \mathbb{k}^m)$ ,  $X$  e  $Y$  bases ordenadas de  $\mathbb{k}^n$  y  $\mathbb{k}^m$  resp., entonces  $B = M_X^Y(f)$  syss para todo  $\mathbf{v} \in \mathbb{k}^n$  se cumple:

$$\pi^Y(f(\mathbf{v})) = \pi^X(\mathbf{v}) \cdot B.$$

DEMOSTRACIÓN:  $\implies$ . Sea  $X = (\mathbf{x}_1, \dots, \mathbf{x}_n)$ ,  $\mathbf{v} = \sum_{i=1}^n v_i \mathbf{x}_i$  y  $B := M_X^Y(f)$ , luego como  $f$  es lineal se cumple que

$$f(\mathbf{v}) = \sum_{i=1}^n v_i f(\mathbf{x}_i).$$

Las proyecciones son también lineales, luego

$$\pi_j^Y(f(\mathbf{v})) = \sum_{i=1}^n v_i \pi_j^Y[f(\mathbf{x}_i)] = \sum_{i=1}^n v_i b_{ij} = (\pi^X(\mathbf{v}) \cdot B)_{1j},$$

como se quería probar.

$\Leftarrow$ . Si se cumple para todo vector, en particular se cumple para los vectores de la base  $X$  y claramente

$$(\mathbf{M}_X^Y(f))_{ij} = \pi_j^Y(f(\mathbf{x}_i)) = \sum_{k=1}^n \delta_{ik} b_{kj} = b_{ij}$$

ergo  $B = \mathbf{M}_X^Y(f)$ . □

**Ejemplo (matriz cambio de base).** Sea  $V$  un  $\mathbb{k}$ -espacio vectorial de dimensión  $n$ . Sean  $X, Y = (\mathbf{v}_1, \dots, \mathbf{v}_n)$  bases ordenadas de  $V$ , luego

$$\pi^X(\mathbf{v}_i) = \pi^X(\text{Id}(\mathbf{v}_i)) = \pi^Y(\mathbf{v}_i) \cdot \mathbf{M}_Y^X(\text{Id}) = \mathbf{e}_i \mathbf{M}_Y^X(\text{Id}) = [\mathbf{M}_X^Y(\text{Id})]_{i,*}.$$

**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.  $\mathbf{M}_X^X(\text{Id}) = I_n$ , donde  $n = |X|$ .
2. Para todo  $\lambda$  escalar se cumple  $\mathbf{M}_X^Y(\lambda f) = \lambda \mathbf{M}_X^Y(f)$ .
3.  $\mathbf{M}_X^Y(f + g) = \mathbf{M}_X^Y(f) + \mathbf{M}_X^Y(g)$ .
4.  $\mathbf{M}_X^Z(f \circ g) = \mathbf{M}_X^Y(f) \cdot \mathbf{M}_Y^Z(g)$ .
5. Son equivalentes:
  - a)  $f$  es invertible.
  - b) Para algún par de bases ordenadas  $X, Y$  se da que  $\mathbf{M}_X^Y(f)$  es invertible.
  - c) Para todo par de bases ordenadas  $X, Y$  se da que  $\mathbf{M}_X^Y(f)$  es invertible.
6.  $L(\mathbb{k}^n, \mathbb{k}^m) \cong \text{Mat}_{n \times m}(\mathbb{k}) \cong \mathbb{k}^{nm}$ . En particular,  $L(\mathbb{k}^n, \mathbb{k}) \cong \mathbb{k}^n$ .

Los últimos dos son los que justifican la definición de matrices.



**Ejemplo.** Si  $X, Y$  son bases ordenadas de  $\mathbb{k}^n$ , entonces

$$I_n = M_X^X(\text{Id}) = M_X^Y(\text{Id}) \cdot M_Y^X(\text{Id}).$$

Luego si  $B \in \text{Mat}_n(\mathbb{k})$  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

$$M_Y^Y(f) = M_Y^X(\text{Id}) \cdot M_X^X(f) \cdot M_X^Y(\text{Id}).$$

**Teorema 3.45:** Si  $B \in \text{Mat}_n(\mathbb{k})$ , entonces son equivalentes:

1.  $B$  es invertible.
2. Para todo  $v \in \mathbb{k}^n$  se cumple que  $v \cdot B = 0$  implica  $v = 0$ .

DEMOSTRACIÓN:  $\implies$ . Si  $B$  es invertible entonces sea  $B^{-1}$  su inversa, luego  $v = (v \cdot B)B^{-1} = 0 \cdot B^{-1} = 0$ .

$\impliedby$ . Si  $X$  es la base canónica, entonces  $f(v) := v \cdot B$  claramente es lineal y cumple que  $B = M_X^X(f)$  (¿por qué?). Si  $f^{-1}(0) = \{0\}$ , entonces  $\dim \ker f = 0$ , luego  $\dim \text{Im} f = n$  y  $f$  es una biyección, luego es invertible, y por el teorema anterior, cualquiera de sus representaciones matriciales (en particular,  $B$ ) lo son.  $\square$

### 3.4 Determinante

**Definición 3.46 – Forma multilineal:** Se dice que una función  $f : (A^n)^n \rightarrow A$  es una **forma multilineal** si es lineal coordenada a coordenada, es decir, si para todo  $v_1, \dots, v_n, v \in A^n$  y todo  $\lambda \in A$  se cumple que

$$f(v_1, \dots, v_i + \lambda v, \dots, v_n) = f(v_1, \dots, v_n) + \lambda f(v_1, \dots, v, \dots, v_n).$$

Además, una forma multilineal se dice **antisimétrica** si intercambiar dos vectores de coordenadas cambia el signo, es decir si

$$f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -f(v_1, \dots, v_j, \dots, v_i, \dots, v_n).$$

Y también se dice **alternada** si es nula si un vector aparece en más de

una coordenada, es decir si

$$f(v_1, \dots, \underset{(i)}{v}, \dots, \underset{(j)}{v}, \dots, v_n) = 0.$$

**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  $(v_1, \dots, v_n) \in (A^n)^n$  se cumple:

$$f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = (\text{sgn } \sigma) \cdot f(v_1, \dots, v_n).$$

**Teorema 3.48:** Para todo  $a \in A$  existe una única forma multilineal  $f$  tal que  $f(e_1, \dots, e_n) = a$ . Y de hecho, si todo  $v_i := (v_{i1}, \dots, v_{in})$ , entonces dicha forma multilineal viene dada por

$$f(v_1, \dots, v_n) = a \sum_{\sigma \in S_n} \text{sgn } \sigma \cdot v_{1\sigma(1)} \cdots v_{n\sigma(n)}.$$

DEMOSTRACIÓN: Utilizando la notación del enunciado  $v_i = \sum_{j=1}^n v_{ij}e_j$ , luego

$$\begin{aligned} f(v_1, \dots, v_n) &= \sum_{j=1}^n v_{1j} f(e_j, v_2, \dots, v_n) \\ &= \sum_{j_1=1}^n \sum_{j_2=1}^n v_{1j_1} v_{2j_2} f(e_{j_1}, e_{j_2}, v_3, \dots, v_n) \\ &= \sum_{j_1=1}^n \cdots \sum_{j_n=1}^n v_{1j_1} \cdots v_{nj_n} f(e_{j_1}, \dots, e_{j_n}). \end{aligned}$$

Notemos que podemos reemplazar los  $j_k$  por funciones desde  $\{1, \dots, n\}$  a  $\{1, \dots, n\}$ , 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:

$$\begin{aligned} f(v_1, \dots, v_n) &= \sum_{\sigma \in S_n} v_{1\sigma(1)} \cdots v_{n\sigma(n)} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) \\ &= a \sum_{\sigma \in S_n} \operatorname{sgn} \sigma \cdot v_{1\sigma(1)} \cdots v_{n\sigma(n)} \end{aligned} \quad \square$$

Nótese que en lugar de considerar el dominio como un espacio  $(A^n)^n$ , se puede reemplazar por  $\operatorname{Mat}_n(A)$  que es isomorfo.

**Definición 3.49 – Determinante:** Se define la función determinante  $\det: \operatorname{Mat}_n(A) \rightarrow A$  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  $\lambda$  tiene determinante  $\lambda \det B$ .
3. Sumarle a una columna (resp. fila)  $\lambda$ -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  $B, C \in \operatorname{Mat}_n(\mathbb{k})$  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,  $B = (B_1, \dots, B_n)$ , donde  $B_1 = (b_{11}, \dots, b_{1n})$ . Luego si  $B' := (B_1, \dots, B_u + \lambda v, \dots, B_n)$ ,  $D := BC$  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  $D'_{u,*} = D_{u,*} + \lambda(vC)_*$ , 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.  $\square$

**Definición 3.53 (Menor complemento):** Dada una matriz  $B \in \text{Mat}_n(A)$  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  $B \in \text{Mat}_n(A)$  con  $n > 1$ , entonces para todo  $i, j \leq n$  se cumple que

$$\det B = \sum_{k=1}^n (-1)^{i+k} b_{ik} M_{ik}(B) = \sum_{k=1}^n (-1)^{k+j} b_{kj} M_{kj}(B). \quad (3.1)$$

**Definición 3.55 (Matriz adjunta):** Dada una matriz  $B \in \text{Mat}_n(A)$  con  $n > 1$ , se le llama **matriz adjunta**, denotado  $\text{adj } B$ , a la matriz

$$\text{adj } B := [(-1)^{i+j} M_{ji}(B)]_{ij}.$$

**Teorema 3.56:** Para todo  $B \in \text{Mat}_n(D)$  con  $n > 1$  se cumple que

$$B \cdot \text{adj } B = \text{adj } B \cdot B = (\det B) \cdot I_n. \quad (3.2)$$

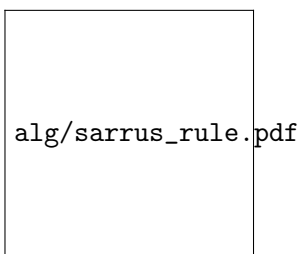
En consecuencia,  $B$  es invertible si y sólo si  $\det B$  es invertible, en cuyo caso,  $B^{-1} = \frac{1}{\det B} \text{adj } B$ . Si  $D$  es un cuerpo, la condición se reduce a notar

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.  $\text{adj} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$
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  $a_1, \dots, a_n \in A$ . 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:

$$\begin{aligned}
 \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} &= \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & 0 \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-2}(a_2 - a_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-2}(a_n - a_1) \end{vmatrix} \\
 &= \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & a_2 - a_1 & a_2(a_2 - a_1) & \cdots & a_2^{n-2}(a_2 - a_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n - a_1 & a_n(a_n - a_1) & \cdots & a_n^{n-2}(a_n - a_1) \end{vmatrix} \\
 &= \begin{vmatrix} a_2 - a_1 & a_2(a_2 - a_1) & \cdots & a_2^{n-2}(a_2 - a_1) \\ a_3 - a_1 & a_3(a_3 - a_1) & \cdots & a_3^{n-2}(a_3 - a_1) \\ \vdots & \vdots & \ddots & \vdots \\ a_n - a_1 & a_n(a_n - a_1) & \cdots & a_n^{n-2}(a_n - a_1) \end{vmatrix} \\
 &= (a_2 - a_1) \begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-2} \\ a_3 - a_1 & a_3(a_3 - a_1) & \cdots & a_3^{n-2}(a_3 - a_1) \\ \vdots & \vdots & \ddots & \vdots \\ a_n - a_1 & a_n(a_n - a_1) & \cdots & a_n^{n-2}(a_n - a_1) \end{vmatrix} \\
 &= (a_n - a_1) \cdots (a_2 - a_1) \begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-2} \\ 1 & a_3 & \cdots & a_3^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^{n-2} \end{vmatrix}
 \end{aligned}$$

finalmente concluimos por hipótesis inductiva.  $\square$

**§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  $\text{GL}(n, k) := \text{Mat}_n(k)^\times$  que, por el teorema anterior, corresponde al conjunto de matrices de determinante no nulo.

Dos matrices cuadradas  $A, B \in \text{Mat}_n(k)$  se dicen **similares** si existe  $C \in \text{GL}(n, k)$  tal que  $C^{-1}AC = B$ .

**Proposición 3.60:** Dos matrices  $A, B \in \text{Mat}_n(k)$  son similares si existe una base ordenada  $X := (\mathbf{v}_1, \dots, \mathbf{v}_n)$  tal que  $M_X^X(A) = B$ .

**Corolario 3.60.1:** Dos matrices similares comparten determinante.

PISTA: Se sigue del teorema 3.52. □

**Definición 3.61:** Dada una matriz  $B \in \text{Mat}_n(\mathbb{k})$  se define su **traza** como

$$\text{tr } B := \sum_{k=1}^n b_{kk}.$$

**Proposición 3.62:** Sean  $A, B \in \text{Mat}_n(\mathbb{k})$  y  $\lambda \in \mathbb{k}$ , entonces:

1.  $\text{tr}(A^t) = \text{tr } A$ .
2.  $\text{tr}(\lambda A) = \lambda \text{tr } A$ .
3.  $\text{tr}(A + B) = \text{tr } A + \text{tr } B$ .
4.  $\text{tr}(AB) = \text{tr}(BA)$ .

DEMOSTRACIÓN: Todas son triviales exceptuando la última:

$$\text{tr}(AB) = \sum_{k=1}^n (A \cdot B)_{kk} = \sum_{k=1}^n \sum_{j=1}^n a_{kj} b_{jk} = \sum_{j=1}^n \sum_{k=1}^n b_{jk} a_{kj} = \text{tr}(BA). \quad \square$$

**Corolario 3.62.1:** 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 3.63:** Dada una matriz  $B \in \text{Mat}_n(\mathbb{k})$ , se define su **polinomio característico** como

$$\psi_B(x) := \det(x \cdot I_n - B) \in k[x].$$

**Proposición 3.64:** Dos matrices similares comparten polinomio característico.

**Proposición 3.65:** Sea  $A \in \text{Mat}_n(\mathbb{k})$  y sea  $\psi_A(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in \mathbb{k}[x]$ . Entonces  $\det A = (-1)^n c_0$  y  $\text{tr } A = -c_{n-1}$ .

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.  $\square$

### §3.4.2 Rango de matrices.

**Definición 3.66:** Dada  $A \in \text{Mat}_{n \times m}(\mathbb{k})$  se le dice *rango por filas* (resp. por columnas) a la dimensión del subespacio generado por sus vectores fila (resp. vectores columna).

**Lema 3.67:** 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  $A \in \text{Mat}_{n \times m}(\mathbb{k})$ . Sin pérdida 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.  $\square$

**Definición 3.68:** Se le dice **rango**, denotado  $\text{rang}(A)$ , de una de una matriz  $A$  al rango por filas o columnas.

**Corolario 3.68.1:** Para toda matriz  $A$  se cumple que  $\text{rang}(A) = \text{rang}(A^t)$ .

**Teorema 3.69:** Dada  $A \in \text{Mat}_{n \times m}(\mathbb{k})$  cualquiera, y sean  $B \in \text{Mat}_n(\mathbb{k})$  y  $C \in \text{Mat}_m(\mathbb{k})$  invertibles. Entonces  $\text{rang}(A) = \text{rang}(BA) = \text{rang}(AC)$ .

De éste modo también podemos definir el rango para transformaciones lineales ya que sería independiente de la base.

**Proposición 3.70:** Una matriz de  $n \times n$  es invertible syss tiene rango  $n$ .

**Teorema 3.71:** Si  $A \in \text{Mat}_{n \times m}(\mathbb{k})$  y  $B \in \text{Mat}_{m \times p}(\mathbb{k})$ , entonces

$$\text{rang}(AB) \leq \text{rang}(A), \quad \text{rang}(AB) \leq \text{rang}(B).$$

Nótese que en este sentido el rango de una matriz sirve como indicador de qué tan «invertible» es.

**Definición 3.72:** Dada una matriz  $A \in \text{Mat}_{n \times m}(R)$ . Una submatriz  $B$  está dado por un par de inyecciones  $\sigma: \{1, \dots, n'\} \rightarrow \{1, \dots, n\}$  y  $\tau: \{1, \dots, m'\} \rightarrow \{1, \dots, m\}$  tal que  $B = [A_{\sigma(i), \tau(j)}]_{ij} \in \text{Mat}_{n' \times m'}(R)$ .

Por ejemplo, si consideramos

$$A := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

entonces algunas de sus submatrices son:

$$\begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix}, \quad \begin{bmatrix} 2 & 3 \\ 8 & 9 \end{bmatrix}.$$

Esta definición puede parecer extraña, pero es útil para lo siguiente:

**Proposición 3.73:** 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  $\text{rang } A \geq n$ . Por otro lado, si  $\text{rang } A = m$ , 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  $\text{rang } A \leq m$ .  $\square$

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. §10.2.3).

### 3.5 Los grupos de matrices

Ya hemos visto que, en general, el grupo de matrices inversibles  $\text{GL}_n(A)$  de tamaño  $n \times n$  con coeficientes en un anillo  $A$  forman un grupo; estos pueden ser de interés particular en la teoría de grupos. Veamos otro ejemplo:

**Definición 3.74:** Sea  $A$  un anillo. Una matriz  $B \in \text{Mat}_n(A)$  se dice *unitriangular* si es triangular superior y tiene puros 1's en su diagonal. Denotaremos por  $\text{UT}_n(A)$  el conjunto de matrices unitriangulares de tamaño  $n \times n$ .

Así, por ejemplo,  $B = \begin{bmatrix} 1 & b_{12} & b_{13} \\ 0 & 1 & b_{23} \\ 0 & 0 & 1 \end{bmatrix}$  es la forma general de una matriz unitriangular de  $3 \times 3$ .

**Proposición 3.75:** Para todo anillo  $A$  y  $n \in \mathbb{N}_{\neq 0}$ , se cumple que  $\text{UT}_n(A)$  es un subgrupo de  $\text{GL}_n(A)$ .

**Proposición 3.76:** Sea  $k$  un cuerpo finito de cardinalidad  $q$ . Para todo  $n \geq 2$  el grupo  $\text{UT}_n(k)$  tiene cardinalidad  $q^{\binom{n}{2}} = q^{n(n-1)/2}$ .

**Proposición 3.77:** Sea  $p$  un primo impar. Entonces, siempre existe un grupo no abeliano  $G$  de cardinalidad  $p^3$  tal que  $g^p = 1$  para todo  $g \in G$ .

**Teorema 3.78:** Sea  $k$  un cuerpo finito de cardinalidad  $q$ . Entonces

$$|\text{GL}_n(k)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

**Corolario 3.78.1:** Sea  $k$  un cuerpo finito de cardinalidad  $q = p^e$  potencia de un primo  $p$ .<sup>2</sup> Entonces el grupo unitriangular  $\text{UT}_n(k)$  es un  $p$ -subgrupo de Sylow de  $\text{GL}_n(k)$ .

**Corolario 3.78.2:** Sea  $p$  un número primo y sea  $G$  un  $p$ -grupo. Entonces  $G$  es isomorfo a un subgrupo de  $\text{UT}_{|G|}(\mathbb{F}_p)$ .

## 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*.

---

<sup>2</sup>Más adelante veremos que todo cuerpo es de esta forma.



Parte II.

---

# TEORÍA DE ANILLOS Y MÓDULOS

---



---

## 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*:

$$\begin{array}{c} K \\ g \downarrow \\ k \end{array}$$

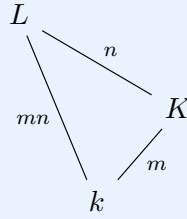
Dada una extensión  $K$  del cuerpo  $k$ , un elemento  $\alpha \in K$  se dice  **$k$ -algebraico** si existe  $f \in k[x]$  tal que  $f(\alpha) = 0$ , de lo contrario se dice  **$k$ -trascendente**. Una extensión  $K$  se dice  **$k$ -algebraica** si todos sus elementos lo son, de lo contrario,  $K$  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  $S := \{1, \alpha, \dots, \alpha^n\}$ . Si alguna potencia de  $\alpha$  se repite, digamos  $\alpha^i = \alpha^j$ , entonces  $f(x) := x^j - x^i$  hace algebraico a  $\alpha$ . 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

$$\sum_{i=0}^n c_i \alpha^i = c_n \alpha^n + \dots + c_1 \alpha + c_0 = 0,$$

pero luego  $f(x) := \sum_{i=0}^n c_i x^i$  es claramente un polinomio que hace que  $\alpha$  sea algebraico; por ende,  $K$  es algebraico.  $\square$

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 irreducibles 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  $\alpha$  es una raíz de  $f$  en  $K$ . □

Cabe destacar que diremos que un elemento es una **raíz cuadrada** de  $a$  si 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 esto 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  $\alpha$  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  $\alpha$  (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 irreducible  $f(x) \in k[x]$  tal que  $f(\alpha) = 0$ . Al que llamaremos **polinomio minimal** de  $\alpha$  sobre  $k$ .
2. Si  $g(x) \in k[x]$  cumple que  $g(\alpha) = 0$ , entonces  $f(x) \mid g(x)$ .

3.  $\text{ev}_\alpha [k[x]] = \text{ev}_\alpha [k(x)] = \{r(\alpha) : r(x) \in k[x] \wedge \deg r < \deg f\}$
4.  $k(\alpha)/k$  es una extensión finita, de hecho  $[k(\alpha) : k] = \deg f =: n$  y  $\{1, \alpha, \dots, \alpha^{n-1}\}$  es base para  $k(\alpha)$ .

DEMOSTRACIÓN:

1. Consideremos  $\pi := \text{ev}_\alpha : k[x] \rightarrow k(\alpha)$  dada por  $\pi(g(x)) = g(\alpha)$ . Claramente  $\pi$  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 irreducible.
2. Supongamos que  $g(x)$  tiene a  $\alpha$  de raíz, entonces  $g(x) \in \ker \pi = (f(x))$ , luego  $f(x) \mid g(x)$ . Si  $g(x)$  es irreducible, 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  $f(x)$ .  $\square$

El teorema anterior nos dice que en un sentido  $k(\alpha)$  es la *mínima* extensión de cuerpos que contiene a  $\alpha$ . En el teorema 4.11 veremos una generalización del teorema anterior que no depende del cuerpo base.

**Corolario 4.7.1:** 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  $\alpha$ . 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  $[k(\beta)(\alpha) : k(\beta)] = \deg g \leq \deg f = [k(\alpha) : k]$ .  $\square$

**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

$$g(a + b\sqrt{2}) = a^2 + 2ab\sqrt{2} + 2b^2 - 3$$

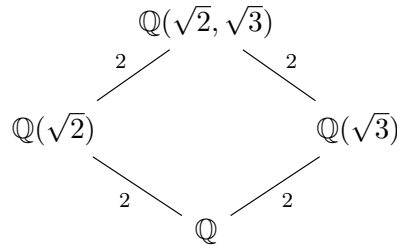
como  $\mathbb{Q}(\sqrt{2})$  es un  $\mathbb{Q}$ -espacio vectorial de base  $\{1, \sqrt{2}\}$  se concluye que

$$\begin{aligned} a^2 + 2b^2 - 3 &= 0, \\ 2ab &= 0. \end{aligned}$$

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

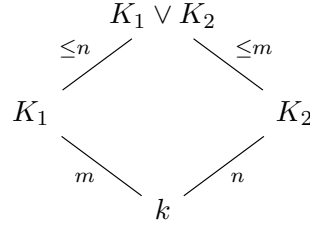
$$r(x) := 2x^2 - 3 = 0$$

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 4.8:** 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.

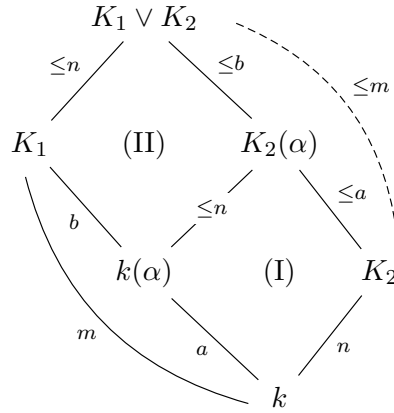
**Proposición 4.9:** Sean  $L/K_1/k$  y  $L/K_2/k$  extensiones de cuerpo con  $K_1, K_2$  finitas. Entonces se satisface el siguiente diagrama de retículos:



DEMOSTRACIÓN: Lo demostraremos por inducción fuerte sobre  $n + m$ : El caso base  $1 + 1$  es trivial, ya que  $K_1 = K_2 = k$  y  $K_1 \vee K_2 = k$ .

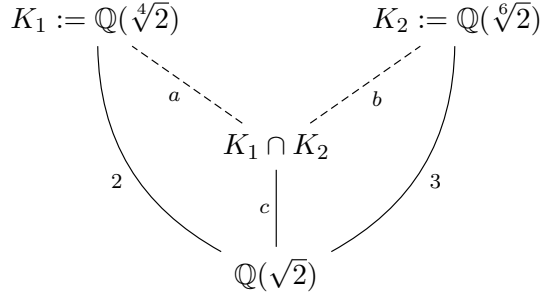
Hagamos la siguiente observación: Si  $K_1 = k(\alpha)$ , entonces el enunciado se satisface. La demostración es la misma del corolario 4.7.1, se toma el polinomio minimal de  $\alpha$  y se nota que es también tiene raíz en  $K_1 \vee K_2 = K_2(\alpha)$  como polinomio de  $K_2$ .

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:



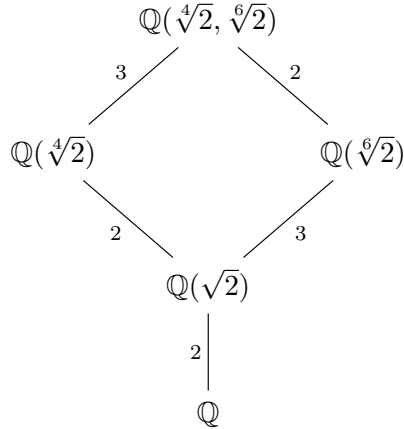
donde el diamante (I) sale de la observación, mientras que el diamante (II) sale por hipótesis inductiva.  $\square$

**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  $\mathbb{Q}(\sqrt[6]{2})$  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  $\leq 2$ . Por ende el diagrama de retículos se ve así:



y en conclusión  $[\mathbb{Q}(\sqrt[6]{2}, \sqrt[4]{2}) : \mathbb{Q}] = 12$

**Teorema 4.10:** Si  $L/K/k$  son extensiones de cuerpos, entonces  $L/k$  es algebraica syss  $L/K$  y  $K/k$  lo son.

DEMOSTRACIÓN:  $\implies$ . Si  $L/k$  es algebraica, claramente  $K/k$  lo es y como  $k$  es subcuerpo de  $K$  se comprueba que  $L/K$  lo es.

$\impliedby$ . Si  $\alpha \in L$  entonces  $\alpha$  es  $K$ -algebraico, luego sean  $\beta_1, \dots, \beta_n$  los coeficientes de su polinomio minimal, luego  $\alpha$  es algebraico sobre  $k(\beta_1, \dots, \beta_n)$ , por ende  $k(\beta_1, \dots, \beta_n)[\alpha]/k(\beta_1, \dots, \beta_n)$  es finita, y como los  $\beta_i$  son  $k$ -algebraicos, entonces  $k(\beta_1, \dots, \beta_n)/k$  es finito, finalmente  $k(\beta_1, \dots, \beta_n, \alpha)/k$  es finito y luego algebraico.  $\square$

**Corolario 4.10.1:** Si  $K/k$  es una extensión de cuerpos, entonces el conjunto de elementos algebraicos de  $K$  es un cuerpo.

DEMOSTRACIÓN: Basta notar que si  $\alpha, \beta$  son algebraicos sobre  $K$ , entonces  $k(\alpha, \beta)/k$  es finita, luego algebraica y por ende  $\alpha + \beta$ ,  $\alpha \cdot \beta$  y  $\alpha/\beta$  (si  $\beta \neq 0$ ) lo son.  $\square$

**Teorema 4.11:** Sean  $K/k$  y  $L/\ell$  extensiones de cuerpo con  $\sigma: k \rightarrow \ell$  un isomorfismo de cuerpo, que induce un morfismo de anillos  $\sigma: k[x] \rightarrow \ell[x]$ . Si  $\alpha \in K$  es algebraico, entonces sea  $f \in k[x]$  su polinomio minimal. Si  $L$  contiene una raíz  $\beta$  de  $\sigma f(x)$ , entonces  $\sigma$  se extiende un isomorfismo de extensiones  $\sigma^*: k(\alpha) \rightarrow \ell(\beta)$  con  $\sigma^*(\alpha) = \beta$ , es decir, existe un  $\sigma^*$  tal que el siguiente diagrama

$$\begin{array}{ccccc}
 & & k[x] & \xrightarrow{\sim \sigma \sim} & \ell[x] \\
 & \swarrow \iota & \downarrow \text{ev}_\alpha & & \downarrow \text{ev}_\beta & \nwarrow \iota \\
 k & & & & & \ell \\
 & \searrow \iota & & & & \swarrow \iota \\
 & & k(\alpha) & \xrightarrow{\sim \sigma^* \sim} & \ell(\beta)
 \end{array}$$

conmuta (en Ring).

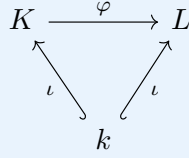
DEMOSTRACIÓN: Sea  $\phi: k[x] \rightarrow k[\alpha]$  el morfismo de evaluación, i.e., tal que  $\phi(g) = g(\alpha)$ . Es claro que  $\ker \phi$  es el ideal  $(f(x))$ , luego por el primer teorema de isomorfismos  $k[x]/(f(x)) \cong k[\alpha]$ .

En primer lugar veamos que  $\sigma f(x)$  ha de ser el polinomio minimal de  $\beta$  en  $\ell$ . Luego, análogamente  $\ell[x]/(\sigma f(x)) \cong \ell[\beta]$ .

Finalmente  $\omega: k[x] \rightarrow \ell[x]$  que fija a la identidad induce un isomorfismo  $k[x]/(f(x)) \cong \ell[x]/(\sigma f(x))$ , de lo que se concluye que  $k[\alpha] \cong \ell[\beta]$ .  $\square$

Ésto nos motiva a formular la siguiente definición:

**Definición 4.12:** Sean  $K/k$  y  $L/k$  extensiones de cuerpo. Entonces decimos que una función  $\varphi: K \rightarrow L$  es 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  $\text{Ext}_k$ .

Se le llama **grupo de Galois** de  $K$ , denotado por  $\text{Gal}(K/k)$ , al conjunto  $\text{Aut}_{\text{Ext}_k}(K)$ ; vale decir,  $\text{Gal}(K/k)$  son los  $k$ -automorfismos de  $K$ .

**Corolario 4.12.1:** Sea  $K/k$  una extensión de cuerpo, donde  $K = k(\alpha)$  y  $f(x) \in k[x]$  es el polinomio minimal de  $\alpha$ . Entonces  $|\text{Gal}(K/k)|$  es la cantidad de raíces distintas de  $f(x)$ ; en particular,

$$|\text{Gal}(K/k)| \leq [K : k],$$

donde  $|\text{Gal}(K/k)| = [K : k]$  syss  $f(x)$  se factoriza en distintos polinomios lineales.

DEMOSTRACIÓN: Sean  $\alpha_1, \dots, \alpha_n$  todas las raíces de  $f(x)$  en  $K$ . Por el teorema anterior siempre existe un único  $k$ -automorfismo  $\sigma_{ij}: k(\alpha_i) \rightarrow k(\alpha_j)$  tal que  $\sigma_{ij}(\alpha_i) = \alpha_j$ . Así pues, para cada  $j$  notemos que  $\sigma_{1j}$  es un  $k$ -automorfismo distinto, por lo que  $|\text{Gal}(K/k)| \geq n$ . Al mismo tiempo si  $\sigma$  es un  $k$ -automorfismo, entonces  $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$ , de modo que  $\sigma(\alpha) = \alpha_i$ , pero el teorema anterior prueba la unicidad de  $\sigma$ , con lo que  $|\text{Gal}(K/k)| = n$ . Como  $n \leq \deg f$  se comprueba la desigualdad.

Ya vimos que  $|\text{Gal}(K/k)|$  es la cantidad de raíces de  $f(x)$ , así que la equivalencia es clara.  $\square$

**Definición 4.13 ( $k$ -conjugados):** Dados  $\alpha, \beta$  algebraicos sobre  $k$ , se dice que son  $k$ -conjugados si comparten el polinomio minimal.

**Teorema 4.14:** Dados  $\alpha, \beta$  algebraicos sobre  $k$ , entonces son  $k$ -conjugados syss existe un  $k$ -isomorfismo  $\sigma: k(\alpha) \rightarrow k(\beta)$  tal que  $\sigma(\alpha) = \beta$ . Más aún,  $\sigma(\alpha)$  siempre es un  $k$ -conjugado de  $\alpha$ .

**Ejemplo.** El polinomio ciclotómico  $p$ -ésimo, con  $p > 2$ , es irreducible luego carece de raíces, así que construyamos  $\mathbb{Q}(\omega)$  donde  $\omega$  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  $\omega^2$  también es raíz de  $\Phi_p(x)$ . De hecho, se concluye que todas las raíces de  $\Phi_p(x)$  son  $\omega^1, \omega^2, \dots, \omega^{p-1}$ ; luego ellos son  $k$ -conjugados.

**Teorema 4.15:** Si  $K/k$  es finito, entonces  $\text{Gal}(K/k)$  también.

DEMOSTRACIÓN: Sea  $S := \{\alpha_1, \dots, \alpha_n\}$  tal que  $K = k(S)$ . Sea  $\sigma \in \text{Gal}(K/k)$  y  $f \in k[S]$ , como  $\sigma$  es un  $k$ -automorfismo se cumple  $\sigma(f(\alpha_1, \dots, \alpha_n)) = f(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$ . Notemos que todo elemento en  $K$  es de la forma  $f(\alpha_1, \dots, \alpha_n)$ , luego dos  $k$ -automorfismos coinciden si lo hacen en  $S$ .

Sea  $f_i$  el polinomio minimal de  $\alpha_i$ , 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  $\sigma$  sólo puede tomar finitos valores en  $\alpha_i$ . Finalmente sólo hay finitas posibilidades para  $\sigma$ , luego  $\text{Gal}(K/k)$  es finito.  $\square$

## 4.2 Extensiones normales y separables

### §4.2.1 Cuerpos de escisión.

**Definición 4.16:** Se dice que un polinomio  $f \in k[x]$  *se escinde*<sup>a</sup> en una extensión de cuerpos  $K/k$ , si existen  $\alpha_0, \alpha_1, \dots, \alpha_n \in K$  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  $K = k(\alpha_1, \dots, \alpha_n)$ .

<sup>a</sup>eng. *splits*.

**Teorema 4.17:** Si  $\sigma: k \rightarrow k'$  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  $\sigma$  a  $\bar{\sigma}: K \rightarrow K'$  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 irreducible. Lo haremos por inducción sobre el grado de  $f$ , donde el caso  $n = 1$  es trivial.

Sea  $f$  de grado  $n + 1$ , sea  $\alpha_{n+1}$  una raíz en  $K$  y sea  $\beta_{n+1}$  una raíz de  $\sigma(f)$  en  $K'$ . Como  $\alpha_{n+1}, \beta_{n+1}$  son  $k$ -conjugados, entonces existe  $\sigma^*: k(\alpha_{n+1}) \rightarrow k'(\beta_{n+1})$  que extiende a  $\sigma$ . 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  $\sigma^*$  (que extiende a  $\sigma$ ) tal que  $\bar{\sigma}: K \rightarrow K'$  es un isomorfismo de cuerpos.  $\square$

**Proposición 4.18:** 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.  $\square$

**EjemploCuerpos de escisión de distintos grados en base a polinomios de mismo grado.** 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  $\omega$  es alguna raíz de  $\Phi_7$ , 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 4.19 – Extensión normal:** Se dice que una extensión de cuerpos  $K/k$  es **normal** si para todo  $f \in k[x]$  irreducible con alguna raíz en  $K$  se escinde en  $K$ .

**Lema 4.20:** 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  $\sigma: K \rightarrow L$  es un  $k$ -monomorfismo se cumple que  $\sigma[K] \subseteq F$  y  $\sigma$  se extiende a un  $k$ -automorfismo de  $F$ , y en consecuencia, se extiende a un  $k$ -automorfismo de  $L$ . En diagramas conmutativos:

$$\begin{array}{ccc}
 F & \xrightarrow{\sim \sim \sim \sigma^* \sim \sim} & F \\
 \uparrow & & \uparrow \text{Id} \\
 K & \xrightarrow{\sigma} & F \\
 \uparrow & & \uparrow \\
 k & \xrightarrow{\text{Id}} & k
 \end{array}$$

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  $\bar{\sigma}: F \rightarrow F'$  es un  $k$ -isomorfismo que extiende a  $\sigma$ .

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  $\alpha_i$ s 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  $\alpha_i$ , de modo que  $F' = \bar{\sigma}(F) \subseteq F$ . En consecuencia  $F' = F$  y  $\bar{\sigma}$  es un  $k$ -automorfismo.  $\square$

**Teorema 4.21:** Una extensión finita  $K/k$  es normal si y sólo si es el cuerpo de escisión de algún polinomio.

DEMOSTRACIÓN:  $\Leftarrow$ . Sea  $f(x) \in k[x]$  el polinomio tal que  $K$  es su cuerpo de escisión. Sea  $g(x) \in k[x]$  irreducible 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  $\alpha_i$  y  $\alpha$  son  $k$ -conjugados, existe  $\sigma: k(\alpha) \rightarrow k(\alpha_i) \subseteq L$  un  $k$ -isomorfismo, luego por el lema  $k(\alpha_i) \subseteq K$ , y como los  $\alpha_i \in K$ ,  $g(x)$  se escinde en  $K$ .

$\Rightarrow$ . 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  $\alpha_i$  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.  $\square$

**Definición 4.22:** 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 4.23:** Toda extensión finita posee una clausura normal que es única salvo isomorfismo.

DEMOSTRACIÓN: Sea  $K = k(\alpha_1, \dots, \alpha_n)$  y  $f_i(x) \in k[x]$  el polinomio minimal de  $\alpha_i$  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.  $\square$

#### §4.2.2 Extensiones separables.

**Definición 4.24 (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 4.25:** 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.  $(f/g)' = \frac{f'g - fg'}{g^2}$ .

**Definición 4.26:** Se dice que la *multiplicidad* de una raíz  $\alpha$  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 4.27:** Dado  $D$  un dominio íntegro y  $\alpha$  raíz de  $f(x) \in D[x]$ .  $\alpha$  es una raíz simple syss  $f'(\alpha) \neq 0$ .

DEMOSTRACIÓN: Supongamos que el grado de  $\alpha$  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  $\alpha$  es una raíz simple.  $\square$

**Definición 4.28:** 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 4.29:** Un cuerpo que posee una extensión que no es separable. Un cuerpo no perfecto. 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  $\omega$  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  $\omega$  no lo es.  $\lrcorner$

**Proposición 4.30:** Sea  $k$  un cuerpo de característica  $p$ . Entonces  $\text{Frob}_k(a) = a^p$  es un endomorfismo, conocido como el *endomorfismo de Frobenius*. Y si  $\text{Frob}_k$  es suprayectivo, entonces  $\text{Frob}_k$  es un automorfismo.

**Proposición 4.31:** Sea  $D$  un dominio íntegro y  $f(x) \in D[x]$  un polinomio no constante, entonces:

1. Si  $\text{car } D = 0$ , entonces  $f'(x) \neq 0$ .
2. Si  $\text{car } D = p$ , entonces  $f'(x) = 0$  si y sólo si  $f(x) = g(x^p)$  con  $g(x) \in D[x]$ .

**Teorema 4.32:** Se cumple:

1. Todo cuerpo de característica nula es perfecto.
2. Si  $\text{car } k = p$ , entonces  $k$  es perfecto si y sólo si  $\text{Frob}_k$  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.  $\Leftarrow$ . 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  $\text{Frob}_k$  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 irreducible, contradicción.

$\Rightarrow$ . 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. 4.29 vimos que la extensión  $\mathbb{F}_p(t, \omega)$  no es separable, pero esto 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 4.33:** 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,  $(\text{Frob}_k)^n(x) = x^{p^n} = x$  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  $L \cong K$ .  $\square$

Denotamos por  $\mathbb{F}_{p^n}$  al único cuerpo de cardinalidad  $p^n$  salvo isomorfismo.

**Teorema 4.34:** Sea  $L/k$  una extensión finita de cuerpos. Son equivalentes:

1.  $L/k$  es separable.
2.  $L = k(\alpha_1, \dots, \alpha_n)$  donde cada  $\alpha_i$  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  $\text{Gal}(K/k)$ . En el teorema 4.15 vimos que ha de ser finito en extensiones finitas y el teorema 4.14 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 4.35:** Sea  $K/k$  una extensión finita, entonces se denota por  $N(K/k)$  a la cantidad de  $k$ -monomorfismos desde  $K$  hasta su clausura normal.

**Proposición 4.36:** Sea  $\alpha$  algebraico, entonces  $N(k(\alpha)/k) = [k(\alpha) : k]$  si  $\alpha$  es separable y  $N(k(\alpha)/k) < [k(\alpha) : k]$  si no.

En general nos enfocaremos en cuerpos separables, pero aún así le dedicaremos un par de teoremas al caso inseparable:

**Teorema 4.37:** Sea  $k$  un cuerpo de 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  $\alpha$  de  $f(x)$  (en alguna extensión  $K/k$ ) se cumple que  $\alpha^q$  es separable en  $k$ .
2. Todas las raíces de  $f(x)$  son separables en  $k(\beta_1, \dots, \beta_n)$ , donde los  $\beta_i$ '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  $\alpha_i$  son las raíces distintas de  $f(x)$  y  $m_i > 0$ . Sea  $\sigma \in \text{Gal}(N/k)$ , 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  $\alpha$  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  $\alpha^q$  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.  $\square$

**Corolario 4.37.1:** 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  $p = \text{car } k$ .

**Corolario 4.37.2:** Sea  $k$  un cuerpo de  $\text{car } k =: p \neq 0$  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 4.38 – Extensión de Galois:** Se dice que  $K/k$  es una extensión de Galois si es normal y separable.

Sea  $H \leq \text{Gal}(K/k)$ , 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

$$H_L := \{\sigma \in \text{Gal}(K/k) : \forall a \in L \sigma(a) = a\}.$$

Nótese que para  $\mathbb{Q}$  basta que una extensión sea normal para que sea de Galois.

**Teorema 4.39:** Sea  $L/K/k$  una extensión normal, entonces  $N(L/k) = N(L/K)N(K/k)$ .

DEMOSTRACIÓN: En ésta demostración  $N$  representa la clausura normal de  $K$ , de modo que  $N(K/k) := |\text{Hom}_k(K, N)|$ . Nótese que  $L/K$  y  $L/k$  son normales, de modo que  $N(L/K) = |\text{Gal}(L/K)|$ .

Sea  $\sigma \in \text{Hom}_k(K, N)$ , por el lema 4.20 se ha de cumplir que  $\sigma$  se extiende a un  $k$ -automorfismo  $\sigma^* \in \text{Gal}(L/k)$ , por lo tanto, el problema se reduce a ver que hay  $N(L/K)$  posibles extensiones.

Sean  $\tau_1, \tau_2$  dos posibles extensiones de  $\sigma$ . Es decir,  $\tau_1, \tau_2$  son  $k$ -automorfismos de  $L$ , pero entonces  $\tau_1 \circ \tau_2^{-1} : L \rightarrow L$  es un  $k$ -automorfismo que de hecho fija a  $K$ , es decir,  $\tau_1 \circ \tau_2^{-1} \in \text{Gal}(L/K)$ . Y así podemos concluir.  $\square$

**Teorema 4.40:** Sea  $K/k$  una extensión finita. Entonces:



1.  $|\text{Gal}(K/k)| \leq N(K/k)$ .
2. Si  $K/k$  es separable, entonces  $N(K/k) = [K : k]$ .
3. Si  $K/k$  no es separable, entonces  $N(K/k) \mid [K : k]$ .
4. Si  $K/k$  es de Galois, entonces  $|\text{Gal}(K/k)| = [K : k]$ .

DEMOSTRACIÓN: Si  $K$  es de Galois, entonces sea  $K = k(\alpha_1, \dots, \alpha_n)$ . Luego aplicando el teorema anterior se tiene que

$$\begin{aligned}
 N(K/k) &= N(K/k(\alpha_1, \alpha_2)) N(k(\alpha_1, \alpha_2), k) \\
 &= N(K/k(\alpha_1, \alpha_2)) N(k(\alpha_1, \alpha_2), k(\alpha_1)) N(k(\alpha_1), k) \\
 &= N(K/k(\alpha_1, \alpha_2)) [k(\alpha_1, \alpha_2) : k(\alpha_1)] [k(\alpha_1) : k] \\
 &= N(K/k(\alpha_1, \alpha_2)) [k(\alpha_1, \alpha_2) : k].
 \end{aligned}$$

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

$$[N : k] = N(N/k) = N(N/K) N(K/k) \leq [N : K] N(K/k),$$

por lo que se concluye que también aplica.  $\square$

Una pregunta curiosa sería ver si el converso es cierto. La respuesta es que sí y la veremos en un teorema más adelante.

**Teorema 4.41 – 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 4.67 más adelante) por lo que tiene un generador  $\gamma$  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  $(\alpha', \beta')$ , donde  $\alpha', \beta'$  son  $k$ -conjugados de  $\alpha$  y  $\beta$  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  $\sigma, \tau$  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,  $\gamma$  posee  $N(K/k)$  conjugados. Pero como  $K$  es separable, entonces vemos que

$$[k(\gamma) : k] = N(k(\gamma)/k) = N(K/k) = [K : k].$$

Luego, como  $K/k(\gamma)$  es una extensión de cuerpos de dimensión 1 se concluye la igualdad.  $\square$

**Corolario 4.41.1:** 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  $\alpha/\beta$  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  $\alpha^q$  es separable en  $L_s$  y luego lo es en  $k$ , y finalmente  $\alpha_q \in L_s$ .  $\square$

**Definición 4.42:** A  $L_s$  le decimos la *clausura separable* de  $k$  en  $L$ , es decir, al máximo subcuerpo tal que  $L_s/k$  es separable.

Podemos mejorar ligeramente el teorema del elemento primitivo:

**Teorema 4.43:** Sea  $k$  un cuerpo infinito, y sea  $K := k(\alpha, \beta)$  una finita extensión de cuerpos, donde  $\alpha$  es separable. Entonces  $K$  es simple.

DEMOSTRACIÓN: ...  $\square$

**Proposición 4.44:** Para toda extensión  $K/k$  y todo  $H \leq \text{Gal}(K/k)$  se cumple que  $F(H)$  es un cuerpo y  $k \leq F(H) \leq K$ .

**Teorema 4.45:** Una extensión finita  $K/k$  es de Galois syss

$$F(\mathrm{Gal}(K/k)) = k.$$

DEMOSTRACIÓN:  $\implies$  . Sea  $\alpha \in K$ , hemos de probar que existe un  $k$ -isomorfismo de  $K$  que mueve a  $\alpha$ . 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  $\beta$  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  $\alpha \in k$ .

$\Leftarrow$ . Sea  $\alpha \in K \setminus k$  de polinomio minimal  $f(x)$ . Sean  $\alpha_1, \dots, \alpha_n$  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  $q(x) \mid f(x)$  por construcción.

Sea  $\sigma \in \text{Gal}(K/k)$ . 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  $\sigma$  cualquiera, de modo que los coeficientes de  $q(x)$  *deben* estar en  $k$ .

Luego, como  $\alpha$  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).  $\square$

**Lema 4.46 (de independencia de Dedekind):** Sean  $\sigma_1, \dots, \sigma_n$  automorfismos de un cuerpo  $K$ . Si  $\sum_{i=1}^n c_i \sigma_i(a) = 0$  para todo  $a \in K$ , entonces  $c_1 = c_2 = \dots = c_n = 0$ .

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.  $\square$

**Teorema 4.47:** Sea  $K/k$  una extensión de cuerpos con  $H \leq \text{Gal}(K/k)$  entonces

$$[K : F(H)] = |H|.$$

En consecuencia,  $K/k$  finita es de Galois syss  $|\text{Gal}(K/k)| = [K : k]$ .

DEMOSTRACIÓN: Lo haremos por contradicción suponiendo que  $\{a_1, \dots, a_m\}$  es una  $F(H)$ -base de  $K$ , y  $H = \{\sigma_1, \dots, \sigma_n\}$ . Supongamos que  $m < n$ : Entonces la aplicación

$$f : K^n \longrightarrow K^m$$

$$(x_1, \dots, x_n) \longmapsto \left( \sum_{i=1}^n x_i \sigma_i(a_1), \sum_{i=1}^n x_i \sigma_i(a_2), \dots, \sum_{i=1}^n x_i \sigma_i(a_m) \right)$$

es lineal y  $n = \dim_K(K^n) = \dim(\ker f) + \dim(\text{Im} f) \leq \dim(\ker f) + m$ , de modo que  $\dim(\ker f) \neq 0$  y el kernel es no vacío y por ende posee un elemento  $(c_1, \dots, c_n) \neq \vec{0}$ . 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  $\lambda_i$  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  $(c_1, \dots, c_n)$ . 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:

$$f : K^{n+1} \longrightarrow K^n$$

$$(x_1, \dots, x_{n+1}) \longmapsto \left( \sum_{i=1}^{n+1} x_i \sigma_1(a_i), \dots, \sum_{i=1}^{n+1} x_i \sigma_n(a_i) \right)$$

tal que posee kernel no vacío y Elegimos  $(c_1, \dots, c_{n+1}) \neq \vec{0}$  que pertenezca al kernel tal que posea la máxima cantidad de coordenadas nulas, podemos

elegirlas de tal modo que  $c_1, \dots, c_p$  sean no nulos y  $c_{p+1}, \dots, c_{n+1}$  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  $\sigma_h$  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  $\sigma_h$  a las  $n$ -tuplas, de modo que

$$\forall j \in \{1, \dots, n\} \quad \sum_{i=1}^{n+1} \sigma_h(c_i) \sigma_j(a_i) = 0$$

finalmente notamos que

$$\forall j \in \{1, \dots, n\} \quad \sum_{i=1}^{n+1} (c_i - \sigma_h(c_i)) \sigma_j(a_i) = 0$$

por lo que  $d_i := c_i - \sigma_h(c_i)$  conforman una tupla del kernel. Sin embargo, nótese que  $d_p, d_{p+1}, \dots, d_n$  son todos nulos, contradiciendo la maximalidad de ceros de  $(c_1, \dots, c_{n+1})$ .  $\square$

**Corolario 4.47.1:** 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  $\text{Gal}(L/k) = \text{Gal}(L/L_i)$ .
4.  $[L : L_i] = [L_s : k]$  y  $[L : L_s] = [L_i : k]$ .

DEMOSTRACIÓN:

1. Sea  $K := F(\text{Gal}(L/k))$  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  $\sigma \in \text{Gal}(L/k)$  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  $\text{Gal}(L/k) = \text{Gal}(L/L_i)$  y también vimos que  $F(\text{Gal}(L/L_i)) = L_i$ , de modo que la extensión es de Galois por el teorema 4.45.
4. Nótese que  $[L : L_i] = |\text{Gal}(L/L_i)| = |\text{Gal}(L/k)| = [L_s : k]$  y la otra igualdad se sigue de la transitividad de grados.  $\square$

**Teorema 4.48 – Teorema fundamental de la teoría de Galois:**

Sea  $K/k$  una extensión finita de Galois. Denotando  $G := \text{Gal}(K/k)$  y

$$\{L : K/L/k \text{ extensiones}\} \xrightleftharpoons[F(H)]{\text{Gal}(K/L)} \{H : H \leq G\}$$

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  $k \subseteq L_1 \subseteq L_2 \subseteq K$ , entonces  $\text{Gal}(K/L_1) > \text{Gal}(K/L_2)$ . En consecuencia,  $F$  es un funtor contravariante biyectivo:

$$\begin{array}{ccc} L_2 & & H_2 \\ \uparrow & \xrightleftharpoons[\text{Gal}(K/L)]{} & \downarrow \\ L_1 & & H_1 \end{array}$$

2. Si  $K/L/k$ , entonces  $K/L$  es de Galois.
3. Si  $K/L/k$ , entonces  $L/k$  es de Galois syss  $\text{Gal}(K/L) \trianglelefteq G$ .
4. Si  $K/L/k$  y  $L/k$  es de Galois, entonces

$$\begin{aligned} r: \text{Gal}(K/k) &\longrightarrow \text{Gal}(L/k) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

es un epimorfismo de grupos y  $\ker r = \text{Gal}(K/L)$ . En consecuencia,  $\text{Gal}(K/k)/\text{Gal}(K/L) \cong \text{Gal}(L/k)$ .

5. Si  $H_1, H_2 \leq \text{Gal}(K/k)$ , 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  $F(\text{Gal}(K/L)) = L$ .

Por otro lado, sea  $H \leq \text{Gal}(K/k)$ , entonces claramente  $H \leq \text{Gal}(K/F(H))$ . Más aún  $K/F(H)$  es de Galois, por lo que  $|H| = [K : F(H)] = |\text{Gal}(K/F(H))|$ , y como  $H$  es finito, se da que  $\text{Gal}(K/F(H)) = H$ .

3.  $\implies$ . Si  $L/k$  es de Galois, entonces es normal. Sea  $\sigma \in \text{Gal}(K/L)$  y  $\tau \in \text{Gal}(K/k)$ , entonces  $\tau^{-1} \in \text{Gal}(K/k)$ . Sea  $\alpha \in L$ , nótese que  $\tau^{-1}$  manda  $\alpha$  a sus  $k$ -conjugados, luego  $\tau^{-1}(\alpha) \in L$ . Como  $\sigma$  fija a  $L$  se cumple que  $\sigma(\tau^{-1}(\alpha)) = \tau^{-1}(\alpha)$  y en consecuente,  $\tau(\sigma(\tau^{-1}(\alpha))) = \alpha$ , por lo que  $\tau^{-1}\sigma\tau \in \text{Gal}(K/L)$ . Es decir,  $\text{Gal}(K/L) \trianglelefteq \text{Gal}(K/k)$  por definición de subgrupo normal.

$\Leftarrow$ . 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  $\alpha$  están en  $L$ . Luego sea  $\beta$  un  $k$ -conjugado de  $\alpha$ , sabemos que existe  $\tau \in \text{Gal}(K/k)$  tal que  $\tau^{-1}(\alpha) = \beta$ .

Como  $F(\text{Gal}(K/L)) = L$ , basta ver que todo  $\sigma$  fija a  $\beta$ . Sea  $\sigma \in \text{Gal}(K/L)$ , entonces

$$\tau(\sigma(\tau^{-1}(\alpha))) = \tau(\sigma(\beta)) = \alpha \iff \sigma(\beta) = \tau^{-1}(\alpha) = \beta.$$

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  $F(H_2)$ .  $\square$

## 4.4 Cuerpos algebraicamente cerrados

**Lema 4.49:** 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 irreducibles 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:  $1 \implies 2$ . Sea  $f(x) \in K[x]$  un polinomio no constante, luego éste posee un factor irreducible  $g(x)$  de manera que existe una extensión  $K(\alpha)/K$  con una raíz  $\alpha$  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  $\alpha$  y por Ruffini se satisface que  $(x - \alpha) \mid f(x)$ , por lo que  $f(x)$  no es irreducible.

$3 \implies 4$ . 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  $\alpha$  es raíz de  $f(x)$ . Como  $K/k$  es algebraico, entonces  $K(c_0, \dots, c_n)$  es una extensión finita y claramente  $[K(c_0, \dots, c_n; \alpha) : K(c_0, \dots, c_n)] < \infty$  de modo que  $\alpha$  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  $L = K$ .  $\square$

**Definición 4.50 – 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 4.51:** 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 4.10) 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  $\alpha_i$  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.  $\square$

**Teorema 4.52:** Si  $k$  es finito, entonces no es algebraicamente cerrado. Conversamente, todo cuerpo algebraicamente cerrado es infinito.

DEMOSTRACIÓN: Si  $k$  es finito entonces sea  $k = \{\alpha_1, \dots, \alpha_n\}$ , 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.  $\square$

**Teorema (TUF) 4.53:** 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  $y_- : \mathcal{P} \rightarrow S$  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:

$$\mathfrak{a} := (f(y_p) : f(x) \in \mathcal{P}).$$

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  $\lambda_i$  posee finitos monomios, cada uno con finitas variables, en definitiva hay solo finitas variables en la ecuación anterior que podemos suponer son  $F := \{y_{f_1}, y_{f_2}, \dots, y_{f_n}, z_1, z_2, \dots, z_m\}$ .

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  $\alpha_i$  y  $z_j$  en 0 se obtiene que

$$\lambda_1(\alpha_1, \dots, \alpha_n, 0, \dots, 0) f_1(\alpha_1) + \cdots + \lambda_n(\alpha_1, \dots, \alpha_n, 0, \dots, 0) f_n(\alpha_n) = 1$$

donde cada término en rojo vale cero por definición de  $\alpha_i$ , 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.*)<sup>1</sup> 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,  $K_0 := \text{Frac}(k[S]/\mathfrak{p})$  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  $\alpha \in K_{n+1} \subseteq K$ .

<sup>1</sup>Idea original de BANASCHEWSKI [0] (1992).

5. Como  $K/k$  es algebraicamente cerrado, por el teorema 4.51 admite un subcuerpo que es una clausura algebraica de  $k$ , que es lo que se quería probar.  $\square$

**Teorema (AE) 4.54:** 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

$$\mathcal{F} := \{(L, \tau) : K_1/L/k \text{ extensión y } \tau : L \rightarrow K_2 \text{ } k\text{-morfismo}\},$$

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

$$L := \bigcup_{(K_i, \sigma_i) \in C} K_i$$

y  $\sigma : L \rightarrow K_2$  dado por  $\sigma(\alpha) = \tau_i(\alpha)$  donde  $\alpha \in K_i$  donde  $(K_i, \sigma_i) \in C$ . Así pues  $(L, \sigma)$  es una cota superior de  $C$  (¿por qué?).

Luego, por el lema de Zorn se cumple que  $\mathcal{F}$  tiene un elemento  $\subseteq$ -maximal  $(M, \sigma)$ . Veamos que  $M = K_1$ : Sea  $\alpha \in K_1$ , entonces  $\alpha$  es  $k$ -algebraico, luego es la raíz de un polinomio  $f(x)$ . Sea  $M' := \sigma[M] \subseteq K_2$ , se cumple que existe  $\beta$  raíz de  $\sigma f(x)$  (por ser algebraicamente cerrado). Luego, por el teorema se tiene que

$$\begin{array}{ccc} M(\alpha) & \xrightarrow{\sim \sigma^* \sim} & M'(\beta) \\ \uparrow & & \uparrow \\ M & \xrightarrow[\sigma]{} & M' \end{array}$$

por lo que  $(M, \sigma) \preceq (M(\alpha), \sigma^*)$ . Pero como  $M$  es maximal se da la igualdad y  $\alpha \in M$ .

Finalmente, veamos que  $\sigma : K_1 \rightarrow K_2$  es suprayectiva: Sea  $\beta \in K_2$ , luego  $\beta$  es  $k$ -algebraico así que es la raíz de  $f(x) \in k[x]$ . Como  $f(x)$  se escinde en  $K_1$  y  $\sigma$  manda raíces de  $f(x)$  en raíces de  $f(x)$ , se ha de cumplir que  $\beta$  tiene preimagen. Como  $\sigma$  es suprayectiva e inyectiva (por ser  $k$ -morfismo), entonces es biyección, luego isomorfismo.  $\square$

También podemos probar a mano el caso finito y evitar el uso de elección:

**Teorema 4.55:** 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  $K_1 = k(\alpha_1, \dots, \alpha_n)$  donde cada  $\alpha_i$  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.  $\square$

**Definición 4.56:** En consecuencia de los teoremas anteriores se denota por  $k^{\text{alg}}$  a la clausura algebraica de  $k$ .

De la construcción de la clausura algebraica, y dado que éstas son isomorfas, podemos notar otro dato útil:

**Proposición 4.57:** 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  $\pi$ , los cuales tratamos en la sección §??.

Un último paréntesis útil:

**Definición 4.58:** Se dice que un cuerpo  $K$  es *separablemente cerrado* si  $L = K$  es su única extensión algebraica separable.

Sea  $k$  un cuerpo, se dice que una extensión  $K/k$  es una *clausura separable* (a secas) de  $k$  si  $K/k$  es una extensión algebraica y  $K$  es separablemente cerrado.

**Proposición 4.59:** Sea  $k$  un cuerpo arbitrario.

1. Todas las clausuras separables de  $k$  son  $k$ -isomorfas. Por tanto, se denotan  $k^{\text{sep}}$ .
2. Sea  $k^{\text{alg}}$  una clausura algebraica, entonces la clausura separable de  $k$  en  $k^{\text{alg}}$  es una clausura separable (a secas) de  $k$ .
3. La extensión  $k^{\text{alg}}/k^{\text{sep}}$  es puramente inseparable.

4. Sea  $L/k$  una extensión algebraica de cuerpos, y sea  $k^{\text{alg}}$  una clausura algebraica tal que  $k^{\text{alg}} \supseteq L$ . Entonces  $L_s = L \cap k^{\text{sep}}$ .

PISTA: Tómense dos clausuras separables  $K_1, K_2$ ; por definición ambas son extensiones algebraicas así que se extienden a clausuras algebraicas de  $k$ , las cuales son  $k$ -isomorfas. Luego, basta notar que «ser separable» (para elementos) se preserva salvo  $k$ -homomorfismos.  $\square$

Similarmente, uno puede construir la *clausura puramente inseparable*, que suele llamarse, *clausura perfecta* de un cuerpo dada por adjuntar todos los elementos algebraicos puramente inseparables. Se puede notar fácilmente que dicha extensión efectivamente dará un cuerpo perfecto, el cuerpo perfecto más pequeño que extiende al cuerpo base. Ésta construcción aparecerá más adelante en §??.

**§4.4.1 Aplicación: El teorema fundamental del álgebra II.** Aquí veremos una aplicación de las extensiones de cuerpo que hemos estudiado.

**Teorema 4.60:** 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  $|\text{Gal}(L/R)| = [L : R] = 2^n m$  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.  $\square$

## 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 4.61:** 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  $\alpha$  como:

$$\begin{aligned} \text{Tr}_{K/k}(\alpha) &:= \text{tr}(m_\alpha), & \text{Nm}_{K/k}(\alpha) &:= \det(m_\alpha), \\ \psi_{\alpha, K/k}(t) &:= \psi_{m_\alpha}(t) \in k[t] \end{aligned}$$

Usualmente la definición es otra, más relacionada con la conjugación, pero veremos que ambas coinciden.

**Proposición 4.62:** Sea  $K/k$  una extensión finita y sean  $\alpha, \beta \in K$ , entonces:

$$\begin{aligned} \text{Tr}_{K/k}(\alpha + \beta) &= \text{Tr}_{K/k}(\alpha) + \text{Tr}_{K/k}(\beta), \\ \text{Nm}_{K/k}(\alpha \cdot \beta) &= \text{Nm}_{K/k}(\alpha) \cdot \text{Nm}_{K/k}(\beta). \end{aligned}$$

**Teorema 4.63:** Sea  $K/k$  una extensión finita:

1. Si  $K/k$  es separable,  $N$  es la clausura normal de  $K$  y  $\{\sigma_1, \dots, \sigma_n\} = \text{Hom}_k(K, N)$ . Entonces para todo  $\alpha \in K$  se satisface que

$$\begin{aligned} \text{Nm}_{K/k}(\alpha) &= \prod_{i=1}^n \sigma_i(\alpha), & \text{Tr}_{K/k}(\alpha) &= \sum_{i=1}^n \sigma_i(\alpha), \\ \psi_{\alpha, K/k}(t) &= (t - \sigma_1(\alpha)) \cdots (t - \sigma_n(\alpha)) \end{aligned}$$

2. Si  $K/k$  es puramente inseparable de grado  $q$ , entonces para todo  $\alpha \in K$  se satisface que

$$\text{Nm}_{K/k}(\alpha) = \alpha^q, \quad \text{Tr}_{K/k}(\alpha) = 0, \quad \psi_{\alpha, K/k}(t) = t^q - \alpha^q.$$

**DEMOSTRACIÓN:** Por la proposición 3.65 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

$\alpha$  es primitivo, entonces  $(1, \alpha, \dots, \alpha^{n-1})$  es una base ordenada de  $K$  como  $k$ -espacio vectorial, de modo que la matriz de la transformación lineal  $m_\alpha$  en dicha base es

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{bmatrix}.$$

De modo que el polinomio característico es el determinante de

$$\begin{bmatrix} t & 0 & \cdots & 0 & c_0 \\ -1 & t & \cdots & 0 & c_1 \\ 0 & -1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t + c_{n-1} \end{bmatrix},$$

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  $(y_1, \dots, y_p)$  de  $L/k$  y una base  $(z_1, \dots, z_q)$  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  $m_\alpha$  en la base  $(y_j)_j$ , es decir,  $\alpha y_i = \sum_{h=1}^p a_{ih} y_h$ . Luego vemos que

$$\alpha(y_i z_j) = (\alpha y_i) z_j = \sum_{h=1}^p a_{ih} y_h z_j.$$

Así pues, la representación matricial de  $m_\alpha$  es

$$\begin{bmatrix} M & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & M & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & M \end{bmatrix} \in \text{Mat}_{pq}(k).$$

De ésto se sigue que si  $\psi_{\alpha, L/k}$  es el polinomio minimal, entonces  $\psi_{\alpha, K/k}(t) = (\psi_{\alpha, L/k}(t))^q$ . Ésto concluye el teorema.  $\square$

Nótese que curiosamente el caso separable como puramente inseparable se deducen de una unificada demostración. Por la transitividad de la norma y de la traza éste enunciado permite entender el comportamiento de todas las extensiones finitas.

De la demostración se deduce lo siguiente:

**Corolario 4.63.1:** Dada una extensión finita  $K/k$  y fijado un elemento  $\alpha \in K$ . Entonces su polinomio característico  $\phi_{\alpha, K/k}(t) = (f(t))^r$ , donde  $f(t) \in k[t]$  es su polinomio minimal y  $r \geq 1$  es algún natural.

**Ejemplo.** En la extensión  $\mathbb{C}/\mathbb{R}$ , la norma y traza son:

$$\text{Nm}_{\mathbb{C}/\mathbb{R}}(z) = z \cdot \bar{z} = |z|^2, \quad \text{Tr}_{\mathbb{C}/\mathbb{R}}(z) = z + \bar{z} = 2\text{Re}(z).$$

**Teorema 4.64 (transitividad de la norma y de la traza):** Sean  $L/K/k$  extensiones finitas, entonces:

$$\text{Nm}_{L/k} = \text{Nm}_{L/K} \circ \text{Nm}_{K/k}, \quad \text{Tr}_{L/k} = \text{Tr}_{L/K} \circ \text{Tr}_{K/k}.$$

**§4.5.2 Raíces de la unidad y extensiones ciclotómicas.** Recordemos que un elemento de un cuerpo  $\omega$  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 4.65:**  $\sum_{d|n} \phi(d) = n$ .

PISTA: Estudie el orden de los elementos del grupo  $\mathbb{Z}/n\mathbb{Z}$ . Si no, cf. [0, Prop. 3.5].  $\square$

**Lema 4.66:** 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:  $\Leftarrow$ . 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

$$\sum_{T_d \neq \emptyset} \phi(d) = |G| = \sum_{d|n} \phi(d),$$

pero, por lo tanto, debe cumplirse que todos los  $T_d$ 's con  $d \mid n$  son no vacíos y, en particular,  $T_n \neq \emptyset$ .

$\Rightarrow$ . Aplíquese el teorema y el razonamiento anterior para comprobar que  $|S_d| = d$ .  $\square$



Con ésto probamos que:

**Teorema 4.67:** Si  $k$  es un cuerpo finito, entonces  $k^\times$  es cíclico.

**Teorema 4.68:** Sea  $\text{car } k = p$  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 4.66.  $\square$

Por ejemplo: claramente el 1 no es una raíz  $n$ -ésima de la unidad primitiva, excepto para  $n = 1$ .

**Definición 4.69:** 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 4.70:** Sea  $K/k$  una extensión de Galois.  $K$  se dice una **extensión cíclica** (resp. **abeliana**) si  $\text{Gal}(K/k)$  es cíclico (resp. abeliano).

**Teorema 4.71:** Sea  $k$  un cuerpo. Entonces:

1. La  $n$ -ésima extensión ciclotómica 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  $\text{car } k \nmid n$  de modo que  $L_n$  es separable y por ende admite una raíz primitiva  $\zeta$  tal que  $L = k(\zeta)$ . Luego todo  $\sigma \in \text{Gal}(L/k)$  está determinado por adónde manda  $\zeta$  y sus conjugados son de la forma  $\zeta^j$  y es fácil notar que si  $\sigma\zeta = \zeta^a$  y  $\tau\zeta = \zeta^b$ , entonces  $\sigma\tau\zeta = \sigma\zeta^b = \zeta^{ab} = \tau\sigma\zeta$ .  $\square$

De ésta demostración se desprenden fácilmente dos consecuencias:

**Teorema 4.72:** Si  $k$  es un cuerpo finito y  $K/k$  es una extensión finita, entonces  $K/k$  es una extensión cíclica.

DEMOSTRACIÓN: Por el teorema 4.33 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.  $\square$

**Teorema 4.73:** Sea  $\zeta_n$  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  $\text{Gal}(K_n/\mathbb{Q})$  es isomorfo a  $U_n := (\mathbb{Z}/n\mathbb{Z})^\times$ .

Desde aquí nos dedicamos a estudiar las extensiones ciclotómicas de  $\mathbb{Q}$ . En particular ya vimos que todas las raíces  $n$ -ésimas de la unidad pueden ser generadas a partir de la siguiente:

$$\zeta_n := \text{cis} \left( \frac{2\pi}{n} \right)$$

vale decir,  $\zeta_n^j$  son todas las raíces  $n$ -ésimas de la unidad. En particular  $\zeta_n^j$  es primitiva syss  $j$  y  $n$  son coprimos.

**Definición 4.74:** 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  $\Phi_n$  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  $\Phi_p$  concuerda con nuestra antigua definición de « $\Phi_p$ ». La segunda observación se puede mejorar a:

**Proposición 4.75:** Sea  $n > 0$ , entonces

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Reordenando la ecuación anterior se obtiene que

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}.$$

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 « $\pm 1$ », 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 4.76:** Para todo  $n > 0$  se cumplen:

1.  $\Phi_n(x)$  es mónico, tiene grado  $\phi(n)$  y está en  $\mathbb{Z}[x]$ .
2.  $\Phi_n$  es irreducible en  $\mathbb{Z}[x]$  y  $\mathbb{Q}[x]$ , de modo que  $\Phi_n$  es el polinomio minimal de  $\zeta_n$  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  $\omega$  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  $\omega^p$  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  $\omega^p$  no es raíz de  $f(x)$ . Entonces  $\omega^p$  es raíz de  $h(x)$ , es decir,  $\omega$  es raíz de  $h(x^p)$  y como  $f$  es el polinomio minimal de  $\omega$  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  $h(x^p) \equiv h(x)^p \pmod{p}$ , 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.  $\square$

**Teorema 4.77:** Sea  $\text{car } k = p$  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  $\gamma$  es raíz de  $x^n - a$  para algún  $a \in k$ .

DEMOSTRACIÓN: Como  $K$  es cíclica, entonces sea  $\langle \sigma \rangle = \text{Gal}(K/k)$  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  $x \cdot \sigma(u(x, t)) = u(x, t)$ . Sea  $\zeta$  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 Dedekind 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  $\gamma$  son  $\gamma, \zeta\gamma, \dots, \zeta^{n-1}\gamma$ , por lo que,  $L = k(\gamma)$  y su producto es  $\pm\gamma^n \in k$  como se quería probar.  $\square$

**Teorema 4.78:** Sea  $\text{car } k = p \neq 0$ , y sea  $f_a(x) := x^p - x - a \in k[x]$ .

1. Si  $f_a(x)$  no tiene raíces en  $k$  y  $\gamma$  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  $\gamma$  es raíz de  $f_a(x)$  para algún  $a \in k$ .

DEMOSTRACIÓN:

1. Basta notar que si  $\gamma$  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  $\langle \sigma \rangle = \text{Gal}(K/k)$ . Por el lema de independencia de Dedekind existe  $\beta \in K$  tal que  $\sum_{i=1}^p \sigma^i(\beta) \neq 0$ . Definamos

$$\delta := \sigma\beta + 2\sigma^2\beta + \dots + (p-1)\sigma^{p-1}\beta.$$

Luego se tiene que  $\delta - \sigma\delta = \sigma\beta + \sigma^2\beta + \dots + \sigma^{p-1}\beta - (p-1)\beta = \sum_{i=1}^p \sigma^i(\beta) \neq 0$ , 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  $\delta$  son  $\delta, \delta + f, \dots, \delta + (p-1)f$ . Definamos  $\gamma := \delta/f$  y nótese que sus conjugados son  $\gamma, \gamma + 1, \dots, \gamma + (p-1)$ . Más aún

$$a := \gamma \cdot (\gamma - 1) \cdots (\gamma - (p-1)) = \text{Nm}_{K/k}(\gamma) \in k.$$

Nótese que  $b \in \mathbb{F}_p$  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  $\gamma$  es raíz de  $f_a(x) \in k[x]$ .  $\square$

**§4.5.3 La insolubilidad de la quintica.** 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 4.79:** Se dice que una extensión  $k(\alpha)/k$  es **pura** si  $\alpha^m \in k$  para algún  $\alpha$ . 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 4.80:** Una extensión es *resoluble (por radicales)* si está contenida en otra extensión radical.

**Proposición 4.81:** Se cumplen:

1.  $\text{Gal}(k(\zeta_n)/k)$  es abeliano.
2. Sea  $\alpha$  raíz del polinomio irreducible  $x^n - \beta \in k[x]$  y supongamos que  $\zeta_n \in k$ . Entonces  $\text{Gal}(k(\alpha)/k)$  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  $\zeta_n$ , un  $\mathbb{Q}$ -automorfismo  $\sigma$  está completamente determinado por su valor en  $\zeta_n$ , en particular denotemos  $\sigma_j(\zeta_n) = \zeta_n^j$ . Nótese que  $\sigma_j$  determina un automorfismo  $\text{syss}(j; n) = 1$ . 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.  $\gamma$  es otra raíz de  $x^n - \beta$   $\text{syss}(\gamma/\alpha)^n = \beta/\beta = 1$ , vale decir, si  $\gamma/\alpha$  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  $\sigma_j(\alpha) = \alpha\zeta_n^j$ .

3. Supongamos que  $K := k(\alpha_1, \dots, \alpha_n)$  es radical, de modo que  $\alpha_{i+1}^{m_{i+1}} \in k(\alpha_1, \dots, \alpha_i)$  para todo  $i$ . Luego consideremos a la clausura normal  $N$  de  $K$ , la cual ha de ser de la forma

$$N = k(\zeta_{m_1}, \dots, \zeta_{m_n}, \alpha_1, \dots, \alpha_n).$$

Finalmente definamos  $N_j := k(\zeta_{m_1}, \dots, \zeta_{m_j})$  para  $j \leq n$  y  $N_j := k(\zeta_{m_1}, \dots, \zeta_{m_n}, \alpha_1, \dots, \alpha_{n-j})$  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  $\text{Gal}(N/k)$ :

$$\text{Gal}(N/k) = \text{Gal}(N/N_0) \text{Gal}(N/N_1) \cdots \text{Gal}(N/N_{2n}) = \{1\}.$$

Pero aún mejor,  $\text{Gal}(N/N_i)/\text{Gal}(N/N_{i+1}) \cong \text{Gal}(N_{i+1}/N_i)$  (por el teorema fundamental de la teoría de Galois) el cual es abeliano por los incisos anteriores. Finalmente, hemos construido una serie abeliana de  $\text{Gal}(N/k)$ , por lo que  $\text{Gal}(N/k)$  es un grupo resoluble.

Además,  $\text{Gal}(N/k)/\text{Gal}(N/K) \cong \text{Gal}(K/k)$ , por el teorema fundamental de la teoría de Galois, y sabemos que todo cociente de un grupo resoluble es también resoluble.  $\square$

**Lema 4.82:** 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  $\alpha$ . Como  $K$  es radical sea una cadena de extensiones puras:

$$K = k(\beta_1, \dots, \beta_n) \supseteq \cdots \supseteq k(\beta_1) \supseteq k$$

donde  $\beta_i^{n_i} = r_i$ . Entonces elijamos a un conjugado de  $\alpha$ , éste ha de ser de la forma  $\sigma(\alpha)$  donde  $\sigma \in \text{Gal}(L/k)$ . Luego podemos construir la siguiente cadena de extensiones puras:

$$K = k(\gamma_1, \dots, \gamma_n) \supseteq \cdots \supseteq k(\gamma_1) \supseteq k$$

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  $\alpha$  sustituyendo  $\beta_i$  por  $\gamma_i$ . Haciendo lo mismo para el resto de raíces se obtiene que  $L$  es radical y claramente es de Galois.  $\square$

Finalmente bastaría encontrar un cuerpo de Galois cuyo grupo no fuese resoluble (e.g.,  $S_n$  con  $n \geq 5$ ) para poder concluir.

**Lema 4.83:** 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

$$p = \text{ord}(\sigma_1 \cdots \sigma_n) = \text{mcm}(\text{ord}(\sigma_1), \dots, \text{ord}(\sigma_n)),$$

de lo que se sigue que necesariamente  $\sigma$  sea un ciclo.

Sea  $\sigma := (a_1, \dots, a_p) \in G$  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  $\sigma$  no fija a ningún elemento y tiene orden  $> 2$ . Así proseguimos construyendo  $(\sigma^j(b), \sigma^j(c))$  para todo  $j \in \{0, 1, \dots, p-1\}$ , las cuales son trasposiciones que pasan por todos los elementos de  $\{1, 2, \dots, p\}$ . En particular hay alguna trasposición de la forma  $(1, d_1)$  y hay una cadena  $(d_1, d_2), (d_2, d_3), \dots, (d_m, 2)$  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  $S_p$ .  $\square$

**Teorema 4.84:** 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  $\text{Gal}(K/\mathbb{Q}) = S_p$ .

DEMOSTRACIÓN: Sean  $\alpha_1, \dots, \alpha_p$  las raíces de  $f(x)$ , de modo que  $f(x) = \prod_{i=1}^p (x - \alpha_i) \in \mathbb{C}[x]$  y llamemos  $G := \text{Gal}(K/\mathbb{Q})$ . Nótese que  $K = \mathbb{Q}(\alpha_1, \dots, \alpha_p)$  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  $\alpha_i$ 's y éstos son conjugados, entonces todo  $\mathbb{Q}$ -automorfismo de  $K$  está determinado por adónde lleva cada  $\alpha_i$  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  $\bar{(\ )}$  denota conjugación compleja, entonces es claro que las dos raíces



no-reales  $\beta_1, \beta_2$  son conjugadas complejas la una de la otra. Además, la conjugación compleja  $\tau$  es claramente un  $K$ -automorfismo. Como  $G$  contiene a  $\sigma$  (de orden  $p$ ) y a  $\tau$  (de orden 2), entonces concluimos que  $G = S_p$  como se quería probar.  $\square$

**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  $\lim_{x \rightarrow \pm\infty} f(x) = \pm\infty$ , 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.

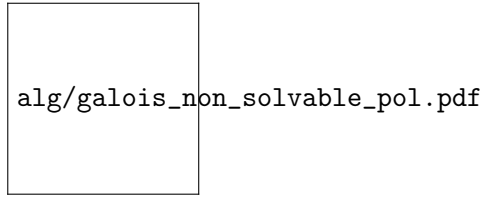


Figura 4.1

## 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 4.85:** Sea  $K/k$  una extensión de cuerpos y sean  $\alpha_1, \dots, \alpha_n$  elementos de  $K$ , éstos se dicen *algebraicamente dependientes* si existe un polinomio  $f \in k[x_1, \dots, x_n]$  no constante tal que  $f(\alpha_1, \dots, \alpha_n) = 0$ ; 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,  $\pi$  y  $\pi^2$  son elementos trascendentes (ésto lo probaremos más adelante), pero claramente sí poseen una relación entre ambos.

**Proposición 4.86:** Sean  $K/k$  y  $K'/k$  extensiones de cuerpo, sean  $S \subseteq K$  y  $S' \subseteq K'$  conjuntos algebraicamente independientes y sea  $f: S \rightarrow S'$  una biyección. Entonces existe un único  $k$ -isomorfismo  $\bar{f}: k(S) \rightarrow k(S')$  tal que  $\bar{f}|_S = f$ .

DEMOSTRACIÓN: Nótese que la biyección  $f$  puede considerarse como una función  $f: S \rightarrow k(S')$  de modo que, como  $k(S')$  es un dominio, entonces podemos extenderlo de manera única al homomorfismo de evaluación  $\tilde{f}: k[S] \rightarrow k(S')$  (teo. 2.60). 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  $\bar{f}: k(S) \rightarrow k(S')$  (teo. 2.54). Finalmente como  $\bar{f}$  es un  $k$ -monomorfismo y  $S' \subseteq \text{Im } \bar{f}$ , entonces  $\bar{f}$  es un  $k$ -isomorfismo.  $\square$

**Corolario 4.86.1:** 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 4.87:** 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:  $\Rightarrow$ . Sea  $f \in k[x_1, \dots, x_n, y]$  tal que  $f(s_1, \dots, s_n, \beta) = 0$  para algunos  $s_i \in S$ . Podemos escribir

$$f(x_1, \dots, x_n, y) = \sum_{j=0}^m g_j(x_1, \dots, x_n) y^j,$$

y definir  $a_j := g_j(s_1, \dots, s_n) \in k(S)$ , de modo que  $h(y) := \sum_{j=0}^m a_j y^j \in$

$k(S)[y]$  es tal que

$$h(\beta) = f(s_1, \dots, s_n, \beta) = 0.$$

Como  $\beta$  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  $g_j = 0 \in k[x_1, \dots, x_n]$ , de lo que se sigue que  $f$  es el polinomio nulo.

$\Leftarrow$ . Ejercicio para el lector.  $\square$

**Definición 4.88:** 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 4.89:** 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) 4.90:** 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 4.87 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  $K/k$ .  $\square$

**Teorema (AE) 4.91:** Sea  $K/k$  una extensión de cuerpos y sean  $S, T$  bases de trascendencia de  $K/k$ . Luego  $|S| = |T|$ .

DEMOSTRACIÓN:

- (a) Si  $S = \{s_1, \dots, s_n\}$  es finito: entonces  $T$  es algebraico sobre  $k(s_1, \dots, s_n)$ , pero no todo elemento de  $T$  es algebraico sobre  $k(s_2, \dots, s_n)$  puesto que de lo contrario  $K/k(T)/k(s_2, \dots, s_n)$  serían extensiones algebraicas y  $s_1$  sería algebraico respecto a  $k(s_2, \dots, s_n)$ . Así pues, sea  $t_1 \in T$  tal que  $t_1$  es trascendente sobre  $k(s_2, \dots, s_n)$  y notemos que, por la proposición 4.87, se cumple que el conjunto  $T' := \{t_1, s_2, \dots, s_n\}$  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  $T = \{t_1, \dots, t_n\}$ .

- (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  $k(\bigcup_{s \in S} T_s)$ , 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. 3.30).  $\square$

**Definición 4.92:** Sea  $K/k$  una extensión de cuerpos. Se define el **grado de trascendencia** de  $K/k$ , denotado  $\text{trdeg}(K/k)$ , a la cardinalidad de cualquiera de sus bases de trascendencia.

**Proposición 4.93:** Sea  $k$  un cuerpo. Entonces:

1. Una extensión  $K/k$  es algebraica syss  $\text{trdeg}(K/k) = 0$ .
2. Sea  $K := k(x_1, \dots, x_n)$  el cuerpo de polinomios en  $n$  variables, entonces  $\text{trdeg}(K/k) = n$ .

**Teorema (AE) 4.94:** Sean  $K, L$  cuerpos algebraicamente cerrados de igual característica, de modo que tienen el mismo cuerpo primo  $k$ , y supongamos que  $\text{trdeg}(K/k) = \text{trdeg}(L/k)$ . 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  $f: S \rightarrow T$  que luego se extiende de manera única a un isomorfismo  $\tilde{f}: k(S) \rightarrow k(T)$ , 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.  $\square$

**Corolario (AE) 4.94.1:** Sea  $K$  un cuerpo no numerable cuyo cuerpo primo es  $k$ , entonces  $\text{trdeg}(K/k) = |K|$ . En consecuencia, dos cuerpos no numerables algebraicamente cerrados de igual característica son isomorfos syss tienen la misma cardinalidad.

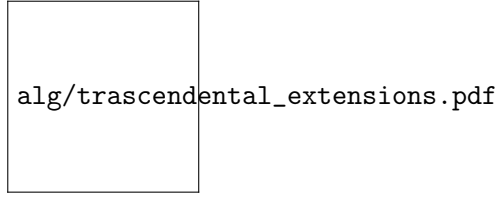
**Ejemplo.** Por el corolario anterior,  $\mathbb{C}$  y  $\mathbb{C}(z)^{\text{alg}}$  son isomorfos como cuerpos, aunque claramente no son  $\mathbb{C}$ -isomorfos.

**Teorema 4.95:** Sean  $L/K/k$  extensiones de cuerpo, entonces

$$\text{trdeg}(L/k) = \text{trdeg}(L/K) + \text{trdeg}(K/k).$$

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  $S \cap T = \emptyset$ ).

Es fácil ver que  $S \cap T = \emptyset$ . 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 4.96:** 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

$$\text{alt } f := \max\{\deg g(x), \deg h(x)\}.$$

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 4.97:** 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

$$\begin{aligned}\varphi &:= \frac{ax+b}{cx+d}, & \psi &:= \frac{ex+f}{gx+h} \\ \varphi \circ \psi &= \frac{(ae+cf)x + (be+df)}{(ag+ch)x + (bg+dh)}.\end{aligned}$$

De aquí es fácil notar que conforma un grupo.  $\square$

El lector atento debería reconocer una forma matricial en la última forma. En efecto,  $\text{LF}(k)$  es *casi* el grupo de matrices invertibles, pero con la restricción de que  $\frac{2x}{2} = \frac{x}{1}$ .

**Proposición 4.98:** Sea  $\varphi = g(x)/h(x) \in k(x)$  no constante con  $g(x), h(x)$  coprimos. Entonces:

1.  $\varphi$  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  $[k(x) : k(\varphi)] = \text{alt } \varphi$ .

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  $n = \text{alt } \varphi$ . 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  $\deg \theta = \text{alt } \varphi$ .

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 2.77.1.  $\square$

**Corolario 4.98.1:** Sea  $\varphi \in k(x)$ , entonces  $k(x) = k(\varphi)$  syss  $\varphi \in \text{LF}(k)$ .

**Teorema 4.99 – 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  $m := \deg_y(\theta) = \text{alt}(\varphi) = [k(x) : k(\varphi)]$ . 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  $\deg_x(\theta^*) = \text{alt}(g_j/h_j) \leq \max_i \{\text{alt}(g_i/h_i)\} \leq \deg_x(I^*)$  (por la propoción 2.79), 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.  $\square$

## Notas históricas

Esta sección está principalmente basada en el artículo KIERNAN [0].

Tal como señalamos en el capítulo 2, el estudio de las extensiones simples algebraicas comienza con la llamada *teoría de divisores* de **Leopold Kronecker** [0], 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  $\zeta_{23}$  es una raíz 23-ésima primitiva de la unidad) no es un DFU (cf. KUMMER [0] (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 búsqueda de una sustitución de la factorización única. El caso general de enteros ciclotómicos para exponentes no necesariamente primos lo estudia en KUMMER [0] (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 [0] (1801) fue el primero en trabajar con la ecuación  $x^p - 1 = 0$  y notar que sus soluciones coinciden 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 quintica. 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 [0] (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 [0] (1826).

Tras probar que, en general, la quintica no es soluble, Abel comienza a investigar qué clase de polinomios sí admiten soluciones por radicales. En ABEL [0] (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 [0] y [0], 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 [0, págs. 73-74]:

En [la] corta y fulgurante vida [de Galois] me parece percibir el comienzo de una gran visión – precisamente la de los «esponsales del número y la magnitud» en una visión geométrica nueva. En alguna parte de Cosechas y Siembras evoco cómo, hace dos años, apareció en mí esta intuición súbita: que en el trabajo matemático que en ese momento ejercía sobre mí la fascinación más poderosa estaba «retomando la herencia de Galois». [...] Con razón o sin ella, me parece que esa visión que desarrollé durante quince años de mi vida, y que siguió madurando en mí y enriqueciéndose durante los dieciséis años que han pasado desde mi salida de la escena matemática – que esa visión también es la que Galois no habría podido dejar de desarrollar, si él hubiera estado en estos

parajes en mi lugar y sin que una muerte precoz viniera a cortar brutalmente un magnífico impulso.

## 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

$$(x, y) + (z, w) := (x + z, y + w), \quad \lambda(x, y) := (\lambda x, \lambda y).$$

para todo  $x, z \in M$ ,  $y, w \in N$  y  $\lambda \in A$ .

El producto directo se puede generalizar a una familia  $\{M_i\}_{i \in I}$  de  $A$ -módulos, cuyos elementos son:

$$(\mathbf{m}_i)_{i \in I} \in \prod_{i \in I} M_i \iff \forall i \in I \mathbf{m}_i \in M_i$$

y cuyas operaciones son:

$$(\mathbf{m}_i)_{i \in I} + (\mathbf{n}_i)_{i \in I} := (\mathbf{m}_i + \mathbf{n}_i)_{i \in I}, \quad \lambda \cdot (\mathbf{m}_i)_{i \in I} := (\lambda \mathbf{m}_i)_{i \in I}.$$

**Proposición 5.2:** Sea  $\{M_i\}_{i \in I}$  una familia de  $A$ -módulos, entonces:

1. Las proyecciones  $\pi_j: \prod_{i \in I} M_i \rightarrow M_j$  son morfismos de  $A$ -módulos para todo  $j \in I$ .
2. Si  $\{\varphi_i: T \rightarrow M_i\}$  es una familia de morfismos de  $A$ -módulos, entonces  $\psi := \Delta_{i \in I} \varphi_i: T \rightarrow \prod_{i \in I} M_i$  es el único morfismo de  $A$ -módulos tal que el siguiente diagrama:  $\psi := \Delta_{i \in I} \varphi_i: T \rightarrow \prod_{i \in I} M_i$  es el único morfismo de  $A$ -módulos tal que el siguiente diagrama:

$$\begin{array}{ccc} N & & \\ \downarrow \exists! \psi & \searrow \varphi_j & \\ \prod_{i \in I} M_i & \xrightarrow{\pi_j} & M_j \end{array}$$

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:

$$\bigoplus_{i \in I} M_i := \left\{ (\mathbf{m}_i)_i \in \prod_{i \in I} M_i : \mathbf{m}_i = \vec{0} \text{ salvo finitos } i\text{'s} \right\}.$$

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  $\iota_j: M_j \rightarrow \bigoplus_{i \in I} M_i$  son morfismos de  $A$ -módulos para todo  $j \in I$ .

2. Si  $\{\varphi_i: M_i \rightarrow N\}$  es una familia de morfismos de  $A$ -módulos, entonces

$$\begin{aligned} \psi := \left(\sum_{i \in I} \varphi_i\right): \bigoplus_{i \in I} M_i &\longrightarrow N \\ \sum_{i \in I} \mathbf{m}_i &\longmapsto \sum_{i \in I} \varphi_i(\mathbf{m}_i) \end{aligned}$$

es el único morfismo de  $A$ -módulos tal que el siguiente diagrama:

$$\begin{array}{ccc} & N & \\ \uparrow \exists! \psi & \nwarrow \varphi_j & \\ \bigoplus_{i \in I} M_i & \xleftarrow{\iota_j} & M_j \end{array}$$

conmuta para todo  $j \in I$ .

(Nótese que  $\psi$  está bien definido ya que sólo finitos de los  $\mathbf{m}_i$ '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

$$\begin{aligned} \mathrm{Hom}_A\left(N, \prod_{i \in I} M_i\right) &\cong \prod_{i \in I} \mathrm{Hom}_A(N, M_i) \\ \mathrm{Hom}_A\left(\bigoplus_{i \in I} M_i, N\right) &\cong \prod_{i \in I} \mathrm{Hom}_A(M_i, N) \end{aligned}$$

(en  $\mathrm{Mod}_A$ ).

**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:

$$\begin{array}{ccc}
\bigoplus_{i \in I} M_i & \xrightarrow{\sum_{i \in I} \varphi_i} & \bigoplus_{i \in I} (M_i/S_i) \\
\uparrow & \nearrow \varphi_j & \uparrow \\
M_j & \xrightarrow{\quad} & M_j/S_j
\end{array}$$

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.  $\square$

**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  $f: M \rightarrow N$  un morfismo de  $A$ -módulos. Entonces:

1.  $\iota: \ker f \rightarrow M$  es un morfismo de  $A$ -módulos tal que  $\iota \circ f = \iota \circ 0_{M,N}$ , donde  $0_{M,N}: M \rightarrow N$  es el morfismo nulo.
2. Si existe otro morfismo  $g: T \rightarrow M$  tal que  $g \circ f = g \circ 0_{M,N}$ , entonces existe un único morfismo  $\bar{g}: T \rightarrow \ker f$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccc}
T & & & & \\
\downarrow \exists! \bar{g} & \searrow g & & & \\
\ker f & \xrightarrow{\iota} & M & \xrightarrow[\quad 0_{M,N}]{f} & N
\end{array}$$

En resumen,  $\ker f$  es un núcleo categorial.

**Definición 5.9:** Sea  $f: M \rightarrow N$  un morfismo de  $A$ -módulos. Puesto que  $\text{Im } f$  es submódulo de  $N$  se define  $\text{coker } f := N/\text{Im } f$ .

Ésto nos permite construir el siguiente objeto:

**Proposición 5.10:** Sea  $f: M \rightarrow N$  un morfismo de  $A$ -módulos. Entonces:

1.  $\pi: N \rightarrow \text{coker } f$  es un morfismo de  $A$ -módulos tal que  $f \circ \pi = 0_{M,N} \circ \pi$ .

2. Si existe otro morfismo  $g: N \rightarrow T$  tal que  $f \circ g = 0_{M,N} \circ g$ , entonces existe un único morfismo  $\bar{g}: \text{coker } f \rightarrow T$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc}
 & & T \\
 & \nearrow g & \uparrow \exists! \bar{g} \\
 M \xrightarrow[\underset{0_{M,N}}{\rightrightarrows}]{} N & \xrightarrow[\pi]{\twoheadrightarrow} & \text{coker } f
 \end{array}$$

En resumen,  $\text{coker } f$  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  $f: M \rightarrow N$  un morfismo de  $A$ -módulos. Entonces  $f$  es suprayectiva syss  $\text{coker } f$  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  $f: M \rightarrow N$  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

$$M \cong \text{Im } f = \ker g, \quad T \cong N / \text{Im } f = \text{coker } f.$$

2. Sean  $S, T$  submódulos de  $M$ , entonces el siguiente diagrama conmuta y las filas son exactas:

$$\begin{array}{ccccccc} 0 & \longrightarrow & S \cap T & \longrightarrow & S & \longrightarrow & \frac{S}{S \cap T} \longrightarrow 0 \\ & & \downarrow \iota & & \downarrow \iota & & \downarrow \wr \\ 0 & \longrightarrow & T & \longrightarrow & S + T & \longrightarrow & \frac{S + T}{T} \longrightarrow 0 \end{array}$$

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  $h: T \rightarrow N$  tal que  $h \circ g = \text{Id}_T$ . 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  $N \cong M \oplus T = \ker g \oplus \text{coker } f$ .

DEMOSTRACIÓN: Sea  $h: T \rightarrow N$  tal que  $h \circ g = \text{Id}_T$ , veremos que  $N = \text{Im } f \oplus \text{Im } h$ .

Sea  $\mathbf{n} \in N$ , luego  $g(\mathbf{n}) \in T$  y además se cumple que  $\mathbf{n} - h(g(\mathbf{n})) \in \ker g$ . Luego como  $\ker g = \text{Im } f$ , existe  $\mathbf{m} \in M$  tal que  $f(\mathbf{m}) = \mathbf{n} - h(g(\mathbf{n}))$ , así que claramente  $N = \text{Im } f + \text{Im } h$ . Más aún, sea  $\mathbf{n} := f(\mathbf{m}) = h(\mathbf{t})$ , luego  $g(\mathbf{n}) = g(f(\mathbf{m})) = \mathbf{t} = \vec{0}$  dado que  $f \circ g = 0$ , pero entonces  $\mathbf{n} = h(\vec{0}) = \vec{0}$ , así que  $\text{Im } f \cap \text{Im } h = \{\vec{0}\}$  como se quería probar.  $\square$



Ya vimos que  $\text{Hom}_A(X, Y)$  es un  $A$ -módulo, así pues podemos establecer el siguiente resultado:

**Proposición 5.16:** Sea  $M$  un  $A$ -módulo y  $f: X \rightarrow Y$  un morfismo de  $A$ -módulos, entonces:

$$\begin{aligned} h^f: \text{Hom}_A(M, X) &\longrightarrow \text{Hom}_A(M, Y) \\ g &\longmapsto g \circ f \end{aligned}$$

y

$$\begin{aligned} h_f: \text{Hom}_A(Y, M) &\longrightarrow \text{Hom}_A(X, M) \\ g &\longmapsto f \circ g \end{aligned}$$

son también morfismos de  $A$ -módulos.

DEMOSTRACIÓN: Sea  $\mathbf{m} \in M$ , entonces:

$$\begin{aligned} ((g + h) \circ f)(\mathbf{m}) &= f((g + h)(\mathbf{m})) = f(g(\mathbf{m}) + h(\mathbf{m})) \\ &= f(g(\mathbf{m})) + f(h(\mathbf{m})) = (g \circ f)(\mathbf{m}) + (h \circ f)(\mathbf{m}). \end{aligned}$$

Y el producto escalar se demuestra análogamente. El resto de resultados queda al lector.  $\square$

**Corolario 5.16.1:** Para todo  $A$ -módulo  $M$  se satisface que el siguiente

$$\begin{array}{ccc} X & & \text{Hom}_A(M, X) \\ f \downarrow & \xrightarrow{\text{Hom}_A(M, -)} & \downarrow h^f \\ Y & & \text{Hom}_A(M, Y) \end{array}$$

es un funtor covariante en  $\text{Mod}_A$ ; y el siguiente:

$$\begin{array}{ccc} X & & \text{Hom}_A(X, M) \\ f \downarrow & \xrightarrow{\text{Hom}_A(-, M)} & \uparrow h_f \\ Y & & \text{Hom}_A(Y, M) \end{array}$$

es un funtor contravariante en  $\text{Mod}_A$ . 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  $\text{Hom}$ '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  $\text{Mod}_A$  es bastante especial.

**Definición 5.17:** Sea  $F: \mathcal{A} \subseteq A\text{-Mod} \rightarrow \mathcal{B} \subseteq B\text{-Mod}$  un funtor (covariante). Entonces  $F$  se dice:

**Aditivo** Si para todo  $M, N \in \mathcal{A}$  se satisface que la aplicación

$$\begin{aligned} \text{Hom}_A(M, N) &\longrightarrow \text{Hom}_B(FM, FN) \\ g &\longmapsto F(g) \end{aligned}$$

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  $F: \mathcal{A}^{\text{op}} \rightarrow \mathcal{B}$ .

En general, que un funtor sea exacto es una condición increíblemente fuerte, y la condición de exactitud por un lado u otro es suficiente.

**Teorema 5.18:** Sea  $M$  un  $A$ -módulo, entonces  $\text{Hom}(M, -)$  es un funtor covariante exacto por la izquierda y  $\text{Hom}(-, M)$  es un funtor contravariante exacto por la derecha.

**Proposición 5.19:** 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  $M$ :

$$\text{Hom}_A(M, X) \xrightarrow{h^f} \text{Hom}_A(M, Y) \xrightarrow{h^g} \text{Hom}_A(M, Z)$$

3. La siguiente sucesión es exacta para todo  $M$ :

$$\text{Hom}_A(X, M) \xleftarrow{h_f} \text{Hom}_A(Y, M) \xleftarrow{h_g} \text{Hom}_A(Z, M)$$

DEMOSTRACIÓN:  $1 \implies 2$ . Sea  $j \in \text{Hom}_A(M, Y)$ , se cumple que  $j \in \ker(h^g)$  syss  $j \circ g = 0$ , es decir para todo  $\mathbf{m} \in M$  se cumple que  $g(j(\mathbf{m})) = \vec{0}$ , o lo que es equivalente,  $\text{Img } j \subseteq \ker g$ . Por otro lado  $j \in \text{Img}(h^f)$  syss  $j = k \circ f$ , luego  $j(\mathbf{m}) = f(k(\mathbf{m}))$ , por lo que  $\text{Img } j \subseteq \text{Img } f = \ker g$ , es decir,  $\text{Img}(h^f) = \ker(h^g)$  como se quería probar.

$2 \implies 1$ . Fijemos  $M = X$ , entonces  $h^f(\text{Id}_X) = f \in \ker(h^g)$ , es decir,  $f \circ g = 0$  y  $\text{Img } f \subseteq \ker g$ . Ahora fijemos  $M = \ker g$ , entonces como  $\ker g \subseteq Y$  existe  $\iota \in \text{Hom}_A(\ker g, Y)$  y claramente  $\iota \circ g = 0$  por lo que  $\iota \in \ker(h^g) = \text{Img}(h^f)$ , luego  $\iota = j \circ f$ , es decir, para todo  $\mathbf{y} \in \ker g$  se cumple que  $\mathbf{y} \in \text{Img } f$ .

El resto son análogas. □

## 5.2 Cadenas de submódulos

### §5.2.1 Módulos noetherianos y artinianos.

**Lema 5.20:** 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 5.21:** 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 5.22:** Se dice que un  $A$ -módulo  $M$  es *artiniano* si para toda cadena descendente 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.** Un anillo noetheriano que no es artiniano  $\mathbb{Z}$  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  $\subseteq$ -descendente de ideales sin  $\subseteq$ -minimal.

**Ejemplo.** Ya vimos que  $k[x_1, x_2, x_3, \dots]$  no es noetheriano, pero tampoco es artiniiano:

$$(x_1, x_2, x_3, \dots) \supset (x_2, x_3, \dots) \supset (x_3, \dots) \supset \dots$$

Ahora, procedemos a dar varias propiedades de los módulos noetherianos que tendrán demostraciones análogas para los módulos artiniianos que, en consecuencia, vamos a obviar.

**Proposición 5.23:** Sea  $M$  un  $A$ -módulo noetheriano (resp. artiniiano). Entonces todo submódulo  $N$  y todo módulo cociente  $M/N$  es noetheriano (resp. artiniiano).

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.  $\square$

**Corolario 5.23.1:** Sea  $A$  un anillo noetheriano (resp. artiniiano) y sea  $\mathfrak{a}$  un ideal de  $A$ . Entonces  $A/\mathfrak{a}$  también es noetheriano (resp. artiniiano).

**Corolario 5.23.2:** Si  $\varphi: M \rightarrow N$  es un morfismo de  $A$ -módulos supra-yectivo y  $M$  es noetheriano (resp. artiniiano), entonces  $N$  también.

### §5.2.2 Módulos (semi)simples y el teorema de Jordan-Hölder.

**Definición 5.24:** Un  $A$ -módulo  $M$  no trivial se dice *simple*<sup>1</sup> 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 5.25 (Schur):** Si  $M$  es un  $A$ -módulo simple, entonces:

1. Todo homomorfismo de  $A$ -módulos  $M \rightarrow N$  es o bien nulo o bien un monomorfismo.
2. Todo homomorfismo de  $A$ -módulos  $N \rightarrow M$  es o bien nulo o bien un epimorfismo.

<sup>1</sup>JACOBSON [0] emplea el término *irreducible*. A sugerencia de MATSUMURA [0, pág. 40] reservamos la palabra para la definición 6.57.

3. Todo endomorfismo de  $A$ -módulos  $M \rightarrow M$  es o bien nulo o bien un automorfismo.

En consecuencia,  $(\text{End}_A(M), +, \circ)$  es un anillo de división.

DEMOSTRACIÓN: Basta notar que el núcleo y la imagen de un homomorfismo es un submódulo.  $\square$

Una versión más común del lema de Schur suele expresarse en términos de representaciones complejas, que aparecerán más adelante, pero explicaremos de igual manera aquí para conveniencia del lector. Una representación de un grupo finito  $G$  involucra un  $\mathbb{C}[G]$ -módulo y  $\mathbb{C}[G]$  es un  $\mathbb{C}$ -espacio vectorial de dimensión finita, de modo que el  $M$  en el enunciado sería un  $\mathbb{C}$ -espacio vectorial de dimensión finita y, por tanto,  $\text{End}_{\mathbb{C}[G]}(M)$  también. No obstante, sobre un cuerpo algebraicamente cerrado  $K$  no hay anillos de división de dimensión finita salvo el mismo  $K$ .

Algo relativamente sencillo de probar es lo siguiente:

**Proposición 5.26:** Un  $A$ -módulo  $M$  es simple syss existe un ideal  $\mathfrak{m} \triangleleft A$  maximal tal que  $M \cong A/\mathfrak{m}$ .

DEMOSTRACIÓN:  $\Rightarrow$ . Sea  $\mathbf{u} \in M$  no nulo, entonces  $\text{Span}_A\{\mathbf{u}\}$  es un submódulo no trivial, luego es todo  $M$ . Por ende, sea  $f: A \rightarrow M$  definido por  $f(a) := a\mathbf{u}$ , ésta función es suprayectiva por lo anterior, luego induce un isomorfismo  $\bar{f}: A/\ker f \rightarrow M$  y  $A/\ker f$  no posee submódulos impropios, luego  $\ker f$  ha de ser un ideal maximal.

$\Leftarrow$ . Es claro.  $\square$

Por ende, parece más interesante analizar el caso de los módulos semi-simples:

**Definición 5.27:** Se dice que un  $A$ -módulo  $M$  es un *sumando directo* de  $N$  si existe  $M'$  tal que  $N = M \oplus M'$ .

**Proposición (AE) 5.28:** Un  $A$ -módulo  $M$  es semisimple syss todo submódulo  $T \leq M$  es un sumando directo de  $M$ .

DEMOSTRACIÓN:  $\Rightarrow$ . 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).

$\Leftarrow$ . Ésto lo haremos en dos pasos:

- (I) Todo submódulo  $B$  impropio de  $M$  contiene un sumando directo simple:

Sea  $\mathbf{u} \in B$  no nulo y, por el lema de Zorn, sea  $C \leq B$  maximal tal que  $\mathbf{u} \notin C$ . 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  $\mathbf{u}$  no puede estar en ambos  $C \oplus E$  y  $C \oplus F$ : de lo contrario,  $\mathbf{u} = \mathbf{c}_1 + \mathbf{e} = \mathbf{c}_2 + \mathbf{f}$  con  $\mathbf{c}_1, \mathbf{c}_2 \in C$ ,  $\mathbf{e} \in E$  y  $\mathbf{f} \in F$ . Pero  $\mathbf{c}_2 - \mathbf{c}_1 = \mathbf{e} - \mathbf{f} \in C \cap D = \{\vec{0}\}$ , luego  $\mathbf{e} = \mathbf{f} \in E \cap F = \{\vec{0}\}$  y por ende  $\mathbf{u} = \mathbf{c}_1 \in C$  lo cual es absurdo. Finalmente, si  $\mathbf{u} \notin C \oplus E$ , 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  $U$ .  $\square$

**Corolario (AE) 5.28.1:** Todo submódulo y todo cociente de un módulo semisimple es también semisimple.

**Definición 5.29:** 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  $\mathfrak{b} \triangleleft \mathfrak{a}$ . Un dominio  $A$  se dice *semisimple* si es la suma directa de ideales minimales.

**Lema 5.30:** 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.  $\square$

**Corolario 5.30.1:** El producto directo de finitos anillos semisimples es

semisimple. En particular, el producto directo de finitos cuerpos es un dominio semisimple.

**Definición 5.31:** Sea  $G$  un grupo y  $k$  un cuerpo. Definimos  $k[G]$  como el anillo dado por los objetos formales:

$$\sum_{i=1}^n a_i g_i \in k[G], \quad \forall i \ a_i \in k, g_i \in G.$$

Donde se definen la suma y multiplicación por:

$$\begin{aligned} \alpha &:= \sum_{g \in G} a_g g, & \beta &:= \sum_{g \in G} b_g g, \\ \alpha + \beta &:= \sum_{g \in G} (a_g + b_g) g, & \alpha \cdot \beta &:= \sum_{g \in G} \left( \sum_{fh=g} a_f b_h \right) g. \end{aligned}$$

**Teorema 5.32 – 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.<sup>a</sup>

<sup>a</sup>Técnicamente 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  $d: k[G] \rightarrow \mathfrak{a}$  tal que  $d|_{\mathfrak{a}} = \text{Id}_{\mathfrak{a}}$ .

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:

$$\begin{aligned} D: k[G] &\longrightarrow k[G] \\ x &\longmapsto \frac{1}{|G|} \sum_{g \in G} g d(g^{-1} x). \end{aligned}$$

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  $\text{Im } D \subseteq \mathfrak{a}$  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:

$$\begin{aligned} gD(x) &= \frac{1}{|G|} \sum_{h \in G} gh d(h^{-1}x) = \frac{1}{|G|} \sum_{h \in G} gh d(h^{-1}g^{-1}gx) \\ &= \frac{1}{|G|} \sum_{j=gh \in G} j d(j^{-1}gx) = D(gx), \end{aligned}$$

donde la última igualdad sale del hecho de que  $h \mapsto gh$  es una mera permutación sobre  $G$ .  $\square$

Desde aquí en adelante podemos hacer una discusión análoga a la de grupos resolubles y las series normales (véase §1.5.2).

**Lema 5.33 (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.  $\frac{B + (B^* \cap C^*)}{B + (B^* \cap C)} \cong \frac{C + (C^* \cap B^*)}{C + (C^* \cap B)}$ .

**Definición 5.34:** 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 5.35:** Un  $A$ -módulo posee una serie de composición si y sólo si es noetheriano y artiniiano.

**Teorema 5.36 (de refinamiento de Schreier):** Dos series de un mismo  $A$ -módulo poseen al menos un refinamiento equivalente.

**Teorema 5.37 – Teorema de Jordan-Hölder.** Todas las series de composición de un  $A$ -módulo (si existen) son equivalentes.

**Definición 5.38:** 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) 5.39:** 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 artinian.

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  $\{x_n : n \in \mathbb{N}\}$  un conjunto linealmente independiente, luego la cadena ascendente:

$$\text{Span}_k\{x_1\} \subset \text{Span}_k\{x_1, x_2\} \subset \text{Span}_k\{x_1, x_2, x_3\} \subset \cdots$$

no posee  $\subseteq$ -maximal, por lo que  $V$  no es noetheriano.

La implicancia  $4 \implies 1$  es análoga. □

**Proposición 5.40:** 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 5.41:** Se dice que un  $A$ -módulo  $M$  es **indecomposable** si no existen  $M_1, M_2 \leq M$  no nulos, tales que  $M = M_1 \oplus M_2$ .

**Proposición 5.42:** Un  $A$ -módulo  $M$  no trivial es indecomposable si y sólo si existe  $\varphi \in \text{End}(M) \setminus \{0, \text{Id}\}$  idempotente.

DEMOSTRACIÓN: Ambas implicancias las haremos por contrarrecíproca.

$\Leftarrow$ . Si  $M = M_1 \oplus M_2$ , entonces la proyección  $\pi_1$  que fija a  $M_1$  y anula a  $M_2$  es idempotente.

$\Rightarrow$ . Sea  $\varphi \in \text{End}(M) \setminus \{0, \text{Id}\}$  idempotente. Definamos  $e_1 := \varphi$  y  $e_2 := \text{Id} - \varphi$ , 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.  $\square$

**Definición 5.43:** Un  $A$ -módulo  $M$  se dice *fuertemente indecomponible* si  $M \neq 0$  y  $\text{End}(M)$  es un anillo local.

**Lema 5.44:** Sean  $M, N$  un par de  $A$ -módulos, con  $M \neq 0$  y  $N$  indecomponible. Si  $f: M \rightarrow N$  y  $g: N \rightarrow M$  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  $\phi := f \circ g: M \rightarrow N$ ,  $\psi := \phi^{-1}: N \rightarrow M$  y  $h := g \circ \psi: N \rightarrow M$ . Claramente  $f \circ h = \text{Id}_M$  y

$$(hf)^2 = hfhf = hf,$$

por lo que  $hf$  es idempotente sobre  $N$ , y por inyectividad de  $f$  es claramente no nula, luego  $hf = \text{Id}$ .  $\square$

**Teorema 5.45:** Sean:

$$M = M_1 \oplus \cdots \oplus M_n, \quad N = N_1 \oplus \cdots \oplus N_m,$$

donde  $M \cong N$  y para todo  $i, j$  se cumple que  $M_i$  es fuertemente indecomponible y  $N_j$  es indecomponible. 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:

$$\begin{array}{ccccc}
M & \xleftarrow{e_1} & M & & \\
\downarrow \scriptstyle \{g\} & & \downarrow h_j & & \\
N & \xrightarrow{f_j} & N & \xrightarrow{f_j} & N \\
& & \downarrow \ell_j & & \downarrow \scriptstyle \{g^{-1}\} \\
& & M & \xleftarrow{e_1} & M
\end{array}$$

luego  $h_j \ell_j = e_1 g f_j g^{-1} e_1$  y de hecho

$$\sum_{j=1}^m h_j \ell_j = \sum_{j=1}^m e_1 g f_j g^{-1} e_1 = e_1 g \left( \sum_{j=1}^m f_j \right) g^{-1} e_1 = e_1.$$

Como  $e_1$  fija a  $M_1$ , en particular podemos considerar las restricciones  $e'_1: M_1 \rightarrow M_1$  y  $(h_j \ell_j)': M_1 \rightarrow M_1$ ; por la ecuación anterior se concluye que  $\sum_{j=1}^m (h_j \ell_j)' = \text{Id}_{M_1}$ , pero como  $\text{End}(M_1)$  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  $h'_1: M_1 \rightarrow N_1$  y  $\ell'_1: N_1 \rightarrow M_1$  son isomorfismos. Para finalizar sólo basta probar que

$$M = g^{-1}[N_1] \oplus (M_2 + \cdots + M_n).$$

Sea  $\mathbf{x} \in g^{-1}[N_1] \cap (M_2 + \cdots + M_n)$ , luego sea  $\mathbf{y} := g(\mathbf{x}) \in N_1$ , como  $\mathbf{x} \in M_2 + \cdots + M_n$ , entonces

$$\vec{0} = e_1(\mathbf{x}) = (g^{-1} \circ e_1)(\mathbf{y}) = (f_1 \circ g^{-1} \circ e_1)(\mathbf{y}) = \ell'_1(\mathbf{y}),$$

por lo que  $\mathbf{y} = \vec{0}$  y  $\mathbf{x}$  también. Por otro lado sea  $\mathbf{x} \in M' := g^{-1}[N_1] + M_2 + \cdots + M_n$ ; luego  $\mathbf{x}, e_2 \mathbf{x}, \dots, e_n \mathbf{x} \in M'$  por lo que  $e_1 \mathbf{x} \in M'$  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  $n$ .  $\square$

**Definición 5.46:** Sea  $M$  un  $A$ -módulo y  $f \in \text{End}(M)$ , entonces se definen:

$$f^\infty M := \bigcap_{n \in \mathbb{N}} f^n[M], \quad f^{-\infty} 0 := \bigcup_{n \in \mathbb{N}} \ker(f^n).$$

Nótese que ambos son submódulos de  $M$ .

**Lema 5.47 (Fitting):** Sea  $M$  un  $A$ -módulo noetheriano y artiniiano, y  $f \in \text{End}(M)$ . 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:

$$M \subseteq f[M] \subseteq f^2[M] \cdots \rightarrow f^\infty M, \quad \ker f \supseteq \ker(f^2) \supseteq \cdots \rightarrow f^{-\infty} 0.$$

Como  $M$  es artiniiano y noetheriano, existe  $n$  suficientemente grande tal que  $f^n[M] = f^\infty M$  y  $\ker(f^n) = f^{-\infty} 0$ .

Sea  $z \in f^\infty M \cap f^{-\infty} 0$ , entonces  $z = f^n(y)$  y  $f^n(z) = \vec{0}$ , pero como  $\ker(f^n) = \ker(f^{2n})$ , entonces  $f^{2n}(y) = \vec{0}$ , y  $y \in \ker(f^{2n}) = \ker(f^n)$ , por lo que  $z = f^n(y) = \vec{0}$ . y en síntesis  $f^n(z - f^n(y)) = \vec{0}$ .

Sea  $x \in M$ , luego,  $f^n(x) \in f^n[M] = f^{2n}[M]$ , por lo que  $f^n(x) = f^{2n}(y)$ , luego  $f^n(x - f^n(y)) = \vec{0}$  y, por ende,

$$x = f^n(y) + (x - f^n(y)) \in f^\infty M + f^{-\infty} 0. \quad \square$$

**Corolario 5.47.1:** Sea  $M$  un  $A$ -módulo noetheriano y artiniiano. Si  $M$  es indecomponible, entonces todo endomorfismo de  $M$  es un automorfismo o es nilpotente. En particular,  $M$  es fuertemente indecomponible.

Finalmente, y aplicando lo visto en el teorema de Jordan-Hölder se obtiene que:

**Teorema 5.48 (Krull-Schmidt):** Sea  $M \neq 0$  un  $A$ -módulo noetheriano y artiniiano, entonces existen  $M_i$ 's indecomponibles 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 5.49:** Sean  $M, N, T$  un trío de  $A$ -módulos. Una aplicación  $\varphi: M \times N \rightarrow T$  es  **$A$ -bilineal** si es un morfismo en cada coordenada, formalmente:

BL1. Si para todo  $\mathbf{n}_0 \in N$  se cumple que la aplicación  $\mathbf{m} \mapsto \varphi(\mathbf{m}, \mathbf{n}_0)$  es un morfismo de  $A$ -módulos.

BL2. Si para todo  $\mathbf{m}_0 \in M$  se cumple que la aplicación  $\mathbf{n} \mapsto \varphi(\mathbf{m}_0, \mathbf{n})$  es un morfismo de  $A$ -módulos.

Se denota por  $\text{Bil}_A(M \times N, T)$  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  $\det: k^2 \times k^2 \rightarrow k$  es claramente  $k$ -bilineal (por definición, de hecho), pero no es  $k$ -lineal en sí misma, de hecho, si  $\text{car } k \neq 2$ , entonces

$$\det((2, 0), (0, 2)) = 4 \neq 2 = 2 \det((1, 0), (0, 1)).$$

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 5.50:** Fijemos un par de  $A$ -módulos  $M, N$ .

1. Para todo  $A$ -módulo  $T$ , se cumple que  $\text{Bil}_A(M \times N, T)$  es un  $A$ -módulo.
2. Dado un homomorfismo de  $A$ -módulos  $f: T_1 \rightarrow T_2$  se cumple que la poscomposición:

$$\begin{aligned} h^f: \text{Bil}_A(M \times N, T_1) &\longrightarrow \text{Bil}_A(M \times N, T_2) \\ \varphi &\longmapsto \varphi \circ f \end{aligned}$$

es también un homomorfismo de  $A$ -módulos.

3. Dado  $\text{Id}_T: T \rightarrow T$  se cumple que  $h^T = \text{Id}: \text{Bil}_A(M \times N, T) \rightarrow \text{Bil}_A(M \times N, T)$ .
4. Dados  $f: T_1 \rightarrow T_2, g: T_2 \rightarrow T_3$  homomorfismos de  $A$ -módulos, se cumple que  $h^{f \circ g} = h^f \circ h^g$ .

En resumen,  $\text{Bil}_A(M \times N, -): \text{Mod}_A \rightarrow \text{Mod}_A$  es un funtor:

$$\begin{array}{ccc} T_1 & \text{Bil}_A(M \times N, T_1) & \\ f \downarrow & \xrightarrow{\text{Bil}_A(M \times N, -)} \downarrow h^f & \\ T_2 & \text{Bil}_A(M \times N, T_2) & \end{array}$$

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 5.51:** Un par  $(M \otimes_A N, \otimes)$  es un producto tensorial de  $M, N$  si:

PT1.  $\otimes: M \times N \rightarrow M \otimes_A N$  es una aplicación  $A$ -bilineal.

PT2. Para toda aplicación  $A$ -bilineal  $\varphi: M \times N \rightarrow T$  existe un único homomorfismo de  $A$ -módulos  $\bar{\varphi}: M \otimes_A N \rightarrow T$  tal que  $\varphi = \otimes \circ \bar{\varphi}$ . Es decir, el siguiente diagrama conmuta (en **Set**):

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes_A N \\ & \searrow \varphi & \downarrow \exists! \bar{\varphi} \\ & & T \end{array}$$

Equivalentemente,  $M \otimes_A N$  es un objeto representado por el funtor  $\text{Bil}_A(M \times N, -)$ .

Cuando no haya ambigüedad sobre los signos podemos obviar el subíndice « $A$ ».

**Teorema 5.52:** 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  $j: M \times N \rightarrow F(M \times N)$  que

manda cada objeto en sí mismo sea bilineal. Sea  $K$  el submódulo generado por todos los elementos de la forma

$$j(\alpha \mathbf{m}_1 + \beta \mathbf{m}_2, \mathbf{n}) - \alpha j(\mathbf{m}_1, \mathbf{n}) - \beta j(\mathbf{m}_2, \mathbf{n})$$

con  $\alpha, \beta \in A$ ,  $\mathbf{m}_1, \mathbf{m}_2 \in M$  y  $\mathbf{n} \in N$ ; y los elementos de la forma

$$j(\mathbf{m}, \alpha \mathbf{n}_1 + \beta \mathbf{n}_2) - \alpha j(\mathbf{m}, \mathbf{n}_1) - \beta j(\mathbf{m}, \mathbf{n}_2)$$

con  $\alpha, \beta \in A$ ,  $\mathbf{m} \in M$  y  $\mathbf{n}_1, \mathbf{n}_2 \in N$ . Finalmente definamos

$$M \otimes N := \frac{F(M \times N)}{K},$$

junto a la aplicación:

$$\begin{array}{ccccc} & & \otimes & & \\ & \searrow & & \swarrow & \\ M \times N & \xrightarrow{j} & F(M \times N) & \xrightarrow{\pi} & M \otimes N \end{array}$$

Nótese de que por construcción de  $K$  se cumple que  $\otimes$  resulte bilineal.

Luego hay que verificar que se satisfaga la propiedad universal. Sea  $\varphi: M \times N \rightarrow T$  bilineal, entonces por definición de módulo libre se cumple que existe:

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi} & T \\ \downarrow j & \nearrow \exists! \hat{\varphi} & \\ F(M \times N) & & \end{array}$$

tal que el diagrama conmuta, donde  $\hat{\varphi}$  es un morfismo de  $A$ -módulos. Basta probar que  $\hat{\varphi}$  se anula en  $K$ :

$$\begin{aligned} & \hat{\varphi}(j(\alpha \mathbf{m}_1 + \beta \mathbf{m}_2, \mathbf{n}) - \alpha j(\mathbf{m}_1, \mathbf{n}) - \beta j(\mathbf{m}_2, \mathbf{n})) \\ &= \hat{\varphi}(j(\alpha \mathbf{m}_1 + \beta \mathbf{m}_2, \mathbf{n})) - \alpha \hat{\varphi}(j(\mathbf{m}_1, \mathbf{n})) - \beta \hat{\varphi}(j(\mathbf{m}_2, \mathbf{n})) \\ &= \varphi(\alpha \mathbf{m}_1 + \beta \mathbf{m}_2, \mathbf{n}) - \alpha \varphi(\mathbf{m}_1, \mathbf{n}) - \beta \varphi(\mathbf{m}_2, \mathbf{n}) \\ &= \vec{0}. \end{aligned}$$

De lo cual se sigue que el siguiente diagrama necesariamente conmuta:



$$\begin{array}{ccc}
M \times N & \xrightarrow{\varphi} & T \\
j \downarrow & & \uparrow \hat{\varphi} \\
F(M \times N) & \xrightarrow{\quad} & \\
\pi \downarrow & & \uparrow \exists! \bar{\varphi} \\
M \otimes N = F(M \times N)/K & & 
\end{array}$$

□

**Definición 5.53:** 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

$$\mathbf{m}_1 \otimes \mathbf{n}_1 + \mathbf{m}_2 \otimes \mathbf{n}_2 + \cdots + \mathbf{m}_s \otimes \mathbf{n}_s,$$

con  $s > 0$ ,  $\mathbf{m}_i \in M$  y  $\mathbf{n}_i \in N$  (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  $\mathbf{m} \otimes \mathbf{n}$  se le dicen *tensores puros*. Nótese que los tensores puros generan al resto de tensores, pero ellos no constituyen necesariamente todos los tensores.

**Proposición 5.54:** Si  $M = \text{Span}_A(B)$  y  $N = \text{Span}_A(C)$ , entonces

$$M \otimes_A N = \text{Span}_A(\{\mathbf{b} \otimes \mathbf{c} : \mathbf{b} \in B, \mathbf{c} \in C\}).$$

DEMOSTRACIÓN: Basta notar que si

$$\mathbf{m} = \lambda_1 \mathbf{b}_1 + \cdots + \lambda_s \mathbf{b}_s$$

entonces  $\mathbf{m} \otimes \mathbf{n} = \sum_{i=1}^s \lambda_i (\mathbf{b}_i \otimes \mathbf{n}_i)$ . □

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 5.55:** Sean  $M, N, T$  un trío de  $A$ -módulos, entonces

$$\text{Hom}_A(M \otimes_A N, T) \cong \text{Hom}_A(M, \text{Hom}_A(N, T))$$

(como  $A$ -módulos).

DEMOSTRACIÓN: Sea  $\alpha \in \text{Hom}_A(M, \text{Hom}_A(N, T))$ , eso quiere decir que  $\alpha(\mathbf{m}) \in \text{Hom}_A(N, T)$ . Luego la siguiente aplicación:

$$\begin{aligned} \varphi: M \times N &\longrightarrow T \\ (\mathbf{m}, \mathbf{n}) &\longmapsto \alpha(\mathbf{m})(\mathbf{n}) \end{aligned}$$

es  $A$ -bilineal, y por ende admite una única factorización  $\bar{\alpha}: M \otimes_A N \rightarrow T$  (que es un morfismo de  $A$ -módulos) tal que  $\otimes \circ \bar{\alpha} = \alpha$ . Queda al lector comprobar que la aplicación  $\alpha \mapsto \bar{\alpha}$  es el isomorfismo de  $A$ -módulos deseado.  $\square$

Ésto puede parecer un resultado parcialmente inofensivo, pero demuestra una intrínseca dualidad especial entre los tensores y los conjuntos  $\text{Hom}$ 's.

**Proposición 5.56:** Sean  $M, N, T$  un trío de  $A$ -módulos, entonces:

1.  $M \otimes_A N \cong N \otimes_A M$ .
2.  $(M \oplus N) \otimes_A T \cong (M \otimes_A T) \oplus (N \otimes_A T)$ .
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  $\{\varphi_i: M_i \otimes T \rightarrow N\}_{i \in I}$  una familia de morfismos de  $A$ -módulos. Vale decir,

$$\varphi_i \in \text{Hom}_A(M_i \otimes_A T, N) \iff \bar{\varphi}_i \in \text{Hom}_A(M_i, \text{Hom}_A(T, N));$$

luego existe una única extensión tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} & \text{Hom}_A(T, N) & \\ \uparrow \exists! \bar{\psi} & \nwarrow \bar{\varphi}_j & \\ \bigoplus_{i \in I} M_i & \longleftarrow & M_j \end{array}$$

finalmente consideramos que  $\bar{\psi} \in \text{Hom}(\bigoplus_{i \in I} M_i, \text{Hom}_A(T, N))$  lo devolvemos a  $\psi \in \text{Hom}((\bigoplus_{i \in I} M_i) \otimes_A T, N)$ . Queda al lector comprobar que  $\psi$  es una extensión única.

Para la sexta emplee  $\otimes: (a, \mathbf{m}) \mapsto a\mathbf{m}$  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  $\text{Hom}$  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  $A/\mathfrak{a} \otimes_A M \cong M/\mathfrak{a}M$ .  $\square$

**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

$$\bar{f} := f \otimes \mathbb{Z}/2\mathbb{Z}: \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

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 5.57 (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.  $\text{Hom}_A(M, \text{Hom}_B(P, N)) \cong \text{Hom}_B(M \otimes_A P, N)$ .
2.  $(M \otimes_A P) \otimes_B N \cong M \otimes_A (P \otimes_B N)$ .

DEMOSTRACIÓN: En la primera, interpretamos que  $\text{Hom}_B(P, N)$  es un  $A$ -módulo con el producto escalar  $\varphi \in \text{Hom}_B(P, N)$  dado por  $a\varphi(x) = \varphi(ax)$ . Dado un homomorfismo de  $B$ -módulos  $\psi: M \otimes_A P \rightarrow N$ , entonces podemos definir

$$\begin{aligned} f(\psi): M &\longrightarrow \text{Hom}_B(P, N) \\ m &\longmapsto (p \mapsto \psi(m \otimes p)). \end{aligned}$$

Recíprocamente, dado  $\phi: M \rightarrow \text{Hom}_B(P, N)$  podemos definir  $\bar{\phi} := g(\phi): M \otimes_A P \rightarrow N$  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 5.55 y aplicamos para un  $B$ -módulo  $T$ :

$$\begin{aligned} \text{Hom}_B((M \otimes_A P) \otimes_B N, T) &\cong \text{Hom}_B(M \otimes_A P, \text{Hom}_B(N, T)) \\ &\cong \text{Hom}_A(M, \text{Hom}_B(P, \text{Hom}_B(N, T))) \\ &\cong \text{Hom}_A(M, \text{Hom}_B(P \otimes_B N, T)) \\ &\cong \text{Hom}_B(M \otimes_A (P \otimes_B N), T). \quad \square \end{aligned}$$

**Definición 5.58:** 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 5.59:** Un  $A$ -módulo  $M = \bigoplus_{i \in I} M_i$  es (fielmente) plano si y sólo si 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 injectivos

**Definición 5.60:** Sea  $P$  un  $A$ -módulo.  $P$  se dice un **módulo proyectivo** si para todo par de  $A$ -módulos  $M, N$ , y todo  $f: P \rightarrow N$  y  $p: M \rightarrow N$  homomorfismos de  $A$ -módulos, con  $p$  suprayectivo, existe un  $g: P \rightarrow M$  tal que el siguiente diagrama:

$$\begin{array}{ccc} & P & \\ g \swarrow & & \downarrow f \\ M & \xrightarrow{p} & N \end{array}$$

conmuta.

**Proposición 5.61:** La suma directa de módulos proyectivos es proyectiva.

DEMOSTRACIÓN: Basta considerar el siguiente diagrama conmutativo:

$$\begin{array}{ccc} P_j & \hookrightarrow & \bigoplus_{i \in I} P_i \\ g_j \downarrow & \swarrow \sum_{i \in I} g_i & \downarrow f \\ M & \xrightarrow{p} & N \end{array}$$

□

Como ejercicio, note que la demostración anterior emplea un uso de elección y encuéntralo. No obstante, dicho uso puede erradicarse empleando la siguiente proposición:

**Proposición 5.62:** Un  $A$ -módulo  $P$  es proyectivo syss el funtor  $\text{Hom}_A(P, -)$  es exacto.

DEMOSTRACIÓN: Ya sabemos que  $\text{Hom}_A(P, -)$  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

$$\text{Hom}_A(P, M) \xrightarrow{h^p} \text{Hom}(P, N) \longrightarrow 0$$

también es exacto, pero ésto es la definición de ser proyectivo.

□

**Corolario 5.62.1:** El producto tensorial de finitos módulos proyectivos es proyectivo.

**Proposición (AE) 5.63:** 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:

$$\begin{array}{ccc} & P & \\ & \downarrow \text{Id}_P & \\ N & \xrightarrow[p]{} & P \end{array}$$

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  $\iota: S \rightarrow P$  induce trivialmente un epimorfismo  $p: F \rightarrow P$ . 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:

$$\begin{array}{ccc} F & \longleftarrow & P \\ & & \downarrow f \\ M & \xrightarrow[p]{} & N \end{array}$$

como  $F = P \oplus P'$  podemos definir  $\hat{f}: F \rightarrow N$  tal que se anule en  $P'$  y coincida con  $f$  en  $P$ . Sea  $X = \{\mathbf{x}_i + \mathbf{y}_i\}_{i \in I}$  una base de  $F$ , donde  $\mathbf{x}_i \in P$  e  $\mathbf{y}_i \in P'$  para todo  $i \in I$ . Podemos definir una función  $h^*: X \rightarrow M$  donde

a cada  $\mathbf{x}_i + \mathbf{y}_i$  le asigne un elemento de  $p^{-1}[\{\hat{f}(\mathbf{x}_i)\}]$  (el cuál existe porque  $p$  es suprayectivo), que luego, por definición de módulo libre, se extiende a un homomorfismo de  $A$ -módulos  $h: F \rightarrow M$ . Finalmente, queda al lector comprobar que efectivamente  $g := \iota \circ h \circ p: P \rightarrow N$  hace conmutar el diagrama.  $\square$

Y otro corolario particularmente útil es el siguiente:

**Teorema (AE) 5.64:** Los  $A$ -módulos proyectivos son planos.

**Proposición (AE) 5.65 (lema de las bases duales):** Sea  $P$  un  $A$ -módulo. Son equivalentes:

1.  $P$  es proyectivo.
2. Existe  $\{\mathbf{x}_i\}_{i \in I}$  en  $P$  y  $\{f_i\}_{i \in I}$  en  $\text{Hom}_A(P, A)$  tales que para todo  $\mathbf{x} \in P$  se cumple que  $f_i(\mathbf{x}) = 0$  para todos salvo finitos  $i \in I$ , y tal que

$$\mathbf{x} = \sum_{i \in I} f_i(\mathbf{x}) \mathbf{x}_i.$$

En cuyo caso  $\{\mathbf{x}_i\}_{i \in I}$  es un sistema generador de  $P$ . Más aún, si  $P$  es finitamente generado podemos exigir que  $I$  sea finito.

DEMOSTRACIÓN:  $\implies$ . Sea  $S := \{\mathbf{x}_i\}_{i \in I}$  un sistema de generadores de  $P$ . Luego sea  $F$  un  $A$ -módulo libre con base  $\{\mathbf{y}_i\}_{i \in I}$ , luego el morfismo  $p: F \rightarrow P$  que manda  $p(\mathbf{y}_i) = \mathbf{x}_i$  es suprayectivo, por lo que se factoriza en  $q: P \rightarrow F$  tal que  $q \circ p = \text{Id}_P$ . Como  $F$  es libre, la aplicación  $\pi_j: F \rightarrow A$  dada por

$$\pi_j \left( \sum_{i \in I} a_i \mathbf{y}_i \right) = a_j$$

está bien definida y es un homomorfismo; más aún, para un  $\mathbf{y} \in F$  fijo,  $\pi_j(\mathbf{y})$  es nulo para todos salvo finitos  $i \in I$ . Luego definimos  $f_i := q \circ \pi_i$  y comprobamos que cumple lo exigido.

$\impliedby$ . Nuevamente, sea  $F$  un  $A$ -módulo libre con base  $\{\mathbf{y}_i\}_{i \in I}$  y considere el epimorfismo  $p: F \rightarrow P$  que manda  $p(\mathbf{y}_i) = \mathbf{x}_i$ . Nótese que trivialmente  $\tau_j: \mathbf{x} \mapsto f_j(\mathbf{x}) \mathbf{y}_j$  es un homomorfismo de módulos, que induce el siguiente homomorfismo

$$s := \sum_{i \in I} \tau_i: P \longrightarrow F$$

$$x \mapsto \sum_{i \in I} f_i(x) y_i$$

que satisface que  $s \circ p = \text{Id}_P$ . Finalmente la sucesión:

$$0 \longrightarrow \ker p \longrightarrow F \xrightarrow{p} P \longrightarrow 0$$

es exacta y se escinde.  $\square$

Pese al nombre no se confunda, ni  $\{x_i\}_{i \in I}$  ni  $\{f_i\}_{i \in I}$  tienen por que ser bases.

Ahora estudiemos un poco a los módulos inyectivos:

**Teorema (AE) 5.66 – Criterio de Baer.** Un  $\Lambda$ -módulo izquierdo  $Q$  es inyectivo syss todo homomorfismo  $f: \mathfrak{a} \rightarrow Q$ , donde  $\mathfrak{a}$  es un ideal izquierdo de  $\Lambda$ , posee una extensión  $g: \Lambda \rightarrow Q$ .

DEMOSTRACIÓN:  $\implies$ . Trivial.

$\impliedby$ . Sea  $f: N \rightarrow Q$  un homomorfismo de módulos, donde  $N$  es un submódulo de  $M$ ; nos basta extender a  $f$  para comprobar que  $Q$  es un módulo inyectivo. Consideremos a la familia  $\mathcal{F}$  de pares ordenados  $(N', h)$ , donde  $N \leq N' \leq M$  y  $h: N' \rightarrow Q$  es un homomorfismo que extiende a  $f$ . Y consideremos, sobre dicho conjunto, la siguiente relación de orden parcial:

$$(N_1, h_1) \preceq (N_2, h_2) \iff N_1 \leq N_2 \wedge h_2 \upharpoonright N_1 = h_1.$$

$(\mathcal{F}, \preceq)$  satisface las hipótesis del lema de Zorn (¿por qué?), luego admite un elemento maximal  $(\tilde{N}, g)$ . Basta ver que  $\tilde{N} = M$ , lo que haremos por contradicción: Si  $\tilde{N} \subset M$ , entonces sea  $x \in M \setminus \tilde{N}$  y consideremos a  $\tilde{N} + \Lambda \cdot x \supset \tilde{N}$ , y definamos

$$\mathfrak{a} := \{r \in \Lambda : rx \in \tilde{N}\}.$$

Nótese que  $\mathfrak{a} = \text{Ann}(\Lambda \cdot x + \tilde{N})$  en  $M/\tilde{N}$ , de modo que es un ideal de  $\Lambda$  e induce el siguiente homomorfismo de módulos:

$$\begin{aligned} h: \mathfrak{a} &\longrightarrow M \\ r &\longmapsto g(rx) \end{aligned}$$

Por hipótesis  $h$  se extiende a  $\bar{h}: \Lambda \rightarrow M$ . Luego nótese que  $\bar{g}(rx + n) := \bar{h}(rx) + g(n)$  para todo  $n \in \tilde{N}$  y todo  $r \in \Lambda$ , es un homomorfismo de módulos bien definido (¿por qué?) que extiende a  $g$ ; lo que contradice la maximalidad de  $(\tilde{N}, g)$ .  $\square$



**Definición 5.67:** Se dice que un  $\Lambda$ -módulo (izquierdo)  $M$  es *divisible* por  $a \in \Lambda_{\neq 0}$  si  $a \cdot M = M$ . Un módulo  $M$  se dice *divisible* (a secas) si para todo  $a \in \Lambda_{\neq 0}$  se cumple que  $aM = M$ .

**Proposición 5.68:** Todo cociente de un módulo divisible es divisible.

**Proposición 5.69:** Se cumplen:

1. Si  $\Lambda$  es un dominio íntegro, entonces todo  $\Lambda$ -módulo inyectivo es divisible.
2. (AE) Más aún, si  $\Lambda$  es un DIP, todo  $\Lambda$ -módulo divisible es inyectivo.

DEMOSTRACIÓN:

1. Sea  $Q$  un  $\Lambda$ -módulo inyectivo, sea  $\mathbf{x} \in Q$  y  $r \in \Lambda_{\neq 0}$ . Como  $\Lambda$  es un dominio íntegro, admite cancelación y luego la aplicación  $ar \mapsto a\mathbf{x}$  es un homomorfismo de módulos bien definido desde  $a\Lambda$  hasta  $Q$ . Sea  $\varphi(1) = \mathbf{y}$ , luego

$$\mathbf{x} = \varphi(r) = r\varphi(1) = r\mathbf{y},$$

y como aplica todo  $\mathbf{x} \in Q$ , se concluye que  $Q$  es divisible por  $r$ .

2. Sea  $M$  un  $\Lambda$ -módulo divisible y sea  $f: (r) \rightarrow M$  un homomorfismo de anillos, donde  $r \in \Lambda$ . Si  $r = 0$ , entonces se puede extender al homomorfismo nulo. Si  $r \neq 0$ , entonces  $f(r) = \mathbf{x}$  y como  $M$  es divisible, existe  $\mathbf{y} \in M$  tal que  $\mathbf{x} = r\mathbf{y}$ ; luego  $g(a) := a\mathbf{y}$  es un homomorfismo de módulos desde  $\Lambda$  hasta  $M$  que extiende a  $f$ , y concluimos por el criterio de Baer.  $\square$

**Corolario (AE) 5.69.1:** Todo cociente de un módulo inyectivo es también un módulo inyectivo.

**Proposición 5.70:** Todo grupo abeliano (visto como  $\mathbb{Z}$ -módulo) está encajado en un  $\mathbb{Z}$ -módulo divisible.

DEMOSTRACIÓN: Sea  $F$  un grupo abeliano libre de base  $\{x_i\}_{i \in I}$ , luego podemos definir a  $F'$  como el  $\mathbb{Q}$ -espacio vectorial libre de base  $\{x_i\}_{i \in I}$ , y, vistos como  $\mathbb{Z}$ -módulos, claramente  $F$  está encajado en  $F'$ , y  $F'$  es divisible. Sea  $M$  un  $\mathbb{Z}$ -módulo arbitrario, entonces  $M \cong F/K$  donde  $F$  es libre; luego  $M \leq F'/K$  que es divisible.  $\square$

**Teorema 5.71:** Sea  $Q$  un  $\Lambda$ -módulo. Son equivalentes:

1.  $Q$  es inyectivo.
2. Toda sucesión exacta corta:

$$0 \longrightarrow Q \xrightarrow{i} M \longrightarrow N \longrightarrow 0$$

se escinde.

3.  $Q$  es el sumando directo de que todo módulo que le contiene.

DEMOSTRACIÓN: 1  $\implies$  2. Análogo al caso de módulos proyectivos.

2  $\implies$  3. Es claro de la proposición 5.15.

3  $\implies$  1. Sea  $M$  un módulo inyectivo tal que  $Q \subseteq M$ , luego  $M = Q \oplus M'$  y en particular existen homomorfismos  $\iota: Q \rightarrow M$  y  $\pi: M \rightarrow Q$  tales que  $\iota\pi = \text{Id}_Q$ . Dados  $q: N' \rightarrow N$  y  $f: N' \rightarrow Q$  homomorfismos, con  $q$  inyectivo, podemos construir el siguiente diagrama conmutativo:

$$\begin{array}{ccc} N' & \xrightarrow{q} & N \\ f \downarrow & \swarrow g \circ \pi & \\ Q & & \\ \pi \uparrow & \nwarrow \exists! g & \\ M & & \end{array}$$

Para verificar que  $h := g \circ \pi$  es el único que hace conmutar el diagrama, supongamos que hubiese otro  $h'$ , entonces necesariamente, en ambos casos,  $g = h \circ \iota = h' \circ \iota$ , y luego  $h = h \circ \iota \circ \pi = h' \circ \iota \circ \pi = h'$ .  $\square$

Ahora nos enfocaremos en tratar de mejorar la inclusión de los módulos en módulos inyectivos y para ello necesitaremos dos conceptos:

**Definición 5.72:** Se dice que un submódulo  $G \leq M$  es **grande** si para todo submódulo  $N \leq G$  no trivial, se cumple que  $N \cap G$  no es trivial. Un homomorfismo  $\varphi: M \rightarrow N$  se dice **esencial** si  $\text{Im } \varphi \leq N$  es un submódulo grande.

El teorema principal nos dirá que todo módulo está esencialmente encajado en un módulo inyectivo.

**Proposición (AE) 5.73:** Un  $\Lambda$ -módulo  $Q$  es inyectivo syss todo monomorfismo esencial  $f: Q \rightarrow M$  es un isomorfismo.

DEMOSTRACIÓN:  $\implies$ . Podemos extenderlo a la siguiente sucesión exacta:

$$0 \longrightarrow Q \xrightarrow{f} M \longrightarrow M/f[Q] \longrightarrow 0$$

de modo que por el teorema anterior se tiene que  $M = f[Q] \oplus M/f[Q]$ . Como  $f$  es un monomorfismo esencial y  $M/f[Q] \cap f[Q] = 0$ , entonces  $M/f[Q] = 0$ , por lo que  $f$  es un isomorfismo.

$\Leftarrow$ . Dada la siguiente sucesión exacta:

$$0 \longrightarrow Q \xrightarrow{f} M \longrightarrow M/f[Q] \longrightarrow 0$$

veremos que se escinde para ver que  $Q$  es inyectivo. Para ello sea  $S \leq M$  el submódulo maximal (por el lema de Zorn) tal que  $f[Q] \cap S$  es trivial. Luego, consideremos el módulo  $M/S$ . La aplicación  $j := f \circ \pi: Q \rightarrow M/S$  es inyectiva y su imagen es  $\frac{f[Q]+S}{S}$ . Sea  $T/S \leq M/S$  con  $S \subseteq T \leq M$  tal que

$$\frac{T}{S} \cap \frac{f[Q]+S}{S} = 0 = \frac{S}{S},$$

entonces  $T \cap (f[Q] + S) \subseteq S$ , por lo que  $T \cap f[Q] \subseteq S \cap f[Q] = 0$ , de modo que  $T = S$  por maximalidad de  $S$ . De modo que  $j$  es un monomorfismo esencial, y por hipótesis, es un isomorfismo. Como

$$\frac{M}{S} = \frac{f[Q]+S}{S} \implies M = f[Q] + S$$

y como  $f[Q] \cap S = 0$ , entonces  $M = f[Q] \oplus S$  por lo que la sucesión original se escinde.  $\square$

**Lema (AE) 5.74:** Dado  $k: Q \rightarrow N$  un monomorfismo esencial y  $j: Q \rightarrow Q_0$  un monomorfismo, donde  $Q_0$  es inyectivo. Entonces existe un monomorfismo  $f: N \rightarrow Q_0$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} Q & \xhookrightarrow{k} & N \\ j \downarrow & \nearrow f & \\ Q_0 & & \end{array}$$

DEMOSTRACIÓN: Como  $Q_0$  es inyectivo, entonces existe  $f$ , por lo que sólo basta ver que es un monomorfismo. Sea  $\mathbf{n} \in \ker f \cap \text{Im } k$ , luego  $\mathbf{n} = k(\mathbf{q})$  para algún  $\mathbf{q} \in Q$  y

$$\vec{0} = f(\mathbf{n}) = f(k(\mathbf{q})) = j(\mathbf{q}),$$

pero  $\ker j = 0$ , luego  $\ker f \cap \text{Im } k = 0$ , pero  $\text{Im } k$  es un módulo grande, así que  $\ker f = 0$ .  $\square$

**Teorema (AE) 5.75:** Para todo módulo  $M$  existe un monomorfismo esencial  $j: M \rightarrow Q$ , donde  $Q$  es inyectivo. Más aún, si existe otro monomorfismo esencial  $k: M \rightarrow Q'$  con  $Q'$  inyectivo, entonces existe un isomorfismo  $\ell: Q \rightarrow Q'$  tal que  $j\ell = k$ .

DEMOSTRACIÓN: Ya sabemos que existe un monomorfismo  $\iota_0: M \rightarrow Q_0$ , donde  $Q_0$  es un módulo inyectivo. Sea  $Q \leq Q_0$  el submódulo maximal (por lema de Zorn) en el que  $\iota_0[M]$  es grande. Llamemos  $\iota := \iota_0|_Q$  y sea  $f: Q \rightarrow Q_0$  la inclusión. Sea  $k: Q \rightarrow N$  un monomorfismo esencial arbitrario, todo se sintetiza en el siguiente diagrama conmutativo:

$$\begin{array}{ccccc} M & \xrightarrow{\iota} & Q & \xrightarrow{k} & N \\ & \searrow \iota_0 & \downarrow f & \nearrow \ell & \\ & & Q_0 & & \end{array}$$

donde la existencia del  $\ell$  viene del lema anterior. Luego  $\ell[N]$  es un submódulo de  $Q_0$  y  $\ell[k[Q]] = Q \leq \ell[N]$  es grande, y como  $\iota[M]$  es grande en  $Q$ , entonces también lo es en  $\ell[N]$  y por maximalidad  $\ell[N] = Q$ , luego  $\ell$  es un isomorfismo y  $Q$  es inyectivo por la proposición 5.73.

La unicidad queda de ejercicio para el lector.  $\square$

**Definición 5.76:** Dado un  $\Lambda$ -módulo  $M$  se dice que su *envoltura inyectiva* es el único módulo inyectivo (salvo isomorfismo) que satisface el teorema anterior.

## 5.5 Módulos sobre DIPs

El primer resultado que queremos ver que sobre un DIP todo submódulo de un módulo libre es libre. Para ello volveremos un poco al tema de grupos abelianos:

**Proposición 5.77:** 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.  $\square$

**Corolario 5.77.1:** 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  $\kappa$ .
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.  $\square$

**Definición 5.78:** Dado un grupo abeliano libre  $G$ , se denota por  $\text{rang } G$  a la cardinalidad de cualquiera de sus bases.

**Proposición 5.79:** Sea  $G$  un grupo abeliano con un conjunto  $X$  tal que satisface lo siguiente: Para todo grupo abeliano  $H$  y toda aplicación  $f: X \rightarrow H$ , existe una única extensión  $f^*: G \rightarrow H$  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  $q: X \rightarrow Y$  de inversa  $p: Y \rightarrow X$ . Luego, por ser libres, ambas funciones se extienden a  $f: G \rightarrow H$  y  $g: H \rightarrow G$ , homomorfismos de grupos. Nótese que además  $p \circ q = \text{Id}_X: X \rightarrow X \subseteq G$  es una aplicación que posee una extensión  $\text{Id}_G: G \rightarrow G$  que es única, y lo mismo vale para  $\text{Id}_H$  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.  $\square$

**Proposición (AE) 5.80:** 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  $g: X \rightarrow M$  dada por  $g([x_i]) := x_i$  admite una extensión única  $g: M/N \rightarrow M$ , tal que  $g \circ \pi$  fija a la base, luego por unicidad, se cumple que  $g \circ \pi = \text{Id}_{M/N}$ . Es decir, la sucesión exacta se escinde y por la proposición 5.15 se cumple el enunciado.  $\square$

Como ejercicio en la demostración anterior ubique el uso de elección.

**Teorema (AE) 5.81:** Sea  $A$  un DIP, entonces todo  $A$ -submódulo  $M$  de un módulo libre  $F$  es también libre; y de hecho  $\text{rang } M \leq \text{rang } F$ .

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

$$F'_\beta := \langle \{x_\alpha : \alpha < \beta\} \rangle, \quad F_\beta := F'_\beta \oplus \langle x_\beta \rangle.$$

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  $M_\beta/M'_\beta$  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  $M_\beta \cong M'_\beta \oplus \langle \mathbf{m}_\beta \rangle$  para algún  $\mathbf{m}_\beta \in M_\beta$  tal que  $\langle \mathbf{m}_\beta \rangle \cong A$ ; si el ideal es nulo entonces  $\mathbf{m}_\beta := \vec{0}$ . Claramente, eliminando los  $\mathbf{m}_\beta$ '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  $M^* := \text{Span}\{\mathbf{m}_\beta\}_{\beta < \kappa}$  y definamos:

$$\mu(\mathbf{m}) := \min\{\alpha : \mathbf{m} \in F_\alpha\}.$$

Supongamos que  $M^* < M$ , entonces definamos  $\gamma$  como el mínimo índice tal que  $\gamma = \mu(\mathbf{m})$  para algún  $\mathbf{m} \in M \setminus M^*$  y sea  $\tilde{\mathbf{m}}$  un elemento que cumpla lo anterior, luego se cumple que

$$\tilde{\mathbf{m}} = \mathbf{a} + \lambda \mathbf{m}_\gamma \in M_\gamma$$

para unos únicos  $\mathbf{a} \in M'_\gamma$  y  $\lambda \in A$ . Luego como  $\mathbf{m}_\gamma \in M^*$  y  $\tilde{\mathbf{m}} \notin M^*$  necesariamente se tiene que  $\mathbf{a} \notin M^*$ . Pero  $\mathbf{a} \in F'_\gamma$ , luego  $\mu(\mathbf{a}) < \gamma$  contradiciendo la minimalidad de  $\gamma$ .  $\square$

Nótese que si  $F$  es finitamente generado, entonces no hay uso de elección.

**Corolario (AE) 5.81.1:** En un DIP todo módulo proyectivo es libre.

Éste teorema se puede mejorar, pero requiere más trabajo (ver teo. 6.45).

**Corolario (AE) 5.81.2:** En un DIP todo submódulo de un módulo proyectivo es también proyectivo.

**Definición 5.82:** Sea  $A$  un dominio íntegro y sea  $M$  un  $A$ -módulo. Entonces para  $a \in A_{\neq 0}$  el endomorfismo  $u \mapsto a \cdot u$  se denota  $M \xrightarrow{\times a} M$ . Se define el **submódulo de  $a$ -torsión** de  $M$ :

$$M[a] := \ker(M \xrightarrow{\times a} M) = \{u \in M : au = 0\}.$$

Se define el **submódulo de torsión** como

$$M_{\text{tors}} := \bigcup_{a \in A_{\neq 0}} M[a] = \{u \in M : \exists a \in A_{\neq 0} \quad au = 0\}.$$

Se dice que  $M$  es un **módulo de pura torsión** si  $M_{\text{tors}} = M$ , o que es **libre de torsión** si  $M_{\text{tors}} = 0$ .

Para elementos de  $M$ , decimos que  $u \in M_{\neq 0}$  es *de torsión* (resp. *libre de torsión*) si  $u \in M_{\text{tors}}$  (resp.  $u \notin M_{\text{tors}}$ ).

Nos adentramos a la clasificación de módulos sobre un DIP, que es una generalización del teorema fundamental de grupos abelianos. El teorema tiene tres pasos: separar apropiadamente un módulo en una parte de torsión y otra libre de torsión, y los otros dos pasos consisten en clasificar ambas partes.

Señala ALUFFI [0] que la torsión es «la manera más espectacular en que un módulo puede no ser libre».

**Teorema 5.83:** Sea  $A$  un DIP y  $M$  un  $A$ -módulo finitamente generado libre de torsión. Entonces  $M$  es libre.

DEMOSTRACIÓN: Denotemos  $\mu(M)$  la cantidad mínima de generadores que admite  $M$ , la cual es finita por hipótesis. Procedemos por inducción sobre  $n := \mu(M)$ . Para el caso  $n = 1$ , tenemos que  $M = A\langle u \rangle$  y como  $u$  es libre de torsión, entonces es  $A$ -linealmente independiente, luego  $\{u\}$  es una base de  $M$ .

Sea  $\{u_1, \dots, u_n\}$  un sistema generador minimal y sea

$$M_1 := \{v \in M : \exists a \in A_{\neq 0} \quad av \in Au_n\},$$

luego  $M/M_1$  está generado por  $\{[u_1], \dots, [u_{n-1}]\}$ . Sea  $w \in M/M_1$  tal que  $bw \equiv 0$  (mód  $M_1$ ), es decir,  $a(bw) = (ab)w \in Au_1$ , de modo que  $w \in M_1$ , es decir,  $[w] = 0$ . Así, comprobamos que  $M/M_1$  es libre de torsión y, por hipótesis inductiva, es libre de rango  $\leq n-1$ . Como  $M/M_1$  es libre, entonces es proyectivo y, por tanto,  $M \cong M_1 \oplus (M/M_1)$ .

Ahora estudiemos a  $M_1$ . Como  $A$  es noetheriano, entonces  $M_1$  es finitamente generado por  $\{y_1, \dots, y_m\}$ . Así pues  $a_i y_i = b_i u_n$  y definamos  $q := a_1 a_2 \cdots a_m$ . Probaremos que si  $av = bu_n$ , entonces  $a \mid bq$ : Nótese que si  $v = \sum_{j=1}^m c_j y_j$ , entonces

$$qv = \sum_{j=1}^m c_j q y_j = \left( \sum_{j=1}^m c_j (q/a_j) b_j \right) u_n.$$

De modo que

$$bqu_n = aqv = a \left( \sum_{j=1}^m c_j (q/a_j) b_j \right) u_n,$$

y así  $a \mid bq$  como se quería probar.

Empleando esto, podemos definir  $\varphi: M_1 \rightarrow A$  dado por  $\varphi(v) = bq/a$ . Ésta aplicación está bien definida pues si  $av = bu_n$  y  $a'v = b'u_n$ , entonces



$a'bu_n = a'av = ba'u_n$ , de modo que  $bq/a = b'q/a'$ . Más aún, es claramente un  $A$ -homomorfismo, de modo que  $\text{Im } \varphi =: \mathfrak{a} \trianglelefteq A$  es un ideal. Además,  $\varphi$  es claramente inyectiva, por lo que,  $M_1 \cong \text{Im } \varphi$  y, como  $A$  es DIP,  $\mathfrak{a} = \alpha A$ , por lo que  $M_1$  es un  $A$ -módulo libre de rango 1 como se quería probar.  $\square$

**Ejemplo.** Lo anterior falla si permitimos que  $M$  no sea finitamente generado. En efecto,  $\mathbb{Q}$  es un  $\mathbb{Z}$ -módulo libre de torsión que no es libre.

**Corolario 5.83.1:** Sea  $A$  un DIP y  $M$  un  $A$ -módulo finitamente generado. Entonces  $M/M_{\text{tors}}$  es libre de torsión y  $M \cong M_{\text{tors}} \oplus (M/M_{\text{tors}})$ .

**Teorema 5.84 – Teorema de estructura de módulos sobre un DIP:** Sea  $A$  un DIP, entonces todo  $A$ -módulo  $M$  finitamente generado se escribe de la forma

$$M = A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_n \oplus A^\beta,$$

donde  $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots \supseteq \mathfrak{a}_n$  son ideales de  $A$ .

## 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 [0] (1938). La construcción fue generalizada por BOURBAKI [0] (1942) quién realizó la construcción en módulos sobre anillos no conmutativos con la distinción de módulo izquierdo y derecho; esto también fue hecho independientemente por E. ARTIN *et al.* [0] (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 si el conjunto de los elementos no invertibles 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 invertible. 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 invertible y luego  $(ax)^{-1}a = x^{-1}$ .  $\square$

**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.  $\square$

**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  $\lambda_S: A \rightarrow S^{-1}A$  dada por  $\lambda_S(a) = a/1$  es un morfismo de anillos. Más aún,  $S^{-1}A$  es un  $A$ -módulo,  $\lambda_S$  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  $r(a_1s_2 - a_2s_1) = 0$  con  $r \in S$ . Nótese que basta ver que

$$\frac{a_1t + bs_1}{s_1t} = \frac{a_2t + bs_2}{s_2t}, \quad \frac{a_1b}{s_1t} = \frac{a_2b}{s_2t}.$$

Para ello nótese que

$$\begin{aligned} r((a_1t + bs_1)s_2t - (a_2t + bs_2)s_1t) &= t^2 \cdot r(a_1s_2 - a_2s_1) = 0, \\ r(a_1bs_2t - a_2bs_1t) &= bt \cdot r(a_1s_2 - a_2s_1) = 0. \end{aligned}$$

Probar que es un anillo es análogo a las demostraciones de que  $\text{Frac}(A)$  lo es. Lo mismo para notar que  $\lambda_S$  es morfismo.  $\square$

**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  $\mathfrak{a} \subseteq A$ .
2. Todos los ideales primos de  $S^{-1}A$  son de la forma  $S^{-1}\mathfrak{p}$  con  $\mathfrak{p} \subseteq A$  primo disjunto de  $S$ .

DEMOSTRACIÓN:

1. Sea  $\mathfrak{b} \subseteq S^{-1}A$  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  $\mathfrak{q} \subseteq S^{-1}A$  un ideal primo, entonces por el enunciado anterior  $\mathfrak{p} := \mathfrak{q} \cap A \subseteq A$  es un ideal primo (¿por qué?). Como  $1 \notin \mathfrak{q}$  se sigue que  $\mathfrak{p} \cap S = \emptyset$ .

Conversamente sea  $\mathfrak{p} \subseteq A$  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  $b/t \in \mathfrak{q}$ .  $\square$

**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  $\mathfrak{p} \triangleleft A$  primo. Luego  $S := A \setminus \mathfrak{p}$  es un sistema multiplicativo tal que  $(S^{-1}A, S^{-1}\mathfrak{p}, \text{Frac}(A/\mathfrak{p}))$  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.  $\square$

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 completaciones (que veremos en el capítulo ??).

**Lema 6.11:** El morfismo  $\lambda_S$  es inyectivo syss  $S$  no posee divisores de cero.

DEMOSTRACIÓN:  $\implies$ . Por contrarrecíproca: si  $a \in S$  es divisor de cero, es decir, si  $ab = 0$  con  $b \neq 0$ , entonces  $\lambda_S(b) = \lambda_S(0)$ .

$\impliedby$ . 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  $a = b$ .  $\square$

**Teorema 6.12:** Sean  $A, B$  dominios y  $S$  un sistema multiplicativo de  $A$ . Sea  $\varphi: A \rightarrow B$  un morfismo tal que  $\varphi[S] \subseteq B^\times$ , entonces el siguiente diagrama conmuta:

$$\begin{array}{ccc}
 A & \xrightarrow{\varphi} & B \\
 \lambda_S \searrow & & \nearrow \exists! S^{-1}\varphi \\
 S^{-1}A & & 
 \end{array}$$

$S^{-1}\varphi: S^{-1}A \longrightarrow B$   
 $a/s \mapsto \varphi(a)/s$

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

$$0 = \varphi(r)(\varphi(at) - \varphi(bs)) = \varphi(a)\varphi(t) - \varphi(b)\varphi(s)$$

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  $\alpha, \beta$  hacen conmutar al diagrama y sea  $a/s \in S^{-1}A$ , entonces

$$\alpha(a/s) = \alpha(a/1)\alpha(1/s) = \varphi(a)\varphi(s)^{-1} = \beta(a/1)\beta(1/s) = \beta(a/s).$$

$\square$

**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

$$(u, s) \sim (v, t) \iff \exists r \in S \quad r(ut - vs) = \vec{0}$$

es de equivalencia.

**Proposición 6.16:**  $S^{-1}M$  es un  $A$ -módulo (y un  $S^{-1}A$ -módulo también) y la función  $\lambda_S: M \rightarrow S^{-1}M$  dada por  $\lambda_S(\mathbf{m}) = \mathbf{m}/1$  es un morfismo de módulos. Más aún,  $\lambda_S$  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:

$$\begin{array}{ccc} S^{-1}f: S^{-1}M_1 \longrightarrow S^{-1}M_2 & \begin{array}{ccc} M_1 & & S^{-1}M_1 \\ f \downarrow & \xrightarrow{S^{-1}-} & \downarrow S^{-1}f \\ M_2 & & S^{-1}M_2 \end{array} \\ \mathbf{m}/s \longmapsto f(\mathbf{m})/s & & \end{array}$$

**Proposición 6.18:** Sea  $M$  un  $A$ -módulo. Entonces las siguientes son equivalentes:

1.  $M = 0$ .
2.  $M_{\mathfrak{p}} = 0$  para todo  $\mathfrak{p} \leq A$  primo.
3.  $M_{\mathfrak{m}} = 0$  para todo  $\mathfrak{m} \leq A$  maximal.

DEMOSTRACIÓN: Claramente  $1 \implies 2 \implies 3$ . Veamos  $3 \implies 1$  por contrarrecíproca: Si  $M \neq 0$  sea  $\mathbf{m} \neq \vec{0} \in M$ . Luego sea  $\mathfrak{a} := \text{Ann}(\mathbf{m}) \neq (1)$ .<sup>1</sup> Por el teorema de Krull, se cumple que  $\mathfrak{a} \subseteq \mathfrak{m}$  maximal. Luego  $\mathbf{m}/1 \in M_{\mathfrak{m}}$  y  $\mathbf{m}/1 \neq \vec{0}$ , puesto que si lo fuera entonces  $s\mathbf{m} = \vec{0}$  con  $s \in A \setminus \mathfrak{m} \subseteq A \setminus \mathfrak{a}$ , lo que es absurdo.  $\square$

<sup>1</sup>Véase def. 6.29.



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  $\text{Supp}(M)$  de todos los ideales primos  $\mathfrak{p} \triangleleft A$  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 6.19.1:** Sea  $\varphi: M \rightarrow N$  un homomorfismo de  $A$ -módulos. Entonces  $\varphi$  es inyectiva (resp. suprayectiva, isomorfismo) syss para todo  $\mathfrak{m} \triangleleft A$  maximal se cumple que  $\varphi_{\mathfrak{m}}: M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$  lo es.

**Proposición 6.20:** 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 6.21:** Sea  $M$  un  $A$ -módulo. Entonces

$$f: S^{-1}A \otimes_A M \longrightarrow S^{-1}M$$

$$\sum_{k=1}^n (a_k/s_k) \otimes \mathbf{m}_k \longmapsto \sum_{k=1}^n a_k \mathbf{m}_k / s_k.$$

es un isomorfismo, y más aún es el único entre dichos dominios.

DEMOSTRACIÓN: Consideremos la aplicación

$$\varphi: S^{-1}A \times M \longrightarrow S^{-1}M$$

$$(a/s, \mathbf{m}) \longmapsto a\mathbf{m}/s.$$

Claramente  $\varphi$  es  $A$ -bilineal y por definición de producto tensorial se cumple que existe una única  $\bar{\varphi}: S^{-1}A \otimes M \rightarrow S^{-1}M$  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

$$t_i := \prod_{\substack{k=1 \\ k \neq i}}^n s_k, \text{ luego:}$$

$$\sum_{k=1}^n \frac{a_k}{s_k} \otimes \mathbf{m}_k = \sum_{k=1}^n \frac{a_k t_k}{s} \otimes \mathbf{m}_k = \sum_{k=1}^n \frac{1}{s} \otimes a_k t_k \mathbf{m} = \frac{1}{s} \otimes \left( \sum_{k=1}^n a_k t_k \mathbf{m} \right).$$

Luego, como  $1/s$  es inversible, se cumple que  $f(1/s \otimes \mathbf{m}) = \mathbf{m}/s = 0$  syss  $\mathbf{m} = \vec{0}$ .  $\square$

**Corolario 6.21.1:**  $S^{-1}A$  es un  $A$ -módulo plano.

### §6.1.2 Radicales.

**Definición 6.22:** Sea  $A$  un dominio, entonces un elemento  $a \in A$  es *nilpotente* si existe  $n \geq 1$  tal que  $x^n = 0$ .

**Proposición (AE) 6.23:** 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:

$$s = r_1 a + p, \quad s' = r_2 b + p'$$

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  $S$ .  $\square$

**Corolario 6.23.1:** 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 6.24:** Dado un ideal  $\mathfrak{a}$  se define su radical como

$$\text{Rad}(\mathfrak{a}) = \{a \in A : \exists n \ a^n \in \mathfrak{a}\}.$$

Se dice que  $\mathfrak{a}$  es **radical** si  $\mathfrak{a} = \text{Rad}(\mathfrak{a})$ .

Se le llama el **nilradical** de  $A$  a  $\mathfrak{N}(A) := \text{Rad}(0)$ , 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 creará 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) 6.25:** Sea  $\mathfrak{a} \trianglelefteq A$ , entonces:

1.  $\text{Rad}(\mathfrak{a}) = \bigcap \{\mathfrak{p} : \mathfrak{a} \subseteq \mathfrak{p} \trianglelefteq A, \mathfrak{p} \text{ primo}\}.$
2.  $\mathfrak{a}$  es un ideal radical syss  $A/\mathfrak{a}$  es un anillo reducido.

**Corolario 6.25.1:** 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 6.26:** 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  $\frac{a}{s} = \frac{ta}{ts} \in S^{-1} \mathfrak{N}(A)$ .  $\square$

**Corolario 6.26.1:**  $A$  es reducido syss  $A_{\mathfrak{m}}$  es reducido para todo  $\mathfrak{m} \triangleleft A$  maximal.

**Proposición 6.27:** Para todo par de ideales  $\mathfrak{a}, \mathfrak{b}$  en  $A$  se cumple:

1. Para todo  $\mathfrak{a} \trianglelefteq A$  se cumple que  $\mathfrak{a} \subseteq \text{Rad}(\mathfrak{a}) \trianglelefteq A$ .
2.  $\text{Rad}(\text{Rad}(\mathfrak{a})) = \text{Rad}(\mathfrak{a})$ , es decir, todo radical de un ideal es un ideal radical.
3.  $\text{Rad}(\mathfrak{a} \cdot \mathfrak{b}) = \text{Rad}(\mathfrak{a} \cap \mathfrak{b}) = \text{Rad}(\mathfrak{a}) \cap \text{Rad}(\mathfrak{b})$ .
4.  $\text{Rad}(\mathfrak{a}) = (1)$  syss  $\mathfrak{a} = (1)$ .
5.  $\text{Rad}(\mathfrak{a} + \mathfrak{b}) = \text{Rad}(\text{Rad}(\mathfrak{a}) + \text{Rad}(\mathfrak{b}))$ .
6. Si  $\mathfrak{p}$  es primo, entonces  $\text{Rad}(\mathfrak{p}^n) = \mathfrak{p}$  para todo  $n > 0$ .
7.  $\mathfrak{a} + \mathfrak{b} = (1)$  syss  $\text{Rad}(\mathfrak{a}) + \text{Rad}(\mathfrak{b}) = (1)$ .

DEMOSTRACIÓN: Probaremos las primeras dos:

1. Definamos  $\mathfrak{r} := \text{Rad}(\mathfrak{a})$ . Claramente se cumple que  $\mathfrak{a} \subseteq \text{Rad}(\mathfrak{a})$ , 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  $\text{Rad}(\mathfrak{a}) \subseteq \text{Rad}(\text{Rad}(\mathfrak{a}))$ . Sea  $a \in \text{Rad}(\text{Rad}(\mathfrak{a}))$ , entonces  $a^n \in \text{Rad}(\mathfrak{a})$  y entonces  $(a^n)^m \in \mathfrak{a}$  para algunos  $n, m$ . Pero entonces  $(a^n)^m = a^{nm} \in \mathfrak{a}$ , luego  $a \in \text{Rad}(\mathfrak{a})$ .  $\square$

**Proposición 6.28:** Sea  $\mathfrak{m} \triangleleft A$  un ideal maximal, y sea  $\mathfrak{n} := \mathfrak{m}A_{\mathfrak{m}}$  el cual es maximal. Para todo  $n \in \mathbb{N}$ , el morfismo

$$\phi_n: A/\mathfrak{m}^n \longrightarrow A_{\mathfrak{m}}/\mathfrak{n}^n$$

$$a + \mathfrak{m}^n \mapsto a + \mathfrak{n}^n$$

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

$$\ker(A/\mathfrak{m}^n \rightarrow A_{\mathfrak{m}}/\mathfrak{n}^n) = (\mathfrak{m}^n)^{ec}/\mathfrak{m}^n.$$

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  $\phi_n$  es inyectiva.

Falta ver que  $\phi_n$  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  $\text{Rad}(\mathfrak{m}^n) = \mathfrak{m}$ , 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.  $\square$

**Definición 6.29:** 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

$$\text{Ann}(T) := (0 : T).$$

**Proposición 6.30:** 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.  $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{bc}) = (\mathfrak{a} : \mathfrak{c} : \mathfrak{b})$ .

$$5. (\bigcap_{i \in I} \mathfrak{a}_i : \mathfrak{b}) = \bigcap_{i \in I} (\mathfrak{a}_i : \mathfrak{b}).$$

$$6. (\mathfrak{a} : \sum_{i \in I} \mathfrak{b}_i) = \bigcap_{i \in I} (\mathfrak{a} : \mathfrak{b}_i).$$

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  $x \in (\mathfrak{a} : \sum_{i \in I} \mathfrak{b}_i)$ , 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  $x \sum_{i \in I} y_i \in \mathfrak{a}$ .  $\square$

**Proposición 6.31:** Denotemos  $D$  el conjunto de los divisores de cero de  $A$ . Entonces

$$D = \bigcup_{x \neq 0} \text{Rad}(\text{Ann}(x)) = \bigcup_{x \neq 0} \text{Ann}(x).$$

**§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 6.32:** Sea  $\varphi: A \rightarrow B$  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:

$$\mathfrak{b}^c := \varphi^{-1}[\mathfrak{b}], \quad \mathfrak{a}^e := (\varphi[\mathfrak{a}]).$$

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  $\iota: \mathbb{Z} \rightarrow \mathbb{Q}$ , 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 6.33:** Sea  $\varphi: A \rightarrow B$  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:

$$\{\mathfrak{a} \trianglelefteq A : \mathfrak{a}^{ec} = \mathfrak{a}\} \xrightleftharpoons[\text{()^c}]{\text{()^e}} \{\mathfrak{b} \trianglelefteq B : \mathfrak{b}^{ce} = \mathfrak{b}\}$$

son biyecciones y son la una la inversa de la otra.

**Proposición 6.34:** Sea  $S$  un sistema multiplicativo de  $A$ ,  $\mathfrak{a} \trianglelefteq A$  y consideremos el morfismo  $\lambda_S: A \rightarrow S^{-1}A$ . 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  $\mathfrak{a} \cap S \neq \emptyset$ .
3.  $\mathfrak{a}$  es una contracción syss ningún elemento de  $S$  es divisor de cero en  $A/\mathfrak{a}$ .
4. Las siguientes aplicaciones:

$$\{\mathfrak{p} \triangleleft A : \mathfrak{p} \text{ primo}, \mathfrak{p} \cap S \neq \emptyset\} \xrightleftharpoons[\text{()^c}]{S^{-1}-} \{\mathfrak{q} \triangleleft S^{-1}A : \mathfrak{q} \text{ primo}\}$$

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.  $\square$

**Proposición 6.35:** Sea  $\varphi: A \rightarrow B$  un morfismo de anillos, y sea  $\mathfrak{p} \triangleleft A$  primo. Entonces  $\mathfrak{p}$  es la contracción de un ideal primo syss es la contracción de un ideal.

DEMOSTRACIÓN:  $\Rightarrow$ . Trivial.

$\Leftarrow$ . 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  $\mathfrak{m} \triangleleft S^{-1}B$ . 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  $\mathfrak{q} \cap S = \emptyset$ . Finalmente  $\mathfrak{q}^c = \mathfrak{p}$ .  $\square$

#### §6.1.4 El lema de Nakayama y sus consecuencias.

**Definición 6.36:** Dado un anillo  $A$ , se define su *radical de Jacobson* como

$$\mathfrak{J}(A) := \bigcap \{\mathfrak{m} : \mathfrak{m} \triangleleft A, \mathfrak{m} \text{ maximal}\}.$$

**Proposición 6.37:** 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  $\mathfrak{m} \triangleleft A$  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.  $\square$

**Teorema 6.38 – Teorema de Cayley-Hamilton:** Sea  $M$  un  $A$ -módulo finitamente generado,  $\varphi: M \rightarrow M$  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  $\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$  un sistema generador finito y luego se ha de cumplir que  $\varphi(\mathbf{x}_i) = \sum_{j=1}^n c_{ij} \mathbf{x}_j$  con  $c_{ij} \in \mathfrak{a}$ , o equivalentemente

$$\sum_{j=1}^n (\delta_{ij} \varphi - c_{ij}) \mathbf{x}_j = \vec{0}$$

para todo  $i$ . Luego formando la matriz  $B := [\delta_{ij} \varphi - c_{ij}]_{ij}$ , nos damos cuenta de que  $B$  aplicado sobre todo  $\mathbf{x}_i$  se anula, por lo que, multiplicando por  $\text{adj } B$  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.  $\square$

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 6.39 – 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  $M/\mathfrak{J}(A)M = \text{Span}_A\{[\mathbf{x}_1], \dots, [\mathbf{x}_n]\}$ , entonces  $M = \text{Span}_A\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ .

DEMOSTRACIÓN:

1. Considere el lema anterior con  $\varphi = \text{Id}$  y sea  $x := 1 + a_{n-1} + \dots + a_1 + a_0$ .
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  $N = \text{Span}_A\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ .  $\square$

**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 6.40:** 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 6.41:** 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  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$  para  $\overline{M}$ , y para cada  $\mathbf{v}_i$  consideramos una preimagen  $\mathbf{u}_i \in M$ , entonces  $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$  es una base minimal de  $M$ .
3. Conversamente, toda base minimal se proyecta en una base para  $\overline{M}$ .
4. Sean  $\{\mathbf{u}_1, \dots, \mathbf{u}_n\}$  y  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$  dos bases minimales de  $M$ , tales que

$$\forall i \in \{1, \dots, n\} \quad \mathbf{u}_i = \sum_{j=1}^n a_{ij} \mathbf{v}_j,$$

y sea  $B := [a_{ij}]_{ij} \in \text{Mat}_n(A)$ . Entonces  $\det(B) \in A^\times$  y  $B$  es inversible.

**Teorema 6.42:** Sea  $A$  un dominio y  $M$  un  $A$ -módulo finitamente generado. Si  $f: M \rightarrow M$  es un homomorfismo de  $A$ -módulos suprayectivo, entonces también es inyectivo y, por ende, es un automorfismo.

DEMOSTRACIÓN: Fijemos a  $f \in \text{Hom}_A(M, M)$ . En particular, podemos ver a  $M$  como un  $A[x]$ -módulo con la operación:

$$\left( \sum_{i=0}^n c_i x^i \right) \cdot \mathbf{m} = \sum_{i=0}^n c_i f^i(\mathbf{m}),$$

donde aquí  $f^i$  representa la composición  $i$  veces, y  $f^0 := \text{Id}$ . 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  $\mathbf{m} \in \ker f$ , luego se tiene que

$$\vec{0} = \left(1 + \sum_{i=1}^N c_i x^i\right) \cdot \mathbf{m} = \mathbf{m} + \sum_{i=1}^N c_i f^i(\mathbf{m}) = \mathbf{m}. \quad \square$$

**Lema 6.43:** 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  $E_\gamma$  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  $F_\alpha$  es una suma directa de  $E_\gamma$ 's.

La construcción es por recursión transfinita: Definimos  $F_0 := (0)$  y si  $\lambda$  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  $\{\mathbf{x}_{11}, \mathbf{x}_{12}, \mathbf{x}_{13}, \dots\}$  un sistema generador de  $Q_1$ . Tómese a  $\mathbf{x}_{11} = \mathbf{m}_{11} + \mathbf{n}_{11}$  con  $\mathbf{m}_{11} \in M$  y  $\mathbf{n}_{11} \in N$ , y definamos  $Q_2$  como la mínima unión de  $E_\gamma$ 's (que son finitos) tales que  $\mathbf{m}_{11}, \mathbf{n}_{11} \in Q_2$ . Sea  $\{\mathbf{x}_{21}, \mathbf{x}_{22}, \dots\}$  un sistema generador de  $Q_2$  y siga el mismo procedimiento, construyendo  $\mathbf{x}_{ij}$ . Finalmente definimos  $F_{\alpha+1} := F_\alpha + \text{Span}_A\{\mathbf{x}_{ij}\}$ .

Nótese que

$$M = \bigcup_{\alpha < \mu} M_\alpha,$$

donde  $M_\alpha$  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  $\lambda$  ordinal límite, finalmente se cumple que

$$M = \bigcup_{\alpha < \mu} \tilde{M}_\alpha. \quad \square$$

**Lema 6.44:** Sea  $A$  un dominio local,  $P$  un  $A$ -módulo proyectivo y  $\mathbf{x} \in P$ . Entonces existe un sumando directo de  $P$  que es libre y contiene a  $\mathbf{x}$ .

DEMOSTRACIÓN: Sea  $F = P \oplus P'$  con  $F$  libre. Elijamos una base  $\{\mathbf{y}_i\}_{i \in I}$  de  $F$  tal que la representación de  $\mathbf{x}$  en la base posea la cantidad minimal de coeficientes no nulos. Sea  $\mathbf{x} = a_1 \mathbf{y}_1 + \cdots + a_n \mathbf{y}_n$  con  $0 \neq a_i \in A$ , entonces se cumple que

$$a_i \notin \sum_{\substack{j \in I \\ j \neq i}} A a_j$$

(¿por qué?). Sea  $\mathbf{y}_i = \mathbf{p}_i + \mathbf{q}_i$  con  $\mathbf{p}_i \in P$  y  $\mathbf{q}_i \in P'$ , luego  $\mathbf{x} = \sum_{i=1}^n a_i \mathbf{p}_i$ . Cada  $\mathbf{p}_i = \sum_{j=1}^n c_{ij} \mathbf{y}_j + \mathbf{s}_i$ , donde  $\mathbf{s}_i$  son sumas de otros elementos de la base, de modo que se tiene que

$$\mathbf{x} = \sum_{i=1}^n a_i \mathbf{y}_i = \sum_{i=1}^n a_i \mathbf{p}_i = \sum_{i=1}^n \left( \sum_{j=1}^n c_{ij} \mathbf{y}_j + \mathbf{s}_i \right).$$

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  $i = 1, \dots, n$  y que  $c_{ij} \in \mathfrak{m}$  para  $i \neq j$ . Luego sea  $C := [c_{ij}]_{ij} \in \text{Mat}_n(A)$ . Nótese que  $\det(C) \equiv 1 \pmod{\mathfrak{m}}$ , luego  $\det(C) \in A^\times$  y luego podemos reemplazar  $\mathbf{y}_i$  con  $\mathbf{p}_i$ , para todo  $i = 1, \dots, n$ . Luego  $\mathbf{x} \in \sum_{i=1}^n A \mathbf{p}_i$  el cual es un sumando directo libre de  $P$ .  $\square$

**Teorema 6.45:** 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  $\mathbf{x}_1, \dots, \mathbf{x}_n$  una base minimal de  $M$  y sea  $F$  el  $A$ -módulo libre generado por  $\{\mathbf{y}_1, \dots, \mathbf{y}_n\}$ . Sea  $\varphi: F \rightarrow M$  que manda  $\varphi(\mathbf{y}_i) = \mathbf{x}_i$ , de modo que es un epimorfismo. Sea  $K := \ker \varphi$ . Por definición de base minimal, debe cumplirse que en  $K$ :

$$\varphi \left( \sum_{i=1}^n a_i \mathbf{x}_i \right) = \sum_{i=1}^n a_i \mathbf{x}_i = \vec{0},$$

con  $a_i \in \mathfrak{m}$ ; por lo que  $K \subseteq \mathfrak{m}F$ . Como  $M$  es proyectivo, entonces existe  $\psi: M \rightarrow F$  tal que  $\psi \circ \varphi = \text{Id}_M$  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  $M = \text{Span}_A\{\mathbf{m}_1, \mathbf{m}_2, \dots\}$ . Luego por el lema anterior sea  $\mathbf{m}_1 \in F_1$ , donde  $M = F_1 \oplus M_1$ ,  $F_1$  es libre y  $M_1$  es proyectivo numerablemente generado. Sea  $\mathbf{m}'_2$  la componente de  $\mathbf{m}_2$  en  $M_1$  y sea  $\mathbf{m}'_2 \in F_2$ , 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.  $\square$

## 6.2 Ideales asociados y descomposición primaria

**Definición 6.46:** Dado un  $A$ -módulo  $M$ , se dice que un ideal primo  $\mathfrak{p} \triangleleft A$  está *asociado* a  $M$ , si existe  $\mathbf{m} \in M_{\neq 0}$  tal que  $\mathfrak{p} = \text{Ann } \mathbf{m}$ . El conjunto de los ideales asociados a  $M$  se denota  $\text{As}_A(M)$ ; obviamos el subíndice  $A$  de no haber ambigüedad sobre los signos. Dado un ideal  $\mathfrak{a} \triangleleft A$ , definimos  $\text{As}(\mathfrak{a}) := \text{As}(A/\mathfrak{a})$ . Decimos que  $a \in A$  es un *divisor de cero* de  $M$  si existe  $\mathbf{m} \in M_{\neq 0}$  tal que  $a\mathbf{m} = \vec{0}$ . Se dice que  $M$  es un *módulo fiel* si no posee divisores de cero además de  $0 \in A$ .

**Proposición 6.47:** Sea  $A$  un dominio noetheriano y  $M$  un  $A$ -módulo no nulo.

1. Todo  $\text{Ann}(\mathbf{x})$  con  $\mathbf{x} \in M_{\neq 0}$  está contenido en algún ideal asociado a  $M$ .
2. Los divisores de cero de  $M$  son  $\bigcup \text{As}(M)$ .

DEMOSTRACIÓN:

1. Definamos  $\mathcal{F} := \{\text{Ann}(\mathbf{x}) : \mathbf{x} \in M_{\neq 0}\}$ . Nótese que toda cadena ascendente se estabiliza porque  $A$  es noetheriano, así que sólo basta ver que algún elemento  $\subseteq$ -maximal  $\mathfrak{p} = \text{Ann}(\mathbf{y})$  es un ideal primo. Para ello, sean  $ab \in \mathfrak{p}$  con  $b \notin \mathfrak{p}$ , es decir,  $ab\mathbf{y} = 0$ , pero  $b\mathbf{y} \neq 0$ . Claramente  $\text{Ann}(\mathbf{y}) \subseteq \text{Ann}(b\mathbf{y})$ , luego se tiene igualdad por maximalidad, y luego  $a \in \mathfrak{p}$ .
2. Ejercicio para el lector. □

**Teorema 6.48:** Sea  $S$  un sistema multiplicativo de  $A$  sin divisores de cero y fijemos el monomorfismo  $\iota: A \rightarrow S^{-1}A$ .

1. Sea  $N$  un  $S^{-1}A$ -módulo (luego, también un  $A$ -módulo), entonces  $\mathfrak{q} \in \text{As}_{S^{-1}A}(N)$  syss  $\mathfrak{q}^c = \mathfrak{q} \cap A \in \text{As}_A(N)$ .
2. Si  $A$  es noetheriano y  $M$  es un  $A$ -módulo, entonces  $\mathfrak{p} \in \text{As}_A(S^{-1}M)$  syss  $\mathfrak{p} \in \text{As}_A(M)$  y  $\mathfrak{p} \cap S = \emptyset$ .

DEMOSTRACIÓN:

1. Es claro que si  $\mathfrak{q} \in \text{As}_{S^{-1}A}(N)$  entonces  $\mathfrak{q}^c = \mathfrak{q} \cap A \in \text{As}_A(N)$ . Recíprocamente si  $\mathfrak{p} \in \text{As}_A(N)$  con  $\mathfrak{p} \cap S = \emptyset$  y  $\mathfrak{p} = \text{Ann}_A(\mathbf{x})$ , entonces  $\mathfrak{p}^e = \text{Ann}_{S^{-1}A}(\mathbf{x})$  es un ideal primo.
2. Sea  $\mathfrak{p} = \text{Ann}(\mathbf{x})$  con  $\mathfrak{p} \cap S = \emptyset$ .  $(a/s)x = 0$  con  $\mathbf{x}/s \in S^{-1}M$  y  $a \in A$  syss  $t(ax - s0) = tax = \vec{0}$  para algún  $t \in S$ . Como  $t \notin \mathfrak{p}$ , entonces necesariamente  $a \in \mathfrak{p}$  y luego vemos que  $\mathfrak{p}^e = \text{Ann}_{S^{-1}A}(\mathbf{x}) \in \text{As}_{S^{-1}A}(S^{-1}M)$  con lo que  $\mathfrak{p} \in \text{As}_A(S^{-1}M)$ .

Recíprocamente si  $\mathfrak{q} = \text{Ann}(\mathbf{x}/s) \in \text{As}_{S^{-1}A}(S^{-1}M)$  y definimos  $\mathfrak{p} := \mathfrak{q}^c$  (que satisface  $\mathfrak{q} = \mathfrak{p}^e$ ). Como  $A$  es noetheriano,  $\mathfrak{p}$  es finitamente generado, digamos  $\mathfrak{p} = (a_1, \dots, a_r)$ , de modo que  $t_i a_i \mathbf{x} = \vec{0}$  para ciertos  $t_i \in S$ , luego tomando el producto  $t = t_1 \cdots t_r \in S$  vemos que  $\mathfrak{p} = \text{Ann}(t\mathbf{x}) \in \text{As}_A(M)$ . □

**Corolario 6.48.1:** Sea  $A$  un dominio noetheriano y  $M$  un  $A$ -módulo, entonces  $\mathfrak{p} \in \text{As}_A(M)$  syss  $\mathfrak{p}^e = \mathfrak{p}A_{\mathfrak{p}} \in \text{As}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$ .

**Teorema 6.49:** Sean  $M_1, M_2, M_3$  un trío de  $A$ -módulos.

1. Dada la sucesión exacta  $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$  se cumple que  $\text{As}(M_1) \subseteq \text{As}(M_2) \subseteq \text{As}(M_1) \cup \text{As}(M_3)$ .

2. En particular, si  $M_2 = M_1 \oplus M_3$ , entonces  $\text{As}(M_2) = \text{As}(M_1) \cup \text{As}(M_3)$ .

DEMOSTRACIÓN:

1. Dado  $\mathfrak{p} \in \text{As}(M_2)$ , entonces  $\mathfrak{p} = \text{Ann}(\mathbf{x})$  para algún  $\mathbf{x} \in M_2$ , luego es fácil notar que  $N := \text{Span}\{\mathbf{x}\} \cong A/\mathfrak{p}$  y, más aún, para todo  $\mathbf{y} \in N_{\neq 0}$  podemos ver que  $\text{Ann}(\mathbf{y}) = \mathfrak{p}$ . Mirando a  $M_1 \subseteq M_3$ , si  $N \cap M_1 \neq \{\vec{0}\}$ , entonces tendríamos que  $\mathfrak{p} \in \text{As}(M_1)$ . 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  $\mathfrak{p} \in \text{As}(M_3)$ .
2. Basta aplicar el inciso anterior para concluir que  $\text{As}(M_1) \subseteq \text{As}(M_2)$  y  $\text{As}(M_3) \subseteq \text{As}(M_2)$ .  $\square$

**Corolario 6.49.1:** 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  $\mathfrak{p}_i \triangleleft A$  es un ideal primo.

DEMOSTRACIÓN: Definamos  $M_0 = \{\vec{0}\}$  y dado  $\mathfrak{p}_1 \in \text{As}(M)$  elegimos  $M_1$  tal que  $M_1 = M_1/M_0 \cong A/\mathfrak{p}_1$ . Luego dado  $\mathfrak{p}_2 \in \text{As}(M/M_1)$  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.  $\square$

**Teorema 6.50:** Sea  $A$  un dominio noetheriano y  $M$  un  $A$ -módulo finitamente generado. Entonces:

1.  $\text{As}(M)$  es un conjunto finito.
2.  $\text{As}(M) \subseteq \text{Supp}(M)$ .
3. Los elementos  $\subseteq$ -minimales de  $\text{As}(M)$  y  $\text{Supp}(M)$  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  $\text{As}(M) \subseteq \text{As}(M_{n-1}) \cup \text{As}(A/\mathfrak{p}_n)$  donde  $\text{As}(A/\mathfrak{p}_n) = \{\mathfrak{p}_n\}$ .

2. Si  $\mathfrak{p} \in \text{As}(M)$  entonces  $0 \rightarrow A/\mathfrak{p} \rightarrow M$  es una sucesión exacta que induce la sucesión exacta  $0 \rightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}}$  es exacta y, por tanto,  $M_{\mathfrak{p}} \neq 0$ .
3. Por el inciso anterior basta probar que todo  $\subseteq$ -minimal de  $\text{Supp}(M)$  está en  $\text{As}(M)$ . Sea  $\mathfrak{p} \in \text{Supp}(M)$  minimal, luego  $M_{\mathfrak{p}} \neq 0$  y sabemos que  $\text{As}(M_{\mathfrak{p}}) \neq \emptyset$ . Dado  $\mathfrak{q} \in \text{As}(M_{\mathfrak{p}})$  notamos que  $\mathfrak{q} \setminus \mathfrak{p} = \emptyset$  (luego  $\mathfrak{q} \subseteq \mathfrak{p}$ ) y  $\mathfrak{q} \in \text{As}(M)$ , pero además  $\mathfrak{q} \in \text{Supp}(M)$  por lo que  $\mathfrak{q} = \mathfrak{p}$ .  $\square$

**Corolario 6.50.1:** Todo dominio noetheriano tiene finitos primos minimales.

**Definición 6.51:** Dado un  $A$ -módulo  $M$  decimos que un submódulo  $N \leq M$  es **primario** si para todo  $a \in A$  y  $\mathfrak{m} \in M \setminus N$  con  $a\mathfrak{m} \in N$  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  $a \in \text{Rad Ann}(M/N)$ . 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  $\text{Rad Ann}(M)$ .

Así pues,  $N$  es un submódulo primario de  $M$  syss  $M/N$  es coprimario.

**Teorema 6.52:** Sea  $A$  un dominio noetheriano y  $M$  un  $A$ -módulo finitamente generado. Un submódulo  $N \leq M$  es primario syss  $\text{As}(M/N)$  sólo posee un elemento  $\mathfrak{p}$ ; en cuyo caso, el ideal  $\mathfrak{a} := \text{Ann}(M/N)$  es primario y  $\text{Rad } \mathfrak{a} = \mathfrak{p}$ .

DEMOSTRACIÓN:  $\Leftarrow$ . Si  $\text{As}(M/N) = \{\mathfrak{p}\}$ , entonces los divisores de cero son exactamente los elementos de  $\mathfrak{p}$ . Es claro que  $\text{Rad Ann}(M/N) \subseteq \mathfrak{p}$ , bastaría ver la otra inclusión. Como  $M$  es finitamente generado, entonces  $M/N$  también y está generado digamos por  $\{\mathbf{u}_1, \dots, \mathbf{u}_r\}$  y luego, podemos notar que

$$\begin{aligned} \mathfrak{q} \in \text{Supp}(M/N) &\iff (M/N)_{\mathfrak{q}} \neq 0 \iff \exists i : \mathbf{u}_i \neq 0 \in (M/N)_{\mathfrak{q}} \\ &\iff \exists i : \text{Ann}(\mathbf{u}_i) \subseteq \mathfrak{q} \iff \text{Ann}(M/N) = \bigcap_{i=1}^r \text{Ann}(\mathbf{u}_i) \subseteq \mathfrak{q}. \end{aligned}$$

Y ahora recuerde que, por el inciso 3 del teorema anterior, que  $\mathfrak{p} \in \text{Supp}(M/N)$ .



$\implies$ . Si  $N$  es primario y  $\mathfrak{p} \in \text{As}(M/N)$ , entonces por la proposición 6.47 se tiene que si  $a \in \mathfrak{p}$  entonces  $a$  es un divisor de cero de  $M/N$ , luego  $a \in \text{Rad}(\text{Ann}(M/N)) = \text{Rad } \mathfrak{a}$  (puesto que  $N$  es primario). De modo que  $\mathfrak{p} \subseteq \text{Rad } \mathfrak{a}$ , pero además,

$$\text{Rad } \mathfrak{a} = \bigcap \text{As}(M/N) \subseteq \mathfrak{p},$$

de lo que se concluye la igualdad.  $\square$

**Definición 6.53:** Si  $N \leq M$  es tal que  $\mathfrak{p} = \text{Rad Ann}(M/N)$  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 6.54:** Si  $\text{Rad Ann}(M)$  es maximal, entonces  $M$  es coprimario. En particular, las potencias de un ideal maximal  $\mathfrak{m}$  son ideales  $\mathfrak{m}$ -primarios.

**Proposición 6.55:** 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  $\text{Rad } \mathfrak{a} = (x_1, \dots, x_r)$  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  $(\text{Rad } \mathfrak{a})^m$  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  $(\text{Rad } \mathfrak{a})^m \subseteq \mathfrak{a}$ .  $\square$

**Corolario 6.55.1:** En un anillo noetheriano el nilradical es nilpotente.

**Corolario 6.55.2:** 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.  $\text{Rad } \mathfrak{q} = \mathfrak{m}$ .
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 6.54.

$2 \implies 3$ . Por la proposición anterior.

$3 \implies 2$ . Basta aplicar radicales a la desigualdad.  $\square$

**Lema 6.56:** Sean  $N_1, \dots, N_r$  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  $\text{As}(M/N_1 \oplus M/N_2) = \{\mathfrak{p}\}$ .  $\square$

**Definición 6.57:** 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 6.58:** 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 descomposición 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  $\text{Rad Ann}(M/N_i)$ 's son distintos.

Dada una descomposición primaria minimal de  $M'$ :

$$M' = \bigcap_{i=1}^r N_i, \quad \text{Rad Ann}(M/N_i) = \mathfrak{p}_i,$$

entonces  $N_i$  se dice la  $\mathfrak{p}_i$ -*componente primaria* de  $M'$ .  $M'$  se dice *decomposable* 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 6.59:** 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 decomponible.
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  $\text{As}(M/N) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ . 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  $\lambda_{\mathfrak{p}}: M \rightarrow M_{\mathfrak{p}}$  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 6.52 se cumple que  $\text{As}(M)$  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  $N_1 \cap \dots \cap N_r = 0$ , podemos ver a  $M$  contenido en  $(M/N_1) \oplus \dots \oplus (M/N_r)$  y

$$\text{As } M \subseteq \text{As} \left( \bigoplus_{i=1}^r M/N_i \right) = \bigcup_{i=1}^r \text{As}(M/N_i) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}.$$

Como la descomposición es irredundante tenemos que  $N_2 \cap \dots \cap N_r \neq 0$  y luego existe  $\mathbf{x} \in N_2 \cap \dots \cap N_r$  no nulo. Luego  $\text{Ann } \mathbf{x} = (0 : \mathbf{x}) = (N_1 : \mathbf{x})$  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  $\mathfrak{p}_1^n \mathbf{x} = 0$  para algún  $n$ . Elijamos dicho  $n$  tal que  $\mathfrak{p}_1^n \mathbf{x} \neq 0$  y  $\mathfrak{p}_1^{n+1} \mathbf{x} = 0$ , y elijamos algún  $\mathbf{y} \in \mathfrak{p}_1^n \mathbf{x}$  no nulo, de modo que  $\mathfrak{p}_1 \mathbf{y} = 0$ . Nótese que  $\mathbf{y} \in N_2 \cup \dots \cup N_r$  de modo que  $\mathbf{y} \notin N_1$  y  $\text{Ann } \mathbf{y} \subseteq \mathfrak{p}_1$ , por lo que  $\text{Ann } \mathbf{y} = \mathfrak{p}_1$  y se concluye que  $\mathfrak{p}_1 \in \text{As } M$ . Así concluimos que  $\text{As } M = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ .

4. Sea  $N = N_1 \cap \cdots \cap N_r$  una descomposición primaria minimal y sea  $\mathfrak{p} := \text{Rad Ann}(M/N_1)$ . 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  $\mathfrak{p}_i^m \subseteq \text{Ann}(M/N_i)$  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.  $\square$

**Definición 6.60:** 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 6.61:** Sea  $\mathfrak{a}$  un ideal decomposable con descomposición minimal  $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$  y con  $\mathfrak{p}_i := \text{Rad } \mathfrak{q}_i$ . Si  $\mathcal{F} := \{\mathfrak{p}_{i_1}, \dots, \mathfrak{p}_{i_j}\}$  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  $\mathfrak{p} \cap S = \emptyset$ . Si  $\mathfrak{p} \notin \mathcal{F}$ , entonces  $\mathfrak{p} \not\subseteq \bigcup_{j=1}^m \mathfrak{p}_{i_j}$  por la proposición 2.52, por lo que  $\mathfrak{p} \cap S \neq \emptyset$ .

Finalmente basta aplicar el resultado anterior para obtener el enunciado.  $\square$

### 6.3 Módulos noetherianos y artinianos, de nuevo

**Teorema 6.62:** 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. artinario).

DEMOSTRACIÓN: Falta probar  $\implies$ : En primer lugar construyamos la siguiente aplicación:

$$\begin{aligned} \Phi: \{T : T \leq M\} &\longrightarrow \{L : L \neq N\} \times \{S : S \leq M/N\} \\ T &\longmapsto \left(T \cap N, \frac{T + N}{N}\right) \end{aligned}$$

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  $\mathbf{x} \in T \setminus E$ , entonces como  $E \cap N = T \cap N$  se ha de cumplir que  $\mathbf{x} \notin N$  y luego  $[\mathbf{x}] \neq [\mathbf{y}]$  para todo  $\mathbf{y} \in E$ , puesto que

de lo contrario  $\mathbf{x} - \mathbf{y} = \mathbf{n} \in N$ , pero entonces  $\mathbf{n} \in T \cap N = E \cap N$ , por lo que  $\mathbf{x} = \mathbf{y} + \mathbf{n} \in E$ ; 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, esto implica que los  $E_i$ 's también se estabilizan desde dicho  $n$ ; luego  $M$  es noetheriano.  $\square$

**Corolario 6.62.1:** La suma directa de  $A$ -módulos noetherianos (resp. artinianos) es también noetheriano (resp. artiniano).

Reescribiendo el último teorema en lenguaje de sucesiones exactas:

**Proposición 6.63:** Si  $0 \rightarrow N \rightarrow M \rightarrow T \rightarrow 0$  es una sucesión exacta de  $A$ -módulos, entonces  $M$  es noetheriano (resp. artiniano) syss  $N, T$  lo son.

**Corolario 6.63.1:** 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:

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^n M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0 \quad \square$$

**Teorema 6.64 (Kaplansky):** Sea  $M$  un  $A$ -módulo noetheriano. Entonces  $\bar{A} := A/\text{Ann}(M)$  es un anillo noetheriano. En particular, si  $M$  es fiel, entonces  $A$  es noetheriano.

DEMOSTRACIÓN: Basta probar el caso en que  $\text{Ann}(M) = 0$  (¿por qué?). Como  $M$  es noetheriano, entonces es finitamente generado y podemos escribir  $M = A \cdot \mathbf{m}_1 + \cdots + A \cdot \mathbf{m}_n$ . Luego podemos considerar el morfismo  $a \mapsto (a\mathbf{m}_1, \dots, a\mathbf{m}_n)$  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.  $\square$

Uno de los resultados más importantes que vimos era el teorema de las bases de Hilbert, el cual dice que  $A[x_1, \dots, x_n]$  es noetheriano si  $A$  lo es.

Podemos sacar la siguiente consecuencia:

**Proposición 6.65:** 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. artinian), entonces todo  $A$ -módulo finitamente generado también es noetheriano (resp. artinian).

Probaremos la siguiente generalización de un teorema de Cohen:

**Teorema (AE) 6.66 (Jothilingam):** Sea  $A$  un dominio y  $M$  un  $A$ -módulo finitamente generado. Son equivalentes:

1.  $M$  es noetheriano.
2. Para todo primo  $\mathfrak{p} \triangleleft A$  se cumple que  $\mathfrak{p}M$  es finitamente generado.

DEMOSTRACIÓN: Claramente  $1 \implies 2$ .

$2 \implies 1$ . Lo haremos por contrarrecíproca, vale decir, si  $M$  no es noetheriano, buscaremos un primo  $\mathfrak{p}$  tal que  $\mathfrak{p}M$  no sea finitamente generado. En primer lugar, nótese que la familia  $\mathcal{F}$  de submódulos  $N \leq M$  que no son finitamente generados satisface que toda  $\subseteq$ -cadena posee una cota superior, de modo que, por el lema de Zorn, admite un elemento  $\subseteq$ -maximal  $N \in \mathcal{F}$ .

Sea  $\mathfrak{p} := \text{Ann}(M/N) = \{a \in A : aM \subseteq N\}$ . Veamos que  $\mathfrak{p}$  es un ideal primo de  $A$ : de lo contrario, habrían  $a, b \notin \mathfrak{p}$  tales que  $(ab)M \subseteq N$ , vale decir,  $N + aM, N + bM \supset N$ , por lo que ambos son finitamente generados. Sean

$$N + aM = \langle n_1 + am_1, \dots, n_r + am_r \rangle, \quad n_i \in N, m_i \in M,$$

y sea  $L := \{m \in M : am \in N\}$ , se puede notar que  $L \supseteq N + bM \supset N$ , por lo que  $L$  es finitamente generado.

Probaremos que

$$N = \sum_{i=1}^r n_i A + aL. \quad (6.1)$$

Como  $(ab)M \subseteq N$ , entonces se comprueba la inclusión « $\subseteq$ ». Veamos la recíproca, sea  $y \in N \subseteq N + aM$ , luego tenemos que

$$y = \sum_{i=1}^r b_i(n_i + am_i) = \sum_{i=1}^r b_i n_i + a \sum_{i=1}^r b_i m_i,$$

así  $a \cdot \sum_{i=1}^r b_i m_i = y - \sum_{i=1}^r b_i n_i \in N$ , de modo que  $\sum_{i=1}^r b_i m_i \in L$ . Así concluimos « $\supseteq$ ». No obstante, nótese que la igualdad (6.1) es absurda, pues  $N$  no es finitamente generado.

Como  $M$  es finitamente generado, sea  $M = \sum_{i=1}^t u_i A$ . Denotamos  $u \mapsto \bar{u}$  a la proyección  $M \twoheadrightarrow M/N$ , de modo que  $M/N = \sum_{i=1}^t \bar{u}_i A$ , luego  $\mathfrak{p} = \bigcap_{i=1}^t \text{Ann}(\bar{u}_i)$ . Por evitamiento de primos, entonces  $\mathfrak{p} = \text{Ann}(\bar{u}_j)$  para algún  $j$ . Como  $N + u_j A \supset N$ , entonces éste módulo es finitamente generado y  $N + u_j A = \sum_{i=1}^s (y_i + a_i u_j) A$ . Un argumento similar al del párrafo anterior prueba que  $N = \sum_{i=1}^s y_i A + u_j \mathfrak{p}$ . Así pues como  $\mathfrak{p}M \subseteq N$  se tiene que

$$N = \sum_{i=1}^s y_i A + u_j \mathfrak{p} \subseteq \sum_{i=1}^s y_i A + \mathfrak{p}M \subseteq \sum_{i=1}^s y_i A + N \subseteq N,$$

de modo que  $N = \sum_{i=1}^s y_i A + \mathfrak{p}M$  sería finitamente generado, lo que es absurdo.  $\square$

Como corolarios:

**Corolario (AE) 6.66.1 (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:** Como los módulos de la forma  $\mathfrak{a}M$  satisfacen la condición de la cadena ascendente, entonces es fácil seguir la equivalencia de ser noetheriano para verificar que  $\mathfrak{a}M$  es finitamente generado y aplicamos el teorema anterior.  $\square$

Como corolario:

**Teorema (AE) 6.67 (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 6.68:** Un dominio artinianiano  $A$  sólo posee finitos ideales maximales.

**DEMOSTRACIÓN:** Considere la familia de las intersecciones finitas de los ideales maximales de  $A$ . Como  $A$  es artinianiano, 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.  $\square$

**Proposición 6.69:** Todo dominio íntegro artiniiano es un cuerpo.

DEMOSTRACIÓN: Sea  $x \in D$  y no es inversible, entonces la siguiente cadena de ideales no posee  $\subseteq$ -minimal:

$$(x) \supset (x^2) \supset (x^3) \supset \cdots \quad \square$$

**Corolario 6.69.1:** En un anillo artiniiano, todo ideal primo es maximal.

**Corolario 6.69.2:** En un anillo artiniiano, el nilradical es igual al radical de Jacobson.

**Teorema 6.70 – Teorema de Akizuki:** Todo dominio noetheriano es artiniiano.

DEMOSTRACIÓN: Procedemos por contradicción: Supongamos que existe un dominio artiniiano  $A$  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 artiniiano). 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  $\varphi: x \mapsto rx$ , 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  $\mathfrak{p} := \text{Ann}(\mathfrak{a})$ . Nótese que si  $r, s \notin \mathfrak{p}$ , ha de ser porque  $r\mathfrak{a} = s\mathfrak{a} = \mathfrak{a}$ ; luego  $rsa = \mathfrak{a}$  y  $rs \notin \mathfrak{p}$ ; en consecuencia,  $\mathfrak{p}$  es un ideal primo. Por lo tanto,  $k := A/\mathfrak{p}$  es un dominio íntegro artiniiano, 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 artiniiano de dimensión infinita; lo cual es absurdo.  $\square$



**Ejemplo 6.71:** Un anillo artinian que es conmutativo, pero no es noetheriano ni unitario 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 artinian. Pero no es noetheriano puesto que la siguiente cadena no posee  $\subseteq$ -maximal:

$$\langle p^{-1} \rangle \subset \langle p^{-2} \rangle \subset \langle p^{-3} \rangle \subset \cdots \quad \lrcorner$$

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 6.72:** 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  $A = K$  es un cuerpo, entonces  $k.\dim K = 0$ .
- Si  $A$  es un DIP que no es un cuerpo, 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  $k.\dim(k[x_1, \dots, x_n]) \geq n$ , pero no es tan fácil establecer igualdad. Nótese que los anillos polinomiales  $k[\mathbf{x}]$ 's son DFUs, así que esto demuestra que los DFUs pueden poseer cualquier dimensión, inclusive  $\infty$ .

Aquí adjuntamos algunos (contra)ejemplos que no son tan necesarios, pero son divertidos.

**Ejemplo 6.73:** Un anillo no noetheriano de dimensión 0 Sea  $k$  un cuerpo y considere el anillo de infinitas variables  $k[x_1, x_2, x_3, \dots]$  y sea  $A$  el cociente por el ideal  $(\{x_i x_j : i, j \in \mathbb{N}\})$ . Éste anillo no es noetheriano pues la siguiente cadena no se estabiliza:

$$(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \dots$$

No obstante, el único ideal primo en  $A$  es  $\mathfrak{p} := (x_1, x_2, x_3, \dots)$ , puesto que  $x_i^2 = 0$  así que si  $\mathfrak{q}$  fuese primo, debe incluir a cada  $x_i$  y casi vemos que  $\mathfrak{q} \supseteq \mathfrak{p}$ , pero  $A/\mathfrak{p} = k$ , así que  $\mathfrak{p}$  es maximal.

Así  $k.\dim A = 0$ , pero  $A$  no es noetheriano. Si además localizamos, entonces  $A_{\mathfrak{p}}$  es un anillo local de dimensión cero que no es noetheriano.<sup>2</sup>  $\square$

**Proposición (AEN) 6.74:** 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 artinian.

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:

$$\mathfrak{a}_0 = A \supset \mathfrak{a}_1 = \mathfrak{m}_1 \supseteq \mathfrak{a}_2 \supset \dots \supset \mathfrak{a}_n = (0).$$

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 6.62 se concluye el enunciado.  $\square$

Ahora podemos mejorar el teorema de Akizuki:

**Teorema 6.75:** Un dominio  $A$  es artinian syss es noetheriano y tiene dimensión 0.

DEMOSTRACIÓN:  $\implies$ . Por el teorema de Akizuki,  $A$  es noetheriano y como todo ideal primo es maximal, entonces  $k.\dim A = 0$ .

$\impliedby$ . Como el ideal nulo es decomponible, 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 6.74.  $\square$

<sup>2</sup>Éste ejemplo es original de Mariano Suárez-Álvarez en <https://mathoverflow.net/a/93290>.

**Corolario 6.75.1:** 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.  $\square$

**Teorema 6.76:** 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 6.27), 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  $A \rightarrow \prod_{i=1}^k (A/\mathfrak{m}_i^{n_i})$  es un isomorfismo.

Ahora veamos la unicidad, supongamos que existe  $\psi: A \rightarrow \prod_{i=1}^n A_i$  un isomorfismo, entonces definamos  $\phi_i := \psi \circ \pi_j: A \rightarrow A_j$ , 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 6.61, por lo que los  $A_i \cong A/\mathfrak{a}_i$ 's también lo son.  $\square$

**Corolario 6.76.1:** Un dominio es artiniano reducido si y sólo se escribe de forma única como producto directo de finitos cuerpos.

**Corolario 6.76.2:** Un dominio noetheriano reducido  $A$  es tal que su anillo de fracciones totales  $K$  es un producto directo de finitos cuerpos.

DEMOSTRACIÓN: Por el corolario anterior, basta notar que  $K$  es un dominio artiniano reducido. Que sea reducido es trivial. Sea  $D$  el conjunto de divisores de cero de  $A$ , entonces  $K = S^{-1}A$  donde  $S := A \setminus D$ . Por la proposición 6.47, se cumple que  $D = \bigcup \text{As}(A)$  y  $\text{As}(A) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$  es finito por el teorema 6.50, luego  $K = \bigcap_{i=1}^n A_{\mathfrak{p}_i}$ .  $\square$

**Proposición 6.77:** Sea  $A$  un dominio y  $M$  un  $A$ -módulo noetheriano y artiniano, con una serie de composición:

$$M = M_0 > M_1 > \cdots > M_n = 0.$$

Entonces:

1. La suma de localizaciones  $M \rightarrow M_{\mathfrak{m}}$  nos da un isomorfismo:

$$M = \bigoplus_{\mathfrak{m}} M_{\mathfrak{m}},$$

donde  $\mathfrak{m}$  recorre los ideales maximales tales que  $M_i/M_{i+1} = A/\mathfrak{m}$ . La cantidad de índices  $i$  tales que  $M_i/M_{i+1} = A/\mathfrak{m}$  coincide con la longitud de  $M_{\mathfrak{m}}$  como  $A_{\mathfrak{m}}$ -módulo.

2.  $M = M_{\mathfrak{m}}$  syss  $\text{Ann}(M) \supseteq \mathfrak{m}^r$  para algún  $r > 0$ .

DEMOSTRACIÓN: Considere el caso  $n = 1$ , de modo que  $M \cong A/\mathfrak{m}$  es un módulo simple. Sea  $\mathfrak{n} \triangleleft A$  un ideal maximal, entonces pueden pasar dos cosas con  $M_{\mathfrak{n}}$ . Si  $\mathfrak{n} \neq \mathfrak{m}$ , entonces  $\mathfrak{m}$  contiene algún elemento que no está en  $\mathfrak{n}$ , luego  $\mathfrak{m}_{\mathfrak{n}} = (1)$  y luego

$$(A/\mathfrak{m})_{\mathfrak{n}} = A_{\mathfrak{n}}/\mathfrak{m}_{\mathfrak{n}} = 0.$$

Si  $\mathfrak{n} = \mathfrak{m}$ , entonces como  $A/\mathfrak{m}$  es un cuerpo (todos los elementos tienen inverso) se nota facilmente que  $(A/\mathfrak{m})_{\mathfrak{m}} = A/\mathfrak{m}$ .

Ahora si consideramos la serie de composición, aplicamos el razonamiento anterior a cada factor y empleamos inducción, donde comprobamos el caso base. Sabemos que  $M_1 = \bigoplus_{\mathfrak{n}} (M_1)_{\mathfrak{n}}$ . El factor  $M_0/M_1$  es simple, así que, denotando  $\mathfrak{m} := \text{Ann}(M_0/M_1)$ , se tiene

$$(M_0/M_1)_{\mathfrak{n}} = \begin{cases} M_0/M_1, & \mathfrak{n} = \mathfrak{m} \\ 0, & \mathfrak{n} \neq \mathfrak{m} \end{cases}$$

de modo que  $(M_1)_{\mathfrak{n}} = M_{\mathfrak{n}}$  si  $\mathfrak{n} \neq \mathfrak{m}$ . Con ésta información debería ser directo concluir el enunciado.  $\square$

**Corolario 6.77.1:** Sea  $A$  un dominio noetheriano y  $M$  un  $A$ -módulo finitamente generado. Son equivalentes:

1.  $M$  tiene longitud finita (es un módulo artiniano).

2.  $\text{Ann}(M) \supseteq \prod_{i=1}^n \mathfrak{m}_i$  para algunos  $\mathfrak{m}_i$  ideales maximales.
3. Si  $\mathfrak{p} \supseteq \text{Ann}(M)$  es un ideal primo, entonces  $\mathfrak{p}$  es maximal.
4.  $A/\text{Ann}(M)$  es artiniano.

DEMOSTRACIÓN:  $1 \implies 2$ . Basta emplear la descomposición de la proposición anterior.

$2 \implies 3$ . Si  $\mathfrak{p} \supseteq \prod_{i=1}^n \mathfrak{m}_i$ , entonces  $\mathfrak{p} \supseteq \mathfrak{m}_j$  para algún  $j$ .

$3 \implies 4$ . Es claro que todo ideal primo en  $A/\text{Ann}(M)$  es maximal, luego  $k.\dim(A/\text{Ann}(M)) = 0$ .

$4 \implies 1$ . Definamos  $B := A/\text{Ann}(M)$ . Como  $B$  es artiniano, tiene longitud finita como  $B$ -módulo, digamos  $m$ , y como  $M$  es un  $B$ -módulo finitamente generado es de la forma  $M \cong B^n/K$ . Luego  $\ell_B(M) \leq nm$ .  $\square$

**Proposición 6.78:** 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  $\mathfrak{a} \not\subseteq \mathfrak{m}^{n+1}$ , 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  $\mathfrak{a} = (x^n)$ .  $\square$

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 [0] (1938). La técnica de *localización* fue introducida por GRELL [0] (1927), un estudiante de E. Noether, y fue generalizado para dominios (anillos conmutativos unitarios) por CHEVALLEY [0]

(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 (afines y de series de potencias) empleando teoría de la eliminación. La teoría fue reescrita por NOETHER [0] (1921), artículo en el cual lo demuestra en el caso general de anillos noetherianos siguiendo las mismas técnicas que nosotros empleamos.

El teorema de Eakin-Nagata fue demostrado independientemente por EAKIN JR. [0] (1968) y NAGATA [0]. Más tarde fue generalizado por FORMANEK [0] (1973) y finalmente por JOTHILINGAM [0] (2000). La demostración del teorema de Jothilingam que incluimos es original de [0].

---

## Cuerpos formalmente reales y cuadrados

---

Comenzamos el capítulo con la observación de que la prueba del teorema fundamental del álgebra dada en 4.60 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  $a_1, \dots, a_n \in R$  tales que

$$-1 = a_1^2 + \dots + a_n^2.$$

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  $\sigma$  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  $P \cup N = R$  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  $xP \cap (1 + P) = \emptyset$  o  $(-x)P \cap (1 + P) = \emptyset$ : De lo contrario, existirían  $a, b, c, d \in P$  tales que

$$\begin{aligned} ax &= 1 + b, & -cx &= 1 + d, \\ -acx^2 &= 1 + b + d + bd, \end{aligned}$$

de modo que reordenando  $-1 = acx^2 + b + d + bd \in P$  lo que es absurdo.

Así pues, supongamos sin pérdida de generalidad que  $xP \cap (1 + P) = \emptyset$  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  $bx = 1 + a \in xP \cap (1 + P) = \emptyset$ , lo que sería absurdo.

Luego, como  $P$  es maximal, entonces  $P = Q$ , y entonces  $-x = 0 - 1x \in P$ .

Análogamente si  $(-x)P \cap (1 + P) = \emptyset$  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.  $\square$

**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 preconó 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  $a_1, \dots, a_n \in k$  no todos nulos. Entonces:

$$\frac{1}{a_1^2 + \dots + a_m^2} = \frac{a_1^2 + \dots + a_m^2}{(a_1^2 + \dots + a_m^2)^2} = \sum_{i=1}^m \left( \frac{a_i}{a_1^2 + \dots + a_m^2} \right)^2. \quad \square$$

**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  $\text{car } R \neq 2$ .
4.  $a_1^2 + \dots + a_n^2 = 0$  si y sólo si  $a_j = 0$  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  $a_1^2 + \dots + a_n^2 = 0$ . 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.

Sea  $F$  un cuerpo formalmente real, entonces una **clausura real** es una extensión  $R/F$  algebraica tal que  $R$  es realmente cerrado.

**Teorema (AE) 7.11:** Si  $R$  es formalmente real, entonces posee una extensión algebraica  $K$  que es realmente cerrada.

De momento estamos obligados a decir «una clausura real» porque la unicidad, al contrario de con las clausuras separables o perfectas, no es tan trivial; ilustrado en el siguiente ejercicio:

**Ejercicio (AE) 7.12:** Sea  $R$  un cuerpo formalmente real que no es realmente cerrado.

1. Fijada una clausura algebraica  $C := R^{\text{alg}}$ , entonces  $C$  contiene una clausura real de  $R$ .
2. Decimos que un elemento  $\alpha \in C$  es *posiblemente real* si  $R(\alpha)$  es formalmente real. Demuestre que el conjunto de elementos posiblemente reales no es siquiera un anillo.
3. Sea  $\alpha \in C$  posiblemente real. Demuestre que existe una clausura real de  $R$  en  $C$  que contiene a  $\alpha$ .

**Teorema 7.13:** 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.<sup>1</sup>

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

$$-1 = \sum_{j=1}^n b_j^2 + a \left( \sum_{j=1}^n c_j^2 \right) + 2 \left( \sum_{j=1}^n b_j c_j \right) \sqrt{a}.$$

Analizando las coordenadas de  $K$  como  $R$ -espacio vectorial, y reordenando, nos queda que

$$1 + \sum_{j=1}^n b_j^2 + a \left( \sum_{j=1}^n c_j^2 \right) = 0 \iff -a = \frac{1 + \sum_{j=1}^n b_j^2}{\sum_{j=1}^n c_j^2}.$$

<sup>1</sup>Se suele emplear el término «orden-isomorfismo», pero creo que «creciente» es más visual fuera del contexto de conjuntos ordenados.

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  $\sigma(b) = \sigma(a) + \sigma(c)^2 \geq \sigma(a)$ .  $\square$

Ahora nos proponemos a clasificar a los cuerpos realmente cerrados.

**Teorema 7.14:** Sea  $k$  un cuerpo de característica cero y  $K/k$  una extensión de cuerpos de grado impar. Dados  $a_1, \dots, a_n \in k$  no nulos tales que  $a_1x_1^2 + \dots + a_nx_n^2 = 0$  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  $\alpha$  es raíz de un polinomio minimal  $g(x) \in k[x]$  de grado  $2m + 1$ . Por extensión de Kronecker sabemos que  $K \cong k[x]/(g(x))$ , de modo que una solución no trivial a la ecuación se traduce a que existen  $f_1, \dots, f_n \in k[x]$  no todos nulos tales que

$$a_1f_1(x)^2 + \dots + a_nf_n(x)^2 = h(x)g(x)$$

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  $\beta$  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  $k$ .  $\square$

**Teorema (AE) 7.15:** 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 preconno 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  $\alpha_i^2 = b_i^2 + a d_i^2 + 2b_i d_i \sqrt{a}$ , de modo que, estudiando la primera coordenada se tiene que

$$0 = 1^2 + \sum_{i=1}^n (c_i b_i^2 + a c_i d_i^2),$$

donde todos los coeficientes yacen en  $R$ . Pero ésto es absurdo puesto que claramente el lado derecho es positivo.  $\square$

**Teorema (AE) 7.16:** 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  $R(i)$  (donde  $i = \sqrt{-1}$ ) 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  $R[i]$  es algebraicamente cerrado se reduce al teorema 4.60.

$3 \implies 1$ . Probaremos que la suma de cuadrados es también un cuadrado en  $R$ : Sean  $a, b \in R$ . Como  $R(i)$  es algebraicamente cerrado, entonces  $a + ib$  posee raíz:

$$a + bi = (c + di)^2 = c^2 - d^2 + 2cdi,$$

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  $K(i)/R(i)$  es algebraica, pero como  $R(i)$  es algebraicamente cerrado, entonces  $K(i) = R(i)$ . Luego  $R(i)/K/R$  son extensiones de cuerpo y como  $[R(i) : R] = 2$ , entonces suceden dos cosas: o bien  $K = R$ , o bien  $K = R(i)$ . En el segundo caso,  $R(i)$  no es formalmente real, lo que comprueba que  $R$  es realmente cerrado.  $\square$

**Lema 7.17:** 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 4.78.

Sea  $\beta$  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  $1, \beta, \dots, \beta^{p-1}$  son linealmente independientes sobre  $k$ , podemos mirar los coeficientes de  $\beta^{p-1}$  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.  $\square$

**Teorema (AE) 7.18:** Sea  $K$  un cuerpo no algebraicamente cerrado, pero cuya clausura algebraica  $K^{\text{alg}}/K$  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 7.16, 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  $\text{Frob}_K$  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  $K \subset K[\sqrt[p]{a}]$  de grado  $p$ , y aplicamos el lema anterior.

Por el párrafo anterior,  $K$  debe ser perfecto y  $K^{\text{alg}}$  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  $\zeta_n$  una  $q^n$ -ésima raíz primitiva de la unidad en  $K^{\text{alg}}$ . 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 4.78. Sea  $\gamma$  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  $\gamma^q$  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,

$$g(x) \in (k(\zeta_{r+1}) \cap L)[x] \quad \text{y} \quad [k(\zeta_{r+1}) : (k(\zeta_{r+1}) \cap L)] = q.$$

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 4.72, 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.  $\square$

Probar que si un grupo no es cíclico y posee dos subgrupos de orden 2, entonces

## 7.2 Teoremas de Pfister

**Definición 7.19:** Sea  $k$  un cuerpo arbitrario. Se le llama el *nivel*<sup>2</sup> 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  $\infty$ ).

**Ejemplo.** • Por la ley de reciprocidad cuadrática, si  $p = 2$  o  $p \equiv 1 \pmod{4}$  entonces  $s(\mathbb{F}_p) = 1$ .

- $s(\mathbb{Q}(\sqrt{-2})) = 2$ , puesto que  $-1 = \sqrt{-2}^2 + 1^2$  y  $-1$  no es cuadrado (¿por qué?).
- $s(\mathbb{Q}(\sqrt{-3})) \leq 3$  puesto que  $-1 = \sqrt{-3}^2 + 1^2 + 1^2$ . Por el mismo razonamiento  $s(\mathbb{Q}(\sqrt{-11})) \leq 3$
- $s(\mathbb{Q}(\sqrt{-d})) \leq 5$  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.

---

<sup>2</sup>de. Stufe.



**Teorema 7.20:** Sea  $k$  un cuerpo arbitrario y sea  $n = 2^m$ . Entonces existen identidades de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \quad (7.1)$$

donde:

$$z_j = \sum_{i=1}^n t_{ij} y_j, \quad t_{ij} \in k(x_1, \dots, x_n).$$

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  $T := [t_{ij}]_{ij}$ , 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

$$\begin{aligned} (x_1^2 + \cdots + x_n^2)(y_1, \dots, y_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} &= (z_1, \dots, z_n) \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \\ &= (y_1, \dots, y_n) t^t t \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \end{aligned}$$

Reordenando los términos equivale a que

$$\begin{aligned} (y_1, \dots, y_n) ((x_1^2 + \cdots + x_n^2) I_n - T^t T) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} &= 0, \\ (x_1^2 + \cdots + x_n^2) I_n &= T^t T. \end{aligned}$$

Ahora, queremos ver que éste es el caso para  $m+1$  y, por ende, para  $2n$ . Sea

$$((x_1, \dots, x_n), (x_{n+1}, \dots, x_{2n})) = (\mathbf{X}_1, \mathbf{X}_n).$$

Por hipótesis inductiva existen  $T_1, T_2$  tales que:

$$(x_1^2 + \cdots + x_n^2) I_n = \mathbf{X}_1 \mathbf{X}_1^t I_n = T_1 T_1^t = T_1^t T_1,$$

$$(x_{n+1}^2 + \cdots + x_{2n}^2)I_n = \mathbf{X}_2 \mathbf{X}_2^t I_n = T_2 T_2^t = T_2^t T_2.$$

Queremos encontrar un  $T$  que funcione para ambas matrices en simultáneo. Sea  $T := \begin{pmatrix} T_1 & T_2 \\ T_2 & M \end{pmatrix}$ , entonces se tiene que

$$\begin{aligned} T^t T &= \begin{bmatrix} T_1^t T_1 + T_2^t T_2 & T_1^t T_2 + T_2^t M \\ T_2^t T_1 + M^t T_2 & T_2^t T_2 + M^t M \end{bmatrix} \\ &= \begin{bmatrix} (x_1^2 + \cdots + x_{2n}^2)I_n & A \\ B & C \end{bmatrix}. \end{aligned}$$

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:

$$\begin{aligned} C &= T_2^t T_2 + M^t M = (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + T_2^t T_1 T_2^{-1} (T_2^t)^{-1} T_1^t T_2 \\ &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + (x_{n+1}^2 + \cdots + x_{2n}^2)^{-1} T_2^t T_1 T_1^t T_2 \\ &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + (x_1^2 + \cdots + x_n^2)I_n. \end{aligned}$$

Ésto completa la demostración.  $\square$

**Lema 7.21 (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  $\text{car } k = 2$ , entonces como  $a^2 + b^2 = (a + b)^2$  se nota que se reduce al caso  $n = 1$ .
- (c) Si  $\text{car } k \neq 2$  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

$$f \cdot h^2 = g_1^2 + \cdots + g_n^2, \quad g_1, \dots, g_n, h \in k[x], h \neq 0.$$

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  $(\zeta, \eta_1, \dots, \eta_n)$  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  $\gamma_j$  es o bien nulo, o bien  $\deg \gamma_j < \deg \zeta$ . Nótese que, por minimalidad de  $\zeta$ , existe algún  $j$  tal que  $\gamma_j \neq 0$ . Definamos

$$\begin{aligned} \alpha &:= \sum_{i=1}^n \lambda_i^2 - f, & \beta &:= \sum_{i=1}^n \lambda_i \eta_i - f\zeta, \\ \bar{\zeta} &:= \alpha\zeta - 2\beta, & \bar{\eta}_j &:= \alpha\eta_j - 2\beta\lambda_j. \end{aligned}$$

Es claro que ambos son polinomios en  $k[x]$ .

- (I)  $(\bar{\zeta}, \bar{\eta}_1, \dots, \bar{\eta}_n)$  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  $4\beta$  común y expandiendo la definición de  $\alpha, \beta$  se reduce a probar que

$$\begin{aligned} 4\beta \cdot \left( \left( \sum_{i=1}^n \lambda_i \eta_i - f\zeta \right) \sum_{j=1}^n \lambda_j^2 - \left( \sum_{i=1}^n \lambda_i^2 - f \right) \sum_{j=1}^n \eta_j \lambda_j \right. \\ \left. - \left( \sum_{j=1}^n \lambda_j \eta_j - f\zeta \right) f + \left( \sum_{i=1}^n \lambda_i^2 - f \right) f\zeta \right) = 0. \end{aligned}$$

- (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  $\gamma_j^2$  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  $\deg(\bar{\zeta}) < \deg \zeta$ .

Esto contradice la minimalidad del grado de  $\zeta$  lo que es absurdo.  $\square$

Varios corolarios:

**Corolario 7.21.1:** Sea  $\text{car } k \neq 2$  y sea  $f(x_1, \dots, x_m) \in k(x_1, \dots, x_m)$  una suma de  $n$  cuadrados. Sean  $a_1, \dots, a_m \in k$  tales que  $f(a_1, \dots, a_m)$  está bien definido (el denominador no es cero), entonces  $f(a_1, \dots, a_m)$  es una suma de  $n$  cuadrados.

**Corolario 7.21.2:** 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: Esto sale del teorema 7.20.  $\square$

**Corolario 7.21.3:** Sea  $\text{car } k \neq 2$  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:  $\Leftarrow$  es claro. Veamos  $\Rightarrow$ : Sea  $x^2 + d = p_1(x)^2 + \cdots + p_n(x)^2$  con  $p_i(x) \in k[x]$  de grado  $\leq 1$ . 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  $\text{car } k \neq 2$ , 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

$$\mathcal{C}^2 + d = (a_1 C + b_1)^2 + \cdots + (a_{n-1} C + b_{n-1})^2 + \mathcal{C}^2,$$

con lo que comprobamos que  $d$  se escribe como suma de  $n-1$  cuadrados.  $\square$

**Corolario 7.21.4:** Considere  $\mathbb{R}(x_1, \dots, x_n)$ , aquí  $x_1^2 + \dots + x_n^2$  no es una suma de  $n - 1$  cuadrados.

PISTA: Aplicar inducción y definir  $k := \mathbb{R}(x_1, \dots, x_n)$  de modo que  $k(x_{n+1}) = \mathbb{R}(x_1, \dots, x_{n+1})$ .  $\square$

**Teorema 7.22:** 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  $a_1^2 + \dots + a_n^2 + a_{n+1}^2 + \dots + a_{2n-1}^2 + 1 = 0$  para algunos  $a_i \in k$  (posiblemente nulos). Sean

$$A := a_1^2 + \dots + a_n^2, \quad B := a_{n+1}^2 + \dots + a_{2n-1}^2 + 1,$$

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  $k := \mathbb{R}(x_1, \dots, x_{n+1})$  y  $L := k(\gamma)$ , donde los  $x_i$ 's son indeterminadas (elementos trascendentes algebraicamente independientes) y  $\gamma$  es raíz del polinomio:

$$\gamma^2 + x_1^2 + \dots + x_{n+1}^2 = 0,$$

dividiendo por  $\gamma^2$  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  $t_1, \dots, t_n \in L$  tales que

$$t_1^2 + \dots + t_n^2 = 0.$$

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  $\alpha_i$  es no nulo, y análogamente se puede ver que algún  $\beta_i$  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 esto contradice el corolario anterior. En conclusión, se cumple que  $n = s(L)$  como se quería probar.  $\square$

¿Los cuerpos de nivel arbitrariamente grande siempre tienen alto grado de trascendencia sobre  $\mathbb{Q}$ ?

Ahora también podemos probar un recíproco del teorema 7.20:

**Teorema 7.23:** 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:

$$z_j = \sum_{i=1}^n t_{ij} y_j, \quad t_{ij} \in k(x_1, \dots, x_n).$$

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 esto es absurdo puesto que  $n < s(k)$ .  $\square$

**§7.2.1 Calculando el nivel.** Ahora veremos cómo calcular el nivel de ciertos cuerpos. Comencemos sencillo con los finitos:

**Proposición 7.24:** 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 7.25 (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

$$t^2 n = \mu_1^2 + \mu_2^2 + \mu_3^2, \quad t, \mu_1, \mu_2, \mu_3 \in \mathbb{Z},$$

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  $q_i \in \mathbb{Z}$  y  $|r_i| \leq 1/2$ . Por minimalidad de  $t$  podemos suponer que algún  $r_i$  es no nulo y definamos:

$$\begin{aligned} a &:= q_1^2 + q_2^2 + q_3^2 - n, & b &:= 2(nt - (\mu_1 q_1 + \mu_2 q_2 + \mu_3 q_3)), \\ \bar{t} &:= at + b, & \bar{\mu}_i &:= a\mu_i + bq_i. \end{aligned}$$

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:

$$\begin{aligned} t \cdot \bar{t} &= at^2 + bt \\ &= t^2 \left( \sum_{i=1}^3 q_i^2 - n \right) + t \left( 2nt - 2 \sum_{i=1}^3 \mu_i q_i \right) \end{aligned}$$

$$\begin{aligned}
&= t^2 \sum_{i=1}^3 q_i^2 - 2t \sum_{i=1}^3 \mu_i q_i + \sum_{i=1}^3 \mu_i^2 \\
&= \sum_{i=1}^3 (tq_i - \mu_i)^2 = t^2(r_1^2 + r_2^2 + r_3^2).
\end{aligned}$$

Y que es menor que  $t$ :

$$\bar{t} = t(r_1^2 + r_2^2 + r_3^2) \leq t \left( \frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^2} \right) = \frac{3}{4}t. \quad \square$$

**Teorema 7.26:** Sea  $d > 0$  un entero libre de cuadrados. Entonces:

$$s(\mathbb{Q}(\sqrt{-d})) = \begin{cases} 1, & d = 1 \\ 2, & d \not\equiv 7 \pmod{8} \\ 4, & d \equiv 7 \pmod{8} \end{cases}$$

Más aún,  $s(\mathbb{Q}(\sqrt{-d})) = 2$  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

$$\begin{aligned}
-1 &= (a_1 + b_1\sqrt{-d})^2 + (a_2 + b_2\sqrt{-d})^2 \\
&= (a_1^2 + a_2^2 - d(b_1^2 + b_2^2)) + 2(a_1b_1 + a_2b_2)\sqrt{-d},
\end{aligned}$$

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.  $\square$



---

## 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  $\pi_j: \prod_{i \in I} G_i \rightarrow G_j$  son homomorfismos de grupos.
2. Si  $H$  es un grupo y  $\{\varphi_i: H \rightarrow G_i\}_{i \in I}$  es una familia de homomorfismos de grupos, entonces existe un único homomorfismo  $\psi := \Delta_{i \in I} \varphi_i: H \rightarrow \prod_{i \in I} G_i$  tal que el siguiente entonces existe un único homomorfismo  $\psi := \Delta_{i \in I} \varphi_i: H \rightarrow \prod_{i \in I} G_i$  tal que el siguiente diagrama:

$$\begin{array}{ccc}
 H & & \\
 \exists! \psi \downarrow & \searrow \varphi_j & \\
 \prod_{i \in I} G_i & \xrightarrow{\pi_j} & G_j
 \end{array}$$

conmuta. En consecuencia,  $\prod_{i \in I} G_i$  es un producto categorial en  $\mathbf{Grp}$ .

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  $\iota_j : G_j \rightarrow \bigoplus_{i \in I} G_i$  son homomorfismos de grupos.
2. Si  $H$  es un grupo y  $\{\varphi_i : G_i \rightarrow H\}_{i \in I}$  es una familia de homomorfismos de grupos, entonces existe un único homomorfismo  $\psi := \sum_{i \in I} \varphi_i : \bigoplus_{i \in I} G_i \rightarrow H$  tal que el siguiente diagrama:

$$\begin{array}{ccc}
 & H & \\
 \exists! \psi \uparrow & \nwarrow \varphi_j & \\
 \bigoplus_{i \in I} G_i & \xleftarrow{\iota_j} & G_j
 \end{array}$$

conmuta. En consecuencia,  $\bigoplus_{i \in I} G_i$  es un coproducto categorial en  $\mathbf{Grp}$ .

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  $\mathbf{Ab}$ , esto 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.  $\square$

**Corolario 8.6.1:** 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  $\kappa$ .
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.  $\square$

**Definición 8.7:** Dado un grupo abeliano libre  $G$ , se denota por  $\text{rank } G$  a la cardinalidad de cualquiera de sus bases.

**Proposición 8.8:** Sea  $G$  un grupo abeliano con un conjunto  $X$  tal que satisface lo siguiente: Para todo grupo abeliano  $H$  y toda aplicación  $f: X \rightarrow H$ , existe una única extensión  $f^*: G \rightarrow H$  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  $q: X \rightarrow Y$  de inversa  $p: Y \rightarrow X$ . Luego, por ser libres, ambas funciones se extienden a  $f: G \rightarrow H$  y  $g: H \rightarrow G$ , homomorfismos de grupos. Nótese que además  $p \circ q = \text{Id}_X: X \rightarrow X \subseteq G$  es una aplicación que posee una extensión  $\text{Id}_G: G \rightarrow G$  que es única, y lo mismo vale para  $\text{Id}_H$  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.  $\square$

**Proposición (AE) 8.9:** 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  $g: X \rightarrow M$  dada por  $g([x_i]) := x_i$  admite una extensión única  $g: M/N \rightarrow M$ , tal que  $g \circ \pi$  fija a la base, luego por unicidad, se cumple que  $g \circ \pi = \text{Id}_{M/N}$ . Es decir, la sucesión exacta se escinde y por la proposición 5.15 se cumple el enunciado.  $\square$

Como ejercicio en la demostración anterior ubique el uso de elección.

**Teorema (AE) 8.10:** Sea  $A$  un DIP, entonces todo  $A$ -submódulo  $M$  de un módulo libre  $F$  es también libre; y de hecho  $\text{rank } M \leq \text{rank } F$ .

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

$$F'_\beta := \langle \{x_\alpha : \alpha < \beta\} \rangle, \quad F_\beta := F'_\beta \oplus \langle x_\beta \rangle.$$

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  $M_\beta/M'_\beta$  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  $M_\beta \cong M'_\beta \oplus \langle \mathbf{m}_\beta \rangle$  para algún  $\mathbf{m}_\beta \in M_\beta$  tal que  $\langle \mathbf{m}_\beta \rangle \cong A$ ; si el ideal es nulo entonces  $\mathbf{m}_\beta := \vec{0}$ . Claramente, eliminando los  $\mathbf{m}_\beta$ '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  $M^* := \text{Span}\{\mathbf{m}_\beta\}_{\beta < \kappa}$  y definamos:

$$\mu(\mathbf{m}) := \min\{\alpha : \mathbf{m} \in F_\alpha\}.$$

Supongamos que  $M^* < M$ , entonces definamos  $\gamma$  como el mínimo índice tal que  $\gamma = \mu(\mathbf{m})$  para algún  $\mathbf{m} \in M \setminus M^*$  y sea  $\tilde{\mathbf{m}}$  un elemento que cumpla lo anterior, luego se cumple que

$$\tilde{\mathbf{m}} = \mathbf{a} + \lambda \mathbf{m}_\gamma \in M_\gamma$$

para unos únicos  $\mathbf{a} \in M'_\gamma$  y  $\lambda \in A$ . Luego como  $\mathbf{m}_\gamma \in M^*$  y  $\tilde{\mathbf{m}} \notin M^*$  necesariamente se tiene que  $\mathbf{a} \notin M^*$ . Pero  $\mathbf{a} \in F'_\gamma$ , luego  $\mu(\mathbf{a}) < \gamma$  contradiciendo la minimalidad de  $\gamma$ .  $\square$

Nótese que su  $F$  es finitamente generado, entonces no hay uso de elección.

**Proposición 8.11:** Sea  $A$  un anillo,  $F$  un  $A$ -módulo libre de base  $X$  y  $M$  otro  $A$ -módulo. Toda aplicación  $f: X \rightarrow M$  admite una única extensión  $f^*: F \rightarrow M$  en un morfismo de  $A$ -módulos.

**Definición 8.12:** Sea  $G$  un grupo abeliano, definimos su *subgrupo de torsión* como

$$G_{\text{tors}} := \{x \in G : \text{ord } x \neq 0\},$$

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  $G_{\text{tors}} = G$ ; y se dice *libre de torsión* si  $G_{\text{tors}} = \{1\}$ .

**Ejemplo.** Todo grupo abeliano finito es un grupo de torsión.  $(\mathbb{Z}, +)$  es libre de torsión.  $(\mathbb{R}^\times, \cdot)$  es tal que  $\mathbb{R}_{\text{tors}}^\times = \{\pm 1\}$ , así que ni es de torsión ni es libre de torsión.

**Proposición 8.13:** Para todo  $G, H$  abelianos, se cumplen:

1.  $G/G_{\text{tors}}$  es libre de torsión.
2. Si  $G \cong H$ , entonces  $G_{\text{tors}} \cong H_{\text{tors}}$  y  $G/G_{\text{tors}} \cong H/H_{\text{tors}}$ .

**Teorema 8.14:** 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  $\text{rank } H \leq \text{rank } G$ .
3. (AE) Todo subgrupo  $H$  de un grupo abeliano libre  $G$  es también abeliano libre y además  $\text{rank } H \leq \text{rank } G$ .

DEMOSTRACIÓN:

1. La demostración es por inducción sobre la cantidad de generadores  $\langle x_1, \dots, x_n \rangle$  del grupo  $G$ . Claramente se satisface el caso base  $n = 1$ .

Para el caso inductivo, sea  $G := \langle x_1, \dots, x_n, x_{n+1} \rangle$  y sea

$$H := \{g \in G : \exists m \in \mathbb{Z}_{\neq 0} \text{ } mg \in \langle x_{n+1} \rangle\}.$$

Claramente  $H \leq G$ , y  $G/H$  es un grupo abeliano, libre de torsión (¿por qué?) que está generado por  $\{[x_1], \dots, [x_n]\}$ , 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  $\varphi: H \rightarrow \mathbb{Q}$  dado por  $\varphi(g) := r/m$ . Nótese que  $\varphi$  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  $\varphi$  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  $F := \langle a_1/b_1, \dots, a_r/b_r \rangle \leq \mathbb{Q}$ . Y sea  $d := \prod_{i=1}^n b_i$ , entonces  $f: D \rightarrow \mathbb{Z}$  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 8.10.  $\square$

**Corolario 8.14.1:** Se cumplen:

1. Todo grupo abeliano finitamente generado  $G$  puede escribirse como

$$G = G_{\text{tors}} \oplus F$$

donde  $F$  es un grupo abeliano libre finitamente generado.

2. Dados  $G, H$  abelianos y finitamente generados. Entonces  $G \cong H$  syss  $G_{\text{tors}} \cong H_{\text{tors}}$  y  $\text{rank}(G/G_{\text{tors}}) \cong \text{rank}(H/H_{\text{tors}})$ .

## 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  $v \mapsto v \cdot B$ .

**Definición 8.15:** Sea  $T: V \rightarrow V$  una función lineal, si existe  $v \in V_{\neq 0}$  tal que  $T(v) = \lambda v$  para algún  $\lambda \in k$ , entonces se dice que  $v$  es un *autovector* y  $\lambda$  es su *autovalor* asociado.

Denotamos por  $\sigma(T)$  al conjunto de los autovalores de  $T$ .

**Teorema 8.16:** Dado  $A \in \text{Mat}_n(k)$ , se cumple que  $\lambda$  es autovalor de  $A$  syss  $\det(\lambda I_n - A) = 0$ .

DEMOSTRACIÓN: Sea  $\lambda$  el autovalor asociado a  $\mathbf{v} \in V_{\neq \vec{0}}$ , es decir,  $\mathbf{v}A = \lambda\mathbf{v}$ . Luego  $\mathbf{v} \cdot (\lambda I_n - A) = \vec{0}$ , por lo que  $\lambda I_n - A$  no es inversible y  $\det(\lambda I_n - A) = 0$ . El recíproco es análogo.  $\square$

**Definición 8.17:** Dado  $A \in \text{Mat}_n(k)$ , 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  $\lambda$  es autovalor de  $A$  syss  $\lambda$  es raíz de  $\psi_A$ .

**Corolario 8.17.1:** Toda matriz de  $n \times n$  posee a lo más  $n$  autovalores.

**Teorema 8.18:** 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

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

$\square$

**Lema 8.19:** Sea  $A \in \text{Mat}_n(k)$ , entonces  $\psi_A(x)$  es un polinomio mónico y el coeficiente que acompaña al monomio  $x^{n-1}$  es  $-(a_{11} + a_{22} + \cdots + a_{nn}) = -\text{tr}(A)$ .

**Proposición 8.20:** Sea  $A \in \text{Mat}_n(\bar{k})$ , tal que sus autovalores son  $\alpha_1, \dots, \alpha_n$  (contando multiplicidades), entonces

$$\text{tr}(A) = - \sum_{i=1}^n \alpha_i, \quad \det(A) = \prod_{i=1}^n \alpha_i.$$

**Definición 8.21:** Se dice que dos matrices  $A, B \in \text{Mat}_n(k)$  son *similares* si existe  $C \in \text{GL}(n, k)$  tal que  $A = C^{-1}BC$ .

**Proposición 8.22:** Dadas dos matrices  $A, B \in \text{Mat}_n(k)$  que son similares se cumple que  $\psi_A = \psi_B$ .

DEMOSTRACIÓN: Sea  $C \in \text{GL}(n, k)$  tal que  $A = C^{-1}BC$ , luego  $\det(xI - A) = \det(xC^{-1}IC - C^{-1}BC) = \det(C^{-1}) \det(xI - B) \det(C)$ .  $\square$

**Definición 8.23:** Se dice que una matriz  $A \in \text{Mat}_n(k)$  es *diagonalizable* si es similar a una matriz diagonal. Equivalentemente, un endomorfismo es diagonalizable si su representación matricial en alguna base es diagonal.

**Teorema 8.24:** Una matriz  $A$  es diagonalizable si y sólo si el conjunto de sus autovectores genera el espacio. En cuyo caso,  $A$  es similar a  $\text{diag}(\alpha_1, \dots, \alpha_n)$ , donde los  $\alpha_i$ 's son los autovalores (contando multiplicidad) de la matriz.

DEMOSTRACIÓN:  $\Leftarrow$ . Sean  $S$  los autovectores de  $A$ . Si  $\text{Span } S = V$ , entonces existe  $B \subseteq S$  base y claramente  $M_B^B(A) = \text{diag}(\alpha_1, \dots, \alpha_n)$ .

$\Rightarrow$ . Sea  $B := C^{-1}AC = \text{diag}(\beta_1, \dots, \beta_n)$ , entonces  $e_1 B = \beta_1 e_1$ ,  $e_2 B = \beta_2 e_2$  y así. Por lo que, definiendo  $v_i := e_i C^{-1}$  se obtiene que  $v_i$  son autovectores de  $A$  que generan el espacio y que los  $\beta_i$ 's eran efectivamente los autovalores de  $A$ .  $\square$

### 8.3 Formas bilineales

Volvemos al contexto general de módulos. Recordemos lo siguiente:

**Definición 8.25:** Sea  $A$  un dominio. Una forma bilineal sobre un  $A$ -módulo  $M$  es una aplicación

$$\beta: M \times M \longrightarrow A$$

tal que  $\beta$  es lineal en cada coordenada.

Se dice que una forma bilineal  $\beta$  es *no degenerada* si para todo homomorfismo de  $R$ -módulos  $\varphi: M \rightarrow R$  se cumple que existe un único  $\mathbf{x}_0$  tal que  $\varphi(\mathbf{y}) = \beta(\mathbf{x}_0, \mathbf{y})$ ; y que existe un único  $\mathbf{y}_0$  tal que  $\varphi(\mathbf{x}) = \beta(\mathbf{x}, \mathbf{y}_0)$ . En cuyo caso, se dice que la forma bilineal es un *producto interno* y se suele denotar  $\beta(\mathbf{x}, \mathbf{y}) =: \mathbf{x} \cdot \mathbf{y}$ .

Si  $\beta$  es una forma bilineal (resp. producto interno) sobre  $M$ , decimos que el par  $(M, \beta)$  es un  *$A$ -módulo de forma bilineal* (resp.  *$A$ -módulo de producto interno*). De no haber ambigüedad sobre los signos omitiremos el  $\beta$ .

Un homomorfismo  $f: (M, \beta) \rightarrow (M', \beta')$  de  $A$ -módulos de forma bilineal es un homomorfismo de  $A$ -módulos  $f: M \rightarrow M'$  tal que

$$\beta'(f(x), f(y)) = \beta(x, y).$$

**Proposición 8.26:** Los  $A$ -módulos de forma bilineal (como objetos) y los homomorfismos entre ellos (como flechas) conforman una categoría, denotada  $\text{Bil}_A$ .

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 8.27:** Un  $A$ -módulo de producto interno  $(M, \beta)$  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 8.28:** Sea  $(M, \beta)$  un  $A$ -módulo libre de forma bilineal de rango finito. Sea  $X = (x_1, \dots, x_n)$  una base ordenada de  $M$ , entonces llamamos *representación matricial de  $\beta$*  a la matriz

$$M_X(\beta) := [\beta(x_i, x_j)]_{ij}.$$

**Proposición 8.29:** Sea  $(M, \beta)$  un  $A$ -módulo libre de forma bilineal de rango finito y sea  $B$  su representación matricial en alguna base ordenada. Entonces  $\beta$  es una forma bilineal (anti)simétrica syss  $B$  es una matriz (anti)simétrica.

**Proposición 8.30:** Sea  $(M, \beta)$  un  $A$ -módulo libre de forma bilineal de rango finito. Sean  $X, Y$  dos bases ordenadas de  $M$  y sea  $A := M_X^Y(\text{Id})$  la matriz de cambio de base, entonces

$$M_Y(\beta) = A \cdot M_X(\beta) \cdot A^t.$$

DEMOSTRACIÓN: Sea  $A = [a_{ij}]_{ij}$ , de modo que  $y_i = \sum_{j=1}^n a_{ij}x_j$ . Luego nótese que

$$\begin{aligned} (M_Y(\beta))_{ij} &= \beta(y_i, y_j) = \beta\left(\sum_{k=1}^n a_{ik}x_k, y_j\right) = \sum_{k=1}^n a_{ik}\beta(x_k, y_j) \\ &= \sum_{k=1}^n a_{ik} \cdot \left(\sum_{\ell=1}^n a_{j\ell}\beta(x_k, x_\ell)\right) \\ &= \sum_{k=1}^n a_{ik} \cdot \left(\sum_{\ell=1}^n \beta(x_k, x_\ell)(A^t)_{\ell j}\right) = (A \cdot M_X(\beta) \cdot A^t)_{ij}. \quad \square \end{aligned}$$

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 8.31:** Sea  $(M, \beta)$  un  $A$ -módulo libre de forma bilineal de rango finito.  $\beta$  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 8.32:** Sean  $(A^n, \beta)$  y  $(A^n, \gamma)$  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 8.33:** Sea  $(M, \beta)$  un  $A$ -módulo libre de forma bilineal de rango finito. Llamamos *determinante* del producto  $\beta$ , denotado  $\det(\beta)$ , al elemento  $[\det(B)] \in A/(A^\times)^2$ , donde  $B$  es la representación matricial de  $\beta$  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 8.34:** Sea  $(e_1, \dots, e_n)$  la base ordenada de un  $A$ -espacio de producto interno. Entonces se le llama base dual  $(f_1, \dots, f_n)$  a la tupla tal que  $\beta(e_i, f_j) = \delta_{ij}$ .

**Proposición 8.35:** A toda base ordenada de un  $A$ -espacio de producto interno le corresponde una única base dual.

**Definición 8.36:** Sean  $(M_1, \beta_1), \dots, (M_n, \beta_n)$  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

$$\beta((u_1, \dots, u_n), (v_1, \dots, v_n)) = \sum_{i=1}^n \beta_i(u_i, v_i).$$

**Proposición 8.37:** Sean  $M_1, \dots, M_n$  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

$$\text{rang} \left( \bigoplus_{i=1}^n M_i \right) = \sum_{i=1}^n \text{rang}(M_i), \quad \det \left( \bigoplus_{i=1}^n M_i \right) = \prod_{i=1}^n \det(M_i).$$

**Definición 8.38:** 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 8.39 (de descomposición ortogonal):** Sea  $M$  un  $A$ -módulo de forma bilineal (anti)simétrica. Supongamos que  $N \leq M$  es tal que  $\beta \upharpoonright N \times N$  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.  $\square$

Nótese que no se le exige a  $\beta$  ser producto interno en todo  $M$ , sino sólo en  $N$ .

**Teorema 8.40:** Sea  $M$  un  $A$ -módulo de forma bilineal (anti)simétrica. Sean  $x_1, \dots, x_k \in M$  tales que la matriz  $[\beta(x_i, x_j)]_{ij} \in \text{Mat}_k(A)$  es invertible, entonces  $x_1, \dots, x_k$  son linealmente independientes y denotando  $N := \text{Span}_A(x_1, \dots, x_k)$  se cumple que

$$M \cong N \oplus N^\perp.$$

**Corolario 8.40.1:** Sea  $M$  un  $A$ -módulo finitamente generado de forma bilineal simétrica. Entonces existe un submódulo  $N \leq M$  y existen  $a_1, \dots, a_k \in A^\times$  tales que

$$M \cong \langle a_1 \rangle \oplus \dots \oplus \langle a_k \rangle \oplus N,$$

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.  $\square$

**Definición 8.41:** 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 8.41.1:** 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

$$M \cong \langle a_1 \rangle \oplus \dots \oplus \langle a_k \rangle \oplus N.$$

Luego  $N$  es un  $A$ -módulo proyectivo sobre un dominio local, ergo es libre (teo. 6.45) y posee una base  $X$ , de la que podemos extraer un conjunto finito  $e_1, \dots, e_n$  que posee una base dual  $f_1, \dots, f_n$  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  $2 \in A^\times$ .  $\square$

### §8.3.2 El teorema de Witt.

**Definición 8.42:** 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  $r: M \rightarrow M$  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.,  $r \circ r = \text{Id}_M$ . Además, las reflexiones son endomorfismos de Bil, i.e., preservan la forma bilineal:

$$\beta(r(x), r(y)) = \beta(x, y).$$

**Lema 8.43:** 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 pérdida de generalidad, si  $\beta(u, u)$  es inversible, entonces  $M = (Au) \oplus (Au)^\perp$  y construimos la reflexión apropiada.  $\square$

**Corolario 8.43.1:** 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  $f: M \rightarrow M$  es la composición de  $n$  reflexiones.

DEMOSTRACIÓN: Basta notar que un automorfismo transforma bases en bases y aplicar inducción.  $\square$



**Teorema 8.44 – 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  $\text{Bil}_A$ ), entonces  $M \cong N$  (en  $\text{Bil}_A$ ).

DEMOSTRACIÓN: Podemos escribir  $P$  como la suma ortogonal de espacios libres de rango 1, así que, aplicando inducción basta considerar  $P = \text{Span}_A(e)$ . Sea  $f: M \oplus P \rightarrow N \oplus P$  un isomorfismo arbitrario, luego  $f(\vec{0}_M, e)$  y  $(\vec{0}_N, e)$  en  $N \oplus P$  satisfacen las hipótesis del lema 8.43, de modo que existe una reflexión  $r: N \oplus P \rightarrow N \oplus P$  tal que  $r(f(\vec{0}_M, e)) = (\vec{0}_N, e)$ . Luego

$$f \circ r: M \oplus P \longrightarrow N \oplus P$$

es un isomorfismo que manda el subespacio  $P_M := \text{Span}_A\{(\vec{0}_M, e)\}$  en el subespacio  $P_N := \text{Span}_A\{(\vec{0}_N, e)\}$  y, por lo tanto, manda los complementos ortogonales  $M = P_M^\perp$  en  $N = P_N^\perp$ .  $\square$

### §8.3.3 El anillo de Witt.

**Lema 8.45:** Sean  $(M_1, \beta_1), \dots, (M_n, \beta_n)$  un conjunto de  $A$ -módulos de forma bilineal. Existe una única forma bilineal  $\beta$  sobre  $N := M_1 \otimes \dots \otimes M_n$  que satisface que

$$\beta(x_1 \otimes \dots \otimes x_n, y_1 \otimes \dots \otimes y_n) = \prod_{i=1}^n \beta_i(x_i, y_i)$$

para todos  $x_i, y_i \in M_i$ .

DEMOSTRACIÓN: Consideremos que la aplicación

$$\begin{aligned} \phi: M_1 \times \dots \times M_n \times M_1 \times \dots \times M_n &\longrightarrow A \\ (x_1, \dots, x_n, y_1, \dots, y_n) &\longmapsto \prod_{i=1}^n \beta_i(x_i, y_i) \end{aligned}$$

es  $2n$ -multilineal, de modo que induce un homomorfismo de  $A$ -módulos

$$M_1 \otimes \dots \otimes M_n \otimes M_1 \otimes \dots \otimes M_n = N \otimes N \longrightarrow A$$

el cual es único. Nótese que  $\phi$  también se extiende a una aplicación  $N \times N \rightarrow A$  bilineal que coincide con  $\beta$  cuya extensión es la misma aplicación superior. Ésto comprueba el enunciado.  $\square$

**Lema 8.46:** Si  $M_1, \dots, M_n$  son  $A$ -espacios de producto interno, entonces  $M_1 \otimes \dots \otimes M_n$  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 5.62.1). Denotemos por  $M^* := \text{Hom}_A(M, A)$ . Luego cada producto interno  $\beta_i$  da lugar a un isomorfismo:

$$\begin{aligned} \bar{\beta}_i: M_i &\longrightarrow M_i^* \\ x &\longmapsto (y \xrightarrow{\bar{\beta}_i(x)} \beta_i(x, y)) \end{aligned}$$

Luego, si  $\eta: M_1^* \otimes \dots \otimes M_n^* \rightarrow (M_1 \otimes \dots \otimes M_n)^*$  es el isomorfismo canónico, entonces podemos definir el siguiente homomorfismo de  $A$ -módulos:

$$\bar{\beta} := (\bar{\beta}_1 \otimes \dots \otimes \bar{\beta}_n) \circ \eta: M_1 \otimes \dots \otimes M_n \longrightarrow (M_1 \otimes \dots \otimes M_n)^*,$$

de modo que se comprueba el enunciado.  $\square$

**Definición 8.47:** Se dice que un  $A$ -espacio de producto interno simétrico  $M$  es un  $A$ -espacio metabólico<sup>1</sup> si existe  $N \leq M$  tal que  $N = N^\perp$  y  $N$  es un sumando directo de  $M$ .

**Lema 8.48:** Sean  $M, M'$  dos  $A$ -espacios metabólicos y  $(N, \beta)$  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

$$M \otimes_A N = (N, \beta) \oplus (N, -\beta). \quad \square$$

**Lema 8.49:** 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

<sup>1</sup>Knebusch [0, pág. 122] emplea «metabólico», mientras que Milnor [0, pág. 12] emplea «se escinde» (eng. *split*).

$A$ -espacio de producto interno es metabólico si 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  $e_1, \dots, e_n$  una base para  $N$ , la cual podemos extender a una base  $e_1, \dots, e_m$  para  $M$ , y sea  $f_1, \dots, f_m$  su base dual.

Claramente, podemos restringir la base dual a  $f_{n+1}, \dots, f_{2n}$  que es base para  $N^\perp = N$ , de modo que podemos sustituir los elementos y obtener la siguiente base de  $M$ :

$$X := (e_1, \dots, e_n, f_1, \dots, f_n).$$

Un mero cálculo comprueba que  $M_X(\beta) = \begin{bmatrix} \mathbf{0} & I \\ I & B \end{bmatrix}$  y el recíproco es claro.

Supongamos que  $2 \in A^\times$  y definamos la matriz  $C := -\frac{1}{2}B$  de modo que

$$\begin{bmatrix} I & \mathbf{0} \\ C & I \end{bmatrix} \begin{bmatrix} \mathbf{0} & I \\ I & B \end{bmatrix} \begin{bmatrix} I & \mathbf{0} \\ C & I \end{bmatrix}^t = \begin{bmatrix} \mathbf{0} & I \\ I & \mathbf{0} \end{bmatrix}. \quad \square$$

**Definición 8.50:** 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 8.51:** 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  $M \otimes_A \langle 1 \rangle \sim M$ , esto, combinado con el trabajo anterior nos comprueba lo siguiente:

**Teorema 8.52:**  $W(A)$  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  $M$ ,  $f \in \text{End}(M)$  y un subespacio  $S$  de  $M$ , se dice que  $S$  es  $f$ -invariante si  $f[S] \subseteq S$ .

**Proposición 9.2:** Para todo  $f \in \text{End}(M)$  se cumple que son subespacios  $f$ -invariantes:

1. El subespacio nulo  $\{0\}$ .
2. Todo subespacio de  $\ker f$ .
3. Todo subespacio que contenga a  $\text{Im} f$ .

**Lema 9.3:** Si  $f \in \text{End}(\mathbb{k}^n)$  y  $X, Y$  son bases ordenadas cualesquiera de  $\mathbb{k}^n$ , entonces para todo  $x \in \mathbb{k}$

$$\det(xI_n - M_X^X(f)) = \det(xI_n - M_Y^Y(f))$$

DEMOSTRACIÓN: Como hemos visto

$$M_Y^Y(f) = M_Y^X(\text{Id}) M_X^X(f) M_X^Y(\text{Id}),$$

luego si llamamos  $B := M_X^Y(\text{Id})$  (que es invertible), cumple que

$$M_Y^Y(f) = B^{-1} M_X^X(f) B,$$

luego

$$\begin{aligned} \det(xI_n - M_Y^Y(f)) &= \det(xI_n - B^{-1} M_X^X(f) B) \\ &= \det(B^{-1}(xI_n - M_X^X(f))B) = \det(xI_n - M_X^X(f)). \end{aligned}$$

□

**Definición 9.4 – Polinomio característico:** Si  $f \in \text{End}(\mathbb{k}^n)$ , entonces dada una base  $X$  cualquiera se define

$$p_f(x) := \det(xI_n - M_X^X(f))$$

conocido como el *polinomio característico* de  $f$ .

**Definición 9.5:** Si  $M$  es un  $A$ -módulo y  $f \in \text{End}(M)$ , entonces  $v \in M_{\neq 0}$  se dice un *autovector* de  $f$  si  $\text{Span}\{v\}$  es  $f$ -invariante, o tradicionalmente, si existe  $\alpha \in M$  tal que  $f(v) = \alpha v$ , en cuyo caso se dice que  $\alpha$  es el *autovalor* asociado a  $v$  de  $f$ . Si  $M = A^n$  y  $B \in \text{Mat}_n(A)$ , 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  $M_X^X(f)$  es una matriz diagonal.

Se le llama *espectro* de  $f$ , denotado por  $\sigma(f)$  al conjunto de sus autovalores.

**Teorema 9.6:** Un escalar  $\lambda \in \sigma(f)$  si y sólo si  $p_f(\lambda) = 0$ .

**Definición 9.7:** Sea  $f \in \text{End}(V)$ . Si  $\alpha \in \mathbb{k}$ , entonces se les llaman *autoespacio* y *autoespacio generalizado* generado por  $\alpha$  de  $f$  a:

$$V_\alpha^f := \{v \in V : f(v) = \alpha v\}, N_\alpha^f := \{v \in V : \exists r \geq 0 (f - \alpha \text{Id})^r v = 0\};$$

de no haber ambigüedad se obvia el “ $f$ ”.

Para un  $\alpha \in \mathbb{k}$  se le dice *multiplicidad geométrica* y *algebraica* resp., a  $\dim V_\alpha$  y  $\dim N_\alpha$ .

**Proposición 9.8:** Para todo  $f \in \text{End}(\mathbb{k}^n)$  y todo  $\alpha \in \mathbb{k}$  se cumple:

1.  $V_\alpha$  y  $N_\alpha$  son submódulos o subespacios vectoriales de  $\mathbb{k}^n$ .
2.  $V_\alpha \leq N_\alpha$ .
3.  $V_\alpha$  y  $N_\alpha$  son  $f$ -invariantes.
4. La multiplicidad geométrica de  $\alpha$  siempre es menor o igual a su multiplicidad algebraica.
5.  $\alpha$  es autovalor syss tiene multiplicidad geométrica no nula syss tiene multiplicidad algebraica no nula.

**Definición 9.9 – Endomorfismo nilpotente:** Se dice que  $f \in \text{End}(V)$  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  $\lambda$  es autovalor de  $f$ , entonces  $f - \lambda \text{Id}$  restringido al autoespacio  $N_\lambda$  es nilpotente.

**Proposición 9.10:** Sea  $f \in \text{End}(V)$ :

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  $(f - \lambda \text{Id})$  es nilpotente en  $N_\lambda$ .

**Proposición 9.11:** Sea  $V$  un módulo sobre un dominio íntegro y  $f \in \text{End}(V)$ . Si  $\alpha \neq \beta$ , entonces  $f - \alpha \text{Id}$  es inyectiva en  $N_\beta$ . Y si el último es de dimensión finita, entonces  $f - \alpha \text{Id}$  es biyección.

DEMOSTRACIÓN: Sea  $v \in N_\beta$  tal que  $(f - \alpha \text{Id})v = 0$ , luego se cumple que

$$(f - \beta \text{Id})v = (\alpha - \beta)v.$$

Si  $v = 0$  entonces  $f - \alpha \text{Id}$  es inyectiva, como se quería probar. Si  $v \neq 0$ , entonces  $v$  es autovector de  $(f - \beta \text{Id})$  con autovalor  $\alpha - \beta \neq 0$ . Pero  $(f - \beta \text{Id})$  es nilpotente en  $N_\beta$ , luego sólo posee autovalores nulos, contradicción.  $\square$

**Teorema 9.12:** Sea  $V$  un módulo sobre un dominio íntegro y  $f \in \text{End}(V)$ . Si  $\alpha_1, \dots, \alpha_n$  son escalares distintos, entonces sus autoespacios generalizados son independientes. En consecuencia, sus autoespacios comunes 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

$$v_1 + \dots + v_n + v_{n+1} = 0,$$

por definición existe  $r > 0$  tal que

$$(f - \alpha_{n+1} \text{Id})^r v_{n+1} = 0,$$

luego aplicando la función al resto de  $v_i$ s se obtiene que

$$(f - \alpha_{n+1} \text{Id})^r v_1 + \dots + (f - \alpha_{n+1} \text{Id})^r v_n = 0,$$

que corresponde al paso inductivo, puesto que  $N_{\alpha_i}$  son invariantes; por lo tanto para todo  $i \in \{1, \dots, n\}$ :

$$(f - \alpha_{n+1} \text{Id})^r v_i = 0.$$

Finalmente aplicamos la proposición anterior que dice que  $(f - \alpha_{n+1} \text{Id})^r$  es biyección en  $N_{\alpha_i}$  para deducir que  $v_i = 0$ .  $\square$

**Corolario 9.12.1:** Sea  $f \in \text{End}(\mathbb{k}^n)$ . Si  $f$  posee  $n$  autovalores distintos, entonces es diagonalizable.

**Teorema 9.13:** Un endomorfismo es diagonalizable si y sólo si existe una base formada por sus autovectores.

**Teorema 9.14:** Son equivalentes:

1.  $\mathbb{k}$  es algebraicamente cerrado.
2. Toda matriz cuadrada con coeficientes en  $\mathbb{k}$  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

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

□

**Definición 9.15:** Se dice que un endomorfismo  $f \in L(\mathbb{k}^n)$  es *triangularizable* si existe una base ordenada  $X$  tal que su representación matricial es triangular. En el caso de matrices cuadradas, si existe  $C \in \text{Mat}_n(\mathbb{k})$  tal que  $C^{-1}BC$  es triangular.

**Teorema 9.16:** 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  $X := (x_1, \dots, x_n)$  la base para la que  $f$  es triangular. Luego la cadena viene dada por  $V_k := \langle x_1, \dots, x_k \rangle$ .

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:

$P(\mathbb{K}, d, r)$ : Todo conjunto  $A_1, \dots, A_r$  de matrices cuyo producto conmuta sobre  $\mathbb{K}^n$  con  $d \nmid n$  posee un autovector en común.

**Lema 9.17:** Si  $P(\mathbb{K}, d, 1)$ , entonces para todo  $r \geq 1$  se cumple que  $P(\mathbb{K}, d, r)$ .

DEMOSTRACIÓN: Probaremos la propiedad  $P(\mathbb{K}, d, r+1)$  por inducción fuerte sobre la dimensión  $n$  del espacio vectorial: El caso  $n = 1$  es trivial. Sean  $A_1, \dots, A_r, A_{r+1}$  matrices conmutativas en  $\mathbb{K}^{n+1}$  con  $d \nmid n+1$ . Como  $P(\mathbb{K}, d, 1)$  se cumple, entonces  $A_{r+1}$  tiene un autovalor  $\lambda$ , luego se define  $B := A_{r+1} - \lambda I$  y se definen

$$U := \ker(B), \quad W := \text{Im}(B),$$

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 cualquier autovector común de  $A_1, \dots, A_r$  lo es con  $A_{r+1}$ .

Si  $U \neq V$ , entonces como  $\dim W + \dim U = \dim V$  hay alguno que tiene dimensión no divisible por  $d$ , sin pérdida de generalidad supongamos que es  $U$ . Luego, por inducción,  $A_1, \dots, A_{r+1}$  tienen un autovector común en  $U \subseteq V$ .  $\square$

**Proposición 9.18:** 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  $B \in \text{Mat}_n(\mathbb{R})$  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.  $\square$

**Definición 9.19 – Matriz hermitiana:** Dada  $B \in \text{Mat}_n(\mathbb{C})$ , se denota por  $B^* := \overline{B}^t$ . Se dice que  $B$  es *hermitiana* (o *auto-adjunta* en algunos libros) si  $B = B^*$ .

**Corolario 9.19.1:** 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.  $\square$

**Lema 9.20:** Se cumple que  $P(\mathbb{C}, 2, 1)$ .

DEMOSTRACIÓN: Sea  $A \in \text{Mat}_n(\mathbb{C})$  con  $n$  impar. Sea  $V$  el  $\mathbb{R}$ -espacio vectorial de las matrices hermitianas de  $\text{Mat}_n(\mathbb{C})$ . Se definen los endomorfismos sobre  $V$ :

$$L_1(B) := \frac{AB + BA^*}{2}, \quad L_2(B) := \frac{AB - BA^*}{2i}.$$

Esta elección deriva de que

$$AB = \frac{AB + B^*A^*}{2} + i \cdot \frac{AB - B^*A^*}{2i},$$

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

$$AB = L_1(B) + iL_2(B) = (\mu + i\lambda)B,$$

osea  $B$  es autovector de  $A$  que es lo que se quería probar.  $\square$

**Teorema 9.21:** 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 algebraicamente cerrado.

DEMOSTRACIÓN: Lo probaremos por inducción fuerte sobre  $k$ , habiendo ya probado el caso base. Sea  $A \in \text{Mat}_n(\mathbb{C})$  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.,  $B \in V$  si y sólo si  $B^t = -B$ ). Se definen los endomorfismos sobre  $V$ :

$$L_1(B) := AB - BA^t, \quad L_2(B) := ABA^t$$

que conmutan (¡ demuéstrela!). 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  $\mathbf{v}$  de  $B$  se tiene que

$$(A^2 - \lambda A + \mu I)\mathbf{v} = 0.$$

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:

$$(A - \alpha I)(A - \beta I)\mathbf{v} = 0$$

Luego o  $(A - \beta I)v = 0$  con lo que  $v$  es autovector de  $A$ , o  $(A - \alpha I)v$  es autovector de  $A$ .  $\square$

**§9.1.2 Teorema de Cayley-Hamilton.** Si  $A$  es un dominio, entonces hemos probado que  $A[x]$  también lo es. Usando esto realizaremos comparaciones entre dos tipos de espacios curiosos:  $\text{Mat}_n(A[x])$ , es decir, el conjunto de matrices del anillo  $A[x]$  de los polinomios de  $A$ ; y  $(\text{Mat}_n A)[x]$ , es decir, el conjunto de polinomios con coeficientes matrices de  $A$ .

Por ejemplo, un elemento de  $\text{Mat}_2(\mathbb{Z}[x])$  podría ser

$$\begin{bmatrix} x^2 + 1 & 3x \\ x^3 - 2x & 0 \end{bmatrix}$$

y un elemento de  $(\text{Mat}_2 \mathbb{Z})[x]$  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  $F \in \text{Mat}_n(A[x])$  entonces convenimos que  $[r_p(F)]_{i,j} := r_p(F_{i,j})$  (en general denotaremos elementos de  $\text{Mat}_n(A[x])$  con letras mayúsculas).

**Proposición 9.22:** Sean  $F, G \in \text{Mat}_n(A[x])$ , 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 algebraica:

$$(r_p(F \cdot G))_{ij} = r_p((F \cdot G)_{ij}) = r_p\left(\sum_{k=1}^n F_{ik}G_{kj}\right)$$

$$\begin{aligned}
&= \sum_{k=1}^n r_p(F_{ik}G_{kj}) = \sum_{k=1}^n \sum_{\ell=0}^p r_\ell(F_{ik})r_{p-\ell}(G_{kj}) \\
&= \sum_{\ell=0}^p \sum_{k=1}^n [r_\ell(F)]_{ik} [r_{p-\ell}(G)]_{kj} = \sum_{\ell=0}^p r_\ell(F)r_{p-\ell}(G).
\end{aligned}$$

□

**Teorema 9.23:**

$$\text{Mat}_n(A[x]) \cong (\text{Mat}_n A)[x]$$

**Teorema 9.24 – 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  $\varphi : \text{Mat}_n(A[x]) \rightarrow (\text{Mat}_n A)[x]$  el isomorfismo canónico. Sabemos que se define

$$p_B(x) := \det(xI - B),$$

y que

$$(\text{adj } B)B = \det(B)I$$

de modo que

$$\text{adj}(xI - B)(xI - B) = p_B(x)I$$

notemos que ésta es una relación sobre  $\text{Mat}_n(A[x])$  (pues la matriz a la derecha tiene por coordenadas polinomios), luego por el teorema anterior se cumple que se traduce a  $(\text{Mat}_n A)[X]$ :

$$\text{adj}(X - B)(X - B) = p_B(X),$$

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  $\mathbb{k}$ -espacio vectorial  $V$ , entonces  $V^* := L(V, \mathbb{k})$  es el espacio formado por funcionales lineales desde  $V$ .

Ésta demostración es de [0].

**Proposición 9.25:** Se cumple:

1. Si  $\dim V < \infty$  entonces  $\dim V = \dim V^*$ .
2. Existe un monomorfismo canónico  $\iota : V \rightarrow V^*$  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  $\{e_i\}_{i \in I}$  es base de  $V$ , de modo que  $\dim V = |I|$ . Para construir el monomorfismo, definimos  $\iota(e_i)$  como el funcional tal que  $[\iota(e_i)](e_j) = \delta_{ij}$ . Luego al extender linealmente a  $\iota$  le definimos sobre todo  $V$  y vemos que la imagen sobre la base genera un conjunto linealmente independiente en  $V^*$ . Claramente  $\iota$  es inyectiva y prueba que  $\dim V \leq \dim V^*$  en todo caso.

Para probar la tercera probaremos varios pasos:

1. **Si  $\aleph \leq \aleph_0$ , 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  $\aleph \times I$ , por lo que,

$$|V| \leq |S| = |\aleph \times I|^{<\aleph_0} = |\aleph| \cdot |\aleph \times I| = |I|.$$

2. **Si  $\aleph \leq \aleph_0$ , entonces  $\dim V < \dim V^*$ :**  
Simple: como toda función lineal viene determinada exclusivamente por los valores en la base, se cumple que

$$|V| = |\text{Func}(I; \aleph)| = |\aleph|^{|I|} \geq 2^{|I|} > |I| = \dim V$$

donde la última desigualdad es el teorema de cardinalidad de Cantor.

3. **Caso arbitrario:**

Notemos que  $\aleph$ , por ser un cuerpo, siempre contiene a otro cuerpo

$$F := \begin{cases} \mathbb{Q}, & \text{car } \aleph = 0 \\ \mathbb{F}_p, & \text{car } \aleph = p \end{cases}$$

Luego si  $W := \text{Span}_F(e_i)_{i \in I}$  vemos que  $\dim_F W = \dim_{\aleph} V$ , y sabemos que  $\dim_F W < \dim_{\aleph} W^*$ , así que basta probar que  $\dim_F W^* \leq \dim_{\aleph} V^*$ .

Sea  $G \in L_F(W^*, V^*)$  definida así: Sea  $\varphi \in W^*$ , es decir,  $\varphi : W \rightarrow F$  es  $F$ -lineal y queremos que  $G(\varphi) : V \rightarrow \aleph$  sea  $\aleph$ -lineal. Sea  $v \in V$ , existe

$(\lambda_i)_{i \in I} \in \mathbb{k}$  tal que es nula excepto en finitos índices y  $\mathbf{v} = \sum_{i \in I} \lambda_i \mathbf{e}_i$ . Luego se define

$$[G(\varphi)](\mathbf{v}) = \sum_{i \in I} \lambda_i \varphi(\mathbf{e}_i)$$

el cual está bien definido y veamos que todo cumple las condiciones esperadas, dados

$$\mathbf{u} = \sum_{i \in I} \alpha_i \mathbf{e}_i, \quad \mathbf{v} = \sum_{i \in I} \beta_i \mathbf{e}_i$$

y dados  $\lambda \in \mathbb{k}$  se cumple

a) Fijada  $\varphi \in W^*$  vemos que

$$\begin{aligned} [G(\varphi)](\mathbf{u} + \mathbf{v}) &= \sum_{i \in I} (\alpha_i + \beta_i) \varphi(\mathbf{e}_i) \\ &= \sum_{i \in I} \alpha_i \varphi(\mathbf{e}_i) + \sum_{i \in I} \beta_i \varphi(\mathbf{e}_i) = [G(\varphi)](\mathbf{u}) + [G(\varphi)](\mathbf{v}). \end{aligned}$$

Y claramente  $[G(\varphi)](\lambda \mathbf{v}) = \lambda [G(\varphi)](\mathbf{v})$  de modo que  $G(\varphi)$  efectivamente es un elemento de  $V^*$ .

- b)  $G$  es efectivamente una aplicación  $F$ -lineal (¿por qué?).  
 c) Si  $\mathbf{u} \in W$ , entonces  $\alpha_i \in F$  y se cumple que

$$\varphi(\mathbf{u}) = \varphi \left( \sum_{i \in I} \alpha_i \mathbf{e}_i \right) = \sum_{i \in I} \alpha_i \varphi(\mathbf{e}_i) = [G(\varphi)](\mathbf{u})$$

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 9.26 – Forma bilineal:** Una forma bilineal  $F \in L(V, V; \mathbb{k})$  es una forma multilinear de  $V \times V$  a  $\mathbb{k}$ , donde  $V$  es un  $\mathbb{k}$ -espacio vectorial. En general también exigiremos que  $F$  sea simétrica, es decir, que  $F(\mathbf{u}, \mathbf{v}) = F(\mathbf{v}, \mathbf{u})$  para todo  $\mathbf{u}, \mathbf{v} \in V$ .

Si  $\mathbf{u}, \mathbf{v}$  cumplen que  $F(\mathbf{u}, \mathbf{v}) = 0$  para una forma bilineal simétrica, entonces diremos que son *ortogonales* respecto a  $F$ , lo que denotaremos por  $\mathbf{u} \perp \mathbf{v}$ .

Sea  $B := (\mathbf{x}_1, \dots, \mathbf{x}_n)$  una base de  $V$ , entonces se le llama representación matricial de la forma bilineal  $F$  según  $B$  a

$$M_B(F) := [F(\mathbf{x}_i, \mathbf{x}_j)]_{ij}$$

Si  $F$  es una forma bilineal simétrica, decimos que  $q : V \rightarrow \mathbb{k}$  definido por  $q(\mathbf{v}) := F(\mathbf{v}, \mathbf{v})$  es su *forma cuadrática* asociada.

**Proposición 9.27:** Dada una forma bilineal  $F$  sobre  $\mathbb{k}^n$  con base ordenada  $B$ , se cumple que una matriz  $M = M_B(F)$  syss para todo  $\mathbf{u}, \mathbf{v} \in \mathbb{k}^n$  se cumple que

$$F(\mathbf{u}, \mathbf{v}) = \pi_B(\mathbf{u})M\pi_B(\mathbf{v})^t.$$

Luego si denotamos  $(\mathbf{u}, \mathbf{v}) := \pi_B(\mathbf{u})\pi_B(\mathbf{v})^t$  para alguna base fijada, como la canónica, entonces toda forma bilineal  $F$  corresponde a

$$F(\mathbf{u}, \mathbf{v}) = (\mathbf{u}A, \mathbf{v}) = (\mathbf{u}, \mathbf{v}A^t)$$

con una matriz  $A$ .

**Proposición 9.28:** Si  $F$  es una forma bilineal simétrica, entonces su representación matricial bajo cualquier base también lo es.

**Teorema 9.29:** Si  $V$  es un  $\mathbb{k}$ -espacio vectorial con  $\text{car } \mathbb{k} \neq 2$  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  $\mathbf{u}, \mathbf{v}$  tales que  $F(\mathbf{u}, \mathbf{v}) \neq 0$ , luego si  $q$  es su forma cuadrática, entonces

$$q(\mathbf{u} + \mathbf{v}) = q(\mathbf{u}) + 2F(\mathbf{u}, \mathbf{v}) + q(\mathbf{v})$$



de modo que  $q$  es no nulo para al menos alguno entre  $\mathbf{u}, \mathbf{v}, \mathbf{u} + \mathbf{v}$ ; sea  $\mathbf{e}_1$  alguno de ellos. Sea

$$W := \{\mathbf{x} \in V : \mathbf{x} \perp \mathbf{e}_1\}.$$

Vamos a probar que  $V = \text{Span}(\mathbf{e}_1) \oplus W$ : Sea  $\mathbf{x} \in \text{Span}(\mathbf{e}_1) \cap W$ , entonces  $\mathbf{x} = \alpha \mathbf{e}_1 \perp \mathbf{e}_1$  satisface que  $F(\mathbf{x}, \mathbf{e}_1) = 0 = \alpha F(\mathbf{e}_1, \mathbf{e}_1)$  de modo que  $\alpha = 0$  y  $\mathbf{x} = \vec{0}$ .

Notemos que  $\mathbf{x} \mapsto F(\mathbf{x}, \mathbf{e}_1)$  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  $\dim(\text{Span}(\mathbf{e}_1) \oplus W) = n$  y se comprueba nuestra hipótesis.

Finalmente como  $W$  tiene dimensión menor, por hipótesis inductiva, posee base ortogonal  $\mathbf{e}_2, \dots, \mathbf{e}_n$  y añadirle  $\mathbf{e}_1$  genera una base ortogonal para  $V$ .  $\square$

Supongamos que sea  $(\mathbf{e}_i)_i$  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

$$F(\mathbf{u}, \mathbf{v}) = (\mathbf{u}A, \mathbf{v}) = ((\mathbf{u}M)B, \mathbf{v}M) = (\mathbf{u}(MBM^t), \mathbf{v})$$

De modo que  $A = MBM^t$ .

**Definición 9.30:** Se dice que dos matrices  $A, B$  son *congruentes* si existe  $M$  invertible tal que  $A = MBM^t$ .

Por ende hemos probado:

**Teorema 9.31:** 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  $(\mathbf{x}_i)_i$ , entonces si  $B$  es la representación diagonal de  $F$  por el teorema anterior,  $B$  tiene por diagonal  $\alpha_i^2 \lambda_i$  donde  $\lambda_i := F(\mathbf{x}_i, \mathbf{x}_i)$  y  $\alpha_i$  es un escalar que multiplicamos por  $\mathbf{x}_i$  a conveniencia, luego es claro que:

**Teorema 9.32:** Si  $\text{car } \mathbb{k} \neq 2$  y todo elemento de  $\mathbb{k}$  posee raíz cuadrada, entonces toda matriz simétrica es congruente a una única matriz  $\underbrace{[1, \dots, 1]_r, 0, \dots, 0}$ .

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 9.33:** Si  $\text{car } \mathbb{K} \neq 2$ , 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 9.34:** Dada una forma cuadrática  $q$  sobre  $V$ , se dice que posee alguna de las siguientes propiedades si para todo  $v \in V$ :

**Definida positiva** Si  $x \neq 0$  implica  $q(x) > 0$ .

**Semidefinida positiva** Si  $q(x) \geq 0$ .

**Definida negativa** Si  $x \neq 0$  implica  $q(x) < 0$ .

**Semidefinida negativa** Si  $q(x) \leq 0$ .

### §9.3.2 Formas sesquilineales, producto interno y “geometría euclídea”.

**Definición 9.35 – Forma sesquilineal:** Sea  $H$  un  $\mathbb{K}$ -espacio vectorial, se dice que  $F : H^2 \rightarrow \mathbb{K}$  es una forma sesquilineal 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.  $F(\alpha u, v) = \alpha F(u, v)$ .

Las mismas nociones de representación matricial y formas cuadráticas (ahora llamadas *hermitianas*) aplica.

**Proposición 9.36:** Si  $F$  es una forma sesquilineal, entonces para todo  $u, v \in \mathbb{K}^n$  y todo  $\alpha \in \mathbb{K}$  se cumple:

1.  $F(u, \alpha v) = \bar{\alpha} F(u, v)$ .
2.  $F(u, u) \in \mathbb{R}$ .

El resultado anterior permite conservar las definiciones para forma cuadrática en  $\mathbb{R}$  y nos permite ver un análogo para la representación matricial:

**Teorema 9.37:** Dada una forma sesquilineal  $F$  sobre  $\mathbb{K}^n$  con base ordenada  $B$ , se cumple que una matriz  $A := M_B(F)$  syss para todo  $\mathbf{u}, \mathbf{v} \in \mathbb{K}^n$  se cumple que

$$F(\mathbf{u}, \mathbf{v}) = \pi_B(\mathbf{u})A\pi_B(\mathbf{v})^*$$

Luego si denotamos  $(\mathbf{u}, \mathbf{v}) := \pi_B(\mathbf{u})\pi_B(\mathbf{v})^*$ , entonces toda forma sesquilineal corresponde a

$$F(\mathbf{u}, \mathbf{v}) = (\mathbf{u}A, \mathbf{v}) = (\mathbf{u}, \mathbf{v}A^*).$$

**Definición 9.38 – Producto interno:** Se dice que una forma sesquilineal  $(, ) : H^2 \rightarrow \mathbb{K}$  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  $\| \cdot \| : H \rightarrow [0, \infty)$  a la aplicación

$$\| \mathbf{x} \| := \sqrt{(\mathbf{x}, \mathbf{x})},$$

que ésta bien definida y sólo toma 0 en el  $\vec{0}$ .

### §9.3.3 Formas hermitianas y espacios de producto interno.

**Definición 9.39 – Forma hermitiana:** Sea  $H$  un  $\mathbb{K}$ -espacio vectorial, se dice que  $f : H^2 \rightarrow \mathbb{K}$  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  $\langle , \rangle : H^2 \rightarrow \mathbb{K}$  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 denotará un espacio prehilbertiano.

**Proposición 9.40:** Si  $f$  es una forma hermitiana sobre  $H$ , entonces, para todo  $u, v \in H$  y  $\alpha \in \mathbb{K}$ :

1.  $f(u, \alpha v) = \bar{\alpha} f(u, v)$ .
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.  $\square$

**Lema 9.41:** 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 9.41.1:** 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 9.41.2:** Sean  $A, B \in \text{End}(H)$ . 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.,  $A = B$ .  $\square$

**Teorema 9.42 – 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

$$\begin{aligned} 0 &\leq \langle x - \alpha y, x - \alpha y \rangle = \langle x, x \rangle - \alpha \langle y, x \rangle - \bar{\alpha} \langle x, y \rangle + |\alpha|^2 \langle y, y \rangle \\ &= \|x\|^2 - 2 \operatorname{Re}(\alpha \langle y, x \rangle) + |\alpha|^2 \|y\|^2. \end{aligned}$$

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.  $\square$

**Teorema 9.43 (Desigualdad traingular):** Para todo  $x, y \in H$  se cumple que

$$\|x + y\| \leq \|x\| + \|y\|,$$

luego,  $\|\cdot\| : H \rightarrow \mathbb{R}$  es una norma.

DEMOSTRACIÓN: Basta aplicar el siguiente procedimiento:

$$\begin{aligned} \|x + y\|^2 &= \langle x + y, x + y \rangle \\ &= \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle \\ &= \|x\|^2 + 2 \operatorname{Re}(\langle x, y \rangle) + \|y\|^2 \\ &\leq \|x\|^2 + 2|\langle x, y \rangle| + \|y\|^2 \\ &\leq \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2. \end{aligned}$$

$\square$

Llamaremos *unitarios* a los vectores de norma 1.

**Definición 9.44 – 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 9.45:** 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

$$\begin{aligned} \left\langle x_k, x - \sum_{i=1}^n \alpha_i x_i \right\rangle &= \langle x_k, x \rangle - \sum_{i=1}^n \langle x_k, \alpha_i x_i \rangle \\ &= \langle x_k, x \rangle - \overline{\alpha_k} \langle x_k, x_k \rangle \stackrel{1}{=} 0. \end{aligned}$$

□

**Teorema 9.46 – 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  $k > 0$ :

$$\text{Span}\{x_1, \dots, x_k\} = \text{Span}\{y_1, \dots, y_k\}$$

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  $\text{Span}(x_1, x_2) = \text{Span}(y_1, y_2)$ , 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 9.47:** 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  $\pi_E : H \rightarrow E$  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  $\pi_E$  lo que hace es anular los coeficientes de  $\{x_i\}_i$  que no están en  $\{y_i\}_i$ .  $\square$

**¿Y cómo se ve el producto interno?** Sea  $\{x_i\}$  una base ortonormal de  $H$  y sean  $u, v \in H$ . Por definición de base existen unas sucesiones de escalares  $(\alpha_i)_i$  y  $(\beta_i)_i$  tales que

$$u = \sum_{i=1} \alpha_i x_i, \quad v = \sum_{i=1} \beta_i x_i$$

luego

$$\begin{aligned} \langle u, v \rangle &= \left\langle \sum_{i=1} \alpha_i x_i, v \right\rangle = \sum_{i=1} \alpha_i \langle x_i, v \rangle \\ &= \sum_{i=1} \alpha_i \left\langle x_i, \sum_{j=1} \beta_j x_j \right\rangle = \sum_{i=1} \alpha_i \sum_{j=1} \bar{\beta}_j \langle x_i, x_j \rangle \\ &= \sum_{i=1} \alpha_i \sum_{j=1} \bar{\beta}_j \delta_{ij} = \sum_{i=1} \alpha_i \bar{\beta}_i. \end{aligned}$$

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

$$\langle (u_1, \dots, u_n), (v_1, \dots, v_n) \rangle = \sum_{i=1}^n u_i \bar{v}_i.$$

Es más, si identificamos  $H := \text{Mat}_{n \times 1}(\mathbb{C})$ , entonces tenemos que para todo  $\mathbf{u}, \mathbf{v} \in H$  se cumple que

$$\langle \mathbf{u}, \mathbf{v} \rangle = \overline{\mathbf{v}}^t \mathbf{u}.$$

**Corolario 9.47.1 (Desigualdad de Bessel):** Sea  $\{x_i\}$  una sucesión<sup>1</sup> 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.  $\square$

**Teorema 9.48:** Sea  $\{x_i\}_{i=0}^n$  una sucesión finita ortonormal y  $x \in H$ . Entonces, los escalares  $\lambda_i \in \mathbb{k}$  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.  $\square$

<sup>1</sup> Aquí se obvian los límites de los índices pues el resultado es válido tanto para sucesiones finitas como infinitas.



**Corolario 9.48.1:** 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 9.49 (Identidad de Parseval):** Una sucesión ortonormal  $\{x_i\}$  es base de  $H$  syss para todo  $x \in H$  se cumple

$$\|x\|^2 = \sum_i |\langle x, x_i \rangle|^2.$$

### §9.3.4 Formas cuadráticas.

**Definición 9.50 – Formas bilineales y cuadráticas:** Sea  $V$  un  $\mathbb{k}$ -espacio vectorial. Se dice que  $F : V^2 \rightarrow \mathbb{k}$  es una *forma bilineal* si para todo  $u, v, w \in V$  y todo  $\alpha, \beta \in \mathbb{k}$  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  $q : V \rightarrow \mathbb{k}$  es  $q(v) := F(v, v).$

**Proposición 9.51:** 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  $\beta: B \times B \rightarrow B$ , 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  $b \in B$ .<sup>a</sup> 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  $\varphi: B \rightarrow C$  de modo que  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$  y que  $\varphi(1_B) = 1_C$ .

---

<sup>a</sup>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  $\text{Alg}_A$ . La subcategoría de  $A$ -álgebras conmutativas se denota  $\text{CAlg}_A$ .

Nótese que las  $A$ -álgebras asociativas pueden verse como anillos que en

cierta forma incluyen a  $A$ . En particular, el producto escalar  $A \times B \rightarrow B$  es una aplicación bilineal y, por ende, induce un homomorfismo de  $A$ -módulos  $A \otimes_A B \rightarrow B$ . Luego, la condición de ser un  $A$ -bimódulo puede entenderse como exigir que el siguiente diagrama conmute:

$$\begin{array}{ccccc}
 & & B \otimes B & & \\
 \varepsilon \otimes \text{Id}_B \nearrow & & \downarrow \beta & \nwarrow \text{Id}_B \otimes \varepsilon & \\
 A \otimes_A B & & & & B \otimes_A A \\
 & \searrow & & \swarrow & \\
 & & B & & 
 \end{array}$$

Mientras que la asociatividad puede entenderse como exigir que el siguiente diagrama conmute:

$$\begin{array}{ccc}
 B \otimes B \otimes B & \xrightarrow{1_B \otimes \beta} & B \otimes B \\
 \beta \otimes 1_B \downarrow & & \downarrow \beta \\
 B \otimes B & \xrightarrow{\beta} & B
 \end{array}$$

**Ejemplo.** Sea  $A$  un dominio.

1. Sea  $G = \{g_1, \dots, g_n\}$  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,<sup>1</sup> entonces también podemos definir  $A[G]$  exactamente del mismo modo, exigiendo que las sumas formales sean finitas,

<sup>1</sup>Si trabajáramos con álgebras no-unitarias, entonces también podríamos 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.

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  $B$ .

**Lema 10.4:** La intersección arbitraria de subálgebras es también una subálgebra.

**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  $S$ .

**Proposición 10.6:** Sea  $B$  una  $A$ -álgebra y sea  $S \subseteq B$  un subconjunto. Entonces:

$$A[S] = \left\{ \sum_{i=1}^n s_i t_i : s_i, t_i \in S \cup A \right\}.$$

**Proposición 10.7:** La unión de una cadena de subálgebras es también una subálgebra.

**Proposición 10.8:** Sean  $B, C$  un par de  $A$ -álgebras y  $\varphi: B \rightarrow C$  un homomorfismo de  $A$ -álgebras. Entonces  $\ker \varphi$  es un ideal de  $B$  e  $\text{Im} \varphi$  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**<sup>a</sup> si posee un sistema generador finito.

<sup>a</sup>MATSUMURA [0] emplea *álgebra finitamente generada*, mientras que ALUFFI [0] sugiere *álgebra de tipo finito*.

**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  $f: X \rightarrow C$  posee una única extensión  $\bar{f}: B \rightarrow C$  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 si y sólo si es un sistema generador libre.

DEMOSTRACIÓN:  $\Leftarrow$ . 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  $f: X \rightarrow C$  es fácil ver que se extiende a una única función  $f^*: P \rightarrow C$  por multiplicación, la cual a su vez se extiende a un único homomorfismo  $\bar{f}: B \rightarrow C$  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.

$\implies$ . Denotemos por  $F := A\langle X \rangle$  al álgebra construida en la parte anterior de la demostración, la cual hemos probado que es libre. Considere la inclusión  $\iota_B: X \rightarrow F$ , por hipótesis se extiende a un único homomorfismo de  $A$ -álgebras  $f: B \rightarrow F$ . Así mismo, la inclusión  $\iota_F: X \rightarrow B$  se extiende a un único homomorfismo de  $A$ -álgebras  $g: F \rightarrow B$ . Luego  $f \circ g: B \rightarrow B$  es un endomorfismo de  $A$ -álgebras que fija a la base, por lo que debe ser la identidad y análogamente con  $g \circ f$ .  $\square$

**Corolario 10.12.1:** 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 10.13:** 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  $f: X \rightarrow C$  posee una única extensión  $\bar{f}: B \rightarrow C$  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 10.14:** 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 10.15 (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 [0, p. 405] le llama a éste resultado el «Nullstellensatz fuerte»; sin embargo, dicho nombre lo reservamos para [0, Teo. 1.14]. 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  $\mathbf{a}$ . Para ver que  $L$  es una extensión finita, basta ver que cada uno de los elementos es algebraico. Para ello sea  $\text{ev}_{\mathbf{a}}: k[x_1, \dots, x_m] \rightarrow L$  el morfismo suprayectiva, entonces viene generado, como  $k$ -espacio vectorial, por todos los monomios de  $k[x_1, \dots, x_m]$  evaluados en  $\mathbf{a}$  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

$$\frac{\lambda_1}{\alpha - \beta_1} + \dots + \frac{\lambda_n}{\alpha - \beta_n} = \frac{p(\alpha)}{q(\alpha)} = 0$$

para algunos  $\lambda_i$  no nulos. Sustituyendo  $\alpha$  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  $\alpha$ , así que  $p(\alpha) = 0$ .

Ésto prueba que  $L$  es algebraico, y como viene generado por finitos elementos, es una extensión finita.  $\square$

Damos otra demostración en la proposición ?? y el corolario ??.

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 10.16 – Teorema débil de ceros de Hilbert:** Si  $k$  es algebraicamente cerrado, entonces un ideal  $\mathfrak{a} \triangleleft k[x_1, \dots, x_n]$  es maximal si y sólo si  $\mathfrak{a} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$  con  $\alpha_i \in k$ .

DEMOSTRACIÓN: Nótese que  $k[x_1, \dots, x_n]/(x_1 - \alpha_1, \dots, x_n - \alpha_n) \cong k$  que es un cuerpo, así que  $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$  es un ideal maximal.

Conversamente sea  $\mathfrak{m} \triangleleft k[x_1, \dots, x_n]$  un ideal maximal, luego se induce un monomorfismo natural  $k \rightarrow k[x_1, \dots, x_n]/\mathfrak{m} =: L$ , 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  $\pi: k[x_1, \dots, x_n] \rightarrow k$  es un epimorfismo de anillos con  $\mathfrak{m} = \ker \pi$ . Definiendo  $\alpha_i := \pi(x_i)$  se cumple que

$$(x_1 - \alpha_1, \dots, x_n - \alpha_n) \subseteq \mathfrak{m} \neq k[x_1, \dots, x_n]$$

y por maximalidad de  $\mathfrak{m}$  se alcanza la igualdad.  $\square$

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 pizarrón y anotó en mayúsculas el nombre de RABINOWITSCH y comenzó a borrar una por una letras hasta quedar RA IN I CH.

## 10.2 Álgebras asociativas

### §10.2.1 Anillos, módulos y álgebras graduadas.

**Definición 10.17:** Una  $A$ -álgebra  $B$  se dice *graduada* por  $B = \bigoplus_{d \in \mathbb{Z}} B_d$  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 (o un ideal)  $C \subseteq B$  se dice *homogéneo* si  $C = \bigoplus_{d \in \mathbb{N}} (C \cap B_d)$ . 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 10.18:** 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,  $1 = e_0$ .  $\square$

**Teorema 10.19:** Sea  $B$  una  $A$ -álgebra graduada. Una subálgebra  $C \subseteq B$  es homogénea syss está generada por un conjunto de elementos homogéneos.

DEMOSTRACIÓN:  $\implies$ . Si  $C$  es homogénea entonces está generada por  $\bigcup_{d \in \mathbb{Z}} C \cap B_d$ .

$\Leftarrow$ . Sea  $T \subseteq B$  tal que sus elementos son homogéneos y sea  $C := B[T]$ . Luego, sea  $f \in C$ , por definición

$$f = g_1 f_1 + \cdots g_n f_n$$

donde  $f_i \in T$  y  $g_i \in B$ . Como  $B$  es graduada, 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  $\lambda_{ji} \in B_0$ . 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,  $f \in \bigoplus_{d \in \mathbb{Z}} (C \cap B_d)$ . La otra inclusión es trivial.  $\square$

**Definición 10.20:** Sean  $B, C$  un par de  $A$ -álgebras graduadas. Se dice que  $\varphi: B \rightarrow C$  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  $d$ . Un **homomorfismo de álgebras graduadas** es una función lineal homogénea de grado 0.

**Lema 10.21:** Sean  $B, C$  un par de  $A$ -álgebras graduadas. Supongamos que  $\{\lambda_g: B \rightarrow C\}_{g \in \mathbb{N}}$  es una familia de funciones lineales homogéneas que tiene las siguientes propiedades:

1. Cada  $\lambda_g$  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  $\lambda_g$ 's son idénticamente nulas.

**Definición 10.22:** Dado un anillo graduado  $A$  como antes, 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  $\varphi: M \rightarrow N$  es un *homomorfismo de  $A$ -módulos graduados* si es un homomorfismo de  $A$ -módulos y  $\varphi[M_n] \subseteq N_n$ .

Sea  $A$  un anillo graduado y  $M$  un  $A$ -módulo graduado. Sea  $f \in A$  homogéneo. Entonces, la localización  $M[1/f]$  está graduada por  $\deg(g/f^n) := \deg g - n \deg f$ .

**Definición 10.23:** Sea  $A$  un anillo graduado,  $M$  un  $A$ -módulo graduado y  $S \subseteq A$  un sistema multiplicativo. Denotamos por  $M_{(S)}$  al submódulo  $S^{-1}M$  que consiste en los elementos homogéneos de grado 0. Si  $\mathfrak{p} \triangleleft A$  es un ideal primo, entonces  $M_{(\mathfrak{p})}$  naturalmente corresponde a los elementos homogéneos de grado 0 de  $M_{\mathfrak{p}}$ .

**Proposición 10.24:** Sea  $A$  un dominio graduado y sea  $\mathfrak{p} \triangleleft A$  un ideal primo.

1.  $A_{(\mathfrak{p})}$  es un anillo local con ideal maximal  $\mathfrak{p}^e := \mathfrak{p}_{(\mathfrak{p})}$ .
2. Si  $A$  es un dominio íntegro y  $\mathfrak{p} = (0)$ , entonces  $A_{(\mathfrak{p})}$  es un subcuerpo de  $\text{Frac}(A)$ .

**Proposición 10.25:** Sea  $A$  un anillo graduado y sean  $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$  homogéneos. Entonces:

1.  $A/\mathfrak{a} = \bigoplus_{d \in \mathbb{Z}} A_d/\mathfrak{a}$ . En consecuencia,  $A/\mathfrak{a}$  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.  $\mathfrak{a} + \mathfrak{b}, \mathfrak{a} \cdot \mathfrak{b}, \mathfrak{a} \cap \mathfrak{b}, (\mathfrak{a} : \mathfrak{b})$  son homogéneos.
4.  $\text{Rad}(\mathfrak{a})$  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 « $\implies$ », 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 pérdida 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  $\mathfrak{p} \leq R$  primo, entonces existe  $\mathfrak{a} \subseteq \mathfrak{p}_h \subseteq \mathfrak{p}$ , donde  $\mathfrak{p}_h$  es primo y homogéneo. Para ello definamos

$$\mathfrak{p}_h := (\{f \in \mathfrak{p} : f \text{ homogéneo}\}),$$

por el inciso anterior se concluye que  $\mathfrak{p}_h$  es primo y claramente  $\mathfrak{a} \subseteq \mathfrak{p}_h$ . Luego, hemos probado que

$$\text{Rad}(\mathfrak{a}) = \bigcap \{\mathfrak{p} : \mathfrak{a} \subseteq \mathfrak{p} \trianglelefteq R \text{ primo y homogéneo}\}$$

de modo que  $\text{Rad}(\mathfrak{a})$  es homogéneo por el inciso anterior.  $\square$

Hay otra demostración de que  $\text{Rad}(\mathfrak{a})$  que no emplea AE (y por ende, no emplea el teorema 6.25), queda al lector proponerla.

**Proposición 10.26:** Sea  $A$  un dominio graduado. 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  $A^+ \triangleleft A$ , entonces  $A^+ = (\alpha_1, \dots, \alpha_s)$  con  $\alpha_i$  homogéneo de grado  $k_i > 0$  y sea  $A' := A_0[\alpha_1, \dots, \alpha_s]$ . 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  $\lambda_i$  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.  $\square$

### §10.2.2 Productos tensoriales y ejemplos de álgebras.

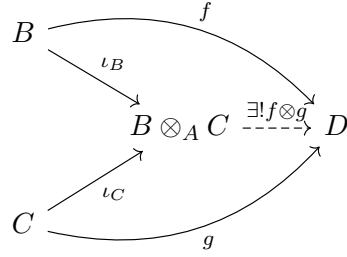
**Definición 10.27:** Sean  $B, C$  un par de  $A$ -álgebras. Considere  $T := B \otimes_A C$  como  $A$ -módulos y definamos un producto en  $T$  que, en los tensores puros, corresponde a

$$(b_1 \otimes c_1) \cdot (b_2 \otimes c_2) = b_1 b_2 \otimes c_1 c_2,$$

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 10.28:** Sean  $B, C, D$  un trío de  $A$ -álgebras, y sean  $f: B \rightarrow D$  y  $g: C \rightarrow D$  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  $(f \otimes g): B \otimes_A C \rightarrow D$  tal que el siguiente diagrama conmuta (en  $\text{Alg}_A$ ):



**Teorema 10.29:** Sean  $B, C$  un par de  $A$ -álgebras conmutativas. Entonces  $B \otimes_A C$  corresponde con el coproducto en la categoría  $\mathbf{CAlg}_A$ .

**Proposición 10.30:** Sean  $\{x_i\}_{i \in I}, \{y_j\}_{j \in J}$  dos conjuntos disjuntos de indeterminadas, entonces

$$A[\{x_i\}_{i \in I}] \otimes_A A[\{y_j\}_{j \in J}] = A[\{x_i, y_j : i \in I, j \in J\}].$$

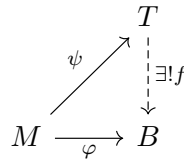
**Ejemplo.** Nótese que  $A[x] \otimes_A A[y] = A[x, y]$  y que  $A[x] = A\langle x \rangle$ , pero que el coproducto en  $\mathbf{Alg}_A$  es

$$A[x] \amalg A[y] = A\langle x \rangle \amalg A\langle y \rangle = A\langle x, y \rangle \not\cong A[x, y].$$

**Definición 10.31:** Sea  $M$  un  $A$ -módulo. Un par  $(T, \psi)$  se dice una **álgebra tensorial** sobre  $M$  si:

AT1.  $T$  es una  $A$ -álgebra y  $\psi: M \rightarrow T$  es un homomorfismo de  $A$ -módulos.

AT2. Si  $\varphi: M \rightarrow B$  es un homomorfismo de  $A$ -módulos, donde  $B$  es una  $A$ -álgebra, entonces existe un único homomorfismo de  $A$ -álgebras  $f: T \rightarrow B$  tal que el siguiente diagrama conmuta:



En resumen  $T(M)$  es un objeto representado por el funtor

$$\mathrm{Hom}_{\mathbf{Mod}_A}(M, -): \mathbf{Alg}_A \rightarrow \mathbf{Set}.$$

**Teorema 10.32:** Dado un  $A$ -módulo  $M$  existe una álgebra tensorial sobre  $M$ , denotada  $T_A(M)$ . 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  $T_A(M)$  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:

$$x \dot{+} y \dot{-} (x + y), \quad \alpha \cdot x \dot{-} (\alpha x).$$

Y definimos  $T_A(M) := F/\mathfrak{a}$ . Construimos el morfismo  $\psi: M \rightarrow T$  dado por composición de inclusión de los elementos en  $F$  y la proyección.

Sea  $\varphi: M \rightarrow B$  un homomorfismo de  $A$ -módulos, donde  $B$  es una  $A$ -álgebra. Por definición de base, se extiende a un único homomorfismo de  $A$ -álgebras  $\bar{\varphi}: F \rightarrow B$ . Luego, nótese que  $\bar{\varphi}$  se anula en  $\mathfrak{a}$ , en particular lo hace sobre sus generadores:

$$\begin{aligned} \bar{\varphi}(x \dot{+} y \dot{-} (x + y)) &= \bar{\varphi}(x) + \bar{\varphi}(y) - \bar{\varphi}(x + y) \\ &= \varphi(x) + \varphi(y) - \varphi(x + y) = 0, \end{aligned}$$

donde empleamos el hecho de que  $\varphi$  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:

$$\begin{array}{ccc} & T_A(M) & \\ \psi \uparrow \pi & \nearrow f & \\ F & \xrightarrow{\bar{\varphi}} & B \\ \downarrow \iota & \searrow \varphi & \\ M & \xrightarrow{\varphi} & B \end{array}$$

□

**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

$$\mathrm{Hom}_{\mathrm{Alg}}(C, B) \approx \mathrm{Hom}_{\mathrm{Mod}}(A, B) \approx \mathrm{Func}(\{1\}, B),$$

donde  $\approx$  denota equipotencia. Pero  $\mathrm{Func}(\{1\}, B) \approx \mathrm{Hom}_{\mathrm{Alg}}(A[x], B)$  pues  $A[x]$  es la  $A$ -álgebra libre con un generador.



Extrapolando el mismo ejercicio se obtiene:

**Proposición 10.33:** 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  $T_A(A^{\oplus S}) = A\langle S \rangle$ .

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 10.34:** Sea  $M, N$  un par de  $A$ -módulos, y sea  $\beta: M^d = \prod_{i=1}^d M \rightarrow N$  un aplicación  $d$ -multilineal. Entonces existe un homomorfismo de  $A$ -módulos  $\varphi: T^d(M) \rightarrow N$  tal que

$$\varphi(m_1 \cdots m_d) = \beta(m_1, \dots, m_d),$$

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 « $\square$ » denota multiplicación en  $F$ . Luego, los elementos de  $\mathfrak{a}$  son sumas de elementos de la forma  $a \square s \square b$  donde  $a, b \in F$  y  $s \in S$ .

Sea  $u \in F_d \cap \mathfrak{a}$ , luego  $u = \sum_{i=1}^n a_i \square s_i \square b_i$ , donde  $s_i \in S$  es homogéneo de grado 1 y donde

$$a_i = \sum_{k=0}^m a_{ik}, \quad b_i = \sum_{\ell=0}^m b_{i\ell},$$

donde  $a_{ik}, b_{i\ell}$  son las componentes homogéneas de grado  $k$  de  $a_i, b_i$  resp. (y donde elegimos a  $m$  suficientemente grande). Luego

$$u = \sum_{i=1}^n \sum_{k,\ell} a_{ik} \square s_i \square b_{i\ell},$$

nótese que cada término  $a_{ik} \square s_i \square b_{i\ell}$  es homogéneo de grado  $k + 1 + \ell$ , luego

como  $u$  es homogéneo de grado  $d$  tenemos la igualdad

$$u = \sum_{i=1}^n \sum_{k+\ell+1=d} a_{ik} \square s_i \square b_{i\ell}.$$

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:

$$x_1 \square \cdots \square x_k \square s \square y_1 \square \cdots \square y_\ell, \quad (10.1)$$

donde  $x_i, y_j \in M$  para todo  $i, j$ ,  $s \in S$  y  $k + \ell + 1 = d$ .

Nótese que el conjunto  $\{z_1 \square \cdots \square z_h : z_i \in M\}$  es una base de  $F_h$ , de modo que dada una aplicación  $h$ -multilineal  $\beta: M^d \rightarrow N$  se extiende a un único homomorfismo de  $A$ -módulos  $\psi: F_d \rightarrow N$ . Es fácil ver que  $\psi$  se anula en  $F_d \cap \mathfrak{a}$  puesto que sus elementos son de la forma descrita en (10.1), luego descendiendo al cociente  $F_d/(F_d \cap \mathfrak{a}) = T^d(M)$  como se quería ver.  $\square$

**Corolario 10.34.1:** Para todo  $d \geq 1$  se cumple que  $T^d(M) \cong M^{\otimes d}$  (como  $A$ -módulos).

**Definición 10.35:** 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 10.36:** Sea  $B$  una  $A$ -álgebra graduada. Supongamos que  $B$  está generada por un sistema  $S = \{x_1, \dots, x_n\}$  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.

**Proposición 10.37:** Toda subálgebra y todo cociente de una álgebra anticonmutativa es también una álgebra anticonmutativa.

**Teorema 10.38:** Sean  $B_1, \dots, B_r$  un conjunto de  $A$ -álgebras anticonmutativas, entonces  $B_1 \otimes_A \dots \otimes_A B_r$  es una álgebra anticonmutativa.

Teoremas pendientes.

**Teorema 10.39:** Sean  $B, C$  un par de  $A$ -álgebras graduadas y sea  $D$  una  $A$ -álgebra anticonmutativa. Supongamos que existen  $\varphi: B \rightarrow D$  y  $\psi: C \rightarrow D$  homomorfismos homogéneos de grado 0. Entonces existe un único homomorfismo de  $A$ -álgebras  $\theta: B \otimes_A C \rightarrow D$  tal que  $\theta(b \otimes c) = \varphi(b)\psi(c)$ .

### §10.2.3 Álgebra exterior y determinantes.

**Definición 10.40:** Sea  $M$  un  $A$ -módulo. Un par  $(E, \psi)$  se dice una *álgebra exterior* sobre  $M$  si:

- AE1.  $E$  es una  $A$ -álgebra y  $\psi: M \rightarrow E$  es un homomorfismo de  $A$ -módulos.
- AE2. Para todo  $\mathbf{m} \in M$  se cumple que  $\psi(\mathbf{m})^2 = 0$ .
- AE3. Si  $\varphi: M \rightarrow B$  es un homomorfismo de  $A$ -módulos, donde  $B$  es una  $A$ -álgebra, tal que  $\varphi(\mathbf{m})^2 = 0$  para todo  $\mathbf{m} \in M$ , entonces existe un único homomorfismo de  $A$ -álgebras  $f: E \rightarrow B$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} & & E \\ & \nearrow \psi & \vdots \\ M & \xrightarrow{\varphi} & B \\ & & \downarrow f \end{array}$$

**Lema 10.41:** 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) 10.42:** Dado un  $A$ -módulo libre  $M$  existe una álgebra exterior sobre  $M$ , denotada  $\bigwedge(M)$ .

DEMOSTRACIÓN: Sea  $X = \{\mathbf{u}_\alpha\}_{\alpha < \kappa}$  una base de  $M$  la cual está indexada por ordinales por AE; construiremos  $E$  como prosigue. Diremos que para

todos  $\mathbf{u}, \mathbf{v} \in X$  distintos, entonces  $\mathbf{u}^2 = 0$  y  $\mathbf{uv} = -\mathbf{vu}$ . 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  $\mathbf{u}_\alpha$  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

$$\bar{u}_{\alpha_1} \cdots \bar{u}_{\alpha_n} = (\text{sgn } \sigma) \cdot \bar{u}_{\alpha_{\sigma(1)}} \cdots \bar{u}_{\alpha_{\sigma(n)}},$$

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  $\psi: M \rightarrow E$  así: dado un  $\mathbf{m} = \sum_{\alpha=0}^{\kappa} c_\alpha \mathbf{u}_\alpha$ , entonces  $\psi(\mathbf{m}) = \sum_{\alpha=0}^{\kappa} c_\alpha \bar{u}_\alpha$ . Luego notamos que

$$\begin{aligned} \left( \sum_{\alpha} c_\alpha \bar{u}_\alpha \right)^2 &= \sum_{\alpha < \beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta + \sum_{\alpha} \cancel{c_\alpha^2 \bar{u}_\alpha^2}^0 + \sum_{\alpha > \beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta \\ &= \sum_{\alpha < \beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta + \sum_{\beta > \alpha} c_\beta c_\alpha \bar{u}_\beta \bar{u}_\alpha \\ &= \sum_{\alpha < \beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta - \sum_{\beta > \alpha} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta = 0. \end{aligned}$$

Ahora bien, sea  $\varphi: M \rightarrow A$  tal que  $\varphi(\mathbf{m})^2 = 0$ , en particular,  $\varphi(\mathbf{u}_\alpha) \cdot \varphi(\mathbf{u}_\alpha) = 0$ . Nótese que

$$0 = \varphi(\mathbf{u}_\alpha + \mathbf{u}_\beta)^2 = \cancel{\varphi(\mathbf{u}_\alpha)^2} + \cancel{\varphi(\mathbf{u}_\beta)^2} + \varphi(\mathbf{u}_\alpha)\varphi(\mathbf{u}_\beta) + \varphi(\mathbf{u}_\beta)\varphi(\mathbf{u}_\alpha).$$

Luego, podemos definir  $f(\bar{u}_{\alpha_1} \cdots \bar{u}_{\alpha_n}) = \varphi(\mathbf{u}_{\alpha_1}) \cdots \varphi(\mathbf{u}_{\alpha_n})$  que está bien definida por la observación anterior.  $\square$

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) 10.42.1:** Si  $M$  es un  $A$ -módulo libre de rango  $\kappa$ , entonces  $\bigwedge(M)$  es libre (como  $A$ -módulo) y  $\text{rang}(\bigwedge(M)) = 2^\kappa$ .

Ahora que hemos construido formalmente la álgebra exterior, admitiremos la notación « $\wedge$ » para su producto, en lugar de « $\cdot$ ».

Otra conclusión de la demostración es que  $\bigwedge(M)$  es de hecho un cociente sobre  $T(M)$  y es fácil notar que el ideal empleado está generado por elementos homogéneos, de modo que  $\bigwedge(M)$  es también una álgebra graduada. Los elementos homogéneos de grado  $d$  son de la forma  $m_1 \wedge \cdots \wedge m_d$ . Luego, si  $M$  es libre de rango  $n$ , entonces  $\bigwedge^d(M)$  es un  $A$ -módulo libre de rango  $\binom{n}{d}$ .

**Corolario 10.42.2:** Sea  $M$  un  $A$ -módulo con una álgebra exterior  $\bigwedge(M)$ . Dado un endomorfismo de  $A$ -módulos  $L: M \rightarrow M$ , se puede construir un endomorfismo de  $A$ -álgebras  $\eta(L): \bigwedge(M) \rightarrow \bigwedge(M)$  dado por el siguiente diagrama conmutativo:

$$\begin{array}{ccc} M & \xrightarrow{\wedge} & \bigwedge(M) \\ L \downarrow & & \downarrow \exists! \eta(L) \\ M & \xrightarrow{\wedge} & \bigwedge(M) \end{array}$$

Si  $L_1, L_2 \in \text{End}_{\text{Mod}}(M)$  entonces:

$$\eta(1_M) = 1_{\bigwedge(M)}, \quad \eta(L_1 \circ L_2) = \eta(L_1) \circ \eta(L_2).$$

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  $\bigwedge_A: \text{FMod}_A \rightarrow \text{Alg}_A$  es un funtor.

Ahora veamos una conexión entre la álgebra exterior y los determinantes: Sea  $L: M \rightarrow M$  un endomorfismo de  $M$  y sea  $B := (\mathbf{u}_1, \dots, \mathbf{u}_n)$  una base ordenada de  $M$ . Definamos  $L(\mathbf{u}_i) = \sum_{j=1}^n a_{ij} \mathbf{u}_j$ , de modo que claramente  $[a_{ij}]_{ij} = M_B^B(L)$ . Luego

$$\begin{aligned} \eta(L)(\bar{u}_1 \cdots \bar{u}_n) &= L(\mathbf{u}_1) \cdots L(\mathbf{u}_n) = \sum_{j_1=1}^n a_{1j_1} \bar{u}_{j_1} L(\mathbf{u}_2) \cdots L(\mathbf{u}_n) \\ &= \sum_{j_1=1}^n \cdots \sum_{j_n=1}^n a_{1j_1} \cdots a_{nj_n} \bar{u}_{j_1} \cdots \bar{u}_{j_n}. \end{aligned}$$

Ahora recordamos que  $\bar{u}_{j_1} \cdots \bar{u}_{j_n}$  se anulará si hay índices 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

$$\eta(L)(\bar{u}_1 \cdots \bar{u}_n) = \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \bar{u}_{\sigma(1)} \cdots \bar{u}_{\sigma(n)}$$

$$= \sum_{\sigma \in S_n} (\text{sgn } \sigma) a_{1, \sigma(1)} \cdots a_{n, \sigma(n)} \bar{u}_1 \cdots \bar{u}_n = (\det L) \bar{u}_1 \cdots \bar{u}_n.$$

Ésto nos otorga otra prueba, más directa aún, de que

$$\det(L_1 \circ L_2) = \det(L_1) \det(L_2).$$

También, debido a esto, denotamos por  $\det(M) := \bigwedge_A^n(M)$  si  $M$  es libre de  $\text{rang}_A M = n$ .

**Teorema 10.43:** Sea  $k$  un cuerpo y sea  $k[\{x_{ij} : 1 \leq i, j \leq n\}]$  el anillo de polinomios. Considere  $X = [x_{ij}]_{ij} \in \text{Mat}_n(k[x_{ij}]_{ij})$ , 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  $i \in \{1, 2, \dots, n\}$ . 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.  $\square$

**Teorema 10.44:** 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  $\text{Mat}_n(k)$ . 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  $A, B \in \text{Mat}_n(k)$ .

Entonces  $Q(X)$  es una potencia de  $\det X$ .

DEMOSTRACIÓN: En primer lugar, nótese que para todo  $A \in \text{Mat}_n(k)$  se tiene que

$$Q(A)Q(\text{adj } A) = Q(A \cdot \text{adj } A) = Q((\det A)I_n) = (\det A)^q.$$

Sabemos que la coordenada  $(\text{adj } X)_{ij} = (-1)^{i+j}M_{ji}(X)$  la cual es un polinomio en  $k[x_{ij}]_{ij}$ , de modo que  $Q(\text{adj } X)$  es también un polinomio en  $k[x_{ij}]_{ij}$ .

Luego  $P(X) := Q(X)Q(\text{adj } X) - (\det X)^q \in k[x_{ij}]_{ij}$  es un polinomio que evaluado en todas las matrices  $A \in \text{Mat}_n(k)$  se anula, y como  $k$  es infinito, eso implica que  $P(X) = 0 \in k[x_{ij}]_{ij}$ , de modo que  $Q(X) \cdot Q(\text{adj } X) = (\det X)^q$ , 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.  $\square$

De hecho, con ello se demuestra que  $q = n^r$  y por igualdad de grados nos queda que  $Q(X) = (\det X)^r$ .

**Definición 10.45:** Sea  $M$  un  $A$ -módulo. Construimos el *álgebra simétrica*, denotada  $\text{Sym}_A(M)$ , como el cociente del álgebra tensorial  $T := T_A(M)$  por el ideal bilateral (respecto al anillo  $T$ ) generado por los elementos de la forma  $u \otimes v - v \otimes u$  con  $u, v \in T$ . El producto en  $\text{Sym}_A(M)$  se denota « $\cdot$ ».

Éste ideal es claramente homogéneo, de modo que  $\text{Sym}_A(M)$  es una  $A$ -álgebra graduada y sus componentes homogéneas se denotan  $\text{Sym}_A^d(M)$ .

**Proposición 10.46:** Sea  $M$  un  $A$ -módulo. Entonces el funtor

$$\text{Hom}_{\text{Mod}_A}(M, -): \text{CAlg}_A \longrightarrow \text{Set}$$

está representado por  $\text{Sym}_A(M)$ .

**Ejemplo.** Sea  $M = A^n$  el  $A$ -módulo libre con  $n$  elementos. Entonces  $\text{Sym}_A(A^n) \cong A[x_1, \dots, x_n]$ .

Para el siguiente resultado es necesario conocer la definición de *categoría filtrada*. La expresión *límite filtrado* siempre refiere a un límite directo.

**Teorema 10.47:** Sea  $A$  un dominio. Los funtores  $T_A, \bigwedge_A, \text{Sym}_A$  preservan límites filtrados.

DEMOSTRACIÓN: Esto se sigue del hecho de que el funtor  $M \otimes_A - : \text{Mod}_A \rightarrow \text{Mod}_A$  preserva límites directos (cfr. teorema de Eilenberg-Watts) y que, si el diagrama es filtrado, es fácil verificar que los límites respetan los ideales mediante los cuales se realiza el cociente.  $\square$

**Corolario 10.47.1:** Sea  $A$  un dominio y  $S \subseteq A$  un sistema multiplicativo. Entonces para todo  $A$ -módulo  $M$  se tiene que

$$\begin{aligned} S^{-1} T_A(M) &\cong T_{S^{-1}M}(S^{-1}M), & S^{-1} \bigwedge_A(M) &\cong \bigwedge_{S^{-1}M}(S^{-1}M), \\ S^{-1} \text{Sym}_A(M) &\cong \text{Sym}_{S^{-1}M}(S^{-1}M). \end{aligned}$$

DEMOSTRACIÓN: Esto se debe a que uno puede caracterizar  $S^{-1}M$  como el límite filtrado de invertir subconjuntos finitos de  $S$ .  $\square$

#### §10.2.4 Representaciones.

**Definición 10.48:** Sea  $M$  un  $A$ -módulo, entonces podemos ver a  $\text{End}_{\text{Mod}}(M)$  como una  $A$ -álgebra: donde  $1 \in \text{End}(M)$  es  $1 = \text{Id}_M$ ,  $L_1 + L_2$  y  $\alpha \cdot L$  son las operaciones coordenada a coordenada y  $L_1 \cdot L_2 := L_1 \circ L_2 \in \text{End}(M)$ .

El álgebra de endomorfismos nos otorga de hecho un teorema similar al de Cayley para grupos:

**Teorema 10.49:** Sea  $B$  un  $A$ -álgebra, entonces  $B$  es isomorfo a una subálgebra de  $\text{End}_{\text{Mod}}(B)$ .

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  $\mu_b$  es un endomorfismo de  $A$ -módulos. Luego la aplicación  $b \mapsto \mu_b$  es un monomorfismo de  $A$ -álgebras (¡ demuéstrela! ) cuya imagen es una subálgebra de  $\text{End}_{\text{Mod}}(B)$ .  $\square$

Supongamos que  $B$  es un  $A$ -módulo libre de rango  $n$ , luego  $\text{End}_{\text{Mod}}(B) = \text{End}_{\text{Mod}}(A^n) = \text{Mat}_n(A)$ . Así pues, a todos los elementos de  $B$  les asignamos un endomorfismo 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:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \quad (10.2)$$

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:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2, \quad (10.3)$$

donde

$$\begin{aligned} z_1 &= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, \\ z_2 &= x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3, \\ z_3 &= x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2, \\ z_4 &= x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1. \end{aligned}$$

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

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \quad (10.4)$$

donde cada  $z_\ell$  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  $\{x_1, \dots, x_n\}$ . Definiendo  $A = [a_{ij}]_{ij}$ , vemos que buscamos una fórmula del estilo:

$$\mathbf{Z} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \mathbf{A}\mathbf{Y}.$$

que satisfaga que

$$\begin{aligned} (x_1^2 + \cdots + x_n^2) \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} I_n &= (x_1^2 + \cdots + x_n^2) \mathbf{Y}^t \mathbf{Y} I_n \\ &= \mathbf{Z}^t \mathbf{Z} = \mathbf{Y}^t \mathbf{A}^t \mathbf{A} \mathbf{Y}. \end{aligned}$$

Reordenando se obtiene que

$$(x_1^2 + \cdots + x_n^2) I_n - \mathbf{A}^t \mathbf{A} = \mathbf{0}.$$

Como cada  $a_{ij}$  es una función lineal de los  $\{x_1, \dots, x_n\}$ , entonces tenemos que

$$a_{ij} = b_{ij}^1 x_1 + b_{ij}^2 x_2 + \cdots + b_{ij}^n x_n,$$

donde en  $b_{ij}^\ell$  el  $\ell$  es un superíndice, no un exponente. Definiendo  $B_\ell := [b_{ij}^\ell]_{ij}$ , se tiene que

$$\mathbf{A} = B_1 x_1 + \cdots + B_n x_n.$$

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 10.50:** 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  $\{1, 2, \dots, n-1\}$  por lo que contiene  $\leq 2^{n-1}$  elementos (puesto que tal vez se repitan).

- (I)  $G$  es simétrica syss  $r \equiv 0$  o  $3$  (mód 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  $MG$  es una permutación de  $\mathcal{G}$  quizás 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  $C_1 C_2 H = C_2 C_1 H$ , 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

$$I_n = \sum_{i_1 < n} \alpha_{i_1} C_{i_1} + \sum_{i_1 < i_2 < n} \alpha_{i_1, i_2} C_{i_1} C_{i_2} + \cdots, \quad (10.5)$$

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 10.51:** Se dice que un par  $(B, Q)$  es una *A-álgebra de composición* si:

1.  $B$  es una  $A$ -álgebra (posiblemente no asociativa) y  $Q: B \rightarrow A$  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:

$$Q(x)Q(z) + \beta(x, y)Q(z) + Q(y)Q(z) = Q(x + y)Q(z) = Q(xz + yz)$$

$$= Q(xz) + \beta(xz, yz) + Q(yz).$$

Con lo que hemos probado que

$$\beta(x, y)Q(z) = \beta(xz, yz), \quad Q(x)\beta(y, z) = \beta(xy, xz).$$

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:

$$\begin{aligned} \overline{(\ )}: \beta &\longrightarrow \beta \\ x &\longmapsto \beta(x, 1)1_B - x. \end{aligned}$$

Aquí el  $1_B$  enfatiza el hecho de que es la unidad de  $B$ . Nótese que  $\overline{(\ )}$  es un endomorfismo de  $A$ -módulos.

**Lema 10.52:** 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

$$\begin{aligned} \beta(x, \bar{y}z) &= \beta(x, \beta(y, 1)z - yz) = \beta(y, 1)\beta(x, z) - \beta(x, yz) \\ &= \beta(yx, z) + \cancel{\beta(yz, \bar{x})} - \cancel{\beta(x, \bar{y}z)} = \beta(yx, z), \end{aligned}$$

donde empleamos la identidad (10.6). Con un razonamiento análogo concluimos que

$$\beta(x, \bar{y}z) = \beta(yx, z), \quad \beta(xy, z) = \beta(x, z\bar{y}), \quad (10.7)$$

luego, nótese que

$$Q(x)\beta(1, y) = \beta(x, xy) = \beta(x, \bar{x}y) = \beta(\bar{x}x, y),$$

o lo que es equivalente,  $\beta(Q(x)1 - \bar{x}x, y) = 0$  para todo  $y$ . Como  $\beta$  es una forma bilineal no degenerada, se concluye que necesariamente  $Q(x)1 = \bar{x}x$ . Para la otra igualdad, sustituimos  $x$  por  $\bar{x}$ :

$$x\bar{x} = \bar{x}\bar{x} = Q(\bar{x})1 = Q(x)1.$$

3. Siga el siguiente procedimiento:

$$\begin{aligned} \beta(\bar{x}(xy), z) &= \beta((\beta(x, 1)1 - x)(xy), z) \\ &= \beta(x, 1)\beta(xy, z) - \beta(x(xy), z) \\ &= \cancel{\beta(x(xy), z)} + \beta(xz, xy) - \cancel{\beta(x(xy), z)} \\ &= Q(x)\beta(z, y) = Q(x)\beta(y, z) = \beta(Q(x)y, z). \end{aligned}$$

4. Ejercicio.

5. Nótese que por la identidad (10.7)

$$\beta((\bar{xy})1, z) = \beta(1, \overline{\bar{xy}z}) = \beta(1, (xy)z).$$

Veremos lo mismo para la otra:

$$\begin{aligned} \beta(\bar{y}\bar{x}, z) &= \beta((\beta(y, 1)1 - y)(\beta(x, 1)1 - x), z) \\ &= \beta(y, 1)\beta(x, 1)\beta(1, z) - \beta(y, 1)\beta(x, z) - \beta(x, 1)\beta(y, z) - \beta(yx, z). \end{aligned}$$

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

$$\begin{aligned} \beta(\bar{y}\bar{x}, z) &= \beta((xy)z, 1) + \beta(x, y)\beta(1, z) - \beta(yz, x) - \beta(xz, y) \\ &= \beta((xy)z, 1). \end{aligned} \quad \square$$

**Definición 10.53:** 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 10.53.1:** Toda álgebra de composición es alternativa.

DEMOSTRACIÓN: Basta emplear el hecho de que  $\bar{x} = \beta(x, 1)1 - x$  y las propiedades 3 y 4 del lema anterior.  $\square$

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 10.54:** Sea  $B$  una  $A$ -álgebra alternativa. Entonces para todo  $x, y, z \in B$  se cumple que

$$(ux)(yu) = u(xy)u, \quad (10.8)$$

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:

$$\begin{aligned} (u^2x)y + 2(ux)(yu) + x(yu^2) &= u((ux)y) + u(x(yu)) + ((ux)y)u + (x(yu))u \\ &= u((ux)y + x(yu)) + ((ux)y + x(yu))u \\ &= u(u(xy) + (xy)u) + (u(xy) + (xy)u)u \\ &= u^2(xy) + 2u(xy)u + (xy)u^2, \end{aligned}$$

con lo que aplicamos la igualdad inicial y concluimos que  $2((ux)(yu) - u(xy)u) = 0$ .  $\square$

Probar caso característica = 2.

**Teorema 10.55:** Sea  $B$  una  $A$ -álgebra. Son equivalentes:

1.  $B$  es una álgebra alternada con una involución  $\overline{(\cdot)}: B \rightarrow B$  tal que  $\bar{x}x = Q(x)$ , donde  $Q: B \rightarrow A$  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

$$\begin{aligned} (Q(x) + \beta(x, y) + Q(y))1 &= Q(x + y)1 \\ &= \overline{(x + y)}(x + y) = \bar{x}x + \bar{y}y + \bar{x}y + \bar{y}x, \end{aligned} \quad (10.9)$$

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  $\bar{x}\bar{y} = \bar{y}x$  se demostraba únicamente empleando las proposiciones anteriores, de modo que también es válido aquí. Luego:

$$\begin{aligned} Q(xy)1 &= \bar{x}\bar{y}(xy) = (\bar{y}\bar{x})(xy) = ((T(y)1 - y)\bar{x})(xy) \\ &= T(y)\bar{x}(xy) - (y\bar{x})(xy) = T(y)Q(x)y - y(\bar{x}x)y \\ &= Q(x)(T(y) - y)y = Q(x)\bar{y}y = Q(x)Q(y)1. \end{aligned} \quad \square$$

**Definición 10.56:** Sea  $B$  una  $A$ -álgebra con una involución  $\overline{(\cdot)}: B \rightarrow B$  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.
- Se tiene:

$$\overline{(x, y)} \cdot (x, y) = (\bar{x}, -y)(x, y) = (\bar{x}x - c\bar{y}y, y\bar{x} - y\bar{x}) = (Q(x) - cQ(y))1.$$



- Definiendo  $Q_C(x, y) := Q(x) - cQ(y)$  notamos que es de hecho una forma cuadrática y que su forma bilineal asociada:

$$\beta_C((u, v), (x, y)) = \beta(u, x) - c\beta(v, y)$$

es no degenerada.

**Ejemplo.** De lo anterior podemos considerar el siguiente caso. Si  $A$  es conmutativo y  $\bar{(\cdot)} = \text{Id}_A$ , entonces, definiendo  $1 := (1, 0)$  y  $i := (0, 1)$ , el  $c$ -duplicado es un  $A$ -módulo libre con base  $\{1, i\}$ , que es una álgebra conmutativa donde  $i^2 = c$ . Recuerdese que definimos la involución  $\overline{a + bi} := a - bi$  sobre el  $c$ -duplicado.

**Teorema 10.57:** 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:

$$[U, X] = ([x, u] + c(\bar{y}v - \bar{v}y), [u, y] + v\bar{x} - x\bar{v}) \quad (10.10)$$

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:

$$\begin{aligned} [U, X, Z] = & ([u, v, x] + c(\bar{w}(yu) - u(\bar{w}y) + \bar{w}(v\bar{x}) - (\bar{x}\bar{w})v + (\bar{y}v)z - (z\bar{y})v, \\ & w(ux) - (wx)u + (yu)\bar{z} - (y\bar{z})u + (v\bar{x})\bar{z} - (v\bar{z})\bar{x} + c(w(\bar{y}v) - v(\bar{y}w))). \end{aligned} \quad (10.11)$$

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  $\Leftarrow$ : 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

$$[X, Y, Z] = \overline{(XY)Z - X(YZ)} = \bar{Z}(\bar{Y}\bar{X}) - (\bar{Z}\bar{Y})\bar{X} = -[\bar{Z}, \bar{Y}, \bar{X}].$$

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

$$[\bar{X}, X, Z] = (c[\bar{x}, \bar{w}, y], -[y, \bar{z}, \bar{x}]),$$

lo que es claramente cero si  $B$  es asociativa, y recíprocamente si  $C$  es alternante entonces la fórmula de arriba permite concluir asociatividad en  $B$ .  $\square$

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 10.58:** Sea  $(B, Q)$  una  $A$ -álgebra de composición y sea  $C$  una subálgebra propia de  $B$  que es invariante por  $(\bar{\cdot})$  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

$$\overline{t(\bar{x}\bar{y})} = (\overline{t\bar{y}})\bar{x} \iff \overline{(\bar{x}\bar{y})t} = (yx)t = (yt)\bar{x},$$

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  $C$ .  $\square$

**Teorema 10.59 – Teorema de Hurwitz.** Sea  $A$  un dominio con  $\text{car } A \neq 2$ . Las álgebras de composición son las siguientes:

- |                               |                                  |
|-------------------------------|----------------------------------|
| (a) $A$ .                     | (c) Las álgebras cuaterniónicas. |
| (b) Las álgebras cuadráticas. | (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 las álgebras octoniónicas no son asociativas y, por ende, no podemos duplicar la construcción.  $\square$

**§10.3.3 Aplicación: álgebras de división.** Veamos ahora cómo se emplea la clasificación de Hurwitz sobre tres casos particulares:

**Teorema 10.60:** 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  $\{1, \beta, \beta^2, \dots, \beta^n\}$  es un conjunto linealmente dependiente, luego, podemos reorganizar la dependencia lineal y obtener que  $\beta$  es raíz de algún polinomio  $p(x) \in k[x]$ , de modo que  $\beta$  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  $\beta$ , y los inversos del hecho de que  $A$  es de división), luego es una extensión algebraica, pero entonces  $k(\beta) = k$  y  $\beta \in k$ .  $\square$

**Teorema 10.61 – 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

$$(u + v)^2 = p(u + v) + q, \quad (u - v)^2 = r(u - v) + s.$$

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  $Q(u) = 0$  si y sólo si  $u = 0$ . 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  $i \in A'$  tal que  $Q(i) = 1$  y notamos que  $i^2 = -1$ , luego  $\mathbb{R}[i] = \mathbb{R} \oplus \mathbb{R} \cdot i$  es una subálgebra conmutativa de  $A$ . Si  $A \supset \mathbb{R}[i]$ , entonces existe  $j \perp \mathbb{R}[i]$  tal que  $Q(j) = 1$ , luego  $j^2 = -1$  y  $-\beta(i, j) = ij + ji = 0$  de modo que  $ij = -ji$ . Definiendo  $k := ij$ , vemos que

$$k = -ji, \quad k^2 = -1, \quad ik + ki = 0 = jk + kj,$$

por lo que  $\mathbb{R}[i, j] = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$  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 duplicar a  $\mathbb{H}$  y obtener a  $\mathbb{O}$ , y por el teorema de Hurwitz no podemos seguir extendiendo las álgebras.  $\square$

**Teorema 10.62 (pequeño 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  $|A| = q^n$ .  $A^\times = A \setminus \{0\}$  es un grupo multiplicativo y  $F^\times$  actúa sobre él, de modo que, por la ecuación de clases se obtiene

$$|A^\times| = q^n - 1 = \sum_a [A^\times : \text{Stab}_a] = q - 1 + \sum_{a \notin F} [A^\times : \text{Stab}_a],$$

donde  $a$  recorre representantes en las clases de equivalencia de la conjugación. Si  $x_i \notin F$ , entonces  $\text{Stab}_{x_i}$  es un subgrupo multiplicativo y, más aún,  $F_i := \text{Stab}_{x_i} \cup \{0\}$  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

$$q^n - 1 = q - 1 + \sum_i \frac{q^n - 1}{q^{d_i} - 1}. \quad (10.12)$$

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  $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$ , donde  $\Phi_d(x) \in \mathbb{Z}[x]$  es el  $d$ -ésimo polinomio ciclotómico; luego

$$\frac{x^n - 1}{x^{d_i} - 1} = \frac{\prod_{d \mid n} \Phi_d(x)}{\prod_{d \mid d_i} \Phi_d(x)} = \prod_{\substack{d \mid n \\ d \nmid d_i}} \Phi_d(x),$$

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  $\Phi_n$  cuando  $n > 1$ , por lo que  $|q - 1| < \prod_{\zeta} |q - \zeta| = |\Phi_n(\zeta)|$  lo cual es absurdo.  $\square$

## 10.4 Introducción a las álgebras centrales simples

En ésta sección introduciremos el lenguaje básico de una de las nociones más interesantes del álgebra abstracta. Las álgebras centrales simples tienen importantes aplicaciones en geometría que se bosquejarán en la siguiente sección, que se enfoca en el caso de dimensión 4. En esta sección y la siguiente haremos casualmente libre uso de la teoría de esquemas.

**Lema 10.63:** Sea  $k$  un cuerpo,  $D$  una  $k$ -álgebra y  $A, B$  un par de subálgebras. Entonces  $D \cong A \otimes_k B$  si y sólo si se satisfacen las siguientes condiciones:

1.  $ab = ba$  para todo  $a \in A, b \in B$ .
2. Existe una  $k$ -base  $\{e_i\}_{i \in I}$  de  $A$ , tal que todo elemento de  $D$  se escribe de manera única como suma finita  $\sum_{i \in I} b_i a_i$  para algunos  $b_i \in B$ .

Si además  $D$  tiene dimensión finita (como  $k$ -espacio vectorial), entonces 2 es equivalente a:

$$2^* \quad D = AB \text{ y } \dim_k D = (\dim_k A)(\dim_k B).$$

**Proposición 10.64:** Sea  $k$  un cuerpo. Para todo  $n, m \in \mathbb{N}$  y toda  $k$ -álgebra  $B$  se cumplen:

1.  $\text{Mat}_n(B) \cong \text{Mat}_n(k) \otimes_k B$ .
2.  $\text{Mat}_n(k) \otimes \text{Mat}_m(k) \cong \text{Mat}_{nm}(k)$ .

**Definición 10.65:** Sea  $k$  un cuerpo y sea  $A$  una  $k$ -álgebra. Se define el **centro** de  $A$  como

$$Z(A) := \{\beta \in A : \forall \alpha \in A \quad \alpha\beta = \beta\alpha\}.$$

En general, se exige que  $Z(A) \supseteq k$ . Se dice que  $A$  es una **álgebra central** si  $Z(A) = k$ .

Se dice que  $A$  es una **álgebra de Azumaya** si es una álgebra asociativa, central, simple, de dimensión finita. Se dice que  $A$  **se escinde** si es  $k$ -isomorfa a  $\text{Mat}_n(k)$  para algún  $n \geq 1$ .

Recuérdese que *simple* significa «sin ideales bilaterales impropios». Sea  $A$  una  $k$ -álgebra simple. Entonces el lema de Schur dice que  $D := \text{End}_k(A)$  es un anillo de división y nótese que  $A$  es un  $D$ -módulo derecho de manera canónica, donde dado  $\varphi \in D$ , se define  $a \cdot \varphi := \varphi(a)$ .

**Lema 10.66 (Rieffel):** Sea  $I$  un ideal derecho no nulo en una  $k$ -álgebra simple  $A$  y sea  $D := \text{End}_A(I)$ . El homomorfismo

$$\begin{aligned} \lambda_I: A &\longrightarrow \text{End}_D(I) \\ a &\longmapsto (\beta \mapsto \beta a) \end{aligned}$$

es un isomorfismo (en Ring).

**DEMOSTRACIÓN:** Como  $\lambda_I$  es no nulo, entonces es inyectivo por el lema de Schur. En primer lugar, nótese que  $\lambda_I[I]$  es un ideal derecho de  $\text{End}_D(I)$  puesto que, para todo  $\varphi \in \text{End}_D(I)$  y todo  $\lambda_I(b)$  con  $b \in I$ , se cumple que

$$\forall c \in I \quad (\lambda_I(b) \circ \varphi)(c) := \varphi(cb) = c\varphi(b) = \lambda_I(\varphi(b))(c).$$

En segundo lugar, el ideal izquierdo  $AI$ , generado por  $I$ , es un ideal bilateral y, por simplicidad,  $AI = A$ . En particular,  $1 = \sum_{i=1}^n a_i b_i$  para algunos

$a_i \in A, b_i \in I$ . Por tanto, para todo  $\varphi \in \text{End}_D(I)$  tenemos que

$$\varphi = 1 \cdot \varphi = \lambda_I(1) \circ \varphi = \sum_{i=1}^n \lambda_I(a_i) \lambda_I(b_i) \varphi,$$

donde el término en rojo pertenece a  $\lambda_I[I]$  puesto que es un ideal derecho. Así pues  $\varphi \in \lambda_I[A] \lambda_I[I] = \lambda_I[AI] = \lambda_I[A]$ .  $\square$

**Teorema 10.67 – Teorema de Wedderburn-Artin:** Sea  $k$  un cuerpo y  $A$  una  $k$ -álgebra de Azumaya. Existe un  $n > 0$  y una única  $k$ -álgebra de división  $D \supseteq k$  tal que  $A \cong \text{Mat}_n(D)$ . En particular, si  $k$  es algebraicamente cerrado, todas sus  $k$ -álgebras de Azumaya se escinden.

DEMOSTRACIÓN: Sobre un cuerpo, todo módulo finitamente generado es artiniiano, por lo que las cadenas descendientes de ideales (derechos) se estabilizan. Sea  $I$  un ideal derecho minimal de  $A$ , es decir, un  $A$ -módulo derecho. Por el lema de Schur,  $D := \text{End}_A(I)$  es una álgebra de división y, por el lema de Rieffel,  $A \cong \text{End}_D(I)$ . Nótese que  $I$  es un  $D$ -módulo derecho finitamente generado, por lo que es libre de rango  $n$  y, por lo tanto,  $\text{End}_D(I) \cong \text{Mat}_n(D)$  (este último isomorfismo es casi mera notación).

La unicidad se sigue de que si  $E$  fuese otra  $k$ -álgebra de división tal que  $A \cong \text{Mat}_m(E)$ , entonces como  $I \cong E^m$  (como  $E$ -módulo), entonces

$$D \cong \text{End}_A(D^n) \cong \text{End}_A(I) \cong \text{End}_A(E^m) \cong E. \quad \square$$

**Lema 10.68:** Sea  $K/k$  una extensión finita de cuerpos y  $A$  una  $k$ -álgebra de dimensión finita. Entonces  $A$  es central simple sobre  $k$  si y sólo si  $A \otimes_k K$  es central simple sobre  $K$ .

DEMOSTRACIÓN:  $\Leftarrow$ . Por contrarrecíproca, si  $A$  no es simple, posee un ideal impropio bilateral  $I \triangleleft A$  y luego  $I \otimes_k K$  es bilateral en  $A \otimes_k K$  e impropio por un argumento de dimensión. Si  $A$  no es central, entonces claramente  $A \otimes_k K$  tampoco.

$\Rightarrow$ . Por el teorema de Wedderburn-Artin y los lemas anteriores, podemos suponer que  $A = D$  es una  $k$ -álgebra de división central. Sea  $v_1, \dots, v_n \in K$  una  $k$ -base, entonces  $1 \otimes v_1, \dots, 1 \otimes v_n$  es una  $D$ -base de  $D \otimes_k K$  como  $D$ -espacio vectorial izquierdo. Si  $\gamma := \sum_{i=1}^n \alpha_i (1 \otimes v_i) \in D \otimes_k K$  está en el centro, entonces la relación

$$\forall d \in D \quad \gamma = (d^{-1} \otimes 1) \gamma (d \otimes 1) = \sum_{i=1}^n (d^{-1} \alpha_i d) (1 \otimes v_i),$$



implica que  $\alpha_i = d^{-1}\alpha_i d$  (por definición de base) y, como  $D$  es central, esto significa que cada  $\alpha_i \in k$ . Así que  $\gamma \in k \otimes_k K = K$ .

Si  $I$  es un ideal bilateral de  $D \otimes_k K$  generado por  $z_1, \dots, z_m$ , los cuales podemos suponer  $D$ -linealmente independientes; entonces los extendemos a una  $D$ -base de  $D \otimes_k K$  añadiendo  $1 \otimes v_{m+1}, \dots, 1 \otimes v_n$  (quizá tras renombrar los índices). Así que, para  $1 \leq i \leq m$ , tenemos que

$$1 \otimes v_i = \sum_{j=m+1}^n \alpha_{ij}(1 \otimes v_j) + y_i,$$

donde  $y_i$  es una combinación  $D$ -lineal de los  $z_j$ 's y son  $D$ -linealmente independientes entre sí (pues los  $1 \otimes v_i$ 's lo son). Como  $I$  es bilateral, entonces cada  $d^{-1}y_i d \in I$ , de modo que existen  $\beta_{i\ell} \in D$  tales que  $d^{-1}y_i d = \sum_{\ell=1}^m \beta_{i\ell} y_\ell$ , o equivalentemente

$$\begin{aligned} (1 \otimes v_i) - \sum_{j=m+1}^n (d^{-1}\alpha_{ij}d)(1 \otimes v_j) &= \sum_{\ell=1}^m \beta_{i\ell}(1 \otimes v_\ell) \\ &\quad - \sum_{\ell=1}^m \beta_{i\ell} \cdot \sum_{j=m+1}^n \alpha_{\ell j}(1 \otimes v_j). \end{aligned}$$

Como los  $1 \otimes v_i$ 's forman una  $D$ -base, comparamos los coeficientes y concluimos que  $\beta_{i\ell} = \delta_{i\ell}$  (la delta de Kronecker) y que  $d^{-1}\alpha_{ij}d = \alpha_{ij}$  para todo  $i, j$ ; por lo que  $\alpha_{ij} \in k$ . Es decir,  $I$  está generado por elementos en  $K$  como  $k$ -módulo y, como  $K$  es un cuerpo, necesariamente  $I \cap K = K$  de modo que  $I = D \otimes_k K$ . Esto prueba la simplicidad.  $\square$

**Teorema 10.69:** Sea  $k$  un cuerpo y  $A$  una  $k$ -álgebra de dimensión finita. Entonces  $A$  es central simple sobre  $k$  si y sólo si existe una extensión finita  $K/k$  tal que  $A \otimes_k K$  se escinde sobre  $K$ . En consecuencia, la dimensión de toda álgebra de Azumaya es un cuadrado.

DEMOSTRACIÓN:  $\Leftarrow$ . Se sigue del lema anterior.

$\Rightarrow$ . Del lema anterior se sigue que  $A \otimes_k k^{\text{alg}}$  es de Azumaya sobre  $k^{\text{alg}}$ , luego se escinde por el teorema de Wedderburn-Artin, es decir,  $A \otimes_k k^{\text{alg}} \cong \text{Mat}_n(k^{\text{alg}})$  para algún  $n$ . Fijando este isomorfismo, denotemos por  $e_1, \dots, e_{n^2}$  la  $k^{\text{alg}}$ -base canónica de  $A \otimes_k k^{\text{alg}}$ . Nótese que las inclusiones  $K \hookrightarrow k^{\text{alg}}$  inducen inclusiones  $A \otimes_k K \hookrightarrow A \otimes_k k^{\text{alg}}$ , así que existe una extensión finita  $K/k$  suficientemente grande de modo que cada  $e_i \in A \otimes_k K$

y tal que, en la identidad

$$e_i e_j = \sum_{\ell=1}^{n^2} a_{i,j,\ell} e_\ell \in A \otimes_k k^{\text{alg}}$$

se satisfaga que  $a_{ij\ell} \in K$ . Entonces se sigue que el isomorfismo fijado se restringe a un isomorfismo  $A \otimes_k K \cong \text{Mat}_n(K)$  como se quería probar.  $\square$

**Definición 10.70:** Sea  $k$  un cuerpo y  $A$  una  $k$ -álgebra de Azumaya. Un *cuerpo de escisión* para  $A$  es una extensión  $K/k$  tal que  $A \otimes_k K$  se escinde. El *grado* de  $A$  es  $\deg A := \sqrt{\dim_k A}$ .

**Proposición 10.71 (Noether-Köthe):** Sea  $k$  un cuerpo y  $A$  una  $k$ -álgebra de Azumaya. Entonces  $A$  posee un cuerpo de escisión separable (y cuya extensión es finita) y, por tanto, también posee un cuerpo de escisión  $K/k$  tal que la extensión es finita y de Galois.

DEMOSTRACIÓN: Supongamos, por contradicción, que para toda extensión finita separable  $K/k$  se cumple que  $A \otimes_k K$  no se escinde. Fijemos unas clausuras algebraicas y separables con respectivas inclusiones  $k \subseteq k^{\text{sep}} \subseteq k^{\text{alg}}$ . Empleando que  $k^{\text{sep}}$  es la unión de las subextensiones separables finitas, vemos que  $A \otimes_k k^{\text{sep}}$  no se escinde sobre  $k^{\text{sep}}$  y, por el teorema de Wedderburn-Artin, existe  $D \supset k^{\text{sep}}$  de división tal que  $A \otimes_k k^{\text{sep}} \cong \text{Mat}_n(D)$ . Sea  $d > 1$  el grado de  $D$  sobre  $k^{\text{sep}}$ , entonces  $D \otimes_{k^{\text{sep}}} k^{\text{alg}} \cong \text{Mat}_d(k^{\text{alg}})$ .

Denotemos por  $L := k^{\text{alg}}$  y  $K := k^{\text{sep}}$ . El isomorfismo de  $L$ -espacios vectoriales  $\text{Mat}_d(L) \cong L^{d^2}$  identifica los elementos de  $\text{Mat}_d(L)$  como puntos  $L$ -valuados del espacio afín  $\mathbb{A}^{d^2}$ , mientras que los puntos  $K$ -valuados se identifican con elementos de  $D$ . Como  $D$  es de división, entonces sus elementos vistos dentro  $\text{Mat}_d(L)$  son matrices invertibles, vale decir, de determinante no nulo. Así pues, considere el polinomio determinante  $P(\mathbf{x}) \in K[x_1, \dots, x_{d^2}]$ , que siempre existe pues sus coeficientes son solo  $\pm 1$ , y nótese que el hiperplano  $H := \mathbf{V}(P) \subseteq \mathbb{A}_K^{d^2}$  es tal que su único punto  $K$ -racional es el origen. Pero esto es absurdo, pues los puntos  $K$ -racionales de  $H$  forman un subconjunto Zariski-denso; así que hay algún cuerpo de escisión separable cuya extensión es finita. El «por lo tanto» se sigue de tomar la clausura normal de alguno de los cuerpos de escisión obtenidos.  $\square$

## 10.5 Álgebras cuaterniónicas II

**Definición 10.72:** Sea  $k$  un cuerpo de car  $k \neq 2$ , y sean  $a, b \in k^\times$  fijados. Se le llama **álgebra cuaterniónica** inducida por  $a, b$ , denotada  $Q_k(a, b)$ , a la  $k$ -álgebra (asociativa) de dimensión 4 con base (ordenada)<sup>2</sup>  $(1, i, j, ij)$  definida por

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

La cuadrupla ordenada  $(1, i, j, ij)$  se dice **base cuaterniónica**. Obviaremos el subíndice  $k$  de no haber ambigüedad. Los elementos de  $Q(a, b)$  se dicen **cuaterniones**. Se dice que un cuaternión  $q \in Q(a, b)$  es **puro** si  $q^2 \in k$ , pero  $q \notin k$ .

Para todo cuaternión  $q := x + yi + zj + wij$ , se define la involución o **conjugación**:

$$\bar{q} := x - yi - zj - wij,$$

y se define la **norma (cuaterniónica)**  $N: Q(a, b) \rightarrow k$  como  $N(q) := q \cdot \bar{q}$ , vale decir:

$$N(q) = x^2 - ay^2 - bz^2 + abw^2.$$

Nótese que, efectivamente, las álgebras cuaterniónicas aquí definidas corresponden a las álgebras definidas anteriormente. En efecto, exigir que  $i^2 = a, j^2 = b$  corresponde a realizar un  $b$ -duplicado de un  $a$ -duplicado de  $k$ , donde comenzamos con la involución identidad sobre  $k$ . Por el teorema 10.57 vemos que las álgebras cuaterniónicas, aquí definidas, están hechas para ser asociativas, pero probablemente no conmutativas.

Se suele denotar el álgebra cuaterniónica como  $(a, b)$  a secas. Esta notación tiene la ventaja de que sugiere que  $(-, -)$  se comporta como una forma bilineal, y el caso es parecido. Efectivamente es simétrico y es fácil probar que dado  $u \in k^\times$  se cumple que  $Q(a, b) \cong Q(u^2a, b)$ ; de modo que esta definido salvo cuadrados.

Es fácil probar:

**Lema 10.73:** Sea  $k$  un cuerpo de car  $k \neq 2$ . Sea  $(H, N)$  una  $k$ -álgebra cuaterniónica con  $N$  su norma. Entonces, un cuaternión  $q \in H$  es invertible syss  $N(q) \neq 0$ . Así,  $H$  es de división syss  $N$  no tiene ceros no triviales.

**Ejemplo.** Sea  $k = R$  un cuerpo formalmente real. La  $R$ -álgebra cuaterniónica de Hamilton es  $Q(-1, -1)$  y es de división.

<sup>2</sup>En general denotaremos una base cuaterniónica con fuentes derechas ( $i$  en lugar de  $i$ ) para no confundir con los índices de una sumatoria.

**Ejemplo 10.74:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$  y sea  $b \in k^\times$  arbitrario. Definamos las matrices:

$$I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}, \quad IJ = \begin{bmatrix} 0 & b \\ -1 & b \end{bmatrix}.$$

Entonces  $\text{Mat}_2(k)$  es una  $k$ -álgebra (asociativa) de dimensión 4 con base  $(\text{Id}, I, J, IJ)$ . Es fácil notar que esta es una base cuaterniónica que prueba el isomorfismo  $\text{Mat}_2(k) \cong \mathbb{Q}_k(1, b)$ .  $\lrcorner$

Así pues, hemos visto que las álgebras cuaterniónicas  $\mathbb{Q}_k(1, b)$  son de Azumaya y se escinden.

**Proposición 10.75:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ , y considere la  $k$ -álgebra cuaterniónica  $\mathbb{Q}(a, b)$ . Son equivalentes:

1.  $\mathbb{Q}(a, b)$  se escinde.
2.  $\mathbb{Q}(a, b)$  no es de división.
- 2'. La norma  $N: \mathbb{Q}(a, b) \rightarrow k$  tiene un cero no trivial.
3.  $b = \text{Nm}_{L/k}(\gamma)$  para algún  $\gamma \in L := k(\sqrt{a})$ .

DEMOSTRACIÓN:  $1 \implies 2$ . Basta verificar que  $\text{Mat}_2(k)$  no es de división (¿por qué es el caso?).

Ya vimos  $2 \iff 2'$ .

$2' \implies 3$ . Sea  $q = x + yi + zj + wij \neq 0$  un cuaternión tal que  $N(q) = 0$ , es decir

$$x^2 - ay^2 - bz^2 + abw^2 = 0 \iff b(z^2 - aw^2) = x^2 - ay^2.$$

Ahora nótese que si  $a$  es un cuadrado, trivialmente  $b = \text{Nm}_{L/k}(b)$  pues  $L = k$ . Si no, entonces  $z^2 - aw^2 \neq 0$  y vemos que

$$b = \text{Nm}_{L/k} \left( \frac{x + y\sqrt{a}}{z + w\sqrt{a}} \right).$$

$3 \implies 1$ . Si  $a$  es un cuadrado, entonces trivialmente  $\mathbb{Q}(a, b) \cong \mathbb{Q}(1, b)$ . Si no, como  $b$  es una norma en  $L/k$ , también  $b^{-1}$  lo es, digamos  $b^{-1} = r^2 - as^2$  para  $r, s \in k$ . Sea  $u := ri + sij \in \mathbb{Q}(a, b)$ , entonces un par de cálculos dan

$$u^2 = br^2 - abs^2 = 1, \quad ui = -iu.$$

De modo que  $v := (1 + a)i + (1 - a)ui$  satisface que  $uv = -vu$  y  $v^2 = 4a^2$ . Así pues,  $(1, u, v, uv)$  es una base cuaterniónica de  $\mathbb{Q}(a, b)$  que prueba que  $\mathbb{Q}(a, b) \cong \mathbb{Q}(1, 4a^2)$ .  $\square$

**Lema 10.76:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$  y  $D$  una  $k$ -álgebra central de división y de  $\dim_k D = 4$ . Si  $D$  contiene una subálgebra isomorfa a una extensión cuadrática  $k(\sqrt{a}) \neq k$  no trivial de  $k$ , entonces  $D \cong Q(a, b)$  para algún  $b \in k^\times$ .

DEMOSTRACIÓN: Por hipótesis, existe  $q \in D$  tal que  $q^2 = a$ . Como  $q \notin Z(D)$ , entonces  $\varphi: D \rightarrow D$  dado por  $\varphi(x) := q^{-1}xq$  es un  $k$ -automorfismo de orden 2. Como automorfismo  $k$ -lineal, entonces es diagonalizable y claramente  $\varphi(1) = 1$ , luego es fácil probar que  $-1$  es el otro valor propio (empleando que  $\varphi \circ \varphi = \text{Id}_D$ ). Así existe  $r$  tal que  $\varphi(r) = -r$  o, equivalentemente,  $qr + rq = 0$ ; de esto se deduce que  $B := (1, q, r, qr)$  es una base (ordenada) de  $D$ . Nótese que  $B$  se fija por  $x \mapsto r^{-2}xr^2$ , de modo que  $r^2$  está en el centro y así  $r^2 = b \in k^\times$ , de modo que  $B$  es una base cuaterniónica.  $\square$

Como ejercicio: ¿realmente se requiere que la característica de  $k$  sea  $\neq 2$ ?

**Proposición 10.77:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ . Toda  $k$ -álgebra central de división  $D$  de  $\dim_k D = 4$  es cuaterniónica.

DEMOSTRACIÓN: Sea  $d \in D \setminus k$ , luego  $\{1, d, d^2, d^3, d^4\}$  es un conjunto  $k$ -linealmente dependiente y así, existe  $f(x) \in k[x]$  no constante tal que  $f(d) = 0$ . Como  $D$  es de división, entonces no posee divisores de cero, de modo que podemos suponer que  $f$  es irreducible. De modo que existe un monomorfismo  $k[x]/(f(x)) \hookrightarrow D$ , de modo que  $[k(d) : k]$  tiene que ser 1, 2 o 4; pero no es 1 pues  $d \notin k$ , ni tampoco 4 puesto que de lo contrario  $D$  sería conmutativo (no lo es, pues  $Z(D) \neq D$ ), así que debe ser 2 y concluimos por el lema.  $\square$

Uno también podría comenzar por tratar de definir las álgebras cuaterniónicas de manera más natural como las álgebras centrales simples de dimensión 4. Esto conlleva a lo que GILLE y SZAMUELY [0] denominan *álgebras cuaterniónicas generalizadas* dadas por una base  $(1, i, j, ij)$  tal que:

$$i^2 + i = a, \quad j^2 = b, \quad ij + ji = j.$$

Este objeto suele denotarse  $[a, b]$  y se estudia en SCHARLAU [0], §8.11.

**Proposición 10.78:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ , sea  $A$  una  $k$ -álgebra cuaterniónica y  $a \in k^\times \setminus k^{\times 2}$ . Son equivalentes:

1.  $A \cong Q(a, b)$  para algún  $b \in k^\times$ .
2.  $A \otimes_k k(\sqrt{a})$  se escinde sobre  $k(\sqrt{a})$ .

3.  $A$  contiene una  $k$ -subálgebra isomorfa a  $k(\sqrt{a})$ .

DEMOSTRACIÓN: En la demostración denotaremos  $L := k(\sqrt{a})$ .

1  $\implies$  2. Basta notar que  $Q_k(a, b) \otimes_k L \cong Q_L(a, b) \cong Q_L(1, b)$ , donde el último isomorfismo viene de que  $a$  es un cuadrado en  $L$ , por tanto, se escinde sobre  $L$  como se quería ver.

2  $\implies$  3. Si  $A \cong \text{Mat}_2(k)$ , entonces se elige un isomorfismo  $\text{Mat}_2(k) \cong Q(1, a)$  y se verifica trivialmente. Si no,  $A$  no se escinde y extendemos la norma a  $A \otimes_k L$  por cambio de base. Como  $A \otimes L$  se escinde, la proposición 10.75 nos permite ver que existen  $q_0, q_1 \in A$  no ambos nulos tales que  $N(q_0 + q_1\sqrt{a}) = 0$ . Sea  $\beta$  la forma bilineal sobre  $A \otimes L$  asociada a  $N$  (que satisface que  $\beta(\gamma, \gamma) = N(\gamma)$ ), entonces

$$0 = \beta(q_0 + q_1\sqrt{a}, q_0 + q_1\sqrt{a}) = N(q_0) + aN(q_1) + 2\beta(q_0, q_1)\sqrt{a},$$

de modo que, como  $k$ -espacio vectorial, implica que

$$N(q_0) = -aN(q_1), \quad 2\beta(q_0, q_1) = q_0\bar{q}_1 + \bar{q}_0q_1 = 0,$$

como  $A$  no se escinde,  $N(q_0) \neq 0 \neq N(q_1)$  y  $q_2 := q_0\bar{q}_1 \in A$  satisface que

$$q_2^2 = q_0\bar{q}_1q_0\bar{q}_1 = -q_0\bar{q}_0q_1\bar{q}_1 = -N(q_0)N(q_1) = aN(q_1)^2,$$

así pues  $q := q_2N(q_1)^{-1} \in A$  satisface que  $q^2 = a$ , de modo que  $k(q) \cong k(\sqrt{a}) \subseteq A$ .

3  $\implies$  1. Si  $A$  se escinde es trivial, sino basta aplicar el lema 10.76.  $\square$

**Proposición 10.79:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ . Sea  $Q(a, b)$  una  $k$ -álgebra cuaterniónica y  $L := k(\sqrt{a})$ . Entonces para todo cuaternión  $q \in Q(a, b)$  y todo  $L$ -isomorfismo  $\varphi: Q(a, b) \otimes L \rightarrow \text{Mat}_2(L)$  se tiene que  $N(q) = \det(\varphi(q))$ .

DEMOSTRACIÓN: Nótese que  $\det(\varphi(q))$  no depende de la elección de  $L$ -isomorfismo, esto se debe a la invarianza del determinante. Así pues, basta considerar el encaje  $Q(a, b) \otimes L \rightarrow \text{Mat}_2(L)$  que manda  $j \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$  y notar que

$$\begin{aligned} \begin{bmatrix} x & y \\ z & w \end{bmatrix} &= \left(\frac{x+w}{2}\right) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \left(\frac{x-w}{2}\right) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + \left(\frac{y+z}{2}\right) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ &\quad + \left(\frac{y-z}{2}\right) \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \end{aligned}$$

de modo que se tiene que:

$$\begin{aligned} N\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) &= \left(\frac{x+w}{2}\right)^2 - \left(\frac{x-w}{2}\right)^2 - \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 \\ &= xw - yz = \det\begin{pmatrix} x & y \\ z & w \end{pmatrix}. \end{aligned} \quad \square$$

**§10.5.1 Allegro: interpretación geométrica.** En ésta subsección veremos cómo vincular las álgebras cuaterniónicas a un objeto geométrico y culminaremos con un teorema de Witt que señala que éste objeto captura toda la información del álgebra. El lector incómodo puede considerar que trabajamos con métodos clásicos (de la escuela de Weil-Zariski), o bien que trabajamos con esquemas.

**Definición 10.80:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ . Definimos la **cónica asociada** a la álgebra  $A := Q_k(a, b)$  como la curva plana proyectiva

$$C_k(A) = C_k(a, b) := \mathbf{V}_+(ax^2 + by^2 - z^2) \subseteq \mathbb{P}_k^2.$$

Nótese que los cambios de base permiten ver que  $C_k(a, b)$  es independiente de la elección de la base cuaterniónica de  $A$  (¿por qué?).

**Proposición 10.81:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ . La álgebra cuaterniónica  $Q_k(a, b)$  se escinde si y sólo si su cónica asociada  $C_k(a, b)$  posee un punto  $k$ -racional.

**Ejemplo.** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ . Para todo  $a \in k \setminus \{0, 1\}$  se tiene que la cónica proyectiva  $C/k: ax^2 + (1-a)y^2 = z^2$  admite el punto  $k$ -racional  $(1, 1, 1)$ , de modo que el álgebra cuaterniónica  $Q_k(a, 1-a)$  se escinde.

Veamos dos aplicaciones sencillas:

**Teorema 10.82:** Sea  $k = \mathbb{F}_q$  un cuerpo finito con  $2 \nmid q$ . Toda  $k$ -álgebra cuaterniónica se escinde.

**DEMOSTRACIÓN:** Por la proposición anterior queremos ver que la cónica proyectiva  $C/k: ax^2 + by^2 = z^2$  posee un punto  $k$ -racional. Para ello fijemos  $z = 1$  y notemos que, como el grupo de unidades  $k^\times$  es cíclico y de  $q-1$  elementos, entonces posee exactamente  $(q-1)/2$  elementos de orden 2, es decir,  $k$  posee  $\ell := 1 + (q-1)/2$  cuadrados (contando el 0). Luego, el conjunto

$\{ax^2 : x \in k\}$  tiene  $\ell$  elementos y análogamente con el conjunto  $\{1 - by^2 : y \in k\}$ ; por lo que los conjuntos no pueden ser disjuntos.  $\square$

**Teorema 10.83:** Sea  $k$  un cuerpo de car  $k \neq 2$  y sea  $t$  una indeterminada sobre  $k$ .

1. La  $k$ -álgebra  $\mathbb{Q}(a, b)$  se escinde (sobre  $k$ ) syss  $\mathbb{Q}(a, b) \otimes_k k(t)$  se escinde (sobre  $k(t)$ ).
2. La  $k(t)$ -álgebra  $\mathbb{Q}_{k(t)}(a, t)$  se escinde syss  $a$  es un cuadrado en  $k$ .

DEMOSTRACIÓN:

1.  $\implies$ . Trivial.

$\Leftarrow$ . Por la proposición 10.81 sea  $[f : g : h]$  un punto  $k(t)$ -racional de la cónica  $C_{k(t)}(a, b)$ , es decir,  $af^2 + bg^2 = h^2$ . Si  $k$  es finito, ya sabemos que  $\mathbb{Q}_k(a, b)$  se escinde, así que supondremos que es infinito. Como  $k$  es infinito, es fácil probar que existe un punto  $u \in k$  tal que todas las funciones racionales  $f(u), g(u), h(u)$  están bien definidas y alguna es no nula, de modo que  $af(u)^2 + bg(u)^2 = h(u)^2$  y  $[f(u) : g(u) : h(u)]$  es un punto  $k$ -racional de  $C_k(a, b)$ .

2.  $\Leftarrow$ . Trivial.

$\implies$ . Nuevamente, sea  $[f : g : h]$  un punto  $k(t)$ -racional de  $C_{k(t)}(a, t)$ . Limpiando denominadores, podemos suponer que  $f(t), g(t), h(t) \in k[t]$ . Nótese que si  $t$  divide a dos de tres elementos, entonces divide al tercero por la ecuación  $af^2 + tg^2 = h^2$  (basta mirarlo mód  $t^2$ ), de modo que suponiendo que  $f, g, h$  son coprimos en conjunto, vemos que a lo más uno es divisible por  $t$ . Evaluando en  $t = 0$  obtenemos que  $af(0)^2 = g(0)^2$  y por divisibilidad  $f(0) \neq 0$ , luego  $a = (g(0)/f(0))^2$  es un cuadrado.  $\square$

Un último ejemplo:

**Ejemplo 10.84:** Sea  $k$  un cuerpo de car  $k \neq 2$ , y sea  $H := \mathbb{Q}_k(a, b)$  una  $k$ -álgebra cuaterniónica. Entonces  $H \otimes_k K(C(H))$  se escinde sobre  $K(C(H)) =: K$ ; en efecto, la curva proyectiva  $C/K : aX^2 + bY^2 = Z^2$  posee el punto  $L$ -racional  $[\alpha : \beta : 1]$ , donde  $\alpha, \beta$  son las imágenes de  $x, y$  del epimorfismo cociente:

$$k[x, y] \longrightarrow \frac{k[x, y]}{(ax^2 + by^2 - 1)} \cong K.$$



Al punto  $[\alpha : \beta : 1]$  le llamamos **Weil-genérico**.<sup>3</sup> ┘

**Lema 10.85:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$  y sea  $Q(a, b)$  una  $k$ -álgebra cuaterniónica. Para todo  $c \in k^\times$  tal que  $c = \text{Nm}_{L/k}(\gamma)$  para algún  $\gamma \in L := k(\sqrt{a})$ , se cumple que  $Q(a, b) \cong Q(a, bc)$ .

DEMOSTRACIÓN: Como  $c = u^2 - av^2$  para algunos  $u, v \in k$ , entonces  $c = N(q)$  donde  $q := u + vi + 0j + 0ij$ , y definimos  $J := q \cdot j = uj + vij$ . Nótese que  $J$  es un cuaternión puro, pues satisface lo siguiente:

$$i \cdot J + J \cdot i = 0, \quad J^2 = -N(J) = -N(q)N(j) = bc,$$

de modo que  $(1, i, J, iJ)$  es una base cuaterniónica de  $Q(a, b)$  que verifica el enunciado. □

**Teorema 10.86 (Witt):** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$  y sean  $H_i := Q(a_i, b_i)$  un par de álgebras cuaterniónicas con  $C_i := C_k(H_i)$ . Entonces  $H_1 \cong H_2$  (en  $\text{Alg}_k$ ) syss  $K(C_1) \cong K(C_2)$  (en  $\text{Fld}_k$ ).

DEMOSTRACIÓN:  $\implies$ . Trivial, pues ya vimos que  $H_1 \cong H_2$  implica  $C_1 \cong C_2$ .

$\impliedby$ . Si  $H_2$  se escinde, entonces  $K(C_2)$  es una extensión trascendente simple de  $k$ , de modo que  $H_1 \otimes K(C_2) \cong H_1 \otimes k(t)$ ; por el ejemplo 10.84, sabemos que  $H_1 \otimes K(C_1)$  se escinde, luego  $H_1 \otimes k(t)$  también y concluimos que  $H_1$  se escinde por el teorema 10.83.

Si  $H_1, H_2$  no se escinden, entonces  $a_1$  no es un cuadrado en  $k^\times$  y  $H_1 \otimes L$  se escinde sobre  $L := k(\sqrt{a_1})$ . Denotemos  $C := C_1$  y  $L(C) := L \otimes K(C)$ , el cual es el cuerpo de funciones racionales de la curva  $C_L = C \times_k \text{Spec } L$  dada por cambio de base. Como  $H_1 \otimes_k L$  se escinde, vemos que  $C_L$  es isomorfa a  $\mathbb{P}_L^1$  y  $L(C) \cong L(t)$  es trascendente simple. Como  $H_2 \otimes_k L(C)$  se escinde sobre  $L(C)$ , entonces por el teorema 10.83, vemos que  $H_2 \otimes L$  se escinde, de modo que  $H_2 \cong Q(a_1, c)$  por la proposición 10.78. Como  $H_2 \otimes_k K(C)$  se escinde sobre  $K(C)$ , entonces  $c = \text{Nm}_{L(C)/K(C)}(f)$  para algún  $f \in L(C)$ .

Nuestro objetivo será calcular explícitamente susodicho  $f$ , para ello comenzamos por invocar la siguiente sucesión exacta

$$0 \longrightarrow L(C)^\times / L^\times \xrightarrow{\text{div}} \text{Div}(C_L) \xrightarrow{\text{deg}} \mathbb{Z} \longrightarrow 0.$$

---

<sup>3</sup>Efectivamente, éste punto es genérico en el sentido de que su clausura es toda la curva. Hacemos la aclaración para que no se confunda con los puntos genéricos en sentido de Grothendieck.

¿Por qué? GILLE  
y SZAMUELY [0,  
págs. 10-11].

El grupo  $\text{Gal}(L(C)/K(C)) = \{1, \sigma\}$  actúa sobre ésta sucesión exacta.  $\square$

### §10.5.2 Álgebras bicuaterniónicas.

**Lema 10.87:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ . Para todos  $a, b, b' \in k^\times$  se tiene que  $Q(a, b) \otimes_k Q(a, b') \cong Q(a, bb') \otimes_k \text{Mat}_2(k)$ .

DEMOSTRACIÓN: Sean  $(1, i, j, ij)$  y  $(1, i', j', i'j')$  bases cuaterniónicas de  $Q(a, b)$  y  $Q(a, b')$  resp. Considere los  $k$ -subespacios:

$$\begin{aligned} A_1 &:= k\langle 1 \otimes 1, i \otimes 1, j \otimes j', ij \otimes j' \rangle, \\ A_2 &:= k\langle 1 \otimes 1, 1 \otimes j', i \otimes i'j', (-b'i) \otimes i' \rangle \end{aligned}$$

de  $Q(a, b) \otimes Q(a, b')$ . Sobre la base es fácil verificar que  $A_1, A_2$  son cerrados bajo el producto, de modo que son subálgebras de  $Q(a, b) \otimes Q(a, b')$  y calculando los cuadrados de  $\{i \otimes 1, j \otimes j'\}$  y  $\{1 \otimes j', i \otimes i'j'\}$  vemos que  $A_1 \cong Q(a, bb')$  y  $A_2 \cong Q(b', -a^2b') \cong Q(b', -b')$ . Es fácil verificar que  $A_2$  se escinde pues la curva  $b'x^2 - b'y^2 = z^2$  posee el punto  $k$ -racional  $[1 : 1 : 0]$ .

Finalmente, es sencillo comprobar que  $A_1 \otimes_k A_2$  es de hecho isomorfo a  $Q(a, b) \otimes Q(a, b')$  empleando argumentos de dimensión.  $\square$

**Corolario 10.87.1:** Sea  $k$  un cuerpo de  $\text{car } k \neq 2$ . Se cumple que  $Q(a, b) \otimes Q(a, b) \cong \text{Mat}_4(k)$ .

DEMOSTRACIÓN: Basta notar que

$$\begin{aligned} Q(a, b) \otimes Q(a, b) &\cong Q(a, bb) \otimes \text{Mat}_2(k) \cong Q(a, 1) \otimes \text{Mat}_2(k) \\ &\cong \text{Mat}_2(k) \otimes_k \text{Mat}_2(k) \cong \text{Mat}_4(k). \end{aligned} \quad \square$$

### Parte III.

---

## MÉTODOS (CO)HOMOLÓGICOS Y ÁLGEBRA NO CONMUTATIVA

---

En esta parte tomamos como prerrequisito el lenguaje básico de categorías (objeto generador, inyectivo, proyectivo; límites inversos, directos, filtrados; flechas adjuntas, etc.) y los métodos propios del álgebra homológica para deducir resultados estructurales más potentes. Así mismo, hay un par de secciones en las que enriquecemos el lenguaje algebraico con estructuras topológicas; no obstante, hay que ser cuidadoso al llevar a cabo estas «generalizaciones», ya que los análogos de los teoremas de isomorfismos pueden fallar en condiciones generales; un arreglo parcial resulta de imponer condiciones de finitud más fuertes, como compacidad, a los objetos.

Solo por ser ligeramente más enfático, los anillos sin hipótesis de conmutatividad se denotarán con letras griegas mayúsculas (e.g.,  $\Lambda, \Gamma$ , etc.), mientras que las letras romanas mayúsculas usuales (e.g.,  $A, B, C$ , etc.) se reservarán para dominios.



# 11

---

## (Co)homología de módulos

---

En el capítulo de categorías abelianas ya vimos el protagonismo que la categoría de módulos posee. Ahora comenzamos a estudiar y aplicar de manera más concreta nuestra teoría, sin nunca dejar de lado las flechas por supuesto.

### 11.1 La categoría de módulos

**Definición 11.1:** Una *sucesión exacta corta* en una categoría abeliana  $\mathcal{C}$  es una sucesión exacta de la forma

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0. \quad (11.1)$$

Decimos que la sucesión (11.1) *se escinde* si  $g$  es una retracción, i.e., si existe  $C \xrightarrow{h} B$  tal que  $h \circ g = 1_C$ .

**Proposición 11.2:** Si una sucesión exacta corta (11.1) se escinde, entonces  $B \cong A \oplus C$ .

Veamos primero un par de lemas para practicar el uso de flechas:

**Lema 11.3 (corto de los cinco):** Dado el siguiente diagrama conmutativo de  $\Lambda$ -módulos:

$$\begin{array}{ccccccc}
0 & \longrightarrow & A & \xrightarrow{\psi} & B & \xrightarrow{\phi} & C \longrightarrow 0 \\
& & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\
0 & \longrightarrow & A' & \xrightarrow{\psi'} & B' & \xrightarrow{\phi'} & C' \longrightarrow 0
\end{array}$$

donde las filas son exactas. Entonces:

1. Si  $\alpha$  y  $\gamma$  son monomorfismos, entonces  $\beta$  es monomorfismo.
2. Si  $\alpha$  y  $\gamma$  son epimorfismos, entonces  $\beta$  es epimorfismo.
3. Si  $\alpha$  y  $\gamma$  son isomorfismos, entonces  $\beta$  es isomorfismo.

DEMOSTRACIÓN:

1. Sea  $\mathbf{b} \in \ker \beta$ , luego  $\vec{0} = \phi'(\beta(\mathbf{b})) = \gamma(\phi(\mathbf{b}))$ , luego  $\phi(\mathbf{b}) \in \ker \gamma = 0$ , así que  $\mathbf{b} \in \ker \phi = \text{Img } \psi$  y existe  $\mathbf{a} \in A$  tal que  $\psi(\mathbf{a}) = \mathbf{b}$ . Por ende  $\beta(\psi(\mathbf{a})) = \psi'(\alpha(\mathbf{a}))$ , pero  $\psi', \alpha$  son monomorfismos, así que  $\mathbf{a} = \vec{0}$ .
2. Sea  $\mathbf{x} \in B'$ , entonces puesto que  $\phi, \gamma$  son epimorfismos, entonces existe  $\mathbf{y} \in B$  tal que  $\phi'(\mathbf{x}) = \gamma(\phi(\mathbf{y}))$ , luego  $\phi'(\mathbf{x} - \beta(\mathbf{y})) = \vec{0}$ , luego  $\mathbf{x} - \beta(\mathbf{y}) \in \ker(\phi') = \text{Img}(\psi')$ , luego puesto que  $\alpha$  es epimorfismo  $\mathbf{x} - \beta(\mathbf{y}) = \psi'(\alpha(\mathbf{a})) = \beta(\psi(\mathbf{a}))$ . Llamando  $\mathbf{z} := \psi(\mathbf{a})$ , se tiene que  $\mathbf{x} = \beta(\mathbf{y} + \mathbf{z})$ .
3. Consecuencia de las anteriores. □

Siguiendo técnicas similares se pueden demostrar los siguientes lemas:

**Lema 11.4 (fuerte de los cuatro):** Dado el siguiente diagrama conmutativo de  $\Lambda$ -módulos:

$$\begin{array}{ccccccc}
M & \longrightarrow & A & \xrightarrow{\zeta} & B & \longrightarrow & N \\
\downarrow \mu & & \downarrow \alpha & & \downarrow \beta & & \downarrow \nu \\
M' & \longrightarrow & A' & \xrightarrow{\xi} & B' & \longrightarrow & N'
\end{array}$$

con filas exactas,  $\mu$  epimorfismo y  $\nu$  monomorfismo. Entonces:

$$\ker \gamma = \zeta[\ker \beta], \quad \text{Img } \beta = \xi^{-1}[\text{Img } \gamma].$$

**Lema 11.5 (de los cinco):** Dado el siguiente diagrama conmutativo de  $\Lambda$ -módulos:

$$\begin{array}{ccccccccc}
A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & A_4 & \longrightarrow & A_5 \\
\downarrow \alpha_1 & & \downarrow \alpha_2 & & \downarrow \alpha_3 & & \downarrow \alpha_4 & & \downarrow \alpha_5 \\
B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & B_4 & \longrightarrow & B_5
\end{array}$$

con filas exactas se cumplen:

1. Si  $\alpha_1$  es epimorfismo y  $\alpha_2, \alpha_4$  son monomorfismos, entonces  $\alpha_3$  es monomorfismo.
2. Si  $\alpha_5$  es monomorfismo y  $\alpha_2, \alpha_4$  son epimorfismos, entonces  $\alpha_3$  es epimorfismo.
3. Si  $\alpha_1, \alpha_2, \alpha_4, \alpha_5$  son isomorfismos, entonces  $\alpha_3$  es isomorfismo.

### §11.1.1 Módulos proyectivos.

**Proposición 11.6:** Sea  $\Lambda$  un anillo. Todo  $\Lambda$ -módulo libre es proyectivo y, en consecuencia, la categoría  $\text{Mod}_\Lambda$  tiene suficientes proyectivos.

DEMOSTRACIÓN: Nótese que  $\Lambda$ , visto como  $\Lambda$ -módulo, es proyectivo; luego  $A^{\oplus \kappa}$  también (por la proposición ??) de modo que efectivamente todo módulo libre es proyectivo. Dado un módulo cualquiera  $M$ , basta considerar a  $M$  como conjunto y construir  $F$  el módulo libre de base  $M$  para tener de forma inmediata un epimorfismo  $F \rightarrow M$  donde  $F$  es proyectivo.  $\square$

**Proposición (AE) 11.7:** Sea  $P$  un  $\Lambda$ -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  $\Lambda$ -módulo libre. Más aún, si  $P$  es finitamente generado, entonces es el sumando directo de un  $\Lambda$ -módulo libre de dimensión finita.

DEMOSTRACIÓN:  $1 \implies 2$ . En la sucesión,  $p$  es suprayectivo, luego basta considerar el siguiente diagrama conmutativo:

$$\begin{array}{ccc}
 & P & \\
 \swarrow \text{dashed} & \downarrow \text{Id}_P & \\
 N & \xrightarrow[p]{} & P
 \end{array}$$

para concluir.

2  $\implies$  3. Sea  $S$  un sistema generador de  $P$ , y sea  $F := \Lambda^{\oplus S}$ , es decir, el  $\Lambda$ -módulo libre que posee a  $S$  como base, de modo que  $\iota: S \rightarrow P$  induce trivialmente un epimorfismo  $p: F \rightarrow P$ . 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:

$$\begin{array}{ccc}
 F & \longleftarrow & P \\
 & & \downarrow f \\
 M & \xrightarrow[p]{} & N
 \end{array}$$

como  $F = P \oplus P'$  podemos definir  $\hat{f}: F \rightarrow N$  tal que se anule en  $P'$  y coincida con  $f$  en  $P$ . Sea  $X = \{\mathbf{x}_i + \mathbf{y}_i\}_{i \in I}$  una base de  $F$ , donde  $\mathbf{x}_i \in P$  e  $\mathbf{y}_i \in P'$  para todo  $i \in I$ . Podemos definir una función  $h^*: X \rightarrow M$  donde a cada  $\mathbf{x}_i + \mathbf{y}_i$  le asigne un elemento de  $p^{-1}[\{\hat{f}(\mathbf{x}_i)\}]$  (el cuál existe porque  $p$  es suprayectivo), que luego, por definición de módulo libre, se extiende a un homomorfismo de  $\Lambda$ -módulos  $h: F \rightarrow M$ . Finalmente, queda al lector comprobar que efectivamente  $g := \iota \circ h \circ p: P \rightarrow N$  hace conmutar el diagrama.  $\square$

Un corolario particularmente útil es el siguiente:

**Teorema (AE) 11.8:** Los  $\Lambda$ -módulos proyectivos son planos.

**Proposición (AE) 11.9:** El producto tensorial de finitos módulos proyectivos es proyectivo.

**Proposición (AE) 11.10 (lema de las bases duales):** Sea  $P$  un  $\Lambda$ -módulo. Son equivalentes:

1.  $P$  es proyectivo.



2. Existe  $\{\mathbf{x}_i\}_{i \in I}$  en  $P$  y  $\{f_i\}_{i \in I}$  en  $\text{Hom}_\Lambda(P, \Lambda)$  tales que para todo  $\mathbf{x} \in P$  se cumple que  $f_i(\mathbf{x}) = 0$  para todos salvo finitos  $i \in I$ , y tal que

$$\mathbf{x} = \sum_{i \in I} f_i(\mathbf{x}) \mathbf{x}_i.$$

En cuyo caso  $\{\mathbf{x}_i\}_{i \in I}$  es un sistema generador de  $P$ . Más aún, si  $P$  es finitamente generado podemos exigir que  $I$  sea finito.

DEMOSTRACIÓN:  $\implies$ . Sea  $S := \{\mathbf{x}_i\}_{i \in I}$  un sistema de generadores de  $P$ . Luego sea  $F$  un  $\Lambda$ -módulo libre con base  $\{\mathbf{y}_i\}_{i \in I}$ , luego el morfismo  $p: F \rightarrow P$  que manda  $p(\mathbf{y}_i) = \mathbf{x}_i$  es suprayectivo, por lo que se factoriza en  $q: P \rightarrow F$  tal que  $q \circ p = \text{Id}_P$ . Como  $F$  es libre, la aplicación  $\pi_j: F \rightarrow \Lambda$  dada por

$$\pi_j \left( \sum_{i \in I} a_i \mathbf{y}_i \right) = a_j$$

está bien definida y es un homomorfismo; más aún, para un  $\mathbf{y} \in F$  fijo,  $\pi_j(\mathbf{y})$  es nulo para todos salvo finitos  $i \in I$ . Luego definimos  $f_i := q \circ \pi_i$  y comprobamos que cumple lo exigido.

$\Leftarrow$ . Nuevamente, sea  $F$  un  $\Lambda$ -módulo libre con base  $\{\mathbf{y}_i\}_{i \in I}$  y considere el epimorfismo  $p: F \rightarrow P$  que manda  $p(\mathbf{y}_i) = \mathbf{x}_i$ . Nótese que trivialmente  $\tau_j: \mathbf{x} \mapsto f_j(\mathbf{x}) \mathbf{y}_j$  es un homomorfismo de módulos, que induce el siguiente homomorfismo

$$s := \sum_{i \in I} \tau_i: P \longrightarrow F$$

$$\mathbf{x} \longmapsto \sum_{i \in I} f_i(\mathbf{x}) \mathbf{y}_i$$

que satisface que  $s \circ p = \text{Id}_P$ . Finalmente la sucesión:

$$0 \longrightarrow \ker p \longrightarrow F \xrightarrow{p} P \longrightarrow 0$$

es exacta y se escinde.  $\square$

Pese al nombre no se confunda, ni  $\{\mathbf{x}_i\}_{i \in I}$  ni  $\{f_i\}_{i \in I}$  tienen por que ser bases.

**Definición 11.11:** Se dice que un  $\Lambda$ -módulo  $M$  es *finitamente presentado* si existe una sucesión exacta corta de la forma:

$$\Lambda^m \longrightarrow \Lambda^n \longrightarrow M \longrightarrow 0.$$

**Proposición 11.12:** Todo  $\Lambda$ -módulo proyectivo finitamente generado es finitamente presentado.

DEMOSTRACIÓN: Sea  $P$  un módulo proyectivo. Que sea finitamente generado significa que existe un epimorfismo  $p: \Lambda^n \rightarrow R$ , luego se extiende a una sucesión exacta corta  $0 \rightarrow \ker p \rightarrow \Lambda^n \rightarrow P \rightarrow 0$  y, como  $P$  es proyectivo, dicha sucesión se escinde, de modo que  $\Lambda^n = P \oplus \ker p$ , luego  $\ker p \leq \Lambda^n$  y por ende es finitamente generado.  $\square$

**Definición 11.13:** Una *presentación proyectiva* de un objeto  $M \in \text{Obj } \mathcal{C}$  es una sucesión exacta corta de la forma

$$0 \longrightarrow K \longrightarrow P \xrightarrow{\varepsilon} M \longrightarrow 0,$$

donde  $P$  es un objeto proyectivo.

**Lema 11.14 (de Schanuel):** Dadas dos presentaciones proyectivas de un objeto  $M \in \text{Obj } \mathcal{C}$  en una categoría abeliana  $\mathcal{C}$ :

$$\begin{aligned} 0 \longrightarrow K_1 \longrightarrow P_1 &\xrightarrow{\varepsilon_1} M \longrightarrow 0, \\ 0 \longrightarrow K_2 \longrightarrow P_2 &\xrightarrow{\varepsilon_2} M \longrightarrow 0. \end{aligned}$$

Existe un isomorfismo  $K_1 \oplus P_2 \cong K_2 \oplus P_1$ .

DEMOSTRACIÓN: En primer lugar, como  $P_1$  es proyectivo existe una flecha  $P_1 \xrightarrow{\beta} P_2$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccccc} 0 & \longrightarrow & K_1 & \xrightarrow{k} & P_1 & \xrightarrow{\varepsilon_1} & M \longrightarrow 0 \\ & & \downarrow \exists! g_f & & \downarrow f & & \parallel \\ 0 & \longrightarrow & K_2 & \xrightarrow{k'} & P_2 & \xrightarrow{\varepsilon_2} & M \longrightarrow 0 \end{array}$$

La unicidad de  $g$  está en función de alguna elección de  $f$ . En cualquier caso,  $K_1$  es el producto fibrado de  $(f, k')$  por la proposición ???. Luego por la proposición ?? tenemos la siguiente sucesión exacta:

$$0 \longrightarrow K_1 \xrightarrow{(k, g)} P_1 \oplus K_2 \xrightarrow{\begin{pmatrix} f \\ -k' \end{pmatrix}} P_2 \longrightarrow 0 \quad (11.2)$$

Lo único no trivial es la exactitud en  $P_2$  que queda al lector. Pero,  $P_2$  es proyectivo, luego la sucesión (11.2) se escinde y  $P_1 \oplus K_2 \cong P_2 \oplus K_1$ .  $\square$

**Corolario 11.14.1:** Sea  $M$  un  $\Lambda$ -módulo finitamente presentado. Para toda sucesión exacta corta de la forma:

$$0 \longrightarrow K \longrightarrow F \longrightarrow M \longrightarrow 0$$

donde  $F$  es libre finitamente generado, se cumple que  $K$  está finitamente generado.

DEMOSTRACIÓN: Por definición de finitamente presentado existe otra presentación  $0 \rightarrow K' \rightarrow F' \rightarrow M \rightarrow 0$  con  $F', K'$  finitamente generados y  $F'$  libre. Por el lema de Schanuel se tiene que  $K \oplus F' \cong K' \oplus F$  el cual es finitamente generado, luego  $K$  es finitamente generado.  $\square$

**Ejemplo 11.15:** Un módulo finitamente generado que no es finitamente presentado Sea  $\Lambda$  un dominio con un ideal  $\mathfrak{a}$  que no es finitamente generado (e.g.,  $\Lambda = k[x_1, x_2, \dots]$  y  $\mathfrak{a} = (x_1, x_2, \dots)$ ). Luego  $M := \Lambda/\mathfrak{a}$  es un  $\Lambda$ -módulo finitamente generado (la clase del 1 es un sistema generador), pero no está finitamente presentado pues  $0 \rightarrow \mathfrak{a} \rightarrow \Lambda \rightarrow M \rightarrow 0$  es una presentación libre que contradice el corolario anterior.  $\lrcorner$

### §11.1.2 Módulos inyectivos.

**Lema 11.16:** Si  $Q$  es un  $\mathbb{Z}$ -módulo inyectivo, entonces  $\text{Hom}_{\mathbb{Z}}(\Lambda, Q)$  es un  $\Lambda$ -módulo inyectivo.

DEMOSTRACIÓN: Hay que probar que si

$$0 \longrightarrow N \xrightarrow{f} N'$$

es una sucesión exacta (en  ${}_{\Lambda}\mathbf{Mod}$ ), entonces

$$0 \longleftarrow \text{Hom}_{\Lambda}(N, \text{Hom}_{\mathbb{Z}}(\Lambda, Q)) \xleftarrow{h_f} \text{Hom}_{\Lambda}(N', \text{Hom}_{\mathbb{Z}}(\Lambda, Q))$$

es una sucesión exacta (en  ${}_{\Lambda}\mathbf{Mod}$ ). Ya hemos visto en la sección de tensores que existe un isomorfismo canónico:

$$\varphi_N: \text{Hom}_{\mathbb{Z}}(N \otimes_{\Lambda} \Lambda, Q) \longrightarrow \text{Hom}_{\Lambda}(N, \text{Hom}_{\mathbb{Z}}(\Lambda, Q)),$$

Y sabemos que  $N \otimes_{\Lambda} \Lambda = N$ , luego se induce el siguiente diagrama conmutativo:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathbb{Z}}(N, Q) & \xrightarrow[\sim]{\varphi_N} & \mathrm{Hom}_{\Lambda}(N, Q) \\
\mathrm{Hom}_{\mathbb{Z}}(f, Q) \downarrow & & \downarrow h_f \\
\mathrm{Hom}_{\mathbb{Z}}(N', Q) & \xrightarrow[\sim]{\varphi_{N'}} & \mathrm{Hom}_{\Lambda}(N', Q)
\end{array}$$

finalmente como  $\mathrm{Hom}_{\mathbb{Z}}(f, Q)$  es suprayectivo y los  $\varphi$ 's son isomorfismos, se concluye que  $h_f = \mathrm{Hom}_{\Lambda}(f, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, Q))$  es suprayectivo, como se quería ver.  $\square$

**Teorema (AE) 11.17:** La categoría  $\mathrm{Mod}_{\Lambda}$  tiene suficientes injectivos, i.e., todo  $\Lambda$ -módulo está encajado en un  $\Lambda$ -módulo inyectivo.

**Teorema (AE) 11.18 (dualidad de Pontrjagin):** Se cumple:

1.  $\mathbb{R}/\mathbb{Z}$  y  $\mathbb{Q}/\mathbb{Z}$  son cogeneradores (de  $\mathrm{Ab}$ ), i.e., para todo grupo abeliano  $G$  y todo  $a \in G_{\neq 0}$  existe un homomorfismo  $f: G \rightarrow \mathbb{R}/\mathbb{Z}$  tal que  $f(a) \neq 0$ .
2.  $\mathbb{R}/\mathbb{Z}$  y  $\mathbb{Q}/\mathbb{Z}$  son  $\mathbb{Z}$ -módulos inyectivos.
3. Si  $G$  es un grupo abeliano finito, entonces

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

DEMOSTRACIÓN:

1. En primer lugar, consideremos una presentación libre para  $G$ , de modo que  $G = F/K$  donde  $F$  es el  $\mathbb{Z}$ -módulo libre generado por  $\{x_i\}_{i \in I}$ . Se tiene que  $a$  es la proyección de alguna palabra en  $F$ , luego viene generado por a lo más finitos  $x_i$ 's, digamos que  $F = F_1 \oplus F_2$  donde  $F_1$  contiene generadores finitos de  $a$  y  $F_2$  no, luego  $G \cong F_1/K \oplus F_2/K$  y elegimos  $f$  que proyectiva  $F_2/K$  a 0. Así basta considerar  $G$  finitamente generado.

En el caso de  $G$  finitamente generado, empleamos la descomposición de  $G$  como grupo abeliano libre:

$$G \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z} \oplus \mathbb{Z}^{\beta}$$

con  $\alpha_1, \dots, \alpha_n, \beta \in \mathbb{N}$  y  $p_1, \dots, p_n$  primos distintos. Si  $a$  es de torsión, está en algún  $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$  y mandamos el generador de dicho grupo a  $1/p_i^{\alpha_i}$ . Si  $a$  no es de torsión, está en  $\mathbb{Z}^{\beta}$  y mandamos los generadores a  $\beta$  distintos números irracionales (que en  $\mathbb{R}/\mathbb{Z}$  serán libres de torsión).

Como ejercicio al lector, modifique la demostración para  $\mathbb{Q}/\mathbb{Z}$ .

2. Basta notar que son  $\mathbb{Z}$ -módulos divisibles.
3. Un grupo abeliano finito es puramente de torsión y basta seguir la demostración del inciso 1 para ver el primer isomorfismo.  $\square$

La dualidad de Pontrjagin será útil, no para establecer que las categorías de  $\Lambda$ -módulos tienen suficientes inyectivos, que ya sabíamos desde antes, sino para establecer una construcción funtorial de las extensiones inyectivas.

**Definición 11.19:** Sea  $M$  un  $\Lambda$ -módulo. Denotamos por  $M^\wedge := \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$  el cual es un  $\Lambda$ -módulo. También definimos el siguiente homomorfismo de  $\Lambda$ -módulos:

$$\begin{aligned} \text{ev}: M &\longrightarrow (M^\wedge)^\wedge \\ u &\longmapsto (\varphi \mapsto \varphi(u)). \end{aligned}$$

**Lema 11.20:** El funtor (contravariante)  $M \mapsto M^\wedge$  sobre  $\text{Mod}_\Lambda$  es exacto.

DEMOSTRACIÓN: Basta emplear que  $\mathbb{Q}/\mathbb{Z}$  es un grupo abeliano inyectivo.  $\square$

**Lema 11.21:** Para todo  $\Lambda$ -módulo  $M$  se cumple que  $\text{ev}: M \rightarrow (M^\wedge)^\wedge$  es un monomorfismo.

DEMOSTRACIÓN: Sea  $u \in M_{\neq 0}$  un elemento no nulo y sea  $\mathbb{Z} \cdot u \hookrightarrow M$  el subgrupo (no submódulo) que induce. Es fácil definir un homomorfismo (en  $\text{Ab}$ )  $\mathbb{Z}u \rightarrow \mathbb{Q}/\mathbb{Z}$  tal que no se anule en  $u$ , el cual, como  $\mathbb{Q}/\mathbb{Z}$  es un grupo abeliano inyectivo, se extiende a un homomorfismo  $\varphi: M \rightarrow \mathbb{Q}/\mathbb{Z}$ . Así,  $\text{ev}(u)(\varphi) = \varphi(u) \neq 0$  como se quería probar.  $\square$

Denotaremos por  $F(N) := \Lambda^{\oplus N}$  al módulo libre generado por los elementos de  $N$ . Trivialmente existe un epimorfismo  $F(N) \twoheadrightarrow N$ . En particular, para  $N := M^\wedge$  tenemos  $F(M^\wedge) \twoheadrightarrow M^\wedge$ , que induce un monomorfismo canónico  $(M^\wedge)^\wedge \hookrightarrow (F(M^\wedge))^\wedge$ .

**Teorema 11.22:** El funtor  $M \mapsto J(M) := (F(M^\wedge))^\wedge$  le asigna a cada  $\Lambda$ -módulo una extensión inyectiva.

DEMOSTRACIÓN: Que sea una extensión se sigue de que  $M \hookrightarrow (M^\wedge)^\wedge$  es monomorfismo. Por exactitud contravariante es fácil comprobar que  $J(M) \cong$

$\prod_{\varphi \in M^\wedge} \Lambda^\wedge$ , así que, como producto de inyectivos es inyectivo, basta probar que  $\Lambda^\wedge$  es inyectivo. Esto se sigue de que para todo  $\Lambda$ -módulo  $N$ :

$$\begin{aligned} \text{Hom}_\Lambda(N, \Lambda^\wedge) &= \text{Hom}_\Lambda(N, \text{Hom}_\mathbb{Z}(\Lambda, \mathbb{Q}/\mathbb{Z})) \cong \text{Hom}_\mathbb{Z}(N \otimes_\Lambda \Lambda, \mathbb{Q}/\mathbb{Z}) \\ &\cong \text{Hom}_\mathbb{Z}(N, \mathbb{Q}/\mathbb{Z}) = N^\wedge, \end{aligned}$$

y concluimos por exactitud de  $()^\wedge$ .

El que la construcción sea funtorial es trivial.  $\square$

### §11.1.3 Módulos y anillos (semi)simples.

**Definición 11.23:** Un anillo  $\Lambda$  se dice *semisimple izquierdo* (resp. *derecho*) si es un  $\Lambda$ -módulo izquierdo (resp. derecho) semisimple. Se dice que  $\Lambda$  es *simple* si lo es como  $\Lambda$ - $\Lambda$ -bimódulo, i.e., si es no nulo y sus únicos ideales *bilaterales* son  $0, \Lambda$ .

**Proposición 11.24:** Sea  $\Lambda$  un anillo que es un  $\Lambda$ -módulo izquierdo (o derecho) simple, entonces  $\Lambda$  es un anillo de división.

DEMOSTRACIÓN: Si  $\Lambda$  es un  $\Lambda$ -módulo simple izquierdo, entonces para todo  $a \in \Lambda_{\neq 0}$  entonces  $\Lambda \cdot a$  es un  $\Lambda$ -submódulo izquierdo que no es el nulo, así que  $\Lambda \cdot a = \Lambda$  y existe  $b \in \Lambda$  tal que  $ba = 1$ , luego  $a$  es invertible.  $\square$

**Lema 11.25 (Schur):** Sea  $M$  un  $\Lambda$ -módulo simple. Entonces:

1. Todo homomorfismo de  $\Lambda$ -módulos  $M \rightarrow N$  es o bien nulo, o bien un monomorfismo.
2. Todo homomorfismo de  $\Lambda$ -módulos  $N \rightarrow M$  es o bien nulo, o bien un epimorfismo.
3. Todo endomorfismo de  $\Lambda$ -módulos  $M \rightarrow M$  es o bien nulo, o bien un automorfismo. En consecuencia,  $(\text{End}(M), +, \circ)$  es un anillo de división.

**Proposición 11.26:** Un  $\Lambda$ -módulo  $M$  es semisimple syss todos sus submódulos son sumandos directos.

DEMOSTRACIÓN:  $\Rightarrow$ . Sea  $M = \bigoplus_{i \in I} S_i$  y sea  $N \leq M$ . Luego

$$N = N \cap M = N \cap \left( \bigoplus_{i \in I} S_i \right) = \bigoplus_{i \in I} (N \cap S_i),$$

como cada  $S_i$  es simple, se tiene que  $S_i \cap N$  es o bien  $S_i$  o bien 0. Sea  $J \subseteq I$  el conjunto de los índices  $j$  tales que  $S_j \cap N = S_j$ . Entonces  $N = \bigoplus_{j \in J} S_j$  y

$$M = \bigoplus_{i \in I} S_i = N \oplus \bigoplus_{i \notin J} S_i.$$

$\Leftarrow$ . En primer lugar, probaremos que todo submódulo no nulo  $C \leq M$  contiene un submódulo simple. Para ello, sea  $c \in C_{\neq 0}$  y sea, por lema de Zorn,  $D$  el submódulo maximal de  $C$  que no contiene a  $c$ . Luego  $C = D \oplus E$  y veremos que  $E$  es simple. Sea  $F \leq E$  un submódulo no nulo, entonces  $E = F \oplus G$  y se cumple que  $c \in F$  o  $c \in G$ . Luego o bien  $D + F$  o bien  $D + G$  son módulos que no contienen a  $c$ . Si  $c \in G$ , entonces  $D + F$  no tiene a  $c$ , luego  $D + F = D$  y  $F = 0$  lo cual es absurdo. Luego  $c \in F$  y  $D + G$  no tiene a  $c$ , luego  $D + G = D$  y  $G = 0$  por lo que  $F = E$ .

Así, definamos  $\mathcal{F} := \{S_i\}_{i \in I}$  una familia  $\subseteq$ -maximal de submódulos disjuntos dos a dos simples de  $M$ . Sea  $B := \bigoplus_{i \in I} S_i$  y vemos que si  $B < M$ , entonces  $M = A \oplus B$  con  $A \neq 0$ , luego  $A$  contiene un submódulo simple  $T$  lo que contradice la maximalidad de  $\mathcal{F}$ . Luego  $B = M$  es semisimple.  $\square$

**Teorema 11.27:** Para un anillo  $\Lambda$  son equivalentes:

1.  $\Lambda$  es semisimple izquierdo.
2. Todo ideal izquierdo de  $\Lambda$  es un sumando directo de  $\Lambda$ .
3. Todo ideal izquierdo de  $\Lambda$  es un módulo inyectivo.
4. Todos los  $\Lambda$ -módulos izquierdos son semisimples.
5. Todas las sucesiones exactas de  $\Lambda$ -módulos izquierdos  $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$  se escinden.
6. Todos los  $\Lambda$ -módulos izquierdos son proyectivos.
7. Todos los  $\Lambda$ -módulos izquierdos son inyectivos.

DEMOSTRACIÓN:  $1 \iff 2$  y  $4 \iff 5$ . Es la proposición anterior.  $5 \iff 6$  y  $5 \iff 7$ . Son claras.  $7 \implies 3$ . Trivial.

$3 \implies 2$ . Sea  $\mathfrak{a} \triangleleft \Lambda$  un ideal izquierdo, entonces la sucesión exacta  $0 \rightarrow \mathfrak{a} \rightarrow \Lambda \rightarrow \Lambda/\mathfrak{a} \rightarrow 0$  se escinde y, por lo tanto,  $\mathfrak{a}$  es un sumando directo de  $\Lambda$ .

$2 \implies 7$ . Sea  $Q$  un  $\Lambda$ -módulo izquierdo y sea  $f: \mathfrak{a} \rightarrow Q$  un homomorfismo de  $\Lambda$ -módulos. Como  $\mathfrak{a}$  es un sumando directo, entonces  $f$  admite una

extensión a  $g: \Lambda \rightarrow Q$ , luego, por el criterio de Baer se cumple que  $Q$  es inyectivo.  $\square$

**Definición 11.28:** Un anillo  $\Lambda$  se dice *hereditario izquierdo* (resp. *derecho*) si todo ideal izquierdo (resp. derecho) de  $\Lambda$  es proyectivo.

Trivialmente todo anillo semisimple izquierdo es hereditario izquierdo.

**Teorema 11.29 (Kaplansky):** Si  $\Lambda$  es hereditario izquierdo, entonces todo submódulo de un  $\Lambda$ -módulo libre es un sumando directo de módulos que son isomorfos a un ideal izquierdo de  $\Lambda$ .

DEMOSTRACIÓN: Sea  $F$  un  $\Lambda$ -módulo libre con una base ordenada  $\{\mathbf{x}_\alpha\}_{\alpha < \gamma}$ . Para un ordinal  $\alpha \leq \gamma$  definamos:

$$F_\alpha := \text{Span}_\Lambda\{\mathbf{x}_\beta : \beta < \alpha\}, \quad \overline{F}_\alpha := \text{Span}_\Lambda\{\mathbf{x}_\beta : \beta \leq \alpha\}.$$

Sea  $M \leq F$ , luego todo  $\mathbf{a} \in M \cap \overline{F}_\alpha$  se escribe de forma única como  $\mathbf{a} = \mathbf{b} + \lambda \mathbf{x}_\alpha$  donde  $\mathbf{b} \in M \cap F_\alpha$ . Sea  $f(\mathbf{b} + \lambda \mathbf{x}_\alpha) = \lambda$  un epimorfismo  $f: M \cap \overline{F}_\alpha \rightarrow \mathfrak{a}_\alpha$ , donde  $\mathfrak{a}_\alpha$  es un ideal izquierdo de  $\Lambda$ . Nótese que  $\ker f = M \cap F_\alpha$ , luego tenemos la siguiente sucesión exacta:

$$0 \longrightarrow M \cap F_\alpha \longrightarrow M \cap \overline{F}_\alpha \xrightarrow{f} \mathfrak{a}_\alpha \longrightarrow 0$$

Como  $\mathfrak{a}_\alpha$  es proyectivo, la sucesión se escinde y  $M \cap \overline{F}_\alpha = M \cap F_\alpha \oplus N_\alpha$ , donde  $N_\alpha \cong \mathfrak{a}_\alpha$ . Finalmente, por inducción transfinita, es fácil ver que  $M = \bigoplus_{\alpha < \gamma} C_\alpha$ .  $\square$

**Corolario 11.29.1:** Todo DIP es hereditario y todo submódulo de un módulo libre es también libre.

DEMOSTRACIÓN: Para ver que un DIP  $\Lambda$  es hereditario, nótese que todo ideal  $\mathfrak{a} \triangleleft \Lambda$  es isomorfo a  $\Lambda$ , luego es claramente proyectivo. Más aún, por el teorema anterior, tenemos que todo submódulo es una suma directa de ideales, pero éstos son isomorfos a  $\Lambda$ , luego conforman un módulo libre.  $\square$

Ésta consecuencia es un teorema típico de álgebra (cf. [0, Teo. 5.94]).

**Teorema 11.30 (Cartan-Eilenberg):** Para un anillo  $\Lambda$  son equivalentes:



1.  $\Lambda$  es hereditario izquierdo.
2. Todo submódulo de un  $\Lambda$ -módulo izquierdo proyectivo es también proyectivo.
3. Todo cociente de un  $\Lambda$ -módulo izquierdo inyectivo es también inyectivo.

DEMOSTRACIÓN:  $1 \implies 2$ . Sea  $P$  un  $\Lambda$ -módulo izquierdo proyectivo y sea  $M \leq P$ . Como  $P$  es sumando directo de un módulo libre,  $M$  es un submódulo de un módulo libre, por lo tanto, es suma directa de ideales izquierdos de  $\Lambda$ , los cuales son proyectivos, y toda suma directa de proyectivos es un módulo proyectivo.

$2 \implies 1$ . Trivial, pues  $\Lambda$  es proyectivo.

$2 \implies 3$ . Por la proposición ?? basta chequearlo sobre módulos proyectivos. Sea  $p: Q \rightarrow Q'$  un epimorfismo e  $\iota: P' \rightarrow P$  un monomorfismo, donde  $P$  es proyectivo y  $Q$  es inyectivo, y sea  $f: P' \rightarrow Q'$  un homomorfismo de módulos. Por hipótesis,  $P'$  es proyectivo, luego se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccc} P & \xleftarrow{\iota} & P' \\ & \swarrow g & \downarrow f \\ Q & \xrightarrow[p]{} & Q' \end{array}$$

de modo que como  $Q$  es inyectivo existe un homomorfismo  $h: P \rightarrow Q$  tal que  $g = \iota \circ h$ . Finalmente  $h \circ p: P \rightarrow Q'$  es el homomorfismo deseado:

$$\begin{array}{ccc} P & \xleftarrow{\iota} & P' \\ \downarrow h & \searrow h \circ p & \downarrow f \\ Q & \xrightarrow[p]{} & Q' \end{array}$$

$3 \implies 2$ . Es dual. □

Recordemos ahora un par de definiciones más avanzadas de álgebra conmutativa:

**Definición 11.31:** Sea  $A$  un dominio íntegro y  $K := \text{Frac } A$ . Un *ideal fraccionario* es un  $A$ -submódulo  $M$  tal que existe  $x \in A_{\neq 0}$  con  $xM \subseteq A$ . La multiplicación entre ideales fraccionarios es la usual:

$$M \cdot N := \left\{ \sum_{i=1}^n m_i n_i : m_i \in M, n_i \in N \right\}.$$

Si  $M$  es un ideal fraccionario y existe otro ideal fraccionario  $N$  tal que  $M \cdot N = A$ , entonces decimos que  $M$  es *invertible* y que  $N$  es su inversa.

Y recordemos que:

**Teorema 11.32:** Un dominio íntegro es un dominio de Dedekind syss todo ideal fraccionario es invertible (cf. [0, Teo. 12.65]).

**Teorema 11.33:** Sea  $A$  un dominio íntegro. Un ideal fraccionario no nulo  $I$  es proyectivo syss es invertible.

DEMOSTRACIÓN: Si el ideal  $I$  es proyectivo entonces, por el lema de las bases duales, existen  $\{a_j\}_{j \in J} \subseteq I$  y funciones  $\{f_j\}_{j \in J} \subseteq \text{Hom}_A(I, A)$  tales que  $f_j(b)$  es nulo para todos salvo finitos  $j$ 's y tal que para todo  $b$  se cumple que  $b = \sum_{j \in J} f_j(b)a_j$ . Luego, para un  $b \in I_{\neq 0}$  fijo, definimos  $q_j := f_j(b)/b \in K$ . Nótese que la definición de  $q_j$  es independiente de la elección de  $b$ , pues para otro  $b' \in I_{\neq 0}$ :

$$bf_j(b') = f_j(bb') = f_j(b'b) = b'f_j(b).$$

Ahora bien, se cumple que  $q_j I \subseteq A$  para cada  $j \in J$ , puesto que  $q_j b = f_j(b) \in A$  para todo  $b \in I$ .

Sea  $b \in I_{\neq 0}$  cualquiera. Por definición de los  $q_j$  podemos ver que todos salvo finitos son nulos, y que

$$b = \sum_{j \in J} f_j(b)a_j = \sum_{j \in J} (q_j b)a_j = b \left( \sum_{j \in J} q_j a_j \right),$$

luego, cancelando a ambos lados, tenemos que  $1 = \sum_{j \in J} q_j a_j$ , de modo que  $N := \sum_{j \in J} q_j \cdot A$ .

Es fácil seguir el proceso a la inversa para obtener una base dual de  $I$ .  $\square$

**Corolario 11.33.1:** Un dominio íntegro es hereditario syss es de Dedekind.<sup>1</sup>

**Teorema 11.34:** Un dominio íntegro  $A$  es de Dedekind syss todo  $A$ -módulo divisible es inyectivo.

Ver [0, 168,  
Teo. 4.24].

<sup>1</sup>ROTMAN [0] define *dominio de Dedekind* como un dominio íntegro hereditario, de modo que éste teorema es una definición.

**Teorema 11.35:** Sea  $A$  un DFU. Entonces un ideal fraccionario  $I$  es proyectivo syss es principal.

DEMOSTRACIÓN: Claramente todo ideal principal es proyectivo. Sea  $I$  proyectivo, entonces es inversible y luego existen  $a_1, \dots, a_n \in I$  y  $q_1, \dots, q_n \in \text{Frac}(A)$  tales que  $1 = \sum_{i=1}^n a_i q_i$  y luego  $q_i \cdot I \subseteq A$  para todo  $i$ . Sea  $q_i = b_i/c_i$ , donde, como  $A$  es un DFU, cada  $b_i, c_i$  son coprimos. Luego como  $b_i(a_i/c_i) \in A$  se cumple que  $c_i \mid a_i$  para cada  $i$ . Así pues, sea  $c := \text{mcm}\{c_1, \dots, c_n\}$ , probaremos que  $I = c \cdot A$ . Nótese que  $c \in I$  puesto que  $c = c(\sum_{i=1}^n b_i a_i / c_i) = \sum_{i=1}^n (b_i c / c_i) a_i$ , donde  $b_i c / c_i \in I$ . Con ello  $(c) \subseteq I$  y la para la inclusión restante, como  $c_i \mid a_i$  tenemos que  $c \mid a_i$  para cada  $i$ , luego  $a_i \in (c)$  y  $I \subseteq (c)$ .  $\square$

**Corolario 11.35.1:** Un dominio de Dedekind es un DFU syss es un DIP.

**Definición 11.36:** Se dice que un anillo  $\Lambda$  es *semihereditario izquierdo* si todo ideal izquierdo finitamente generado es un  $\Lambda$ -módulo proyectivo. Un anillo  $A$  es *de Prüfer* si es un dominio íntegro semihereditario.

Siguiendo la demostración del teorema de Kaplansky vemos que:

**Teorema 11.37:** Si  $\Lambda$  es semihereditario izquierdo, entonces todo submódulo finitamente generado de un  $\Lambda$ -módulo izquierdo libre es un sumando directo de módulos que son isomorfos a un ideal izquierdo de  $\Lambda$ .

Y siguiendo la demostración del teorema de Cartan-Eilenberg:

**Proposición 11.38 (Albrecht):** Para un anillo  $\Lambda$  son equivalentes:

1.  $\Lambda$  es semihereditario izquierdo.
2. Todo submódulo finitamente generado de un  $\Lambda$ -módulo izquierdo proyectivo finitamente generado es proyectivo.
3. Todo cociente finitamente generado de un  $\Lambda$ -módulo izquierdo inyectivo finitamente generado es inyectivo.

## 11.2 Extensiones y el funtor $\text{Ext}$

Cambiando un poco el convenio, en general en éste capítulo  $\Lambda$  denotará un anillo base para poder emplear libremente  $A, B, C$ , etc. para  $\Lambda$ -módulos.

**Definición 11.39:** Dada una sucesión exacta corta de la forma

$$E: \quad 0 \longrightarrow A \xhookrightarrow{f} B \twoheadrightarrow^g C \longrightarrow 0,$$

diremos que la sucesión  $E$  (o el módulo  $B$ ) corresponde a una **extensión** de  $A$  sobre  $C$ .

Esta terminología es intuitiva puesto que  $A$  está contenido en  $B$  el cual a su vez se proyecta en  $C$ . En general, en cualquier categoría abeliana (y de hecho basta aditiva) la siguiente es una extensión de  $A$  sobre  $C$ :

$$0 \longrightarrow A \xrightarrow{\iota_A} A \oplus C \xrightarrow{\pi_C} C \longrightarrow 0.$$

**Definición 11.40:** Sean  $A, C$  dos  $\Lambda$ -módulos. Dos extensiones  $E_1, E_2$  de  $A$  sobre  $C$  se dicen **equivalentes** si existe un homomorfismo  $\xi: B_1 \rightarrow B_2$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccccc} E_1: & 0 & \longrightarrow & A & \longrightarrow & B_1 & \longrightarrow C \longrightarrow 0 \\ & & & \parallel & & \downarrow \xi & \parallel \\ & \downarrow \xi & & & & & \\ E_2: & 0 & \longrightarrow & A & \longrightarrow & B_2 & \longrightarrow C \longrightarrow 0. \end{array}$$

Nótese que por el lema corto de los cinco se concluye que  $\xi$  es un isomorfismo y es fácil concluir que de hecho establece una relación de equivalencia. Las clases de equivalencia de las extensiones  $A$  sobre  $C$  se denotan  $E(C, A)$ .

Nótese que como las extensiones de  $A$  sobre  $C$  son objetos cociente de  $C$ , entonces  $E(C, A)$  será un conjunto si nuestra categoría base está bien copotenciada, como es el caso con  $\text{Mod}_\Lambda$ .

Veamos que, mediante nuestro conocimiento categorial podemos determinar una construcción relativa a la coordenada  $C$ : Sea  $f: C \rightarrow C'$  un homomorfismo de  $\Lambda$ -módulos y sea  $E \in E(C', A)$  una extensión de módulos. Podemos definir  $B^f$  como un producto fibrado:

$$\begin{array}{ccccccc} & & & B^f & \overset{\beta'}{\dashrightarrow} & C & \\ & & & \downarrow & \lrcorner & \downarrow f & \\ 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{\beta} & C' \longrightarrow 0 \end{array}$$

Ahora bien, como  $B^f$  es un producto fibrado, y  $\beta$  es epimorfismo, por el teorema ?? se cumple que  $\beta'$  también es epimorfismo. Además, por la proposición ?? tenemos que se induce el siguiente diagrama, con filas exactas:

$$\begin{array}{ccccccc}
E^f: & 0 & \longrightarrow & A & \xrightarrow{\exists!} & B^f & \longrightarrow C \longrightarrow 0 \\
\downarrow f^* & & & \parallel & & \downarrow \lrcorner & \downarrow f \\
E: & 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow C' \longrightarrow 0
\end{array}$$

Dualizando, a partir de un homomorfismo de  $\Lambda$ -módulos  $g: A \rightarrow A'$  se obtiene:

$$\begin{array}{ccccccc}
E: & 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow C \longrightarrow 0 \\
\downarrow g_* & & & \downarrow g & & \downarrow \lrcorner & \parallel \\
E_g: & 0 & \longrightarrow & A' & \longrightarrow & B_g & \xrightarrow{\exists!} C \longrightarrow 0
\end{array} \tag{11.3}$$

**Teorema 11.41:** Para  $\Lambda$ -módulos, la aplicación  $E(-, -): \text{Mod}_\Lambda^{\text{op}} \times \text{Mod}_\Lambda \rightarrow \text{Set}$  determina un bifunctor, contravariante en la primera coordenada y covariante en la segunda.

DEMOSTRACIÓN: Para ver que es un bifunctor hay que verificar que se trata de un funtor en cada coordenada fijada y, por el lema ??, de que  $f^* \circ g_* = g_* \circ f^*$ . Para verificar cada coordenada basta notar que las extensiones vienen completamente determinadas por los  $B^-$  que son productos fibrados y emplear el lema de los productos fibrados (y su dual para ver funtorialidad en la segunda coordenada).

Sea  $(f^*, g): (C', A) \rightarrow (C, A')$  y  $E \in E(C', A)$  una extensión, entonces se tiene el siguiente diagrama: ...  $\square$

Ahora vamos a definir otro bifunctor y ver que, de hecho, coinciden.

**Definición 11.42:** Sea  $C$  un  $\Lambda$ -módulo. Una *presentación proyectiva* de  $C$  es una sucesión exacta corta:

$$0 \longrightarrow R \xrightarrow{\mu} P \xrightarrow{\varepsilon} C \longrightarrow 0 \tag{11.4}$$

donde  $P$  es un  $\Lambda$ -módulo proyectivo.

Como los módulos libres son proyectivos, todo  $\Lambda$ -módulo admite una presentación proyectiva, aunque, al igual que con los módulos libres, hay presentaciones más óptimas que otras. Nótese que solo es necesaria la flecha  $\varepsilon$  de la presentación (11.4), puesto que  $\mu := \ker(\varepsilon)$ .

Ahora bien, dado otro  $\Lambda$ -módulo  $A$ , la presentación (11.4) induce la siguiente sucesión exacta bajo el funtor  $\text{Hom}_\Lambda(-, A)$ :

$$\mathrm{Hom}_\Lambda(R, A) \xleftarrow{h_\mu} \mathrm{Hom}_\Lambda(P, A) \xleftarrow{h_\varepsilon} \mathrm{Hom}_\Lambda(C, A) \xleftarrow{\quad} 0$$

Donde  $h_\mu$  es una abreviación del homomorfismo  $\mathrm{Hom}_\Lambda(\mu, A)$ . Luego, podemos definir  $\mathrm{Ext}_\Lambda^\varepsilon(C, A) := \mathrm{coker}(\mathrm{Hom}_\Lambda(\mu, A))$ . La notación no lo sugiere, pero la definición depende, al menos en principio, de la presentación proyectiva fijada para  $C$ .

Supongamos que un homomorfismo de  $\Lambda$ -módulos  $g: A \rightarrow A'$ . Entonces tenemos la transformación natural  $h^g: \mathrm{Hom}_\Lambda(-, A) \rightarrow \mathrm{Hom}_\Lambda(-, A')$ , de modo que induce un homomorfismo  $g_*: \mathrm{Ext}_\Lambda^\varepsilon(C, A) \rightarrow \mathrm{Ext}_\Lambda^\varepsilon(C, A')$ . Se puede ver que  $\mathrm{Ext}_\Lambda^\varepsilon(C, -): \mathbf{Mod}_\Lambda \rightarrow \mathbf{Ab}$  es un funtor (covariante).

Por otro lado, si tenemos un homomorfismo  $f: C \rightarrow C'$ , y tenemos dos presentaciones proyectivas  $R \xrightarrow{\mu} P \xrightarrow{\varepsilon} C$  y  $R' \xrightarrow{\mu'} P' \xrightarrow{\varepsilon'} C'$ . Entonces por definición de proyectivo tenemos la existencia de un  $\pi$ :

$$\begin{array}{ccc} P & \xrightarrow{\varepsilon} & C \\ \pi \downarrow & \searrow & \downarrow f \\ P' & \xrightarrow[\varepsilon']{} & C' \end{array}$$

Ahora bien, nótese que

$$\mu \circ \pi \circ \varepsilon' = \mu \circ \varepsilon \circ f = 0 \circ f = 0.$$

Luego, como la presentación es una sucesión exacta, tenemos que  $R' = \ker(\varepsilon')$  y luego tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \longrightarrow & P & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow \exists! \sigma & & \downarrow \pi & & \downarrow f & & \\ 0 & \longrightarrow & R' & \xrightarrow[\ker(\varepsilon')]{} & P' & \xrightarrow[\varepsilon']{} & C' & \longrightarrow & 0 \end{array}$$

Ahora bien, nótese que hay una elección en el  $\pi$  de modo que diremos que el  $\pi$  es una elevación de  $f$ . Luego podemos ver el siguiente diagrama conmutativo:

$$\begin{array}{ccccc} 0 \longleftarrow \mathrm{Ext}_\Lambda^\varepsilon(C, A) & \xleftarrow{k} & \mathrm{Hom}_\Lambda(R, A) & \xleftarrow{h_\mu} & \mathrm{Hom}_\Lambda(P, A) \\ & \uparrow \exists! \pi^* & \uparrow h_\sigma & & \uparrow h_\pi \\ 0 \longleftarrow \mathrm{Ext}_\Lambda^{\varepsilon'}(C', A) & \longleftarrow & \mathrm{Hom}_\Lambda(R', A) & \xleftarrow{h_{\mu'}} & \mathrm{Hom}_\Lambda(P', A) \end{array}$$

La existencia y unicidad del  $\pi^*$  deriva del hecho de que  $\mathrm{Ext}_\Lambda^{\varepsilon'}(C', A) = \mathrm{coker}(h_{\mu'})$  y

$$h_{\mu'} \circ h_\sigma \circ k = h_\pi \circ h_\mu \circ k = h_\pi \circ 0 = 0.$$

Le llamamos  $\pi^*$  porque, si bien en realidad también depende de  $\sigma$ ,  $\sigma$  está completamente determinado por  $\pi$ .

**Lema 11.43:**  $\pi^*$  sólo depende del homomorfismo  $f: C \rightarrow C'$  no de la elección del  $\pi: P \rightarrow P'$ .

DEMOSTRACIÓN: Sean  $\pi_1, \pi_2: P \rightarrow P'$  dos elevaciones de  $f$  con  $\sigma_i: R \rightarrow R'$  inducidas. Recordemos que las elevaciones vienen de la proyectividad de  $P$ , en particular, de la sucesión exacta:

$$0 \longrightarrow \text{Hom}_\Lambda(P, R') \xrightarrow{h^{\mu'}} \text{Hom}_\Lambda(P, P') \xrightarrow{h^{\varepsilon'}} \text{Hom}_\Lambda(P, C') \longrightarrow 0.$$

Como  $\pi_i \circ \varepsilon' = \varepsilon \circ f$  (constante), tenemos que  $\pi_1 - \pi_2 \in \ker(h^{\varepsilon'}) = (h^{\mu'})$ , de modo que existe  $\tau: P \rightarrow R'$  tal que  $\pi_1 - \pi_2 = \tau \circ \mu'$  y luego  $\sigma_1 - \sigma_2 = \mu \circ \tau$ .

Sea  $\varphi \in \text{Hom}_\Lambda(R', A)$  y consideremos su clase  $[\varphi] \in \text{Ext}_\Lambda^{\varepsilon'}(C', A)$ , luego

$$\pi_1^*[\varphi] = [\sigma_1 \circ \varphi] = [\sigma_2 \varphi + (\sigma_1 - \sigma_2)\varphi] = [\sigma_2 \varphi + \mu \tau \varphi] = [\sigma_2 \varphi] = \pi_2^*[\varphi],$$

donde  $[\mu \circ x] = 0$  puesto que  $\text{coker}(h_\mu) := \text{Hom}_\Lambda(R, A)/(h_\mu)$ .  $\square$

Ésto es lo que queremos puesto que entonces  $\text{Ext}_\Lambda(-, A)$  induce un funtor contravariante. Para enfatizar ésta dependencia, denotaremos al homomorfismo:

$$(f; P, P'): \text{Ext}_\Lambda^{\varepsilon'}(C', A) \longrightarrow \text{Ext}_\Lambda^{\varepsilon}(C, A).$$

**Corolario 11.43.1:** Dadas dos presentaciones proyectivas  $R \rightarrow P \xrightarrow{\varepsilon} C$  y  $R' \rightarrow P' \xrightarrow{\varepsilon'} C'$ , entonces la transformación natural

$$(1_C; P, P'): \text{Ext}_\Lambda^{\varepsilon'}(C', -) \Longrightarrow \text{Ext}_\Lambda^{\varepsilon}(C, -).$$

es una equivalencia (de funtores).

Luego podemos obviar el superíndice  $\varepsilon$  dado que hemos probado que  $\text{Ext}_\Lambda$  es independiente de la presentación proyectiva elegida. Es fácil probar:

**Teorema 11.44:**  $\text{Ext}_\Lambda(-, -): \text{Mod}_\Lambda^{\text{op}} \times \text{Mod}_\Lambda \rightarrow \text{Ab}$  es un bifuntor.

Claramente  $\text{Ext}_\Lambda(-, -)$  también induce un bifuntor en la categoría de conjuntos que anotaremos con los mismos símbolos. La conexión relevante es la siguiente:

**Teorema 11.45:** Hay una equivalencia natural entre los bifuntores de conjuntos  $\eta: E(-, -) \Rightarrow \text{Ext}_\Lambda(-, -)$ .

DEMOSTRACIÓN: En primer lugar queremos formar una función de conjuntos. Sea  $A \rightarrow B \rightarrow C$  una extensión de  $A$  sobre  $C$ , luego tomamos algún módulo proyectivo  $P \xrightarrow{\varphi} B$  y con eso formamos el siguiente diagrama:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \longrightarrow & C \longrightarrow 0 \\ & & \downarrow \exists! \psi & & \downarrow \varphi & & \parallel \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \longrightarrow & C \longrightarrow 0 \end{array}$$

Luego tenemos  $[\psi] \in \text{Ext}_\Lambda(C, A)$ . Para que  $\eta$  como función esté bien definida queremos que  $[\psi]$  no dependa de la elección del  $\varphi$  (pues ya sabemos que no depende de la elección de la presentación proyectiva). Sean dos  $\varphi_1, \varphi_2$  con  $\psi_1, \psi_2 \in \text{Hom}_\Lambda(R, A)$  inducidos. Luego  $\varphi_1 - \varphi_2 = \tau \circ \alpha$  para algún  $\tau \in \text{Hom}_\Lambda(P, A)$  y  $\sigma_1 - \sigma_2 = \mu \circ \tau$ , de lo que vemos que  $[\psi_1] = [\psi_2] \in \text{Ext}_\Lambda(C, A)$ . El que sea una transformación natural en  $A$  queda de ejercicio, para lo que basta construir un diagrama como (11.3).

Queremos ahora construir una transformación natural inversa. Sea  $[\psi] \in \text{Ext}_\Lambda(C, A)$ , i.e.,  $\psi: R \rightarrow A$ . Al igual que en (11.3) construimos:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R & \xrightarrow{\mu} & P & \longrightarrow & C \longrightarrow 0 \\ & & \downarrow \psi & & \downarrow & & \parallel \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\exists!} & C \longrightarrow 0 \end{array}$$

Si  $[\psi] = [\psi']$  es porque existe  $\tau \in \text{Hom}_\Lambda(P, A)$  tal que  $\psi' = \psi + \mu \circ \tau$ . Es fácil verificar que con  $\phi' := \varphi + \tau \alpha$  el siguiente diagrama conmuta:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R & \longrightarrow & P & \longrightarrow & C \longrightarrow 0 \\ & & \downarrow \psi' & \swarrow \tau & \downarrow \varphi' & & \parallel \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0 \end{array}$$

de modo que la extensión  $A \rightarrow B \rightarrow C$  es independiente de la elección de  $\psi$ . Con ello construimos una aplicación

$$\xi(C, A): \text{Ext}_\Lambda(C, A) \longrightarrow E(C, A).$$

Queda al lector comprobar que  $\xi(-, -)$  determina una transformación natural y que es la inversa a  $\eta$ .  $\square$



Como  $E(C, A)$  ahora tiene una estructura de grupo abeliano, entonces, por ejemplo, tiene neutro 0. ¿Cómo identificar que una extensión de módulos sea nula en  $\text{Ext}_\Lambda(C, A)$ ? Sea  $R \rightarrow P \rightarrow C$  una presentación proyectiva y  $A \rightarrow B \rightarrow C$  una extensión de módulos con  $\psi \in \text{Hom}_\Lambda(R, A)$ . Que  $[\psi] = [0]$  corresponde a que existe  $\tau \in \text{Hom}_\Lambda(P, A)$  con  $\mu \circ \tau = \psi$ , luego  $\mu(\varphi - \tau\alpha) = 0$ , por lo que, como  $C = \text{coker } \mu$ , existe un único  $\sigma$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccc} R & \xrightarrow{\mu} & P & \xrightarrow{\varepsilon} & C \\ & \searrow 0 & \downarrow \varphi - \tau\alpha & \swarrow \exists! \sigma & \\ & & B & & \end{array}$$

Queremos ver que  $\sigma \circ \beta = 1_C$ . Para ello, recuerde que  $\varepsilon$  es epimorfismo y note que

$$\varepsilon \circ (\sigma\beta) = (\varphi - \tau\alpha)\beta = \varphi\beta - \tau(\alpha\beta) \xrightarrow{0} \varepsilon.$$

De modo que tenemos que la sucesión se escinde. Es fácil comprobar el recíproco.

Luego también concluimos lo siguiente:

**Corolario 11.45.1:** Se cumplen:

1. Sea  $P$  un  $\Lambda$ -módulo proyectivo e  $I$  un módulo inyectivo. Para todo par de módulos  $C, A$  se cumple que  $\text{Ext}_\Lambda(P, A) = \text{Ext}_\Lambda(C, I) = 0$ .
2. Sean  $P, I$  un par de  $\Lambda$ -módulos. Si para todo par de módulos  $C, A$  se cumple que  $\text{Ext}_\Lambda(P, A) = \text{Ext}_\Lambda(C, I) = 0$ , entonces  $P$  es proyectivo e  $I$  es inyectivo.

**DEMOSTRACIÓN:** Para la segunda nótese que como  $\text{Ext}_\Lambda(-, -) = E(-, -)$ , vemos que la condición de que  $\text{Ext}_\Lambda(P, A) = 0$  se traduce en que toda sucesión exacta corta de la forma  $0 \rightarrow A \rightarrow B \rightarrow P \rightarrow 0$  se escinde, lo que equivale a ser proyectivo.  $\square$

Nótese que la demostración de que  $\text{Ext}_\Lambda(C, I) = 0$  también podría hacerse recordando que  $\text{Hom}_\Lambda(-, I)$  es un funtor exacto. ¿Podríamos emplear un argumento del mismo tipo para ver que  $\text{Ext}_\Lambda(P, A) = 0$ ?

Comenzamos por ver el proceso inverso:

**Definición 11.46:** Sea  $A$  un  $\Lambda$ -módulo. Una *presentación inyectiva* de  $A$  es una sucesión exacta corta:

$$0 \longrightarrow A \xrightarrow{\nu} I \xrightarrow{\eta} S \longrightarrow 0 \quad (11.5)$$

donde  $I$  es un  $\Lambda$ -módulo inyectivo.

Al contrario de las presentaciones proyectivas no es inmediatamente claro que todo módulo admita una presentación proyectiva, lo que equivale a decir que no es obvio que exista un monomorfismo hasta un módulo inyectivo, pero éste sí resulta ser el caso (cf. [0, Teo. 5.82]). Nuevamente  $\eta := \text{coker}(\nu)$  de modo que la única flecha importante de (11.5) es  $\nu$ .

Dado un  $\Lambda$ -módulo  $C$  aplicamos  $\text{Hom}(C, -)$  en (11.5) para obtener:

$$0 \longrightarrow \text{Hom}_\Lambda(C, A) \xrightarrow{h^\nu} \text{Hom}_\Lambda(C, I) \xrightarrow{h^\eta} \text{Hom}_\Lambda(C, S)$$

Y, al igual que antes, definimos  $\overline{\text{Ext}}'_\Lambda(C, A) := \text{coker}(\text{Hom}_\Lambda(C, \eta))$ .

Dualizando todo lo anterior se podría obtener fácilmente una equivalencia natural  $E(-, -) \Rightarrow \overline{\text{Ext}}_\Lambda(-, -)$  entre bifuntores de conjuntos, pero veremos otro camino que nos dará, más fuerte aún, que  $\overline{\text{Ext}}_\Lambda(-, -)$  y  $\text{Ext}_\Lambda(-, -)$  son equivalentes como bifuntores de grupos abelianos.

**Lema 11.47:** Dado el siguiente diagrama conmutativo de  $\Lambda$ -módulos con filas exactas:

$$\begin{array}{ccccc} A & \xrightarrow{\psi} & B & \xrightarrow{\phi} & C \\ \alpha \downarrow & \Sigma_1 & \downarrow \beta & \Sigma_2 & \downarrow \gamma \\ A' & \xrightarrow{\psi'} & B' & \xrightarrow{\phi'} & C' \end{array} \quad (11.6)$$

Se cumple que

$$\frac{\ker(\phi \circ \gamma)}{\ker \phi + \ker \beta} \cong \frac{\beta \cap \psi'}{(\psi \circ \beta)}.$$

DEMOSTRACIÓN: Sea  $x \in \ker(\phi \circ \gamma) \leq B$ . Claramente  $\beta(x) \in \beta$  y, por otro lado,  $\phi'(\beta(x)) = (\beta \circ \phi')(x) = (\phi \circ \gamma)(x) = 0$ , de modo que  $\beta(x) \in \ker(\phi') = (\psi')$  por exactitud. Así que  $\beta$  induce el siguiente homomorfismo:

$$\bar{\beta}: \ker(\phi \circ \gamma) \longrightarrow \beta \cap \psi' \longrightarrow \frac{\beta \cap \psi'}{(\psi \circ \beta)}.$$

Veamos que es un epimorfismo: Sea  $y \in \beta \cap \psi'$ , luego existe  $x \in B$  tal que  $\beta(x) = y$  y:

$$(\phi \circ \gamma)(x) = (\beta \circ \phi')(x) = \phi'(y) = 0$$

pues  $(\psi') = \ker(\phi')$ ; así que  $x \in \ker(\phi \circ \gamma)$ .

Finalmente veamos que  $\ker(\bar{\beta}) = \ker \phi + \ker \beta$ . si  $\bar{\beta}(x) = 0$  es por que  $\beta(x) \in (\psi \circ \beta)$ , de modo que  $x \in \ker \beta$  o  $x \in \psi = \ker \phi$ . El recíproco es claro.  $\square$

**Definición 11.48:** Dado un cuadrado conmutativo de  $\Lambda$ -módulos:

$$\begin{array}{ccc} A & \xrightarrow{\psi} & B \\ \alpha \downarrow & \Sigma & \downarrow \beta \\ A' & \xrightarrow{\psi'} & B' \end{array}$$

Se define:

$$\ker \Sigma := \frac{\ker(\psi \circ \beta)}{\ker \psi + \ker \alpha}, \quad \Sigma := \frac{\beta \cap \psi'}{(\psi \circ \beta)}.$$

Así, el lema anterior dice que dado un diagrama (11.6) conmutativo con filas exactas se induce:

$$\ker \Sigma_2 = \Sigma_1.$$

Ahora sí, veamos que:

**Teorema 11.49:** Para toda presentación proyectiva  $R \rightarrow P \xrightarrow{\varepsilon} C$  y toda presentación inyectiva  $A \xrightarrow{\nu} I \rightarrow S$  se induce un isomorfismo de grupos abelianos:

$$\text{Ext}_{\Lambda}^{\varepsilon}(C, A) \cong \overline{\text{Ext}}_{\Lambda}^{\nu}(C, A).$$

DEMOSTRACIÓN: Basta construir el siguiente diagrama conmutativo con filas y columnas exactas:

$$\begin{array}{ccccccc} \text{Hom}(C, A) & \cdots \rightarrow & \text{Hom}(C, I) & \rightarrow & \text{Hom}(C, S) & \rightarrow & \overline{\text{Ext}}_{\Lambda}(C, A) \\ \vdots \downarrow & & \downarrow & \Sigma_2 & \downarrow & \Sigma_1 & \downarrow \\ \text{Hom}(P, A) & \rightarrow & \text{Hom}(P, I) & \rightarrow & \text{Hom}(C, S) & \longrightarrow & 0 \\ \downarrow & \Sigma_4 & \downarrow & \Sigma_3 & \downarrow & & \\ \text{Hom}(R, A) & \rightarrow & \text{Hom}(R, I) & \rightarrow & \text{Hom}(R, S) & & \\ \downarrow & \Sigma_5 & \downarrow & & & & \\ \text{Ext}_{\Lambda}(C, A) & \longrightarrow & 0 & & & & \end{array}$$

Notar que  $\ker \Sigma_1 = \overline{\text{Ext}}_\Lambda(C, A)$  y que  $\ker \Sigma_5 = \text{Ext}_\Lambda(C, A)$ , y emplear el lema anterior:

$$\overline{\text{Ext}}_\Lambda(C, A) = \ker \Sigma_1 = \Sigma_2 = \ker \Sigma_3 = \Sigma_4 = \ker \Sigma_5 = \text{Ext}_\Lambda(C, A). \quad \square$$

**Proposición 11.50:** Sean  $(C_i)_{i \in I}, (A_j)_{j \in J}$  familias de  $\Lambda$ -módulos. Entonces:

$$\begin{aligned} \text{Ext}_\Lambda \left( \bigoplus_{i \in I} C_i, A \right) &= \prod_{i \in I} \text{Ext}_\Lambda(C_i, A), \\ \text{Ext}_\Lambda \left( C, \prod_{j \in J} A_j \right) &= \prod_{j \in J} \text{Ext}_\Lambda(C, A_j). \end{aligned}$$

DEMOSTRACIÓN: Sean  $R_i \rightarrow P_i \rightarrow C_i$  presentaciones proyectivas. Entonces se induce el siguiente diagrama conmutativo:

$$\begin{array}{ccccccc} \text{Hom} \left( \bigoplus_{i \in I} P_i, A \right) & \rightarrow & \text{Hom} \left( \bigoplus_{i \in I} R_i, A \right) & \rightarrow & \text{Ext}_\Lambda \left( \bigoplus_{i \in I} C_i, A \right) & \rightarrow & 0 \\ \downarrow \wr & & \downarrow \wr & & & & \\ \prod_{i \in I} \text{Hom}(P_i, A) & \rightarrow & \prod_{i \in I} \text{Hom}(R_i, A) & \rightarrow & \prod_{i \in I} \text{Ext}_\Lambda(C_i, A) & \rightarrow & 0 \end{array}$$

donde las filas son exactas. Luego es fácil concluir. La segunda igualdad queda al lector.  $\square$

**Teorema 11.51:** Dada una sucesión exacta  $0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0$  de  $\Lambda$ -módulos y otro módulo  $C$ , se induce la siguiente sucesión exacta:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_\Lambda(C, A_1) & \longrightarrow & \text{Hom}_\Lambda(C, A_2) & \longrightarrow & \text{Hom}_\Lambda(C, A_3) \\ & & & & \searrow \omega & & \uparrow \\ & & \text{Ext}_\Lambda(C, A_1) & \longrightarrow & \text{Ext}_\Lambda(C, A_2) & \longrightarrow & \text{Ext}_\Lambda(C, A_3) \end{array}$$

DEMOSTRACIÓN: Recordemos que el funtor  $\text{Hom}(X, -)$  siempre es exacto por la izquierda, pero si  $X$  es proyectivo entonces es un funtor exacto. Así pues, estamos en condiciones de emplear el lema de la serpiente sobre el diagrama (ver fig. 11.1).  $\square$

**Teorema 11.52:** Dada una sucesión exacta  $0 \rightarrow C_1 \rightarrow C_2 \rightarrow C_3 \rightarrow 0$  de  $\Lambda$ -módulos y otro módulo  $A$ , se induce la siguiente sucesión exacta:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \text{Hom}_\Lambda(C, A_1) & \longrightarrow & \text{Hom}_\Lambda(C, A_2) & \longrightarrow & \text{Hom}_\Lambda(C, A_3) \\
\parallel & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \text{Hom}_\Lambda(P, A_1) & \cdots \longrightarrow & \text{Hom}_\Lambda(P, A_2) & \cdots \longrightarrow & \text{Hom}_\Lambda(P, A_3) \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \text{Hom}_\Lambda(R, A_1) & \cdots \longrightarrow & \text{Hom}_\Lambda(R, A_2) & \cdots \longrightarrow & \text{Hom}_\Lambda(R, A_3) \\
& & \downarrow & & \downarrow & & \downarrow \\
& & \text{Ext}_\Lambda(C, A_1) & \longrightarrow & \text{Ext}_\Lambda(C, A_2) & \longrightarrow & \text{Ext}_\Lambda(C, A_3)
\end{array}$$

(A green arrow labeled  $\omega$  points from  $\text{Hom}_\Lambda(P, A_2)$  to  $\text{Ext}_\Lambda(C, A_1)$ . A green curved arrow connects the top row to the bottom row.)

**Figura 11.1.** Demostración del teorema 11.51.

$$\begin{array}{ccccccc}
0 & \longrightarrow & \text{Hom}_\Lambda(C_3, A) & \longrightarrow & \text{Hom}_\Lambda(C_2, A) & \longrightarrow & \text{Hom}_\Lambda(C_1, A) \\
& & & & \searrow \omega & & \\
& & \text{Ext}_\Lambda(C_3, A) & \longrightarrow & \text{Ext}_\Lambda(C_2, A) & \longrightarrow & \text{Ext}_\Lambda(C_1, A)
\end{array}$$

Así, podemos verificar que  $\text{Ext}_\Lambda(-, -)$  es un funtor que «arregla el fallo de exactitud de  $\text{Hom}_\Lambda(-, -)$ ».

**Corolario 11.52.1:** En un anillo hereditario (izquierdo)  $\Lambda$  (e.g., un DIP):

1. Dada una sucesión exacta  $0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0$  de  $\Lambda$ -módulos (izquierdos) y otro módulo  $C$ , se induce la siguiente sucesión exacta:

$$\text{Ext}_\Lambda(C, A_1) \longrightarrow \text{Ext}_\Lambda(C, A_2) \longrightarrow \text{Ext}_\Lambda(C, A_3) \longrightarrow 0$$

2. Dado un  $\Lambda$ -módulo (izquierdo)  $A$  y una sucesión exacta  $0 \rightarrow C_1 \rightarrow C_2 \rightarrow C_3 \rightarrow 0$  de  $\Lambda$ -módulos, se induce la siguiente sucesión exacta:

$$\text{Ext}_\Lambda(C_3, A) \longrightarrow \text{Ext}_\Lambda(C_2, A) \longrightarrow \text{Ext}_\Lambda(C_1, A) \longrightarrow 0$$

DEMOSTRACIÓN: Sea  $R \rightarrow P \rightarrow C$  una presentación proyectiva de  $C$ . Como  $\Lambda$  es hereditario y  $R \leq P$ , entonces  $R$  es proyectivo, luego basta mirar el diagrama 11.1 para concluir. Para la segunda, la demostración es similar empleando que todo cociente de un módulo inyectivo es inyectivo.  $\square$

Otra manera de reformular el corolario anterior es que si  $\Lambda$  es hereditario, entonces  $\text{Ext}_\Lambda(-, -)$  es un funtor exacto por la derecha. Somos más explícitos para dar a entender que ésto complementa los dos diagramas generales anteriores.

**Lema 11.53:** Sea  $A$  un grupo abeliano de rango numerable. Si todo subgrupo de rango finito es libre, entonces  $A$  también es libre.

**Teorema 11.54 (Stein-Serre):** Sea  $A$  un grupo abeliano de rango numerable.  $A$  es  $\mathbb{Z}$ -proyectivo syss  $A$  es libre syss  $\text{Ext}(A, \mathbb{Z}) = 0$ .

DEMOSTRACIÓN: La primera equivalencia se debe a que  $\mathbb{Z}$  es un DIP, y luego es hereditario.  $\square$

Añadir demostración  
[0, §3.6, pp. 106-109].

## 11.3 Tensores y el funtor Tor

**§11.3.1 Tensores (caso no conmutativo).** En [0, §5.3] ya estudiamos los productos tensoriales sobre dominios (i.e., anillos unitarios conmutativos). Aquí olvidamos dichas restricciones y consideramos a  $R$  como posiblemente no conmutativo; las demostraciones son las mismas *verbatim*, así que obviaremos las construcciones asumiendo que el lector interesado va a leer de la referencia. Para ello tendremos que tener cuidado con que un  $R$ -módulo sea o bien derecho, o bien izquierdo; para enfatizar ésta diferencia denotaremos por  ${}_R M$  a un  $R$ -módulo izquierdo  $M$  y  $M_R$  a un  $R$ -módulo derecho.

En primer lugar, la siguiente definición:

**Definición 11.55:** Se dice que  $M$  es un  $R$ - $S$ -bimódulo (denotado  ${}_R M_S$ ) si:

BM1.  $(M, +)$  es un grupo abeliano.

BM2.  $(M, +, r \cdot -)$  es un  $R$ -módulo izquierdo.

BM3.  $(M, +, - \cdot s)$  es un  $S$ -módulo derecho.

BM4. Para todo  $m \in M, r \in R, s \in S$  se cumple  $(rm)s = r(ms)$

La ventaja que teníamos en el caso conmutativo ahora es clara: todo  $R$ -módulo ya era simultáneamente un  $R$ - $R$ -bimódulo de forma canónica. Ésto introduce diferencias fundamentales, pero que añaden un toque de color adicional a la teoría. En el caso de que tengamos un objeto sin tanta estructura, por ejemplo un módulo que no sea un bimódulo, podemos «rellenar» los anillos restantes por  $\mathbb{Z}$ , de modo que recuperamos los casos clásicos. Un  $\mathbb{Z}$ - $\mathbb{Z}$ -bimódulo no es más que un grupo abeliano.

**Proposición 11.56:** Sean  $R, S, T$  anillos y sean  ${}_S M_R, {}_T N_R$  bimódulos. Entonces  $\text{Hom}_R({}_S M_R, {}_T N_R)$  es un  $T$ - $S$ -bimódulo con las acciones:

$$\forall s \in S, t \in T, \mathbf{m} \in M \quad (fs)(\mathbf{m}) := f(sm), \quad (tf)(\mathbf{m}) := tf(\mathbf{m}).$$

**Definición 11.57:** Sean  ${}_S M_R, {}_R N_T, {}_S P_T$  bimódulos. Se dice que una aplicación  $\varphi: M \times N \rightarrow P$  es  $(M, N)$ -**balanceada** si:

- BA1. Para todo  $m_1, m_2 \in M, n \in N$  se cumple  $\varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$ .
- BA2. Para todo  $m \in M, n_1, n_2 \in N$  se cumple  $\varphi(m, n_1 + n_2) = \varphi(m, n_1) + \varphi(m, n_2)$ .
- BA3. Para todo  $r \in R$  se cumple que  $\varphi(mr, n) = \varphi(m, rn)$ .
- BA4. Para todo  $s \in S, t \in T$  se cumple que  $\varphi(sm, n) = s\varphi(m, n)$  y  $\varphi(m, nt) = \varphi(m, n)t$ .

Denotamos por  $\text{Bil}_R(M, N; P)$  al conjunto de aplicaciones  $(M, N)$ -balanceadas hacia  $P$ .

**Lema 11.58:** Sean  ${}_S M_R, {}_R N_T, {}_S P_T$  bimódulos. Se cumplen:

1.  $\text{Bil}_R({}_S M_R, {}_R N_T; {}_S P_T)$  es un  $S$ - $T$ -bimódulo.
2. Sea  $f: {}_S M'_R \rightarrow {}_S M_R$  un homomorfismo de  $R$ -módulos derechos. Entonces

$$\begin{aligned} h_f: \text{Bil}_R(M, N; P) &\longrightarrow \text{Bil}_R(M', N; P) \\ \varphi(m, n) &\longmapsto \varphi(f(m'), n) \end{aligned}$$

es un homomorfismo de grupos abelianos. Así,  $\text{Bil}_R({}_S M_R, {}_R N_T; {}_S P_T): {}_S \text{Mod}_R \rightarrow {}_S \text{Mod}_T$  es un funtor contravariante.

3. Sea  $g: {}_R N'_T \rightarrow {}_R N_T$  un homomorfismo de  $R$ -módulos izquierdos. Entonces

$$\begin{aligned} h_g: \text{Bil}_R(M, N; P) &\longrightarrow \text{Bil}_R(M, N'; P) \\ \varphi(m, n) &\longmapsto \varphi(m, g(n')) \end{aligned}$$

es un homomorfismo de grupos abelianos. Así,  $\text{Bil}_R(M, {}_R N_T; {}_S P_T): {}_R \text{Mod}_T \rightarrow {}_S \text{Mod}_T$  es un funtor contravariante.

4. Sea  $\psi: {}_S P_T \rightarrow {}_S P'_T$  un homomorfismo de  $S$ - $T$ -bimódulos. Entonces

$$\begin{aligned} h^\psi: \text{Bil}_R(M, N; P) &\longrightarrow \text{Bil}_R(M, N; P') \\ \varphi(m, n) &\longmapsto \psi(\varphi(m, n)) \end{aligned}$$

es un homomorfismo de grupos abelianos. Así,  $\text{Bil}_R(M, N; {}_S -_T): {}_S \mathbf{Mod}_T \rightarrow {}_S \mathbf{Mod}_T$  es un funtor covariante.

**Teorema 11.59:** El funtor  $\text{Bil}_R({}_S M_R, {}_R N_T; {}_S -_T)$  es representable por un objeto  ${}_S M \otimes_R N_T$ . Vale decir, para todo bimódulo  ${}_S P_T$  y toda aplicación  $\varphi \in \text{Bil}_R(M, N; P)$  existe un único homomorfismo de  $S$ - $T$ -bimódulos  $\bar{\varphi}: M \otimes_R N \rightarrow P$  tal que el siguiente diagrama conmuta (en Set):

$$\begin{array}{ccc} {}_S M_R \times {}_R N_T & \xrightarrow{\varphi} & {}_S P_T \\ & \searrow \otimes & \nearrow \exists! \bar{\varphi} \\ & {}_S M \otimes_R N_T & \end{array}$$

A  $M \otimes_R N$  se le dice el **producto tensorial** de  ${}_S M_R, {}_R N_T$ .

Recordemos un par de hechos acerca del producto tensorial:

- La aplicación  $\otimes: M \times N \rightarrow M \otimes_R N$  induce elementos de la forma  $m \otimes n$  llamados **tensores puros**. Éstos no corresponden a la totalidad de elementos de  ${}_S M \otimes_R N_T$ , sino que generan (como  $S$ - $T$ -bimódulo) a la totalidad de tensores.
- En consecuencia, si queremos construir un homomorfismo  $f: {}_S M \otimes_R N_T \rightarrow {}_S P_T$  podemos hacerlo especificando sus valores exclusivamente en los tensores puros. Ésta es una práctica de todos los libros de álgebra.
- Otra consecuencia es que si  $X \subseteq M$  e  $Y \subseteq N$  son sistemas generadores de  ${}_S M_R, {}_R N_T$  resp. entonces  $X \otimes_R Y = \{x \otimes y : x \in X, y \in Y\}$  es un sistema generador de  ${}_S M \otimes_R N_T$ .

**Lema 11.60:** Sean  ${}_S M_R, {}_R N_T$  un par de módulos. Dados  $f: {}_S M_R \rightarrow {}_S M'_R$  y  $g: {}_R N_T \rightarrow {}_R N'_T$  homomorfismos de  $R$ -módulos. Entonces

$$\begin{aligned} f \otimes g: M \otimes_R N &\longrightarrow M' \otimes_R N' \\ m \otimes n &\longmapsto f(m) \otimes g(n) \end{aligned}$$

es un homomorfismo de  $S$ - $T$ -bimódulos. Así,  $- \otimes_R -: {}_S \mathbf{Mod}_R \times {}_R \mathbf{Mod}_T \rightarrow {}_S \mathbf{Mod}_T$  es un bifunctor.



**Teorema 11.61:** Sean  ${}_S M_R, {}_R N_T$  un par de bimódulos. Entonces para todo  ${}_S P_T$  bimódulo se cumple:

$$\mathrm{Hom}_{{}_S \mathrm{Mod}_T}(M \otimes_R N, P) \cong \mathrm{Hom}_{{}_S \mathrm{Mod}_T}(M, \mathrm{Hom}_T(N, P)).$$

Así,  ${}_S -_R \otimes_R N \dashv \mathrm{Hom}_T(N, {}_S -_T)$ .

**Proposición 11.62:** Sean  $R, S, T$  anillos.

1. Dados  $(M_i)_{i \in I}$  una familia de  $S$ - $R$ -módulos y  ${}_R N_T$ , entonces:

$$\left( \bigoplus_{i \in I} M_i \right) \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N)$$

(en  ${}_S \mathrm{Mod}_T$ ).

2. Dados  ${}_S M_R$  y  $(N_j)_{j \in J}$  una familia de  $R$ - $T$ -módulos, entonces:

$$M \otimes_R \left( \bigoplus_{j \in J} N_j \right) \cong \bigoplus_{j \in J} (M \otimes_R N_j).$$

3. Si  ${}_S M_R$  es un bimódulo, entonces  $M \otimes_R R \cong M$  (en  ${}_S \mathrm{Mod}_R$ ).
4. Si  ${}_R N_T$  es un bimódulo, entonces  $R \otimes_R N \cong N$  (en  ${}_R \mathrm{Mod}_T$ ).
5. Sean  ${}_S M_R, {}_R N_T$  un par de bimódulos. Entonces los funtores  $- \otimes_R N: {}_S \mathrm{Mod}_R \rightarrow {}_S \mathrm{Mod}_T$  y  $M \otimes_R -: {}_R \mathrm{Mod}_T \rightarrow {}_S \mathrm{Mod}_T$  son exactos por la derecha.

**Definición 11.63:** Un  $R$ -módulo  $M_R$  se dice **plano** si el funtor  $M \otimes_R -: {}_R \mathrm{Mod} \rightarrow \mathbf{Ab}$  es exacto.

Otra propiedad útil:

**Teorema 11.64:** Todo  $R$ -módulo proyectivo es plano.

### §11.3.2 El teorema de Eilenberg-Watts y equivalencia de Morita.

Ahora nos adentramos a demostrar el resultado mencionado en la introducción. En primer lugar, un poco de terminología: recuerde que un funtor aditivo (entre categorías aditivas) es uno que preserva coproductos finitos.

Un funtor exacto por la derecha es un funtor aditivo que preserva conúcleos, luego es lo mismo que un funtor que preserva límites directos finitos. Así, un funtor exacto por la derecha que preserva coproductos pequeños es precisamente lo mismo que un funtor que preserva límites directos.

En primer lugar, veamos qué esperaríamos de la categoría de módulos. Ya sabemos que ésta categoría es bicompleta, bien potenciada y bien co-potenciada así que, para emplear a diestra y siniestra el teorema especial del funtor adjunto habría que entender a los generadores de la categoría de módulos. Una definición preliminar:

**Definición 11.65:** Sea  $M_\Lambda$  un módulo. Se define el *ideal traza* de  $M$  como:

$$T(M) := \{\varphi(x) : x \in M, \varphi \in \text{Hom}_\Lambda(M, \Lambda)\}.$$

**Teorema 11.66:** Sea  $G$  un  $\Lambda$ -módulo. Son equivalentes:

1.  $G$  es un objeto generador de  $\text{Mod}_\Lambda$ .
2. El ideal traza  $T(G) = \Lambda$ .
3. Existe un  $n$  tal que  $\Lambda$  es la imagen epimórfica de algún  $G^{\oplus n}$ .
4. Todo módulo es la suma de imágenes epimórficas de  $G$ .

DEMOSTRACIÓN:  $1 \implies 2$ . Consideremos el homomorfismo de  $\Lambda$ -módulos  $\pi: \Lambda \rightarrow \Lambda/T(G)$ . Para todo  $g \in \text{Hom}_\Lambda(G, \Lambda)$  y todo  $x \in G$  tenemos que  $g(x) \in T(G)$  por definición, luego  $g \circ \pi = 0$  para todo  $g \in \text{Hom}_\Lambda(G, \Lambda)$ , es decir,  $h^\pi = 0$ . Como  $G$  es proyectivo, esto significa que  $\pi = 0$  y luego  $\Lambda = T(G)$ .

$2 \implies 3$ . Por definición, tenemos que  $1 = \sum_{i=1}^n f_i(x_i)$  donde  $x_i \in G$  y  $f_i \in \text{Hom}_\Lambda(G, \Lambda)$ . Fijamos los  $f_i$ 's y notamos que la siguiente aplicación:

$$\begin{aligned} g: G^{\oplus n} &\longrightarrow \Lambda \\ (y_1, \dots, y_n) &\longmapsto \sum_{i=1}^n f_i(y_i) \end{aligned}$$

es un epimorfismo.

$3 \implies 4$ . Todo módulo es la suma de  $\Lambda$ .

$4 \implies 1$ . Sean  $M, N$  un par de  $\Lambda$ -módulos arbitrarios.  $G$  es un objeto proyectivo syss  $\text{Hom}_\Lambda(G, -)$  es fiel, lo que equivale a ver que para todo homomorfismo  $f: M \rightarrow N$  no nulo se cumple que  $\text{Hom}(G, f)$  no es nulo.

Como  $M$  es una suma de imágenes epimórficas de  $G$ , se cumple que  $M = \sum_{g \in \text{Hom}(G, M)} g[G]$ , luego si  $g \circ f = 0$  para todo  $g \in \text{Hom}(G, M)$ , se ha de cumplir que  $f[M] = \sum_{g \in \text{Hom}(G, M)} f[g[G]] = 0$ , por lo que  $f = 0$  como se quería ver.  $\square$

Como corolario,  $\Lambda$  siempre es un generador de  $\text{Mod}_\Lambda$ .

**Lema 11.67:** La categoría  $\text{Mod}_\Lambda$  posee un cogenerador inyectivo.

DEMOSTRACIÓN: Sea  $B := \coprod_{\mathfrak{a}} \Lambda/\mathfrak{a}$ , donde  $\mathfrak{a}$  recorre todos los ideales derechos de  $\Lambda$ , y sea  $C$  un módulo inyectivo que contenga a  $B$  (por ejemplo, su envoltura inyectiva). Veremos que para todo  $\Lambda$ -módulo  $M$  y todo  $\mathbf{m} \in M \neq 0$  existe un  $f: M \rightarrow C$  tal que  $f(\mathbf{m}) \neq 0$ . Para ello, nótese que el submódulo  $N := \mathbf{m} \cdot \Lambda$  es isomorfo a  $\Lambda/\mathfrak{a}$ , donde  $\mathfrak{a} \trianglelefteq \Lambda$  es un ideal derecho. Luego existe un monomorfismo  $g: N \rightarrow C$  que, en particular, es una flecha que no se anula en  $\mathbf{m}$  y tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} & & C \\ & \nearrow f & \uparrow g \\ M & \xleftarrow{\iota} & N \end{array}$$

Luego  $f: M \rightarrow C$  no se anula en  $\mathbf{m}$  como queríamos.  $\square$

Ahora podríamos emplear el teorema especial del funtor adjunto, pero el siguiente teorema nos dirá bastante más:

**Teorema 11.68 – Teorema de Eilenberg-Watts:** Sea  $F: \text{Mod}_\Lambda \rightarrow \text{Mod}_\Gamma$  un funtor que preserva límites directos. Entonces existe un bimódulo  ${}_\Lambda N_\Gamma$  tal que  $F$  es equivalente a  $- \otimes_\Lambda N$  y, de hecho,  $N = F(\Lambda)$ .

DEMOSTRACIÓN: Definamos  $N := F\Lambda$ , el cual es un  $\Gamma$ -módulo derecho. En primer lugar para todo módulo  $M_\Lambda$  y todo  $\mathbf{m} \in M$  se cumple que

$$\begin{aligned} \varphi_{\mathbf{m}}: \Lambda &\longrightarrow M \\ r &\longmapsto \mathbf{m}r \end{aligned}$$

es un homomorfismo de  $\Lambda$ -módulos derechos. Luego induce un homomorfismo  $F(\varphi_{\mathbf{m}}): N \rightarrow FM$  y definimos:

$$\begin{aligned} \tau_M: M \times N &\longrightarrow FM \\ (\mathbf{m}, x) &\longmapsto F(\varphi_{\mathbf{m}})(x) \end{aligned}$$

el cual es una aplicación  $\mathbb{Z}$ -balanceada, pero podemos decir más. Considerando  $M = \Lambda$ , vemos que  $\tau_\Lambda$  le da una estructura de bimódulo a  ${}_\Lambda N_\Gamma$ . Bajo ésta estructura es fácil ver que para un módulo arbitrario  $M_\Lambda$  tenemos que  $\tau_\Lambda$  es una aplicación  $\Lambda$ -balanceada. Luego existe un único homomorfismo de  $\Gamma$ -módulos  $\sigma_M: M \otimes_\Lambda N \rightarrow FM$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi_M} & FM \\ & \searrow \otimes_\Lambda & \nearrow \exists! \sigma_M \\ & M \otimes_\Lambda N & \end{array}$$

Es fácil ver que  $\sigma: - \otimes_\Lambda N \Rightarrow F$  es una transformación natural. Por definición se satisface que  $\sigma_\Lambda: \Lambda \otimes_\Lambda N \rightarrow N$  es un isomorfismo, y como tanto  $- \otimes_\Lambda N$  como  $F$  preservan coproductos, tenemos que  $\sigma$  es un isomorfismo sobre todos los  $\Lambda$ -módulos libres.

Sea  $M_\Lambda$  arbitrario, y sea  $A \rightarrow B \rightarrow M \rightarrow 0$  una sucesión exacta con  $A, B$  libres. Luego se induce el siguiente diagrama conmutativo con filas exactas (en  $\mathbf{Mod}_\Gamma$ ):

$$\begin{array}{ccccccc} A \otimes_\Lambda N & \longrightarrow & B \otimes_\Lambda N & \longrightarrow & M \otimes_\Lambda N & \longrightarrow & 0 \\ \sigma_A \downarrow \wr & & \sigma_B \downarrow \wr & & \sigma_M \downarrow & & \\ F(A) & \longrightarrow & F(B) & \longrightarrow & F(M) & \longrightarrow & 0 \end{array}$$

Luego aplicando el lema de los cinco, concluimos que  $\sigma_M$  también es un isomorfismo.  $\square$

**Corolario 11.68.1:** Dado un funtor  $F: \mathbf{Mod}_\Lambda \rightarrow \mathbf{Mod}_\Gamma$ . Son equivalentes:

1.  $F$  preserva límites directos.
2.  $F$  es exacto por la derecha y preserva coproductos.
3.  $F$  es equivalente a  $- \otimes_\Lambda N$  para algún bimódulo  ${}_\Lambda N_\Gamma$ .
4.  $F$  tiene adjunta derecha.

Veamos las otras formas (semi)duales de Eilenberg-Watts:<sup>2</sup>

<sup>2</sup>Decimos «semiduales», porque *a priori* no tenemos ninguna estructura conocida para la categoría  $\mathbf{Mod}_\Lambda^{\text{op}}$ , aun que éstas versiones si se encargan de funtores contravariantes o de otras clases de límites.

**Teorema 11.69 – Teorema de Eilenberg-Watts:** 1. Sea  $F: \text{Mod}_\Lambda \rightarrow {}_\Gamma\text{Mod}$  un funtor contravariante que transforma límites directos en límites inversos. Entonces existe un bimódulo  ${}_ \Gamma N_\Lambda$  tal que  $F \cong \text{Hom}_\Lambda(-, N)$ .

2. Sea  $G: \text{Mod}_\Lambda \rightarrow \text{Mod}_\Gamma$  un funtor que preserva límites inversos. Entonces existe un bimódulo  ${}_ \Gamma N_\Lambda$  tal que  $F \cong \text{Hom}_\Lambda(N, -)$ .

DEMOSTRACIÓN:

1. Nuevamente elegimos  $N := F\Lambda$  y dado un módulo  $M_\Lambda$  para todo  $\mathbf{m} \in M$  definimos:

$$\begin{aligned}\varphi_{\mathbf{m}}: \Lambda &\longrightarrow M \\ r &\longmapsto \mathbf{m}r.\end{aligned}$$

Así pues, obtenemos  $F(\varphi_{\mathbf{m}}): FM \rightarrow N$  y definamos:

$$\begin{aligned}\tau_M: M \times FM &\longrightarrow N \\ (\mathbf{m}, x) &\longmapsto F(\varphi_{\mathbf{m}})(x).\end{aligned}$$

En particular, con  $M = \Lambda$  tenemos una estructura de  $\Gamma$ - $\Lambda$ -bimódulo para  $N$ .

Luego queremos construir una transformación natural  $\sigma_M: FM \rightarrow \text{Hom}_\Lambda(M, N)$  que a cada  $x \in FM$  le asigna  $\sigma_M(x)$  que es un homomorfismo sobre  $M$ , digamos  $\sigma_M(x)(\mathbf{m}) := \tau_M(\mathbf{m}, x)$ . Siguiendo la demostración anterior llegamos a la misma conclusión.

2. También podríamos seguir un procedimiento similar, pero he aquí un procedimiento más ingenioso. Por el teorema especial del funtor adjunto tenemos que  $G$  admite adjunta izquierda  $F: \text{Mod}_\Gamma \rightarrow \text{Mod}_\Lambda$ , la cual preserva límites directos; luego por Eilenberg-Watts tenemos que  $F \cong - \otimes_\Gamma N$  para algún bimódulo  ${}_ \Gamma N_\Lambda$  y, por lo tanto, la adjunta derecha de  $F$  es  $\text{Hom}_\Lambda(N, -)$ ; pero la adjunta es única salvo isomorfismo (entre funtores).  $\square$

Ahora procedemos a demostrar los resultados centrales de la teoría de Morita. Seguimos la enumeración de JACOBSON [0], Vol. II, §3.12 y §3.15

**Corolario 11.69.1 (Morita II):** Sean  $\Gamma, \Lambda$  un par de anillos y sea  $F: \text{Mod}_\Gamma \rightarrow \text{Mod}_\Lambda$  un funtor. Son equivalentes:

1.  $F$  es una equivalencia de categorías.
2. Existen bimódulos  ${}_{\Gamma}P_{\Lambda}$  y  ${}_{\Lambda}Q_{\Gamma}$  e isomorfismos de bimódulos  $\tau: P \otimes_{\Lambda} Q \xrightarrow{\sim} \Gamma$  y  $\mu: Q \otimes_{\Gamma} P \xrightarrow{\sim} \Lambda$ , tales que  $F = - \otimes_{\Lambda} Q$ .

DEMOSTRACIÓN: Basta notar que toda equivalencia de categorías preserva límites inversos y directos, de modo que es de la forma  $- \otimes_{\Lambda} Q$ . Lo mismo aplica para una cuasi-inversa suya, y las transformaciones naturales prueban los isomorfismos descritos.  $\square$

**Definición 11.70:** Dos anillos  $\Gamma, \Lambda$  se dicen *Morita-equivalentes* si sus categorías de módulos izquierdos  $\text{Mod}_{\Gamma}, \text{Mod}_{\Lambda}$  son equivalentes. Por el corolario anterior, esto equivale a que exista una tupla  $(\Lambda, \Gamma, P, Q, \tau, \mu)$  como antes, llamada un *contexto de Morita*.

Un  $\Lambda$ -módulo (izquierdo) se dice un *progenerador* si es un generador proyectivo finitamente generado (izquierdo).

Por el corolario anterior, esto equivale a que sus categorías de módulos derechos sean equivalentes.

**Lema 11.71:** Sea  ${}_{\Lambda}M$  un  $\Lambda$ -módulo izquierdo y sea  $\Gamma := \text{End}_{\Lambda}(M)$ . Si  ${}_{\Lambda}M$  es un generador (resp. módulo proyectivo finitamente generado), entonces  $M_{\Gamma}$  es un módulo proyectivo finitamente generado (resp. generador).

DEMOSTRACIÓN: Sabemos que las categorías de  $\Lambda$ -módulos son cocompletas, de modo que  $M$  es un generador syss existe un epimorfismo (i.e., un homomorfismo sobreyectivo)  $\varphi: M^{\oplus \kappa} \rightarrow \Lambda$  para algún  $\kappa$ ; así el  $1 \in \Lambda$  es la imagen de alguna tupla con finitas coordenadas no nulas, lo que comprueba que podemos suponer que  $\kappa = n$  es finito. Como  $\Lambda$  es un objeto proyectivo, entonces  $M^n \cong \Lambda \oplus K$  para algún  ${}_{\Lambda}K$  y, aplicando  $\text{Hom}_{\Lambda}(-, M)$  a ambos lados, obtenemos que  $\Gamma^n \cong M \oplus \text{Hom}_{\Lambda}(K, M)$ . Así pues,  $M$  es proyectivo (por ser sumando directo de un módulo libre) y finitamente generado.  $\square$

**Teorema 11.72 (de Morita I):** Sean  $\Gamma, \Lambda$  un par de anillos con bimódulos  ${}_{\Gamma}P_{\Lambda}, {}_{\Lambda}Q_{\Gamma}$ , y homomorfismos sobreyectivos de bimódulos  $\tau: P \otimes_{\Lambda} Q \rightarrow \Gamma, \mu: Q \otimes_{\Gamma} P \rightarrow \Lambda$  tales que los siguientes diagramas conmutan:

$$\begin{array}{ccc}
Q \otimes_{\Gamma} P \otimes_{\Lambda} Q & \xrightarrow{\text{Id}_Q \otimes_{\Gamma} \tau} & Q \otimes_{\Gamma} \Gamma \\
\mu \otimes_{\Lambda} \text{Id}_Q \downarrow & & \downarrow \wr \\
\Lambda \otimes_{\Lambda} Q & \xrightarrow{\sim} & Q
\end{array}
\quad
\begin{array}{ccc}
P \otimes_{\Lambda} Q \otimes_{\Gamma} P & \xrightarrow{\text{Id}_P \otimes_{\Lambda} \mu} & P \otimes_{\Lambda} \Lambda \\
\tau \otimes_{\Gamma} \text{Id}_P \downarrow & & \downarrow \wr \\
\Gamma \otimes_{\Gamma} P & \xrightarrow{\sim} & P
\end{array}$$

Entonces:

1.  $(\Gamma, \Lambda, P, Q, \tau, \mu)$  es un contexto de Morita; vale decir,  $\tau, \mu$  son isomorfismos de bimódulos.
2.  $\text{Hom}_{\Lambda}(P, \Lambda) \cong Q$ ,  $\text{Hom}_{\Gamma}(Q, \Gamma) \cong P$ ,  $\text{Hom}_{\Lambda}(Q, \Lambda) \cong P$  y  $\text{Hom}_{\Gamma}(P, \Gamma) \cong Q$ .
3. Los homomorfismos canónicos de anillos son isomorfismos:

$$\text{End}_{\Lambda}(P) \xleftarrow{\sim} \Gamma \xrightarrow{\sim} \text{End}_{\Lambda}(Q) \quad \text{End}_{\Gamma}(P) \xleftarrow{\sim} \Lambda \xrightarrow{\sim} \text{End}_{\Gamma}(Q)$$

4.  $P_{\Lambda}, Q_{\Gamma}, {}_{\Gamma}P, {}_{\Lambda}Q$  son progeneradores.
5. Los centros de  $\Gamma, \Lambda$  son isomorfos.

DEMOSTRACIÓN: En la demostración, dados  $p \in P, q \in Q$  denotamos por corchetes  $(p, q) := \tau(p \otimes_{\Lambda} q)$  y  $[q, p] := \mu(q \otimes_{\Gamma} p)$ . La conmutatividad de los diagramas ahora se traduce en las identidades:

$$\forall x \in {}_{\Lambda}P, y \in Q_{\Gamma} \quad (p, q)x = p[q, x], \quad y(p, q) = [y, p]q.$$

1. Como  $\tau, \mu$  son sobreyectivos por construcción basta probar que tienen núcleos nulos. Sean  $\sum_{i=1}^n x_i \otimes y_i \in \ker \tau$ , vale decir,  $\sum_{i=1}^n (x_i, y_i) = 0$ . Sean  $p_j \in P, q_j \in Q$  tales que  $\sum_{j=1}^m (p_j, q_j) = 1 \in \Lambda$ . Entonces

$$\begin{aligned}
\sum_{i=1}^n x_i \otimes y_i &= \sum_{i,j} x_i \otimes y_i(p_j, q_j) = \sum_{i,j} x_i \otimes [y_i, p_j]q_j \\
&= \sum_{i,j} x_i[y_i, p_j] \otimes q_j = \sum_{i,j} (x_i, y_i)p_j \otimes q_j = 0,
\end{aligned}$$

como se quería probar. El caso de  $\mu$  es análogo.

2. Como  $(\Gamma, \Lambda, P, Q, \tau, \mu)$  es un contexto de Morita, entonces  $F := - \otimes_{\Gamma} P$  es una equivalencia de categorías cuya inversa es  $G := - \otimes_{\Lambda} Q$ . Empleando que  $\text{Hom}(FX, FY) \cong \text{Hom}(X, Y)$  para un funtor  $F$  plenamente fiel, tenemos que

$$\text{Hom}_{\Gamma}(A, Q) \cong \text{Hom}_{\Lambda}(A \otimes_{\Gamma} P, Q \otimes_{\Gamma} P) \cong \text{Hom}_{\Lambda}(A \otimes_{\Gamma} P, \Lambda) \cong \text{Hom}_{\Gamma}(A, \text{Hom}_{\Lambda}(P, \Lambda)).$$

Por lo que el lema de Yoneda nos dice que  $Q \cong \text{Hom}_\Lambda(P, \Lambda)$ .

Un ejercicio similar sirve para el resto.

3. Es análogo al inciso anterior.

4. Es una mera aplicación del lema anterior.

5. ... □

En consecuencia del último inciso, la equivalencia de Morita sobre dominios (i.e., anillos conmutativos) se reduce a isomorfismo. La teoría de Morita tiene sus importantes consecuencias, un ejemplo es el siguiente:

**Teorema 11.73 – Teorema de Wedderburn-Artin:** Sea  $\Lambda$  un anillo. Son equivalentes:

1.  $\Lambda$  es simple y posee un ideal izquierdo (resp. derecho) minimal.
2.  $\Lambda \cong \text{End}_D(V)$ , donde  $D$  es un anillo de división y  $V$  es un  $D$ -espacio vectorial de dimensión finita.
3.  $\Lambda$  es un anillo simple, artinian por la izquierda y derecha, y noetheriano por la izquierda y derecha.

DEMOSTRACIÓN:  $1 \implies 2$ . Sea  $\mathfrak{a}$  un ideal izquierdo minimal de  $\Lambda$ , de modo que es un  $\Lambda$ -módulo simple. Considere  $\mathfrak{a}\Lambda = \sum_{\lambda \in \Lambda} \mathfrak{a}\lambda$ , el cual es un ideal bilateral que contiene a  $\mathfrak{a}$ . Por simplicidad  $\mathfrak{a}\Lambda = \Lambda$  y, por tanto,  $1 = \sum_{i=1}^m a_i \lambda_i$  para algunos  $a_i \in \mathfrak{a}, \lambda_i \in \Lambda$ . Así pues,  $\Lambda = \sum_{i=1}^m \mathfrak{a}\lambda_i$  y para cada  $\lambda \in \Lambda$  vemos que  $a \mapsto a\lambda$  es un homomorfismo de  ${}_A\mathfrak{a}$  de modo que por el lema de Schur, o bien  $\mathfrak{a}\lambda = 0$  o bien  $\mathfrak{a}\lambda \cong \mathfrak{a}$  como  $\Lambda$ -módulos izquierdos. En conclusión,  ${}_A\Lambda$  es un  $\Lambda$ -módulo izquierdo semisimple y por el teorema 5.28 vemos que  $\Lambda \cong \mathfrak{a} \oplus \mathfrak{b}$ , donde  $\mathfrak{b}$  es otro  $\Lambda$ -módulo izquierdo.

Así pues,  $\mathfrak{a}$  es un  $\Lambda$ -módulo proyectivo y está generado por un solo elemento, por lo que, por el lema de las bases duales,  $T(\mathfrak{a}) \neq 0$  y como es un ideal bilateral, entonces  $T(\mathfrak{a}) = A$ . Por lo tanto,  $\mathfrak{a}$  es un progenerador. Definiendo  $\Gamma := \text{End}({}_A\mathfrak{a})$ , vemos que es un anillo de división por el lema de Schur, y  $\mathfrak{a}^* := \text{Hom}_\Lambda(\mathfrak{a}, \Lambda)$  es tal que  $(\Lambda, \Gamma, \mathfrak{a}, \mathfrak{a}^*, \tau, \mu)$  conforma un contexto de Morita, donde  $\tau, \mu$  son los homomorfismos canónicos inducidos por adjunción del tensor. Por el teorema de Morita I vemos que  $\Lambda \cong \text{End}_\Gamma(\Gamma\mathfrak{a}^*)$ , donde  $\Gamma = D$  es un anillo de división y  $\mathfrak{a}^*$  es un  $\Gamma$ -espacio vectorial de dimensión finita.

$2 \implies 3$ . Sea  $\Lambda := \text{End}_D(V)$  por construcción, donde  $D$  es de división y  $V$  es un  $D$ -espacio vectorial izquierdo de dimensión finita. Pasando al anillo



opuesto  $\Delta := D^{\text{op}}$  vemos a  $V$  como  $\Delta$ -espacio vectorial derecho, el cual es un objeto proyectivo de dimensión finita. Más aún,  $T(V_\Delta) = \Delta$ , por lo que  $V_\Delta$  es un progenerador. Así,  $(\Lambda, \Delta := \text{End}(V_\Delta), V, V^* := \text{Hom}(V_\Delta, \Delta), \tau, \mu)$  conforma un contexto de Morita y, mediante las equivalencias functoriales, hay un isomorfismo entre el retículo de ideales izquierdos de  $\Lambda$  y los submódulos de  $V^*$ , y un isomorfismo entre el retículo de ideales derechos de  $\Gamma$  y los submódulos de  $V$ . Como tanto  $V$  como  $V^*$  son espacios vectoriales de dimensión finita sobre anillos de división, entonces ambos son noetherianos y artinianos, de lo que se concluye lo exigido.

3  $\implies$  1. Trivial.  $\square$

**Proposición 11.74:** Sean  $\Gamma, \Lambda$  un par de anillos Morita-equivalentes, entonces tienen retículos de ideales bilaterales isomorfos. En consecuencia,  $\Gamma$  es (semi)simple syss  $\Lambda$  lo es.

**§11.3.3 El funtor Tor.** Así como Ext arregla el fallo de exactitud de Hom, uno quiere un funtor que arregle el fallo de exactitud de  $\otimes$ .

**Definición 11.75:** Sea  $\Lambda$  un anillo y  $A$  un  $\Lambda$ -módulo. Una *presentación plana* de  $A$  es una sucesión exacta corta del estilo:

$$0 \longrightarrow R \xrightarrow{\ker(\varepsilon)} P \xrightarrow{\varepsilon} A \longrightarrow 0,$$

donde  $P$  es un  $\Lambda$ -módulo plano.

Como los módulos proyectivos son planos, entonces todo módulo admite una presentación plana.

**Definición 11.76:** Sea  $\Lambda$  un anillo y  $A_\Lambda, {}_\Lambda B$  módulos. Sea  $R \rightarrow P \xrightarrow{\varepsilon} B$  una presentación plana de  $B$ , se define:

$$0 \longrightarrow \text{Tor}_\varepsilon^\Lambda(A, B) \xrightarrow{\exists!} A \otimes_\Lambda R \longrightarrow A \otimes_\Lambda P \longrightarrow A \otimes_\Lambda B \longrightarrow 0$$

Análogamente, sea  $S \rightarrow Q \xrightarrow{\eta} A$  una presentación plana de  $A$ , se define:

$$0 \longrightarrow \overline{\text{Tor}}_\eta^\Lambda(A, B) \xrightarrow{\exists!} S \otimes_\Lambda B \longrightarrow Q \otimes_\Lambda B \longrightarrow A \otimes_\Lambda B \longrightarrow 0$$

**Proposición 11.77:** Sean  $A_\Lambda, {}_\Lambda B$  un par de módulos. Entonces:

1. Si  $A$  es plano, entonces  $\text{Tor}^\Lambda(A, B) = 0$ . Si  $B$  es plano, entonces  $\overline{\text{Tor}}^\Lambda(A, B) = 0$ .

- Teorema 11.78:** Sea  $R \rightarrow P \xrightarrow{\varepsilon} B$  una presentación plana de  ${}_A B$  y sea  $S \rightarrow Q \xrightarrow{\eta} A$  una presentación plana de  $A_A$ . Entonces (en  $\mathbf{Ab}$ ):

En consecuencia,  $\text{Tor}^\Lambda(A, B)$  es independiente de la elección de  $\varepsilon$  o de  $\eta$ .

$$\begin{array}{ccccccc}
& & & & 0 & \longrightarrow & \overline{\mathrm{Tor}}_{\eta}^{\Lambda}(A, B) \\
& & & & \downarrow & \searrow \Sigma_1 & \downarrow \\
& & S \otimes_{\Lambda} R & \longrightarrow & S \otimes_{\Lambda} P & \longrightarrow & S \otimes_{\Lambda} B \\
& & \downarrow & \searrow \Sigma_3 & \downarrow & \searrow \Sigma_2 & \downarrow \\
0 & \longrightarrow & Q \otimes_{\Lambda} R & \longrightarrow & Q \otimes_{\Lambda} P & \longrightarrow & Q \otimes_{\Lambda} B \\
& \downarrow \Sigma_5 & \downarrow & \searrow \Sigma_4 & \downarrow & & \downarrow \vdots \\
\mathrm{Tor}_{\varepsilon}^{\Lambda}(A, B) & \longrightarrow & A \otimes_{\Lambda} R & \longrightarrow & A \otimes_{\Lambda} P & \cdots \cdots \longrightarrow & A \otimes_{\Lambda} B
\end{array}$$
$$\mathrm{Tor}_\varepsilon^\Lambda(A, B) \cong \overline{\mathrm{Tor}}_\eta^\Lambda(A, B) \cong \mathrm{Tor}_{\varepsilon'}^\Lambda(A, B). \quad \square$$

**Teorema 11.79:** Dada una sucesión exacta  $0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0$  de  $\Lambda$ -módulos izquierdos y otro módulo  $B_\Lambda$ , se induce la siguiente sucesión exacta:

$$\begin{array}{ccccccc} \mathrm{Tor}^\Lambda(A_1, B) & \longrightarrow & \mathrm{Tor}^\Lambda(A_2, B) & \longrightarrow & \mathrm{Tor}^\Lambda(A_3, B) & \xrightarrow{\quad\quad\quad} \\ & & & & & \searrow \scriptstyle \omega \\ & & & & & A_3 \otimes_\Lambda B \\ & & & & & \downarrow \\ & & & & & 0 \end{array}$$

<sup>3</sup>No, no me refiero al lema de Zorn, aunque buena elección.

**Teorema 11.80:** Dada una sucesión exacta  $0 \rightarrow B_1 \rightarrow B_2 \rightarrow B_3 \rightarrow 0$  de  $\Lambda$ -módulos derechos y otro módulo  ${}_A A$ , se induce la siguiente sucesión exacta:

$$\begin{array}{ccccccc} \mathrm{Tor}^\Lambda(A, B_1) & \longrightarrow & \mathrm{Tor}^\Lambda(A, B_2) & \longrightarrow & \mathrm{Tor}^\Lambda(A, B_3) & \longrightarrow & 0 \\ & & & & \searrow \omega & & \\ & & & & & & \\ \downarrow & & & & & & \\ A \otimes_\Lambda B_1 & \longrightarrow & A \otimes_\Lambda B_2 & \longrightarrow & A \otimes_\Lambda B_3 & \longrightarrow & 0 \end{array}$$

**Corolario 11.80.1:** Se cumplen:

1. Si  $\Lambda$  es hereditario izquierdo, dada una sucesión exacta  $0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0$  de  $\Lambda$ -módulos izquierdos y otro módulo  $B_\Lambda$ , se induce la siguiente sucesión exacta:

$$0 \longrightarrow \mathrm{Tor}^\Lambda(A_1, B) \longrightarrow \mathrm{Tor}^\Lambda(A_2, B) \longrightarrow \mathrm{Tor}^\Lambda(A_3, B)$$

2. Si  $\Lambda$  es hereditario derecho, dado un módulo  ${}_A A$  y una sucesión exacta  $0 \rightarrow B_1 \rightarrow B_2 \rightarrow B_3 \rightarrow 0$  de  $\Lambda$ -módulos derechos, se induce la siguiente sucesión exacta:

$$0 \longrightarrow \mathrm{Tor}^\Lambda(A, B_1) \longrightarrow \mathrm{Tor}^\Lambda(A, B_2) \longrightarrow \mathrm{Tor}^\Lambda(A, B_3)$$

**Proposición 11.81:** Sea  $\Lambda$  un anillo.

1. El  $\Lambda$ -módulo (derecho)  $\Lambda$  es plano.
2. Una suma directa  $\bigoplus_{i \in I} M_i$  de  $\Lambda$ -módulos  $M_i$  es plana syss cada  $M_i$  es plano.
3. Todo  $\Lambda$ -módulo proyectivo es plano.

DEMOSTRACIÓN:

1. Ejercicio para el lector.
2. Como tensorizar es un funtor exacto por la derecha, entonces preserva límites directos y, por tanto,  $(\bigoplus_{i \in I} M_i) \otimes_\Lambda N \cong \bigoplus_{i \in I} (M_i \otimes_\Lambda N)$ .
3. Basta recordar que todo módulo proyectivo es el sumando directo de algún módulo libre, los cuales son planos por el inciso anterior.  $\square$

**Proposición 11.82:** Sea  $M_\Lambda$  un  $\Lambda$ -módulo (derecho). Si todo submódulo finitamente generado de  $M$  es plano, entonces  $M$  también lo es.

DEMOSTRACIÓN: Sea  $0 \rightarrow {}_\Lambda A \xrightarrow{\varphi} {}_\Lambda B$  una sucesión exacta, basta ver que  $\ker(\text{Id}_M \otimes \varphi) = 0$ . Para ello nótese que todo elemento  $u \in \ker(\text{Id}_M \otimes \varphi)$  es de la forma

$$u = \sum_{j=1}^n m_j \otimes a_j, \quad m_j \in M, a_j \in A.$$

Definiendo  $N := \sum_{j=1}^n m_j \Lambda \leq M$  es claro que es un submódulo finitamente generado, y vemos que  $u \in N \otimes_\Lambda A$  y, más específicamente,  $u \in \ker(\text{Id}_N \otimes \varphi)$ . Finalmente  $\ker(\text{Id}_N \otimes \varphi) = 0$  por hipótesis, por lo que  $\ker(\text{Id}_M \otimes \varphi) = 0$  como se quería probar.  $\square$

Finalmente, concluimos el capítulo con el siguiente breve paréntesis, vinculando el funtor Tor con la torsión.

**Definición 11.83:** Sea  $A$  un dominio íntegro y sea  $M$  un  $A$ -módulo. Para todo  $a \in A_{\neq 0}$  se le llama el **submódulo de  $a$ -torsión** de  $M$  a:

$$M[a] := \{u \in M : au = 0\},$$

y se tiene la sucesión exacta  $0 \rightarrow M[a] \rightarrow M \xrightarrow{\times a} M$ . Se le llama el **submódulo de torsión** de  $M$  a  $M_{\text{tors}} := \bigcup_{a \in A_{\neq 0}} M[a]$ .<sup>4</sup> Se dice que  $M$  es **libre de torsión** (resp. **pura torsión**) si  $M_{\text{tors}} = 0$  (resp.  $M_{\text{tors}} = M$ ).

Nótese que, bajo cierta perspectiva, tener  $a$ -torsión es dual a ser divisible por  $a$ . A veces, los módulos divisibles se les llaman de *cotorsión* para enfatizar esto.

**Proposición 11.84:** Sea  $A$  un dominio íntegro con  $K := \text{Frac } A$  y sea  $M$  un  $A$ -módulo. Entonces:

1. Todo módulo plano es libre de torsión.
2.  $K$  es plano y libre de torsión.
3. Se tiene la siguiente sucesión exacta:

$$0 \rightarrow M/M_{\text{tors}} \rightarrow M \otimes_A K \rightarrow M \otimes_A (K/A) \rightarrow 0 \quad (11.7)$$

<sup>4</sup>En general, la unión de submódulos no es un submódulo, a menos que la familia sea una  $\subseteq$ -cadena, lo cual no es el caso. Demuestre que aquí, la unión sí es un submódulo.

O equivalentemente,  $M_{\text{tors}} = \text{Tor}^A(M, K/A)$ .

4.  $M$  es de pura torsión syss  $M \otimes_A K = 0$ .

DEMOSTRACIÓN:

1. Probaremos la contrarrecíproca. Sea  $a \in A_{\neq 0}$  tal que  $M[a] \neq 0$ . Como  $A$  es íntegro, entonces la sucesión  $0 \rightarrow A \xrightarrow{\times a} A$  es exacta, así que tensorizamos por  $M$  y obtenemos la sucesión  $0 \rightarrow M \xrightarrow{\varphi} M$ , donde  $\varphi(u) = au$ , que no es exacta pues  $\ker \varphi = M[a] \neq 0$ .
2.  $K$  es trivialmente libre de torsión y que sea plano es un ejercicio para el lector.
3. Empleando la sucesión derivada:

$$\begin{array}{ccccccc} & & \text{Tor}^A(M, K) = 0 & \longrightarrow & \text{Tor}^A(M, K/A) & \searrow & \\ & & & & \omega & \longleftarrow & \\ \hookrightarrow & M = M \otimes_A A & \xrightarrow{\psi} & M \otimes_A K & \longrightarrow & M \otimes_A (K/A) & \longrightarrow 0 \end{array}$$

es fácil notar que  $\text{Tor}^A(M, K/A) = \omega = \ker \psi = M_{\text{tors}}$ . El que ambas afirmaciones sean equivalentes queda al lector.

4. Basta considerar la sucesión derivada anterior y notar que  $\omega$  es epimorfismo syss  $M \otimes_A K = 0$ .  $\square$

**Corolario 11.84.1:** Sea  $A$  un DIP. Entonces un  $A$ -módulo es plano syss es libre de torsión.

DEMOSTRACIÓN:  $\implies$ . Trivial de la proposición anterior.

$\impliedby$ . Sea  $M$  un  $A$ -módulo finitamente generado, entonces por el teorema estructural tenemos que  $M$  se escribe como una parte libre y una parte de torsión. Si  $M$  es libre de torsión, entonces es libre, luego también plano. Para el caso general, sea  $M$  libre de torsión, entonces vemos que todo submódulo finitamente generado es plano, luego  $M$  también siendo un límite directo...  $\square$

### §11.3.4 El teorema de coeficientes universales.

**Teorema 11.85 (fórmula de Künneth):** Sea  $\cdots \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \rightarrow 0$  un complejo de cadenas de  $\Lambda$ -módulos derechos planos, tales que cada  $dP_n := d_n[P_n] \leq P_{n-1}$  sea también plano. Entonces para cada  $\Lambda$ -módulo izquierdo  $M$  y cada  $q \in \mathbb{Z}$  se tiene la siguiente sucesión exacta:

$$0 \longrightarrow h_q(P_\bullet) \otimes_\Lambda M \longrightarrow h_q(P_\bullet \otimes_\Lambda M) \longrightarrow \text{Tor}_1^\Lambda(h_{q-1}(P_\bullet), M) \longrightarrow 0$$

DEMOSTRACIÓN: Aplicando la sucesión exacta en  $\text{Tor}^\Lambda$  de  $0 \rightarrow Z_n \rightarrow P_n \rightarrow dP_n \rightarrow 0$ , vemos que  $Z_n$  es también plano, por lo que la siguiente sucesión es exacta

$$0 \longrightarrow Z_n \otimes M \longrightarrow P_n \otimes M \longrightarrow dP_n \otimes M \longrightarrow 0$$

para todo  $n \in \mathbb{Z}$ . De modo que obtenemos una sucesión exacta de complejos  $0 \rightarrow Z_\bullet \otimes M \rightarrow P_\bullet \otimes M \rightarrow dP_\bullet \otimes M \rightarrow 0$ , donde  $Z_\bullet$  y  $dP_\bullet$  los consideramos con los diferenciales nulos. Por tanto, la sucesión exacta larga en homología dice que

$$\begin{array}{ccccccc} h_{q+1}(dP \otimes M) & \xrightarrow{\partial_{q+1}} & h_q(Z \otimes M) & \rightarrow & h_q(P \otimes M) & \rightarrow & h_q(dP \otimes M) \xrightarrow{\partial_q} h_{q-1}(Z \otimes M) \\ \wr \downarrow & & \wr \downarrow & & \wr \downarrow & & \wr \downarrow \\ dP_{q+1} \otimes M & & Z_q \otimes M & & dP_q \otimes M & & Z_{q-1} \otimes M \end{array}$$

es exacto. Se sigue de la definición de  $\partial_q$  que  $\partial_{q+1} = i_{q+1} \otimes \text{Id}_M$ , donde  $i_{q+1}: dP_{q+1} \hookrightarrow Z_q$  es la inclusión. Por otro lado, la sucesión  $0 \rightarrow dP_{q+1} \rightarrow Z_q \rightarrow h_q(P_\bullet) \rightarrow 0$  es una resolución plana de  $h_q(P)$ , por lo que  $\text{Tor}_\bullet(h_q(P), M)$  es la homología de

$$0 \longrightarrow dP_{q+1} \otimes M \xrightarrow{q} Z_q \otimes M \longrightarrow 0 \quad \square$$

**Teorema 11.86 (teorema de coeficientes universales en homología):** Sea  $A$  un dominio de Dedekind (e.g., un DIP) y sea  $P_\bullet$  un complejo de cadenas de  $A$ -módulos proyectivos. Entonces para cada  $A$ -módulo  $M$  y cada  $q \in \mathbb{Z}$  existe un isomorfismo

$$h_q(P_\bullet \otimes_A M) \cong h_q(P_\bullet) \otimes_A M \oplus \text{Tor}_1^A(h_{q-1}(P_\bullet), M).$$

DEMOSTRACIÓN: Recuértese que un dominio de Dedekind es un dominio íntegro hereditario, de modo que  $dP_n \hookrightarrow P_{n+1}$  es un módulo proyectivo y, por tanto, el epimorfismo  $P_n \rightarrow dP_n$  se escinde, lo que da un isomorfismo

$$P_n \cong Z_n \oplus dP_n. \quad (11.8)$$

Tras aplicar el funtor  $- \otimes_A M$ , vemos que  $Z_n \otimes M$  es un sumando directo de  $P_n \otimes M$  y, luego, también es un sumando directo de

$$\ker(d_n \otimes \text{Id}_M: P_n \otimes M \longrightarrow P_{n-1} \otimes M) \leq P_n \otimes M.$$

Cocientando  $Z_n \otimes M$  y  $\ker(d_n \otimes \text{Id}_M)$  por  $(d_{n+1} \otimes \text{Id}_M)$ , concluimos que  $h_n(P) \otimes M$  es un sumando directo de  $h_n(P \otimes M)$ ; finalmente, la fórmula de Künneth nos dice que el sumando restante es  $\text{Tor}_1^A(h_{q-1}(P_\bullet), M)$ .  $\square$



El isomorfismo (11.8) no es canónico, de modo que  $h_n(P \otimes M) \not\cong h_n(P) \otimes M$  en general.

Aplicando una prueba dual para los dos resultados anteriores obtenemos lo siguiente:

**Teorema 11.87 (teorema de coeficientes universales en cohomología):** Sea  $P_\bullet$  un complejo de cadenas de módulos proyectivos sobre un dominio  $A$ , tales que  $dP_n$  sea también proyectivo. Entonces para todo  $A$ -módulo  $M$  y cada  $q \in \mathbb{Z}$  existe una sucesión exacta que se escinde:

$$0 \longrightarrow \text{Ext}_A^1(h_{q-1}(P_\bullet), M) \longrightarrow h^q(\text{Hom}_A(P_\bullet, M)) \longrightarrow \text{Hom}_A(h_q(P_\bullet), M) \longrightarrow 0$$

## Notas históricas

Es claro que la historia entre las categorías abelianas y el álgebra homológica están entrelazadas, así que referencias se disputan.

Aquí las revoluciones son mucho mayores y dispersas. El primer resultado clave fue la inclusión de las *sucesiones exactas* que ya vimos en el capítulo de categorías abelianas, las cuales fueron inventadas por el topólogo **Witold Hurewicz** en [0] (1941); hasta cierto punto, la definición de *categoría exacta* de Buchsbaum es la de una categoría en la que hay herramientas para sucesiones exactas. Ésta noción fue clave para la axiomatización de la teoría de homología por EILENBERG y STEENROD [0] (1945).

**Reinhold Baer** estudió las extensiones de grupos (no necesariamente abelianos) en [0] (1934). Allí descubrió que se le podía dotar a las extensiones de una suma y que, cuando los extremos eran abelianos, le dotaba a  $E(A, B)$  de una estructura de grupo abeliano. Además, dió la definición de  $\text{Ext}$  como un conúcleo, que es la definición actual, mediante una presentación libre (en lugar de una presentación proyectiva, como hemos hecho nosotros); aunque las *presentaciones libres* no serían estudiadas sino hasta una década más tarde. Más tarde, BAER [0] (1940) definiría los *módulos inyectivos*,<sup>5</sup> de-

<sup>5</sup>Originalmente emplea el término «módulo completo».

mostraría el famoso *criterio de Baer* y caracterizaría a los anillos semisimples como aquellos en donde todo módulo es inyectivo.

En 1941, Mac Lane dió una serie de lecturas sobre extensiones de grupos en la Universidad de Michigan. Eilenberg no alcanzó a llegar a tiempo, por lo cual, Mac Lane ofreció impartirle su lectura en privado. Eilenberg notó que uno de los cálculos que hacía Mac Lane coincidía con los de los grupos de homología de Steenrod, por lo que ambos comenzaron a investigar en conjunto cuál era el funcionamiento del funtor  $\text{Ext}$ , lo que culminó el artículo [0] (1942) en donde, por vez primera, se estudiaban los funtores  $\text{Ext}$  y  $\text{Hom}$  con dicha terminología.



---

## Bibliografía

---

- 0. BAER, R. Erweiterung von Gruppen und ihren Isomorphismen. *Math. Z.* doi:10.1007/BF01170643 (1934).
- 0. BAER, R. Abelian groups that are direct summands of every containing abelian group. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1940-07306-9 (1940).
- 0. CUEVAS, J. *Álgebra* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf> (2022).
- 0. EILENBERG, S. y MAC LANE, S. Group Extensions and Homology. *Ann. Math.* doi:10.2307/1968966 (1942).
- 0. EILENBERG, S. y STEENROD, N. E. Axiomatic approach to Homology Theory. *Proc. Natl. Acad. Sci. USA.* doi:10.1073/pnas.31.4.117 (1945).
- 0. HILTON, P. J. y STAMMBACH, U. *A Course in Homological Algebra Graduate Texts in Mathematics* 4 (Springer-Verlag New York, 1971).
- 0. HUREWICZ, W. On duality theorems. *Bull. Amer. Math. Soc.* (1941).
- 0. ROTMAN, J. J. *An Introduction to Homological Algebra* 2.<sup>a</sup> ed. (Springer Science+Business Media, 1979).

## Álgebra abstracta

- 0. ALUFFI, P. *Algebra. Chapter 0* (American Mathematical Society, 1960).
- 0. CASTILLO, C. I. *Álgebra* <https://www.uv.es/ivorra/Libros/Al.pdf> (2020).

0. FINE, B. y ROSENBERGER, G. *The Fundamental Theorem of Algebra* (Springer-Verlag New York, 1997).
0. JACOBSON, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
0. LANG, S. *Algebra* (Springer-Verlag New York, 2002).
0. NAGATA, M. *Theory of Commutative Fields Translations in Mathematical Monographies* **125** (American Mathematical Society, 1967).
0. ROTMAN, J. J. *Advanced Modern Algebra* 3.<sup>a</sup> ed. 2 vols. *Graduate Studies in Mathematics* 165, 180 (American Mathematical Society, 2015).

## Formas cuadráticas y temas afines

0. CHEVALLEY, C. *The Construction and Study of Certain Important Algebras* (The Mathematical Society of Japan, 1955).
0. CHEVALLEY, C. *Fundamental Concepts of Algebra* (Academic Press, 1956).
0. GILLE, P. y SZAMUELY, T. *Central Simple Algebras and Galois Cohomology* (Cambridge University Press, 2006).
0. PRESTEL, A. *Lectures on Formally Real Fields Lecture Notes in Mathematics* **1093** (American Mathematical Society, 1975).
0. RAJWADE, A. R. *Squares* (Cambridge University Press, 1993).
0. SCHARLAU, W. *Quadratic and Hermitian forms* (Springer-Verlag Berlin, 1984).

## Álgebra lineal

0. CURTIS, M. L. *Abstract Linear Algebra* (Springer-Verlag New York Inc., 1990).
0. IBORT, A. y RODRÍGUEZ, M. A. *Notas de Álgebra Lineal* [http://mimosa.pntic.mec.es/jgomez53/matema/docums/ibort-algebra\\_lineal.pdf](http://mimosa.pntic.mec.es/jgomez53/matema/docums/ibort-algebra_lineal.pdf) (2014).
0. KATZNELSON, Y. y KATZNELSON, Y. R. *A (Terse) Introduction to Linear Algebra* (American Mathematical Society, 2008).
0. MILNOR, J. y HUSEMOLLER, D. *Symmetric Bilinear Forms* (Springer-Verlag Berlin Heidelberg, 1973).

## Álgebra conmutativa

- 0. ATIYAH, M. F. y McDONALD, I. G. *Introduction to Commutative Algebra* (Addison-Wesley, 1969).
- 0. EISENBUD, D. *Commutative Algebra with a View Toward Algebraic Geometry* (Springer Science+Business Media, 1994).
- EGA IV<sub>1</sub>. GROTHENDIECK, A. y DIEUDONNÉ, J. *Éléments de Géométrie Algébrique. IV.1: Étude locale des schémas et des morphismes de schémas* **20** (Publ. Math. IHÉS, 1964).
- 0. MATSUMURA, H. *Commutative Algebra* <https://github.com/AareyanManzoor/Matsumura-Commutative-Algebra> (W.A. Benjamin, Inc., 1969).
- 0. MATSUMURA, H. *Commutative Ring Theory* trad. por REID, M. *Cambridge Studies in Advanced Mathematics* **8** (Cambridge University Press, 1986).
- 0. NAGATA, M. *Local Rings* (Interscience, 1962).
- 0. SERRE, J.-P. *Local Algebra* (Springer-Verlag Berlin Heidelberg, 1965).
- 0. ZARISKI, O. y SAMUEL, P. *Commutative Algebra* 2 vols. (D. Van Nostrand, 1958).

## Grupos topológicos y cohomología de grupos

- 0. MORRIS, S. A. *Pontryagin duality and the structure of locally compact abelian groups* (Cambridge University Press, 1977).
- 0. WILSON, J. S. *Profinite groups* (Oxford University Press, 1999).

## Otros recursos

- 0. BANASCHEWSKI, B. Algebraic closure without choice. *Mathematical Logic Quarterly*. doi:10.1002/malq.19920380136 (1992).
- 0. BANASCHEWSKI, B. A New Proof that “Krull implies Zorn”. *Mathematical Logic Quarterly*. doi:10.1002/malq.19940400405 (1994).
- 0. BLASS, A. Existence of Basis implies the Axiom of Choice. *Contemporary Mathematics* **31**. <http://www.math.lsa.umich.edu/~ablass/bases-AC.pdf> (1984).
- 0. CONRAD, K. Simplicity of  $A_n$ . <https://kconrad.math.uconn.edu/blurbs/grouptheory/Ansimple.pdf> (2018).
- 0. CONRAD, K. The Sylow Theorems. <https://kconrad.math.uconn.edu/blurbs/grouptheory/sylowpf.pdf> (2018).

0. CONRAD, K. Zorn's Lemma and some applications. <https://kconrad.math.uconn.edu/blurbs/zorn1.pdf> (2018).
0. DERKSEN, H. The Fundamental Theorem of Algebra and Linear Algebra. *Amer. Math. Mon.* doi:10.2307/3647746 (2003).
0. ENGELKING, R. *General Topology* (Heldermann Verlag, 1989).
0. JANUSZ, G. J. *Algebraic Number Fields* 2.<sup>a</sup> ed. *Graduate Studies in Mathematics* **7** (American Mathematical Society, 1973).
0. NAGHIPOUR, A. R. A Simple Proof of Cohen's Theorem. *Amer. Math. Mon.* **112**, 825-826. doi:10.1080/00029890.2005.11920257 (2005).

## Documentos históricos

0. 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/CB09781139245807.004.
0. 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/CB09781139245807.008.
0. ABEL, N. H. Mémoire sur une classe particulière d'équations résolubles algébriquement. *J. Reine Angew. Math.* doi:10.1515/crll.1829.4.131 (1829).
0. ARTIN, E., NESBITT, C. J. y THRALL, R. M. *Rings with minimum condition* (University of Michigan Press, 1946).
0. BOURBAKI, N. *Éléments de Mathématique*. 2.1: *Algèbre. Chapitres 1-3* (Hermann, 1942).
0. CHEVALLEY, C. On the Theory of Local Rings. *Ann. of Math.* doi:10.2307/1969105 (1944).
0. COHEN, I. S. y SEIDENBERG, A. Prime ideals and integral dependence. *Bull. Amer. Math. Soc.* **52**, 252-261. doi:10.1090/S0002-9904-1946-08552-3 (1946).
0. DEDEKIND, R. Sur la théorie des nombres entiers algébriques. *Bull. Sci. Math. et Astronomiques*. doi:10.1007/978-3-322-98606-1\_3 (1876).
0. DIRICHLET, P. G. L. *Vorlesungen über Zahlentheorie* (ed. DEDEKIND, R.) (Braunschweig, 1863).

0. EAKIN JR., P. M. The converse to a well known theorem on Noetherian rings. *Math. Ann.* **177**, 278-282. doi:10.1007/BF01350720 (1968).
0. FORMANEK, E. Faithful Noetherian modules. *Proc. Amer. Math. Soc.* **41**, 381-383. doi:10.1090/S0002-9939-1973-0379477-X (1973).
0. 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.
0. 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.
0. 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).
0. GRELL, H. Beziehungen zwischen den Idealen verschiedener Ringe. *Math. Ann.* doi:10.1007/BF01447879 (1927).
0. HILBERT, D. Ueber die Theorie der algebraischen Formen. *Math. Ann.* doi:10.1007/BF01208503 (1890).
0. HILBERT, D. Ueber die vollen Invariantensysteme. *Math. Ann.* doi:10.1007/978-3-642-52012-9\_19 (1893).
0. KRONECKER, L. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. Reine Angew. Math.* doi:10.1515/crll.1882.92.1 (1882).
0. KRULL, W. Beiträge zur Arithmetik kommutativer Integritätsbereiche. III. Zum Dimensionsbegriff der Idealtheorie. *Math. Z.* **42**, 745-766. <https://eudml.org/doc/168748> (1937).
0. KRULL, W. Dimensionstheorie in Stellenringen. *J. Reine Angew. Math.* doi:10.1515/crll.1938.179.204 (1938).
0. KUMMER, E. E. *De Numeris Complexis, Qui Radicibus Unitatis Et Numeris Integris Realibus Constant* (Kessinger Publishing, 1844).
0. 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).
0. LASKER, E. Zur Theorie der moduln und Ideale. *Math. Ann.* doi:10.1007/BF01447495 (1905).
0. NAGATA, M. Some Remarks on Local Rings. *Nagoya Math. J.* **6**, 53-58. doi:10.1017/S0027763000016974 (1953).
0. NAGATA, M. A General Theory of Algebraic Geometry Over Dedekind Domains, I: The Notion of Models. *Amer. J. Math.* **78**, 78-116. doi:10.2307/2372486 (1956).

0. NAGATA, M. A type of subrings of a noetherian ring. *J. Math. Kyoto Univ.* **8**, 465-467. doi:10.1215/kjm/1250524062 (1968).
0. NOETHER, E. Idealtheorie in Ringbereichen. *Math. Ann.* doi:10.1007/978-3-642-39990-9\_19 (1921).
0. NOETHER, E. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik  $p$ . *Nachr. Ges. Wiss. Göttingen*, 28-35. <https://eudml.org/doc/59193> (1926).
0. NOETHER, E. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. *Math. Ann.* **96**, 26-61. doi:10.1007/BF01209152 (1927).
0. WHITNEY, H. Tensor products of abelian groups. *Duke Mathematical Journal*. doi:10.1215/S0012-7094-38-00442-9 (1938).
0. ZARISKI, O. Foundations of a general theory of birational correspondence. *Trans. Amer. Math. Soc.* **53**, 490-542. doi:10.1090/S0002-9947-1943-0008468-9 (1943).

## Historia

0. EDWARDS, H. M. The Genesis of Ideal Theory. *Archive for History of Exact Sciences*. doi:10.1007/bf00327914 (1980).
0. GROTHENDIECK, A. *Cosechas y Siembras* trad. por NAVARRO, J. A. <http://matematicas.unex.es/~navarro/res/> (1986).
0. KIERNAN, B. M. The development of Galois theory from Lagrange to Artin. *Archive for History of Exact Sciences*. doi:10.1007/BF00327219 (1971).
0. KLINE, M. *Mathematical Thought from Ancient to Modern Times* 3 vols. (Oxford University Press, 1972).

## Libros de autoría propia

0. CUEVAS, J. *Geometría algebraica* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/geo-alg/geometria-algebraica.pdf> (2022).
0. CUEVAS, J. *Teoría de categorías y álgebra homológica* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/cats/teoria-categorias.pdf> (2022).
0. CUEVAS, J. *Teoría de Conjuntos* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/conjuntos/conjuntos.pdf> (2022).

- 
0. CUEVAS, J. *Teoría de Números* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/teo-numeros/main.pdf> (2022).
  0. CUEVAS, J. *Topología y Análisis* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf> (2022).





# 12

---

## Cohomología y representaciones de grupos

---

### 12.1 Cohomología de grupos

**Definición 12.1:** Sea  $G$  un grupo. Recuérdesse que un  $G$ -conjunto  $A$  es un conjunto con una acción derecha  $\alpha: G \curvearrowright A$ . Un  $G$ -módulo *derecho*  $A$  es un grupo abeliano  $(A, +)$  con un homomorfismo de grupos  $\alpha: G \rightarrow \text{Aut}_{\text{Ab}}(A)$ , lo que equivale a tener una acción derecha denotada  $a \cdot g := \alpha(g)(a)$  tal que

$$\forall a, b \in A \quad a \cdot (gh) = (a \cdot g) \cdot h, \quad (a + b) \cdot g = a \cdot g + b \cdot g.$$

Se dice que un  $G$ -módulo  $A$  es o *posee acción trivial* si el homomorfismo  $\alpha: G \rightarrow \text{Aut}(A)$  es nulo.

Dado un  $G$ -módulo  $A$  fijo, podemos definir el  $G$ -submódulo *invariante* como el  $G$ -submódulo con acción trivial maximal:

$$A^G := \{a \in A : \forall g \in G \quad a \cdot g = a\}.$$

La noción de  $G$ -módulo izquierdo es análoga.

**Lema 12.2:** Sea  $G$  un grupo y  $\Lambda$  un anillo. Todo homomorfismo de grupos  $f: G \rightarrow \Lambda^\times$  se extiende a un único homomorfismo de anillos

$$f^*: \mathbb{Z}[G] \rightarrow \Lambda.$$

En consecuencia, si  $A$  es un  $G$ -módulo derecho, el homomorfismo de la acción  $\alpha: G \rightarrow \text{Aut}(A) = \text{End}_{\text{Ab}}(A)^\times$  se extiende de manera única a un homomorfismo de anillos  $\mathbb{Z}[G] \rightarrow \text{End}(A)$ , de modo que  $A$  es un  $\mathbb{Z}[G]$ -módulo derecho usual (¡explícite el producto escalar!). Mediante esta identificación podemos dar la definición de un **homomorfismo de  $G$ -módulos**.

**Definición 12.3:** Sea  $G$  un grupo. El **homomorfismo de augmentación** es aquel dado por

$$\text{aug} = \varepsilon: \mathbb{Z}[G] \longrightarrow \mathbb{Z}, \quad \sum_{g \in G} a_g g \longmapsto \sum_{g \in G} a_g.$$

Su núcleo se denomina el **ideal de augmentación** y se denota  $\mathfrak{I}[G] := \ker(\varepsilon)$ , o simplemente  $\mathfrak{I}$  de no haber ambigüedad.

Dado un  $G$ -módulo  $A$  podemos definir su  **$G$ -módulo coinvariante** como  $A_G := A/\mathfrak{I}A$ .

**Ejercicio 12.4:** Demuestre que para todo grupo  $G$  y todo  $G$ -módulo  $A$ , el  $G$ -módulo coinvariante  $A_G$  es el  $G$ -módulo cociente de  $A$  con acción trivial maximal.

Como la categoría  $\text{Mod}_G$  es entonces isomorfa a  $\text{Mod}_{\mathbb{Z}[G]}$  se verifica lo siguiente:

**Lema 12.5.A:** La categoría de  $G$ -módulos (derechos o izquierdos) posee suficientes inyectivos y proyectivos.

**Lema 12.5.B:** Sea  $G$  un grupo. Para todo  $G$ -módulo  $A$  se tienen los siguientes isomorfismos naturales

$$A_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A, \quad A^G \cong \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

En consecuencia,  $A \mapsto A_G$  es un funtor exacto por la derecha y  $A \mapsto A^G$  es exacto por la izquierda.

**Definición 12.5:** Sea  $G$  un grupo finito. Para todo  $G$ -módulo  $A$  y todo  $q \geq 0$  entero, definimos su  **$q$ -ésimo grupo de homología y de cohomología** resp. como:

$$H_q(G, A) := \mathbb{L}^q A_G = \text{Tor}_q^{\mathbb{Z}[G]}(\mathbb{Z}, A), \quad H^q(G, A) := \mathbb{R}^q A^G = \text{Ext}_{\mathbb{Z}[G]}^q(\mathbb{Z}, A).$$

Aquí, los símbolos  $L^q$  y  $R^q$  denotan el  $q$ -ésimo funtor derivado izquierdo y derecho resp. De este modo, aplicando los resultados del capítulo anterior, obtenemos sucesiones exactas largas en homología y cohomología de  $G$ -módulos.

Otra cuestión importante es que, por álgebra homológica categorial, la sucesión de los  $H^n$  y  $H_n$ 's está únicamente determinada por su valor en  $n = 0$ , donde:

**Corolario 12.5.1:** Sea  $G$  un grupo y  ${}_G A, B_G$  un par de  $G$ -módulos. Entonces:

1. Si  $A$  es inyectivo, entonces  $H^p(G, A) = 0$  para todo  $p > 0$ .
2. Si  $B$  es plano (e.g., proyectivo), entonces  $H_p(G, B) = 0$  para todo  $p > 0$ .

**Proposición 12.6:** Sea  $G$  un grupo y sean  $A, B$  un par de  $G$ -módulos izquierdos (resp. derechos), entonces para todo  $q \in \mathbb{Z}$  tenemos que

$$\begin{aligned} H^q(G, A \oplus B) &\cong H^q(G, A) \oplus H^q(G, B), \\ H_q(G, A \oplus B) &\cong H_q(G, A) \oplus H_q(G, B). \end{aligned}$$

**Proposición 12.7:** Para todo grupo  $G$ , se cumple que

$$H_1(G, \mathbb{Z}) \cong \mathfrak{I}/\mathfrak{I}^2 \cong G^{\text{ab}}.$$

DEMOSTRACIÓN: Para el primer isomorfismo considere la sucesión exacta  $0 \rightarrow \mathfrak{I} \rightarrow \mathbb{Z}[G] \xrightarrow{\text{aug}} \mathbb{Z} \rightarrow 0$  de  $G$ -módulos, y luego aplique la sucesión exacta larga en homología

$$0 = H_1(G, \mathbb{Z}[G]) \rightarrow H_1(G, \mathbb{Z}) \xrightarrow{\alpha} \mathfrak{I}_G \rightarrow (\mathbb{Z}[G])_G \xrightarrow{\beta} \mathbb{Z} \rightarrow 0.$$

Ahora bien, como  $(\mathbb{Z}[G])_G = \mathbb{Z}$  por definición de «elementos  $G$ -invariantes», se verifica que  $\beta$  es un isomorfismo, de lo que se sigue que  $\alpha$  debe ser un epimorfismo y, por tanto, un isomorfismo.

Para el segundo isomorfismo  $\mathfrak{I}/\mathfrak{I}^2 \cong G^{\text{ab}}$ , considere la función

$$\theta: G \rightarrow \mathfrak{I}/\mathfrak{I}^2, \quad g \mapsto g - 1 \pmod{\mathfrak{I}^2}$$

este es un homomorfismo pues, para todo  $g, h \in G$ , se satisface que

$$\theta(gh) = gh - 1 = g - 1 + h - 1 + (g - 1)(h - 1)$$

$$\equiv g - 1 + h - 1 \pmod{\mathfrak{I}^2}.$$

Como  $\mathfrak{I}/\mathfrak{I}^2$  es un grupo abeliano, se sigue que  $\theta$  anula al conmutador  $[G, G]$ . Luego podemos definir el homomorfismo de  $\mathbb{Z}$ -módulos inducido por

$$\sigma: \mathfrak{I} \longrightarrow G^{\text{ab}}, \quad g - 1 \longmapsto g \pmod{[G, G]}$$

y como  $(g - 1)(h - 1) = gh - 1 - (g - 1) - (h - 1)$ , vemos que  $\sigma((g - 1)(h - 1)) = ghg^{-1}h^{-1} \equiv 1 \pmod{[G, G]}$ , de lo que se sigue que  $\sigma$  induce un homomorfismo de grupos abelianos  $\mathfrak{I}/\mathfrak{I}^2 \rightarrow G^{\text{ab}}$ , y que (la proyección de)  $\theta$  es su inversa.  $\square$

**Corolario 12.7.1:** Sea  $G$  un grupo y  $A$  un  $G$ -módulo de acción trivial. Entonces:

$$H_p(G, A) \cong \begin{cases} A, & p = 0, \\ G^{\text{ab}} \otimes_{\mathbb{Z}} A, & p = 1, \\ H_p(G, \mathbb{Z}) \otimes_{\mathbb{Z}} A \oplus \text{Tor}_1^{\mathbb{Z}}(H_{p-1}(G, \mathbb{Z}), A), & p \geq 2. \end{cases}$$

DEMOSTRACIÓN: Sea  $P_{\bullet} \rightarrow \mathbb{Z}$  una resolución proyectiva de  $\mathbb{Z}[G]$ -módulos derechos. Empleando que  $P_{\bullet} \otimes_{\mathbb{Z}[G]} A = (P_{\bullet} \otimes_{\mathbb{Z}[G]} \mathbb{Z}) \otimes_{\mathbb{Z}} A$ , podemos emplear el teorema de coeficientes universales en homología sobre  $\mathbb{Z}$ -módulos.  $\square$

**Definición 12.8:** Si  $G$  es un grupo finito, entonces dentro de  $\mathbb{Z}[G]$  existe el *elemento norma*:

$$N := \sum_{g \in G} g \in \mathbb{Z}[G].$$

Este induce, para cada  $G$ -módulo  $A$ , un endomorfismo de  $G$ -módulos  $\times N: A \rightarrow A$ ; será útil considerar su núcleo, llamado la  *$N$ -torsión*

$$A[N] := \ker(A \xrightarrow{\times N} A) = \left\{ a \in A : \sum_{g \in G} a \cdot g = 0 \right\}.$$

**Ejemplo.** Cuando  $G = C_m = \langle g \rangle$  es el grupo cíclico de orden  $m$ , se verifican fácilmente dos cosas:  $\mathfrak{I} = (g - 1)\mathbb{Z}$  y  $N = \sum_{j=0}^{m-1} g^j$ . Así, nótese que  $a \in A$  es  $G$ -invariante syss  $(g - 1)a = 0$ , en cuyo caso,  $Na = ma$ .

**Teorema 12.9:** Sea  $G = C_m = \langle g \rangle$  un grupo cíclico finito, y sea  $A$  un  $G$ -módulo, entonces

$$H_q(C_m, A) = \begin{cases} A/(g-1)A, & q = 0, \\ A^G/NA, & q \geq 1, 2 \nmid q, \\ A[N]/(g-1)A, & q \geq 1, 2 \mid q, \end{cases}$$

$$H^q(C_m, A) = \begin{cases} A^G, & q = 0, \\ A[N]/(g-1)A, & q \geq 1, 2 \nmid q, \\ A^G/NA, & q \geq 2, 2 \mid q. \end{cases}$$

DEMOSTRACIÓN: Para ello comenzaremos por notar que dado  $\beta \in \mathbb{Z}[G]$  entonces  $\beta N = \text{aug}(\beta)N$  (¡pruébelo!), de modo que  $\ker(\mathbb{Z}[G] \xrightarrow{\times N} \mathbb{Z}[G]) = \mathfrak{I}$ . Desde aquí es un mero ejercicio probar que la sucesión de  $G$ -módulos

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\text{aug}} \mathbb{Z}[G] \xleftarrow{\times(\sigma-1)} \mathbb{Z}[G] \xleftarrow{\times N} \mathbb{Z}[G] \xleftarrow{\times(\sigma-1)} \mathbb{Z}[G] \longleftarrow \cdots,$$

es exacta, por lo que es una resolución libre de  $\mathbb{Z}$ , que se descompone en las siguientes sucesiones exactas cortas

$$0 \longleftarrow \mathbb{Z} \cdot N \xleftarrow{\times N} \mathbb{Z}[G] \longleftarrow \mathfrak{I} \longleftarrow 0, \quad 0 \longleftarrow \mathfrak{I} \xleftarrow{\times(g-1)} \mathbb{Z}[C_m] \longleftarrow \mathbb{Z} \cdot N \longleftarrow 0.$$

Ahora el enunciado sale de aplicarle los funtores  $-\otimes_{\mathbb{Z}[G]} A$  y  $\text{Hom}_G(A, -)$ .  $\square$

**§12.1.1 Interpretación del  $H^1$ .** Para la mayoría de cálculos la sucesión exacta es suficiente, aunque en ocasiones los grupos de dimensiones bajas suelen tener «interpretaciones útiles».

**Definición 12.10:** Sea  $G$  un grupo y  $A$  un  $G$ -módulo izquierdo. Un **homomorfismo cruzado** (o *derivación*) es una función  $D: G \rightarrow A$  tal que para todo  $g, h \in G$  se cumple

$$D(g \cdot h) = g \cdot D(h) + D(g).$$

El conjunto de homomorfismos cruzados se denota  $\text{Der}(G, A)$ . Los homomorfismos cruzados con la suma coordenada a coordenada forman un grupo abeliano.

**Observación 12.10.1:** El lector interesado podría considerar a los homomorfismos cruzados como derivaciones en un sentido usual, donde  $A$  se

identifica como un  $G$ - $G$ -bimódulo, con estructura de  $G$ -módulo derecho de acción trivial.

**Ejemplo 12.11:** Sea  $G$  un grupo y  $A$  un  $G$ -módulo izquierdo. Para un elemento  $a \in A$  arbitrario, la función  $D_a(g) := g \cdot a - a$  es un homomorfismo cruzado pues

$$D_a(gh) = gh \cdot a - a = g \cdot (ha - a) + g \cdot a - a = g \cdot D_a(h) - D_a(g).$$

Los homomorfismos cruzados de la forma  $D_a$  se dicen *principales*, y el conjunto de ellos se denota  $\text{PDer}(G, A)$ . Como  $D_a + D_b = D_{a+b}$ , se comprueba que  $\text{PDer}(G, A)$  es un subgrupo de  $\text{Der}(G, A)$ .  $\square$

**§12.1.2 (Co)homología entre subgrupos.** En primer lugar, obsérvese lo siguiente:

**Lema 12.12:** La aplicación  $G \mapsto \mathbb{Z}[G]$  determina un funtor  $\mathbb{Z}[-]: \text{Grp} \rightarrow \text{Ring}$ , donde un homomorfismo de grupos  $\varphi: G \rightarrow H$  induce el homomorfismo de anillos

$$\mathbb{Z}\varphi: \mathbb{Z}[G] \longrightarrow \mathbb{Z}[H], \quad \sum_{g \in G} a_g g \longmapsto \sum_{h \in H} \left( \sum_{\varphi(g)=h} a_g \right) h.$$

Esto permite que:

**Corolario 12.12.1:** Todo homomorfismo de grupos  $\varphi: G \rightarrow H$  induce un funtor semiolvidadizo  $U_\varphi: \text{Mod}_H \rightarrow \text{Mod}_G$ .

**Lema 12.13:** Sea  $G$  un grupo y  $H \leq G$ . Entonces:

1.  $\mathfrak{I}[G]$  es un grupo abeliano libre con base  $W := \{g - 1 : g \in G_{\neq 1}\}$ .
2. Si  $S \subseteq G$  es un sistema generador (como grupo), entonces  $S - 1 := \{s - 1 : s \in S\}$  es un sistema generador (como  $G$ -módulo) de  $\mathfrak{I}[G]$ .
3.  $\mathbb{Z}[G]$  es un  $\mathbb{Z}[H]$ -módulo derecho (o izquierdo) libre.

DEMOSTRACIÓN:

1. Claramente  $W$  es un conjunto  $\mathbb{Z}$ -linealmente independiente y genera a todo  $\mathfrak{I}[G]$  pues dado  $\sum_{g \in G} a_g g \in \mathfrak{I}[G]$  tenemos que

$$\sum_{g \in G} a_g g = \sum_{g \in G} a_g g - \sum_{g \in G} a_g = \sum_{g \in G} a_g (g - 1).$$

2. Sean  $x, y \in S$ , entonces nótese que

$$xy - 1 = x(y - 1) + (x - 1), \quad x^{-1} - 1 = -x^{-1}(x - 1) \in (S - 1) \cdot \mathbb{Z}.$$

Así pues, para todo elemento  $g$  generado por  $S$  se cumple que  $g - 1$  está generado por  $S - 1$  y concluimos por el inciso anterior.

3. Basta tomar un conjunto de representantes de clases laterales  $\{g_i\}_{i \in I}$ , de modo que  $\mathbb{Z}[H]g_i \cong \mathbb{Z}[H]$  son  $\mathbb{Z}[H]$ -submódulos de  $\mathbb{Z}[G]$  tales que  $\mathbb{Z}[G] = \bigoplus_{i \in I} \mathbb{Z}[H]g_i$ .  $\square$

**Corolario 12.13.1:** Sea  $G$  un grupo. Todo  $G$ -módulo proyectivo (resp. inyectivo) es un  $H$ -módulo proyectivo (resp. inyectivo) para todo subgrupo  $H \leq G$ .

**Definición 12.14:** Dado un  $H$ -módulo izquierdo  $A$ , definimos el  $G$ -**módulo inducido** como  $\text{Ind}_H^G(A) := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$  y también definimos el  $G$ -**módulo coinducido** como  $\text{Coind}_H^G(A) := \text{Hom}_H(\mathbb{Z}[G], A)$ . Ambos son  $G$ -módulos izquierdos.

**Observación 12.14.1:** Para dar una definición para  $H$ -módulos derechos, basta redefinir el  $G$ -módulo inducido como  $A \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$ . Por abuso de notación, a éste también lo denotaremos como  $\text{Ind}_H^G(A)$  de ser necesario.

Las relaciones de adjunción entre « $\otimes$ » y « $\text{Hom}$ » ahora se traducen en lo siguiente:

**Corolario 12.14.2:** Sea  $G$  un grupo y  $H \leq G$ . Considere el funtor semiolvidadizo  $U: \text{Mod}_G \rightarrow \text{Mod}_H$  del corolario 12.12.1, entonces los funtores  $\text{Ind}_H^G$  y  $\text{Coind}_H^G: \text{Mod}_H \rightarrow \text{Mod}_G$  satisfacen que

$$\text{Ind}_H^G \dashv U \dashv \text{Coind}_H^G.$$

**Teorema 12.15 (lema de Shapiro):** Sea  $G$  un grupo,  $H \leq G$  y  $A$  un  $H$ -módulo (izquierdo). Entonces para todo  $q \in \mathbb{Z}$  tenemos los isomorfismos

naturales

$$H_q(G, \text{Ind}_H^G(A)) \cong H_q(H, A), \quad H^q(G, \text{Coind}_H^G(A)) \cong H^q(H, A).$$

DEMOSTRACIÓN: Sea  $P_\bullet \rightarrow \mathbb{Z}$  una resolución por  $G$ -módulos derechos proyectivos. La homología del complejo de cadenas

$$P_\bullet \otimes_{\mathbb{Z}[G]} \text{Ind}_H^G(A) = P_\bullet \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A) \cong P_\bullet \otimes_{\mathbb{Z}[H]} A$$

es, gracias al corolario 12.13.1:

$$H_q(G, \text{Ind}_H^G(A)) = \text{Tor}_q^{\mathbb{Z}[G]}(\mathbb{Z}, \text{Ind}_H^G(A)) \cong \text{Tor}_q^{\mathbb{Z}[H]}(\mathbb{Z}, A) = H_q(H, A).$$

Por otro lado, dada una resolución  $P_\bullet \rightarrow \mathbb{Z}$  de  $G$ -módulos izquierdos proyectivos, la cohomología del cocomplejo de cadenas (donde el isomorfismo viene dado por adjunción)

$$\text{Hom}_G(P_\bullet, \text{Coind}_H^G(A)) = \text{Hom}_G(P_\bullet, \text{Hom}_H(\mathbb{Z}[G], A)) \cong \text{Hom}_H(P_\bullet, A)$$

es

$$H^q(G, \text{Coind}_H^G(A)) = \text{Ext}_{\mathbb{Z}[G]}^q(\mathbb{Z}, \text{Coind}_H^G(A)) \cong \text{Ext}_{\mathbb{Z}[H]}^q(\mathbb{Z}, A) = H^q(H, A). \quad \square$$

Con  $H = 1$  el subgrupo trivial, obtenemos lo siguiente:

**Corolario 12.15.1:** Sea  $G$  un grupo y  $A$  un grupo abeliano. Entonces para todo  $q \in \mathbb{Z}$  tenemos los isomorfismos naturales

$$H_q(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} A) \cong H^q(G, \text{Hom}_{\text{Ab}}(\mathbb{Z}[G], A)) \cong \begin{cases} A, & q = 0, \\ 0, & q \neq 0. \end{cases}$$

**Definición 12.16:** Sea  $G$  un grupo. Diremos que  $A$  es un  $G$ -módulo *relativamente inyectivo* (resp. *relativamente proyectivo*) si es un sumando directo de  $\text{Coind}_1^G(A) = \text{Hom}_{\text{Ab}}(\mathbb{Z}[G], A)$  (resp.  $\text{Ind}_1^G(A) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ ).

**Corolario 12.16.1:** Sea  $G$  un grupo y  $A$  un  $G$ -módulo. Si  $A$  es relativamente inyectivo (resp. relativamente proyectivo), entonces  $H^p(G, A) = 0$  (resp.  $H_p(G, A) = 0$ ) para todo  $p > 0$ .

DEMOSTRACIÓN: Si  $A \oplus B \cong \text{Coind}_1^G(A)$ , entonces por la proposición 12.6 comprobamos que  $H^q(G, A) \oplus H^q(G, B) = H^q(G, \text{Coind}_1^G(A))$  lo cual se anula por el lema de Shapiro. Para módulos relativamente proyectivos la prueba es *mutatis mutandis* la misma.  $\square$



**Proposición 12.17:** Sea  $G$  un grupo y sea  $H \leq G$  un subgrupo de índice finito. Entonces, para todo  $H$ -módulo  $A$  se cumple que  $\text{Ind}_H^G(A) \cong \text{Coind}_H^G(A)$ .

DEMOSTRACIÓN: Basta notar que, tras elegir un conjunto de representantes  $X$  de las clases laterales  $gH$ , tenemos el isomorfismo  $\mathbb{Z}[G] = \bigoplus_{g \in X} g\mathbb{Z}[H] \cong \mathbb{Z}[H]^{[G:H]}$ , del cual se sigue que

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A \cong A^{[G:H]} \cong \text{Hom}_H(\mathbb{Z}[H]^{[G:H]}, A). \quad \square$$

El isomorfismo depende de la elección del conjunto de representantes  $X$ , de modo que no es canónico a medida que cambiamos el  $H$  (y/o el  $G$ ), pero sí es funtorial si fijamos la elección de  $X$  y cambiamos el  $A$ .

Aplicando la proposición con  $H = 1$  el subgrupo trivial se obtiene:

**Corolario 12.17.1:** Si  $G$  es un grupo finito, entonces para todo grupo abeliano  $A$  y todo entero  $q \neq 0$  se cumple que

$$H^q(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} A) = H_q(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} A) = 0.$$

En consecuencia, ser relativamente inyectivo es lo mismo que relativamente proyectivo como  $G$ -módulos.

**Definición 12.18:** Sea  $\rho: H \rightarrow G$  un homomorfismo de grupos. Denotaremos por  $\rho^\sharp: \text{Mod}_G \rightarrow \text{Mod}_H$  al funtor semiolvidadizo (cfr. corolario 12.12.1). Dado un  $G$ -módulo  $A$  tenemos un monomorfismo (en  $\text{Ab}$ ) canónico  $A^G \hookrightarrow (\rho^\sharp A)^H$  entre módulos invariantes y un epimorfismo canónico  $(\rho^\sharp A)_H \rightarrow A_G$  entre módulos coinvariantes; ambos inducen homomorfismos entre grupos de cohomología y homología resp., llamados *restricción* y *corestricción* resp.:

$$\text{res}_H^G: H^\bullet(G, A) \longrightarrow H^\bullet(H, \rho^\sharp A), \quad \text{cor}_H^G: H_\bullet(H, \rho^\sharp A) \longrightarrow H_\bullet(G, A).$$

**§12.1.3 Cohomología modificada de Tate.** Principalmente para la teoría de cuerpos de clase (tópico en teoría algebraica de números), Tate propuso una modificación a la cohomología de grupos que procedemos a detallar.

Si  $G$  es un grupo *finito* y  $A$  es un  $G$ -módulo, entonces tenemos el endomorfismo norma  $N_A := \times N: A \rightarrow A$ . Nótese que  $\text{Im}(N_A) \subseteq A^G = H^0(G, A) \subseteq A$  y que  $\ker(N_A) \supseteq \mathfrak{I}A$ , de modo que se induce el siguiente homomorfismo de  $G$ -módulos:

$$N_A^*: A/\mathfrak{I}A = H_0(G, A) \longrightarrow H^0(G, A).$$

**Definición 12.19:** Sea  $G$  un grupo finito y  $A$  un  $G$ -módulo. Para  $q \in \mathbb{Z}$  definimos el  $q$ -ésimo grupo de cohomología de Tate como

$$\widehat{H}^q(G, A) := \begin{cases} H^q(G, A), & q \geq 1, \\ \text{coker}(N_A^*) = A^G/NA, & q = 0, \\ \ker(N_A^*) = A[N]/\mathfrak{I}A, & q = -1, \\ H_{-q-1}(G, A), & q \leq -2. \end{cases}$$

Por ejemplo, el cálculo del teorema 12.9 para grupos cíclicos ahora se traduce en que:

**Proposición 12.20:** Sea  $G$  un grupo cíclico finito. Para todo  $G$ -módulo  $A$  y todo  $q \in \mathbb{Z}$  se cumple que  $\widehat{H}^{q+2}(G, A) = \widehat{H}^q(G, A)$ .

De modo que, cuando el grupo es cíclico, los únicos grupos de cohomología de Tate importantes suceden en  $q \in \{-1, 0\}$ .

**Teorema 12.21:** Sea  $G$  un grupo finito y sea  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  una sucesión exacta de  $G$ -módulos. Entonces induce una sucesión exacta larga en cohomología de Tate:

$$\begin{array}{ccccccc} & & & & \cdots & \longrightarrow & \widehat{H}^{q-1}(G, C) \\ & & & \swarrow \partial & & \searrow & \\ & & & & & & \\ \widehat{H}^q(G, A) & \longrightarrow & \widehat{H}^q(G, B) & \longrightarrow & \widehat{H}^q(G, C) & & \\ & & \swarrow \partial & & \searrow & & \\ \widehat{H}^{q+1}(G, A) & \longrightarrow & \cdots & & & & \end{array}$$

Además, si  $A$  es relativamente inyectivo, entonces  $\widehat{H}^q(G, A) = 0$  para todo  $q \in \mathbb{Z}$ .

DEMOSTRACIÓN: La exactitud en  $q \geq 1$  y  $q \leq -2$  se deduce de la definición de grupos de cohomología y homología resp., por lo que nos enfocaremos en  $q \in \{-1, 0\}$ , los cuales se deducen del lema de la serpiente.

Cuando el grupo base  $G$  es finito,  $A$  es relativamente proyectivo también, por lo que  $\widehat{H}^q(G, A) = 0$  para todo  $q \notin \{0, 1\}$ . Como se verifica fácilmente que

$$\widehat{H}^q(G, A \oplus B) \cong \widehat{H}^q(G, A) \oplus \widehat{H}^q(G, B),$$

entonces vemos que podemos suponer que  $A = \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$ , identificamos  $M \subseteq A$  y vemos a  $A$  como suma directa de todos los subconjuntos  $gM$  para  $g \in G$ . Así que todo  $a \in A$  puede escribirse de la forma  $a = \sum_{g \in G} gm_g$ , donde cada  $m_g \in M$ , y  $a \in A^G$  si y sólo si todos los  $m_g$ 's coinciden, es decir, si  $a = N \cdot m$  para  $m \in M$ . De ello se sigue de que  $\widehat{H}^0(G, A) = 0$  y el caso  $q = -1$  es análogo.  $\square$

**Corolario 12.21.1:** Sea  $G$  un grupo finito y sea  $0 \rightarrow A \rightarrow I \rightarrow B \rightarrow 0$  una sucesión exacta de  $G$ -módulos, donde  $I$  es relativamente inyectivo. Entonces para todo  $q \in \mathbb{Z}$  tenemos isomorfismos canónicos  $\widehat{H}^q(G, B) = \widehat{H}^{q+1}(G, A)$ .

**Corolario 12.21.2 («hexágono exacto»):** Sea  $G$  un grupo finito cíclico y sea  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  una sucesión exacta de  $G$ -módulos. Entonces induce el siguiente diagrama conmutativo exacto:

$$\begin{array}{ccccc}
 & & \widehat{H}^0(G, A) & \longrightarrow & \widehat{H}^0(G, B) \\
 & \nearrow & & & \searrow \\
 \widehat{H}^{-1}(G, C) & & & & \widehat{H}^0(G, C) \\
 & \nwarrow & & & \swarrow \\
 & & \widehat{H}^{-1}(G, B) & \longleftarrow & \widehat{H}^{-1}(G, A)
 \end{array}$$

DEMOSTRACIÓN: Esto se sigue de la sucesión exacta larga en cohomología de Tate sumado a la proposición 12.20, aunque queda el detalle restante de que las flechas sean las mismas en distintos grados. Para ello, hay que recordar que las flechas vienen de la (co)homología de grupos usual, que se calcula como las flechas inducidas por las resoluciones proyectivas de objetos (vuelva a ver la demostración del teo. 12.9), las cuales sí que son 2-periódicas, inclusive en flechas.  $\square$

**Definición 12.22:** Sea  $G$  un grupo finito y  $M$  un  $G$ -módulo tal que

$$|\widehat{H}^{-1}(G, M)| < \infty, \quad |\widehat{H}^0(G, M)| < \infty. \quad (12.1)$$

Se define su *cociente de Herbrand* como

$$h(G, M) := \frac{|\widehat{H}^0(G, M)|}{|\widehat{H}^{-1}(G, M)|}.$$

Por ejemplo, (12.1) se satisface cuando  $M$  es finito.

**Proposición 12.23 (Herbrand):** Sea  $G$  un grupo cíclico y sea  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  una sucesión exacta corta de  $G$ -módulos tales que (12.1) se satisface para dos de tres  $G$ -módulos. Entonces también se satisface para el tercero y

$$h(G, B) = h(G, A) h(G, C).$$

Además, para todo  $G$ -módulo finito  $A$ , se cumple que  $h(G, A) = 1$ .

DEMOSTRACIÓN: Denotaremos por  $h^p(X) := |\widehat{H}^p(G, X)|$ . Del hexágono exacto deducimos la siguiente sucesión exacta:

$$\begin{array}{ccccccc} 0 & \rightarrow & I & \rightarrow & \widehat{H}^0(G, A) & \rightarrow & \widehat{H}^0(G, B) \rightarrow \widehat{H}^0(G, C) \\ & & & & & \searrow & \\ & & & & \widehat{H}^1(G, A) & \rightarrow & \widehat{H}^1(G, B) \rightarrow \widehat{H}^1(G, C) \rightarrow I \rightarrow 0 \end{array}$$

donde

$$I := (\widehat{H}^1(G, B) \rightarrow \widehat{H}^1(G, C)) = \ker(\widehat{H}^0(G, A) \rightarrow \widehat{H}^0(G, B)).$$

Denotando por  $s := |I|$ , entonces la sucesión exacta implica que tenemos la siguiente identidad en cardinalidades:

$$sh^0(B)h^1(A)h^1(C) = h^0(A)h^0(C)h^1(B)s,$$

que despejando nos da la identidad en cocientes de Herbrand.

Sea  $A$  un  $G$ -módulo finito, nos queda probar que  $h(G, A) = 1$ . Sea  $g$  un generador de  $G$ , entonces tenemos la siguiente sucesión exacta

$$0 \longrightarrow H^0(G, A) \longrightarrow A \xrightarrow{\times(g-1)} A \longrightarrow H_0(G, A) \longrightarrow 0,$$

de lo que se sigue que  $H^0(G, A)$  y  $H_0(G, A)$  comparten cardinalidad (finita); análogamente de la sucesión exacta

$$0 \longrightarrow \widehat{H}^{-1}(G, A) \longrightarrow H_0(G, A) \xrightarrow{N_A^*} H^0(G, A) \longrightarrow \widehat{H}^0(G, A) \longrightarrow 0,$$

se sigue que  $h^{-1}(A) = h^0(A)$ , como se quería probar.  $\square$

---

## *Bibliografía*

---

- 0. HARARI, D. *Galois Cohomology and Class Field Theory* (Springer-Verlag, 2020).
- 0. WEIBEL, C. A. *An introduction to homological algebra Cambridge Studies in Advanced Mathematics* **38** (Cambridge University Press, 1994).



# 13

---

## Grupos topológicos y profinitos

---

El material de este capítulo está principalmente extraído del libro MORRIS [0].

### 13.1 Grupos topológicos

**Definición 13.1:** Un *grupo topológico* es un espacio topológico  $G$  con una operación de grupo  $*$ , tal que las aplicaciones  $*$ :  $G \times G \rightarrow G$  y  $()^{-1}$ :  $G \rightarrow G$  son continuas.

Sea  $g \in G$ . Denotamos  $\tau_g^l(h) := gh$  y  $\tau_g^r(h) := hg$ ; estas aplicaciones se denominan *traslaciones*.

Es fácil comprobar que las aplicaciones  $()^{-1}$ ,  $\tau_g^l$  y  $\tau_g^r$  son todos homeomorfismos, de modo que, gracias a ellas, se observa una clara «rigidez» en la estructura topológica que podemos explotar. Las propiedades locales se pueden verificar sobre un único punto, tradicionalmente el neutro  $e \in G$ , así que para ser localmente compacto, basta que  $e$  posea un entorno compacto, por ejemplo.

**Ejemplo.** 1. Sea  $G$  un grupo arbitrario. Si le dotamos la topología discreta, entonces  $G$  se convierte en un grupo topológico, llamado *discreto*. Lo mismo si lo dotamos de la topología indiscreta, pero éste último caso no será de tanta utilidad.

2.  $(\mathbb{R}^n, +)$  es un grupo topológico, donde  $\mathbb{R}^n$  posee la topología producto de la topología usual sobre  $\mathbb{R}$ . También con las topologías usuales,  $(\mathbb{Z}^n, +)$  y  $(\mathbb{Q}^n, +)$  son grupos topológicos.
3.  $(\mathbb{R}^\times, \cdot)$  es un grupo topológico, también con la topología subespacio de la usual. Similarmente,  $\mathbb{Q}^\times$  y  $\mathbb{C}^\times$  lo son.
4. Un poco más generalmente, el grupo general lineal  $\mathrm{GL}_n(\mathbb{R})$  y especial lineal  $\mathrm{SL}_n(\mathbb{R})$  son grupos topológicos con el producto, vistos como subespacios de<sup>1</sup>  $\mathrm{Mat}_n(\mathbb{R}) \approx \mathbb{R}^n$ . Similarmente con  $\mathbb{Q}$  y  $\mathbb{C}$ .
5. El **círculo**  $\mathbb{S}^1$  es un grupo topológico compacto, visto como subgrupo topológico:

$$\mathbb{S}^1 = \{z \in \mathbb{C}^\times : |z| = 1\} \leq \mathbb{C}^\times.$$

En consecuencia, el  $n$ -toro  $\mathbb{T}^n := (\mathbb{S}^1)^n$  es un grupo topológico compacto.

Nótese que todos estos son grupos topológicos de Hausdorff.

**Proposición 13.2:** Sean  $G, H$  un par de grupos topológicos y sea  $f: G \rightarrow H$  un homomorfismo de grupos. Son equivalentes:

1.  $f$  es continuo.
2.  $f$  es continuo en algún  $a \in G$ .
- 2'  $f$  es continuo en  $1 \in G$ .
3. Para todo entorno  $V$  de  $1 \in H$ , existe un entorno  $U$  de  $1 \in G$  tal que si  $x^{-1}y \in U$ , entonces  $f(x)^{-1}f(y) \in V$ .

**Proposición 13.3:** Los grupos topológicos (como objetos) con los homomorfismos continuos (como flechas) conforman una categoría, denotada  $\mathrm{TopGrp}$ . De manera canónica, existen dos funtores (fieles) semiolvidadizos  $\mathrm{TopGrp} \rightarrow \mathrm{Grp}$  y  $\mathrm{TopGrp} \rightarrow \mathrm{Top}$ , no obstante, ninguno de los funtores son plenos.

**Teorema 13.4:** Sea  $G$  un grupo topológico y  $A, B \subseteq G$  subconjuntos.

1. Si  $A$  es abierto, entonces  $AB$  y  $BA$  son abiertos.
2. Si  $A, B$  son compactos, entonces  $AB$  es compacto.

---

<sup>1</sup>Aquí « $\approx$ » denota «homeomorfismo».



3. Si  $A$  es cerrado y  $B$  es compacto, entonces  $AB$  y  $BA$  son cerrados.

DEMOSTRACIÓN:

1. Basta notar que  $AB = \bigcup_{b \in B} Ab$  y que la traslación de abiertos es abierta.
2. Basta emplear que el conjunto  $A \times B \subseteq G \times G$  es compacto por el teorema de Tychonoff, de modo que su imagen  $*$ :  $A \times B \rightarrow AB$  es compacta.
3. ... □

**Ejemplo 13.5** (producto de cerrados puede no ser cerrado): Considere el grupo topológico  $(\mathbb{R}, +)$ . El subconjunto  $\mathbb{Z}$  es cerrado, así como  $\alpha\mathbb{Z} = \{n\alpha : n \in \mathbb{Z}\}$  para todo  $\alpha \in \mathbb{R}$ . En particular, escogiendo  $\alpha$  irracional, se comprueba que  $\mathbb{Z} + \alpha\mathbb{Z}$  es denso (¿por qué?), pero claramente no es todo  $\mathbb{R}$ . ┘

Demostrar que cerrado \* compacto = cerrado.

**Definición 13.6:** Sea  $G$  un grupo topológico. Se dice que un entorno  $U$  de 1 es *simétrico* si  $U = U^{-1}$ .

**Proposición 13.7:** Todo grupo topológico  $G$  posee una base de entornos simétricos del 1.

DEMOSTRACIÓN: Basta notar que si  $V$  es un entorno de 1, entonces  $V \cap V^{-1}$  es un subentorno simétrico del 1. □

**Corolario 13.7.1:** Todo grupo topológico es  $T_3$  (i.e., todo entorno  $g \in U$  admite un subentorno  $V$  tal que  $g \in V \subseteq \overline{V} \subseteq U$ ).

DEMOSTRACIÓN: Aplicando traslaciones basta probar la propiedad para el neutro. Sea  $U$  un entorno de 1, como  $1 \cdot 1^{-1} = 1$ , entonces existe un entorno  $1 \in V$  tal que  $V \cdot V^{-1} \subseteq U$ . Sea  $g \in \overline{V}$ , entonces todo entorno de  $g$  corta a  $V$ , luego la traslación  $gV$  da un entorno de  $g$ , de modo que  $gV \cap V \neq \emptyset$ , es decir, existe  $b \in V$  tal que  $gb = a \in V$ . Por lo tanto,  $g = ab^{-1} \in V \cdot V^{-1} \subseteq U$  y, así probamos que  $\overline{V} \subseteq U$ . □

Así que, si un grupo topológico es  $T_0$ , entonces es Hausdorff y regular.

**Proposición 13.8:** Sea  $G$  un grupo topológico y sean  $A, B \subseteq G$ . Entonces:

1.  $\overline{A} \cdot \overline{B} \subseteq \overline{A \cdot B}$ .
2.  $\overline{A}^{-1} = \overline{A^{-1}}$ .
3.  $g\overline{A}h = \overline{gAh}$ .

Más aún, si  $G$  es Hausdorff, entonces:

4. Si  $ab = ba$  para todo  $a \in A, b \in B$ , entonces  $ab = ba$  para todo  $a \in \overline{A}, b \in \overline{B}$ .

DEMOSTRACIÓN:

1. Ejercicio para el lector.
2. Se sigue de que  $()^{-1}: G \rightarrow G$  es un homeomorfismo.
3. Se sigue de que las traslaciones  $\tau_a^l$  y  $\tau_b^r$  son homeomorfismos.
4. La aplicación  $\varphi: G \times G \rightarrow G$  dada por  $\varphi(x, y) := xyx^{-1}y^{-1}$  es continua. Como  $\{1\}$  es cerrado, entonces  $D := \{(x, y) \in G \times G : xyx^{-1}y^{-1} = 1\}$  es cerrado y la hipótesis se traduce en que  $A \times B \subseteq D$ . Como  $\overline{A \times B} = \overline{A} \times \overline{B} \subseteq D$  se comprueba lo pedido.  $\square$

**Corolario 13.8.1:** Sea  $G$  un grupo topológico. Si  $H \subseteq G$  es un subgrupo (normal), entonces su clausura  $\overline{H}$  también es un subgrupo (normal). Más aún, si  $G$  es Hausdorff y  $H$  es abeliano, entonces  $\overline{H}$  también es abeliano.

**Corolario 13.8.2:** Sea  $G$  un grupo topológico. Entonces  $N := \overline{\{1\}} \trianglelefteq G$  es un subgrupo normal (de hecho, el subgrupo cerrado mínimo de  $G$ ) y  $G/N$ , con la topología cociente, es un grupo topológico Hausdorff.

El corolario anterior debería ser completamente intuitivo desde su enunciado, nótese que  $N$  es precisamente el conjunto de puntos topológicamente indistinguibles del  $\{1\}$ , de modo que el proceso es similar a aquel que realizamos para convertir un espacio pseudométrico en métrico. Aquí solo debemos cocientar la clausura del neutro, pues la homogeneidad del grupo la esparce.

**Proposición 13.9:** Sea  $G$  un grupo topológico y  $H \leq G$  un subgrupo.

1.  $H$  es abierto syss  $\text{Int } H \neq \emptyset$  (syss  $H$  contiene a un subconjunto abierto).

2. Si  $H$  es abierto, entonces también es cerrado.
3. Si  $H$  es cerrado y de índice finito, entonces también es abierto.
4. Si  $G$  es compacto, entonces todo subgrupo abierto tiene índice finito.

DEMOSTRACIÓN:

1. Claramente si  $H$  es abierto, entonces su interior es no vacío. Si  $U \subseteq H$  es abierto en  $G$ , entonces las traslaciones  $Uh$  con  $h \in H$  también son abiertas y  $H = \bigcup_{h \in H} hU$  es abierto.
2. Basta notar que  $G \setminus H = \bigcup_{g \notin H} gH$  es abierto.
3. Si  $H$  es de índice finito, entonces  $G \setminus H$  es la unión disjunta de finitas clases laterales de  $H$  por lo que, si  $H$  es cerrado, entonces  $G \setminus H$  también.
4. Basta notar que  $G$  es la unión disjunta de clases laterales de  $H$ , todas abiertas, por lo que, por definición de compacidad,  $H$  tiene que tener índice finito.  $\square$

**Definición 13.10:** Sea  $G$  un grupo topológico. Denotaremos  $H \leq_o G$  (resp. « $\leq_c$ ») si  $H$  es un subgrupo abierto (resp. cerrado) de  $G$ . Lo mismo con  $\trianglelefteq_o$  y  $\trianglelefteq_c$ .

**Proposición 13.11:** Sea  $G$  un grupo topológico Hausdorff. Todo subgrupo  $H$  de  $G$  que sea localmente compacto (e.g., discreto) es cerrado.

**Proposición 13.12:** Sea  $G$  un grupo topológico y sea  $U$  un entorno simétrico del neutro 1.

1. Entonces  $H := \bigcup_{n=1}^{\infty} U^n \leq_o G$  es un subgrupo abierto (y cerrado).
2. En particular, si  $G$  es conexo, entonces  $G = \bigcup_{n=1}^{\infty} U^n$ .
3. La componente conexa  $G^\circ$  del neutro 1 es un subgrupo normal cerrado.

**Proposición 13.13:** Sea  $G$  un grupo topológico.

1. Si  $G$  es (localmente) compacto, entonces todo cociente  $G/N$  también es (localmente) compacto.

2. El cociente  $G/N$  es discreto syss  $N \trianglelefteq_o G$  es abierto. En particular,  $G$  es discreto syss 1 es un punto aislado.
3. El cociente  $G/N$  es de Hausdorff syss  $N \trianglelefteq_c G$  es cerrado.

DEMOSTRACIÓN:

1. Basta notar que la imagen de un espacio localmente compacto es localmente compacta.
2. Basta probar la parte de «en particular» pues  $N \trianglelefteq_o G$  es abierto syss el neutro está aislado en el cociente  $G/N$ . La parte de «en particular» se sigue de trasladar el neutro para ver que todos los puntos están aislados.
3. Nuevamente, basta notar que el neutro es cerrado en  $G/N$  syss  $N \trianglelefteq_c G$  es cerrado.  $\square$

**Definición 13.14:** Sean  $\{G_i\}_{i \in I}$  una familia de grupos. Se define su **producto restringido** como el subgrupo  $\prod_{i \in I}^r G_i \leq \prod_{i \in I} G_i$  cuyos elementos son las tuplas  $(g_i)_{i \in I}$  donde  $g_i = 1$  para todos salvo finitos índices  $i \in I$ .

Si los  $G_i$ 's son grupos topológicos, entonces podemos dotar al producto restringido de la topología subespacio a la del producto usual.

**Proposición 13.15:** Sea  $\{G_i\}_{i \in I}$  una familia de grupos topológicos. Se cumplen:

1. El producto restringido  $\prod_{i \in I}^r G_i \leq \prod_{i \in I} G_i$  es denso.
2.  $\prod_{i \in I} G_i$  es localmente compacto syss cada  $G_i$  es localmente compacto y todos salvo finitos  $G_i$ 's son compactos.
3.  $\prod_{i \in I}^r G_i$  es de Hausdorff localmente compacto syss cada  $G_i$  es de Hausdorff localmente compacto y todos salvo finitos  $G_i$ 's son triviales.

**Definición 13.16:** Se dice que un grupo  $G$  es **divisible** si para cada  $g \in G$  y cada  $n \geq 1$  entero existe  $h$  tal que  $h^n = g$ .

Por ejemplo,  $\mathbb{Q}$  (o cualquier cuerpo de característica 0) es un grupo abeliano divisible.

**Lema 13.17:** Sea  $G$  un grupo abeliano arbitrario y sean  $g, h \in G$  dos elementos distintos. Entonces, existe un homomorfismo  $\varphi: G \rightarrow \mathbb{R}/\mathbb{Z}$  tal que  $\varphi(g) \neq \varphi(h)$ .

En la demostración emplearemos notación aditiva.

DEMOSTRACIÓN: Defínase  $H := \langle g, h \rangle \leq G$ , el cual es un subgrupo finitamente generado. Dividimos en los siguientes dos casos:

- $H$  es cíclico: En cuyo caso, sin pérdida de generalidad está generado por  $g$ . Si  $g$  es de torsión y tiene orden  $n > 1$ , entonces existe  $\psi: H \rightarrow \mathbb{R}/\mathbb{Z}$  dado por  $\psi(g) = [1/n]$  el cual es inyectivo y, en particular,  $\psi(g) \neq \psi(h)$ .

Si  $g$  no es de torsión, sea  $h = m \cdot g$  y definamos  $\psi: H \rightarrow \mathbb{R}/\mathbb{Z}$  dado por  $\psi(g) = [1/2m]$ ; así  $\psi(h) = [1/m] \neq \psi(g)$ .

- $H$  no es cíclico: En cuyo caso,  $H \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ , donde  $g = (1, 0)$  y  $h = (0, 1)$  mediante este isomorfismo y donde elegimos  $a, b$  positivos (posiblemente nulos). Nótese que todo homomorfismo  $H \rightarrow D$  se define mediante un par de homomorfismos  $\mathbb{Z}/a\mathbb{Z} \rightarrow D$  y  $\mathbb{Z}/b\mathbb{Z} \rightarrow D$ , para los cuales uno puede construir a mano homomorfismos con valores distintos.

Así obtenemos  $\psi: H \rightarrow D$  tal que  $\psi(g) \neq \psi(h)$ . Finalmente, un grupo abeliano es divisible si y sólo si es un  $\mathbb{Z}$ -módulo inyectivo, de modo que  $\psi$  se extiende a un homomorfismo  $\varphi: G \rightarrow D$  como se quería.  $\square$

**Ejemplo.** Si dotamos a  $\mathbb{R}$  con la topología usual, entonces el cociente de grupos topológicos  $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1 = \mathbb{T}^1$ . Esto puede verificarse notando que  $\mathbb{R}/\mathbb{Z}$  es topológicamente el cociente del intervalo  $[0, 1]$  con los extremos identificados.

Escribiremos  $\mathbb{R}/\mathbb{Z}$  cuando nos referimos al grupo (sin topología) y  $\mathbb{S}^1$  cuando lo vemos con la topología del círculo.

**Teorema (DE) 13.18:** Sea  $G$  un grupo abeliano infinito. Entonces existe una topología de modo que  $G$  sea un grupo topológico Hausdorff no discreto.

DEMOSTRACIÓN: Definamos  $H := \prod_{\psi \in \text{Hom}(G, \mathbb{R}/\mathbb{Z})} \mathbb{S}^1$ , donde  $\text{Hom}$  denota los homomorfismos usuales de grupos; así  $H$  es un grupo topológico Hausdorff

compacto. Definamos el siguiente homomorfismo de grupos usuales

$$\begin{aligned}\varphi: G &\longrightarrow H \\ g &\longmapsto (\psi(g))_{\psi \in \text{Hom}(G, \mathbb{R}/\mathbb{Z})}.\end{aligned}$$

Nótese que  $\varphi$  es inyectivo por el lema anterior, de modo que  $G \cong \varphi[G]$  (en  $\mathbf{Grp}$ ). Ahora,  $\varphi[G]$  posee una topología de Hausdorff; veamos que no es discreto. Si fuera discreto, entonces por la proposición 13.11, sería cerrado; pero como  $H$  es compacto, entonces  $\varphi[G]$  sería discreto compacto, luego sería finito, lo cual es absurdo. Así  $\varphi[G]$  no es discreto.  $\square$

**Teorema 13.19 (de la función abierta):** Sea  $G$  un grupo localmente compacto y  $\sigma$ -compacto (i.e.,  $G = \bigcup_{n=1}^{\infty} X_n$ , donde cada  $X_n$  es compacto). Entonces, todo homomorfismo continuo suprayectivo  $\varphi: G \rightarrow H$ , donde  $H$  es un grupo topológico de Hausdorff localmente compacto, es una función abierta.

Como corolario:

**Corolario 13.19.1 (teoremas de isomorfismos):** Sean  $G, H$  un par de grupos de Hausdorff localmente compactos y  $\sigma$ -compactos (e.g., compactos).

1. Dado un homomorfismo continuo  $\varphi: G \rightarrow H$  se factoriza por:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \downarrow & & \uparrow \\ G/\ker \varphi & \xrightarrow{\sim} & \text{Img } \varphi \end{array}$$

2. Sean  $F \leq_c G$  y  $N \trianglelefteq_c G$ , entonces

$$\frac{FN}{N} \cong \frac{F}{F \cap N}.$$

3. Sean  $F \leq_c N \trianglelefteq_c G$  tales que  $F \trianglelefteq G$ , entonces

$$\frac{G}{N} \cong \frac{G/F}{N/F}.$$

(Donde todas las flechas e isomorfismos están en  $\mathbf{TopGrp}$ .)



La hipótesis de  $\sigma$ -compacidad es necesaria, como muestra el siguiente ejemplo:

**Ejemplo.** Sea  $\mathbb{R}$  el grupo aditivo del cuerpo de los reales con la topología usual y sea  $\mathbb{R}_{\text{disc}}$  el grupo aditivo con la topología discreta. Ambos son grupos de Hausdorff, localmente compactos y abelianos. No obstante, la identidad induce un homomorfismo continuo  $\mathbb{R}_{\text{disc}} \rightarrow \mathbb{R}$  que, pese a ser biyectivo, no es un isomorfismo topológico. Esto es posible pues  $\mathbb{R}_{\text{disc}}$  no es  $\sigma$ -compacto.

**Proposición 13.20:** Sea  $G \leq \mathbb{R}$  un subgrupo de  $\mathbb{R}$ .

1. Si  $G$  no es discreto, entonces es denso.
2. En consecuencia, los subgrupos cerrados propios de  $\mathbb{R}$  son los de la forma  $\alpha\mathbb{Z}$  para algún  $\alpha \geq 0$ .
3. Los cocientes propios de  $\mathbb{R}$  que son Hausdorff son siempre topológicamente isomorfos a  $\mathbb{S}^1$ .

**Corolario 13.20.1:** Los subgrupos cerrados propios del círculo  $\mathbb{S}^1$  son finitos.

## 13.2\* Uniformidades y métricas

Solo porque es divertido. Las uniformidades son una versión más general (y, por tanto, más débil) que las métricas, pero que demuestran una determinada regularidad sobre el espacio que claramente los grupos topológicos ponen en manifiesto.

Para ésta sección emplearemos la noción de espacios uniformes (cfr. ENGELKING [0], Ch. 8).

**Definición 13.21:** Sea  $G$  un grupo topológico y sea  $\mathcal{V}$  la familia de entornos simétricos del 1. Para todo  $V \in \mathcal{V}$  definimos:

$$V_s := \{(x, y) : x^{-1}y \in V\}, \quad V_d := \{(x, y) : xy^{-1} \in V\}.$$

Definimos la *uniformidad izquierda* (resp. *derecha*) a aquella inducida por la base de uniformidades  $\mathcal{B}_s := \{V_s : V \in \mathcal{V}\}$  (resp. la base  $\mathcal{B}_d := \{V_d : V \in \mathcal{V}\}$ ).

**Lema 13.22:** Sea  $G$  un grupo topológico y sea  $\mathcal{V}$  la familia de entornos simétricos del 1. Las familias:

$$\mathcal{B}_s := \{V_s : V \in \mathcal{V}\}, \quad \mathcal{B}_d := \{V_d : V \in \mathcal{V}\}$$

son bases de uniformidades sobre  $G$ , denominadas **uniformidad izquierda** (resp. *derecha*) sobre  $G$  y denotadas  $\mathcal{U}_s$  (resp.  $\mathcal{U}_d$ ).

DEMOSTRACIÓN: El que los elementos de  $\mathcal{B}_*$  sean bandas viene dado por el hecho de que claramente contienen a la diagonal y son simétricos, pues los elementos de  $\mathcal{V}$  son entornos simétricos del 1. Sean  $U_1, U_2 \in \mathcal{B}_*$ , es decir, cada  $U_i = (V_i)_*$  para algún  $V_i \in \mathcal{V}$ . Luego es fácil comprobar que  $U_1 \cap U_2 = (V_1 \cap V_2)_* \in \mathcal{B}_*$ . Finalmente, sea  $V_* \in \mathcal{B}_*$  dado por  $V \in \mathcal{V}$ . Entonces existe  $W \in \mathcal{V}$  tal que  $W \cdot W \subseteq V$  y es fácil comprobar que  $W_* + W_* = (W \cdot W)_* \subseteq V_*$ , como se quería probar.  $\square$

**Lema 13.23:** Sea  $G$  un grupo topológico y  $V$  un entorno simétrico del neutro. Para todo  $x \in G$  se tiene que  $B_{V_s}(x) = xV$  y  $B_{V_d}(x) = Vx$ . En consecuencia, las traslaciones izquierdas (resp. derechas) son uniformemente continuas en  $(G, \mathcal{U}_s)$  (resp.  $(G, \mathcal{U}_d)$ ).

**Teorema 13.24:** Si  $G$  es un grupo topológico, entonces su topología es la inducida por la uniformidad izquierda (y derecha). En consecuencia:

1. Todo grupo topológico es un espacio uniformizable.
2. (DE) Si  $G$  es un grupo topológico  $T_0$ , entonces es un espacio de Tychonoff.

DEMOSTRACIÓN: La segunda consecuencia se sigue de que todo espacio uniforme  $T_0$  es de Tychonoff (cfr. ENGELKING [0], cor. 8.1.13; o bien [top], cor. 5.62).  $\square$



Si bien las uniformidades izquierda y derecha inducen la misma topología, en general no son equivalentes (a menos que el grupo sea abeliano) y dan lugar a distintas nociones de funciones uniformemente continuas.

**Corolario 13.24.1:** Sean  $G, H$  un par de grupos topológicos y sea  $f: G \rightarrow H$  un homomorfismo de grupos. Entonces  $f$  es continua si y sólo si es uniformemente continua (con respecto a cualquier uniformidad).

**Teorema 13.25 (Birkhoff-Kakutani):** Sea  $G$  un grupo topológico. Entonces  $G$  es metrizable si y sólo si es Hausdorff y 1AN. Más aún, de ser metrizable admite una métrica  $d$  que es invariante por la izquierda, vale decir, tal que

$$\forall g, x, y \in G \quad d(gx, gy) = d(x, y).$$



### 13.3 Dualidad de Pontryagin-van Kampen

**Definición 13.26:** Sea  $G$  un grupo abeliano topológico. Un *character* es un homomorfismo continuo  $\gamma: G \rightarrow \mathbb{S}^1$ . El conjunto de todos los caracteres de  $G$  es el *grupo dual (topológico)*  $\hat{G} := \text{Hom}_{\text{TopGrp}}(G, \mathbb{S}^1)$ . Decimos que dos grupos abelianos topológicos  $G, H$  son *duales* entre sí si  $G \cong \hat{H}$  y  $H \cong \hat{G}$ . Se dice que  $G$  es *autodual* si  $G \cong \hat{G}$ .

Decimos que un grupo es *l.c.a.* si es de Hausdorff, localmente compacto y abeliano.

Nótese que no siempre  $G$  y  $\hat{G}$  son duales entre sí (similar al caso de espacios vectoriales, donde esto falla para dimensión infinita). El propósito de esta sección es probar que si  $G$  es l.c.a., entonces  $G$  y  $\hat{G}$  son duales.

**Ejemplo.** Considere  $G$  cualquier grupo topológico no abeliano. Entonces  $\hat{G}$  siempre es abeliano (pues emplea la operación puntual en el codominio  $\mathbb{S}^1$ , el cual sí es abeliano), de modo que  $G, \hat{G}$  nunca son duales entre sí.

**Ejemplo.** Son grupos l.c.a. autoduales:

- $\mathbb{R}$ .

Esto se debe a que la imagen de un compacto conexo es otro compacto conexo, así que a menos que el caracter sea nulo, uno puede restringirse a un intervalo suficientemente pequeño del 0 en  $\mathbb{R}$  de modo que el caracter determina un homeomorfismo con su imagen. Esto prueba que todo caracter no nulo  $\mathbb{R} \rightarrow \mathbb{S}^1$  se factoriza por  $\mathbb{R} \rightarrow \mathbb{R} \rightarrow \mathbb{R}/\mathbb{Z}$ , y es un típico ejercicio de cálculo el verificar que los únicos endomorfismos continuos de  $\mathbb{R}$  son los lineales.

- Los grupos finitos (discretos).

Toda función desde un espacio discreto a otro es continua, así que al formular caracteres podemos «olvidar la continuidad». Ahora se convierte en un ejercicio (notando que si  $n \cdot x = 1$  en  $G$ , entonces  $\varphi(x) \in \langle 1/n \rangle \subseteq \mathbb{R}/\mathbb{Z}$ ). Esto es particularmente directo si el grupo es cíclico finito, y de ahí puede usar la clasificación de grupos abelianos finitos.

**Lema 13.27:** Tanto la topología de convergencia puntual, como la de convergencia uniforme y la de convergencia uniforme sobre compactos son tales que  $\hat{G}$  sea un grupo topológico.

DEMOSTRACIÓN: Ejercicio para el lector.  $\square$

**Teorema 13.28:** Sea  $G$  un grupo l.c.a., entonces su dual  $\hat{G}$  con la topología compacto-abierta es l.c.a.

**Teorema 13.29:** Sea  $G$  un grupo l.c.a. Si  $G$  es compacto, entonces  $\hat{G}$  es discreto y si  $G$  es discreto, entonces  $\hat{G}$  es compacto.

**Ejemplo.** El dual topológico del círculo  $\widehat{\mathbb{S}^1}$  es  $\mathbb{Z}$ . Más explícitamente, los caracteres, identificando  $\mathbb{S}^1 \leq \mathbb{C}^\times$ , son  $z \mapsto z^n$  con  $n \in \mathbb{Z}$ . Similarmente  $\hat{\mathbb{Z}} \cong \mathbb{S}^1$ , esto se ve del que todo homomorfismo es automáticamente continuo y que  $\text{Hom}(\mathbb{Z}, G) \cong G$  para todo grupo  $G$ . Así que  $\mathbb{Z}, \mathbb{S}^1$  son duales entre sí.

**Proposición 13.30:** Sea  $G$  un grupo l.c.a. Entonces el homomorfismo canónico

$$\alpha: G \longrightarrow \hat{\hat{G}}, \quad \alpha(x)(f) := f(x)$$

es continuo. Más aún,  $\alpha$  es inyectiva si y sólo si los caracteres de  $G$  separan puntos (i.e., si para todo  $g \neq h \in G$  existe  $\chi \in \hat{G}$  tal que  $\chi(g) \neq \chi(h)$ ).

DEMOSTRACIÓN: Para la continuidad de  $\alpha$ , emplearemos métodos casi-categoriales (también puede intentarlo como ejercicio). Denotaremos por  $C_c(X, Y)$  al espacio de funciones continuas con la topología compacto-abierta, entonces  $\alpha$  viene de la adjunción topológica:

$$\text{Hom}(G, \hat{\hat{G}}) \subseteq C_c(G, C_c(\hat{G}, \mathbb{S}^1)) \approx C_c(G \times \hat{G}, \mathbb{S}^1),$$

donde « $\approx$ » denota homeomorfismo de espacios (en **Top**). En el lado derecho tomamos la aplicación de evaluación  $\text{ev}(x, f) := f(x)$  la cual es continua y se corresponde mediante los isomorfismos a  $\alpha$ .

La inyectividad queda de ejercicio al lector.  $\square$

## 13.4 Grupos profinitos

Recuérdese lo siguiente de su curso de topología (e.g., ENGELKING [0]):

**Definición 13.31:** Un conjunto parcialmente ordenado  $(I, \leq)$  se dice *conjunto dirigido* si para cada  $i, j \in I$  existe  $k \in I$  tal que  $i \leq k$  y  $j \leq k$ .

Un *sistema inverso* en una categoría  $\mathcal{C}$  es un diagrama

$$X_- : \text{Poset}(I)^{\text{op}} \rightarrow \mathcal{C};$$

vale decir, es una familia  $\{X_i\}_{i \in I}$  de objetos en  $\mathcal{C}$  con una familia de flechas  $\{X_j \xrightarrow{\varphi_{ji}} X_i\}_{i \leq j}$  tales que:

1.  $\varphi_{ii} = 1_{X_i}$ .
2.  $\varphi_{kj} \circ \varphi_{ji} = \varphi_{ki}$  para  $i \leq j$  y  $j \leq k$ .

(El curioso ordenamiento de índices está para enfatizar que el dominio se dualiza.)

Si la categoría  $\mathcal{C}$  es concreta, se dice que el sistema inverso es *suprayectivo* si las funciones  $\varphi_{ij}$  lo son.

Técnicamente, **Top** ya es una categoría completa, de modo que admite límites inversos de todo tipo, pero la restricción a sistemas inversos está dada porque facilita el calculo concreto de dicho límite.

**Proposición 13.32:** Sea  $G := \varprojlim_{i \in I} G_i$  un límite cofiltrado de grupos compactos de Hausdorff con proyecciones  $p_i : G \rightarrow G_i$ , y sea  $N \trianglelefteq_o G$ . Entonces  $\ker(p_i) \leq_c N$  para algún  $i$  y, por lo tanto,  $G/N$  es isomorfo (en **TopGrp**) al cociente de algún subgrupo de algún  $G_i$ . Si además el sistema inverso es suprayectivo, entonces  $G/N$  es el cociente de algún  $G_i$ .

DEMOSTRACIÓN: Como  $G$  es un límite cofiltrado de espacios topológicos, entonces

$$\{p_i^{-1}[U_i] : U_i \subseteq G_i \text{ abierto}\}_{i \in I}$$

es una base de la topología, por lo tanto, como  $N$  es un entorno del neutro 1, entonces  $N \supseteq p_i^{-1}[U]$  para algún  $U \subseteq G_i$  entorno del 1. Como  $N$  es Hausdorff, entonces  $\ker(p_i)$  es un subespacio cerrado y es un subgrupo. El tercer teorema de isomorfismos dice que

$$\frac{G}{N} \cong \frac{G/\ker(p_i)}{N/\ker(p_i)},$$

y como  $G/\ker(p_i) \cong \text{Img}(p_i)$  por el primer teorema de isomorfismos (con topologías), entonces  $G/N$  es un cociente de  $\text{Img}(p_i)$  como se quería probar.  $\square$

**Proposición 13.33:** Sea  $G$  un grupo topológico y sea  $\mathcal{F}$  una base de filtro conformada por subgrupos normales cerrados. Así  $(\mathcal{F}, \supseteq)$  es un conjunto dirigido e induce el sistema inverso  $\pi_M^N: G/N \rightarrow G/M$  para  $N \supseteq M$  en  $\mathcal{F}$ . Sea  $(\widehat{G}, p_N) := \varprojlim_{N \in \mathcal{F}} G/N$ , entonces el homomorfismo continuo inducido  $\varphi: G \rightarrow \widehat{G}$  satisface lo siguiente:

- (a) Tiene núcleo  $\ker \varphi = \bigcap_{N \in \mathcal{F}} N$ .
- (b) Es dominante, i.e., tiene imagen densa.
- (c) Si  $G$  es compacto, entonces  $\varphi$  es suprayectivo.

DEMOSTRACIÓN: De manera concreta se construye  $\widehat{G}$  como el subgrupo de  $P := \prod_{N \in \mathcal{F}} G/N$  de hebras, y el homomorfismo  $\varphi: G \rightarrow \widehat{G}$  es la restricción (en el codominio) del homomorfismo canónico  $\bar{\varphi}: G \rightarrow P$ . Nótese que entonces

$$\ker \varphi = \ker \bar{\varphi} = \bigcap_{N \in \mathcal{F}} N.$$

Lo que prueba (a), y como  $p_N[\varphi[G]] = G/N$  para todo  $N \in \mathcal{F}$ , entonces vemos que  $\varphi$  es dominante (¿por qué?). Finalmente, nótese que, por construcción  $P$  es un grupo topológico de Hausdorff, con lo que si  $G$  es compacto, entonces su imagen es compacta, luego es cerrada, por lo que  $\varphi$  es suprayectivo.  $\square$

**Lema 13.34 (D. van Dantzig):** Sea  $G$  un grupo topológico Hausdorff, localmente compacto y hereditariamente desconexo. Entonces todo entorno compacto de 1 contiene un subgrupo abierto y compacto.

Lo interesante no es el que contenga un subentorno abierto y cerrado, lo que sería trivial de la equivalencia entre ser hereditariamente desconexo y cerodimensional (cfr. ENGELKING [0], thm. 6.2.10), sino que lo llamativo es que sea un subgrupo.

DEMOSTRACIÓN: Sea  $U$  un entorno del neutro 1. Como el espacio es hereditariamente desconexo, entonces es cerodimensional y, por tanto, existe un subentorno compacto  $K \subseteq U$  del 1 y, por el lema anterior, existe un entorno simétrico  $V$  del 1 tal que  $K \cdot V \subseteq K$  y, por tanto,  $K \cdot V = K$ . Definiendo

$$L := \{g \in G : K \cdot g = K\}$$

vemos que es un subgrupo y satisface que  $V \subseteq L$ , por lo tanto, es abierto y también cerrado, ergo, compacto.  $\square$

**Teorema 13.35:** Sea  $\mathcal{C}$  una clase de grupos finitos (a los que dotamos de la topología discreta) cerrada bajo subgrupos y productos. Para un grupo topológico  $G$  son equivalentes:

1.  $G$  es un **grupo pro- $\mathcal{C}$**  (i.e., es el límite cofiltrado de grupos en  $\mathcal{C}$ ).
2.  $G$  es isomorfo a un subgrupo cerrado de un producto cartesiano de grupos en  $\mathcal{C}$ .
3.  $G$  es compacto y  $\bigcap \{N : N \trianglelefteq_o G, G/N \in \mathcal{C}\} = \{1\}$ .
4.  $G$  es compacto, hereditariamente desconexo y para todo  $N \trianglelefteq_o G$ , existe  $M \trianglelefteq_o G$  tal que  $M \leq_c N$  y  $G/M \in \mathcal{C}$ .

Si además  $\mathcal{C}$  es cerrado bajo cocientes, entonces las anteriores son equivalentes a:

- 4\*  $G$  es compacto, hereditariamente desconexo y  $G/N \in \mathcal{C}$  para todo  $N \trianglelefteq_o G$ .

DEMOSTRACIÓN:  $1 \implies 2 \wedge 4$ . Son claras.

$2 \implies 3$ . Sea  $G$  un subgrupo cerrado de  $P := \prod_{i \in I} G_i$ , donde cada  $G_i \in \mathcal{C}$ , y sea  $K_i$  el núcleo de la proyección  $P \twoheadrightarrow G_i$ . Entonces  $P$  es compacto y  $G$  también. Sea  $N_i := K_i \cap G \trianglelefteq_o G$ , entonces claramente  $\bigcap_{i \in I} N_i = \{1\}$  y

$$\frac{G}{N_i} \cong \frac{GK_i}{K_i} \leq_c \frac{P}{K_i} \cong G_i,$$

de modo que  $G/N_i \in \mathcal{C}$  como se quería ver.

$3 \implies 1$ . Sea  $\mathcal{F} := \{N \trianglelefteq_o G : G/N \in \mathcal{C}\}$ . Dados  $N, M \in \mathcal{F}$ , nótese que el homomorfismo continuo

$$G \rightarrow G/N \times G/M, \quad g \mapsto (Ng, Mg)$$

tiene núcleo  $N \cap M$ , de modo que  $N \cap M \in \mathcal{C}$ . Así que  $\mathcal{F}$  es una base de filtro conformada por subgrupos normales cerrados,  $\bigcap_{N \in \mathcal{F}} N = \{1\}$  y como  $G$  es cerrado, entonces se sigue de la proposición anterior que  $G \cong \varprojlim_{N \in \mathcal{F}} G/N$ .

$4 \implies 3$ . Nótese que  $\overline{\{1\}}$  será conexo por ser la clausura de un conjunto conexo, luego como  $G$  es hereditariamente desconexo, entonces esto comprueba que  $\overline{\{1\}} = \{1\}$ , por lo que,  $G$  es de Hausdorff. Sea  $U \subseteq G$  un subconjunto abierto no vacío, entonces para todo  $x \in U$  existe un subgrupo normal abierto  $N_x \subseteq Ux^{-1}$ , de modo que  $U = \bigcup_{x \in U} N_x x$ . Así pues,

$$x \notin \overline{S} \iff \exists x \in U \text{ abierto : } U \cap S = \emptyset \iff \exists N \trianglelefteq_o G : Nx \cap S = \emptyset.$$

Con lo que probamos que  $\bar{S} = \bigcap_{N \leq_o G} N \cdot S$ , y en particular,  $\{1\} = \bigcap_{N \leq_o G} N$ .

La equivalencia  $4 \iff 4^*$  sale del tercer teorema de isomorfismos.  $\square$

Nótese que si  $\mathcal{C}$  es la clase de todos los grupos finitos, entonces la condición  $4^*$  se reduce a que  $G$  sea un espacio de Stone (i.e., un espacio topológico que sea el límite de espacios discretos finitos).

Objetos de $\mathcal{C}$	Grupos pro- $\mathcal{C}$
Grupos finitos	Grupos profinitos
Grupos cíclicos	Grupos procíclicos
Grupos abelianos	Grupos proabelianos
$p$ -grupos	Grupos pro- $p$

**Figura 13.1.** Nomenclatura de grupos.

**Definición 13.36:** Un *número supernatural* (o *número de Steinitz*) es un producto formal  $a := \prod_p p^{a_p}$ , donde cada  $a_p \in \mathbb{N} \cup \{\infty\}$  y  $p$  recorre todos los números primos. Dados  $a, b := \prod_p p^{b_p}$  un par de números supernaturales, denotamos

$$a \mid b \iff \forall p \quad a_p \leq b_p.$$

Dado un conjunto  $\{n_i\}_{i \in I}$  de números supernaturales con  $n_i = \prod_p p^{n_{i,p}}$  definimos su *mínimo común múltiplo* como

$$\text{mcm}\{n_i\}_i := \prod_p p^{m_p}, \quad m_p := \sup\{n_{i,p} : i \in I\}.$$

**Definición 13.37:** Sea  $G$  un grupo profinito y sea  $H \leq_c G$  un subgrupo cerrado. Se define el *índice* como el siguiente número supernatural

$$[G : H] := \text{mcm}\{[G : U] : G \subseteq U \leq_o G\}.$$

Se define el *orden* de  $G$  como  $|G| := [G : 1]$  y dado  $x \in G$  se define su *orden* como  $|\langle x \rangle|$ .

Nótese que cuando los números supernaturales son de hecho naturales entonces coinciden con las nociones clásicas.

**Proposición 13.38 (Lagrange):** Sea  $G$  un grupo profinito y sean  $K \leq_c H \leq_c G$ , entonces  $[G : K] = [G : H][H : K]$ .

DEMOSTRACIÓN: Si  $N \trianglelefteq_o G$ , entonces el índice  $[G : N]$  es finito y  $NK, NH \leq_c G$ , de modo que también tienen índice finito. Por lo tanto, podemos aplicar el teorema de Lagrange usual:

$$[G : NK] = [G : NH] [NH : NK] = [G : NH] [H : (N \cap H)K],$$

donde para la tercera igualdad usamos el segundo teorema de isomorfismos. Así  $[G : K]$  divide a  $[G : H] [H : K]$ .

Recíprocamente, si  $N_1 \trianglelefteq_o G$  y  $N_2 \trianglelefteq_o H$ , entonces  $N_2$  es la intersección de un abierto de  $G$  con  $H$ , es decir, existe  $M \trianglelefteq_o G$  tal que  $M \cap H \leq_c N_2$ . Sea  $N := M \cap N_1 \trianglelefteq_o G$ , entonces  $[G : N_1H] [H : N_2K]$  divide a  $[G : NH] [H : (N \cap H)K] = [G : NK]$ , de modo que  $[G : H] [H : K]$  divide a  $[G : K]$ .  $\square$

**Definición 13.39:** Sea  $G$  un grupo profinito y sea  $p$  un número primo. Un  *$p$ -subgrupo de Sylow*<sup>2</sup>  $P$  de  $G$  es un subgrupo cerrado tal que  $|P|$  es una potencia (posiblemente infinita) de  $p$  y tal que  $p \nmid [G : P]$ .

Equivalentemente, un  $p$ -subgrupo de Sylow es un subgrupo cerrado pro- $p$  maximal en  $G$ .

**Lema 13.40:** Sea  $G$  un grupo profinito y sea  $\{H_i \leq_c G\}_{i \in I}$  una familia de subgrupos que satisfaga que para todo  $i, j \in I$  exista un  $k \in I$  tal que  $H_k \leq_c H_i \cap H_j$ . Entonces:

$$\left[ G : \bigcap_{i \in I} H_i \right] = \text{mcm}\{[G : H_i] : i \in I\}.$$

DEMOSTRACIÓN: Por el teorema de Lagrange (profinito) es claro que el lado derecho divide al lado izquierdo.

Sea  $U \trianglelefteq_o G$  tal que contiene a  $\bigcap_{i \in I} H_i$ , entonces  $\bigcap_{i \in I} (H_i \cap (G \setminus U)) = \emptyset$  y, como los  $H_i \cap (G \setminus U)$  son cerrados, por compacidad se cumple que

$$\bigcap_{j=1}^r (H_{i_j} \cap (G \setminus U)) = \emptyset.$$

Así pues,  $\bigcap_{j=1}^r H_{i_j} \leq_c U$ . Elijamos  $k \in I$  tal que  $H_k \leq_c H_{i_j}$  para cada  $1 \leq j \leq r$ , de modo que  $[G : U]$  divide a  $[G : H_k]$ . Es decir, hemos probado que el lado izquierdo divide al derecho.  $\square$

<sup>2</sup>Varios autores emplean *subgrupo de  $p$ -Sylow* que es en cierta medida mejor puesto que técnicamente no son  $p$ -subgrupos, sino subgrupos pro- $p$ .

**Proposición 13.41 (teoremas de Sylow profinitos):** Sea  $G$  un grupo profinito y sea  $p$  un número primo. Se cumplen:

1.  $G$  posee  $p$ -subgrupos de Sylow.
2. Si  $P$  es un  $p$ -subgrupo de Sylow de  $G$  y  $H \leq_c G$  es un subgrupo pro- $p$ , entonces existe  $g \in G$  tal que  $gHg^{-1} \leq_c P$ . En consecuencia, todos los  $p$ -subgrupos de Sylow son conjugados entre sí.
3. Todo subgrupo (cerrado) pro- $p$  de  $G$  está contenido en un  $p$ -subgrupo de Sylow.
4. Si  $G$  es abeliano, entonces es el producto directo de sus  $p$ -subgrupos de Sylow.

DEMOSTRACIÓN:

1. Sea  $\mathcal{F}$  la familia de subgrupos cerrados de  $G$  de índice coprimo a  $p$ , el cual es no vacío ya que  $G \in \mathcal{F}$ , y es un conjunto parcialmente ordenado respecto a  $\subseteq$ . Por el lema anterior, si  $C \subseteq \mathcal{F}$  es una cadena, entonces  $\bigcap C \in \mathcal{F}$ ; de modo que por el lema de Zorn,  $\mathcal{F}$  admite un elemento  $\subseteq$ -minimal  $P$ . Esto significa que para todo  $H \leq_c P$  se cumple que  $p \mid [P : H]$  por el teorema de Lagrange.

Ahora bien, si  $P$  no fuese un grupo pro- $p$ , entonces existiría  $N \trianglelefteq_o P$  tal que  $[P : N]$  no es potencia de  $p$ ; luego por el primer teorema de Sylow (usual), existe un  $p$ -subgrupo de Sylow  $Q/N \leq P/N$  y, por el tercer teorema de isomorfismos,  $p \nmid [P/N : Q/N] = [P : Q] \neq 1$ , lo cual es absurdo. Así que  $P$  es un  $p$ -subgrupo de Sylow como se quería ver.

2. Sea  $N \trianglelefteq_o G$ , de modo que  $N \cap P \trianglelefteq_o P$  y por el segundo teorema de isomorfismos

$$\frac{NP}{P} \cong \frac{P}{N \cap P},$$

de modo que  $NP/N$  es un  $p$ -grupo. Además,  $[G : NP]$  divide a  $[G : P]$ , por lo que  $NP/N$  es un  $p$ -subgrupo de Sylow de  $G/N$ . Análogamente,  $NH/H$  es un  $p$ -subgrupo de Sylow de  $G/N$ . Por el segundo teorema de Sylow, vemos que el conjunto

$$R(N) := \{g \in G : g(NH)g^{-1} \subseteq NP\}$$

es no vacío y, como es la unión de clases laterales de  $N$ , es cerrado.



Si  $M \trianglelefteq_o G$  es tal que  $M \leq_c N$ , entonces claramente  $R(M) \subseteq R(N)$ , por lo que si  $N_1, \dots, N_r$  son subgrupos normales abiertos de  $G$  tenemos que

$$R(N_1) \cap \dots \cap R(N_r) \supseteq R(N_1 \cap \dots \cap N_r) \neq \emptyset.$$

Así que la familia  $\{R(N) : N \trianglelefteq_o G\}$  está conformada por cerrados y posee la p.i.f. (propiedad de intersecciones finitas), por lo que, por compacidad, existe  $g \in \bigcap_{N \trianglelefteq_o G} R(N)$  y, por definición,

$$\forall N \trianglelefteq_o G \quad gHg^{-1} \subseteq NP \implies gHg^{-1} \leq \bigcap_{N \trianglelefteq_o G} NP = P.$$

3. Basta tomar cocientes y aplicar el inciso 1.
4. Se deduce del caso finito, el cual a su vez se deduce del teorema fundamental de grupos abelianos.  $\square$

**Ejemplo.** Considere los grupos cíclicos  $(\mathbb{Z}/n\mathbb{Z})_{n \in \mathbb{N}}$  donde si  $n \mid m$ , denotamos por  $\pi_{n,m} : \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  a la reducción módulo  $n$ . Así, los elementos de  $\mathbb{N} \setminus \{0\}$  ordenados por divisibilidad con estos homomorfismos forman un sistema inverso y definimos

$$\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

Si consideramos en el sistema inverso solo los índices  $n = p^r$  para un número primo  $p$  fijo, obtenemos el **anillo de enteros  $p$ -ádicos**

$$\mathbb{Z}_p := \varprojlim_r \mathbb{Z}/p^r\mathbb{Z},$$

el cual es claramente un subgrupo cerrado pro- $p$  de  $\widehat{\mathbb{Z}}$  y es, además, el  $p$ -subgrupo de Sylow de  $\widehat{\mathbb{Z}}$  (¿por qué?). Así el inciso 4 del teorema anterior nos dice que

$$\widehat{\mathbb{Z}} \cong \prod_{p \text{ primo}} \mathbb{Z}_p.$$

Los subgrupos de Sylow se generalizan en:

**Definición 13.42:** Sea  $\pi \subseteq \mathbb{N}$  un subconjunto no vacío (posiblemente infinito) de primos. Se dice que un grupo profinito es **pro- $\pi$**  si su orden es divisible por primos exclusivamente en  $\pi$ . Dado un grupo profinito  $G$ , se dice

que  $H \leq_c G$  es un  $\pi$ -*subgrupo de Hall* si es un subgrupo pro- $\pi$  y su índice  $[G : H]$  es coprimo con  $\pi$  (o equivalente, si todo primo que divide a  $[G : H]$  no pertenece a  $\pi$ ).

Si  $\pi = \{p\}$ , entonces un  $\{p\}$ -subgrupo de Hall equivale a un  $p$ -subgrupo de Sylow. Si  $\pi$  es el conjunto de todos los primos distintos de  $p$ , entonces un  $\pi$ -subgrupo de Hall se llama un  $p$ -*complemento*.

Todo  $\pi$ -subgrupo de Hall es un subgrupo pro- $\pi$  maximal, pero el recíproco no es cierto.

**Proposición 13.43:** Un grupo profinito  $G$  es prosoluble si y sólo si posee  $p$ -complementos para todo primo  $p$ .

#### §13.4.1 Teoría de Galois infinita.

**Definición 13.44:** Sea  $L/k$  una extensión de Galois posiblemente infinita. Denotaremos por  $\mathcal{F}_L$  al conjunto dirigido, cuyos elementos son subextensiones  $k \subseteq F \subseteq L$  tales que  $F/k$  es finito, y cuya relación de orden parcial es la inclusión.

En la teoría de categorías, los diagramas filtrados (o los diagramas contravariantes filtrados, llamados *cofiltrados*) suelen gozar de buenas propiedades, como intercambios de límite.

**Lema 13.45:** Sea  $L/k$  una extensión de Galois. Entonces:

1.  $L = \varinjlim_{F \in \mathcal{F}_L} F$ .
2.  $\text{Gal}(L/k) = \varprojlim_{F \in \mathcal{F}_L} \text{Gal}(F/k)$ , donde, si  $L \subseteq L'$ , entonces el homomorfismo de vínculo es

$$\rho_L^{L'} : \text{Gal}(L'/k) \longrightarrow \text{Gal}(L/k), \quad \sigma \longmapsto \sigma|_L.$$

DEMOSTRACIÓN:

1. Esto es un mero ejercicio de comprobar que si  $F, F' \in \mathcal{F}$ , entonces  $F \vee F' \in \mathcal{F}$ ; y que todo elemento de  $\alpha \in L$ , siendo algebraico y separable, pertenece a una subextensión de Galois finita, vale decir, la clausura normal de  $k(\alpha)$ .

2. En primer lugar, veamos qué homomorfismos determinan el cono  $\{\rho_F^L: \text{Gal}(L/k) \rightarrow \text{Gal}(F/k)\}_{F \in \mathcal{F}_L}$ . Como puede adivinar, el homomorfismo está dado por  $\rho_F^L(\sigma) := \sigma|_F$ , el cual está bien definido pues un automorfismo de extensiones de cuerpos manda un elemento en sus conjugados, y  $F$  está cerrado bajo conjugación. Claramente, estos homomorfismos son también compatibles.

Finalmente, para ver que el cono es de hecho un límite, basta notar que una familia  $\{\sigma_F: F \rightarrow F\}_{F \in \mathcal{F}_L}$  de  $K$ -automorfismos compatibles con las restricciones se pega de manera única en un  $K$ -automorfismo  $\sigma: L \rightarrow L$ .

Una demostración alternativa es la siguiente sucesión de isomorfismos canónicos:

$$\begin{aligned} \text{Gal}(L/k) &= \text{Hom}_K(L, L) = \text{Hom}_K\left(\varinjlim_F F, L\right) \\ &\cong \varprojlim_{(1)}_F \text{Hom}_K(F, L) = \varprojlim_{(2)}_F \text{Hom}_K(F, F) = \varprojlim_F \text{Gal}(F/k), \end{aligned}$$

donde (1) sale de que  $\text{Hom}_K(-, N)$  es un funtor contravariante con adjunta derecha (contravariante), de modo que transforma límites directos en inversos, y (2) sale de que  $F/k$  sea una extensión de Galois.  $\square$

Así, el grupo de Galois de una extensión de Galois arbitraria siempre es un grupo profinito con la topología inducida por el límite de la proposición anterior, la cual denominamos **topología de Krull** sobre  $\text{Gal}(L/k)$ .

**Lema 13.46:** Sea  $L/k$  una extensión de Galois. Entonces:

1. Los subgrupos  $\text{Gal}(L/F) \leq \text{Gal}(L/k)$ , donde  $F \in \mathcal{F}_L$ , forman una base de entornos abiertos y cerrados del neutro  $\text{Id}_L$ .
2. En consecuencia, para toda subextensión  $k \subseteq K \subseteq L$ , donde  $K/k$  es finita (no necesariamente normal), se cumple que  $\text{Gal}(L/K)$  es un subgrupo abierto y cerrado de  $\text{Gal}(L/k)$ .
3. Si dotamos a  $L$  de la topología discreta, entonces la topología de Krull sobre  $\text{Gal}(L/k)$  es la inicial de manera que las aplicaciones

$$\text{ev}_\alpha: \text{Gal}(L/k) \rightarrow L, \quad \sigma \mapsto \sigma(\alpha)$$

sean continuas para cada  $\alpha \in L$ .

DEMOSTRACIÓN:

1. Una base para la topología de Krull está conformada por los abiertos básicos de la forma

$$U := (\rho_{F_1}^L)^{-1}[A_1] \cap \cdots (\rho_{F_n}^L)^{-1}[A_n],$$

donde cada  $F_i \in \mathcal{F}_L$ , donde  $\rho_F^L$  denota la restricción canónica y donde cada  $A_i \subseteq \text{Gal}(F_i/k)$  es un subconjunto abierto, o equivalentemente, cualquier subconjunto. Como los  $A_i$ 's son abiertos y cerrados, también lo es  $U$ . Así fijamos esta base para la topología de Krull.

Para que  $U$  sea entonces un entorno básico de  $\text{Id}_L$ , es necesario que  $\rho_{F_i}^L(\text{Id}_L) = \text{Id}_{F_i} \in A_i$ , de modo que  $U$  debe contener al subentorno básico

$$V := (\rho_{F_1}^L)^{-1}[\{\text{Id}_{F_1}\}] \cap \cdots (\rho_{F_n}^L)^{-1}[\{\text{Id}_{F_n}\}].$$

Finalmente, nótese que

$$\sigma \in V \iff \forall i \quad \sigma|_{F_i} = \rho_{F_i}^L(\sigma) = \text{Id}_{F_i} \iff \sigma|_F = \text{Id}_F,$$

donde  $F := F_1 \vee F_2 \vee \cdots \vee F_n$ . Así concluimos que  $V = \text{Gal}(L/F)$ .

2. Sea  $F$  la clausura normal de  $K$  en  $L$ , entonces  $\text{Gal}(L/F)$  es un subgrupo abierto de  $\text{Gal}(L/k)$  por el inciso anterior. Para todo  $\sigma \in \text{Gal}(L/K)$ , nótese que  $U_\sigma := \mu_\sigma^{-1}[\text{Gal}(L/F)] \subseteq \text{Gal}(L/K)$  (¿por qué?) es abierto, pues la traslación  $\mu_\sigma^{-1}$  es un homeomorfismo, y claramente  $\sigma \in U_\sigma$ . Por lo tanto,

$$\text{Gal}(L/K) = \bigcup_{\sigma \in \text{Gal}(L/K)} U_\sigma \subseteq \text{Gal}(L/k)$$

es abierto.

Además, si  $\tau \notin \text{Gal}(L/K)$ , entonces  $U_\tau \cap \text{Gal}(L/K) = \emptyset$ , por lo que  $\text{Gal}(L/K)$  también es cerrado. Otra posible demostración es que basta notar que la topología subespacio de  $\text{Gal}(L/K)$  es la de Krull para ver que es compacto, y un subconjunto compacto de un espacio de Hausdorff es cerrado.

3. Veamos primero que las aplicaciones de evaluación son continuas. Sean  $\alpha, \beta \in L$  y sea  $U := \text{ev}_\alpha^{-1}[\{\beta\}]$ . Si es vacío, entonces es abierto; si no existe  $\sigma \in U$  y notamos que  $\tau \in U$  si y sólo si  $\tau(\alpha) = \sigma(\alpha)$  si y sólo si  $(\sigma^{-1} \circ \tau)(\alpha) = \alpha$ , o equivalentemente, si  $\tau \in \sigma \cdot \text{Gal}(L/k(\alpha))$ , donde el punto denota aplicar la traslación (izquierda en este caso).

Para ver que la topología de Krull es de hecho la inicial, basta probar que los entornos básicos  $\text{Gal}(L/F)$  del neutro  $\text{Id}_L$ , donde  $F \in \mathcal{F}_L$  están generados por abiertos de la topología inicial. Como  $F$  es finito, está generado por un conjunto finito  $\alpha_1, \dots, \alpha_n \in F$  (de hecho, con uno solo por el teorema del elemento primitivo), así que

$$\text{Gal}(L/F) = \text{ev}_{\alpha_1}^{-1}[\{\alpha_1\}] \cup \dots \cup \text{ev}_{\alpha_n}^{-1}[\{\alpha_n\}]. \quad \square$$

**Corolario 13.46.1:** Sea  $L/k$  una extensión de Galois. Se cumplen:

1. Para todo  $\sigma \in \text{Gal}(L/k)$ , la familia

$$V_K(\sigma) := \{\tau \in \text{Gal}(L/k) : \sigma|_F = \tau|_F\},$$

donde  $K$  recorre las subextensiones  $L/K/k$  finitas (no necesariamente Galois), es una base de entornos de  $\sigma$ .

2. Dado un subconjunto  $S \subseteq \text{Gal}(L/k)$ , su clausura viene dada por

$$\overline{S} = \{\sigma \in \text{Gal}(L/k) : \forall F \in \mathcal{F}_L \exists \tau \in S : \tau|_F = \sigma|_F\}.$$

DEMOSTRACIÓN:

1. Basta notar que es la traslación de la base de entornos  $\text{Gal}(L/K)$  del neutro  $\text{Id}_L$ .
2. Basta seguir lo siguiente

$$\begin{aligned} \overline{S} &= \{\sigma : \forall L/K/k \text{ finita } V_K(\sigma) \cap S \neq \emptyset\} \\ &= \{\sigma : \forall L/K/k \text{ finita } \exists \tau \in S : \tau|_K = \sigma|_K\} \\ &= \{\sigma : \forall F \in \mathcal{F}_L \exists \tau \in S : \tau|_F = \sigma|_F\} \end{aligned}$$

donde la última igualdad sale de que todo automorfismo sobre una extensión finita  $K/k$  se extiende a un automorfismo sobre una extensión finita de Galois  $F/k$ .  $\square$

**Proposición 13.47:** Sea  $L/k$  una extensión de Galois y sea  $F \in \mathcal{F}_L$ . Entonces la restricción  $\rho_F^L: \text{Gal}(L/k) \rightarrow \text{Gal}(F/k)$  es un epimorfismo de grupos y una identificación topológica (i.e.,  $\text{Gal}(F/k)$  es un espacio cociente de  $\text{Gal}(L/k)$  mediante  $\rho_F^L$ ).

DEMOSTRACIÓN: Que sea suprayectivo se sigue del lema 4.20 que dice que todo monomorfismo desde una extensión normal hasta otra admite una (¡no única!) extensión a un automorfismo. El que sea una identificación topológica equivale a verificar un subconjunto  $A \subseteq \text{Gal}(F/k)$  es abierto syss  $(\rho_F^L)^{-1}[A]$  es abierto y como todo  $A$  es abierto, basta verificar que  $\rho_F^L$  es continua.  $\square$

**Corolario 13.47.1:** Sea  $L/k$  una extensión de Galois y sea  $k \subseteq K \subseteq L$  una subextensión de Galois. Entonces  $\text{Gal}(L/K) \leq_c \text{Gal}(L/k)$  es un subgrupo cerrado.

DEMOSTRACIÓN: Basta notar que

$$\text{Gal}(L/K) = \bigcap_{\alpha \in K} \text{Gal}(L/k(\alpha)),$$

donde los últimos son cerrados por el lema.  $\square$

**Lema 13.48:** Sea  $L/k$  una extensión de Galois y sea  $G \leq_c \text{Gal}(L/k)$  un subgrupo cerrado. Entonces  $F(G) = k$  syss  $G = \text{Gal}(L/k)$ .

DEMOSTRACIÓN: La implicancia « $\Longleftarrow$ » es trivial, veamos « $\Longrightarrow$ »: Para cada  $F \in \mathcal{F}_L$  sea

$$H_F = \rho_F^L[G] = \{\sigma|_F : \sigma \in G\} \subseteq \text{Gal}(F/k).$$

Y por hipótesis,  $\text{Fix}(H_F) = \text{Fix}(G) \cap F = k$ , de modo que  $H_F = \text{Gal}(F/k)$ . Así hemos probado que cada  $\sigma \in \text{Gal}(L/k)$  satisface que

$$\forall F \in \mathcal{F}_L \quad \sigma|_F \in H_F \iff \forall F \in \mathcal{F}_L \exists \tau \in G : \sigma|_F = \tau|_F \iff \sigma \in \overline{G},$$

donde la última equivalencia viene del inciso 2 del corolario 13.46.1. Así probamos que  $G = \overline{G} = \text{Gal}(L/k)$ .  $\square$

**Teorema 13.49 – Teorema de Galois-Krull:** Sea  $L/k$  una extensión de Galois, entonces las siguientes aplicaciones

$$\{G \leq \text{Gal}(L/k) \text{ cerrado}\} \xrightleftharpoons[\text{Gal}(L/F)]{\text{Fix}(G)} \{k \subseteq K \subseteq L : K/k \text{ de Galois}\}$$

son la inversa la una de la otra y determinan anti-isomorfismos entre los

retículos de subgrupos cerrados (con inclusión) y el de las subextensiones de Galois (con inclusión).

DEMOSTRACIÓN: Nótese que, por los lemas anteriores, la aplicación  $F \mapsto \text{Gal}(L/F)$  está bien definida (i.e.,  $\text{Gal}(L/F)$  es un subgrupo cerrado) y es claro que  $G \mapsto \text{Fix}(G)$  es una subextensión de cuerpos, y es fácil verificar que es de Galois (¿por qué?).

Por otro lado, si  $G \leq_c \text{Gal}(L/k)$  es un subgrupo cerrado, entonces

$$G \subseteq \text{Gal}(L/\text{Fix}(G)) \subseteq \text{Gal}(L/k),$$

y aplicando el lema anterior con  $k = \text{Fix}(G)$ , notando que  $G$  es cerrado en  $\text{Gal}(L/\text{Fix}(G))$ , obtenemos que  $G = \text{Gal}(L/\text{Fix}(G))$ .

Recíprocamente, dada una subextensión  $L/K/k$  de Galois, entonces trivialmente

$$K \subseteq \text{Fix}(\text{Gal}(L/K)) \subseteq L,$$

y  $L/K$  es una extensión de Galois. Sea  $\alpha \in \text{Fix}(\text{Gal}(L/K))$ , entonces existe una subextensión  $L/F/K$  de Galois finita, tal que  $\alpha \in F$ . Por el lema 4.20, todo  $K$ -automorfismo de  $F$  es la restricción de un  $K$ -automorfismo de  $L$  y, como  $\alpha$  está fijo por todos los  $K$ -automorfismos de  $L$ , también lo está por todos los  $K$ -automorfismos de  $F$ , es decir

$$\alpha \in \text{Fix}(\text{Gal}(F/K)) = K. \quad \square$$

**Teorema 13.50 (Leptin):** Para todo grupo profinito  $G$  existe una extensión de cuerpos  $L/k$  de Galois tal que  $\text{Gal}(L/k) \cong G$ .

## 13.5 Cohomología de Galois

**Lema 13.51:** Sea  $G$  un grupo profinito y sea  $X$  un espacio topológico discreto con una acción  $\alpha: X \times G \rightarrow X$ . Son equivalentes:

1.  $\alpha: G \times X \rightarrow X$  es continuo.
2. Para todo  $x \in X$ , el estabilizador

$$\text{Stab}_x = \{g \in G : x^g = x\} \leq G$$

es un subgrupo abierto.

3.  $X = \bigcup_{U \leq_o G} X^U$ , donde

$$X^U := \text{Fix}_X(U) = \{x \in X : \forall u \in U \quad x^u = x\}.$$

**Definición 13.52:** Sea  $G$  un grupo profinito. Un  $G$ -**módulo (derecho) topológico** es un grupo abeliano topológico  $M$  con una acción derecha  $\alpha: G \rightarrow \text{Aut}_{\text{TopGrp}}(M)$  tal que la función inducida  $M \times G \rightarrow M$  es continua; denotaremos que  $\alpha: G \curvearrowright M$ . Un  $G$ -**módulo** (a secas) será un  $G$ -módulo derecho discreto, i.e., donde  $M$  sea un grupo abeliano dotado siempre de la topología discreta.

Dados un par de  $G$ -módulos topológicos  $(A, \alpha), (B, \beta)$ . Un **homomorfismo de  $G$ -módulos topológicos** es un homomorfismo continuo  $\varphi: A \rightarrow B$  tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} A \times G & \xrightarrow{f \times \text{Id}_G} & B \times G \\ \alpha \downarrow & & \downarrow \beta \\ A & \xrightarrow{f} & B \end{array}$$

**Lema 13.53.A:** Sea  $G$  un grupo profinito. Entonces la categoría  $\text{DMod}_G$  de  $G$ -módulos discretos es una categoría abeliana con suficientes injectivos.

**Lema 13.53.B:** Sea  $G$  un grupo profinito, el funtor  $(-)^G: \text{DMod}_G \rightarrow \text{DMod}_G$  es exacto por la izquierda.

**Definición 13.53:** Sea  $G$  un grupo profinito, y sea  $A$  un  $G$ -módulo (discreto). Se define el  $q$ -ésimo grupo de cohomología (continua)  $H_{\text{cont}}^q(G, A)$  como el  $q$ -ésimo funtor derivado derecho  $R^q(-)^G$  evaluado en  $A$ .

No obstante, la siguiente descripción será útil:

**Definición 13.54:** Sea  $\Gamma$  un grupo profinito y sea  $M$  un  $\Gamma$ -módulo. Denotamos por  $C^n(\Gamma, M)$  al conjunto de todos los homomorfismos continuos  $\Gamma^n \rightarrow M$  y por  $d: C^n(\Gamma, M) \rightarrow C^{n+1}(\Gamma, M)$  el homomorfismo de cofrontera definido para  $f \in C^n(\Gamma, M)$  por

$$\begin{aligned} (df)(g_1, \dots, g_{n+1}) &:= g_1 \cdot f(g_2, \dots, g_{n+1}) \\ &+ \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_n) + (-1)^{n+1} f(g_1, \dots, g_n). \end{aligned}$$

Así  $K^\bullet(\Gamma, M) := (C^n(\Gamma, M), d^n)$  es un complejo de cocadenas (¿por qué?) cuyos grupos de cohomología se denotan  $H_{\text{cont}}^q(\Gamma, M) := h^q(K^\bullet(\Gamma, M))$ .



**Situación 13.55:** Sea  $\{G_i\}_{i \in I}$  un sistema inverso de grupos profinitos (donde los vínculos son homomorfismos continuos). Sea  $G := \varprojlim_{i \in I} G_i$  el límite inverso, el cual es también un grupo profinito.

**Lema 13.56.A:** En situación 13.55, sea  $A$  un  $G$ -módulo discreto. Dada una función localmente constante  $f: G^q \rightarrow A$ , existe  $j \in I$  tal que para todo  $\mathbf{x} \in G^q$  el valor  $f(\mathbf{x})$  solo depende de  $p_j(\mathbf{x}) \in G_j^q$ .

DEMOSTRACIÓN: Como  $f$  es localmente constante y  $G^q$  es constante, existen abiertos  $V_1, \dots, V_r$  en  $G^q$  donde  $f$  es constante. Para cada  $V_\ell$  existe  $U_{j_\ell} \subseteq G_{j_\ell}^q$  tal que  $p_{j_\ell}^{-1}[U_{j_\ell}] = V_\ell$ , de modo que para un  $j$  suficientemente grande, existen abiertos  $U_1, \dots, U_r \subseteq G_j^q$  tales que  $p_j^{-1}[U_j] = V_j$ .  $\square$

**Lema 13.56.B:** En situación 13.55, sea  $A$  un  $G$ -módulo discreto. Para toda función localmente constante  $f: G^q \rightarrow A$ , existe  $j \in I$  y  $f_j: G_j^q \rightarrow A$  localmente constante tal que  $f = p_j \circ f_j$ .

**Proposición 13.56:** En situación 13.55, sea  $A_i$  un  $G_i$ -módulo discreto para cada  $i \in I$  (los cuales vemos de forma canónica como  $G$ -módulos) con vínculos compatibles. Para todo  $q \in \mathbb{Z}$  se cumple que

$$H_{\text{cont}}^q \left( G, \varinjlim_{i \in I} A_i \right) = \varinjlim_{i \in I} H_{\text{cont}}^q (G_i, A_i).$$

DEMOSTRACIÓN: Basta probar que los homomorfismos inducido

$$u_q: \varinjlim_{i \in I} K^q(G_i, A_i) \longrightarrow K^q(G, A)$$

es un isomorfismo.

- (a)  $u_q$  es inyectivo: Sea  $f_j: G_j^q \rightarrow A_j$  un homomorfismo localmente constante; por compacidad de  $G_j^q$ , se sigue que  $f_j$  toma finitos valores  $F \subseteq A_j$ . Supongamos que  $f_{i_0}$  induce el homomorfismo nulo en  $K^q(G, A)$ . Como  $F$  es finito, podemos suponer que, para un índice  $i_1$  mayor, el homomorfismo  $G^q \rightarrow A_{i_1}$  es nulo. Para todo  $j \geq i_1$ , sea  $E_j \subseteq G_j^q$  el conjunto de elementos  $\mathbf{x} \in G_j^q$  tales que su imagen a través de  $G_j^q \rightarrow A_i$  sea no nulo; como el conjunto de valores  $F$  es finito, entonces cada  $E_j$  es cerrado (y luego compacto). Así que los  $E_j$ 's forman un sistema inverso y  $\varprojlim_{j \geq i_1} E_j = \emptyset$ , por lo que algún  $E_j = \emptyset$ , como se quería probar.

- (b)  $u_q$  es sobreyectivo: Sea  $f: G^q \rightarrow A$  un homomorfismo localmente constante, de modo que toma solo finitos valores. Como  $A = \varinjlim_{i \in I} A_i$ , existe  $i_0 \in I$  tal que  $f$  se factoriza a través de  $A_{i_0} \rightarrow A$ . Por el lema anterior, sea  $j \geq i_0$  tal que  $g: G^q \rightarrow A_{i_0}$  se factoriza:

$$\begin{array}{ccccc} G^q & \xrightarrow{g} & A_{i_0} & \longrightarrow & A \\ & \searrow p_j & \nearrow \exists! & & \\ & & G_j^q & & \end{array}$$

lo que induce un homomorfismo localmente  $G_j^q \rightarrow A_j$  que induce  $f$ .  $\square$

Los siguientes corolarios son inmediatos:

**Corolario 13.56.1:** Sea  $G$  un grupo profinito y  $A$  un  $G$ -módulo discreto. Entonces

$$\forall q \geq 1, \quad H_{\text{cont}}^q(G, A) = \varinjlim_{U \trianglelefteq_o G} H^q(G/U, A^U).$$

**Corolario 13.56.2:** Sea  $G$  un grupo profinito y  $A$  un  $G$ -módulo discreto. Entonces para todo  $q \geq 1$ , el grupo abeliano  $H_{\text{cont}}^q(G, A)$  es de pura torsión.

DEMOSTRACIÓN: Basta notar que  $H^q(G/U, A^U)$  es de pura torsión, cuando  $U \trianglelefteq_o G$  es un subgrupo normal abierto.  $\square$

**Corolario 13.56.3:** Sea  $G$  un grupo profinito y  $A$  un  $G$ -módulo discreto. Entonces

$$\forall q \in \mathbb{N}, \quad H_{\text{cont}}^q(G, A) = \varinjlim_{B \leq A} H_{\text{cont}}^q(G, B),$$

donde  $B$  recorre los  $G$ -submódulos finitamente generados de  $A$ .

---

## *Índice alfabético*

---

- $p$ -subgrupo de Sylow, 445
- abelianización (grupo), 43
- acción, 27
  - fiel, 27
  - transitiva, 28
- álgebra, 313
  - alternativa, 341
  - anticonmutativa, 328
  - asociativa, 313
  - central, 349
  - conmutativa, 313
  - cuaterniónica, 353
  - de composición, 338
  - de tipo finito, 316
  - exterior, 329
  - graduada, 319
  - simétrica, 333
  - tensorial, 325
- algebraicamente dependientes
  - (elementos), 167
- algebraico (elemento, extensión), 125
- algoritmo
  - de Horner-Ruffini, 76
  - división polinómica, 74
- anillo, 51
  - artiniano, 186
  - de división, 52
  - de fracciones totales, 221
  - de Prüfer, 377
  - graduado, 320
  - hereditario, 374
  - local, 217
  - noetheriano, 58
  - ordenado, 53
  - semihereditario, 377
  - semisimple, 372
  - simple, 372
- asociado (ideal), 235
- asociatividad, 3
- automorfismo, 9
- autovalor, 279
- autovector, 279
- balanceada
  - (aplicación), 389
- base, 100
  - (álgebra), 316
  - canónica, 103

- cuaterniónica, 353
- de trascendencia, 169
- minimal, 232
- ortogonal, 285
- bilineal (función), 196
- bimódulo, 388
- cancelación, 5
- caracter, 439
- $c$ -duplicado (álgebra), 342
- centralizador, 18
- centro, 18
  - (álgebra), 349
- ciclo, 13
- círculo, 430
- clase lateral, 10
- clausura
  - algebraica, 150
  - normal, 137
  - real (cuerpo), 256
  - separable, 144
  - separable (cuerpo), 154
- cociente
  - de Herbrand, 425
- coeficiente
  - líder, 71
  - polinomio, 70
- complemento
  - ortogonal, 307
- congruentes
  - (matrices), 303
- cónica
  - asociada (a una álgebra), 357
- conjugado
  - (cuaternión), 353
- conjunto
  - dirigido, 440
  - libre, 100, 316
  - ligado, 100
- conmutador, 25
- conmutatividad, 3
- cono positivo, 254
- contexto
  - de Morita, 396
- coprimario (módulo), 238
- correstricción (homomorfismo), 423
- criterio
  - de Baer, 206
  - de irreducibilidad
    - de Eisenstein, 84
    - de Gauss, 82
- cuaternión, 353
  - puro, 353
- cuerpo, 52
  - algebraicamente cerrado, 150
  - de escisión, 134
  - de escisión (álgebra), 352
  - de fracciones, 69
  - de residuos, 217
  - formalmente real, 254
  - ordenado, 253
  - perfecto, 138
  - primo, 61
  - realmente cerrado, 256
  - separablemente cerrado, 154
- decomposable (submódulo), 240
- decomposición
  - irreducible, 240
  - primaria, 240
- descomposición
  - primaria, 240
    - minimal, 240
- desigualdad
  - de Bessel, 310
  - de Cauchy-Schwarz, 306
- determinante, 113
- diagonalizable, 281
- divisor

- de cero, 52
  - (módulo), 235
- impropio, 62
- dominio, 52
  - de factorización única (DFU), 63
  - de ideales principales (DIP), 54
  - euclídeo, 57
  - íntegro, 52
- duales (grupos topológicos), 439
- ecuación
  - de clases, 31
- elemento
  - irreducible, 62
  - neutro, 3
  - norma, 418
  - primo, 62
- endomorfismo, 9
  - de Frobenius, 139
  - nilpotente, 293
- entorno
  - simétrico, 431
- epimorfismo, 9
- equivalentes (extensiones), 378
- escalar, 95
- esencial (homomorfismo), 208
- espacio
  - de producto interno, 282
  - metabólico, 288
  - prehilbertiano, 305
  - vectorial, 95
- exacto
  - (functor), 185
  - por la derecha (functor), 184
  - por la izquierda (functor), 184
- extensión, 378
  - abeliana, 159
  - ciclotómica, 159
  - cíclica, 159
  - de cuerpos, 125
  - de Galois, 142
  - normal, 136
  - puramente inseparable, 138
  - puramente trascendente, 167
  - separable, 138
  - trascendente simple, 171
- fiel (módulo), 235
- finitamente presentado (módulo), 367
- forma
  - bilineal, 302
  - hermitiana, 305
  - multilineal, 111
  - sesquilineal, 304
- fórmula
  - de Grassman, 106
- fuertemente indecomponible (módulo), 193
- función
  - indicatriz de Euler, 11
  - lineal, 96
    - homogénea, 321
- functor
  - aditivo, 184
- $G$ -módulo, 415, 454
  - coinducido, 421
  - coinvariante, 416
  - de acción trivial, 415
  - inducido, 421
  - invariante, 415
  - relativamente inyectivo, 422
  - relativamente proyectivo, 422
  - topológico, 454
- grado
  - (álgebra de Azumaya), 352
  - de un polinomio, 71

- grande (submódulo), 208
- grupo, 4
  - abeliano, 4
  - libre, 275
  - autodual, 439
  - cíclico, 7
  - de Galois, 133
  - de torsión, 278
  - diedral, 16
  - divisible, 434
  - dual (topológico), 439
  - finitamente generado, 7
  - l.c.a., 439
  - libre, 38
  - multiplicativo de  $n$ , 11
  - pro- $\mathcal{C}$ , 443
  - simple, 35
  - soluble, 45
  - topológico, 429
    - discreto, 429
  - trivial, 4
- homomorfismo, 9
  - cruzado, 419
  - principal, 420
  - de augmentación, 416
  - de  $G$ -módulos, 454
  - de álgebras graduadas, 321
- ideal, 54
  - de augmentación, 416
  - fraccionario, 375
  - homogéneo, 320
  - impropio, 54
  - irrelevante, 320
  - maximal, 58, 64
  - primo, 64
  - principal, 54
  - traza, 392
- identidad
  - de Parseval, 311
- indecomponible (módulo), 192
- índice, 10
  - (subgrupo cerrado), 444
- invertible (ideal), 376
- invertible (elemento), 4, 52
- irredundante (descomposición), 240
- isomorfías (estructuras), 9
- isomorfismo, 9
- $k$ -conjugados (elementos), 133
- lema
  - de Cassels, 264
  - de descomposición ortogonal, 284
  - de Gauss, 81
  - de Nakayama, 231
  - de Schanuel, 368
  - de Zariski, 318
- ley
  - del paralelogramo, 307
- libre
  - de torsión (grupo), 278
- libre de torsión (módulo), 213, 402
- matriz
  - adjunta, 114
  - de Vandermonde, 115
  - hermitiana, 296
  - unitriangular, 120
- máximo
  - común divisor, 66
- menor
  - complemento, 114
- minimal (ideal), 189
- mínimo
  - común múltiplo, 66
- módulo, 95

- 
- artiniano, 186
  - de pura torsión, 213
  - divisible, 207
  - fielmente plano, 202
  - libre, 100
  - noetheriano, 186
  - plano, 202
  - proyectivo, 203
  - pura torsión, 402
  - monoide, 4
  - monomio, 70
  - monomorfismo, 9
  - Morita-equivalentes (anillos), 396
  - multiplicidad (raíz), 138
  - módulo
    - graduado, 321
    - plano, 391
  - nilpotente (elemento), 224
  - nilradical, 225
  - norma
    - (cuaterniónica), 353
    - (elemento de  $\mathbb{Z}[G]$ ), 418
    - euclídea, 57
  - normalizador, 18
  - núcleo, 9
  - número
    - complejo, 88
  - órbita, 13
  - orden
    - (grupo profinito), 444
  - ortogonales (vectores), 307
  - ortonormal, 307
  - $p$ -subgrupo, 32
    - de Sylow, 34
  - $p$ -complemento, 448
  - $\mathfrak{p}$ -componente primaria, 240
  - $p$ -grupo, 32
  - polinomio
    - característico, 117, 292
    - ciclotómico, 85, 160
    - de interpolación de Lagrange, 77
    - derivado, 137
    - minimal, 127
    - mónico, 71
    - primitivo, 80
  - precono positivo, 254
  - presentación
    - inyectiva, 383
    - plana, 399
    - proyectiva, 368, 379
  - primario (submódulo), 238
  - producto
    - directo, 25
    - interno, 282, 305
    - restringido, 434
    - semidirecto, 29
    - tensorial, 390
  - progenerador (módulo), 396
  - $\pi$ -subgrupo de Hall, 448
  - punto
    - fijo, 13
  - radical (ideal), 225
  - rango
    - (matriz), 119
  - raíz
    - $n$ -ésima, 127
    - cuadrada, 127
    - cúbica, 127
    - de un polinomio, 71
    - simple, 138
  - reducible (submódulo), 240
  - reducido (anillo), 225
  - reflexión, 286
  - regla
    - de Ruffini, 76
  - restricción (homomorfismo), 423

- se escinde
  - (álgebra de Azumaya), 349
- se escinde (sucesión), 363
- semigrupo, 4
- semisimple (anillo), 189
- semisimple (módulo), 187
- similares (matrices), 116, 281
- simple (módulo), 187
- sistema
  - generador, 97
  - inverso, 441
  - suprayectivo, 441
- sistema generador, 7
- soporte (módulo), 223
- subálgebra, 315
  - homogénea, 320
- subanillo, 54
- subespacio
  - $f$ -invariante, 291
- subgrupo, 5
  - derivado, 43
  - normal, 18
- submódulo
  - de torsión, 213
- submódulo, 97
  - de torsión, 402
  - impropio, 97
- sucesión
  - exacta, 21
  - corta, 363
- sueño del aprendiz, 61
- suma
  - ortogonal, 284
- sumando directo, 188
- supernatural (número), 444
- tensor, 199
  - puro, 199, 390
- teorema
  - chino del resto, 11, 68
  - de Akizuki, 246
  - de bases de Hilbert, 77
  - de Cartan-Eilenberg, 374
  - de Cauchy, 33
  - de Cayley, 13
  - de Cayley-Hamilton, 230, 299
  - de ceros de Hilbert, 319
  - de coeficientes universales, 404
  - de De Moivre, 89
  - de Eakin-Nagata, 245
  - de Eilenberg-Watts, 393
  - de estructura de módulos
    - sobre un DIP, 215
  - de extensión de Kronecker, 126
  - de Frobenius, 346
  - de Galois-Krull, 452
  - de Hurwitz, 345
  - de isomorfismos
    - (primero), 20
    - (segundo), 21
    - (tercero), 21
  - de Jordan-Hölder, 49
  - de Kaplansky, 374
  - de Krull, 78
  - de la correspondencia, 23
  - de Lagrange, 10
  - de Lüroth, 173
  - de Maschke, 190
  - de Pitágoras, 307
  - de Sylow
    - (cuarto), 36
    - (primero), 34
    - (segundo), 35
    - (tercero), 35
  - de Wedderburn (pequeño), 347
  - de Wedderburn-Artin, 350, 398



- 
- de Witt, 287
  - del binomio de Newton, 60
  - del elemento primitivo, 143
  - fundamental
    - de la teoría de Galois, 148
    - de los grupos abelianos, 26
    - del álgebra, 91
  - topología
    - de Krull, 449
  - transformación
    - lineal fraccionaria, 171
  - traslación, 429
  - trasposición, 13
  - uniformidad
    - derecha, 437
    - izquierda, 437, 438
  - vector, 95
    - unitario, 307
  - álgebra
    - de Azumaya, 349



---

## *Lista de tareas pendientes*

---

Probar que si un grupo no es cíclico y posee dos subgrupos de orden	
2, entonces . . . . .	262
Revisar bien el ejercicio. . . . .	286
Teoremas pendientes. . . . .	329
Probar caso característica = 2. . . . .	341
¿Por qué? GILLE y SZAMUELY [0, págs. 10-11]. . . . .	360
Ver [0, 168, Teo. 4.24]. . . . .	376
Añadir demostración [0, §3.6, pp. 106-109]. . . . .	388
Demostrar que cerrado * compacto = cerrado. . . . .	431