

Álgebra

José Cuevas Barrientos

16 de septiembre de 2022

Índice general

	INTRODUCCIÓN	VII
I	Álgebra Abstracta Elemental	1
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
	1.3.3 Acciones, ecuación de clases y p -grupos	28
	1.4 Teoremas de Sylow	31
	1.4.1 Acciones	31
	1.4.2 Teoremas de Sylow	32
	1.5 Otros tópicos de grupos	36
	1.5.1 Grupos libres y presentación	36
	1.5.2 Grupos resolubles	41
2	ANILLOS Y CUERPOS	49
	2.1 Definiciones elementales	49
	2.1.1 Teorema del binomio	57
	2.1.2 Característica	58
	2.2 Divisibilidad en anillos	59
	2.3 Polinomios	68

2.4	Divisibilidad de polinomios	78
2.4.1	Raíces básicas	85
2.5	Números complejos	85
2.5.1	El teorema fundamental del álgebra I	88
3	MÓDULOS Y VECTORES	91
3.1	Módulos	91
3.2	Módulos libres y bases	96
3.2.1	Finitamente generados	96
3.2.2	Espacios de dimensión infinita	99
3.2.3	Fórmulas con la dimensión	101
3.3	Matrices y transformaciones lineales	102
3.4	Determinante	107
3.4.1	Invariantes: traza y polinomio característico	112
3.4.2	Rango de matrices	114
II	Teoría de Anillos y Módulos	117
4	EXTENSIONES DE CUERPO	119
4.1	Extensiones algebraicas	119
4.2	Extensiones normales y separables	128
4.2.1	Cuerpos de escisión	128
4.2.2	Extensiones separables	131
4.3	Teoría y extensiones de Galois	134
4.4	Cuerpos algebraicamente cerrados	142
4.4.1	Aplicación: El teorema fundamental del álgebra II	146
4.5	Otras aplicaciones	147
4.5.1	Norma y traza	147
4.5.2	Raíces de la unidad y extensiones ciclotómicas	148
4.5.3	La insolubilidad de la quintica	154
4.6	Trascendencia	157
4.6.1	Grado de trascendencia	157
4.6.2	Teorema de Lüroth	161
5	MÓDULOS, OTRA VEZ	165
5.1	La categoría de módulos	165
5.2	Cadenas de submódulos	173
5.2.1	Módulos noetherianos y artinianos	173
5.2.2	Módulos (semi)simples y el teorema de Jordan-Hölder	174
5.3	Productos tensoriales	182
5.4	Módulos proyectivos e inyectivos	187
5.5	Módulos sobre DIPs	196
5.6	¿Por qué las cosas fallan?	199

6	INTRODUCCIÓN AL ÁLGEBRA CONMUTATIVA	203
6.1	Anillos locales y radicales	203
6.1.1	Localización	203
6.1.2	Radicales	209
6.1.3	Extensión y contracción de ideales	214
6.1.4	El lema de Nakayama y sus consecuencias	216
6.2	Descomposición primaria de anillos	221
6.3	Módulos noetherianos y artinianos, de nuevo	224
7	CUERPOS FORMALMENTE REALES Y CUADRADOS	233
7.1	Cuerpos formalmente reales	233
7.2	Teoremas de Pfister	242
7.2.1	Calculando el nivel	248
8	ÁLGEBRA LINEAL AVANZADA	251
8.1	Grupos abelianos libres, y de torsión	251
8.2	Formas canónicas	257
8.3	Formas bilineales	259
8.3.1	Módulos libres de forma bilineal	260
8.3.2	El teorema de Witt	264
8.3.3	El anillo de Witt	265
9	TEORÍA ESPECTRAL	269
9.1	Diagonalización	269
9.1.1	El teorema fundamental del álgebra II	274
9.1.2	Teorema de Cayley-Hamilton	276
9.2	Espacios duales	277
9.3	Formas bilineales	279
9.3.1	Formas bilineales	279
9.3.2	Formas sesquilineales, producto interno y “geometría euclídea”	282
9.3.3	Formas hermitianas y espacios de producto interno	283
9.3.4	Formas cuadráticas	289
10	ÁLGEBRAS	291
10.1	Definiciones elementales	291
10.1.1	Álgebras (asociativas) libres	294
10.2	Álgebras asociativas	296
10.2.1	Anillos, módulos y álgebras graduadas	296
10.2.2	Álgebra tensorial	298
10.2.3	Álgebras anticonmutativas	301
10.2.4	Álgebra exterior y determinantes	302
10.2.5	Representaciones	306

10.3	El problema de Hurwitz	307
10.3.1	El problema aritmético de Hurwitz	307
10.3.2	Álgebras de composición y su clasificación	311
11	ÁLGEBRA HOMOLÓGICA	319
11.1	Resumen de categorías	319
11.1.1	Las serpientes y sus amigos	326
11.2	Homologías y cohomologías	328
11.2.1	Aplicación: El lema de la serpiente	335
11.3	Extensiones y resoluciones	337
11.4	Hom y \otimes	338
III	Geometría Algebraica	341
12	TEORÍA DE VALUACIÓN	343
12.1	Dependencia íntegra	343
12.2	Valores absolutos y valuaciones	356
12.3	Dominios de valuación discreta y de Dedekind	362
13	COMPLECIONES Y TEORÍA DE LA DIMENSIÓN	369
13.1	Serie de potencias	369
13.2	Compleciones	372
13.3	Anillos y módulos graduados	376
13.4	Teoría de la dimensión	387
14	VARIEDADES ALGEBRAICAS	397
14.1	Variedades afines	398
14.2	Variedades proyectivas	405
14.3	Funciones polinómicas y regulares	410
14.4	Dimensión	414
	ÍNDICE DE NOTACIÓN	415
	BIBLIOGRAFÍA	421
	Álgebra abstracta	421
	Álgebra lineal	422
	Álgebra homológica	422
	Álgebra conmutativa	422
	Geometría algebraica	423
	Artículos	423
	Libros de autoría propia	424
	ÍNDICE ALFABÉTICO	425

Introducción

El álgebra es el estudio de las estructuras matemáticas, esto es, conjuntos dotados de relaciones y/u operaciones que satisfacen una serie de condiciones que lo dotan de una *forma*. Ésto tal vez en principio difiera con la imagen que uno pueda tener del álgebra, pero hay varias consideraciones que tener de esta sentencia, por ejemplo, las estructuras son bastante comunes, los conjuntos numéricos son el ejemplo más importante, de hecho, abren la puerta a una pregunta más fundamental: ¿qué es un número? El lector puede creer que esto es una pregunta trivial ya que conoce números como 1, 0, π o $\sqrt{2}$. ¿Y qué hay de \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 enfocararlo 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.

Parte I.

ÁLGEBRA ABSTRACTA
ELEMENTAL

1

Teoría de grupos

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

1.1 Estructuras algebraicas

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

Definición 1.1 – Grupos: Una función $\cdot : G^2 \rightarrow G$ 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.

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

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

Ejemplo. Son grupos:

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

Los cuatro primeros incisos son grupos abelianos.

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

1. Si posee elemento neutro es único.

Si es semigrupo:

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

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Si es grupo entonces:

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

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

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

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

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

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

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

Proposición 1.4 (Asociatividad generalizada): Si $g_1, \dots, g_n \in G$ 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 hace por inducción. □

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

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

1. Si para todo $a, b \in S$ existen $x, y \in S$ tales que $ax = b$ e $ya = b$, entonces S es un grupo.
2. Si es finito entonces es grupo syss posee cancelación por la izquierda y la derecha.

Definición 1.6 – Subgrupo: Sea G un grupo. Se dice que $S \subseteq G$ es subgrupo si $(S, \cdot \upharpoonright S^2)$ 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 (Criterio de subgrupos): $S \leq G$ si y sólo si S no es vacío y para todo $x, y \in S$ se cumple que $xy^{-1} \in S$.

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

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

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

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

Corolario 1.10: $S \leq G$ si y sólo si $\langle S \rangle = S$.

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

$$x = x_1 x_2 \cdots x_n$$

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

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

DEMOSTRACIÓN: Si son iguales, entonces el resultado está probado. De lo contrario, sin 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 1.13: Si $\{H_i : i \in I\}$ es una \subseteq -cadena¹ 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 1.14 – Potencias y generadores: Sea $x \in G$ y $n \in \mathbb{Z}$, entonces se le llama n -ésima potencia de x a:

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

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

Se dice que B es una base si genera a G , i.e., si $\langle B \rangle = G$. Un grupo G que posee una base finita se dice un *grupo finitamente generado*. Un grupo se dice *cíclico* si posee una base singular. Se define el orden de un elemento x , denotado por $\text{ord } x$, 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 1.15: 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 $\text{ord } x = |\langle x \rangle|$.

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

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

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

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

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

Proposición 1.16: 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 1.17: Si $a, b \in G$ conmutan, entonces

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

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

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

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

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

DEMOSTRACIÓN: La demostración aplica el lema de Zorn. Sea $S \subsetneq G$ 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

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

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

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

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

Definición 1.20 – Morfismos: 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 $G \cong H$. Cuando queramos decir que un morfismo es un mono- o epimorfismo diremos que es mónico o épico resp.

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

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

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

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

Ejemplo. • En todo grupo G , la identidad $x \mapsto x$ es un automorfismo.

• En todo grupo abeliano, la inversa $x \mapsto x^{-1}$ es un automorfismo.

• En $(\mathbb{Q}, +)$ se cumple que $f(x) = kx$ con $k \neq 0$ también es un automorfismo.

• En $(\mathbb{Z}, +)$ la función $f(x) = 2x$ es un endomorfismo mónico pero no épico, pues 1 no tendría preimagen.

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

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

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

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

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

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

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

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

1. $a \in aH$.
2. $aH = bH$ o $aH \cap bH = \emptyset$.
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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ahora veamos que f es inyectiva: Si

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

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

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

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

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

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

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

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

1.2 Ejemplos de grupos

§1.2.1 Grupos simétrico y alternante. Dados nuestros conocimientos en teoría de conjuntos debería de ser fácil probar que $(\text{Func}(S), \circ)$ 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 1.34: Se cumple:

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

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

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

DEMOSTRACIÓN: Vamos a definir $\varphi_a : G \rightarrow G$ 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 1.36 (Órbitas y ciclos): 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* si 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 $(5, 2, 3)$. **Ojo:** los ciclos están ordenados, no es lo mismo $(2, 3, 5)$ que $(5, 3, 2)$. Los ciclos de orden 2 se denominarán *trasposiciones*.

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

Teorema 1.37: Se cumplen:

1. El orden de los ciclos es el cardinal de su órbita no trivial.
2. La inversa de un ciclo $(a_1, a_2, \dots, a_{n-1}, a_n)$ 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 1.38: Si $\sigma \in S_n$ cumple que

$$\sigma = \prod_{i=1}^n \tau_{1,i} = \prod_{i=1}^m \tau_{2,i}$$

donde $\tau_{j,i}$ es una trasposición, entonces $n \equiv m \pmod{2}$.

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

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

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

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

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

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

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

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

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

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

Definición 1.39: Si una permutación σ 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 1.40: 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 1.41: El signo se conserva entre inversas y conjugados.

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

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

Proposición 1.42: Se cumple:

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

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

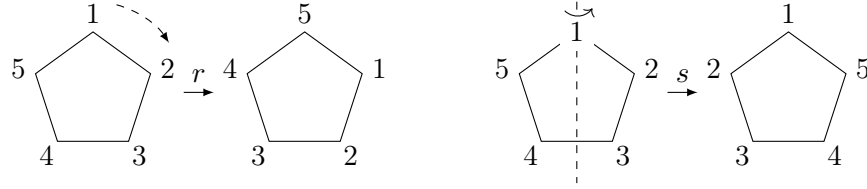


Figura 1.1. Ejemplo con un pentágono.

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

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

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

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

Proposición 1.44: Para todo grupo diedral se cumple:

1. En D_{2n} se cumple que $\text{ord } r = n$ y $\text{ord } s = 2$.
2. $rs = sr^{-1}$ y más generalmente $r^k s = sr^{-k}$. Esto equivale a que $sr s^{-1} = r^{-1}$ 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 1.45: Sea $N \leq G$. Entonces son equivalentes:

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

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

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

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

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

Teorema 1.48: Si $N \trianglelefteq G$, entonces la relación $x \sim y$ dada por $xN = yN$ determina una clase de equivalencia. Más aún, G/N posee estructura de grupo, la proyección sobre clases de equivalencia $\pi: G \rightarrow G/N$ 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 π es además homomorfismo de anillos, y es trivial que es suprayectivo. Finalmente sea $x \in \ker \pi$, vale decir, $xN = 1 \cdot N$, luego $x \in xN = N$; y es claro que si $x \in N$, entonces $x \in \ker \pi$. \square

Proposición 1.49: Un homomorfismo de grupos $\varphi: G \rightarrow H$ es inyectivo si y sólo 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 1.50: Se le llama *centralizador* $Z(S)$ de S al conjunto de todos los elementos que conmutan con todos los elementos de S , i.e.

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

al centralizador de todo G , se le dice el *centro*. Llamamos *normalizador* $N_G(S)$ 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 1.51: 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 1.52: Todo subgrupo de índice dos es normal.

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

Proposición 1.53: 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 1.54: Para $n \geq 3$ se cumple que $Z(S_n) = \langle 1 \rangle$ y que $Z(D_{2n}) = \langle 1 \rangle$ si n impar, y $Z(D_{2n}) = \langle r^{n/2} \rangle$ 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 1.55 – 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:

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

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

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

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

DEMOSTRACIÓN: Sea $\varphi : H \rightarrow HK/K$ 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 φ . Notemos que $1 \in \ker \varphi$ y $\varphi(1) = K$, asimismo, para todo $k \in K$ se cumple que $\varphi(k) = K$, luego $H \cap K \subseteq \ker \varphi$ y ya hemos visto que la otra implicancia también se da, luego por el primer teorema de isomorfismos se cumple el enunciado. \square

Teorema 1.58 – 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 1.59 (Sucesión exacta): Dada una sucesión de morfismos:

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

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

Proposición 1.60: 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

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

conmuta.

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

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

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

DEMOSTRACIÓN: Sea $f: H \times K \rightarrow HK$ 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 1.62: Si $H_1 \trianglelefteq G_1$ y $H_2 \trianglelefteq G_2$, entonces

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

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

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

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

DEMOSTRACIÓN:

1. (I) Φ es inyectiva: Sean $S_1 \neq S_2$ subgrupos de H . Entonces si $x \in \overline{S_2 \setminus S_1}$, e y es tal que $\varphi(y) = x$, de modo que $y \in \Phi(S_2)$, e $y \notin \Phi(S_1)$ pues si $y \in \Phi(S_1) = \varphi^{-1}[S_1]$, entonces $\varphi(y) \in S_1$, lo que es absurdo.
- (II) Φ es suprayectiva: Sea S tal que $\ker \varphi \leq S \leq G$. Luego $L := \overline{\varphi[S]} \leq H$, y $\Phi(L) \supseteq S$. Más aún, si $x \in \Phi(L)$, entonces $y = \varphi(x)$ con $y \in L$, ergo existe $z \in S$ tal que $y = \varphi(z)$. Luego

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

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

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

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

§1.3.2 Productos directos y semidirectos de grupos.

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

1. $HK \leq G$ si y sólo si $HK = KH$.
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 1.65 (Conmutador): Definamos el conmutador $[x, y] := x^{-1}y^{-1}xy$, que satisface que $xy = yx[x, y]$, luego $xy = yx$ syss $[x, y] = 1$.

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

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

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

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

Proposición 1.68: Sean G, H grupos, entonces:

1. $G \times H$ es también un grupo y las proyecciones $\pi_1(g, h) := g$ y $\pi_2(g, h) := h$ son homomorfismos de grupos.
2. Si K es un grupo y $\alpha: K \rightarrow G$ y $\beta: K \rightarrow H$ son homomorfismos de grupos, entonces la diagonal $\gamma := \alpha \Delta \beta: K \rightarrow G \times H$ 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.

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

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

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

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

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

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

En particular, se cumple para grupos abelianos finitos.

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

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

Finalmente agrupando todo nos da el enunciado. \square

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

Veamos dos aplicaciones de esto:

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

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

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

Proposición 1.74: Todo grupo de cardinal 6 es \mathbb{Z}_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 $\mathbb{Z}_2 \times \mathbb{Z}_3$ o \mathbb{Z}_6 , pero por el teorema chino del resto $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

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

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

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

es un grupo.

DEMOSTRACIÓN: Veamos que se cumplen las propiedades:

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

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

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

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

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

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

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

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

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

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

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

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

y así por inducción se deduce que $r^k = (k \bmod n, 0)$, 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

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

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

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

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

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

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

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

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

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

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

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

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

a los que llamamos órbita y estabilizador de a resp.

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

Ejemplos. Son acciones:

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

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

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

DEMOSTRACIÓN: Sean $x, y \in G$ y sea $z \in C_G(x) \cap C_G(y)$, luego, existen $g_1, g_2 \in G$ tales que $g_1^{-1}xg_1 = g_2^{-1}yg_2$, ergo $y = (g_1g_2^{-1})^{-1}x(g_1g_2^{-1})$ y por ende $C_G(y) \subseteq C_G(x)$. El caso converso es análogo y por doble inclusión se concluye que los conjuntos son iguales. \square

Teorema 1.83 – 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 1.84: Se dice que G es un p -grupo si posee de cardinal alguna potencia de p . También se dice que H es un p -subgrupo de G si $H \leq G$ y H es un p -grupo.

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

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

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

Corolario 1.87: Se cumplen:

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

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

1.4 Teoremas de Sylow

§1.4.1 Acciones.

Teorema 1.88: Si G actúa sobre S , entonces:

1. $\text{Stab}_a \leq G$.
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/Stab_a y 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 disjuntos entonces son iguales, para ello si $a, b \in S$ basta probar que $\text{Orb}_a \subseteq \text{Orb}_b$. 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 φ es una biyección. □

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

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

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

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

Teorema 1.91: 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 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 1.92: Si G , un p -grupo, actúa sobre S que no es de cardinal múltiplo de p , entonces S posee al menos un punto fijo global.

§1.4.2 Teoremas de Sylow. Los teoremas de Sylow son un conjunto de cuatro teoremas² 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\text{Fix}_Q(G/P)$ 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 1.99: G posee un único p -subgrupo de Sylow syss es éste es normal.

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

Ejemplo. Los grupos cíclicos de orden primo son simples.

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

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

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

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

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

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

Probaremos ahora, por contradicción, que P es el único punto fijo de su acción. Sea $Q \in \text{Syl}_p(G)$ 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 1.103 – 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

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

DEMOSTRACIÓN: Supongamos que se da aquello, luego consideremos la acción $\alpha : G \rightarrow \text{Sym}(\text{Syl}_p(G)) \cong S_{n_p}$ 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 1.105: No hay grupos de cardinalidad < 60 que sean simples y no-abelianos.

DEMOSTRACIÓN: En primer lugar todo grupo de cardinalidad p, pq con p, q primos distintos es abeliano. Si su cardinalidad es p^n , entonces su centro es siempre 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 K 2-subgrupo de Sylow, nótese que no posee elementos de orden 7 (pues sus elementos sólo pueden tener orden $\{1, 2, 4, 8\}$) y posee 8 elementos dando 56. Pero como hay más de un 2-subgrupo de Sylow, entonces existe $g \notin K$ de orden no 7, es decir, el grupo tiene al menos 57 elementos, lo cuál es imposible. \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 1.106: 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:

$$\text{Hom}(G, H) \approx \text{Func}(X, H), \quad (1.1)$$

donde \approx significa equipotencia de conjuntos.

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

DEMOSTRACIÓN: Definimos $\bar{S} := S \times \{+1, -1\}$ donde $()^{-1}: \bar{S} \rightarrow \bar{S}$ 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 $w := xxyx^{-1}y^{-1}yx^{-1}$, o formalmente una tupla ordenada finita de \bar{S} , donde su longitud viene dada por la de tupla ordenada, denotada $|w|$. El gran problema es que las palabras no reducidas pueden tener partes redundantes pues en el ejemplo anterior:

$$xxyx^{-1}y^{-1}yx^{-1} = xxyx^{-1}x^{-1}$$

Así, definimos una reducción elemental³ $R_e: \bar{S}^{<\omega} \rightarrow \bar{S}^{<\omega}$ 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 concideramos 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.

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

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

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

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

Luego se cumple que

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

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

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

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

\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.

\implies . 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 $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. \square

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

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

DEMOSTRACIÓN:

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

Una aplicación de los grupos libres como tal son las demostraciones de la paradoja de Banach-Tarski (véase [42, §A.1.2.]).

Teorema 1.111: 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 1.112: Sea $R \subseteq F(X)$, entonces R se dice un conjunto de *relaciones* sobre X . Se dice que un generador Y de un grupo G *satisface* las relaciones R si existe una aplicación $f: X \rightarrow Y$ 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 1.113 (von Dyck): Sea $G = \langle X : R \rangle$ y sea H un grupo con un generador que satisface las relaciones R , luego existe un epimorfismo $f: G \rightarrow H$.

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

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

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

§1.5.2 Grupos resolubles.

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

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

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 1.115: Se cumplen:

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

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

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

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

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

Proposición 1.117: Se cumplen:

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

DEMOSTRACIÓN: Probaremos la 2: \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 $G' \leq N$.

\impliedby . 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 1.118: Si G es finito, entonces son equivalentes:

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

DEMOSTRACIÓN: Es claro que (1) \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 1.119 – Grupo resoluble: Un grupo es resoluble si cumple las condiciones del lema anterior.

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

Teorema 1.121: Se cumple:

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

DEMOSTRACIÓN:

1. Sea $G \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$ 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

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

es una serie abeliana pues

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

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

3. Si N es resoluble, 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 resoluble y $HK/H \cong K/(H \cap K)$ es resoluble por ser cociente de K que es resoluble. \square

Definición 1.122: 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 1.123 (de Zassenhaus o de la mariposa): Sean $A \leq A^*$ y $B \leq B^*$ tales que A^*, B^* son subgrupos de G . Entonces:

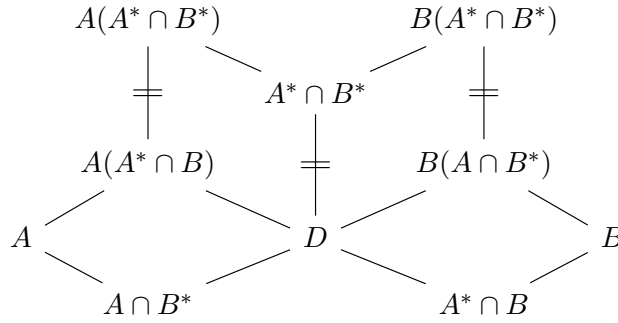
1. $A(A^* \cap B) \leq A(A^* \cap B^*)$.
2. $B(B^* \cap A) \leq B(B^* \cap A^*)$.
3. $\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}$.

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:⁴



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

Definición 1.124: 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 1.125 (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:

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

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

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

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

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

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

De lo que se concluye que ambos refinamientos son equivalentes. \square

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

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

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

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

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

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

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

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

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

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

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

DEMOSTRACIÓN:

- i) A_5 es simple: Si $\{1\} \neq N \trianglelefteq A_5$, entonces un elemento no neutro de N es de la forma (a, b, c) , $(a, b)(c, d)$ o (a, b, c, d, e) .

En el primer caso el lema prueba que $N = A_5$.

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

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

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

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

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

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

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

Corolario 1.130: Si $n \geq 5$, entonces A_n no es 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 1.131: A_5 es el primer (en cardinalidad) grupo simple no abeliano y grupo no soluble.

DEMOSTRACIÓN: Ya vimos que A_5 es simple, y ver que todo grupo de cardinalidad menor no puede ser simple y no-abeliano quedó 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 [1] definen anillo con neutro multiplicativo y «anillo» (en inglés, *rng*), sin 1 , 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 divisor izquierdo e y derecho. A se dice un *dominio íntegro* si es un dominio sin divisores de cero.

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

Teorema 2.2: En todo anillo se cumple:

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

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

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

Corolario 2.4: Todo cuerpo es un dominio íntegro.

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

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

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

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

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

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

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

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

Definición 2.8 – Subanillo, ideal: Se dice que $\emptyset \neq B \subseteq A$ 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 2.9: Si $1 \in B \leq A$ (como anillo), entonces $B^\times \leq A^\times$ (como grupos).

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

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

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

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

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

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

Ejemplo. \mathbb{Z} es un DIP.

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

DEMOSTRACIÓN: Sean $x, y \in S$, luego $x \in S_x \in \mathcal{F}$ e $y \in S_y \in \mathcal{F}$, 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 2.14: 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 2.15: Todo ideal \mathfrak{a} de un anillo unitario A es propio syss no contiene elementos invertibles.

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

Definición 2.17 – Morfismos: Una aplicación $\varphi: A \rightarrow B$ 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 2.18: 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 2.19: Si $\varphi: A \rightarrow B$ es un homomorfismo de anillos. Entonces:

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

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

Lema 2.20: Dado $\mathfrak{a} \leq A$ 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 2.21: Dado $\mathfrak{a} \leq A$ propio, entonces $(A/\mathfrak{a}, +, \cdot)$ es también un anillo.

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

Teorema 2.23 – 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 2.24: Si $\varphi : A \rightarrow B$ es morfismo, entonces:

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

Definición 2.25 – Dominio euclídeo: Sea A un dominio íntegro ordenado es un *dominio euclídeo* syss existe una función $d : A_{\neq 0} \rightarrow \mathbb{N}$, 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 2.26: Todo dominio euclídeo es un DIP.

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

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

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

- (1) Todo ideal de A está finitamente generado.
- (2) Para toda cadena ascendente de ideales de A

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

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

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

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

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

(3) \implies (1). Si el ideal \mathfrak{a} de A no fuese finitamente generado, podríamos considerar $a_0 \in \mathfrak{a}$ 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 2.28 – Anillo noetheriano: Un dominio íntegro es un *anillo noetheriano* si cumple con las condiciones del teorema 2.27.

Corolario 2.29: Todo DIP es noetheriano.

¹Véase [40, Def. 2.3]

§2.1.1 Teorema del binomio.

Definición 2.30: Dado n natural se define por recursividad:

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

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

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

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

Proposición 2.31: Se cumple:

1.

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

2.

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

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

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

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

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

Lo que completa la demostración. \square

§2.1.2 Característica.

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

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

Definición 2.34: 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 φ es el morfismo del lema anterior.

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

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

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

Teorema 2.37: 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 Fld_0 y \mathbb{F}_p el de Fld_p .

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

Teorema 2.39 (Sueño del aprendiz): Si $\text{car } \mathbb{k} = p \neq 0$, 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 2.40 – Divisibilidad: Sea A un dominio con $a, b \in A$. Escribimos $a \mid b$ cuando existe $q \in A$ tal que $b = aq$. Si dos elementos cumplen que $a \mid b$ y $b \mid a$, diremos que son *asociados*.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Si no se comprende la unicidad, déjeme aclarárselo con un ejemplo. El número 6 puede descomponerse en factores 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 2.44: En un DFU un elemento es primo si y sólo si es irreducible.

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

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

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

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

Luego, el conjunto $I = \{a : \exists n \in \mathbb{N} \ x_n \mid a\}$ es un ideal y veremos que no puede ser finitamente generado. Para ello, consideremos que los elementos y_0, \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 σ 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 2.46: Sea A un anillo. Diremos que un ideal \mathfrak{p} en A es *primo* syss $\mathfrak{p} \neq A$ y si para todo $ab \in \mathfrak{p}$ se cumple que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

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

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

DEMOSTRACIÓN: \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 2.48: 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 2.49: 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.

\impliedby . Es análogo. \square

Teorema 2.50: 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 2.16 es un cuerpo.

\impliedby . Es análogo. \square

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

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

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

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

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

Teorema 2.53: Todo DIP es un DFU.

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

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

Teorema 2.55 (Identidad de Bézout): Sea A un DIP con $a_0, \dots, a_n \in A$; 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 2.56: Si $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$, entonces se denota

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

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

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

Proposición 2.58: Se cumplen:

1. Sean $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ 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

Teorema 2.59 – 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. φ es suprayectiva syss $\mathfrak{a}_i + \mathfrak{a}_j = A$ para todo $i \neq j$.
3. φ es inyectiva syss $\bigcap_{i=1}^n \mathfrak{a}_i = (0)$.

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

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

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 2.60: Si A es un dominio y $\mathfrak{a}_1, \dots, \mathfrak{a}_n \trianglelefteq A$, entonces el homomorfismo φ 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 2.61: Todo dominio íntegro A está contenido en un cuerpo k , tal que si $\varphi: A \hookrightarrow K$ con K cuerpo, entonces existe un único homomorfismo $\bar{\varphi}: k \hookrightarrow K$. Es decir, se satisface el siguiente diagrama:

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

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, veámoslo:

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

Definición 2.63: Por el corolario anterior se denota por $\text{Frac}(A)$ 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 ϵ_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 2.64 – 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 director* o *líder*. Si el coeficiente director es 1, se dice que el polinomio es *mónico*.

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

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

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

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

mediante sus representaciones, por ejemplo

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

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

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

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

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

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

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

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

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

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

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

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

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

DEMOSTRACIÓN: Notemos que como a_n, b_m son no nulos y no divisores de cero, se da $\sum_{i+j=n+m} a_i b_j = a_n b_m \neq 0$, pues para todo $i > n$ y $j > m$ ocurre $a_i = b_j = 0$, es decir, $\deg(fg) \leq \deg f + \deg g$, por tricotomía, $\deg(fg) = \deg f + \deg g$. \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 2.67: Si A es un dominio íntegro y S un conjunto de indeterminadas, entonces $A[S]^\times = A^\times$.

DEMOSTRACIÓN: Por el teorema 2.66 vemos que multiplicar polinomios sólo incrementa el grado de éste, por ende, el polinomio debe ser constante para ser invertible, luego, debe ser una unidad de A . \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 2.68: 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 2.69 – Algoritmo de división polinómica: Sea A un anillo con $\alpha \in A[x]$ un polinomio no nulo cuyo coeficiente director es una unidad de A y $\beta \in A[x]$ cualquiera. Existen unos únicos polinomios $q, r \in A[x]$ tales que

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

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

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

Caso m : Consideremos que $\beta(x) = b_0 + \cdots + b_mx^m$ 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 α 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 2.70: Si A es un cuerpo, entonces $A[x]$ es un dominio euclídeo cuya norma es el grado.

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

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

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

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

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

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

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

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

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

entonces se cumple que

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

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

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

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

Podemos ver que es correcto, pues

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

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

Figura 2.1. Aplicación del algoritmo de Horner-Ruffini.

Teorema 2.76 – 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^a

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

^aEn 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 2.73. \square

Teorema 2.77 – 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. 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 ≥ 1), pero no es finitamente generado.

Veamos una aplicación de los anillos de polinomios:

Teorema 2.78: Son equivalentes:

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

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

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

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

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

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

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

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

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

Consideremos $R \cdot U^{-1} \leq \text{Frac}(R)$, 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 λ tal que $c := p + \lambda q$ es una combinación lineal conservativa. Como c es combinación de elementos en \mathfrak{a} , entonces $c \in \mathfrak{a} \subseteq (D)$, donde D es alguna dispersión. Luego todos los monomios de c están en (D) , y por consecuente $m, q \in (D)$; además $q + \mu m \in D$ para todo $\mu \in R$. En consecuente $\mathfrak{a} \subseteq \mathfrak{a} + Rm \subseteq T$ y como $\mathfrak{a} + Rm$ es un ideal propio, entonces $\mathfrak{a} = \mathfrak{a} + Rm$ y $m \in \mathfrak{a}$; es decir, alguna indeterminada de m está en \mathfrak{a} y luego en K . Finalmente $m \in (K)$ y como aplica para todo monomio de p , entonces $p \in (K)$ como se quería probar.

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

2.4 Divisibilidad de polinomios

Definición 2.79 (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 2.80 – 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 2.81: Si $p(x) \in \mathbb{Q}[x]$ es mónico, entonces sus raíces (si las tiene) son enteras.

Lema 2.82 (de primitividad de Gauss): Sea A un DFU con $f, g \in A[x]$ primitivos, entonces $f \cdot g$ es primitivo.

DEMOSTRACIÓN: Sean $f(x) = a_0 + a_1x + \cdots + a_nx^n$ 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

$$p \mid c_{u+v} - a_ub_v = \sum_{i=0}^{u-1} b_i c_{u+v-i} + \sum_{i=0}^{v-1} b_{u+v-i} c_i$$

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

Teorema 2.83: Sean $f, g \in A[x]$ y $k \in A$, entonces

1. $c(kf) = (k)c(f)$.
2. $c(fg) = c(f)c(g)$.

DEMOSTRACIÓN:

1. Por propiedades del mcd.
2. Consideremos que $c(f) = a$, $c(g) = b$; por lo que $f = af^*$, $g = bg^*$ con f^*, g^* primitivas. Entonces $c(fg) = c((ab)f^*g^*) = (ab)c(f^*g^*)$. Pero por lema de primitividad de Gauss, f^*g^* es primitiva, por ende el teorema. \square

Lema 2.84: Sea A un DFU con K su cuerpo de cocientes y $f, g \in A[x]$ polinomios primitivos no-constantes. f y g son asociados en $K[x]$ syss lo son en $A[x]$.

DEMOSTRACIÓN: Si lo son, entonces existen $a, b \in A$ no-nulos tales que $f = (a/b)g$, es decir, $af = bg$. Observe que

$$(a) = (a)c(f) = c(af) = c(bg) = (b)c(g) = (b),$$

por lo que a, b son asociados y existe una unidad $u \in A$ tal que $b = au$. Con esto $af = bg = aug$, por cancelación, nos queda que, efectivamente, f, g son asociados en $A[x]$. \square

Teorema 2.85: 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 2.86 – 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 2.87: 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 2.88: 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 2.89: Sea A un DFU, $k = \text{Frac}(A)$ y $f(x) \in k[x]$ no nulo. Entonces existe $c(f) \in k$ tal que $f = c(f)f^*$ con $f^* \in A[x]$ primitivo. Más aún, si existiera otro $q \in k$ tal que $f/q \in A[x]$ es primitivo, entonces existe $u \in A^\times$ tal que $q = uc(f)$.

DEMOSTRACIÓN: Denotemos

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

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 2.90: 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 2.91: Si A es un DFU y S es un conjunto arbitrario (posiblemente infinito) de indeterminadas, entonces $A[S]$ es un DFU.

DEMOSTRACIÓN: Veamos primero el caso finito, el cual, por inducción, se reduce a ver que $A[x]$ es un DFU: Sea $p(x) \in A[x]$ un polinomio que no es inversible ni nulo, luego $p(x) = cq(x)$, de modo que $q(x)$ es primitivo. Como A es un DFU, c admite descomposición única, así que toda descomposición de $p(x)$ sólo depende de $q(x)$. Asumamos que $q(x)$ posee dos factorizaciones

$$q(x) = q_1(x) \cdots q_n(x) = r_1(x) \cdots r_m(x)$$

en irreducibles. Luego, dichas factorizaciones en irreducibles lo son en $K[x]$ por el criterio anterior, donde $K := \text{Frac}(A)$; pero $K[x]$ es un DFU, luego las factorizaciones son equivalentes en $K[x]$ y claramente también lo son en $A[x]$.

Para el caso infinito basta notar que si un polinomio posee dos factorizaciones, éstas yacen en un anillo de polinomios de finitas indeterminadas, luego son equivalentes. \square

Teorema 2.92 – Criterio de Irreducibilidad de Eisenstein: Sean A un DFU, $K := \text{Frac}(A)$ y $f = \sum_{i=0}^n a_i x^i \in A[x]$ no-constante. Sea $p \in A$ un primo, luego f es irreducible en K si:

1. $p \nmid a_n$.
2. $p \mid a_i$ para $i = 0, 1, \dots, n-1$.
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 2.93: Sea A un dominio con $a \in A$ invertible y $b \in A$ cualquiera, entonces $p(x)$ es irreducible si y sólo si $p(ax + b)$ 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 1 (polinomios ciclotómicos): Para todo p primo, llamamos polinomio ciclotómico p -ésimo a

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = 1 + x + \cdots + x^{p-1},$$

veamos que son 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 $p \mid \binom{p}{n}$.

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 2.94 (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 $p(1) \equiv 1 \pmod{2}$, así que efectivamente es irreducible en \mathbb{F}_2 ; luego es irreducible en $\mathbb{Z}[x]$ por el criterio por reducción.

Ejemplo 2: Consideremos el polinomio $p(x) := x^4 + 1 \in \mathbb{Z}[x]$. En primer lugar, nótese que

$$(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

de modo que por el criterio de Eisenstein (con $p = 2$) se concluye que es irreducible en $\mathbb{Z}[x]$.

Ahora procedemos a probar que $p(x)$ es reducible en todo $\mathbb{F}_p[x]$ por casos:

(a) Si $-1 = a^2$ (incluye a $p = 2$): Entonces

$$x^4 + 1 = x^4 - a^2 = (x^2 - a)(x^2 + a).$$

(b) Si $p \neq 2$ y $2 = b^2$: Entonces

$$x^4 + 1 = (x^2 + 1)^2 - (bx)^2 = (x^2 + 1 - bx)(x^2 + 1 + bx).$$

- (c) En otro caso: Si -1 y 2 no son cuadrados, como \mathbb{F}_p^\times es cíclico, se concluye que -2 ha de ser un cuadrado. En particular $-2 = c^2$ y:

$$x^4 + 1 = (x^2 + 1)^2 - (cx)^2 = (x^2 + 1 - cx)(x^2 + 1 + cx).$$

Corolario 2.95: Sea A un DFU, $K := \text{Frac}(A)$ 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 2.96: Dado $\alpha \in \mathbb{k}$, decimos que β es una n -ésima raíz de α si $\beta^n = \alpha$ o alternativamente si β es raíz del polinomio $x^n - \alpha$.

Lema 2.97: Si β es una raíz cuadrada de α , entonces $-\beta$ y β son todas las raíces cuadradas de α .

Teorema 2.98 (Fórmula cuadrática): Si $p(x) = x^2 + rx + s$, entonces llamamos definimos $\Delta := r^2 - 4s$ como el *discriminante* de $p(x)$. Finalmente p tiene raíces syss existe α raíz cuadrada de Δ , en cuyo caso las raíces de p son

$$\frac{-r + \alpha}{2}, \quad \frac{-r - \alpha}{2}.$$

DEMOSTRACIÓN: Es fácil comprobar que éste es el caso, pero la deducción viene de que si

$$\begin{aligned} x^2 + rx + s = 0 &\iff x^2 + 2x \cdot \frac{r}{2} = -s \\ &\iff x^2 + 2x \cdot \frac{r}{2} + \frac{r^2}{4} = \left(x - \frac{r}{2}\right)^2 = \frac{r^2}{4} - s = \frac{\Delta}{4} \end{aligned}$$

Luego si α es raíz de Δ , entonces $\pm\alpha/2 = x - r/2$ y así se deduce el enunciado. \square

Corolario 2.99: 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 2.100 – Números complejos: Se define \mathbb{C} como el conjunto \mathbb{R}^2 con las operaciones:

$$(a, b) + (c, d) := (a + c, b + d), \quad (a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

Usualmente denotamos $(a, b) = a + ib$. 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 *módulo*^a de z y a \bar{z} el *conjugado* de z .

^aAlgunos textos prefieren usar $\| \|$ para los complejos y dejar $| |$ para los reales. Mi convenio es usar $\| \|$ para sus espacios vectoriales.

Proposición 2.101: Para todo $z, w \in \mathbb{C}$ se cumple:

1. $|z| = 0$ syss $z = 0$.
2. $\overline{\bar{z}} = z$.
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, $\bar{}$ 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 2.102: $(\mathbb{C}, +, \cdot)$ es un cuerpo.

DEMOSTRACIÓN: Lo único que no es obvio es que la existencia de los inversos multiplicativos, lo cual se consigue notando que si $z \in \mathbb{C}_{\neq 0}$, entonces $z^{-1} = \bar{z}/|z|^2$ mediante las propiedades anteriores. \square

Teorema 2.103: La aplicación $x \mapsto (x, 0)$ es un monomorfismo de cuerpos. Esto se interpreta como que \mathbb{C} contiene un subcuerpo isomorfo a \mathbb{R} .

Proposición 2.104: Todo complejo tiene raíz cuadrada. En consecuencia, todo polinomio cuadrático es reductible en los complejos.

Proposición 2.105: Si $P, Q \in \mathbb{C}[x]$, entonces:

1. Para todo $z \in \mathbb{C}$ que $\overline{P(z)} = P(\bar{z})$.
2. $P \in \mathbb{R}[x]$ si y sólo si $P(z) = \overline{P(z)}$.
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 2.106: 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 2.107: Si $z \in \mathbb{C}_{\neq 0}$, entonces $z = |z| \text{cis}(\arg z)$.

Teorema 2.108 – 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

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

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 2.109: Todo $z \in \mathbb{C}$ tiene una raíz n -ésima compleja, dada por

$$|z|^{1/n} \operatorname{cis} \left(\frac{\arg z}{n} \right).$$

Definición 2.110: Sea $n > 1$, entonces se le llaman *raíces n -ésimas de la unidad* a los $z \in \mathbb{C}$ tales que $z^n = 1$. Se denota también

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

de modo que todas las raíces n -ésimas de la unidad son simplemente las potencias de ζ_n .

§2.5.1 El teorema fundamental del álgebra I. Usando un poco de cálculo diferencial de una variable se otorga una demostración al teorema fundamental del álgebra.

Lema 2.111: Si $f \in \mathbb{C}[x]$ es no constante, entonces $|f(z)| \rightarrow \infty$ 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 2.112: Para todo $f \in \mathbb{C}[x]$ no constante, existe x_0 que minimiza $|f(x_0)|$.

DEMOSTRACIÓN: Sea $R := |f(0)| + 1$, por el lema anterior existe r tal que para todo $|z| \leq r$ se cumple que $|f(z)| \leq R$. Luego como la imagen continua de compactos es compacta, entonces $|f|$ alcanza su mínimo en $\overline{B}_r(0)$, que es mínimo en todo el dominio. \square

Teorema 2.113 – Teorema fundamental del álgebra: Todo polinomio no constante en \mathbb{C} tiene al menos una raíz.

DEMOSTRACIÓN: Por el lema anterior todo polinomio alcanza su mínimo en módulo, así que probaremos que ese mínimo no puede ser no nulo. Sea $f \in \mathbb{C}[x]$ y x_0 el punto que le minimiza a un valor no nulo. Reemplazando $g(x) := f(x_0 + x)/|f(x_0)|$ se obtiene que $g(0) = 1$, basta probar que el mínimo de g no es 1. Sea k el mínimo natural no nulo tal que g posee un término no nulo con z^k , es decir, que g es de la forma

$$g(z) = 1 + az^k + \cdots,$$

luego, si α es una k -ésima raíz de a , entonces

$$g(\alpha z) = 1 - z^k + z^{k+1}h(z)$$

donde $h \in \mathbb{C}[x]$.

Por desigualdad triangular

$$|g(\alpha z)| \leq |1 - z^k| + |z|^{k+1}|h(z)|,$$

luego si x es un real tal que $x \in [0, 1)$, entonces

$$|g(\alpha x)| \leq 1 - x^k(1 - x|h(x)|)$$

por lo que, por límites existe un $x_1 \in (0, 1)$ tal que $x_1|h(x_1)| < 1$, por ende, $|g(\alpha x_1)| < 1$ contradiciendo la minimalidad de $g(0) = 1$. \square

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: 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 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 « $(G, +)$ » es un grupo abeliano de neutro « $\vec{0}$ » y nótese que ya hemos probado en el primer capítulo que todos los axiomas son ciertos; ésto es lo que motiva el uso de «notación aditiva» al tratarse de grupos abelianos.

Definición 3.3 – Morfismos de módulos: Una aplicación $f: M \rightarrow N$ 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 3.4: 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 3.5: Dados X, Y no vacíos se cumple que $\text{Func}(X; A) \cong \text{Func}(Y; A)$ syss $|X| = |Y|$. Luego, dado un cardinal κ denotamos A^κ a un A -módulo $\text{Func}(S; A)$ genérico¹ con $|S| = \kappa$.

Definición 3.6 – Submódulo: Dado M un A -módulo, se dice que N es submódulo de M (denotado $N \leq M$) si N es también un A -módulo. Trivialmente, M y $\{\vec{0}\}$ son submódulos de M y se dicen *impropios*. Un submódulo se dice *simple* (o *irreducible*) si no admite submódulos propios.

Teorema 3.7 (Criterio del submódulo): N es submódulo del A -módulo M syss N es no vacío y para todo $u, v \in N$ y todo $\lambda \in A$ se cumpla que $\lambda u + v \in N$.

Lema 3.8: La intersección de submódulos es un submódulo.

Definición 3.9: Si $S \subseteq M$ donde M es un A -módulo, se le llama *submódulo generado por S* a

$$\langle S \rangle := \bigcap \{N : S \subseteq N \leq M\}.$$

Se dice que S es un *sistema generador* de M si $\langle S \rangle = M$.

¹En particular consideramos la representación ordinal-conjuntista de κ .

Proposición 3.10: 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 3.11: 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 3.12 – 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 3.13 (Suma de submódulos): Si $\{N_i\}_{i \in I}$ son submódulos de M , entonces se define su suma como

$$\sum_{i \in I} N_i := \left\langle \bigcup_{i \in I} N_i \right\rangle,$$

en particular $S + T := \langle S \cup T \rangle$.

Se dice que una familia de submódulos $\{N_i\}_{i \in I}$ es *independiente* si para todo $i \in I$ se cumple que $N_i \cap \sum_{j \neq i} N_j = \{0\}$. La suma de una familia independiente de submódulos se dice *directa* y se denota como $\bigoplus_{i \in I} N_i$.

Teorema 3.14: Sea M un A -módulo y $\{N_i\}_{i \in I}$ una familia de submódulos tales que $M = \sum_{i \in I} N_i$, son equivalentes:

- a) $M = \bigoplus_{i \in I} N_i$.
- b) Si $\sum_{i \in I} \mathbf{m}_i = \vec{0}$ 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 3.15: Sea M un A -módulo con $X \subseteq M$. Diremos que X es *libre* o que sus elementos son *linealmente independientes* syss la ecuación

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

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 5: Es fácil notar que con la suma y producto normal \mathbb{Q} es un \mathbb{Z} -módulo, sin embargo, no es libre (¿por qué?).

§3.2.1 Finitamente generados.

Definición 3.16: Se dice que un A -módulo M es *finitamente generado* si posee un sistema generador finito. Otra manera de decir lo mismo, pero que será útil más adelante, es que existe alguna tupla $(\mathbf{x}_1, \dots, \mathbf{x}_n)$ 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. 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 3.17: Sea M un A -módulo, entonces $M \cong A^n$ syss posee una base de cardinal n .

DEMOSTRACIÓN: Notemos que si X es una base cualquiera de M , entonces

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

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 3.18: 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 3.19: 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 3.20: Todo sistema generador finito en un espacio vectorial contiene una base. En consecuencia, todo espacio vectorial finitamente generado es libre.

Teorema 3.21: Todo par de bases de un espacio vectorial finitamente generado posee el mismo cardinal.

DEMOSTRACIÓN: Sean $X := \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ 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 3.22: Todo conjunto libre en un espacio vectorial finitamente generado se puede extender a una base.

Definición 3.23 – 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: 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

$$e_1 := (1, 0), \quad e_2 := (0, 1).$$

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 s 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 (bases de Hamel). Si se asume el AE, \mathbb{R} como \mathbb{Q} -espacio vectorial tiene una base H , usualmente llamada *de Hamel*. Queda al lector probar que todas las bases de Hamel no son ni finitas ni numerables. No sólo es complejo, sino imposible construir manualmente una base de Hamel, puesto que se ha demostrado que la existencia de esta base es independiente a la teoría elemental ZF. Algunos textos prueban que las bases de Hamel son conjuntos tan “raros” que las hay tanto Lebesgue-medibles como no.

Teorema (AE) 3.29: Todo par de bases de un espacio vectorial son equipotentes.

DEMOSTRACIÓN: Sean X, Y bases del espacio, podemos suponer que ambas son infinitas, pues el caso restante ya fue probado. Para todo $x \in X$ admitamos que Y_x es un subconjunto finito de Y tal que $x \in \langle Y_x \rangle$, notemos que $Y' := \bigcup_{x \in X} Y_x$ cumple que $X \subseteq \langle Y' \rangle$, de modo que Y' es base, luego $Y = Y'$. Como se asume AE cada Y_x puede ser enumerado y como son finitos los índices han de ser naturales, de modo que se puede definir $f: Y \rightarrow X \times \mathbb{N}$

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 3.30: Si V es un espacio vectorial y $W \leq V$, entonces:

1. $\dim V = \dim W + \dim(V/W)$.
2. Si $\dim V = \dim W$ y es finito, entonces $V = W$.

DEMOSTRACIÓN:

1. Sea B_W una base de W , sabemos que se puede extender a una base B_V de V , simplemente basta ver que $B := \{[v] : v \in B_V \setminus B_W\}$ 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 3.31 – Fórmula de Grassman: Si $A, B \leq V$ con V un espacio vectorial, entonces

$$\dim A + \dim B = \dim(A + B) + \dim(A \cap B).$$

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

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

3.3 Matrices y transformaciones lineales

Teorema 3.33: 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 $\bar{f} : M \rightarrow N$ tal que $\bar{f}|_X = f$.

Teorema 3.34: Si $f \in L(V, W)$, entonces:

1. f es inyectiva syss $\ker f = \{0\}$.
2. f es suprayectiva syss su imagen contiene a alguna base, y por ende a todas ellas.
3. En particular, si $n := \dim V = \dim W < +\infty$ entonces f es un isomorfismo de módulos syss es inyectiva o suprayectiva, lo que se reduce a ver que $\dim \ker f = 0$ o $\dim \operatorname{Im} f = n$.

Corolario 3.35: Dos espacios vectoriales son isomorfos syss comparten dimensión.

Definición 3.36: Si $B := (e_i)_{i \in I}$ es una base (ordenada) de un A -módulo M , entonces $\pi_i^B : M \rightarrow A$ 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 π_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 π_i^X es un funcional.
2. Para todo i, j se cumple que $\pi_i^X(x_j) = \delta_{ij}$.
3. π^X es un isomorfismo con A^n .

Por ello en lugar de denotar un A -módulo de dimensión finita denotaremos A^n .

Supongamos entonces que si $f : M \rightarrow N$ 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 $\pi^X(\mathbf{v}) \in \text{Mat}_{1 \times n}(A)$.

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 $B = M_X^Y(f)$ si y sólo si 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 λ 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 λ tiene determinante $\lambda \det B$.
3. Sumarle a una columna (resp. fila) λ -veces otra columna (resp. fila) distinta no varía el determinante.
4. Si para todo $i < j$ (o que $j < i$) se cumple que $b_{ij} = 0$, entonces $\det B = b_{11}b_{22} \cdots b_{nn}$.

Proposición 3.51: Para toda matriz B cuadrada se cumple $\det(B^t) = \det(B)$.

Teorema 3.52: Para todos $B, C \in \operatorname{Mat}_n(\mathbb{k})$ 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:

$$1. \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

$$2. \operatorname{adj} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

$$3. \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - (afh + bdi + ceg) \text{ (regla de Sarrus).}$$

Una técnica de mnemotecnica se basa en la fig. 3.1, donde las diagonales verdes se suman y las rojas se restan.

$$\begin{bmatrix} a & b & c & a & b & c \\ d & e & f & d & e & f \\ g & h & i & g & h & i \end{bmatrix}$$

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 3.61: Dos matrices similares comparten determinante.

PISTA: Se sigue del teorema 3.52. □

Definición 3.62: 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 3.63: 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 3.64: Dos matrices similares comparten traza.

Ya hemos visto que el determinante de una matriz es de hecho una expresión polinómica en términos de los coeficientes de la matriz. Ésto nos sirve para construir un polinomio que también es relevante para nuestros fines:

Definición 3.65: Dada una matriz $B \in \text{Mat}_n(\mathbb{k})$, se define su *polinomio característico* como

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

Proposición 3.66: Dos matrices similares comparten polinomio característico.

Proposición 3.67: 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 3.68: 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 3.69: El rango por filas, el rango por columnas y la dimensión de la imagen de una matriz concuerdan.

DEMOSTRACIÓN: Sean r_f y r_c el rango por filas y por columnas resp. de una matriz fijada $A \in \text{Mat}_{n \times m}(\mathbb{k})$. 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 3.70: Se le dice *rango*, denotado $\text{rank}(A)$, de una de una matriz A al rango por filas o columnas.

Corolario 3.71: Para toda matriz A se cumple que $\text{rank}(A) = \text{rank}(A^t)$.

Teorema 3.72: 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 $\text{rank}(A) = \text{rank}(BA) = \text{rank}(AC)$.

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

Proposición 3.73: Una matriz de $n \times n$ es invertible syss tiene rango n .

Teorema 3.74: Si $A \in \text{Mat}_{n \times m}(\mathbb{k})$ y $B \in \text{Mat}_{m \times p}(\mathbb{k})$, entonces

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

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

Definición 3.75: Dada una matriz $A \in \text{Mat}_{n \times m}(R)$. 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:

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

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

Proposición 3.76: El rango de una matriz A , es el mayor n tal que existe una submatriz de A de tamaño $n \times n$ inversible.

DEMOSTRACIÓN: Sea A de dimensiones $u \times v$. Claramente si A posee una submatriz de $n \times n$ inversible, entonces necesariamente $\text{rank } A \geq n$. Por otro lado, si $\text{rank } A = m$, 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 $\text{rank } A \leq n$. \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. §10.2.4).

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*:

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

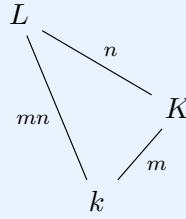
Dada una extensión K del cuerpo k , un elemento $\alpha \in K$ se dice *k -algebraico* si existe $p \in k[x]$ tal que $p(\alpha) = 0$, de lo contrario se dice *k -trascendente*. Una extensión K se dice *k -algebraica* si todos sus elementos lo son, de lo contrario, K se dice *k -trascendente*. De no 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 α se repite, digamos $\alpha^i = \alpha^j$, entonces $p(x) := x^j - x^i$ hace algebraico a α . De lo contrario, como S tiene $n + 1$ elementos no puede ser base, ergo existen $c_i \in k$ tales que son no nulos y

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

pero luego $p(x) := \sum_{i=0}^n c_i x^i$ es claramente un polinomio que hace que α 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 $p(x) \in k[x]$ no constante y sin raíces, entonces existe una extensión K/k que posee una raíz de $p(x)$.

DEMOSTRACIÓN: Si $p(x)$ 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 $q(x)$ uno de ellos. Como $(q(x))$ es un ideal maximal, entonces $K := k[x]/(q(x))$ 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 $q(x)$ que divide a $p(x)$ tenemos que

$$0 = [p(x)] = \sum_{i \geq 0} [a_i][x]^i = \sum_{i \geq 0} a_i \alpha^i = p(\alpha),$$

osea que α es una raíz de p en K . \square

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 ésto no tiene nada que ver con la función real $\sqrt[n]{x}$, pues se define de otra manera (ver def. 1.50 de [Top]).

Definición 4.6: Sea k un cuerpo con $p(x) \in k[x]$ un polinomio no-constante sin raíz. Entonces denotando α como una raíz de p , entonces $k(\alpha)$ es la extensión de k construida en condiciones de la demostración anterior.

Nótese que para todo $p(x) \in k[x]$,

$$[p(x)] = \sum_{i \geq 0} [a_i][x]^i = \sum_{i \geq 0} a_i \alpha^i = p(\alpha),$$

es decir, que la extensión que hemos construido resulta ser el cuerpo de polinomios de α (de ahí la notación). De igual manera podríamos construir una extensión con un polinomio que si tuviese raíz, pero es inmediato notar que es el mismo k .

Teorema 4.7: Si K/k es una extensión de cuerpos y $\alpha \in K$ es algebraico, entonces:

1. Existe un único polinomio mónico irreducible $p(x) \in k[x]$ tal que $p(\alpha) = 0$. Al que llamaremos *polinomio minimal* de α sobre k .
2. Si $q(x) \in k[x]$ cumple que $q(\alpha) = 0$, entonces $p(x) \mid q(x)$.

3. $\text{ev}_\alpha [k[x]] = \text{ev}_\alpha [k(x)] = \{r(\alpha) : r(x) \in k[x] \wedge \deg r < \deg p\}$
4. $k(\alpha)/k$ es una extensión finita, de hecho $[k(\alpha) : k] = \deg p =: n$ 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 $\pi(q(x)) = q(\alpha)$. Claramente π es un epimorfismo de anillos, luego $\ker \pi$ es un ideal de $k[x]$, y como éste es un PID, entonces es generado por un polinomio $p(x)$. Como $k(\alpha) \cong k[x]/(p(x))$ es un dominio íntegro, entonces $(p(x))$ es primo y $p(x)$ es irreducible.
2. Supongamos que $q(x)$ tiene a α de raíz, entonces $q(x) \in \ker \pi = (p(x))$, luego $p(x) \mid q(x)$. Si $q(x)$ es irreducible, entonces q y p 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 $q(\alpha)$ con $\deg q < n$, 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 $p(x)$. \square

El teorema anterior nos dice que en un sentido $k(\alpha)$ es la *mínima* extensión de cuerpos que contiene a α . En el teorema 4.13 veremos una generalización del teorema anterior que no depende del cuerpo base.

Corolario 4.8: Sea K/k una extensión de cuerpos y sean $\alpha, \beta \in K$ algebraicos, entonces

$$[k(\alpha, \beta) : k] \leq [k(\alpha) : k] \cdot [k(\beta) : k].$$

En consecuencia si $S \subseteq K$ es finito y algebraico, entonces $k(S)/k$ es una extensión finita.

DEMOSTRACIÓN: Por transitividad de grados sabemos que

$$[k(\alpha, \beta) : k] = [k(\beta)(\alpha) : k(\beta)] \cdot [k(\beta) : k],$$

por ende basta notar que $[k(\beta)(\alpha) : k(\beta)] \leq [k(\alpha) : k]$. Para ello, el teorema anterior demuestra que $[k(\alpha) : k] = \deg f$, donde $f(x) \in k[x]$ es el polinomio

minimal de α . Pero $f(x) \in k(\beta)[x]$, así que por el teorema anterior se cumple que es múltiplo del polinomio minimal $g(x)$ en $k(\beta)$, por lo que $[k(\beta)(\alpha) : k(\beta)] = \deg g \leq \deg f = [k(\alpha) : k]$. \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.:

$$p(x) = x^2 - 2, \quad q(x) = x^2 - 3.$$

Para notar que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ hay que ver que $q(x)$ no tiene raíces en $\mathbb{Q}(\sqrt{2})$. Para ello nótese que

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

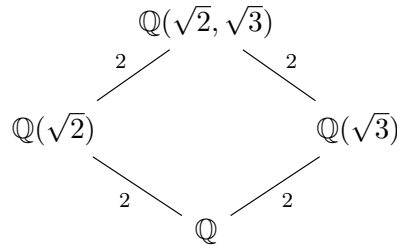
como $\mathbb{Q}(\sqrt{2})$ es un \mathbb{Q} -espacio vectorial de base $\{1, \sqrt{2}\}$ se concluye que

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

De la segunda línea se comprueba que $a = 0$ o $b = 0$. Si $b = 0$, entonces se reduce al caso de $q(x)$ en \mathbb{Q} que sabemos no tiene solución. Si $a = 0$, entonces nos queda que

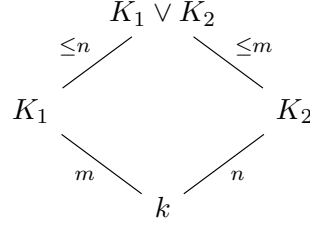
$$r(x) := 2x^2 - 3 = 0$$

Pero por criterio de Eisenstein el polinomio $r(x)$ es irreducible, luego no tiene raíces. En conclusión $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Luego $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] > 1$ y por el corolario $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Así se concluye que:



Definición 4.9: Sean $L/K_1/k$ y $L/K_2/k$ extensiones de cuerpo. Entonces $K_1 \cap K_2$ y $K_1 \vee K_2 := K_1(K_2) = K_2(K_1)$ son k -extensiones de cuerpo.

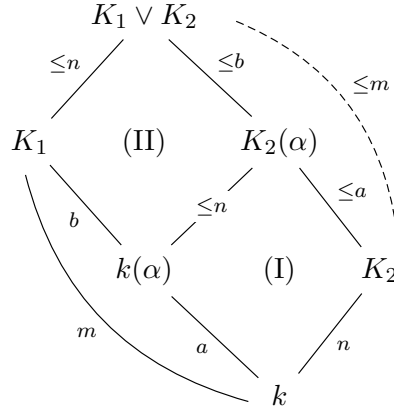
Proposición 4.10: Sean $L/K_1/k$ y $L/K_2/k$ extensiones de cuerpo con K_1, K_2 finitas. Entonces se satisface el siguiente diagrama de retículos:



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

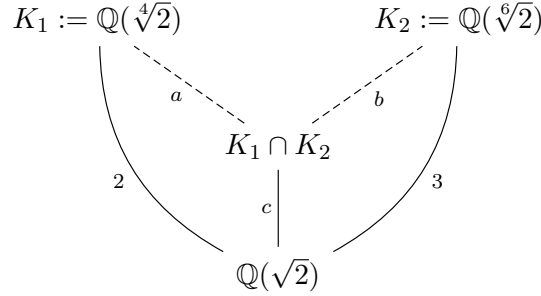
Hagamos la siguiente observación: Si $K_1 = k(\alpha)$, entonces el enunciado se satisface. La demostración es la misma del corolario 4.8, se toma el polinomio minimal de α y se nota que es también tiene raíz en $K_1 \vee K_2 = K_2(\alpha)$ como polinomio de K_2 .

Para el caso general, si $K_1 = k$ es trivial. Si no, sea $\alpha \in K_1 \setminus k$, entonces como K_1 es finita, entonces es algebraica y se cumple que $[K_1 : k] = m = [K_1 : k(\alpha)] \cdot [k(\alpha) : k]$. Luego la demostración consiste en construir el siguiente diagrama de retículos:



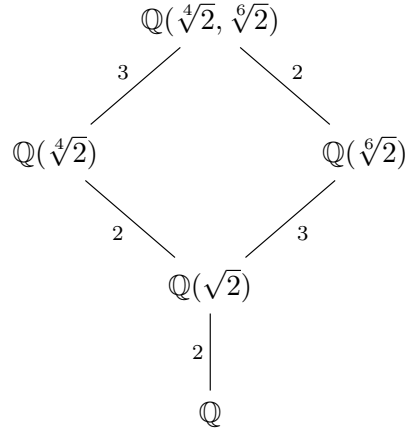
donde el diamante (I) sale de la observación, mientras que el diamante (II) sale por hipótesis inductiva. \square

Ejemplo. Consideremos $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$. Nótese que como $p(x) := (x^4 - 2)$ 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 $\sqrt[4]{2} \notin Q(\sqrt[6]{2})$, puesto que de lo contrario, se tendría la torre $[Q(\sqrt[6]{2}) : Q(\sqrt[4]{2})] \cdot [Q(\sqrt[4]{2}) : Q] = 4n = 6$ y no existe un n entero que la satisfaga. Luego $[Q(\sqrt[6]{2}, \sqrt[4]{2}) : Q(\sqrt[4]{2})] > 1$ y por el corolario es ≤ 2 . Por ende el diagrama de retículos se ve así:



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

Teorema 4.11: Si $L/K/k$ son extensiones de cuerpos, entonces L/k es algebraica syss L/K y K/k lo son.

DEMOSTRACIÓN: \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 α es K -algebraico, luego sean β_1, \dots, β_n los coeficientes de su polinomio minimal, luego α 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 β_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 4.12: Si K/k es una extensión de cuerpos, entonces el conjunto de elementos algebraicos de K es un cuerpo.

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

Teorema 4.13: Sean K/k y L/ℓ 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 $p \in k[x]$ su polinomio minimal. Si L contiene una raíz β de $\sigma p(x)$, entonces σ se extiende un isomorfismo de extensiones $\sigma^* : k(\alpha) \rightarrow \ell(\beta)$ con $\sigma^*(\alpha) = \beta$, es decir, existe un σ^* 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).

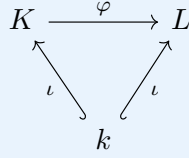
DEMOSTRACIÓN: Sea $\phi : k[x] \rightarrow k[\alpha]$ el morfismo de evaluación, i.e., tal que $\phi(g) = g(\alpha)$. Es claro que $\ker \phi$ es el ideal $(p(x))$, luego por el primer teorema de isomorfismos $k[x]/(p(x)) \cong k[\alpha]$.

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

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

Ésto nos motiva a formular la siguiente definición:

Definición 4.14: Sean K/k y L/k extensiones de cuerpo. Entonces decimos que una función $\varphi : K \rightarrow L$ 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 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 4.15: Sea K/k una extensión de cuerpo, donde $K = k(\alpha)$ y $p(x) \in k[x]$ es el polinomio minimal de α . Entonces $|\text{Gal}(K/k)|$ es la cantidad de raíces distintas de $p(x)$; en particular,

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

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

DEMOSTRACIÓN: Sean $\alpha_1, \dots, \alpha_n$ todas las raíces de $p(x)$ 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 σ_{1j} es un k -automorfismo distinto, por lo que $|\text{Gal}(K/k)| \geq n$. Al mismo tiempo si σ es un k -automorfismo, entonces $p(\sigma(\alpha)) = \sigma(p(\alpha)) = 0$, de modo que $\sigma(\alpha) = \alpha_i$, pero el teorema anterior prueba la unicidad de σ , con lo que $|\text{Gal}(K/k)| = n$. Como $n \leq \deg p$ se comprueba la desigualdad.

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

Definición 4.16 (k -conjugados): Dados α, β algebraicos sobre k , se dice que son k -conjugados si comparten el polinomio minimal.

Teorema 4.17: Dados α, β algebraicos sobre k , entonces son k -conjugados syss existe un k -isomorfismo $\sigma : k(\alpha) \rightarrow k(\beta)$ tal que $\sigma(\alpha) = \beta$. Más aún, $\sigma(\alpha)$ siempre es un k -conjugado de α .

Ejemplo. El polinomio ciclotómico p -ésimo, con $p > 2$, es irreducible luego carece de raíces, así que construyamos $\mathbb{Q}(\omega)$ donde ω es una raíz.

Como $\Phi_p(x) \cdot (x - 1) = x^p - 1$, entonces todas las raíces del polinomio son raíces p -ésimas de la unidad, ergo $\omega^p = 1$, luego $(\omega^2)^p = 1^2 = 1$, por lo que ω^2 también es raíz de $\Phi_p(x)$. De hecho, se concluye que todas las raíces de $\Phi_p(x)$ son $\omega^1, \omega^2, \dots, \omega^{p-1}$; luego ellos son k -conjugados.

Teorema 4.18: 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 $p \in k[S]$, como σ es un k -automorfismo se cumple $\sigma(p(\alpha_1, \dots, \alpha_n)) = p(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$. Notemos que todo elemento en K es de la forma $p(\alpha_1, \dots, \alpha_n)$, luego dos k -automorfismos coinciden si y sólo si lo hacen en S .

Sea p_i el polinomio minimal de α_i , entonces $p(\alpha_i) = 0 = \sigma(p(\alpha_i)) = p(\sigma(\alpha_i))$. Y se sabe que un polinomio no nulo tiene finitas raíces, luego σ sólo puede tomar finitos valores en α_i . Finalmente sólo hay finitas posibilidades para σ , luego $\text{Gal}(K/k)$ es finito. \square

4.2 Extensiones normales y separables

§4.2.1 Cuerpos de escisión.

Definición 4.19: Se dice que un polinomio $p \in k[x]$ se escinde (en inglés, *split*) en una extensión de cuerpos K/k , si existen $\alpha_0, \alpha_1, \dots, \alpha_n \in K$ tales que

$$p(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_n).$$

También llamamos *cuerpo de escisión* de p sobre k a la extensión K/k tal que p escinde en K y $K = k(\alpha_1, \dots, \alpha_n)$.

Teorema 4.20: Si $\sigma : k \rightarrow k'$ es un isomorfismo de cuerpos, K es un cuerpo de escisión de $p(x) \in k[x]$ y K' de $\sigma(p)(x)$, entonces se extiende σ 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 p es irreducible. Lo haremos por inducción sobre el grado de p , donde el caso $n = 1$ es trivial. Sea p de grado $n+1$, sea α_{n+1} una raíz en K y sea β_{n+1} una raíz de $\sigma(p)$ 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 σ . Luego sea $p(x) = (x - \alpha_{n+1})q(x)$ de modo que K es un cuerpo de escisión de $q(x)$ (de grado n) en $k(\alpha_{n+1})$ y K' lo es de $\sigma^*(q(x))$

en $k'(\beta_{n+1})$; por lo que, por hipótesis inductiva, existe $\bar{\sigma}$ que extiende a σ^* (que extiende a σ) tal que $\bar{\sigma} : K \rightarrow K'$ es un isomorfismo de cuerpos. \square

Proposición 4.21: Si $p \in k[x]$ es de grado $n \geq 1$, entonces posee un cuerpo de escisión y ésta tiene grado a lo más $n!$

PISTA: Usar inducción. \square

Ejemplo. Consideremos el polinomio

$$\Phi_7(x) := \frac{x^7 - 1}{x - 1} = 1 + x + x^2 + \cdots + x^6$$

que es irreducible por ser ciclotómico. Si ω es alguna raíz de Φ_7 , entonces $\mathbb{Q}(\omega)$ es su cuerpo de escisión y tiene grado 6.

Consideremos ahora el polinomio

$$p(x) := x^6 - 2$$

que posee una raíz $\sqrt[6]{2}$. Nótese que $p(x)$ **no** se escinde en $\mathbb{Q}(\sqrt[6]{2})$. En primer lugar, como $\sqrt{2} \in \mathbb{Q}(\sqrt[6]{2})$ se tiene que

$$p(x) = (x^3 - \sqrt{2})(x^3 + \sqrt{2})$$

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 si su discriminante tiene raíces, el cual es

$$\sqrt[6]{2}^2 - 4\sqrt[3]{2} = -3\sqrt[3]{2}.$$

Como $\sqrt[6]{2} \in \mathbb{R}$ se tiene que $\mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{R}$ y \mathbb{R} no posee raíces de números negativos, así que $\mathbb{Q}(\sqrt[6]{2})$ tampoco; y por tanto el polinomio no se escinde.

Definición 4.22 – Extensión normal: Se dice que una extensión de cuerpos K/k es *normal* si para todo $p \in k[x]$ irreducible con alguna raíz en K se escinde en K .

Lema 4.23: Si $L/F/K/k$ son extensiones algebraicas de cuerpo de modo que F es un cuerpo de escisión de algún polinomio $p(x) \in k[x]$. Entonces si $\sigma : K \rightarrow L$ es un k -monomorfismo se cumple que $\sigma[K] \subseteq F$ y σ se extiende a un k -automorfismo de F , y en consecuencia, se extiende a un k -automorfismo de L . En diagramas conmutativos:

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

DEMOSTRACIÓN: Supongamos que $p(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_n)$ 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 σ .

Sea $\beta \in K$, como $F = K(\alpha_1, \dots, \alpha_n)$, entonces existe $g(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ tal que $g(\alpha_1, \dots, \alpha_n) = \beta$, pero como los α_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 α_i , de modo que $F' = \bar{\sigma}(F) \subseteq F$. En consecuencia $F' = F$ y $\bar{\sigma}$ es un k -automorfismo. \square

Teorema 4.24: Una extensión finita K/k es normal si y sólo si es el cuerpo de escisión de algún polinomio.

DEMOSTRACIÓN: \Leftarrow . Sea $p(x) \in k[x]$ el polinomio tal que K es su cuerpo de escisión. Sea $q(x) \in k[x]$ irreducible en $k[x]$ pero con raíz $\alpha \in K$. Sea L el cuerpo de escisión de q sobre K , de modo que si las raíces de $q(x)$ son $\alpha_1, \dots, \alpha_n$, entonces $L = K(\alpha_1, \dots, \alpha_n)$. Como α_i y α son k -conjugados, existe $\sigma : k(\alpha) \rightarrow k(\alpha_i) \subseteq L$ un k -isomorfismo, luego por el lema $k(\alpha_i) \subseteq K$, y como los $\alpha_i \in K$, $q(x)$ 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 $p_i(x)$ denota el polinomio minimal de α_i sobre k , entonces vemos que K se escinde en $p(x) := p_1(x) \cdots p_n(x)$ y es fácil ver que K es de hecho su cuerpo de escisión. \square

Definición 4.25: Sea K/k una extensión finita. Entonces N se dice una *clausura normal* de K si $N/K/k$ es extensión y si $N/N'/K/k$ es tal que N' es normal, entonces $N' = N$.

Proposición 4.26: Toda extensión finita posee una clausura normal que es única salvo isomorfismo.

DEMOSTRACIÓN: Sea $K = k(\alpha_1, \dots, \alpha_n)$ y $p_i(x) \in k[x]$ el polinomio minimal de α_i resp. Entonces sea $q(x) := \prod_{i=1}^n p_i(x) \in k[x]$, luego el cuerpo de escisión N de $q(x)$ es una extensión normal de K . Sea N' otra extensión normal de K , entonces todos los $p_i(x)$ 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 $q(x)$, que es único salvo isomorfismo. \square

§4.2.2 Extensiones separables.

Definición 4.27 (Polinomio derivado): Si D es un dominio íntegro y

$$p(x) = \sum_{k=0}^n a_k x^k \in D[x]$$

llamamos *polinomio derivado* de $p(x)$, denotado por $p'(x)$, a

$$p'(x) := \sum_{k=1}^n k a_{k-1} x^{k-1}.$$

Proposición 4.28: Si D es un dominio íntegro, entonces para todo $p, q \in D[x]$ y $\lambda \in D$:

1. $(\lambda p)' = \lambda p'$.
2. $(p + q)' = p' + q'$.
3. $(pq)' = p'q + pq'$.
4. $(p/q)' = \frac{p'q - pq'}{q^2}$.

Definición 4.29: Se dice que la *multiplicidad* de una raíz α de un polinomio $p(x) \in D[x]$ es el máximo entero n tal que $(x - \alpha)^n \mid p(x)$. Si una raíz es de multiplicidad 1, entonces se dice que es una raíz *simple*.

Teorema 4.30: Dado D un dominio íntegro y α raíz de $p(x) \in D[x]$. α es una raíz simple syss $p'(\alpha) \neq 0$.

DEMOSTRACIÓN: Supongamos que el grado de α en p es n de modo que $p(x) = (x - \alpha)^n q(x)$ y $q(\alpha) \neq 0$, luego

$$p'(\alpha) = n(x - \alpha)^{n-1}q(x) + (x - \alpha)^n q'(x) = n(x - \alpha)^{n-1}q(x)$$

lo cual es no nulo syss $n - 1 = 0$, i.e., si α es una raíz simple. \square

Definición 4.31: Sea K/k una extensión de cuerpos. Un elemento algebraico $\alpha \in K$ se dice *separable* syss es la raíz simple de su polinomio minimal.

Si todos los elementos de K son separables, entonces K se dice una *extensión separable*. 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 trascendentales separables o no.

Ejemplo 6: Consideremos $k := \mathbb{F}_p(t)$ como cuerpo. Estudiemos el polinomio $p(x) := x^p - t \in k[x]$. Nótese que para todo $\alpha \in k$ se cumple que $(x - \alpha)^p = x^p - \alpha^p$, luego si ω es una raíz de $p(x)$ en alguna extensión K/k se cumple que $p(x) = (x - \omega)^p$. Notemos que dicho polinomio es irreducible (al menos en el caso de $p = 2$), de modo que K/k no es una extensión separable, dado que ω no lo es.

Proposición 4.32: Sea k un cuerpo de característica p . Entonces $\text{Frob}_k(a) = a^p$ es un endomorfismo, conocido como el endomorfismo de Frobenius. Y si Frob_k es suprayectivo, entonces Frob_k corresponde a un automorfismo.

Proposición 4.33: Sea D un dominio íntegro y $p(x) \in D[x]$ un polinomio no constante, entonces:

1. Si $\text{car } D = 0$, entonces $p'(x) \neq 0$.
2. Si $\text{car } D = p$, entonces $p'(x) = 0$ syss $p(x) = q(x^p)$ con $q(x) \in D[x]$.

Teorema 4.34: Se cumple:

1. Todo cuerpo de característica nula es perfecto.
2. Si $\text{car } k = p$, entonces k es perfecto y Frob_k es un automorfismo.
3. Todo cuerpo finito es perfecto.

DEMOSTRACIÓN:

1. Sea $\alpha \in K$ algebraico, cuyo polinomio minimal es $p(x)$. Si $p'(\alpha) = 0$, entonces $p(x) \mid p'(x)$, pero como $p'(x) \neq 0$ esto no tiene sentido por grados de polinomios.
2. \Leftarrow . Sea $\alpha \in K/k$ algebraico y cuyo polinomio minimal es $p(x)$. Asumiremos que $p'(x) = 0$ de modo que $p(x) = q(x^p)$. Sea $q(x) = \sum_{i=0}^n a_i x^i$. Como Frob_k es endo-, existen b_i tales que $a_i = b_i^p$, luego

$$p(x) = q(x^p) = \sum_{i=0}^n a_i (x^p)^i = \sum_{i=0}^n b_i^p (x^i)^p = \sum_{i=0}^n (b_i x^i)^p = \left(\sum_{i=0}^n b_i x^i \right)^p,$$

por lo que p 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 $p(x)$ el polinomio minimal de b . Sabemos que b es raíz de $(x - a)^p$, por ende $p(x) \mid (x - a)^p$ de modo que $p(x) = (x - a)^n$ 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. 6 vimos que la extensión $\mathbb{F}_p(t, \omega)$ no es separable, pero ésto ocurre como extensión de $\mathbb{F}_p(t)$, nótese que $\mathbb{F}_p(t, \omega)$ no es una extensión trascendental de \mathbb{F}_p .

Teorema 4.35: Existe una correspondencia biunívoca entre cuerpos finitos y números de la forma p^n con p primo y $n \geq 1$. Es decir, para todo p primos y $n \geq 1$ existe un único cuerpo de cardinalidad p^n y todo cuerpo tiene cardinalidad de esa forma.

DEMOSTRACIÓN: Sea k un cuerpo finito, luego tiene característica p y es un \mathbb{F}_p -espacio vectorial de dimensión finita n , luego su cardinalidad es de la forma p^n .

Sea $p(x) := x^{p^n} - x \in \mathbb{F}_p[x]$, 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 $p(x)$; 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

En general denotamos por \mathbb{F}_{p^n} al único cuerpo de cardinalidad p^n salvo isomorfismos.

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 4.18 vimos que ha de ser finito en extensiones finitas y el teorema 4.17 nos caracteriza los k -automorfismos en términos de las raíces de un polinomio minimal. Sin embargo, podrían darse varias situaciones desfavorables: podría ser que las raíces se repitan y, por lo tanto, que el grupo esté más restringido, o podría darse que un polinomio no se escinda y luego no podamos conjugar las raíces a causa de no tenerlas. Por ello, reorientaremos el problema:

Definición 4.36: 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 4.37: Sea α algebraico, entonces $N(k(\alpha)/k) = [k(\alpha) : k]$ si α 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:

Proposición 4.38: Sea K/k una extensión de cuerpos y $\alpha \in K$ algebraico. Si $\text{car } k = p$, entonces existe algún $n \in \mathbb{N}$ tal que

$$[k(\alpha) : k] = p^n N(k(\alpha)/k)$$

y que α^{p^n} es separable. En consecuencia, $N(k(\alpha)/k) \mid [k(\alpha) : k]$.

DEMOSTRACIÓN: Sea $f(x) \in k[x]$ el polinomio minimal de α , entonces en la clausura normal N de K sobre k se cumple que

$$f(x) = \prod_{i=1}^r (x - \alpha_i)^{m_i}$$

donde α_i son las raíces distintas de $f(x)$, $m_i > 0$ y $\alpha_1 = \alpha$. 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 α no es separable, entonces α es raíz común de $f(x)$ y $f'(x)$; pero por definición del polinomio minimal se debe cumplir entonces que $f'(x) = 0$, por lo que $f(x) = g(x^p)$ con $g(x) \in k[x]$. Además, claramente $\deg g < \deg f$. Luego procedemos recursivamente hasta encontrar el n más grande tal que $f(x) = h(x^{p^n})$ y necesariamente $h'(x) \neq 0$, por lo que α^{p^n} ha de ser una raíz separable de h .

Por la relación entre g y f claramente ha de cumplirse que

$$[k(\alpha) : k(\alpha^p)] = p$$

Por lo que, por inducción se debe dar que $[k(\alpha) : k(\alpha^{p^n})] = p^n$. Más aún, claramente α_i es raíz de f syss $\alpha_i^{p^n}$ es raíz de h , luego $[k(\alpha^{p^n}) : k] = r$ y $k(\alpha^{p^n})/k$ es una extensión separable, por lo que, $N(k(\alpha^{p^n})/k) = r$. Y de hecho, por la correspondencia entre raíces de f y de h se concluye una correspondencia entre los k -morfismos, de modo que $N(k(\alpha^{p^n})/k) = N(k(\alpha)/k)$ y, en síntesis,

$$[k(\alpha) : k] = [k(\alpha) : k(\alpha^{p^n})][k(\alpha^{p^n}) : k] = p^n N(k(\alpha)/k). \quad \square$$

Definición 4.39 – 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 4.40: 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 4.23 se ha de cumplir que σ 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 τ_1, τ_2 dos posibles extensiones de σ . Es decir, τ_1, τ_2 son k -automorfismos de L , pero entonces $\tau_1 \circ \tau_2^{-1} : L \rightarrow L$ 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 4.41: 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 4.42 – 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 4.63 más adelante) por lo que tiene un generador γ y claramente $K = k(\gamma)$.

Si k es infinito: Por inducción basta probar el caso cuando K/k está generado por dos elementos. Así pues, sea $K = k(\alpha, \beta)$, queremos probar que $K = k(\gamma)$. Sea A el conjunto de todos los pares (α', β') , donde α', β' son k -conjugados de α y β resp. Si $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in A$, entonces existe a lo más un $u \in k$ tal que $\alpha_1 + u\beta_1 = \alpha_2 + u\beta_2$. Como A es finito y k infinito, entonces existe un $v \in k$ tal que $\alpha_1 + v\beta_1 \neq \alpha_2 + v\beta_2$ para todo $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in A$.

Sea $\gamma := \alpha + v\beta$ y sean σ, τ dos k -monomorfismos de K en una clausura normal de K . Luego, como $(\sigma(\alpha), \sigma(\beta)), (\tau(\alpha), \tau(\beta)) \in A$, entonces

$$\sigma(\gamma) = \sigma(\alpha) + v\sigma(\beta) \neq \tau(\alpha) + v\tau(\beta) = \tau(\gamma).$$

Es decir, γ posee $N(K/k)$ 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

Proposición 4.43: 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 4.44: Una extensión finita K/k es de Galois syss

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

DEMOSTRACIÓN: \implies . Sea $\alpha \in K$, hemos de probar que existe un k -isomorfismo de K que mueve a α . Sea $p(x)$ su polinomio minimal, como K es de escisión sobre $p(x)$ contiene a todas sus raíces, así que si existe otra raíz β de $p(x)$ existe un k -isomorfismo tal que $\sigma(\alpha) = \beta$. Si no existe otra raíz entonces $p(x) = (x - \alpha)^n$ y por separabilidad $n = 1$ por lo que $\alpha \in k$.

\Leftarrow . Sea $\alpha \in K \setminus k$ de polinomio minimal $p(x)$. Sean $\alpha_1, \dots, \alpha_n$ todas las raíces distintas de $p(x)$ en K , entonces definimos

$$q(x) := (x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$$

que satisface que $q(x) \mid p(x)$ por construcción.

Sea $\sigma \in \text{Gal}(K/k)$. Como $\sigma(\alpha_i) = \alpha_j$ por ser k -conjugados, entonces se cumple que $(q \circ \sigma)(x) = \prod_{i=1}^n (x - \sigma(\alpha_i)) = q(x)$ de modo que todos los coeficientes de $q(x)$ están fijados por un k -automorfismo σ cualquiera, de modo que los coeficientes de $q(x)$ **deben** estar en k .

Luego, como α es raíz de $q(x) \in k[x]$ se cumple que $p(x) \mid q(x)$. Pero entonces $p(x)$ y $q(x)$ están asociados, y como ambos son mónicos entonces son iguales, probando que p se escinde en K (luego es normal) y que sus raíces son simples (luego es separable). \square

Lema 4.45 (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 4.46: 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 λ_i están fijos bajo los k -automorfismos, se cumple que

$$\sum_{j=1}^n c_j \sigma_j(\beta) = \sum_{j=1}^n \sum_{i=1}^m c_j \lambda_i \sigma_j(a_i) = \sum_{i=1}^m \lambda_i \left(\sum_{j=1}^n c_j \sigma_j(a_i) \right) = 0$$

que es nulo, pues los términos en rojo lo son por definición de (c_1, \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 σ_h tal que $\sigma_h(c_1) \neq c_1$. Nótese que como H es grupo, el producto $\tau \mapsto \tau \circ \sigma_h$ es una permutación, de modo que al aplicar σ_h a las n -tuplas, de modo que

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

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

Teorema 4.47 – Teorema fundamental de la teoría de Galois:

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

$$\{L : K/L/k \text{ extensiones}\} \begin{matrix} \xrightarrow{\text{Gal}(K/L)} \\ \xleftarrow{F(H)} \end{matrix} \{H : H \leq G\}$$

entonces:

1. $F(H)$ y H_L son biyecciones, la una la inversa de la otra. Más aún, si $H_1 < H_2 \leq G$, entonces $K \supseteq F(H_2) \supset F(H_1)$, y si $k \subseteq L_1 \subset L_2 \subseteq K$, entonces $\text{Gal}(K/L_1) > \text{Gal}(K/L_2)$. En consecuencia, F es un funtor contravariante biyectivo:

$$\begin{array}{ccc} L_2 & & H_2 \\ \uparrow & \begin{matrix} \xrightarrow{\text{Gal}(K/L)} \\ \xleftarrow{F(H)} \end{matrix} & \downarrow \\ L_1 & & H_1 \end{array}$$

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 $p(x) \in k[x]$. Luego $p(x) \in L[x]$ y claramente K es el cuerpo de escisión de $p(x)$. 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 τ^{-1} manda α a sus k -conjugados, luego $\tau^{-1}(\alpha) \in L$. Como σ 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.

\impliedby . Sea $\alpha \in L$ y sea $p(x) \in k[x]$ su polinomio minimal. Para probar que L/k es normal, basta ver que todos los k -conjugados de α están en L . Luego sea β un k -conjugado de α , sabemos que existe $\tau \in \text{Gal}(K/k)$ tal que $\tau^{-1}(\alpha) = \beta$.

Como $F(\text{Gal}(K/L)) = L$, basta ver que todo σ fija a β . 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 4.48: 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 $p(x) \in K[x]$ un polinomio no constante, luego éste posee un factor irreducible $q(x)$ de manera que existe una extensión $K(\alpha)/K$ con una raíz α de $q(x)$, pero $K(\alpha) = K$ puesto que toda extensión finita es algebraica, de modo que $\alpha \in K$.

$2 \implies 3$. Sea $p(x) \in K[x]$ con $\deg p > 1$. Entonces $p(x)$ posee raíz α y por Ruffini se satisface que $(x - \alpha) \mid p(x)$, por lo que $p(x)$ 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 $p(x) = \sum_{i=0}^n c_i x^i \in K[x]$ tal que α es raíz de $p(x)$. 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 α es k -algebraico y, por lo tanto, es raíz de un polinomio $q(x) \in k[x]$. Pero como $q(x)$ 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 4.49 – 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 4.50: Sea K/k una extensión algebraicamente cerrada, entonces

$$L := \{\alpha \in K : \alpha \text{ es } k\text{-algebraico}\}$$

es un cuerpo y de hecho L/k es una clausura algebraica.

DEMOSTRACIÓN: Ya vimos que L forma una extensión de cuerpo (por el teorema 4.11) y es claro que es algebraica, así pues basta notar que es algebraicamente cerrado.

Sea $p(x) \in k[x]$ no constante, entonces p se escinde en K por definición de algebraicamente cerrado, luego

$$p(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_n),$$

luego $\alpha_0 \in k \subseteq L$ y cada α_i es k -algebraico, luego está en L .

Como L/k es una extensión algebraica tal que todo polinomio de k se escinde en L , se concluye que L es algebraicamente cerrado. \square

Teorema 4.51: 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 $p(x) := 1 + \prod_{i=1}^n (x - \alpha_i)$ 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) 4.52: 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 $y_{p(x)}$ donde $p(x) \in \mathcal{P}$. Así, construyamos $k[S]$, es decir, el anillo de polinomios cuyas variables son los y_p 's. Y construyamos el siguiente ideal:

$$\mathfrak{a} := (p(y_p) : p(x) \in \mathcal{P}).$$

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 $p_i \in \mathcal{P}$ tales que

$$\lambda_1 p_1(y_{p_1}) + \cdots + \lambda_n p_n(y_{p_n}) = 1.$$

Nótese que como cada λ_i posee finitos monomios, cada uno con finitas variables, en definitiva hay solo finitas variables en la ecuación anterior que podemos suponer son $F := \{y_{p_1}, y_{p_2}, \dots, y_{p_n}, z_1, z_2, \dots, z_m\}$.

Luego, la combinación lineal también vale en $k[F]$, pero he aquí un truco: Como hay finitos polinomios p_i 's, entonces existe una extensión finita L/k tal que $\alpha_i \in L$ es raíz de p_i resp. Como $k \subseteq L$, entonces la ecuación también vale en $L[F]$. Pero evaluando y_{p_i} en α_i y z_j en 0 se obtiene que

$$\lambda_1(\alpha_1, \dots, \alpha_n, 0, \dots, 0) p_1(\alpha_1) + \cdots + \lambda_n(\alpha_1, \dots, \alpha_n, 0, \dots, 0) p_n(\alpha_n) = 1$$

donde cada término en rojo vale cero por definición de α_i , es decir, $0 = 1$; lo que es absurdo.

2. Por el teorema de Krull, existe $\mathfrak{m} \supseteq \mathfrak{a}$ que es un ideal maximal. Luego $K_0 := k[S]/\mathfrak{m}$ es un cuerpo que extiende a k .
- 2.* (*Si se quiere evitar el AE.*)¹ Como \mathfrak{a} es ideal propio, existe \mathfrak{p} primo que le contiene. Luego $k[S]/\mathfrak{p}$ es un dominio íntegro y, por lo tanto, $K_0 := \text{Frac}(k[S]/\mathfrak{p})$ 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 $p(x) \in \mathcal{P}$, luego $\alpha := [y_p]$ satisface que

$$p(\alpha) = [p(y_p)] = 0$$

puesto que $p(y_p) \in \mathfrak{a} \subseteq \mathfrak{m}$.

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 $p(x) \in K[x]$ no constante, luego posee finitos coeficientes los cuales están contenidos en algún K_n para un n suficientemente grande, es decir, $p(x) \in K_n[x]$. Pero por construcción, existe $\alpha \in K_{n+1}[x]$ que es raíz de $p(x)$ y $\alpha \in K_{n+1} \subseteq K$.

¹Ésta idea fue propuesta por Banaschewski (véase [31]).

5. Como K/k es algebraicamente cerrado, por el teorema 4.50 admite un subcuerpo que es una clausura algebraica de k , que es lo que se quería probar. \square

Teorema (AE) 4.53: Las clausuras algebraicas de k son 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, σ) es una cota superior de C (¿por qué?).

Luego, por el lema de Zorn se cumple que \mathcal{F} tiene un elemento \subseteq -maximal (M, σ) . Veamos que $M = K_1$: Sea $\alpha \in K_1$, entonces α es k -algebraico, luego es la raíz de un polinomio $p(x)$. Sea $M' := \sigma[M] \subseteq K_2$, se cumple que existe β raíz de $\sigma p(x)$ (por ser algebraicamente cerrado). Luego, por el teorema se tiene que

$$\begin{array}{ccc} M(\alpha) & \overset{\sigma^*}{\rightsquigarrow} & M'(\beta) \\ \uparrow & & \uparrow \\ M & \rightsquigarrow_{\sigma} & M' \end{array}$$

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 β es k -algebraico así que es la raíz de $p(x) \in k[x]$. Como $p(x)$ se escinde en K_1 y σ manda raíces de $p(x)$ en raíces de $p(x)$, se ha de cumplir que β tiene preimagen. Como σ es suprayectiva e inyectiva (por ser k -morfismo), entonces es biyección, luego isomorfismo. \square

Teorema 4.54: 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 α_i es raíz de $p_i(x) \in k[x]$. Luego sea $q(x) := p_1(x)p_2(x) \cdots p_n(x) \in k[x]$. Entonces K_1 es el cuerpo de escisión de $q(x)$ y así se puede concluir el enunciado. \square

Definición 4.55: En consecuencia de los teoremas anteriores se denota por \bar{k} a la clausura algebraica de k .

§4.4.1 Aplicación: El teorema fundamental del álgebra II. Aquí veremos una aplicación de las extensiones de cuerpo que hemos estudiado.

Teorema 4.56: 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 4.57: Sea K/k una extensión finita y sea $\alpha \in K$. Nótese que $m_\alpha(x) := \alpha \cdot x$ es una k -transformación lineal sobre K y como K es de dimensión finita se pueden definir la *norma*, la *traza* y el *polinomio característico* de α como:

$$\begin{aligned} \mathrm{Tr}_{K/k}(\alpha) &:= \mathrm{tr}(m_\alpha), & \mathrm{Nm}_{K/k}(\alpha) &:= \det(m_\alpha), \\ \psi_{\alpha, K/k}(t) &:= \psi_{m_\alpha}(t) \in k[t] \end{aligned}$$

Usualmente la definición es otra, más relacionada con la conjugación, pero veremos que ambas coinciden.

Proposición 4.58: Sea K/k una extensión finita y sean $\alpha, \beta \in K$, entonces:

$$\mathrm{Tr}_{K/k}(\alpha + \beta) = \mathrm{Tr}_{K/k}(\alpha) + \mathrm{Tr}_{K/k}(\beta), \quad \mathrm{Nm}_{K/k}(\alpha \cdot \beta) = \mathrm{Nm}_{K/k}(\alpha) \cdot \mathrm{Nm}_{K/k}(\beta).$$

Teorema 4.59: Dada una extensión finita K/k , N su clausura normal de K y sea $\{\sigma_1, \dots, \sigma_n\} = \mathrm{Hom}_k(K, N)$. Entonces para todo $\alpha \in K$ se satisface que

$$\begin{aligned} \mathrm{Nm}_{K/k}(\alpha) &= \prod_{i=1}^n \sigma_i(\alpha), & \mathrm{Tr}_{K/k}(\alpha) &= \sum_{i=1}^n \sigma_i(\alpha), \\ \psi_{\alpha, K/k}(t) &= (t - \sigma_1(\alpha)) \cdots (t - \sigma_n(\alpha)) \end{aligned}$$

DEMOSTRACIÓN: Por la proposición 3.67 basta demostrar la identidad con el polinomio característico. Sea $\alpha \in K$ un elemento primitivo de K , de modo que su polinomio minimal es $p(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$. Como α 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_α en dicha base es

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

De modo que el polinomio característico es el determinante de

$$\begin{bmatrix} t & 0 & \cdots & 0 & a_0 \\ -1 & t & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & t + a_{n-1} \end{bmatrix},$$

el cual es de hecho el polinomio minimal $p(t)$ (¿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_α en la base $(y_j)_j$, es decir, $\alpha y_i = \sum_{h=1}^p a_{ih} y_h$. Luego vemos que

$$\alpha(y_i z_j) = (\alpha y_i) z_j = \sum_{h=1}^p a_{ih} y_h z_j.$$

Así pues, la representación matricial de m_α es

$$\begin{bmatrix} M & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & M & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & M \end{bmatrix} \in \text{Mat}_{pq}(k).$$

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

Ejemplo. En la extensión \mathbb{C}/\mathbb{R} , la norma y traza son:

$$\text{Nm}_{\mathbb{R}}^{\mathbb{C}}(z) = z \cdot \bar{z} = |z|^2, \quad \text{Tr}_{\mathbb{R}}^{\mathbb{C}}(z) = z + \bar{z} = 2 \text{Re}(z).$$

Teorema 4.60 (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 ω se dice una n -ésima raíz de la unidad si $\omega^n = 1$. Ésto lo habíamos estudiado en el caso complejo, pero la teoría de cuerpos admite mayor diámetro. Comenzaremos con un teorema curioso que prueba ser útil en teoría de números y teoría de la representación.

Teorema 4.61: $\sum_{d|n} \phi(d) = n$.

PISTA: Estudie el orden de los elementos del grupo $\mathbb{Z}/n\mathbb{Z}$. Si no, cf. [41, Prop. 3.5]. \square

Lema 4.62: 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 4.63: Si k es un cuerpo finito, entonces k^\times es cíclico.

Teorema 4.64: 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 4.62. \square

Por ejemplo: claramente el 1 no es una raíz n -ésima de la unidad primitiva, excepto para $n = 1$.

Definición 4.65: 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 4.66: 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 4.67: 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 ζ tal que $L = k(\zeta)$. Luego todo $\sigma \in \text{Gal}(L/k)$ está determinado por adónde manda ζ y sus conjugados son de la forma ζ^j y es fácil notar que si $\sigma\zeta = \zeta^a$ y $\tau\zeta = \zeta^b$, entonces $\sigma\tau\zeta = \sigma\zeta^b = \zeta^{ab} = \tau\sigma\zeta$. \square

De ésta demostración se desprenden fácilmente dos consecuencias:

Teorema 4.68: Si k es un cuerpo finito y K/k es una extensión finita, entonces K/k es una extensión cíclica.

DEMOSTRACIÓN: Por el teorema 4.35 vemos que todas las extensiones K/\mathbb{F}_p son ciclotómicas y, por tanto, cíclicas. Luego, basta notar que todo cociente de un grupo cíclico es también cíclico para concluir. \square

Teorema 4.69: Sea ζ_n una n -ésima raíz primitiva de la unidad en \mathbb{C} , y sea $K_n := \mathbb{Q}(\zeta_n)$. La extensión K_n/\mathbb{Q} es de Galois y $\text{Gal}(K_n/\mathbb{Q})$ 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, ζ_n^j son todas las raíces n -ésimas de la unidad. En particular ζ_n^j es primitiva syss j y n son coprimos.

Definición 4.70: Se define el n -ésimo *polinomio ciclotómico* como

$$\Phi_n(x) := \prod_{\substack{j=1 \\ (j;n)=1}}^n (x - \zeta_n^j) \in \mathbb{C}[x].$$

De momento sabemos poco del polinomio ciclotómico exceptuando por tres detalles triviales: El primero es que todas las raíces de Φ_n son exactamente las raíces n -ésimas primitivas de la unidad, el segundo es que $\Phi_n \mid (x^n - 1)$ y el tercero es que Φ_p concuerda con nuestra antigua definición de « Φ_p ». La segunda observación se puede mejorar a:

Proposición 4.71: 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 « ± 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 4.72: Para todo $n > 0$ se cumplen:

1. $\Phi_n(x)$ es mónico, tiene grado $\phi(n)$ y está en $\mathbb{Z}[x]$.
2. Φ_n es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$, de modo que Φ_n es el polinomio minimal de ζ_n sobre \mathbb{Q} .
3. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es un cuerpo de Galois de grado $\phi(n)$ que es, de hecho, el cuerpo de escisión de $x^n - 1$.

DEMOSTRACIÓN: Para la primera todas son triviales excepto que $\Phi_n \in \mathbb{Z}[x]$, lo cual se demuestra por inducción fuerte empleando nuestro conocimiento sobre el caso primo. Y la tercera es equivalente a la segunda, que es la que vamos a probar.

Para ello, veremos lo siguiente: Si ω es una raíz n -ésima de la unidad primitiva cualquiera, $f(x) \in \mathbb{Q}[x]$ es su polinomio minimal y $p \nmid n$, entonces ω^p también es raíz de $f(x)$. Como todo número coprimo a n se obtiene multiplicando primos que no dividen a n , entonces al comprobar ésto veremos que necesariamente f tiene por raíces a todas las raíces n -ésimas primitivas de la unidad, por lo que $f = \Phi_n$.

Definamos $h(x)$ tal que $x^n - 1 = f(x)h(x)$, y supongamos, por contradicción, que ω^p no es raíz de $f(x)$. Entonces ω^p es raíz de $h(x)$, es decir, ω es raíz de $h(x^p)$ y como f es el polinomio minimal de ω se cumple que existe

$g \in \mathbb{Q}[x]$ tal que

$$h(x^p) = f(x)g(x).$$

Y como h, f tienen coeficientes enteros, entonces g también. Luego, podemos llevar la igualdad anterior a \mathbb{F}_p y notar que $h(x^p) \equiv h(x)^p \pmod{p}$, 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 4.73: 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 γ 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 ζ una n -ésima raíz primitiva de la unidad, entonces como $\zeta \in k$, entonces $\sigma\zeta = \zeta$ y por lo tanto,

$$\zeta \cdot \sigma(\zeta) \cdots \sigma^{n-1}(\zeta) = \zeta^n = 1,$$

El lema de independencia de 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 γ 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 4.74: 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 γ es una raíz, entonces $k(\gamma)$ es cíclica de grado p .
2. Si K/k es una extensión cíclica de grado p , entonces $K = k(\gamma)$ donde γ es raíz de $f_a(x)$ para algún $a \in k$.

DEMOSTRACIÓN:

1. Basta notar que si γ es raíz y $b \in \mathbb{F}_p$, entonces $\gamma + b$ es raíz de $f_a(x)$ (por el sueño del aprendiz y el pequeño teorema de Fermat); ésto nos otorga todas las p raíces del polinomio.
2. Como K es cíclica, sea $\langle \sigma \rangle = \text{Gal}(K/k)$. Por el lema de independencia de Dedekind existe $\beta \in K$ tal que $\sum_{i=1}^p \sigma^i(\beta) \neq 0$. Definamos

$$\delta := \sigma\beta + 2\sigma^2\beta + \cdots + (p-1)\sigma^{p-1}\beta.$$

Luego se tiene que $\delta - \sigma\delta = \sigma\beta + \sigma^2\beta + \cdots + \sigma^{p-1}\beta - (p-1)\beta = \sum_{i=1}^p \sigma^i(\beta) \neq 0$, de modo que $\delta \notin k$ y necesariamente $K = k(\delta)$ (puesto que un grupo de orden p es simple). Es fácil notar que $\sigma^i\delta - \sigma^{i+1}\delta = \delta - \sigma\delta =: f$, por lo que, los conjugados de δ son $\delta, \delta + f, \dots, \delta + (p-1)f$. 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 $b \in \mathbb{F}_p$ syss es raíz de $x^p - x = \prod_{b \in \mathbb{F}_p} (x - b)$, de lo que se sigue que $\gamma^p - \gamma = a$, o equivalentemente, que γ es raíz de $f_a(x) \in k[x]$. \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 4.75: Se dice que una extensión $k(\alpha)/k$ es *pura* si $\alpha^m \in k$ para algún α . Se dice que una extensión finita K/k es *radical* si existe una cadena de extensiones de cuerpos:

$$K =: K_0 \supseteq K_1 \supseteq \cdots \supseteq K_n = k$$

tales que K_i/K_{i+1} es una extensión pura.

La definición de extensión radical ya debería hacer eco de los grupos resolubles, pero además debería tener sentido ésta definición. De hecho, la fórmula cuadrática ya nos otorga una demostración constructiva de que toda extensión de grado 2 de \mathbb{Q} es radical.

Sin embargo, una observación vital es que ésta definición puede parecer no ser tan general, dado que no necesariamente se cumpliría que toda subextensión de una radical sea también radical, por ello se define lo siguiente:

Definición 4.76: Una extensión es *resoluble (por radicales)* si está contenida en otra extensión radical.

Proposición 4.77: Se cumplen:

1. $\text{Gal}(k(\zeta_n)/k)$ es abeliano.
2. Sea α raíz del polinomio irreducible $x^n - \beta \in k[x]$ y supongamos que $\zeta_n \in k$. Entonces $\text{Gal}(k(\alpha)/k)$ 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 ζ_n , un \mathbb{Q} -automorfismo σ está completamente determinado por su valor en ζ_n , en particular denotemos $\sigma_j(\zeta_n) = \zeta_n^j$. Nótese que σ_j determina un automorfismo $\text{syss}(j; n) = 1$. 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. γ es otra raíz de $x^n - \beta$ $\text{syss}(\gamma/\alpha)^n = \beta/\beta = 1$, vale decir, si γ/α es una raíz n -ésima de la unidad. Pero por hipótesis k posee a todas las raíces n -ésimas de la unidad, luego $k(\alpha)/k$ es una extensión normal. Más aún, es claro que el grupo de automorfismos es abeliano puesto que todos son de la forma $\sigma_j(\alpha) = \alpha\zeta_n^j$.
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 $\text{Gal}(N/k)$:

$$\text{Gal}(N/k) = \text{Gal}(N/N_0) \supseteq \text{Gal}(N/N_1) \supseteq \dots \supseteq \text{Gal}(N/N_{2n}) = \{1\}.$$

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 4.78: Toda extensión separable radical está contenida en una extensión de Galois radical.

DEMOSTRACIÓN: Sea K/k una extensión separable radical, en particular es una extensión finita y por el teorema del elemento primitivo se cumple que $K = k(\alpha)$ y consideremos la clausura normal L de K que está generada por el resto de raíces del polinomio minimal de α . Como K es radical sea una cadena de extensiones puras:

$$K = k(\beta_1, \dots, \beta_n) \supseteq \dots \supseteq k(\beta_1) \supseteq k$$

donde $\beta_i^{n_i} = r_i$. Entonces elijamos a un conjugado de α , éste ha de ser de la forma $\sigma(\alpha)$ donde $\sigma \in \text{Gal}(L/k)$. Luego podemos construir la siguiente cadena de extensiones puras:

$$K = k(\gamma_1, \dots, \gamma_n) \supseteq \dots \supseteq k(\gamma_1) \supseteq k$$

donde $\gamma_i := \sigma(\beta_i)$ y es pura pues $\gamma_i^{n_i} = \sigma(r_i)$. Luego $\sigma(\alpha)$ se obtiene con la misma combinación para α sustituyendo β_i por γ_i . Haciendo lo mismo para el resto de raíces se obtiene que L es radical y claramente es de Galois. \square

Finalmente bastaría encontrar un cuerpo de Galois cuyo grupo no fuese resoluble (como S_5) para poder concluir y, en efecto:

Ejemplo. Considere el polinomio $p(x) = x^5 - 4x + 2 \in \mathbb{Q}$. Por el criterio de Eisenstein se concluye que $p(x)$ es irreducible, veamos lo siguiente: $p(x)$ debe tener tres raíces reales y dos complejas: ésto debido a que $\lim_{x \rightarrow \pm\infty} p(x) = \pm\infty$, a que $p(0) = 2$ y $p(1) = -1$, y que $p'(x) = x^4 - 4$ tiene por únicas raíces $\pm\sqrt{2}$. Así pues, llamemos K al cuerpo de escisión de $p(x)$.

Como \mathbb{Q} es perfecto, entonces K es separable y $p(x)$ tiene cinco raíces distintas; luego claramente $\text{Gal}(\mathbb{Q}/K) \leq S_5$, dado que cada automorfismo de K permuta las cinco raíces. ...

Completar demostración de que su grupo de Galois no es soluble.

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 4.79: 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, π y π^2 son elementos trascendentes (ésto lo probaremos más adelante), pero claramente sí poseen una relación entre ambos.

Proposición 4.80: 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. 2.68). Como S es algebraicamente independiente, entonces se concluye que \tilde{f} tiene núcleo nulo, luego es un k -monomorfismo. Como $k[S]$ es un dominio íntegro, cuyo cuerpo de fracciones es $k(S)$ y \tilde{f} es un monomorfismo, entonces admite una única extensión $\bar{f}: k(S) \rightarrow k(S')$ (teo. 2.61). Finalmente como \bar{f} es un k -monomorfismo y $S' \subseteq \text{Im } \bar{f}$, entonces \bar{f} es un k -isomorfismo. \square

Corolario 4.81: 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 4.82: 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: \implies . 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 β es trascendente, ésto implica que $h = 0 \in k(S)[y]$, y luego $a_j = 0$ para todo j . Pero S es algebraicamente independiente, luego $g_j = 0 \in k[x_1, \dots, x_n]$, de lo que se sigue que f es el polinomio nulo.

\Leftarrow . Ejercicio para el lector. □

Definición 4.83: 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 4.84: 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) 4.85: Sea K/k una extensión de cuerpos y sea $S \subseteq K$.

1. Si $K/k(S)$ es una extensión algebraica, entonces S contiene alguna base de trascendencia.
2. Si S es algebraicamente independiente, entonces S se extiende a alguna base de trascendencia.

DEMOSTRACIÓN: Veamos la 1: Por el lema de Zorn, sea $T \subseteq S$ un subconjunto algebraicamente independiente \subseteq -maximal. Entonces, por la proposición 4.82 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) 4.86: 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 4.82, 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. 3.29). \square

Definición 4.87: 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 4.88: 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) 4.89: 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 $\bar{f}: k(S) \rightarrow k(T)$, 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

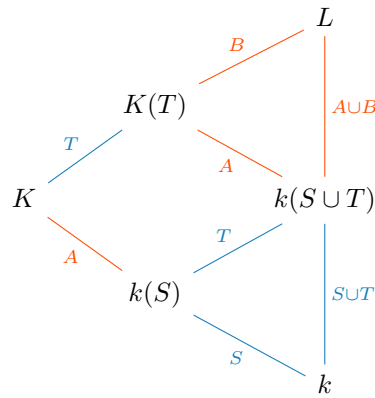
Corolario (AE) 4.90: Sea K un cuerpo no numerable cuyo cuerpo primo es k , entonces $\text{trdeg}(K/k) = |K|$. En consecuencia, dos cuerpos no numerables algebraicamente cerrados de igual característica son isomorfos syss tienen la misma cardinalidad.

Teorema 4.91: 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 4.92: 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 4.93: 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. □

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 4.94: Sea $\varphi = g(x)/h(x) \in k(x)$ no constante con $g(x), h(x)$ coprimos. Entonces:

1. φ es k -trascendente.
2. $k(x)/k(\varphi)$ es una extensión finita de cuerpos.

3. El polinomio minimal de x sobre $k(\varphi)$ es

$$\theta(y) := g(y) - \varphi \cdot h(y) \in k(\varphi)[y],$$

de modo que $[k(x) : k(\varphi)] = \text{alt } \varphi$.

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 2.88. \square

Corolario 4.95: Sea $\varphi \in k(x)$, entonces $k(x) = k(\varphi)$ syss $\varphi \in (k)$.

Teorema 4.96 – 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 2.90), de modo que $\deg_x(a^*) + m \leq m$ y necesariamente $\deg_x(a^*) = 0$, es decir, $a^* \in k[y]$. Pero como $\theta^*(y, x) = -\theta^*(x, y)$, entonces necesariamente $\deg_y(a^*) = 0$ también y, por ende, $a^* \in k$. Finalmente notamos que

$$m = \deg_x(\theta^*) = \deg_x(a^*) + \deg_x(I^*) = 0 + n,$$

lo que concluye el teorema. □

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 consecuencia, 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:

$$\bigoplus_{i \in I} M_i := \{(\mathbf{m}_i)_i \in \prod_{i \in I} M_i : \mathbf{m}_i = \vec{0} \text{ salvo finitos } i\text{'s}\}.$$

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 $\prod_{i \in I} M_i$ 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 ψ está bien definido ya que sólo finitos de los \mathbf{m}_i 's son no nulos.)

En consecuencia, 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 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:

$$\begin{array}{ccc}
\bigoplus_{i \in I} M_i & \xrightarrow{\sum_{i \in I} \varphi_i} & \bigoplus_{i \in I} (M_i/S_i) \\
\uparrow & \nearrow \varphi_j & \uparrow \\
M_j & \longrightarrow & M_j/S_j
\end{array}$$

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:

$$\begin{array}{ccccc}
T & & & & \\
\downarrow \exists! \bar{g} & \searrow g & & & \\
\ker f & \xrightarrow{\iota} & M & \xrightarrow[\quad 0_{M,N}]{\quad f \quad} & N
\end{array}$$

En consecuencia, $\ker f$ 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:

$$\begin{array}{ccc} & & T \\ & \nearrow g & \uparrow \exists! \bar{g} \\ M \xrightarrow[\text{0}_{M,N}]{f} N & \xrightarrow{\pi} & \text{coker } f \end{array}$$

En consecuencia, $\text{coker } f$ 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 5.17: 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 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 Mod_A . Éstos funtores se llaman *funtores de representación*.

En la teoría de conjuntos se demuestra que los funtores de representación siempre existen y están bien definidos; la sorpresa radica en que, en general, los conjuntos Hom 's no suelen ser elementos de la categoría y los funtores de representación tampoco suelen traducirse en flechas de la categoría; ésto indica que la categoría Mod_A es bastante especial.

Definición 5.18: Sea $F: \mathcal{A} \subseteq A\text{-Mod} \rightarrow \mathcal{B} \subseteq B\text{-Mod}$ 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 5.19: 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.

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 $N_n = N_m$.

Ejemplo. Todo cuerpo es noetheriano y artiniiano. Ya vimos también que todo DIP es noetheriano.

Ejemplo. \mathbb{Z} es un dominio euclídeo, luego es un DIP y luego es noetheriano. Sin embargo, no es artiniiano puesto que

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

es una cadena \subseteq -descendiente de ideales sin \subseteq -minimal.

Ejemplo. Ya vimos que $k[x_1, x_2, x_3, \dots]$ no es noetheriano, pero tampoco es artiniiano:

$$(x_1, x_2, x_3, \dots) \supset (x_2, x_3, \dots) \supset (x_3, \dots) \supset \cdots$$

Ahora, procedemos a dar varias propiedades de los módulos noetherianos que tendrán demostraciones análogas para los módulos artinianos que, en consecuencia, vamos a obviar.

Proposición 5.23: 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 5.24: 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 5.25: Si $\varphi: M \rightarrow N$ es un morfismo de A -módulos suprayectivo y M es noetheriano (resp. artiniiano), entonces N también.

§5.2.2 Módulos (semi)simples y el teorema de Jordan-Hölder.

Definición 5.26: Un A -módulo M no trivial se dice *simple* si sus únicos submódulos son $\{\vec{0}\}$ y M . M se dice *semisimple* si es la suma directa de (posiblemente infinitos) A -módulos simples.

Algo relativamente sencillo de probar es lo siguiente:

Proposición 5.27: Un A -módulo M es simple syss existe un ideal $\mathfrak{m} \triangleleft A$ maximal tal que $M \cong A/\mathfrak{m}$.

DEMOSTRACIÓN: \implies . 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 $\tilde{f}: A/\ker f \rightarrow M$ y $A/\ker f$ no posee submódulos impropios, luego $\ker f$ ha de ser un ideal maximal.

\impliedby . Es claro. \square

Por ende, parece más interesante analizar el caso de los módulos semi-simples:

Definición 5.28: Se dice que un A -módulo M es un *sumando directo* de N si existe M' tal que $N = M \oplus M'$.

Proposición (AE) 5.29: Un A -módulo M es semisimple syss todo submódulo $T \leq M$ es un sumando directo de M .

DEMOSTRACIÓN: \implies . 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).

\impliedby . 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 $u \notin C \oplus E$, 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) 5.30: Todo submódulo y todo cociente de un módulo semisimple es también semisimple.

Definición 5.31: Un ideal $\mathfrak{a} \trianglelefteq A$ no nulo se dice *minimal* 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 5.32: 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 5.33: El producto directo de finitos anillos semisimples es semisimple. En particular, el producto directo de finitos cuerpos es un dominio semisimple.

Definición 5.34: 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 5.35 – Teorema de Maschke: Sea G un grupo finito y k un cuerpo de característica p (posiblemente cero) tal que p no divide a $|G|$. Entonces $k[G]$ es un anillo semisimple izquierdo.^a

^aTécnicamente 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:

$$\begin{aligned} gD(x) &= \frac{1}{|G|} \sum_{h \in G} g h d(h^{-1}x) = \frac{1}{|G|} \sum_{h \in G} g h d(h^{-1}g^{-1}gx) \\ &= \frac{1}{|G|} \sum_{j=gh \in G} j d(j^{-1}gx) = D(gx), \end{aligned}$$

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 5.36 (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 5.37: 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 5.38: Un A -módulo posee una serie de composición syss es noetheriano y artiniano.

Teorema 5.39 (de refinamiento de Schreier): Dos series de un mismo A -módulo poseen al menos un refinamiento equivalente.

Teorema 5.40 – Teorema de Jordan-Hölder: Todas las series de composición de un A -módulo (si existen) son equivalentes.

Definición 5.41: 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) 5.42: Para un k -espacio vectorial V , las siguientes condiciones son equivalentes:

1. V tiene dimensión finita.
2. V tiene longitud finita.
3. V es noetheriano.
4. V es artiniano.

Más aún, si ese es el caso, entonces $\ell(V) = \dim_k(V)$.

DEMOSTRACIÓN: Es claro que $1 \implies 2$, y $2 \implies 3$ y $2 \implies 4$. Para ver que $3 \implies 1$, veamos la contrarrecíproca: Si V tiene dimensión infinita, entonces sea $\{x_n : n \in \mathbb{N}\}$ 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. \square

Proposición 5.43: 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 5.44: 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 5.45: 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 π_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 $e_1e_2 = e_1(1 - e_1) = 0 = e_2e_1$ (¿por qué?). Finalmente $M_i := e_i[M]$ satisface lo exigido. \square

Definición 5.46: Un A -módulo M se dice *fuertemente indecomposable* si $M \neq 0$ y $\text{End}(M)$ es un anillo local.

Lema 5.47: Sean M, N un par de A -módulos, con $M \neq 0$ y N indecomposable. 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 5.48: 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:

$$\begin{array}{ccccc} M & \xleftarrow{e_1} & M & & \\ \downarrow g & & \downarrow h_j & & \\ N & \xrightarrow{f_j} & N & \xrightarrow{f_j} & N \\ & & \downarrow \ell_j & & \downarrow g^{-1} \\ & & M & \xleftarrow{e_1} & M \end{array}$$

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

$$\vec{0} = e_1(\mathbf{x}) = (g^{-1} \circ e_1)(\mathbf{y}) = (f_1 \circ g^{-1} \circ e_1)(\mathbf{y}) = \ell'_j(\mathbf{y}),$$

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 5.49: 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 5.50 (Fitting): Sea M un A -módulo noetheriano y artinian, 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:

$$M \supseteq f[M] \supseteq f^2[M] \cdots \rightarrow f^\infty M, \quad \ker f \supseteq \ker(f^2) \supseteq \cdots \rightarrow f^{-\infty} 0.$$

Como M es artinian y noetheriano, existe n suficientemente grande tal que $f^n[M] = f^\infty M$ y $\ker(f^n) = f^{-\infty} 0$.

Sea $\mathbf{z} \in f^\infty M \cap f^{-\infty} 0$, entonces $\mathbf{z} = f^n(\mathbf{y})$ y $f^n(\mathbf{z}) = \vec{0}$, pero como $\ker(f^n) = \ker(f^{2n})$, entonces $f^{2n}(\mathbf{y}) = \vec{0}$, y $\mathbf{y} \in \ker(f^{2n}) = \ker(f^n)$, por lo que $\mathbf{z} = f^n(\mathbf{y}) = \vec{0}$. y en síntesis $f^n(\mathbf{z} - f^n(\mathbf{y})) = \vec{0}$.

Sea $\mathbf{x} \in M$, luego, $f^n(\mathbf{x}) \in f^n[M] = f^{2n}[M]$, por lo que $f^n(\mathbf{x}) = f^{2n}(\mathbf{y})$, luego $f^n(\mathbf{x} - f^n(\mathbf{y})) = \vec{0}$ y, por ende,

$$\mathbf{x} = f^n(\mathbf{y}) + (\mathbf{x} - f^n(\mathbf{y})) \in f^\infty M + f^{-\infty} 0. \quad \square$$

Corolario 5.51: Sea M un A -módulo noetheriano y artinian. 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 5.52 (Krull-Schmidt): Sea $M \neq 0$ un A -módulo noetheriano y artiniano, entonces existen M_i 's irreducibles 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 5.53: 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.

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.

Sean M, N un par de A -módulos, definimos la categoría $\text{Bil}(M \times N)$ como aquella que posee por objetos las aplicaciones bilineales desde $M \times N$,

y por flechas los morfismos de A -módulos que conmuten con las aplicaciones bilineales. Vale decir, $\varphi_1 \xrightarrow{\psi} \varphi_2$ en $\text{Bil}(M \times N)$ si y sólo si $\varphi_i: M \times N \rightarrow T_i$ es bilineal, $\psi: T_1 \rightarrow T_2$ es un morfismo de A -módulos y el siguiente diagrama conmuta:

$$\begin{array}{ccc} & & T_1 \\ & \nearrow \varphi_1 & \downarrow \psi \\ M \times N & & \\ & \searrow \varphi_2 & \downarrow \\ & & T_2 \end{array}$$

Definición 5.54: Un producto tensorial $M \otimes N$ es un objeto inicial de $\text{Bil}(M \times N)$; es decir, es tal que para toda aplicación A -bilineal $\varphi: M \times N \rightarrow T$ se cumple que el siguiente diagrama conmuta:

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi} & T \\ \downarrow \otimes & \nearrow \exists! \bar{\varphi} & \\ M \otimes N & & \end{array}$$

Teorema 5.55: 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:

$$\begin{array}{ccccc}
 & & \otimes & & \\
 & \nearrow & & \searrow & \\
 M \times N & \xrightarrow{j} & F(M \times N) & \xrightarrow{\pi} & M \otimes N
 \end{array}$$

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:

$$\begin{array}{ccc}
 M \times N & \xrightarrow{\varphi} & T \\
 j \downarrow & \nearrow \exists! \hat{\varphi} & \\
 F(M \times N) & &
 \end{array}$$

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:

$$\begin{array}{ccc}
 M \times N & \xrightarrow{\varphi} & T \\
 j \downarrow & \nearrow \hat{\varphi} & \\
 F(M \times N) & & \\
 \pi \downarrow & \nearrow \exists! \hat{\varphi} & \\
 M \otimes N = F(M \times N)/K & &
 \end{array}
 \quad \square$$

Definición 5.56: Los objetos de $M \otimes N$ se le llaman *tensores*. Nótese que como $M \times N$ es base de $F(M \times N)$, entonces son un 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 5.57: Si $M = \text{Span}_A(B)$ y $N = \text{Span}_A(C)$, entonces

$$M \otimes N = \text{Span}_A(\{\mathbf{b} \otimes \mathbf{c} : \mathbf{b} \in B, \mathbf{c} \in C\}).$$

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 $\dim_k(V \otimes W) \leq \dim_k(V) \cdot \dim_k(W)$. Pero ésta afirmación se puede mejorar.

Primero comenzaremos con la siguiente observación:

Teorema 5.58: Sean M, N, T un trío de A -módulos, entonces

$$\text{Hom}_A(M \otimes N, T) \cong \text{Hom}_A(M, \text{Hom}_A(N, T))$$

(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 $\bar{\alpha}: M \otimes N \rightarrow T$ (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. □

Ésto puede parecer un resultado parcialmente inofensivo, pero demuestra una intrínseca dualidad especial entre los tensores y los conjuntos Hom 's.

Proposición 5.59: Sean M, N, T un trío de A -módulos, entonces:

1. $M \otimes N \cong N \otimes M$.
2. $(M \oplus N) \otimes T \cong (M \otimes T) \oplus (N \otimes T)$.

3. En general, si $\{M_i\}_{i \in I}$ es una familia de A -módulos, entonces

$$\left(\bigoplus_{i \in I} M_i \right) \otimes T \cong \bigoplus_{i \in I} (M_i \otimes T).$$

4. En particular, $A^{\oplus X} \otimes A^{\oplus Y} \cong A^{\oplus(X \times Y)}$.

5. Más en particular, si k es cuerpo, entonces $k^n \otimes k^m = k^{nm}$.

6. $A \otimes M \cong M$ y $0 \otimes M \cong 0$.

7. $- \otimes N$ es un funtor exacto por la derecha.

8. Sea \mathfrak{a} un ideal de A , entonces

$$\frac{A}{\mathfrak{a}} \otimes M \cong \frac{M}{\mathfrak{a}M}.$$

9. Sean $\mathfrak{a}, \mathfrak{b}$ ideales de A , entonces

$$\frac{A}{\mathfrak{a}} \otimes \frac{A}{\mathfrak{b}} \cong \frac{A}{\mathfrak{a} + \mathfrak{b}}.$$

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,

$$\varphi_i \in \text{Hom}_A(M_i \otimes T, N) \iff \bar{\varphi}_i \in \text{Hom}_A(M_i, \text{Hom}_A(T, N));$$

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 $\psi \in \text{Hom}((\bigoplus_{i \in I} M_i) \otimes T, N)$. Queda al lector comprobar que ψ 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 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

$$\mathfrak{a} \otimes M \longrightarrow A \otimes M \cong M \longrightarrow A/\mathfrak{a} \otimes M \longrightarrow 0 \otimes M \cong 0$$

Nótese además que $\mathfrak{a} \otimes M \cong \mathfrak{a}M$. Luego existe una transformación canónica que completa el que $A/\mathfrak{a} \otimes M \cong M/\mathfrak{a}M$. \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.

Definición 5.60: Se dice que el A -módulo N es *plano* si $- \otimes N$ es un funtor exacto.

Proposición 5.61: Un A -módulo $M = \bigoplus_{i \in I} M_i$ es plano si y sólo si cada M_i es plano.

5.4 Módulos proyectivos e injectivos

Definición 5.62: 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 5.63: La suma directa de módulos proyectivos es proyectiva.

DEMOSTRACIÓN: Basta considerar el siguiente diagrama conmutativo:

$$\begin{array}{ccc}
 P_j & \hookrightarrow & \bigoplus_{i \in I} P_i \\
 \downarrow g_j & \swarrow \sum_{i \in I} g_i & \downarrow f \\
 M & \xrightarrow{p} & N
 \end{array}
 \quad \square$$

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 5.64: 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. \square

Corolario 5.65: El producto tensorial de finitos módulos proyectivos es proyectivo.

Proposición (AE) 5.66: 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:

$$\begin{array}{ccc} & P & \\ \swarrow & \downarrow \text{Id}_P & \\ N & \xrightarrow[p]{} P & \end{array}$$

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) 5.67: Los A -módulos proyectivos son planos.

Proposición (AE) 5.68 (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.

\Leftarrow . 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

$$s := \sum_{i \in I} \tau_i: P \longrightarrow F$$

$$\mathbf{x} \longmapsto \sum_{i \in I} f_i(\mathbf{x}) \mathbf{y}_i$$

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. □

Pese al nombre no se confunda, ni $\{\mathbf{x}_i\}_{i \in I}$ ni $\{f_i\}_{i \in I}$ tienen por que ser bases.

Dualizar el concepto de módulo proyectivo da:

Definición 5.69: Sea Q un A -módulo. Q se dice un *módulo inyectivo* si para todo par de A -módulos M, N , y todo $f: M \rightarrow Q$ y $q: M \rightarrow N$ homomorfismos de módulos, con q inyectivo, existe un $g: N \rightarrow Q$ tal que el siguiente diagrama:

$$\begin{array}{ccc} M & \xrightarrow{q} & N \\ f \downarrow & \swarrow g & \\ Q & & \end{array}$$

conmuta.

Proposición (AE) 5.70: El producto de módulos inyectivos es inyectivo.

Proposición 5.71: Un A -módulo Q es inyectivo syss el funtor $\text{Hom}_A(-, Q)$ es exacto.

Proposición (AE) 5.72 (criterio de Baer): Un A -módulo Q es inyectivo syss todo homomorfismo $f: \mathfrak{a} \rightarrow Q$, donde \mathfrak{a} es un ideal de A , posee una extensión $g: A \rightarrow Q$.

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 $\mathbf{x} \in M \setminus \tilde{N}$ y consideremos a $\tilde{N} + A \cdot \mathbf{x} \supset \tilde{N}$, y definamos

$$\mathfrak{a} := \{r \in A : r\mathbf{x} \in \tilde{N}\}.$$

Nótese que $\mathfrak{a} = \text{Ann}(A \cdot \mathbf{x} + \tilde{N})$ en M/\tilde{N} , de modo que es un ideal de A e induce el siguiente homomorfismo de módulos:

$$\begin{aligned} h: \mathfrak{a} &\longrightarrow M \\ r &\longmapsto g(r\mathbf{x}) \end{aligned}$$

Por hipótesis h se extiende a $\bar{h}: A \rightarrow M$. Luego nótese que $\bar{g}(r\mathbf{x} + \mathbf{n}) := \bar{h}(r\mathbf{x}) + g(\mathbf{n})$ para todo $\mathbf{n} \in \tilde{N}$ y todo $r \in A$, es un homomorfismo de módulos bien definido (¿por qué?) que extiende a g ; lo que contradice la maximalidad de (\tilde{N}, g) . \square

Definición 5.73: Se dice que un A -módulo M es *divisible* por $a \in A_{\neq 0}$ si $a \cdot M = M$. M se dice un *módulo divisible* (a secas) si para todo $a \in A_{\neq 0}$ se cumple que $aM = M$.

Proposición 5.74: Todo cociente de un módulo divisible es divisible.

Proposición 5.75: Se cumplen:

1. Si A es un dominio íntegro, entonces todo A -módulo inyectivo es divisible.
2. (AE) Más aún, si A es un DIP, todo A -módulo divisible es inyectivo.

DEMOSTRACIÓN:

1. Sea Q un A -módulo inyectivo, sea $\mathbf{x} \in Q$ y $r \in A_{\neq 0}$. Como A es un dominio íntegro, admite cancelación y luego la aplicación $ar \mapsto a\mathbf{x}$ es un homomorfismo de módulos bien definido desde (a) hasta Q . Luego admite una extensión $\varphi: A \rightarrow Q$. 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 A -módulo divisible y sea $f: (r) \rightarrow M$ un homomorfismo de anillos, donde $r \in A$. 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 A hasta M que extiende a f , y concluimos por el criterio de Baer. \square

Corolario (AE) 5.76: Todo cociente de un módulo inyectivo es también un módulo inyectivo.

Lema 5.77: 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

Corolario (AE) 5.78: Todo \mathbb{Z} -módulo está encajado en un módulo divisible

Lema 5.79: Si Q es un \mathbb{Z} -módulo inyectivo, entonces $\text{Hom}_{\mathbb{Z}}(A, Q)$ es un A -módulo inyectivo.

DEMOSTRACIÓN: Hay que probar que si

$$0 \longrightarrow N \xrightarrow{f} N'$$

es una sucesión exacta (en $A\text{-Mod}$), entonces

$$0 \longleftarrow \text{Hom}_A(N, \text{Hom}_{\mathbb{Z}}(A, Q)) \xleftarrow{h_f} \text{Hom}_A(N', \text{Hom}_{\mathbb{Z}}(A, Q))$$

es una sucesión exacta (en $A\text{-Mod}$). Ya hemos visto en la sección de tensores que existe un isomorfismo canónico:

$$\varphi_N: \text{Hom}_{\mathbb{Z}}(N \otimes_A A, Q) \longrightarrow \text{Hom}_A(N, \text{Hom}_{\mathbb{Z}}(A, Q)),$$

Y sabemos que $N \otimes_A A = N$, luego se induce el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \text{Hom}_{\mathbb{Z}}(N, Q) & \xrightarrow{\varphi_N} & \text{Hom}_A(N, Q) \\ \text{Hom}_{\mathbb{Z}}(f, Q) \downarrow & & \downarrow h_f \\ \text{Hom}_{\mathbb{Z}}(N', Q) & \xrightarrow{\varphi_{N'}} & \text{Hom}_A(N', Q) \end{array}$$

finalmente como $\text{Hom}_{\mathbb{Z}}(f, Q)$ es suprayectivo y los φ 's son isomorfismos, se concluye que $h_f = \text{Hom}_A(f, \text{Hom}_{\mathbb{Z}}(A, Q))$ es suprayectivo, como se quería ver. \square

Teorema (AE) 5.80: Todo A -módulo está encajado en un A -módulo inyectivo.

Teorema (AE) 5.81: Sea Q un A -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:

$$\begin{array}{ccc} N' & \xrightarrow{q} & N \\ f \downarrow & \swarrow g \circ \pi & \uparrow \\ Q & & \\ \pi \uparrow & \nwarrow \exists! g & \\ M & & \end{array}$$

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 5.82: 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) 5.83: Un A -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) 5.84: 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:

$$\begin{array}{ccc} Q & \xhookrightarrow{k} & N \\ j \downarrow & \swarrow f & \\ Q_0 & & \end{array}$$

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) 5.85: 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:

$$\begin{array}{ccccc} M & \xrightarrow{\iota} & Q & \xrightarrow{k} & N \\ & \searrow \iota_0 & \downarrow f & \swarrow \ell & \\ & & Q_0 & & \end{array}$$

donde la existencia del ℓ 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 ℓ es un isomorfismo y Q es inyectivo por la proposición 5.83.

La unicidad queda de ejercicio para el lector. \square

Definición 5.86: Dado un A -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 5.87: 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 5.88: Se cumplen:

1. Todo grupo abeliano libre finitamente generado es isomorfo a \mathbb{Z}^n para algún n . Más generalmente, definiendo $\mathbb{Z}^{\oplus \kappa} := \bigoplus_{\alpha=1}^{\kappa} \mathbb{Z}$, se cumple que todo grupo abeliano libre es isomorfo a $\mathbb{Z}^{\oplus \kappa}$ para algún número cardinal κ .
2. Más aún, $\mathbb{Z}^n \cong \mathbb{Z}^m$ syss $n = m$. De modo que todo par de bases de un grupo abeliano libre finitamente generado son de igual cardinalidad.
3. (AE) $\mathbb{Z}^{\oplus \kappa} \cong \mathbb{Z}^{\oplus \mu}$ syss $\kappa = \mu$. De modo que todo par de bases de un grupo abeliano libre son de igual cardinalidad.

DEMOSTRACIÓN: Para probar la segunda y la tercera basta tomar un grupo abeliano libre G y considerar a $G/2G$ como \mathbb{F}_2 -espacio vectorial. Luego la unicidad de cardinalidad de bases de un espacio vectorial induce la unicidad de cardinalidad de bases como grupo abeliano libre. \square

Definición 5.89: Dado un grupo abeliano libre G , se denota por $\text{rank } G$ a la cardinalidad de cualquiera de sus bases.

Proposición 5.90: 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 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) 5.91: 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) 5.92: 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_β/M'_β es isomorfo a un ideal de A , pero todos los ideales de A son principales, luego o son el ideal nulo o son isomorfos (como A -módulos) a A . Si el ideal no es nulo, entonces por la proposición anterior se cumple que $M_\beta \cong M'_\beta \oplus \langle \mathbf{m}_\beta \rangle$ 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}_β '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 γ 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 γ . \square

Nótese que su F es finitamente generado, entonces no hay uso de elección.

Corolario (AE) 5.93: En un DIP todo módulo proyectivo es libre.

Éste teorema se puede mejorar, pero requiere más trabajo (ver teo. 6.48).

Corolario (AE) 5.94: En un DIP todo submódulo de un módulo proyectivo es también proyectivo.

5.6 ¿Por qué las cosas fallan?

Para entender por qué la teoría de módulos es tan radicalmente distinta de la de los espacios vectoriales y los módulos libres, tenemos que volver a ellos para caracterizar su elegancia mediante otras perspectivas. Volvamos a la proposición 5.15, y consideremos lo siguiente:

Proposición 5.95: Sea k un cuerpo, entonces toda sucesión exacta:

$$0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow 0$$

en Vect_k se escinde. En consecuencia, $V \cong U \oplus W$.

De modo que por nuestra teoría de dimensión se cumple que si

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

es exacta, entonces $\dim V = \dim U + \dim W$.

Definición 5.96: Se dice que una sucesión

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots$$

es un *complejo de cadenas* si $\varphi_{i+1} \circ \varphi_i = 0$, o equivalentemente, si

$$\text{Img}(\varphi_{i+1}) \subseteq \ker(\varphi_i).$$

Un complejo de cadenas se dice *corto* si es finito. Dado un complejo de cadenas M_\bullet , entonces se define su *homología* como

$$H_i(M_\bullet) := \frac{\ker(\varphi_i)}{\text{Img}(\varphi_{i+1})},$$

en particular, una sucesión exacta es un complejo de cadenas cuya homología en todo punto es nula.

Dado un complejo corto de cadenas V_\bullet :

$$V_\bullet: \quad 0 \longrightarrow V_N \xrightarrow{\alpha_N} \cdots \longrightarrow V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

se define su *característica de Euler*:

$$\chi(V_\bullet) := \sum_{i=0}^N (-1)^i \dim(V_i).$$

Proposición 5.97: Sea V_\bullet un complejo corto de cadenas, entonces:

$$\chi(V_\bullet) := \sum_{i=0}^N (-1)^i \dim(H_i(V_\bullet)).$$

En particular, si V_\bullet es una sucesión exacta, entonces $\chi(V_\bullet) = 0$.

DEMOSTRACIÓN: Procedemos por inducción. El caso $N = 0$ es trivial. Si por hipótesis inductiva aplica para una sucesión exacta de N elementos definamos:

$$V_\bullet: \quad 0 \longrightarrow \cdots \longrightarrow V_N \xrightarrow{\alpha_N} \cdots \longrightarrow V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

$$V'_\bullet: \quad 0 \longrightarrow V_{N+1} \xrightarrow{\alpha_{N+1}} V_N \xrightarrow{\alpha_N} \cdots \longrightarrow V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

Luego nótese que

$$\chi(V'_\bullet) = \chi(V_\bullet) + (-1)^{N+1} \dim(V_{N+1}),$$

y como se satisface que

$$\forall 1 \leq i < N \quad H_i(V'_\bullet) = H_i(V_\bullet),$$

entonces, cancelando términos y dividiendo por $(-1)^{N+1}$, el problema se reduce a probar que

$$\begin{aligned} \dim(V_{N+1}) - \dim(H_N(V_\bullet)) &= \dim(H_{N+1}(V'_\bullet)) - \dim(H_N(V'_\bullet)) \\ \iff \dim(V_{N+1}) - \dim \ker(\alpha_N) &= \dim(\ker \alpha_{N+1}) - \dim\left(\frac{\ker \alpha_N}{\text{Im} \alpha_{N+1}}\right), \end{aligned}$$

lo que sigue de las fórmulas de la dimensión. \square

Nótese que la proposición anterior generaliza las fórmulas de Grassman.

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. \square

Proposición 6.3: Se cumplen:

1. Un dominio es un anillo local syss el conjunto de los elementos no inversibles constituye un ideal, en cuyo caso, corresponde al único ideal

maximal.

2. Sea A un anillo con un ideal maximal \mathfrak{m} tal que para todo $x \in \mathfrak{m}$ se cumpla que $1 + x$ es inversible. Entonces A es un anillo local.

DEMOSTRACIÓN: La primera es consecuencia de la proposición anterior.

Para la segunda sea $x \notin \mathfrak{m}$, luego por maximalidad $(x, \mathfrak{m}) = A$, es decir, $ax + y = 1$ para algún $a \in A, y \in \mathfrak{m}$. Luego $ax = 1 - y \in 1 + \mathfrak{m}$, por lo que es inversible y luego $(ax)^{-1}a = x^{-1}$. \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, λ_S un morfismo de módulos y todo elemento de S es inversible en $S^{-1}A$.

DEMOSTRACIÓN: Hay que ver primero que las operaciones están bien definidas: Para ello sean $a_1/s_1 = a_2/s_2$ tales que $r(a_1 s_2 - a_2 s_1) = 0$ con $r \in S$. Nótese que basta ver que

$$\frac{a_1 t + b s_1}{s_1 t} = \frac{a_2 t + b s_2}{s_2 t}, \quad \frac{a_1 b}{s_1 t} = \frac{a_2 b}{s_2 t}.$$

Para ello nótese que

$$\begin{aligned} r((a_1 t + b s_1) s_2 t - (a_2 t + b s_2) s_1 t) &= t^2 \cdot r(a_1 s_2 - a_2 s_1) = 0, \\ r(a_1 b s_2 t - a_2 b s_1 t) &= b t \cdot r(a_1 s_2 - a_2 s_1) = 0. \end{aligned}$$

Probar que es un anillo es análogo a las demostraciones de que $\text{Frac}(A)$ lo es. Lo mismo para notar que λ_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 $\mathfrak{a} \trianglelefteq A$.
2. Todos los ideales primos de $S^{-1}A$ son de la forma $S^{-1}\mathfrak{p}$ con $\mathfrak{p} \trianglelefteq A$ primo disjunto de S .

DEMOSTRACIÓN:

1. Sea $\mathfrak{b} \trianglelefteq S^{-1}A$ y definamos $\mathfrak{a} := \mathfrak{b} \cap A$. Sea $x = a/s \in \mathfrak{b}$, entonces $sx = a \in \mathfrak{b} \cap A = \mathfrak{a}$, de modo que $\mathfrak{b} = S^{-1}\mathfrak{a}$.
2. Sea $\mathfrak{q} \trianglelefteq S^{-1}A$ un ideal primo, entonces por el enunciado anterior $\mathfrak{p} := \mathfrak{q} \cap A \trianglelefteq A$ es un ideal primo (¿por qué?). Como $1 \notin \mathfrak{q}$ se sigue que $\mathfrak{p} \cap S = \emptyset$.

Conversamente sea $\mathfrak{p} \trianglelefteq A$ disjunto de S , y sea $\mathfrak{q} := S^{-1}\mathfrak{p}$, veamos que ha de ser un ideal primo: Supongamos que $\frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{q}$, de modo que como $s, t \in S$, existe $r \in S$ tal que $rab \in \mathfrak{p}$. Como \mathfrak{p} es primo y $r \notin \mathfrak{p}$, entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, de lo que se sigue que $a/s \in \mathfrak{q}$ o $b/t \in \mathfrak{q}$. \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 $(S^{-1}A, S^{-1}\mathfrak{p}, A/\mathfrak{p})$ es un anillo local. En éste caso, denotamos por $A_{\mathfrak{p}}$ a dicho anillo y le llamamos la *localización de \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 13).

Lema 6.11: El morfismo λ_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 $\lambda_S(b) = \lambda_S(0)$.

\Leftarrow . 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 α, β hacen conmutar al diagrama y sea $a/s \in S^{-1}A$, entonces

$$\alpha(a/s) = \alpha(a/1)\alpha(1/s) = \varphi(a)\varphi(s)^{-1} = \beta(a/1)\beta(1/s) = \beta(a/s).$$

□

Antes de seguir, nótese la siguiente observación:

Proposición 6.13: 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 6.14: Sea S un sistema multiplicativo de A y sea M un A -módulo, entonces la relación \sim sobre $M \times S$ dada por

$$(\mathbf{u}, s) \sim (\mathbf{v}, t) \iff \exists r \in S \quad r(\mathbf{u}t - \mathbf{v}s) = \vec{0}$$

es de equivalencia.

Proposición 6.15: $S^{-1}M$ 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, λ_S es inyectiva syss S no posee al cero ni a divisores de cero.

Proposición 6.16: Sea S un sistema multiplicativo de A . Entonces determina un functor covariante exacto entre los A -módulos:

$$\begin{array}{ccc} S^{-1}f: S^{-1}M_1 & \longrightarrow & S^{-1}M_2 \\ \mathbf{m}/s \longmapsto f(\mathbf{m})/s & & \end{array} \qquad \begin{array}{ccc} M_1 & & S^{-1}M_1 \\ f \downarrow & \xrightarrow{S^{-1}-} & \downarrow S^{-1}f \\ M_2 & & S^{-1}M_2 \end{array}$$

Proposición 6.17: Sea M un A -módulo. Entonces las siguientes son equivalentes:

1. $M = 0$.
2. $M_{\mathfrak{p}} = 0$ para todo $\mathfrak{p} \trianglelefteq A$ primo.
3. $M_{\mathfrak{m}} = 0$ para todo $\mathfrak{m} \trianglelefteq A$ maximal.

DEMOSTRACIÓN: Claramente $1 \implies 2 \implies 3$. Veamos $3 \implies 1$ por contrarrecíproca: Si $M \neq 0$ sea $\mathbf{m} \neq \vec{0} \in M$. Luego sea $\mathfrak{a} := \text{Ann}(\mathbf{m}) \neq (1)$.¹ 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

Ésto es un sumo útil, pues permite reducir varios problemas al caso de anillos locales, un ejemplo:

Corolario 6.18: Sea $\varphi: M \rightarrow N$ un homomorfismo de A -módulos. Entonces φ es inyectiva (resp. suprayectiva, isomorfismo) syss para todo $\mathfrak{m} \trianglelefteq A$ maximal se cumple que $\varphi_{\mathfrak{m}}: M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$ lo es.

Proposición 6.19: 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 $S^{-1}M$.

¹Véase def. 6.32.

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 6.20: 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 φ 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 $f(1/s \otimes \mathbf{m}) = \mathbf{m}/s = 0$ si y sólo si $\mathbf{m} = \vec{0}$. \square

Corolario 6.21: $S^{-1}A$ 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 6.24: 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 6.25: 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 $\mathfrak{N} := \text{Rad}(0)$, es decir, al conjunto de los elementos nilpotentes. Un dominio está *reducido* si $\mathfrak{N} = (0)$.

El corolario anterior entonces se puede reescribir así:

$$\mathfrak{N} = \bigcap \{\mathfrak{p} : \mathfrak{p} \trianglelefteq A \text{ primo}\}.$$

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) 6.26: Si \mathfrak{a} es un ideal de A , entonces

$$\text{Rad}(\mathfrak{a}) = \bigcap \{\mathfrak{p} : \mathfrak{a} \subseteq \mathfrak{p} \trianglelefteq A, \mathfrak{p} \text{ primo}\}.$$

Corolario 6.27: 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 6.28: Para todo sistema multiplicativo S de A se cumple que $S^{-1}\mathfrak{N}$ es el nilradical de $S^{-1}A$.

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 6.29: A es reducido syss $A_{\mathfrak{m}}$ es reducido para todo $\mathfrak{m} \triangleleft A$ maximal.

Proposición 6.30: 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 6.31: 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

$$\begin{aligned} \phi_n: A/\mathfrak{m}^n &\longrightarrow A_{\mathfrak{m}}/\mathfrak{n}^n \\ a + \mathfrak{m}^n &\longmapsto a + \mathfrak{n}^n \end{aligned}$$

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 ϕ_n es inyectiva.

Falta ver que ϕ_n es suprayectiva: para ello sea $a/s \in A_{\mathfrak{m}}$ con $a \in A, s \in S$. Todo ideal maximal que contiene a \mathfrak{m}^n contiene a $\text{Rad}(\mathfrak{m}^n) = \mathfrak{m}$, 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 6.32: 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

$$\text{Ann}(T) := (0 : T).$$

Se dice que un A -módulo M es *fiel* si $\text{Ann}(M) = 0$, i.e., si $a \mapsto am$ es una aplicación inyectiva.

Proposición 6.33: 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. $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = (\mathfrak{a} : \mathfrak{c} : \mathfrak{b})$.
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 6.34: 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 6.35: 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 6.36: 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:

$$\{\mathfrak{a} \trianglelefteq A : \mathfrak{a}^{ec} = \mathfrak{a}\} \xrightleftharpoons[()^c]{()^e} \{\mathfrak{b} \trianglelefteq B : \mathfrak{b}^{ce} = \mathfrak{b}\}$$

son biyecciones y son la una la inversa de la otra.

Proposición 6.37: 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[(\)^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. □

Proposición 6.38: Sea $\varphi: A \rightarrow B$ un morfismo de anillos, y sea $\mathfrak{p} \trianglelefteq A$ primo. Entonces \mathfrak{p} es la contracción de un ideal primo syss es la contracción de un ideal.

DEMOSTRACIÓN: \implies . Trivial.

\impliedby . 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 $\mathfrak{q}^c = \mathfrak{p}$. □

§6.1.4 El lema de Nakayama y sus consecuencias.

Definición 6.39: Dado un anillo A , se le llama su *radical de Jacobson* a

$$\mathfrak{J}(A) := \bigcap \{\mathfrak{m} : \mathfrak{m} \triangleleft A, \mathfrak{m} \text{ maximal}\}$$

Proposición 6.40: 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 6.41 – Teorema de Cayley-Hamilton: Sea M un A -módulo finitamente generado, $\varphi: M \rightarrow M$ un morfismo 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 esto 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 6.42 – 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 $M/\mathfrak{J}(A)M = \text{Span}_A\{[x_1], \dots, [x_n]\}$, entonces $M = \text{Span}_A\{x_1, \dots, x_n\}$.

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 $N = \text{Span}_A\{x_1, \dots, x_n\}$. □

Ejemplo. Considere a \mathbb{Q} , el cual es un $\mathbb{Z}_{(p)}$ -módulo, pero *no* es finitamente generado. Nótese que $p \cdot \mathbb{Q} = \mathbb{Q}$, pero $\mathbb{Q} \neq \{0\}$.

Definición 6.43: 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 6.44: Sea (A, \mathfrak{m}, k) un dominio local, sea M un A -módulo finitamente generado y sea $\bar{M} := M/\mathfrak{m}M$. Entonces:

1. \bar{M} es un k -espacio vectorial de dimensión finita n .
2. Si elegimos una base $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ para \bar{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 \bar{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 6.45: 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 6.46: Sea F un A -módulo que es una suma directa de módulos numerablemente generados. Si M es un sumando directo de F , entonces es también la suma directa de submódulos numerablemente generados.

DEMOSTRACIÓN: Sea $F = M \oplus N = \bigoplus_{\gamma < \kappa} E_\gamma$, donde cada E_γ es numerablemente generado. Queremos construir una familia $\{F_\alpha\}_{\alpha < \mu}$ con las siguientes propiedades:

1. Si $\alpha < \beta$, entonces $F_\alpha \subset F_\beta$.
2. $F = \bigcup_{\alpha < \mu} F_\alpha$.
3. $F_{\alpha+1}/F_\alpha$ es numerablemente generado.
4. $F_\alpha = M_\alpha \oplus N_\alpha$, donde $M_\alpha = M \cap F_\alpha$ y $N_\alpha = N \cap F_\alpha$.
5. Cada F_α es una suma directa de E_γ 's.

La construcción es por recursión transfinita: Definimos $F_0 := (0)$ y si λ es un ordinal límite, entonces $F_\lambda = \bigcup_{\delta < \lambda} F_\delta$. Para el caso del sucesor, sea $E_\gamma \not\subset F_{\alpha+1}$ 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_γ '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_α es un sumando directo de $M_{\alpha+1}$. Más aún,

$$\frac{F_{\alpha+1}}{F_\alpha} = \frac{M_{\alpha+1}}{M_\alpha} \oplus \frac{N_{\alpha+1}}{N_\alpha},$$

donde $M_{\alpha+1}/M_\alpha$ es numerablemente generado. Luego $M_{\alpha+1} = M_\alpha \oplus \tilde{M}_\alpha$, donde \tilde{M}_α es numerablemente generado. Definiendo $M_\lambda = 0$ para λ ordinal límite, finalmente se cumple que

$$M = \bigcup_{\alpha < \mu} \tilde{M}_\alpha. \quad \square$$

Lema 6.47: 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 $\mathbf{x} = a_1 \mathbf{y}_1 + \dots + a_n \mathbf{y}_n$ 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 6.48: 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

$$M = \bigoplus_{n=1}^{\infty} F_n.$$

\square

6.2 Descomposición primaria de anillos

Definición 6.49: Un ideal $\mathfrak{q} \triangleleft A$ (distinto de A), se dice *primario* si para todo $xy \in \mathfrak{q}$, entonces $x \in \mathfrak{q}$ o existe algún n tal que $y^n \in \mathfrak{q}$.

Equivalentemente, \mathfrak{q} es primario si A/\mathfrak{q} es no nulo y no posee nilpotentes no nulos.

Proposición 6.50: Si \mathfrak{q} es primario, entonces $\text{Rad } \mathfrak{q}$ es el mínimo ideal primo que contiene a \mathfrak{q} .

PISTA: Sólo basta probar que $\text{Rad } \mathfrak{q}$ es primo. \square

Definición 6.51: Si \mathfrak{q} es primario y $\mathfrak{p} = \text{Rad } \mathfrak{q}$, entonces \mathfrak{q} se dice *\mathfrak{p} -primario*.

Proposición 6.52: Si $\text{Rad } \mathfrak{a}$ es maximal, entonces \mathfrak{a} es primario. En particular, las potencias de un ideal maximal \mathfrak{m} son ideales \mathfrak{m} -primarios.

Lema 6.53: Sean $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ ideales \mathfrak{p} -primarios, entonces $\mathfrak{q} := \bigcap_{i=1}^n \mathfrak{q}_i$ también es \mathfrak{p} -primario.

DEMOSTRACIÓN: En primer lugar, nótese que

$$\text{Rad} \left(\bigcap_{i=1}^n \mathfrak{q}_i \right) = \bigcap_{i=1}^n \text{Rad}(\mathfrak{q}_i) = \mathfrak{p}.$$

Más aún, si $xy \in \mathfrak{q}$ con $y \notin \mathfrak{q}$, se cumple que existe un i tal que $xy \in \mathfrak{q}_i$ con $y \notin \mathfrak{q}_i$, luego $x^n \in \mathfrak{q}_i$ y luego $x \in \mathfrak{p}$. Por definición del radical se cumple que $x^n \in \mathfrak{q}$ para algún n . \square

Definición 6.54: Sea \mathfrak{a} un ideal. Una *descomposición primaria* de \mathfrak{a} es una expresión:

$$\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$$

con \mathfrak{q}_i primario. Una descomposición primaria es *minimal* si los $\text{Rad } \mathfrak{q}_i$'s son todos distintos. \mathfrak{a} se dice *decomposable* si posee alguna descomposición primaria.

Por el lema anterior toda descomposición primaria se puede reducir a una descomposición minimal, de ahí dicho concepto.

Lema 6.55: Sea $x \in A$ y \mathfrak{q} un ideal \mathfrak{p} -primario. Entonces:

1. Si $x \in \mathfrak{q}$ entonces $(\mathfrak{q} : x) = (1)$.
2. Si $x \notin \mathfrak{q}$ entonces $(\mathfrak{q} : x)$ es \mathfrak{p} -primario y, en particular, $\text{Rad}(\mathfrak{q} : x) = \mathfrak{p}$.
3. Si $x \notin \mathfrak{p}$ entonces $(\mathfrak{q} : x) = \mathfrak{q}$.

DEMOSTRACIÓN:

1. Es claro y de hecho aplica para todo ideal \mathfrak{q} no necesariamente primario.
2. Sea $yz \in (\mathfrak{q} : x)$ y $z \notin (\mathfrak{q} : x)$, vale decir, $(yz)x \in \mathfrak{q}$ pero $zx \notin \mathfrak{q}$. Luego $(yz)x = y(zx) \in \mathfrak{q}$, por lo que $y^n \in \mathfrak{q}$ para algún n y, por ser ideal, $y^n x \in \mathfrak{q}$, y luego $y^n \in (\mathfrak{q} : x)$.

Como $\mathfrak{q} \subseteq (\mathfrak{q} : x)$, entonces $\text{Rad } \mathfrak{q} \subseteq \text{Rad}(\mathfrak{q} : x)$; veremos la otra inclusión: Sea $t \in \text{Rad}(\mathfrak{q} : x)$, entonces $t^n \in (\mathfrak{q} : x)$ para algún n , vale decir, $t^n x \in \mathfrak{q}$, pero como $x \notin \mathfrak{q}$, entonces $(t^n)^m = t^{nm} \in \mathfrak{q}$ para algún m ; por ende, $t \in \text{Rad } \mathfrak{q}$.

3. Ejercicio para el lector. □

Definición 6.56: Dado un ideal $\mathfrak{a} \trianglelefteq A$ se dice que un ideal primo \mathfrak{p} está asociado a \mathfrak{a} si existe $x \in A$ tal que $(\mathfrak{a} : x) = \mathfrak{p}$. Se denota por $\text{As } \mathfrak{a}$ al conjunto de los ideales primos asociados a \mathfrak{a} .

Teorema 6.57: Sea $\mathfrak{a} \triangleleft A$ un ideal decomponible, con descomposición primaria minimal $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$. Entonces $\text{As}(\mathfrak{a}) = \{\text{Rad } \mathfrak{q}_i\}_{i=1}^n$. En consecuencia, toda descomposición primaria minimal posee los mismos radicales y tiene la misma longitud.

DEMOSTRACIÓN: Sea $x \in A$, luego

$$\text{Rad}(\mathfrak{a} : x) = \text{Rad} \left(\bigcap_{i=1}^n \mathfrak{q}_i : x \right) = \bigcap_{i=1}^n \text{Rad}(\mathfrak{q}_i : x) = \bigcap_{i=1}^n \mathfrak{p}_i.$$

Luego si $\text{Rad}(\mathfrak{a} : x)$ es primo, entonces es algún \mathfrak{p}_j .

Fijemos un j . Como la descomposición es minimal, entonces claramente existe $x \notin \mathfrak{p}_j$ tal que $x \in \mathfrak{q}_i$ para todo $i \neq j$. Por el lema anterior se cumple que:

$$\text{Rad}(\mathfrak{a} : x) = \bigcap_{\substack{i=1 \\ i \neq j}}^n \text{Rad}(\mathfrak{q}_i : x) \cap \text{Rad}(\mathfrak{q}_j : x) = \text{Rad}(1) \cap \text{Rad } \mathfrak{q}_j = \mathfrak{p}_j. \quad \square$$

Proposición 6.58: Sea \mathfrak{a} un ideal decomposable y $\mathfrak{p} \supseteq \mathfrak{a}$ un ideal primo. Entonces \mathfrak{p} contiene un ideal asociado a \mathfrak{a} . En consecuencia, los ideales primos minimales contenidos en \mathfrak{p} que contienen a \mathfrak{a} son exactamente los minimales de $\text{As } \mathfrak{a}$.

DEMOSTRACIÓN: Basta notar que

$$\mathfrak{p} = \text{Rad } \mathfrak{p} \subseteq \text{Rad } \mathfrak{a} = \bigcap_{i=1}^n \text{Rad } \mathfrak{q}_i = \bigcap_{i=1}^n \mathfrak{p}_i,$$

y recordar que como \mathfrak{p} es primo, entonces $\mathfrak{p} \supseteq \mathfrak{p}_j$ para algún j por la proposición 2.58. \square

Proposición 6.59: Si $\mathfrak{a} \triangleleft A$ es decomposable y $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ es una descomposición minimal con $\mathfrak{p}_i := \text{Rad } \mathfrak{q}_i$, entonces:

$$\bigcup_{i=1}^n \mathfrak{p}_i = \{x \in A : (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

En particular, la unión de todos los ideales primos asociados al (0) es igual a los divisores de cero de A .

Proposición 6.60: Sea S un sistema multiplicativo de A y \mathfrak{q} un ideal \mathfrak{p} -primario. Entonces:

1. $S \cap \mathfrak{p} \neq \emptyset$, entonces $S^{-1}\mathfrak{q} = S^{-1}A$.
2. $S \cap \mathfrak{p} = \emptyset$, entonces $S^{-1}\mathfrak{q}$ es $S^{-1}\mathfrak{p}$ -primario y su contracción es \mathfrak{q} .

DEMOSTRACIÓN:

1. Ejercicio para el lector.
2. $\mathfrak{q} = (S^{-1}\mathfrak{q})^c = \mathfrak{q}^{ec}$ syss ningún elemento de S es divisor de cero en A/\mathfrak{q} . Nótese que si existe $s \in S$ y $x \in A$ tales que $[sx] = 0$ en A/\mathfrak{q} con $[x] \neq 0$, entonces $x \notin \mathfrak{q}$ y por ende $x \notin \mathfrak{p}$, y además $s \notin \mathfrak{p}$, pero $sx \in \mathfrak{q} \subseteq \mathfrak{p}$, lo cual es absurdo dado que \mathfrak{p} es primo.

Comprobar la primalidad queda de ejercicio al lector. \square

Proposición 6.61: Sea S un sistema multiplicativo y \mathfrak{a} un ideal decomposable con descomposición minimal $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ tal que $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ son

disjuntos de S y $\mathfrak{q}_{m+1}, \dots, \mathfrak{q}_n$ cortan a S . Entonces:

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^m S^{-1}\mathfrak{q}_i, \quad S(\mathfrak{a}) = \bigcap_{i=1}^m \mathfrak{q}_i.$$

DEMOSTRACIÓN: Sabemos que S^{-1} distribuye uniones y el resto es aplicar la proposición anterior. \square

Definición 6.62: 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 6.63: 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 2.58, 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 6.64: 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 6.65: La suma directa de A -módulos noetherianos (resp. artinianos) es también noetheriano (resp. artiniano).

Reescribiendo el último teorema en lenguaje de sucesiones exactas:

Proposición 6.66: 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 6.67: 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 6.68: 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 6.69: 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).

Teorema (AE) 6.70 (Formanek): Sea A un dominio y M un A -módulo fiel finitamente generado. Si todos los submódulos de M de la forma $\mathfrak{a}M$, con $\mathfrak{a} \trianglelefteq A$, satisfacen la condición de la cadena ascendente; entonces A es noetheriano.

DEMOSTRACIÓN: Por el teorema anterior, basta notar que M es noetheriano. Procedemos por contradicción: si M no lo fuese, entonces considere la familia de submódulos:

$$\mathcal{F} := \{\mathfrak{a}M : \mathfrak{a} \triangleleft A, M/\mathfrak{a}M \text{ no es noetheriano}\}$$

luego $\{\vec{0}\} \in \mathcal{F}$, así que no es vacío y por hipótesis posee un elemento maximal $\mathfrak{a}M$. Sustituyendo M por $M/\mathfrak{a}M$ y A por $A/\text{Ann}(M/\mathfrak{a}M)$, podemos asumir que M no es noetheriano, pero que todos los módulos de la forma $M/\mathfrak{a}M$ con $\mathfrak{a} \neq (0)$ si lo son.

Sea

$$\mathcal{G} := \{N : N < M, M/N \text{ es fiel sobre } A\},$$

nótese que $\{\vec{0}\} \in \mathcal{G}$, y que se satisface que si $M = \text{Span}_A\{\mathbf{m}_1, \dots, \mathbf{m}_n\}$

$$N \in \mathcal{G} \iff \forall a \in A_{\neq 0} \{a\mathbf{m}_1, \dots, a\mathbf{m}_n\} \not\subseteq N.$$

Luego, aplicando el lema de Zorn, \mathcal{G} posee un elemento maximal N_0 . Si M/N_0 fuese noetheriano, entonces A lo sería y en consecuencia M también, lo que es absurdo. Así pues $\bar{M} := M/N_0$ posee las siguientes propiedades:

1. \bar{M} no es noetheriano.
2. Para todo $\mathfrak{a} \neq (0)$ ideal de A se cumple que $\bar{M}/\mathfrak{a}\bar{M}$ sí es noetheriano.
3. Para todo $N \neq (0)$ submódulo, \bar{M}/N no es fiel.

Sea N un submódulo arbitrario de \bar{M} . Como \bar{M}/N no es fiel, existe $a \in A_{\neq 0}$ tal que $a \cdot \bar{M}/N = 0$, es decir, $a\bar{M} \subseteq N$. Por la propiedad 2, $\bar{M}/(a)\bar{M}$ es noetheriano, luego $N/(a)\bar{M}$ es finitamente generado. Como \bar{M} es finitamente generado y $(a)\bar{M}$ también, entonces N es finitamente generado; luego \bar{M} es noetheriano, lo que es absurdo. \square

Como corolario:

Teorema (AE) 6.71 (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.

Definición 6.72: Sea $\mathfrak{a} \triangleleft A$ un ideal propio, entonces se dice que es *irreducible* si para todo $\mathfrak{b}, \mathfrak{c} \trianglelefteq A$ tales que $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ entonces $\mathfrak{a} = \mathfrak{b}$ o $\mathfrak{a} = \mathfrak{c}$.

Lema 6.73: En un dominio noetheriano A todo ideal es la intersección de finitos ideales irreducibles.

DEMOSTRACIÓN: Procedamos por contradicción: Como A es noetheriano podemos elegir un \subseteq -maximal \mathfrak{a} que no es la intersección de finitos ideales irreducibles, en particular, \mathfrak{a} ha de ser reducible, luego $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ con $\mathfrak{a} \subset \mathfrak{b}$ y $\mathfrak{a} \subset \mathfrak{c}$. Por maximalidad, $\mathfrak{b}, \mathfrak{c}$ han de ser la intersección de finitos irreducibles y luego \mathfrak{a} igual, lo que es absurdo. \square

Lema 6.74: En un dominio noetheriano A todo ideal irreducible es primario.

DEMOSTRACIÓN: Basta probar el caso en que si el ideal nulo es irreducible, entonces es primario. Sea $xy = 0$ con $y \neq 0$, hemos de probar que $x^n \in (0)$ para algún n , es decir, x es nilpotente. En primer lugar, por hipótesis $y \in \text{Ann}(x)$ y podemos construir la siguiente cadena \subseteq -ascendente de ideales:

$$\text{Ann}(x) \subseteq \text{Ann}(x^2) \subseteq \text{Ann}(x^3) \subseteq \cdots$$

que, como A es noetheriano, debe estabilizarse, vale decir, $\text{Ann}(x^n) = \text{Ann}(x^{n+1}) = \cdots$, para algún $n \in \mathbb{N}$.

Veamos que $(x^n) \cap (y) = (0)$: En efecto, sea $a \in (x^n) \cap (y)$, luego $ax = 0$ (por estar en (y)) y $a = bx^n$, por lo que $bx^{n+1} = 0$, es decir, $b \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n)$, por lo que $a = bx^n = 0$. Finalmente, como $(y) \neq (0)$ y (0) es primario, entonces $(x^n) = (0)$, es decir, $x^n \in (0)$ como se quería probar. \square

Teorema 6.75: En un dominio noetheriano todo ideal es decomponible.

Proposición 6.76: 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 6.77: En un anillo noetheriano el nilradical es nilpotente.

Corolario 6.78: 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 6.52.

$2 \implies 3$. Por la proposición anterior.

$3 \implies 2$. Basta aplicar radicales a la desigualdad. \square

Proposición 6.79: 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 6.80: En un anillo artiniiano, todo ideal primo es maximal.

Corolario 6.81: En un anillo artiniiano, el nilradical es igual al radical de Jacobson.

Teorema 6.82 – Teorema de Akizuki: Todo dominio noetheriano es artinian.

DEMOSTRACIÓN: Procedemos por contradicción: Supongamos que existe un dominio artinian 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 artinian). 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 artinian, 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 artinian de dimensión infinita; lo cual es absurdo. \square

Ejemplo 7: 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:

$$\langle p^{-1} \rangle \subset \langle p^{-2} \rangle \subset \langle p^{-3} \rangle \subset \dots$$

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.

Corolario 6.83: En un dominio artiniano el nilradical es nilpotente.

Definición 6.84: En un dominio A , se denota por $n := k\text{-dim } A$ 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 $k\text{-dim } A$ se le dice la *dimensión de Krull* del anillo.

Ahora podemos mejorar el teorema de Akizuki:

Proposición (AEN) 6.85: Sea A un dominio donde $(0) = \prod_{i=1}^n \mathfrak{m}_i$, donde \mathfrak{m}_i son ideales maximales (posiblemente iguales). Entonces A es noetheriano syss es artiniano.

DEMOSTRACIÓN: Definamos por recursión $\mathfrak{a}_0 := A$ y $\mathfrak{a}_{i+1} := \mathfrak{a}_i \cdot \mathfrak{m}_i$, entonces se tiene la siguiente cadena de ideales:

$$\mathfrak{a}_0 = A \supset \mathfrak{a}_1 = \mathfrak{m}_1 \supseteq \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n = (0).$$

Además $\mathfrak{a}_i/\mathfrak{a}_{i+1} = \mathfrak{a}_i/(\mathfrak{a}_i \cdot \mathfrak{m}_i)$ es un A/\mathfrak{m}_i -espacio vectorial (¿por qué?), luego los cocientes son noetherianos syss son artinianos. Luego empleando inducción, recordando que $\mathfrak{a}_{n-1}/\mathfrak{a}_n = \mathfrak{a}_{n-1}$ y empleando el teorema 6.64 se concluye el enunciado. \square

Teorema 6.86: Un dominio A es artiniano 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 $k\text{-dim } A = 0$.

\impliedby . Como el ideal nulo es decomposable, entonces A posee finitos ideales primos, los cuales son maximales puesto que $k\text{-dim } A = 0$. 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 6.85. \square

Corolario 6.87: 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 artinian.

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 artinian. \square

Teorema 6.88: Todo dominio artinian se escribe de manera única (salvo isomorfismo) como producto directo de finitos anillos artinianos locales.

DEMOSTRACIÓN: En todo dominio artinian 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 6.30), 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 artinian), 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 6.63, por lo que los $A_i \cong A/\mathfrak{a}_i$'s también lo son. \square

Proposición 6.89: Sea (A, \mathfrak{m}, k) un dominio artinian 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.

Cuerpos formalmente reales y cuadrados

Comenzamos el capítulo con la observación de que la prueba del teorema fundamental del álgebra dada en 4.56 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 σ es la conjugación, y notamos que éste también es un orden válido en el cual $\sqrt{2} <^* 0$.

Definición 7.4: Sea R un cuerpo arbitrario. Un *cono positivo* P es un subconjunto $P \subseteq R$ que satisface:

CP1. Si $a, b \in P$, entonces $a + b, ab \in P$.

CP2. Si $N := \{-a : a \in P\}$, entonces $P \cup N = R$ 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.

Teorema (AE) 7.11: Si R es formalmente real, entonces posee una extensión algebraica K que es realmente cerrada.

Aquí estaríamos tentados a decir que esta clase de extensiones se llaman *clausuras reales* pero aún falta probar unicidad.

Teorema 7.12: Sea R un cuerpo realmente cerrado. Entonces:

1. Para todo $a \in R$ existe $b \in R$ tal que $a = \pm b^2$.
2. R sólo posee un ordenamiento posible, o equivalentemente, sólo posee un cono positivo.
3. Todos los automorfismos de R son aplicaciones crecientes.¹

DEMOSTRACIÓN:

1. Supongamos que existe $a \in R$ tal que a no es un cuadrado. Entonces $K := R(\sqrt{a})$ es una extensión algebraica propia de R , de modo que no es formalmente real. Luego $-1 = \gamma_1^2 + \cdots + \gamma_n^2$ con $\gamma_j = b_j + c_j\sqrt{a} \in K$. Expandiendo nos queda que

$$-1 = \sum_{j=1}^n b_j^2 + a \left(\sum_{j=1}^n c_j^2 \right) + 2 \left(\sum_{j=1}^n b_j c_j \right) \sqrt{a}.$$

Analizando las coordenadas de K como R -espacio vectorial, y reordenando, nos queda que

$$1 + \sum_{j=1}^n b_j^2 + a \left(\sum_{j=1}^n c_j^2 \right) = 0 \iff -a = \frac{1 + \sum_{j=1}^n b_j^2}{\sum_{j=1}^n c_j^2}.$$

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.

¹Se suele emplear el término «orden-isomorfismo», pero creo que «creciente» es más visual fuera del contexto de conjuntos ordenados.

Teorema 7.13: Sea k un cuerpo de característica cero y K/k una extensión de cuerpos de grado impar. Dados $a_1, \dots, a_n \in k$ 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 α es raíz de un polinomio minimal $g(x) \in k[x]$ de grado $2m+1$. Por extensión de Kronecker sabemos que $K \cong k[x]/(g(x))$, 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 β es una raíz de h_1 , entonces definimos $L := k(\beta)$. Como los f_i 's son coprimos tenemos que las clases $[f_i] \in k[x]/(h_1(x)) \cong L$ no son todas nulas y, por lo tanto, determinan una solución no trivial en L . Luego procedemos recursivamente obteniendo soluciones en cuerpos de grado impar cada vez menor de modo que en un máximo de m pasos obtenemos una solución no trivial en k . \square

Teorema (AE) 7.14: Sea (R, \leq) un cuerpo ordenado y K/R una extensión finita de cuerpos tal que se da alguno de los casos:

- (a) $K = R(\sqrt{a})$ con $a > 0$.
- (b) $[K : R]$ es impar.

Entonces K es formalmente real y posee un orden que extiende al de R .

DEMOSTRACIÓN: Probaremos que el conjunto:

$$P := \left\{ \sum_{j=1}^n c_j \alpha_j^2 : c_j \in R, \alpha_j \in K, c_j > 0 \right\}$$

es un 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 $\alpha_i^2 = b_i^2 + ad_i^2 + 2b_i d_i \sqrt{a}$, de modo que, estudiando la primera coordenada se tiene que

$$0 = 1^2 + \sum_{i=1}^n (c_i b_i^2 + ac_i d_i^2),$$

donde todos los coeficientes yacen en R . Pero ésto es absurdo puesto que claramente el lado derecho es positivo. \square

Teorema (AE) 7.15: Sea R un cuerpo, entonces son equivalentes:

1. R es realmente cerrado.
2. Todo polinomio de grado impar en $R[x]$ posee raíz, y existe un ordenamiento bajo el cual todos los positivos son exactamente los cuadrados de R .
3. R no es algebraicamente cerrado y $R(i)$ (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 4.56.

$3 \implies 1$. 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

$$a^2 + b^2 = (c^2 - d^2)^2 + 4c^2 d^2 = (c^2 + d^2)^2.$$

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 7.16: Sea k un cuerpo de característica $p \neq 0$ con una extensión finita de cuerpos de grado p . Entonces para todo $n \in \mathbb{N}_{\neq 0}$ existe una cadena de extensiones

$$k = K_0 \subset K_1 \subset \cdots \subset K_n$$

tal que K_{i+1}/K_i es de grado p .

DEMOSTRACIÓN: Sea $a \in k$, definimos $\phi(a) := a^p - a$. Entonces, nótese que posee las siguientes propiedades:

1. $\phi(a) + \phi(b) = \phi(a + b)$.
2. Si $a \in k$ y $b \in \mathbb{F}_p$, entonces $\phi(ab) = b\phi(a)$.
3. $a \in \mathbb{F}_p$ syss $\phi(a) = 0$.
4. Si $a \notin \phi[k]$, entonces $f_a(x) = x^p - x - a$ es irreducible en $k[x]$

La 1 es el sueño del aprendiz, la 2 es corolario de la 1, la 3 es el pequeño teorema de Fermat y la 4 es parte del teorema 4.74.

Sea β raíz de $f_a(x)$, probaremos que $a\beta^{p-1} \notin \phi[k(\beta)]$: De lo contrario, para algún

$$\gamma = c_0 + c_1\beta + \cdots + c_{p-1}\beta^{p-1} \in k(\beta)$$

con $c_i \in k$, se tiene que $\gamma^p - \gamma = \phi\gamma = a\beta^{p-1}$. Como $\beta^p = \beta + a$ se tiene que

$$a\beta^{p-1} = \sum_{i=0}^{p-1} c_i^p (\beta^p)^i - \sum_{i=0}^{p-1} c_i \beta^i = \sum_{i=0}^{p-1} c_i^p (\beta + a)^i - \sum_{i=0}^{p-1} c_i \beta^i.$$

Como $1, \beta, \dots, \beta^{p-1}$ son linealmente independientes sobre k , podemos mirar los coeficientes de β^{p-1} y obtener la relación $a = c_{p-1}^{p-1} - c_{p-1} = \phi(c_{p-1})$; pero $a \notin \phi[k]$ lo que es absurdo. \square

Teorema (AE) 7.17: Sea K un cuerpo no algebraicamente cerrado, pero cuya clausura algebraica \overline{K}/K es una extensión finita. Entonces K es realmente cerrado y $\overline{K} = K(\sqrt{-1})$.

DEMOSTRACIÓN: Si $\overline{K} = K(\sqrt{-1})$, entonces basta aplicar el teorema 7.15, así que supondremos que $K(\sqrt{-1}) \subset \overline{K}$.

Si K no es un cuerpo perfecto, entonces tiene característica $p \neq 0$ y Frob_K no es un automorfismo (en particular, no es suprayectivo), de modo que existe $a \in K$ tal que para todo $b \in K$ se cumple que $x^p - a \in K[x]$ no posee raíces y así construimos una extensión de cuerpos $K \subset K[\sqrt[p]{a}]$ de grado p , y aplicamos el lema anterior.

Por el párrafo anterior, K debe ser perfecto y \overline{K} debe ser una extensión de Galois. Sea $G := \text{Gal}(\overline{K}/K(\sqrt{-1}))$ y, por el teorema de Cauchy, sea $H \leq G$ cíclico de orden primo q (luego es un grupo simple), y sea L su cuerpo fijado. Nótese que $q \neq p$ pues de lo contrario volvemos a aplicar el lema anterior para probar que la extensión es infinita. Sea ζ_n una q^n -ésima raíz primitiva de la unidad en \overline{K} . 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 $\overline{K} = L(\sqrt[q]{a})$ para algún $a \in L$ por el teorema 4.74. Sea γ una raíz de $x^{q^2} - a$, de modo que $x^{q^2} - a = \prod_{i=1}^{q^2} (x - \zeta_2^i \gamma)$. Como $[\overline{K} : L] = q$, entonces $x^{q^2} - a$ es reducible sobre L , así pues posee algún factor irreducible mónico $h(x)$ de grado q . El coeficiente libre de $h(x)$ es de la forma $\gamma^q \zeta_2^j$. Como γ^q es raíz de $x^q - a$, entonces $\gamma^q \notin L$ y luego $\overline{K} = L(\zeta_2)$.

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 4.68, 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 7.18: Sea k un cuerpo arbitrario. Se le llama el *nivel*² del cuerpo, denotado $s(k)$, al mínimo n tal que

$$-1 = a_1^2 + \cdots + a_n^2,$$

donde $a_i \in k$. Si k es formalmente real, denotamos $s(k) := \infty$.

El objetivo de ésta sección es entender qué clase de valores puede tomar $s(k)$ (además de ∞).

Ejemplo. • Por la ley de reciprocidad cuadrática, si $p = 2$ o $p \equiv 1 \pmod{4}$ 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.

Teorema 7.19: Sea k un cuerpo arbitrario y sea $n = 2^m$. Entonces existen identidades de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \quad (7.1)$$

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

²de. Stufe.

$T := [t_{ij}]_{ij}$, entonces se reescribe como

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = T \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Empleando productos internos podemos reescribir la identidad como

$$\begin{aligned} (x_1^2 + \cdots + x_n^2)(y_1, \dots, y_n) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} &= (z_1, \dots, z_n) \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \\ &= (y_1, \dots, y_n) t^t t \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \end{aligned}$$

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:

$$\begin{aligned} (x_1^2 + \cdots + x_n^2) I_n &= \mathbf{X}_1 \mathbf{X}_1^t I_n = T_1 T_1^t = T_1^t T_1, \\ (x_{n+1}^2 + \cdots + x_{2n}^2) I_n &= \mathbf{X}_2 \mathbf{X}_2^t I_n = T_2 T_2^t = T_2^t T_2. \end{aligned}$$

Queremos encontrar un T que funcione para ambas matrices en simultáneo.

Sea $T := \begin{pmatrix} T_1 & T_2 \\ T_2^t & M \end{pmatrix}$, entonces se tiene que

$$\begin{aligned} T^t T &= \begin{bmatrix} T_1^t T_1 + T_2^t T_2 & T_1^t T_2 + T_2^t M \\ T_2^t T_1 + M^t T_2 & T_2^t T_2 + M^t X \end{bmatrix} \\ &= \begin{bmatrix} (x_1^2 + \cdots + x_{2n}^2) I_n & A \\ B & C \end{bmatrix}. \end{aligned}$$

Y queremos elegir a M de modo que $A = B = 0$ y $C = (x_1^2 + \cdots + x_{2n}^2)I_n$. Para forzar las primeras dos condiciones elegimos $M = -(T_2^t)^{-1}T_1^{-1}T_2$ (¿por qué?), pero milagrosamente también satisface la tercera condición:

$$\begin{aligned} C &= T_2^t T_2 + M^t M = (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + T_2^t T_1 T_2^{-1} (T_2^t)^{-1} T_1^t T_2 \\ &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + (x_{n+1}^2 + \cdots + x_{2n}^2)^{-1} T_2^t T_1 T_1^t T_2 \\ &= (x_{n+1}^2 + \cdots + x_{2n}^2)I_n + (x_1^2 + \cdots + x_n^2)I_n. \end{aligned}$$

Ésto completa la demostración. \square

Lema 7.20 (Cassels): Sea $f(x) \in k[x] \subseteq k(x)$. Si $f(x)$ es una suma de n cuadrados en $k(x)$, entonces también es una suma de n cuadrados en $k[x]$.

DEMOSTRACIÓN: Veamos un par de casos aislados:

- (a) Si $n = 1$, entonces es trivial.
- (b) Si $\text{car } k = 2$, 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 γ_j es o bien nulo, o bien

$\deg \gamma_j < \deg \zeta$. Nótese que, por minimalidad de ζ , existe algún j tal que $\gamma_j \neq 0$. Definamos

$$\begin{aligned}\alpha &:= \sum_{i=1}^n \lambda_i^2 - f, & \beta &:= \sum_{i=1}^n \lambda_i \eta_i - f\zeta, \\ \bar{\zeta} &:= \alpha\zeta - 2\beta, & \bar{\eta}_j &:= \alpha\eta_j - 2\beta\lambda_j.\end{aligned}$$

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 4β común y expandiendo la definición de α, β 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

$$\begin{aligned}\bar{\zeta} &= \left(\sum_{j=1}^n \left(\frac{\eta_j^2}{\zeta^2} - \frac{2\eta_j\Lambda_j}{\zeta} + \Lambda_j^2 \right) - f \right) \zeta - 2 \left(\sum_{j=1}^n \left(\frac{\eta_j}{\zeta} - \Lambda_j \right) \eta_j - f\zeta \right) \\ &= (\Lambda_1^2 + \dots + \Lambda_n^2)\zeta = \frac{1}{\zeta} \sum_{j=1}^n \gamma_j^2.\end{aligned}$$

Como $s(k) \geq n$, mirando el mayor coeficiente de γ_j^2 concluimos que la suma es no nula.

- (III) $\deg(\bar{\zeta}) < \deg \zeta$: Por la última igualdad tenemos que $\zeta \cdot \bar{\zeta} = \sum_{j=1}^n \gamma_j^2$, de modo que $\deg \zeta + \deg \bar{\zeta} = 2 \max_j (\gamma_j) < 2 \deg \zeta$ (puesto que $\deg \gamma_j < \deg \zeta$ para todo j), de modo que $\deg(\bar{\zeta}) < \deg \zeta$.

Ésto contradice la minimalidad del grado de ζ lo que es absurdo. \square

Varios corolarios:

Corolario 7.21: 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 7.22: Sea k un cuerpo arbitrario. Denotemos por $G_n(k)$ a los elementos no nulos que se pueden escribir con n cuadrados, donde n es una potencia de 2. Entonces $G_n(k)$ es un grupo con la multiplicación.

DEMOSTRACIÓN: Ésto sale del teorema 7.19. \square

Corolario 7.23: 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 $x^2 + d = p_1(x)^2 + \dots + p_n(x)^2$ con $p_i(x) \in k[x]$ de grado ≤ 1 . Luego $p_i = a_i x + b_i$ y tenemos

$$x^2 + d = (a_1 x + b_1)^2 + \dots + (a_n x + b_n)^2,$$

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

$$\cancel{C}^2 + d = (a_1 C + b_1)^2 + \dots + (a_{n-1} C + b_{n-1})^2 + \cancel{C}^2,$$

con lo que comprobamos que d se escribe como suma de $n - 1$ cuadrados. \square

Corolario 7.24: 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 7.25: Sea k un cuerpo no formalmente real. Entonces $s(k)$ es una potencia de 2. Recíprocamente, dada la potencia 2^m existe un cuerpo k tal que $s(k) = 2^m$.

DEMOSTRACIÓN:

(I) Los niveles son potencias de 2: Nótese que siempre existe m tal que

$$n := 2^m \leq s(k) < 2^{m+1} = 2n.$$

Así pues, sea $a_1^2 + \cdots + a_n^2 + a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1 = 0$ para algunos $a_i \in k$ (posiblemente nulos). Sean

$$A := a_1^2 + \cdots + a_n^2, \quad B := a_{n+1}^2 + \cdots + a_{2n-1}^2 + 1,$$

Como $s(k) \geq n$ entonces podemos elegir los a_i 's de modo que $A \neq 0 \neq B$ y la condición se traduce en que $A+B=0$, o equivalentemente, $A=-B$. Por definición $A, B \in G_n(k)$, de modo que $A/B = -1 \in G_n(k)$, por ser grupo multiplicativo, luego -1 se escribe como una suma de n cuadrados y $s(k) \leq n$. Por antisimetría del \leq , $s(k) = n$ como se quería probar.

(II) Las potencias de 2 son niveles: El caso $n=1$ es conocido (e.g., $s(\mathbb{C})=1$). Sea $n=2^m > 1$ y sean $k := \mathbb{R}(x_1, \dots, x_{n+1})$ y $L := k(\gamma)$, donde los x_i 's son indeterminadas (elementos trascendentes algebraicamente independientes) y γ es raíz del polinomio:

$$\gamma^2 + x_1^2 + \cdots + x_{n+1}^2 = 0,$$

dividiendo por γ^2 se concluye que $s(L) \leq n+1$ y por ende $s(L) \leq n$ puesto que tiene que ser una potencia de 2.

Si $s(L) < n$, entonces existen $t_1, \dots, t_n \in L$ tales que

$$t_1^2 + \cdots + t_n^2 = 0.$$

Como L/k es una extensión de grado 2, entonces cada $t_i = \alpha_i \gamma + \beta_i$. Luego, la igualdad superior se reescribe como

$$\left(\gamma^2 \cdot \sum_{i=1}^n \alpha_i^2 + \sum_{i=1}^n \beta_i^2 \right) + 2\gamma \sum_{i=1}^n \alpha_i \beta_i = 0.$$

Como k es formalmente real, entonces algún α_i es no nulo, y análogamente se puede ver que algún β_i es no nulo. Enfocándonos en el primer paréntesis, nos queda que

$$-\gamma^2 = x_1^2 + \cdots + x_{n+1}^2 = \frac{\sum_{i=1}^n \beta_i^2}{\sum_{i=1}^n \alpha_i^2} \in G_n(k),$$

puesto que $G_n(k)$ es un grupo bajo multiplicación. Pero 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 7.19:

Teorema 7.26: Sea n un número que no es potencia de 2. Entonces existe un cuerpo k en donde no se satisface una identidad de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2,$$

donde:

$$z_j = \sum_{i=1}^n t_{ij} y_j, \quad t_{ij} \in k(x_1, \dots, x_n).$$

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 7.27: Sea $q = p^\alpha$. Entonces:

$$s(\mathbb{F}_q) = \begin{cases} 1, & p = 2 \vee p \equiv 1 \pmod{4} \vee \alpha \text{ par}, \\ 2, & p \equiv 3 \pmod{4} \wedge \alpha \text{ impar}. \end{cases}$$

En particular, el nivel es fácil de determinar en característica $\neq 0$. El siguiente es el caso de los cuerpos cuadráticos. Primero necesitaremos el siguiente resultado:

Lema 7.28 (Davenport-Cassels): Supongamos que $n \in \mathbb{Z}$ puede escribirse como suma de tres cuadrados racionales, entonces también puede escribirse como suma de tres cuadrados enteros.

DEMOSTRACIÓN: Sea $n = \lambda_1^2 + \lambda_2^2 + \lambda_3^2 \in \mathbb{Q}$. Limpiando denominadores se obtiene que

$$t^2 n = \mu_1^2 + \mu_2^2 + \mu_3^2, \quad t, \mu_1, \mu_2, \mu_3 \in \mathbb{Z},$$

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 $q_j \in \mathbb{Z}$ y $|r_i| \leq 1/2$. Por minimalidad de t podemos suponer que algún r_i es no nulo y definamos:

$$\begin{aligned} a &:= q_1^2 + q_2^2 + q_3^2 - n, & b &:= 2(nt - (\mu_1 q_1 + \mu_2 q_2 + \mu_3 q_3)), \\ \bar{t} &:= at + b, & \bar{\mu}_i &:= a\mu_i + bq_i. \end{aligned}$$

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:

$$\begin{aligned} t \cdot \bar{t} &= at^2 + bt \\ &= t^2 \left(\sum_{i=1}^3 q_i^2 - n \right) + t \left(2nt - 2 \sum_{i=1}^3 \mu_i q_i \right) \\ &= t^2 \sum_{i=1}^3 q_i^2 - 2t \sum_{i=1}^3 \mu_i q_i + \sum_{i=1}^3 \mu_i^2 \\ &= \sum_{i=1}^3 (tq_i - \mu_i)^2 = t^2(r_1^2 + r_2^2 + r_3^2). \end{aligned}$$

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 7.29: 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:

$$\begin{array}{ccc}
H & & \\
\downarrow \exists! \psi & \searrow \varphi_j & \\
\prod_{i \in I} G_i & \xrightarrow{\pi_j} & G_j
\end{array}$$

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:

$$\begin{array}{ccc}
H & & \\
\uparrow \exists! \psi & \nwarrow \varphi_j & \\
\bigoplus_{i \in I} G_i & \xleftarrow{\iota_j} & G_j
\end{array}$$

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 8.7: Se cumplen:

1. Todo grupo abeliano libre finitamente generado es isomorfo a \mathbb{Z}^n para algún n . Más generalmente, definiendo $\mathbb{Z}^{\oplus \kappa} := \bigoplus_{\alpha=1}^{\kappa} \mathbb{Z}$, se cumple que todo grupo abeliano libre es isomorfo a $\mathbb{Z}^{\oplus \kappa}$ para algún número cardinal κ .
2. Más aún, $\mathbb{Z}^n \cong \mathbb{Z}^m$ syss $n = m$. De modo que todo par de bases de un grupo abeliano libre finitamente generado son de igual cardinalidad.
3. (AE) $\mathbb{Z}^{\oplus \kappa} \cong \mathbb{Z}^{\oplus \mu}$ syss $\kappa = \mu$. De modo que todo par de bases de un grupo abeliano libre son de igual cardinalidad.

DEMOSTRACIÓN: Para probar la segunda y la tercera basta tomar un grupo abeliano libre G y considerar a $G/2G$ como \mathbb{F}_2 -espacio vectorial. Luego la unicidad de cardinalidad de bases de un espacio vectorial induce la unicidad de cardinalidad de bases como grupo abeliano libre. \square

Definición 8.8: Dado un grupo abeliano libre G , se denota por $\text{rank } G$ a la cardinalidad de cualquiera de sus bases.

Proposición 8.9: Sea G un grupo abeliano con un conjunto X tal que satisface lo siguiente: Para todo grupo abeliano H y toda aplicación $f: X \rightarrow H$, 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 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) 8.10: Sea M un A -módulo y $N \leq M$ tal que M/N es un módulo libre. Entonces existe $F \leq M$ tal que $M/N \cong F$ y $M = N \oplus F$.

DEMOSTRACIÓN: Si N es un submódulo de M , entonces la siguiente sucesión:

$$0 \longrightarrow N \longrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$$

es exacta. Como M/N es libre entonces posee una base $X = \{[x_i]\}_{i \in I}$, por tanto, la aplicación $g: X \rightarrow M$ 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) 8.11: 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_β/M'_β es isomorfo a un ideal de A , pero todos los ideales de A son principales, luego o son el ideal nulo o son isomorfos (como A -módulos) a A . Si el ideal no es nulo, entonces por la proposición anterior se cumple que $M_\beta \cong M'_\beta \oplus \langle \mathbf{m}_\beta \rangle$ 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}_β '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 γ 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 γ . \square

Nótese que su F es finitamente generado, entonces no hay uso de elección.

Proposición 8.12: Sea A un anillo, F un A -módulo libre de base X y M otro A -módulo. Toda aplicación $f: X \rightarrow M$ admite una única extensión $f^*: F \rightarrow M$ en un morfismo de A -módulos.

Definición 8.13: Sea G un grupo abeliano, definimos su *subgrupo de torsión* como

$$T(G) := \{x \in G : \text{ord } x \neq 0\},$$

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 $T(G) = G$; y se dice *libre de torsión* si $T(G) = \{1\}$.

Ejemplo. Todo grupo abeliano finito es un grupo de torsión. $(\mathbb{Z}, +)$ es libre de torsión. $(\mathbb{R}^\times, \cdot)$ es tal que $T(\mathbb{R}^\times) = \{\pm 1\}$, así que ni es de torsión ni es libre de torsión.

Proposición 8.14: Para todo G, H abelianos, se cumplen:

1. $G/T(G)$ es libre de torsión.
2. Si $G \cong H$, entonces $T(G) \cong T(H)$ y $G/T(G) \cong H/T(H)$.

Teorema 8.15: Se cumplen las siguientes:

1. Todo grupo abeliano finitamente generado y libre de torsión es un grupo abeliano libre. En consecuencia dicho grupo será isomorfo a \mathbb{Z}^n para algún n .
2. Todo subgrupo H de un grupo abeliano libre finitamente generado G es también abeliano libre y además $\text{rank } H \leq \text{rank } G$.
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 φ está bien definido: En efecto, si $r'x_{n+1} = m'g$ con r', m' distintos, entonces $r'rx_{n+1} = m'mg$, pero x_{n+1}, g tienen orden 0, así que necesariamente $r'r = m'm$ y $r'/m' = r/m$. Además φ es un homomorfismo de grupos inyectivo (¿por qué?), así que basta probar que todo subgrupo finitamente generado F de \mathbb{Q} sea abeliano libre para poder concluir éste inciso.

Sea $F := \langle a_1/b_1, \dots, a_r/b_r \rangle \leq \mathbb{Q}$. 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 8.11. \square

Corolario 8.16: Se cumplen:

1. Todo grupo abeliano finitamente generado G puede escribirse como

$$G = \mathbb{T}(G) \oplus F$$

donde F es un grupo abeliano libre finitamente generado.

2. Dados G, H abelianos y finitamente generados. Entonces $G \cong H$ si y sólo si $\mathbb{T}(G) \cong \mathbb{T}(H)$ y $\text{rank}(G/\mathbb{T}(G)) \cong \text{rank}(H/\mathbb{T}(H))$.

8.2 Formas canónicas

En ésta sección trabajaremos exclusivamente con espacios vectoriales de dimensión finita.

Daremos varias definiciones para endomorfismos lineales, y nos daremos la libertad de asumir que las definiciones también aplicar singularmente a matrices mediante el endomorfismo $v \mapsto v \cdot B$.

Definición 8.17: 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 λ es su *autovalor* asociado.

Denotamos por $\sigma(T)$ al conjunto de los autovalores de T .

Teorema 8.18: Dado $A \in \text{Mat}_n(k)$, se cumple que λ es autovalor de A syss $\det(\lambda I_n - A) = 0$.

DEMOSTRACIÓN: Sea λ el autovalor asociado a $\mathbf{v} \in V_{\neq \vec{0}}$, 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 8.19: 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 λ es autovalor de A syss λ es raíz de ψ_A .

Corolario 8.20: Toda matriz de $n \times n$ posee a lo más n autovalores.

Teorema 8.21: Son equivalentes:

1. k es algebraicamente cerrado.
2. Toda matriz cuadrada con coeficientes en k tiene un autovector.

DEMOSTRACIÓN: Claramente $1 \implies 2$, veremos la recíproca: Para ello basta probar por inducción que todo polinomio está asociado al polinomio característico de una matriz. En particular el polinomio característico de

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

es

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.$$

\square

Lema 8.22: 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 8.23: 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 8.24: 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 8.25: 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 8.26: 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 8.27: 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 α_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 β_i 's eran efectivamente los autovalores de A . \square

8.3 Formas bilineales

Volvemos al contexto general de módulos. Recordemos lo siguiente:

Definición 8.28: Sea A un dominio. Una forma bilineal sobre un A -módulo M es una aplicación

$$\beta: M \times M \longrightarrow A$$

tal que β es lineal en cada coordenada.

Se dice que una forma bilineal β es *no degenerada* si para todo homomorfismo de R -módulos $\varphi: M \rightarrow R$ 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 β es una forma bilineal (resp. producto interno) sobre M , decimos que el par (M, β) es un *A -módulo de forma bilineal* (resp. *A -módulo de producto interno*). De no haber ambigüedad sobre los signos omitiremos el β .

Un homomorfismo $f: (M, \beta) \rightarrow (M', \beta')$ 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 8.29: Los A -módulos de forma bilineal (como objetos) y los homomorfismos entre ellos (como flechas) conforman una categoría, denotada Bil_A .

Ésto permite una definición natural de isomorfismo de A -módulos de forma bilineal. Además existe un claro funtor olvidadizo a la categoría de A -módulos, pero no haremos mucho uso de ambos hechos.

Definición 8.30: Un A -módulo de producto interno (M, β) se dice un *espacio de producto interno* si M es un A -módulo finitamente generado y proyectivo.

§8.3.1 Módulos libres de forma bilineal.

Definición 8.31: Sea (M, β) un A -módulo libre de forma bilineal de rango finito. Sea $X = (x_1, \dots, x_n)$ una base ordenada de M , entonces llamamos *representación matricial de β* a la matriz

$$M_X(\beta) := [\beta(x_i, x_j)]_{ij}.$$

Proposición 8.32: Sea (M, β) un A -módulo libre de forma bilineal de rango finito y sea B su representación matricial en alguna base ordenada. Entonces β es una forma bilineal (anti)simétrica syss B es una matriz (anti)simétrica.

Proposición 8.33: Sea (M, β) un A -módulo libre de forma bilineal de rango finito. Sean X, Y dos bases ordenadas de M y sea $A := M_X^Y(\text{Id})$ 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 8.34: Sea (M, β) un A -módulo libre de forma bilineal de rango finito. β es un producto interno syss su representación matricial en una base (y, por tanto, en todas) es invertible.

Con la proposición anterior, también hemos probado algo más fuerte:

Lema 8.35: Sean (A^n, β) y (A^n, γ) dos A -módulos de formas bilineales. Entonces son isomorfos syss dada una base ordenada X de A^n (e.g., la base canónica) existe una matriz invertible B tal que

$$M_X(\beta) = B \cdot M_X(\gamma) \cdot B^t.$$

Definición 8.36: Sea (M, β) un A -módulo libre de forma bilineal de rango finito. Llamamos *determinante* del producto β , denotado $\det(\beta)$, al elemento $[\det(B)] \in A/(A^\times)^2$, donde B es la representación matricial de β en alguna base ordenada.

Nótese que la necesidad del cociente es para asegurar unicidad. En el capítulo de cuerpos formalmente reales veremos que éste cociente es parti-

cularmente interesante si A es un cuerpo formalmente real, lo que explica la necesidad de elaborar otra teoría para anillos como \mathbb{C} .

Definición 8.37: Sea (e_1, \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 8.38: A toda base ordenada de un A -espacio de producto interno le corresponde una única base dual.

Definición 8.39: Sean $(M_1, \beta_1), \dots, (M_n, \beta_n)$ 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 8.40: 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) si y sólo si 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 8.41: Sea M un A -módulo de forma bilineal (anti)simétrica. Sea $N \subseteq M$, entonces llamamos su *complemento ortogonal*, denotado N^\perp , al conjunto de los $x \in M$ tales que $\beta(x, y) = 0$ para todo $y \in N$.

Lema 8.42 (de descomposición ortogonal): Sea M un A -módulo de forma bilineal (anti)simétrica. Supongamos que $N \leq M$ es tal que $\beta \upharpoonright N \times N$ 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 β ser producto interno en todo M , sino sólo en N .

Teorema 8.43: Sea M un A -módulo de forma bilineal (anti)simétrica. Sean $x_1, \dots, x_k \in M$ 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 8.44: 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 8.45: Sea M un A -módulo libre de forma bilineal (anti)simétrica. Se dice que $X \subseteq M$ es una *base ortogonal* si es una base y para todo $x, y \in X$ distintos se cumple que $\beta(x, y) = 0$.

Corolario 8.46: Sea A un dominio local en donde $2 \in A^\times$, entonces todo A -espacio de producto interno simétrico posee una base ortogonal.

DEMOSTRACIÓN: Por el corolario anterior podemos anotar

$$M \cong \langle a_1 \rangle \oplus \dots \oplus \langle a_k \rangle \oplus N.$$

Luego N es un A -módulo proyectivo sobre un dominio local, ergo es libre (teo. 6.48) 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 8.47: Sea M un A -módulo de forma bilineal simétrica y sea $M \cong N_1 \oplus N_2$. Una *reflexión* de M en torno a (N_1, N_2) es un endomorfismo $r: M \rightarrow M$ 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 8.48: Sea A un dominio local con $2 \in A^\times$, y sea M un A -módulo de forma bilineal simétrica. Entonces:

1. Toda involución que preserva la forma bilineal es una reflexión.
2. Supongamos que $x, y \in M$ satisfacen que

$$\beta(x, x) = \beta(y, y) \in A^\times,$$

entonces existe una reflexión que lleva x a y .

DEMOSTRACIÓN:

Revisar bien el ejercicio.

1. Ejercicio para el lector.
2. Definamos $u := \frac{x+y}{2}$ y $v := \frac{x-y}{2}$. Nótese que $\beta(u, v) = 0$, de modo que

$$\beta(x, x) = \beta(u, u) + \beta(v, v),$$

luego como A es local, entonces alguno debe ser inversible (¿por qué?). Sin pérdida de generalidad, si $\beta(u, u)$ es inversible, entonces $M = (Au) \oplus (Au)^\perp$ y construimos la reflexión apropiada. \square

Corolario 8.49: Sea A un dominio local con $2 \in A^\times$, y sea M un A -espacio de producto interno simétrico de rango n . Entonces todo automorfismo $f: M \rightarrow M$ es la composición de n reflexiones.

DEMOSTRACIÓN: Basta notar que un automorfismo transforma bases en bases y aplicar inducción. \square

Teorema 8.50 – Teorema de Witt: Sea A un dominio local con $2 \in A^\times$. Supongamos que M, N, P son A -espacios de producto interno simétrico tales que $M \oplus P \cong N \oplus P$ (en Bil_A), entonces $M \cong N$ (en Bil_A).

DEMOSTRACIÓN: Podemos escribir P como la suma ortogonal de espacios libres de rango 1, así que, aplicando inducción basta considerar $P = \text{Span}_A(e)$. 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 8.48, 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 8.51: Sean $(M_1, \beta_1), \dots, (M_n, \beta_n)$ un conjunto de A -módulos de forma bilineal. Existe una única forma bilineal β 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 ϕ también se extiende a una aplicación $N \times N \rightarrow A$ bilineal que coincide con β cuya extensión es la misma aplicación superior. Ésto comprueba el enunciado. \square

Lema 8.52: 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 5.65). Denotemos por $M^* := \text{Hom}_A(M, A)$. Luego cada producto interno β_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 8.53: Se dice que un A -espacio de producto interno simétrico M es un A -espacio metabólico¹ si existe $N \leq M$ tal que $N = N^\perp$ y N es un sumando directo de M .

Lema 8.54: Sean M, M' dos A -espacios metabólicos y (N, β) un A -espacio de producto interno arbitrario. Entonces:

1. $M \oplus M$ es metabólico.
2. $M \otimes_A N$ es metabólico.
3. $(N, \beta) \oplus (N, -\beta)$ es metabólico.

DEMOSTRACIÓN: Para la última sólo basta notar que $M := \langle 1 \rangle \oplus \langle -1 \rangle$ es metabólico y que

$$M \otimes_A N = (N, \beta) \oplus (N, -\beta). \quad \square$$

Lema 8.55: Sea A un anillo en donde todo A -módulo finitamente generado proyectivo es libre (e.g., un cuerpo, un DIP o un dominio local). Un

¹Knebusch [39, pág. 122] emplea «metabólico», mientras que Milnor [16, pág. 12] emplea «se escinde» (eng. *split*).

A -espacio de producto interno es metabólico syss la representación de su producto interno es de la forma

$$\begin{bmatrix} \mathbf{0} & I \\ I & B \end{bmatrix}$$

para alguna base. Más aún, si $2 \in A^\times$, entonces podemos elegir la base de modo que $B = \mathbf{0}$.

DEMOSTRACIÓN: Sea M un A -espacio metabólico que, por hipótesis, es un A -módulo libre de rango finito. Sea $N \leq M$ un sumando directo, el cual es libre, y sea e_1, \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 8.56: Dos A -espacios de producto interno simétrico N_1, N_2 se dice que pertenecen a la misma clase de Witt, denotado $N_1 \sim N_2$, si existen dos espacios metabólicos M_1, M_2 tales que $N_1 \oplus M_1 \cong N_2 \oplus M_2$. Se denota por $W(A)$ el conjunto de todas las clases de Witt.

Lema 8.57: Sean $M \sim M'$ y $N \sim N'$, entonces $M \oplus N \sim M' \oplus N'$ y $M \otimes_A N \sim M' \otimes_A N'$.

Recordemos que $(M, \beta) \oplus (M, -\beta) \sim 0$ y $M \otimes_A \langle 1 \rangle \sim M$, ésto, combinado con el trabajo anterior nos comprueba lo siguiente:

Teorema 8.58: $W(A)$ es un dominio (i.e., anillo unitario conmutativo) donde $1 = [\langle 1 \rangle]$, $[M] + [N] = [M \oplus N]$ y $[M] \cdot [N] = [M \otimes_A N]$.

Por ello, a $W(A)$, se le llama el *anillo de Witt* de A .

9

Teoría espectral

9.1 Diagonalización

En esta sección se desarrollan varios resultados para endomorfismos sobre espacios vectoriales de dimensión finita, nótese que toda B puede verse como el endomorfismo $x \mapsto Bx$, así que obviaremos mencionar cosas como “ésta definición se aplica para matrices así...”.

Definición 9.1 – Subespacio f -invariante: Dado un módulo M , $f \in \text{End}(M)$ 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 α 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 α de f a:

$$V_\alpha^f := \{v \in V : f(v) = \alpha v\}, N_\alpha^f := \{v \in V : \exists r \geq 0 (f - \alpha \text{Id})^r v = 0\};$$

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_α y N_α son submódulos o subespacios vectoriales de \mathbb{k}^n .
2. $V_\alpha \leq N_\alpha$.
3. V_α y N_α son f -invariantes.
4. La multiplicidad geométrica de α siempre es menor o igual a su multiplicidad algebraica.
5. α 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 λ es autovalor de f , entonces $f - \lambda \text{Id}$ restringido al autoespacio N_λ 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_λ .

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_β . 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_β , 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_{α_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_{α_i} para deducir que $v_i = 0$. \square

Corolario 9.13: Sea $f \in \text{End}(\mathbb{k}^n)$. Si f posee n autovalores distintos, entonces es diagonalizable.

Teorema 9.14: Un endomorfismo es diagonalizable si y sólo si existe una base formada por sus autovectores.

Teorema 9.15: 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 9.16: 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 9.17: Para un endomorfismo sobre V , son equivalentes:

1. f es triangularizable.
2. Existe una cadena maximal de subespacios f -invariantes:

$$0 =: V_0 \subset V_1 \subset \cdots \subset V_n := V$$

DEMOSTRACIÓN: 1) \implies 2). Si f es triangularizable, entonces sea $X := (x_1, \dots, x_n)$ 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 9.18: 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 λ , 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 9.19: Se cumple que $P(\mathbb{R}, 2, r)$ para todo $r \in \mathbb{N}_{\neq 0}$

DEMOSTRACIÓN: Para ésto basta ver que $P(\mathbb{R}, 2, 1)$, lo que equivale a ver que toda matriz $B \in \text{Mat}_n(\mathbb{R})$ 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 9.20 – 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 9.21: El conjunto de las matrices hermitianas de $n \times n$ es un \mathbb{R} -espacio vectorial de dimensión n^2 .

PISTA: Recuerde que en la diagonal de una matriz hermitiana sólo pueden ir números reales. \square

Lema 9.22: 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 9.23: Para todo $k > 0$ se cumple que $P(\mathbb{C}, 2^k, 1)$. En consecuencia, toda matriz tiene autovalores en \mathbb{C} , y \mathbb{C} resulta ser 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 9.24: 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 9.25:

$$\text{Mat}_n(A[x]) \cong (\text{Mat}_n A)[x]$$

Teorema 9.26 – Teorema de Cayley-Hamilton: Si B es una matriz cuadrada de polinomio característico $p_B(x) = a_0 + a_1x + \cdots + a_nx^n$, entonces

$$p_B(B) = a_0I + a_1B + \cdots + a_nB^n = 0.$$

DEMOSTRACIÓN: Sea $\varphi : \text{Mat}_n(A[x]) \rightarrow (\text{Mat}_n A)[x]$ 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 [34].

Proposición 9.27: 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 ι le definimos sobre todo V y vemos que la imagen sobre la base genera un conjunto linealmente independiente en V^* . Claramente ι es inyectiva y prueba que $\dim V \leq \dim V^*$ en todo caso.

Para probar la tercera probaremos varios pasos:

1. **Si $\mathbb{k} \leq \aleph_0$, 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 $\mathbb{k} \times I$, por lo que,

$$|V| \leq |S| = |\mathbb{k} \times I|^{<\aleph_0} = |\aleph_0| \cdot |\mathbb{k} \times I| = |I|.$$

2. **Si $\mathbb{k} \leq \aleph_0$, entonces $\dim V < \dim V^*$:**

Simple: como toda función lineal viene determinada exclusivamente por los valores en la base, se cumple que

$$|V| = |\text{Func}(I; \mathbb{k})| = |\mathbb{k}|^{|I|} \geq 2^{|I|} > |I| = |V|$$

donde la última desigualdad es el teorema de cardinalidad de Cantor.

3. **Caso arbitrario:**

Notemos que \mathbb{k} , por ser un cuerpo, siempre contiene a otro cuerpo

$$F := \begin{cases} \mathbb{Q}, & \text{car } \mathbb{k} = 0 \\ \mathbb{F}_p, & \text{car } \mathbb{k} = p \end{cases}$$

Luego si $W := \text{Span}_F(e_i)_{i \in I}$ vemos que $\dim_F W = \dim_{\mathbb{k}} V$, y sabemos que $\dim_F W < \dim_{\mathbb{k}} W^*$, así que basta probar que $\dim_F W^* \leq \dim_{\mathbb{k}} V^*$.

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 $G(\varphi) : V \rightarrow \mathbb{k}$ sea \mathbb{k} -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 9.28 – 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 9.29: 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 9.30: Si F es una forma bilineal simétrica, entonces su representación matricial bajo cualquier base también lo es.

Teorema 9.31: Si V es un \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 9.32: Se dice que dos matrices A, B son *congruentes* si existe M invertible tal que $A = MBM^t$.

Por ende hemos probado:

Teorema 9.33: Toda matriz simétrica sobre un campo escalar de característica distinta de 2 es congruente a una matriz diagonal.

Sea F una forma bilineal simétrica con base ortonormal $(\mathbf{x}_i)_i$, 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 α_i es un escalar que multiplicamos por \mathbf{x}_i a conveniencia, luego es claro que:

Teorema 9.34: 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 $\underbrace{[1, \dots, 1]_r}_{r}, 0, \dots, 0]$.

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 9.35: 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 9.36: 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 9.37 – 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 9.38: 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 9.39: 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 9.40 – 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 9.41 – 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 denotara un espacio prehilbertiano.

Proposición 9.42: Si f es una forma hermitiana sobre H , entonces, para todo $u, v \in H$ y $\alpha \in \mathbb{K}$:

1. $f(u, \alpha v) = \bar{\alpha} f(u, v)$.
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 9.43: Sea $x \in H$. Se cumple que $x = \mathbf{0}$ syss para todo $y \in H$ se cumple que $\langle x, y \rangle = 0$.

Corolario 9.44: Sean $x, y \in H$. Se cumple que $x = y$ syss para todo $z \in H$ se cumple que $\langle x, z \rangle = \langle y, z \rangle$.

Corolario 9.45: Sean $A, B \in \text{End}(H)$. 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 9.46 – Desigualdad de Cauchy-Schwarz: Para todo $x, y \in H$ se cumple:

$$|\langle x, y \rangle| \leq \|x\| \|y\|$$

DEMOSTRACIÓN: Supongamos que $y \neq 0$ (pues $y = 0$ es trivial), entonces notemos que

$$\begin{aligned} 0 &\leq \langle x - \alpha y, x - \alpha y \rangle = \langle x, x \rangle - \alpha \langle y, x \rangle - \bar{\alpha} \langle x, y \rangle + |\alpha|^2 \langle y, y \rangle \\ &= \|x\|^2 - 2 \operatorname{Re}(\alpha \langle y, x \rangle) + |\alpha|^2 \|y\|^2. \end{aligned}$$

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 9.47 (Desigualdad traingular): Para todo $x, y \in H$ se cumple que

$$\|x + y\| \leq \|x\| + \|y\|,$$

luego, $\|\cdot\| : H^2 \rightarrow \mathbb{R}$ 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 9.48 – Ortogonalidad: Un par $x, y \in H$ se dicen *ortogonales* si $\langle x, y \rangle = 0$, en cuyo caso se escribe $x \perp y$. Más aún, dado un subconjunto $A \subseteq H$, le llamamos *complemento ortogonal* a

$$A^\perp := \{x \in H : \forall a \in A (x \perp a)\}.$$

Diremos que una sucesión (finita o infinita) de vectores es *ortogonal*, si los vectores lo son dos a dos. Diremos que una sucesión es *ortonormal*, si los vectores son unitarios y la sucesión es ortogonal.

Teorema 9.49: Se cumple:

1. $\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2$ (ley del paralelogramo).
2. $x \perp y$ syss $\|x + y\|^2 = \|x\|^2 + \|y\|^2$ (teorema de Pitágoras I).
3. Si $\{x_i\}_{i=1}^n$ es una sucesión ortonormal, entonces para todo $i \leq n$ se cumple $x_i \perp \sum_{j \neq i} x_j$.

4. Si $\{x_i\}_{i=1}^n$ es una sucesión ortonormal, entonces para todo $x \in H$ se cumple

$$\|x\|^2 = \sum_{i=1}^n |\alpha_i|^2 + \left\| x - \sum_{i=1}^n \alpha_i x_i \right\|^2,$$

donde $\alpha_i := \langle x, x_i \rangle$ (teorema de Pitágoras II).

DEMOSTRACIÓN:

4. Obsérvese que

$$x = \sum_{i=1}^n \alpha_i x_i + \left(x - \sum_{i=1}^n \alpha_i x_i \right).$$

Donde hay $n+1$ vectores, hemos de probar que todos son ortogonales entre sí para aplicar el teorema de Pitágoras. Es claro que $x_i \perp x_j$ con $i \neq j$, por ende, basta notar que

$$\begin{aligned} \left\langle x_k, x - \sum_{i=1}^n \alpha_i x_i \right\rangle &= \langle x_k, x \rangle - \sum_{i=1}^n \langle x_k, \alpha_i x_i \rangle \\ &= \langle x_k, x \rangle - \overline{\alpha_k} \langle x_k, x_k \rangle \stackrel{1}{=} 0. \end{aligned}$$

□

Teorema 9.50 – Ortogonalización de Gram-Schmidt. Si $\dim H \leq \aleph_0$ tiene una base $\{x_i\}_i$, entonces posee una base ortonormal $\{z_i\}_i$ que satisface que para todo $k > 0$:

$$\text{Span}\{x_1, \dots, x_k\} = \text{Span}\{y_1, \dots, y_k\}$$

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 9.51: Se cumple:

1. Si $S \subseteq H$, entonces $S^\perp \leq H$.
2. Para todo $S \subseteq H$ se cumple que $S \subseteq (S^\perp)^\perp$.

Si exigimos que $\dim H \leq \aleph_0$, entonces para todo $E \leq H$ se cumple que:

3. Existe una única transformación lineal $\pi_E : H \rightarrow E$ 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 π_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 9.52 (Desigualdad de Bessel): Sea $\{x_i\}$ una sucesión¹ 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 9.53: 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

¹ Aquí se obvian los límites de los índices pues el resultado es válido tanto para sucesiones finitas como infinitas.

Corolario 9.54: Si una sucesión ortonormal $\{x_i\}$ genera un subespacio V de H , entonces todo $x \in V$ se escribe de forma única como combinación lineal con

$$x = \sum_i \langle x, x_i \rangle x_i.$$

Proposición 9.55 (Identidad de Parseval): Una sucesión ortonormal $\{x_i\}$ es base de H syss para todo $x \in H$ se cumple

$$\|x\|^2 = \sum_i |\langle x, x_i \rangle|^2.$$

§9.3.4 Formas cuadráticas.

Definición 9.56 – 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 9.57: Si el campo escalar de V es de característica distinta de 2, entonces: Si F es una forma bilineal simétrica sobre V con forma cuadrática asociada q , entonces F está completamente determinada por

$$F(u, v) = \frac{q(u+v) - q(u) - q(v)}{2}.$$

De éste modo podemos definir una forma cuadrática de tal modo que la función descrita cumpla ser una forma bilineal simétrica.

10

Álgebras

10.1 Definiciones elementales

Definición 10.1: Sea A un dominio. Una A -álgebra B es un A -(bi)módulo con una forma bilineal $\beta: B \times B \rightarrow B$, 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 $b \in B$.^a Se dice que B es una A -álgebra *asociativa* (resp. *conmutativa*) si el producto es asociativo (resp. conmutativo).

Un homomorfismo de A -álgebras es un homomorfismo de A -bimódulos $\varphi: B \rightarrow C$ de modo que $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ y que $\varphi(1_B) = 1_C$.

^aAlgunos 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 \mathbf{Alg}_A . La subcategoría de A -álgebras conmutativas se denota \mathbf{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 coordinada a coordinada, 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 si G es un grupo abeliano. Llamamos a $A[G]$ la A -álgebra asociada al grupo G .

2. De hecho no es necesario que sea un grupo ni que sea finito. Si G es un monoide arbitrario,¹ entonces también podemos definir $A[G]$ exactamente del mismo modo, exigiendo que las sumas formales sean finitas,

¹Si 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.
6. Considere el grupo finito Q_4 de cuaterniones. Se denota por $\mathbb{H} := \mathbb{R}[Q_4]$, el cual es una \mathbb{R} -álgebra asociativa no-conmutativa y sus elementos son de la forma $a + bi + cj + dk$, donde

$$i^2 = j^2 = k^2 = ijk = -1, \quad ij = k, \quad ik = -j, \quad jk = i.$$

Algunas definiciones típicas:

Definición 10.3: Sea B una A -álgebra. Un subconjunto $C \subseteq B$ se dice que es una *subálgebra* si es un A -submódulo, contiene al 1 y es cerrado bajo la multiplicación de B .

Un *ideal* es una subálgebra $\mathfrak{b} \subseteq B$ tal que $B\mathfrak{b} = \mathfrak{b}B = \mathfrak{b}$ y en particular, si B es una álgebra asociativa, entonces un ideal (como álgebra) es un ideal izquierdo y derecho (como anillo) que es también una subálgebra. Es fácil comprobar que el anillo cociente B/\mathfrak{b} es también una A -álgebra, de modo que le llamamos una A -álgebra cociente.

Lema 10.4: La intersección arbitraria de subálgebras (resp. ideales) es también una subálgebra (resp. un ideal).

Definición 10.5: Sea B una A -álgebra. Dado un subconjunto $S \subseteq B$, denotamos por $A[S]$ a la mínima subálgebra de B que contiene a S . Si B es una álgebra asociativa, entonces denotamos por $A + (S)$ al mínimo ideal de B que contiene a S .

Proposición 10.6: Sea B una A -álgebra y sea $S \subseteq B$ un subconjunto. Entonces:

$$A[S] = \left\{ \sum_{i=1}^n s_i t_i : s_i, t_i \in S \cup A \right\},$$

$$A + (S) = \left\{ \sum_{i=1}^n b_i s_i c_i : b_i, c_i \in B, s_i \in S \cup A \right\}.$$

Proposición 10.7: La unión de una cadena de subálgebras (resp. ideales) es también una subálgebra (resp. un ideal).

Proposición 10.8: Sean B, C un par de A -álgebras y $\varphi: B \rightarrow C$ 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* si posee un sistema generador finito.

Otros textos emplean la expresión «álgebra finitamente generada» o «álgebra finita», pero creo que ésto ocasiona confusiones con ser finitamente generado como módulo o ser finito en cardinalidad. Es claro que hay álgebras de tipo finito que no tienen cardinalidad finita, pero más aún:

Ejemplo. Considere el álgebra polinomial $A[x]$. Ésta álgebra es de tipo finito (está generada por $\{x\}$), pero no es un A -módulo finitamente generado, pues su base es $\{1, x, x^2, \dots\}$.

En general, reservaré las letras x y similares para las indeterminadas, de modo que $A[x]$ siempre será el álgebra polinomial y $A[a]$ representa el subálgebra generada por a .

§10.1.1 Álgebras (asociativas) libres.

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.

\Rightarrow . 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 $\iota_F: X \rightarrow F$ 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 10.13: Dos álgebras libres $A\langle X \rangle, A\langle Y \rangle$ son isomorfas si $|X| = |Y|$.

El recíproco parecería sencillo pero, ¡inténtelo! En esencia, el problema resulta difícil, incluso si A es un cuerpo, porque los elementos de la base son algebraicamente independientes; se asimila a probar la unicidad del grado de

trascendencia, pero con la problemática de la falta de conmutatividad. No obstante, nótese que, por un argumento de cardinalidad, si las bases tienen mayor cardinalidad que $\aleph_0 + |A|$, entonces el recíproco es trivial.

Definición 10.14: Sea B una A -álgebra asociativa conmutativa. Un subconjunto $X \subseteq B$ es una *base* si para toda A -álgebra asociativa conmutativa C toda función $f: X \rightarrow C$ 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 10.15: Sea A un dominio y S un conjunto arbitrario.

1. La álgebra polinomial $A[S]$ es una álgebra asociativa conmutativa libre que tiene a S por base.
2. Si S, T son dos conjuntos de indeterminadas con la misma cardinalidad, entonces $A[S] \cong A[T]$.
3. Recíprocamente, si F_1, F_2 son álgebras conmutativas libres, entonces son álgebras polinomiales con la misma cantidad de indeterminadas.

Como señalé anteriormente, la última parte la podemos concluir por los argumentos desarrollados en la teoría de trascendencia (cf. §4.6).

10.2 Álgebras asociativas

§10.2.1 Anillos, módulos y álgebras graduadas.

Definición 10.16: Se dice que un anillo unitario A es *graduado*^a si existe una familia $(A_d)_{d \in \mathbb{N}}$, donde:

AG1. Cada A_i es un subgrupo abeliano bajo la suma.

AG2. $A = \bigoplus_{d \in \mathbb{N}} A_d$.

AG3. Para cada $d, e \geq 0$ se satisface que $A_d \cdot A_e \subseteq A_{d+e}$.

En consecuencia de AG3., se satisface que cada A_d es un A_0 -módulo y A también. Dicha descomposición se dice una *graduación*, y cada $f \in A_d$ se dice un elemento *homogéneo de grado d* . Más que sólo un módulo, A es una A_0 -álgebra y decimos que es una *álgebra graduada*.

Una subálgebra $S \subseteq A$ se dice *homogéneo* si $S = \bigoplus_{d \in \mathbb{N}} (S \cap A_d)$. Un ideal se dice *homogéneo* si es una subálgebra homogénea. El conjunto $A^+ := \bigoplus_{d > 0} A_d$ es un ideal homogéneo llamado el *ideal irrelevante*.

^aCHEVALLEY [3] emplea el término Γ -graduado pues admite la posibilidad de graduar un anillo (o una álgebra) con un grupo abstracto Γ . En otros textos también emplea *regularmente graduado*.

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 10.17: 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 10.18: Sea A un anillo graduado. Una subálgebra $S \subseteq A$ es homogénea syss está generada por un conjunto de elementos homogéneos.

DEMOSTRACIÓN: \implies . Si S es homogénea entonces está generada por $\bigcup_{d \in \mathbb{N}} S \cap A_d$.

\impliedby . Sea T tal que $\mathfrak{a} = (T)$ y tal que los elementos de T son homogéneos. Luego, sea $f \in \mathfrak{a}$, por definición

$$f = g_1 f_1 + \cdots g_n f_n$$

donde $f_i \in T$ y $g_i \in A$. Como A es graduado, y los g_i 's son finitos, podemos encontrar suficientes h_j 's homogéneos tales que

$$g_i = \lambda_{1i} h_1 + \cdots + \lambda_{mi} h_m,$$

donde $\lambda_{ji} \in A_0$. Por lo tanto,

$$f = \lambda_{11} h_1 f_1 + \lambda_{21} h_2 f_1 + \cdots \lambda_{mn} h_m f_n.$$

donde cada $h_j f_i$ es homogéneo. Es decir, $f \in \bigoplus_{d \in \mathbb{N}} (\mathfrak{a} \cap A_d)$. La otra inclusión es trivial. \square

Definición 10.19: 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 .

Lema 10.20: 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 λ_g es homogénea de grado g .
2. Para todo $b \in B$ se cumple que $\lambda_g(b) = 0$ para todos salvo finitos g 's.
3. $\sum_{g \in \mathbb{N}} \lambda_g = 0$.

Entonces todas las λ_g 's son idénticamente nulas.

§10.2.2 Álgebra tensorial.

Definición 10.21: Sea M un A -módulo. Un par (T, ψ) se dice una *álgebra tensorial* sobre M si:

AT1. T es una A -álgebra y $\psi: M \rightarrow T$ 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:

$$\begin{array}{ccc} & & T \\ & \nearrow \psi & \downarrow \exists! f \\ M & \xrightarrow{\varphi} & B \end{array}$$

Teorema 10.22: Dado un A -módulo M existe una álgebra tensorial sobre M , denotada $T(M)$. Más aún, todas las álgebras tensoriales sobre M son isomorfas.

DEMOSTRACIÓN: La unicidad de las álgebras es un típico ejercicio de categorías.

Para construir a $T(M)$ considere a M como un conjunto de variables y considere $F := A\langle M \rangle$ el álgebra libre con base en M . Para distinguir las operaciones en F de las operaciones en M diremos que para todo $\alpha \in A$, los símbolos $x + y, x - y, \alpha x$ denotan operaciones en M y $x \dot{+} y, x \dot{-} y, \alpha \cdot x$ las operaciones en F . Luego, al igual que con los tensores, construimos el ideal \mathfrak{a} generado por elementos de la forma:

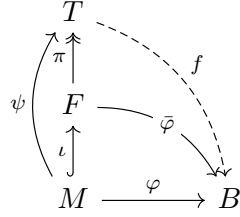
$$x \dot{+} y \dot{-} (x + y), \quad \alpha \cdot x \dot{-} (\alpha x).$$

Y definimos $T(M) := F/\mathfrak{a}$. 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 φ es lineal; y es análogo con los otros generadores. Finalmente podemos proyectar $\bar{\varphi}$ en F/\mathfrak{a} y nos dará una aplicación f . Visualmente:



□

Ejemplo. Sea A un dominio. Luego A mismo es un A -módulo libre con base $\{1\}$, afirmamos que $T(A) = A[x]$. Hay una manera más larga de proceder, pero con las caracterizaciones categoriales es sencillo: sea B una A -álgebra arbitraria, entonces queremos C tal que

$$\mathrm{Hom}_{\mathrm{Alg}}(C, B) \approx \mathrm{Hom}_{\mathrm{Mod}}(A, B) \approx \mathrm{Func}(\{1\}, B),$$

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 10.23: Sea A un dominio. Sea S un conjunto arbitrario y denotemos por $A^{\oplus S}$ el A -módulo libre con base S , se cumple que $T(A^{\oplus S}) = A\langle S \rangle$.

Otra propiedad de las álgebras tensoriales (en particular de su construcción) es que son álgebras graduadas: En efecto, nótese que $A\langle M \rangle$ es un álgebra graduada por ser libre, y que las combinaciones lineales formales de elementos en M son los elementos homogéneos de grado 1. Luego el ideal construido está generado por elementos homogéneos y luego es un ideal homogéneo, de modo que el cociente es una álgebra graduada.

Teorema 10.24: Sea M, N un par de A -módulos, y sea $\beta: M^d = \prod_{i=1}^d M \rightarrow N$ una 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

$$u = \sum_{i=1}^n \sum_{k,\ell}^m a_{ik} \square s_i \square b_{i\ell},$$

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 ψ se anula en $F_d \cap \mathfrak{a}$ puesto que sus elementos son de la forma descrita en (10.1), luego descende al cociente $F_d/(F_d \cap \mathfrak{a}) = T_d(M)$ como se quería ver. \square

Corolario 10.25: Para todo $d \geq 1$ se cumple que $T_d(M) \cong M^{\otimes d}$ (como A -módulos).

§10.2.3 Álgebras anticonmutativas.

Definición 10.26: 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 10.27: 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.

Teorema 10.28: Toda subálgebra y todo cociente de una álgebra anticonmutativa es también una álgebra anticonmutativa.

Teorema 10.29: 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 10.30: 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 $\theta(b \otimes c) = \varphi(b)\psi(c)$.

§10.2.4 Álgebra exterior y determinantes.

Definición 10.31: Sea M un A -módulo. Un par (E, ψ) se dice una *álgebra exterior* sobre M si:

- AE1. E es una A -álgebra y $\psi: M \rightarrow E$ 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:

$$\begin{array}{ccc} & & E \\ & \nearrow \psi & \downarrow \exists! f \\ M & \xrightarrow{\varphi} & B \end{array}$$

Lema 10.32: 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) 10.33: Dado un A -módulo libre M existe una álgebra exterior sobre M , denotada $E(M)$.

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 $\mathbf{u}\mathbf{v} = -\mathbf{v}\mathbf{u}$. Para ello consideremos los conjuntos finitos S de X y en particular podemos verlo como los índices y denotaremos \bar{u}_α en lugar de \mathbf{u}_α 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

$$\begin{aligned} \left(\sum_{\alpha} c_\alpha \bar{u}_\alpha \right)^2 &= \sum_{\alpha < \beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta + \sum_{\alpha} c_\alpha^2 \bar{u}_\alpha^2 + \sum_{\alpha > \beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta \\ &= \sum_{\alpha < \beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta + \sum_{\beta > \alpha} c_\beta c_\alpha \bar{u}_\beta \bar{u}_\alpha \\ &= \sum_{\alpha < \beta} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta - \sum_{\beta > \alpha} c_\alpha c_\beta \bar{u}_\alpha \bar{u}_\beta = 0. \end{aligned}$$

Ahora bien, sea $\varphi: M \rightarrow A$ 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) 10.34: Si M es un A -módulo libre de rango κ , entonces $\text{rang}(E(M)) = 2^\kappa$.

Otra conclusión de la demostración es que $E(M)$ es de hecho un cociente sobre $T(M)$ y es fácil notar que el ideal empleado está generado por elementos homogéneos, de modo que $E(M)$ es también una álgebra graduada. Los elementos homogéneos de grado d son de la forma $\bar{m}_1 \cdots \bar{m}_d$. Luego, si M es libre de rango n , entonces $E_d(M)$ es un A -módulo libre de rango $\binom{n}{d}$.

Corolario 10.35: Sea M un A -módulo con una álgebra exterior $E(M)$. Dado un endomorfismo de A -módulos $L: M \rightarrow M$, se puede construir un endomorfismo de A -álgebras $\eta(L): E(M) \rightarrow E(M)$ dado por el siguiente diagrama conmutativo:

$$\begin{array}{ccc} M & \xrightarrow{\psi} & E(M) \\ L \downarrow & & \downarrow \exists! \eta(L) \\ M & \xrightarrow[\psi]{} & E(M) \end{array}$$

Si $L_1, L_2 \in \text{End}_{\text{Mod}}(M)$ entonces:

$$\eta(1_M) = 1_{E(M)}, \quad \eta(L_1 \circ L_2) = \eta(L_1) \circ \eta(L_2).$$

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 $(E, \eta): \text{FMod}_A \rightarrow \text{Alg}_A$ 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

$$\begin{aligned} \eta(L)(\bar{u}_1 \cdots \bar{u}_n) &= \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \bar{u}_{\sigma(1)} \cdots \bar{u}_{\sigma(n)} \\ &= \sum_{\sigma \in S_n} (\text{sgn } \sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \bar{u}_1 \cdots \bar{u}_n = (\det L) \bar{u}_1 \cdots \bar{u}_n. \end{aligned}$$

Ésto nos otorga otra prueba, más directa aún, de que

$$\det(L_1 \circ L_2) = \det(L_1) \det(L_2).$$

Teorema 10.36: 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 10.37: 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 $Q(X) = (\det X)^r$.

§10.2.5 Representaciones.

Definición 10.38: 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 10.39: 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 μ_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:

$$\text{Tr}_{B/A}(b) := \text{tr}(\mu_b), \quad \text{Nm}_{B/A}(b) := \det(\mu_b), \quad \psi_{b,B/A}(x) := \psi_{\mu_b}(x) \in k[x].$$

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

$$\begin{aligned} z_1 &= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, \\ z_2 &= x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3, \end{aligned}$$

$$z_3 = x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2,$$

$$z_4 = x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1.$$

Una de las particularidades es que éstas identidades son *puramente* algebraicas, en el sentido de que son válidas sobre cualquier cuerpo. Naturalmente que uno puede ser tramposo y trabajar en \mathbb{F}_2 en donde el sueño del aprendiz nos otorga identidades para todo n , por ello se imponen éstas restricciones. Para continuar el patrón en 1822 C. F. Degan encontró otra identidad para $n = 8$ cuadrados. Ésto establece la curiosa insinuación de que éstas identidades sólo aparecen en potencias de dos y, siguiendo un olfato matemático, uno se vería tentado a buscar una identidad para $n = 16$.

En 1898, Hurwitz ahondó en ésta pregunta, lo que nos devuelve al contexto de álgebras: ya mencionamos que para la identidad (10.2) tenemos una intuición asociada a los complejos \mathbb{C} , pero para (10.3) podemos encontrar una fórmula asociada al álgebra de los cuaterniones \mathbb{H} propuesta por Hamilton y para la identidad de 8 términos de Degan podemos asociar otra álgebra, cuyos elementos se conocen como los *octoniones* de Cayley (1845). Así pues, la pregunta tiene un estrecho vínculo con el estudio de álgebras.

Formalizando, la pregunta es la siguiente: dado $n > 0$ existe una identidad de la forma

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \quad (10.4)$$

donde cada z_ℓ es una función bilineal sobre x_i e y_j . Para arruinar la sorpresa ésto sólo funciona para $n \in \{1, 2, 4, 8\}$, ésto lo iremos probando progresivamente.

Comencemos por reformular el problema (10.4): busquemos 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

$$(x_1^2 + \cdots + x_n^2)I_n - A^t A = \mathbf{0}.$$

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}^ℓ el ℓ es un superíndice, no un exponente. Definiendo $B_\ell := [b_{ij}^\ell]_{ij}$, se tiene que

$$A = B_1 x_1 + \cdots + B_n x_n.$$

De modo que buscamos que

$$(x_1^2 + \cdots + x_n^2)I_n = (B_1^t x_1 + \cdots + B_n^t x_n)(B_1 x_1 + \cdots + B_n x_n).$$

Como aplica para todo $x_i \in k$, entonces podemos elegir $x_j = \delta_{ij}$ para algún i fijo (es decir, todos los x_j 's nulos exceptuando el $x_i = 1$) de modo que obtenemos que:

- $B_i^t B_i = I_n$ para todo i .
- $B_i^t B_j + B_j^t B_i = \mathbf{0}$ para $i \neq j$.

Podemos definir $C_i := B_n^t C_i$ y un cálculo comprueba:

1. $C_i^t C_i = I_n$. En consecuencia, $\det(C_i) \neq 0$.
2. $C_i^t + C_i = \mathbf{0}$ o $C_i^t = -C_i$.
3. $C_i^t C_j + C_j^t C_i = \mathbf{0}$ con $i \neq j$.
4. $C_i^2 = -I_n$ para $i \neq n$ (por 1 y 2).
5. $C_i C_j = -C_j C_i$ para $i \neq j$ (por 3 y 2).

Sabemos que $\det(C_i) = \det(C_i^t) = \det(-C_i) = (-1)^n \det(C_i)$ luego n es necesariamente par y hemos probado:

Proposición 10.40: 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 $M\mathcal{G}$ 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 10.41: 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:

$$\begin{aligned} Q(x)Q(z) + \beta(x, y)Q(z) + Q(y)Q(z) &= Q(x + y)Q(z) = Q(xz + yz) \\ &= Q(xz) + \beta(xz, yz) + Q(yz). \end{aligned}$$

Con lo que hemos probado que

$$\beta(x, y)Q(z) = \beta(xz, yz), \quad Q(x)\beta(y, z) = \beta(xy, xz).$$

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:

$$\begin{aligned} \overline{(\cdot)}: B &\longrightarrow B \\ x &\longmapsto \beta(x, 1)1_B - x. \end{aligned}$$

Aquí el 1_B enfatiza el hecho de que es la unidad de B . Nótese que $\overline{(\cdot)}$ es un endomorfismo de A -módulos.

Lema 10.42: Sea (B, Q) una A -álgebra de composición. Para todo $x, y \in B$ se tiene lo siguiente:

1. $\overline{(\cdot)}$ 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

$$\begin{aligned}\beta(x, \bar{y}z) &= \beta(x, \beta(y, 1)z - yz) = \beta(y, 1)\beta(x, z) - \beta(x, yz) \\ &= \beta(yx, z) + \cancel{\beta(yz, \bar{x})} - \cancel{\beta(x, y\bar{z})} = \beta(yx, z),\end{aligned}$$

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 β es una forma bilineal no degenerada, se concluye que necesariamente $Q(x)1 = \bar{x}x$. Para la otra igualdad, sustituimos x por \bar{x} :

$$x\bar{x} = \bar{\bar{x}}\bar{x} = Q(\bar{x})1 = Q(x)1.$$

3. Siga el siguiente procedimiento:

$$\begin{aligned}\beta(\bar{x}(xy), z) &= \beta((\beta(x, 1)1 - x)(xy), z) \\ &= \beta(x, 1)\beta(xy, z) - \beta(x(xy), z) \\ &= \cancel{\beta(x(xy), z)} + \beta(xz, xy) - \cancel{\beta(x(xy), z)} \\ &= Q(x)\beta(z, y) = Q(x)\beta(y, z) = \beta(Q(x)y, z).\end{aligned}$$

4. Ejercicio.

5. Nótese que por la identidad (10.7)

$$\beta((\overline{xy})1, z) = \beta(1, \overline{xy}z) = \beta(1, (xy)z).$$

Veremos lo mismo para la otra:

$$\begin{aligned} \beta(\overline{y}x, z) &= \beta((\beta(y, 1)1 - y)(\beta(x, 1)1 - x), z) \\ &= \beta(y, 1)\beta(x, 1)\beta(1, z) - \beta(y, 1)\beta(x, z) - \beta(x, 1)\beta(y, z) - \beta(yx, z). \end{aligned}$$

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

$$\begin{aligned} \beta(\overline{y}x, z) &= \beta((xy)z, 1) + \beta(x, y)\beta(1, z) - \beta(yz, x) - \beta(xz, y) \\ &= \beta((xy)z, 1). \end{aligned} \quad \square$$

Definición 10.43: 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 10.44: Toda álgebra de composición es alternativa.

DEMOSTRACIÓN: Basta emplear el hecho de que $\overline{x} = \beta(x, 1)1 - x$ y las propiedades 3 y 4 del lema anterior. \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 10.45: 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 10.46: Sea B una A -álgebra. Son equivalentes:

1. B es una álgebra alternada con una involución $\bar{(\)}: 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 $\bar{x}\bar{y} = \bar{y}\bar{x}$ se demostraba únicamente empleando las proposiciones anteriores, de modo que también es válido aquí. Luego:

$$\begin{aligned} Q(xy)1 &= \bar{xy}(xy) = (\bar{y}\bar{x})(xy) = ((T(y)1 - y)\bar{x})(xy) \\ &= T(y)\bar{x}(xy) - (y\bar{x})(xy) = T(y)Q(x)y - y(\bar{x}x)y \\ &= Q(x)(T(y) - y)y = Q(x)\bar{y}y = Q(x)Q(y)1. \end{aligned} \quad \square$$

Definición 10.47: Sea B una A -álgebra con una involución $\bar{}: B \rightarrow B$ 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.
-

$$\overline{(x, y)} \cdot (x, y) = (\bar{x}, -y)(x, y) = (\bar{x}x - c\bar{y}y, y\bar{x} - y\bar{x}) = (Q(x) - cQ(y))1.$$

- 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.

Teorema 10.48: 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

$$\overline{[X, Y, Z]} = \overline{(XY)Z - X(YZ)} = \bar{Z}(\bar{Y}\bar{X}) - (\bar{Z}\bar{Y})\bar{X} = -[\bar{Z}, \bar{Y}, \bar{X}].$$

De modo que también concluye el caso restante. Si B es alternativo, entonces empleando $U = \bar{X}$ en (10.11) y recordando que $[\bar{x}, y, x] = 0$ y que $w(\bar{y}y) = y(\bar{y}w)$ y análogos, se obtiene que

$$[\bar{X}, X, Z] = (c[\bar{x}, \bar{w}, y], -[y, \bar{z}, \bar{x}]),$$

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 10.49: Sea (B, Q) una A -álgebra de composición y sea C una subálgebra propia de B que es invariante por $\bar{(\)}$ y tal que Q es no degenerada en C . Entonces C está encajado en una subálgebra de B que es también de composición y que es isomorfa a un c -duplicado de C .

DEMOSTRACIÓN: En primer lugar, nótese que como $Q|_C$ es no degenerada, entonces induce un producto interno y por descomposición ortogonal $B = C \oplus C^\perp$. Sea $t \in C^\perp$ tal que $c := -Q(t) \neq 0$. Como C es una subálgebra, entonces $1 \in C$ y luego $\beta(1, t) = 0$ de modo que $\bar{t} = -t$ y $t^2 = -\bar{t}t = -Q(t)1 = c1$. Por la ec. (10.9) se tiene que para todo $x \in C$ se cumple

$$\bar{x}t + \bar{t}x = \beta(x, t) = 0 \iff \bar{x}t = tx.$$

Sean $x, y \in C$ arbitrarios. Luego, por (10.7), se tiene que $\beta(x, yt) = \beta(\bar{y}x, t) = 0$ puesto que $\bar{y}x \in C$; de modo que $C \cdot t \subseteq C^\perp$ y $D := C \oplus C \cdot t$.

Como B es de composición se tiene que $\bar{x}(xy) = Q(x)y$, de lo que se deduce que

$$\bar{x}(zy) + \bar{z}(xy) = \beta(x, z)y,$$

empleando $z = t$ se obtiene que $\bar{x}(ty) = t(xy) = (\bar{y}\bar{x})t$ lo que, sustituyendo por sus conjugados nos da que

$$x(yt) = (yx)t.$$

Luego aplique $\overline{(\)}$ y nótese que

$$\bar{t}(\bar{x}\bar{y}) = (\bar{t}\bar{y})\bar{x} \iff \overline{(\bar{x}\bar{y})}t = (yx)t = (yt)\bar{x},$$

sustituyendo x por \bar{x} se obtiene que $(yt)x = (y\bar{x})t$. Por último,

$$(xt)(yt) = (t\bar{x})(yt) = t(\bar{x}y)t = (\bar{y}x)t^2 = c\bar{y}x.$$

Empleando todo ésto, se tiene que el producto en D está determinado por

$$(u + vt)(x + yt) = ux + c\bar{y}v + (v\bar{x} + yu)t,$$

que es claramente isomorfo al c -duplicado de C . \square

Teorema 10.50 – Teorema de Hurwitz: Sea A un dominio con $\text{car } A \neq 2$. Las álgebras de composición son las siguientes:

- (a) A .
- (b) Las álgebras cuadráticas.
- (c) Las álgebras cuaterniónicas.
- (d) Las álgebras octoniónicas.

DEMOSTRACIÓN: Sea (B, Q) una A -álgebra de composición. Si $B = A$ entonces estamos en el caso (a), y si no $A \subset B$ en cuyo caso, por el lema anterior, B contiene una A -álgebra cuadrática B_1 no degenerada e invariante salvo $(\bar{})$; 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 10.51: 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 β es raíz de algún polinomio $p(x) \in k[x]$, de modo que β es k -algebraico. Más aún, $k(\beta)$ tiene que ser claramente un cuerpo (la conmutatividad se sigue trivial de la conmutatividad de las potencias de β , y los inversos del hecho de que A es de división), luego es una extensión algebraica, pero entonces $k(\beta) = k$ y $\beta \in k$. \square

Teorema 10.52 – 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, busquemos $i \in A'$ tal que $Q(i) = 1$ y notamos que $i = -1$, 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 10.53 – Teorema de Wedderburn: Todo anillo de división finito es un cuerpo.

DEMOSTRACIÓN: Sea A un anillo de división finito de centro F , el cual es necesariamente un cuerpo. Definamos $q := |F|$ y $n := [A : F]$, de modo que $|A| = q^n$. $A^\times = A_{\neq 0}$ es un grupo multiplicativo y F^\times actúa sobre él, de modo que, por la ecuación de clases se obtiene

$$|A^\times| = q^n - 1 = \sum_a [A^\times : \text{Stab}_a] = q - 1 + \sum_{a \notin F} [A^\times : \text{Stab}_a],$$

donde a recorre representantes en las clases de equivalencia de la conjugación. Si $x_i \notin F$, entonces 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 (??) 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. Luego, las divisibilidades descienden a \mathbb{Z} y se obtiene que $\Phi_n(q) \mid q^n - 1$ y a los sumandos, de modo que $\Phi_n(q) \mid q - 1$. Ahora bien, $\Phi_n(q) = \prod_{\zeta} (q - \zeta)$ donde $\zeta \in \mathbb{C}$ recorre todas las raíces n -ésimas primitivas de la unidad, pero por desigualdad triangular $q \leq |q - \zeta| + 1$ donde la igualdad sólo se alcanza para la raíz de la unidad $\zeta = 1$ la que no está en Φ_n cuando $n > 1$, por lo que $|q - 1| < \prod_{\zeta} |q - \zeta| = |\Phi_n(\zeta)|$ lo cual es absurdo. \square

11.1 Resumen de categorías

Aquí haremos un resumen de los capítulos de categorías en mi libro de teoría de conjuntos [40]. Evitaré la mayoría de ejemplos que veo con detalle en el otro texto, la ventaja es que varias de las propiedades ya están expuestas incluso con el lenguaje categorial adecuado en el resto de éste texto.

Definición 11.1 – Categoría: Una categoría \mathcal{C} consta de:

1. Una clase $\text{Obj } \mathcal{C}$ de *objetos*.
2. Una clase $\text{Mor } \mathcal{C}$ de *morfismos* o *flechas*.
3. Un par de aplicaciones $\text{Dom}, \text{Cod}: \text{Mor } \mathcal{C} \rightarrow \text{Obj } \mathcal{C}$. Si $f \in \text{Mor } \mathcal{C}$ cumple que $\text{Dom}(f) = A$ y $\text{Cod}(f) = B$, entonces abreviaremos todo esto como que $A \xrightarrow{f} B$. Se define

$$\begin{aligned}\text{Hom}_{\mathcal{C}}(A, B) &:= \{f \in \text{Mor}(\mathcal{C}) : A \xrightarrow{f} B\}, \\ \text{End}_{\mathcal{C}}(A) &:= \text{Hom}_{\mathcal{C}}(A, A).\end{aligned}$$

(Se obviarán los subíndices cuando no haya ambigüedad sobre la categoría.)

Los morfismos de $\text{End}_{\mathcal{C}}(A)$ se llaman *endomorfismos*.

4. Una operación \circ tal que $A \xrightarrow{f} B$ y $B \xrightarrow{g} C$ cumpla que $A \xrightarrow{f \circ g} C$. Diremos que el siguiente diagrama:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow h & \downarrow g \\ & & C \end{array}$$

conmuta si $h = f \circ g$, o también cuando dos conjuntos de flechas que parten y terminan en los mismos lugares son iguales bajo composición.

Otra condición para la composición es que sea asociativa, i.e., que el diagrama

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & & \\ & \searrow f \circ g & \downarrow g & \searrow g \circ h & \\ & & C & \xrightarrow{h} & D \end{array}$$

conmute.

Se usaran flechas punteadas para indicar que existe un morfismo que hace que el diagrama conmute.

5. Una aplicación $1_- : \text{Obj}(\mathcal{C}) \rightarrow \text{Mor}(\mathcal{C})$ tal que $1_A \in \text{End}_{\mathcal{C}}(A)$, y que hace que el siguiente diagrama siempre conmute:

$$\begin{array}{ccc} A & \xrightarrow{1_A} & A \\ f \downarrow & \searrow f & \downarrow f \\ B & \xrightarrow{1_B} & B \end{array}$$

Dado eso podemos denotar $\mathcal{C} = (\text{Obj } \mathcal{C}, \text{Mor } \mathcal{C}, \text{Dom}, \text{Cod}, \circ, \text{Id})$.

Ejemplo. Ya lo hemos explicitado, pero casi todas las estructuras algebraicas aquí expuestas conforman categorías. En particular los grupos (Grp), los grupos abelianos (Ab), los anillos (Rng), los anillos unitarios (Ring), los dominios (CRing), los cuerpos (Fld), los R -módulos izquierdos (${}_R\text{Mod}$), los

R -módulos derechos (Mod_R), los k -espacios vectoriales (Vect_k) y las extensiones de cuerpo de k (Ext_k) son categorías con sus respectivas flechas.

Definición 11.2 – Funtor. Dadas dos categorías \mathcal{A} y \mathcal{B} , se dice que una función F es un *funtor (covariante)* entre ambas si:

1. Para todo $X \in \text{Obj } \mathcal{A}$ se cumple que $F(X) \in \text{Obj } \mathcal{B}$. En general denotaremos FX para ahorrar notación.
2. Para todo morfismo $X \xrightarrow{f} Y$ en \mathcal{A} se cumple que $FX \xrightarrow{F(f)} FY$ en \mathcal{B} .
3. Si $X \xrightarrow{f} Y$ y $Y \xrightarrow{g} Z$ en \mathcal{A} , entonces $F(f) \circ F(g) = F(f \circ g)$.
4. $F(1_X) = 1_{FX}$.

Se suele denotar que $F: \mathcal{A} \rightarrow \mathcal{B}$. En varios casos, ahorraremos todo esto mediante el siguiente diagrama:

$$\begin{array}{ccc} X & & FX \\ f \downarrow & \xRightarrow{F} & \downarrow F(f) \\ Y & & FY \end{array}$$

Motivados por el ejemplo de la categoría opuesta decimos que una función $F: \mathcal{A} \rightarrow \mathcal{B}$ es un *funtor contravariante* si:

1. Para todo morfismo $X \xrightarrow{f} Y$ en \mathcal{A} se cumple que $FY \xrightarrow{F(f)} FX$ (en \mathcal{B}).
2. Si $X \xrightarrow{f} Y$ y $Y \xrightarrow{g} Z$ en \mathcal{A} , entonces $F(g) \circ F(f) = F(f \circ g)$.
3. $F(1_X) = 1_{FX}$.

Cuando no se agregue nada a «funtor» se asume que es covariante.

Ejemplo. • Fijada una estructura algebraica X el funtor $\text{Hom}(X, -)$ es covariante y el funtor $\text{Hom}(-, X)$ es contravariante. Si la estructura es un grupo (abeliano), entonces el funtor tiene como categoría de codominio los grupos (abelianos). Si la estructura es un R -módulo, entonces el funtor tiene como categoría de codominio los R -módulos.

- Dado $f: X \rightarrow Y$ una función de conjuntos, podemos definir $F(f)$ como el único homomorfismo de grupos (resp. grupos abelianos, R -módulos) que extiende a la función $f \circ \iota: X \rightarrow F(Y)$ hasta $F(f): F(X) \rightarrow F(Y)$, donde $F(X)$ es el grupo (resp. grupo abeliano, R -módulo) libre que tiene por base al conjunto X . Ésto induce un funtor covariante desde Set hasta Grp (resp. Ab , Mod_R).

Definición 11.3: Sean $F, G: \mathcal{A} \rightarrow \mathcal{B}$ funtores. Se dice que φ es una *transformación natural* entre F y G si:

1. Para todo $X \in \text{Obj } \mathcal{A}$, $\varphi(X) \in \text{Hom}_{\mathcal{B}}(FX, GX)$.
2. Para todo $X \xrightarrow{f} Y$ en \mathcal{A} se cumple que el siguiente diagrama:

$$\begin{array}{ccc} FX & \xrightarrow{\varphi(X)} & GX \\ F(f) \downarrow & & \downarrow G(f) \\ FY & \xrightarrow{\varphi(Y)} & GY \end{array}$$

conmuta (en \mathcal{B}).

Ésto se denota como $\varphi: F \Rightarrow G$.

Análogamente si $F, G: \mathcal{A} \rightarrow \mathcal{B}$ funtores contravariantes. Se denota que $\varphi: F \Rightarrow G$ si el siguiente diagrama:

$$\begin{array}{ccccc} X & & FX & \xrightarrow{\varphi(X)} & GX \\ f \downarrow & \Longrightarrow & \uparrow F(f) & & \uparrow G(f) \\ Y & & FY & \xrightarrow{\varphi(Y)} & GY \end{array}$$

conmuta (en \mathcal{B}).

Definición 11.4: Se dice que un objeto X de una categoría \mathcal{C} es *inicial* (resp. *final*) si para todo objeto A existe un único morfismo $X \xrightarrow{f} A$ (resp. $A \xrightarrow{f} X$).

Un objeto es un *objeto nulo* si es inicial y final.

Ejemplo. En general, nuestras categorías constan de objetos nulos aparentes:

- El grupo trivial $\{e\}$ y el módulo trivial $\{\vec{0}\}$ son objetos nulos de los grupos y los módulos resp.
- El anillo trivial es un objeto nulo de \mathbf{Rng} , pero \mathbf{Ring} no tiene objeto nulo (pues el anillo trivial no es unitario).
- El cuerpo base k es el objeto inicial de \mathbf{Ext}_k y así se ve que dicha categoría no posee objeto final.

Definición 11.5 (Ecualizador y coecualizador): Sean $f, g \in \text{Hom}(X, Y)$. Un par (K, k) se dice un *ecualizador* de f, g si:

1. K es un objeto y $K \xrightarrow{k} X$ tales que $k \circ f = k \circ g$.
2. Si existe otro $M \xrightarrow{m} X$ tal que $m \circ f = m \circ g$, entonces existe un único morfismo $M \xrightarrow{n} K$ tal que $m = n \circ k$. Es decir, si el siguiente diagrama

$$\begin{array}{ccccc} M & & & & \\ \downarrow \exists! n & \searrow m & & & \\ K & \xrightarrow{k} & A & \xrightleftharpoons[f]{g} & B \end{array}$$

conmuta.¹

El dual de un ecualizador es un *coecualizador* entre f, g , el cual es un par (C, c) tal que:

1. C es un objeto e $Y \xrightarrow{c} C$ tal que $f \circ c = g \circ c$.
2. Si existe otro $Y \xrightarrow{m} M$ tal que $f \circ m = g \circ m$, entonces existe un único morfismo $C \xrightarrow{n} M$ tal que $m = c \circ n$. Es decir, si el siguiente diagrama

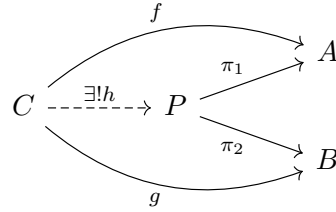
$$\begin{array}{ccccc} & & & & M \\ & & & \nearrow m & \uparrow \exists! n \\ A & \xrightleftharpoons[f]{g} & B & \xrightarrow{c} & C \end{array}$$

¹Aquí debe subentenderse que f y g no son necesariamente iguales, pero que el resto de composiciones si conmutan en el diagrama.

conmuta.

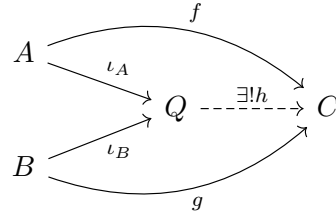
Si la categoría posee objetos nulos, llamamos el núcleo (resp. conúcleo) de f como el ecualizador (resp. coecualizador) con la flecha nula, y denotamos a éste objeto como $\ker f$ (resp. $\operatorname{coker} f$).

Definición 11.6 (Productos y coproductos): Dados los objetos de una categoría A, B ; entonces decimos que un objeto P es el *producto* de A con B si está dotado de unos morfismos $P \xrightarrow{\pi_1} A$ y $P \xrightarrow{\pi_2} B$ que llamamos *proyecciones naturales*, tal que para todo objeto C con morfismos $C \xrightarrow{f} A$ y $C \xrightarrow{g} B$ existe un único morfismo denotado $h := (f, g)$ tal que el siguiente diagrama



conmuta.

Así mismo, se dice que Q es el *coproducto* de A con B si está dotado de unos morfismos $A \xrightarrow{\iota_A} Q$ y $B \xrightarrow{\iota_B} Q$, que llamamos *inclusiones naturales*, tal que para todo objeto C con morfismos $A \xrightarrow{f} C$ y $B \xrightarrow{g} C$ existe un único morfismo denotado $h := f \amalg g$ tal que el siguiente diagrama



conmuta.

Definición 11.7: Se dice que una categoría \mathcal{D} es pequeña si sus objetos y flechas conforman un conjunto. Se le llama un *diagrama* en \mathcal{C} a un funtor fiel $X_-: \mathcal{D} \rightarrow \mathcal{C}$ tal que \mathcal{D} es una categoría pequeña a la que llamamos *categoría de índices*.

Definición 11.8: Dado un diagrama $X_-: \mathcal{D} \rightarrow \mathcal{C}$, un *cono* consiste de:

1. $C \in \text{Obj } \mathcal{C}$, un objeto.
2. Para cada $i \in \text{Obj } \mathcal{D}$, un morfismo $C \xrightarrow{p_i} A_i$.

Tales que para todo $i \xrightarrow{f} j$ en \mathcal{D} se cumpla que el siguiente diagrama

$$\begin{array}{ccc} & C & \\ p_i \swarrow & & \searrow p_j \\ A_i & \xrightarrow{Ff} & A_j \end{array}$$

conmute. Lo anterior se resume en « $(C, (p_i)_{i \in \mathcal{D}})$ es un cono».

La noción dual es un *co-cono*, que consiste de:

1. $C \in \text{Obj } \mathcal{C}$, un objeto.
2. Para cada $i \in \text{Obj } \mathcal{D}$, un morfismo $A_i \xrightarrow{q_i} C$.

Tales que para todo $i \xrightarrow{f} j$ en \mathcal{D} se cumpla que el siguiente diagrama

$$\begin{array}{ccc} A_i & \xrightarrow{Ff} & A_j \\ q_i \searrow & & \swarrow q_j \\ & C & \end{array}$$

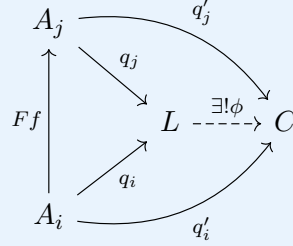
conmute.

Definición 11.9: Dado un diagrama $X_-: \mathcal{D} \rightarrow \mathcal{C}$, se dice que un *límite inverso* es un cono $(L, (p_i)_{i \in \mathcal{D}})$ tal que si $(C, (p'_i)_{i \in \mathcal{D}})$ es otro cono, se cumple que existe un único morfismo $C \xrightarrow{\phi} L$ tal que para todo $i \in \mathcal{D}$ se cumple que $p'_i = \phi \circ p_i$. En diagrama conmutativo:

$$\begin{array}{ccccc} & & p'_j & \rightarrow & A_j \\ & & \nearrow & & \nearrow p_j \\ C & \xrightarrow{\exists! \phi} & L & & \\ & & \searrow & & \searrow p_i \\ & & p'_i & \rightarrow & A_i \end{array} \quad \begin{array}{c} \uparrow \\ Ff \end{array}$$

Así mismo, un *límite directo* es un co-cono $(L, (q_i)_{i \in \mathcal{D}})$ tal que si $(C, (q'_i)_{i \in \mathcal{D}})$ es otro co-cono, se cumple que existe un único morfismo

$L \xrightarrow{\phi} C$ tal que para todo $i \in \mathcal{D}$ se cumple que $q'_i = q_i \circ \phi$. En diagrama conmutativo:



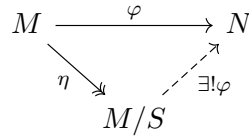
Algo interesante es que los límites inversos y directos generalizan las nociones de ecualizadores, coecualizadores, productos y coproductos; incluso, si la categoría es pequeña generalizan los objetos iniciales y finales.

La unicidad de todos éstos objetos se sigue de la siguiente proposición:

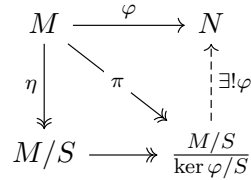
Proposición 11.10: Si un diagrama en \mathcal{C} posee límites (resp. colímites) entonces todos ellos son isomorfos.

§11.1.1 Las serpientes y sus amigos. En [40, §4.1.1] probamos el lema de la serpiente y otros lemas en el contexto general de categorías abelianas, aquí hacemos un repaso restringiéndonos a las categorías de módulos.

Proposición 11.11: Sea $\varphi: M \rightarrow N$ un homomorfismo de R -módulos, y sea $S \subseteq \ker \varphi$. Entonces existe un único homomorfismo de módulos $\psi: M/S \rightarrow N$ tal que el siguiente diagrama conmuta:



DEMOSTRACIÓN: Basta construir el siguiente diagrama y aplicar el tercer teorema de isomorfismos:



□

Lema 11.12 (corto de los cinco): Dado el siguiente diagrama conmutativo de R -módulos:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\psi} & B & \xrightarrow{\phi} & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & A' & \xrightarrow{\psi'} & B' & \xrightarrow{\phi'} & C' & \longrightarrow & 0 \end{array}$$

donde las filas son exactas. Entonces:

1. Si α y γ son monomorfismos, entonces β es monomorfismo.
2. Si α y γ son epimorfismos, entonces β es epimorfismo.
3. Si α y γ son isomorfismos, entonces β 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 $\mathbf{b} \in \ker \phi = \text{Im } \psi$ y existe $\mathbf{a} \in A$ tal que $\psi(\mathbf{a}) = \mathbf{b}$. Por ende $\beta(\psi(\mathbf{a})) = \psi'(\alpha(\mathbf{a}))$, pero ψ', α son monomorfismos, así que $\mathbf{a} = \vec{0}$.
2. Sea $\mathbf{x} \in B'$, entonces puesto que ϕ, γ 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 $\mathbf{x} - \beta(\mathbf{y}) \in \ker(\phi') = \text{Im}(\psi')$, luego puesto que α 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 11.13 (fuerte de los cuatro): Dado el siguiente diagrama conmutativo de R -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, μ epimorfismo y ν monomorfismo. Entonces:

$$\ker \gamma = \zeta[\ker \beta], \quad \text{Im } \beta = \xi^{-1}[\text{Im } \gamma].$$

Lema 11.14 (de los cinco): Dado el siguiente diagrama conmutativo de R -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 α_1 es epimorfismo y α_2, α_4 son monomorfismos, entonces α_3 es monomorfismo.
2. Si α_5 es monomorfismo y α_2, α_4 son epimorfismos, entonces α_3 es epimorfismo.
3. Si $\alpha_1, \alpha_2, \alpha_4, \alpha_5$ son isomorfismos, entonces α_3 es isomorfismo.

11.2 Homologías y cohomologías

Ahora definiremos el principal objeto de estudio del álgebra homológica. Veremos el caso particular de Mod_R , pero aplica para cualquier categoría abeliana.

Definición 11.15: Dado un anillo R , entonces una sucesión $\{K_n, \partial_n\}_{n \in \mathbb{Z}}$ se dice una *cadena de complejos* si cada K_n es un R -módulo, $\partial_n: K_n \rightarrow K_{n-1}$ es un homomorfismo de R -módulos y $\partial_{n+1}\partial_n = 0$, vale decir, si $\text{Img}(\partial_{n+1}) \subseteq \ker(\partial_n)$. La cadena se visualiza así:

$$K_\bullet: \cdots \leftarrow K_{-2} \xleftarrow{\partial_{-1}} K_{-1} \xleftarrow{\partial_0} K_0 \xleftarrow{\partial_1} K_1 \xleftarrow{\partial_2} K_2 \leftarrow \cdots$$

A los ∂_n 's se les llaman *operadores de borde*. Para toda cadena de complejos K_\bullet se define:

1. Los elementos de $Z_n(K_\bullet) := \ker(\partial_n: K_n \rightarrow K_{n-1})$ se dicen n -ciclos.
2. Los elementos de $B_n(K_\bullet) := \text{Img}(\partial_{n+1}: K_{n+1} \rightarrow K_n)$ se dicen n -fronteras.
3. El módulo

$$H_n(K_\bullet) := \frac{Z_n}{B_n} = \frac{\ker(\partial_n)}{\text{Img}(\partial_{n+1})},$$

se dice la *homología* n -dimensional de K_\bullet .

Dos n -ciclos c_1, c_2 se dicen *homólogos*, a veces denotado $c_1 \sim c_2$, si poseen la misma clase lateral en el $H_n(K_\bullet)$, vale decir, si $c_1 - c_2 \in B_n(K_\bullet)$. Se denota por $\text{cls}(c_1)$ la clase de homología de c_1 en $H_n(K_\bullet)$.

Así pues, K_\bullet se dice exacto en n si $H_n(K_\bullet) = 0$.

Dadas dos cadenas de complejos K_\bullet, K'_\bullet , se dice que una aplicación $f: K_\bullet \rightarrow K'_\bullet$, que es en realidad una sucesión de homomorfismos $(f_n: K_n \rightarrow K'_n)_{n \in \mathbb{Z}}$, es una *transformación de cadenas* si $\partial_n \circ f_{n-1} = f_n \circ \partial'_n$, vale decir si el siguiente diagrama conmuta:

$$\begin{array}{ccccccc} K_\bullet: & & \cdots & \longleftarrow & K_{-1} & \xleftarrow{\partial_0} & K_0 & \xleftarrow{\partial_1} & K_1 & \longleftarrow & \cdots \\ & & & & \downarrow f_{-1} & & \downarrow f_0 & & \downarrow f_1 & & \\ K'_\bullet: & & \cdots & \longleftarrow & K'_{-1} & \xleftarrow{\partial'_0} & K'_0 & \xleftarrow{\partial'_1} & K'_1 & \longleftarrow & \cdots \end{array}$$

Proposición 11.16: Las cadenas de complejos (como objetos) y las transformaciones de cadenas (como flechas) conforman una categoría, denotada $\text{Ch}(\mathcal{C})$; donde \mathcal{C} es una categoría abeliana de base, usualmente Mod_R o Ab .

Proposición 11.17: La n -ésima homología es un funtor covariante sobre las cadenas de complejos, formalmente si $f: K_\bullet \rightarrow K'_\bullet$ es una transformación de cadenas, entonces:

$$\begin{array}{ccc} H_n(f): H_n(K_\bullet) \longrightarrow H_n(K'_\bullet) & & \begin{array}{ccc} K_\bullet & & H_n(K_\bullet) \\ f \downarrow & \xRightarrow{H_n} & \downarrow H_n(f) \\ K'_\bullet & & H_n(K'_\bullet) \end{array} \\ c + B_n(K_\bullet) \longmapsto c + B_n(K'_\bullet) & & \end{array}$$

Definición 11.18: Dadas las transformaciones de cadenas $f, g: K_\bullet \rightarrow K'_\bullet$ se dice que una *homotopía de cadenas* s , denotada $s: f \simeq g$, a una sucesión de homomorfismos $(s_n: K_n \rightarrow K'_{n+1})_{n \in \mathbb{Z}}$ tal que

$$\partial_n \circ s_{n-1} + s_n \circ \partial'_{n+1} = f_n - g_n.$$

Teorema 11.19: Sean K_\bullet, K'_\bullet dos cadenas de complejos, $f, g: K_\bullet \rightarrow K'_\bullet$ dos transformaciones de cadenas y $s: f \simeq g$. Entonces $H_n(f) = H_n(g)$ para todo $n \in \mathbb{Z}$.

DEMOSTRACIÓN: Sea n fijo y $c \in Z_n$ un n -ciclo de K_n , basta ver que $f_n(c)$ y $g_n(c)$ son homólogos lo que se sigue de:

$$\begin{aligned} f_n(c) - g_n(c) &= s_{n-1}(\partial_n(c)) + \partial'_{n+1}(s_n(c)) \\ &\equiv s_{n-1}(\partial_n(c)) = s_{n-1}(0) = 0. \quad (\text{mód } B_n) \end{aligned} \quad \square$$

Definición 11.20: Una transformación de cadenas $f: K_\bullet \rightarrow K'_\bullet$ se dice una *equivalencia de cadenas* si existe otra transformación $g: K'_\bullet \rightarrow K_\bullet$ tal que $f \circ g \simeq \text{Id}_K$ y $g \circ f \simeq \text{Id}_{K'}$. En cuyo caso, g se dice una *inversa homotópica* de f .

Corolario 11.21: Si $f: K_\bullet \rightarrow K'_\bullet$ es una equivalencia de cadenas, entonces $H_n(f): H_n(K_\bullet) \rightarrow H_n(K'_\bullet)$ es un isomorfismo para todo $n \in \mathbb{Z}$.

Dado que desde ahora se asume familiaridad con las nociones categoriales podemos darnos libertades en nuestras definiciones:

Definición 11.22: Dado una cadena de complejos K_\bullet , se dice que una cadena S_\bullet es una *subcadena* de K_\bullet si la inclusión $\iota: S_\bullet \rightarrow K_\bullet$ es una transformación de cadenas. Ésto significa que cada S_n es un submódulo de K_n y que los operadores de borde de S_\bullet son las restricciones de los de K_\bullet , y naturalmente también satisfacen que $\text{Img}(\partial_n|_{S_n}) \subseteq \ker(\partial_{n+1}|_{S_{n+1}})$; en general, por abuso de notación, obviaremos los símbolos de restricción que están implícitos.

Dada una subcadena $S_\bullet \subseteq K_\bullet$ se define el *cociente de cadenas*, denotado por $(K/S)_\bullet$, como la cadena de complejos junto a los únicos operadores de borde ∂'_n tales que para todo $n \in \mathbb{Z}$ el siguiente diagrama conmuta:

$$\begin{array}{ccccccc} K_\bullet: & \cdots & \longleftarrow & K_n & \xleftarrow{\partial_{n+1}} & K_{n+1} & \longleftarrow \cdots \\ & & & \downarrow \pi_n & & \downarrow \pi_{n+1} & \\ (K/S)_\bullet: & \cdots & \longleftarrow & K_n/S_n & \xleftarrow{\partial'_{n+1}} & K_{n+1}/S_{n+1} & \longleftarrow \cdots \end{array}$$

Nótese que dichos ∂'_n existen y son únicos por la proposición 11.11. En consecuencia, todo cociente de cadenas viene con una transformación canónica $\pi: K_\bullet \rightarrow (K/S)_\bullet$.

Proposición 11.23: Dada una subcadena $S_\bullet \subseteq K_\bullet$, entonces la siguiente sucesión es exacta (en Ch):

$$0 \longrightarrow S_\bullet \xrightarrow{\iota} K_\bullet \xrightarrow{\pi} (K/S)_\bullet \longrightarrow 0.$$

Definición 11.24: Dada una transformación de cadenas $f: K_\bullet \rightarrow K'_\bullet$ se define $\ker f$ como la subcadena de K_\bullet dada por los módulos $\ker(f_n)$ con las restricciones de ∂_n . Similarmente, $\text{Img}(f)$ es una subcadena de K'_\bullet y podemos definir $\text{coker}(f) := (K'/\text{Img } f)_\bullet$.

Proposición 11.25: Dada una transformación de cadenas $f: K_\bullet \rightarrow K'_\bullet$, entonces $\ker(f)$ y $\text{coker}(f)$ son efectivamente el núcleo y conúcleo de f en la categoría Ch . En consecuencia, la siguiente sucesión es exacta:

$$0 \longrightarrow \ker f \longrightarrow K_\bullet \xrightarrow{f} K'_\bullet \longrightarrow \text{coker } f \longrightarrow 0.$$

Definición 11.26: Dada una cadena de complejos K_\bullet , es útil cambiar $\partial_{-n}: K_{-n} \rightarrow K_{-n-1}$ por $\delta^n: K^n \rightarrow K^{n+1}$, esto se conoce como «la notación por superíndices» y cuando querramos enfatizarla denotaremos K^\bullet , en cuyo caso diremos que K^\bullet es un *co-cadena de complejos*. Así pues, una co-cadena de complejos K^\bullet se dice *positiva* si $K^n = 0$ para todo $n < 0$, es decir, que la cadena se ve así:

$$K^\bullet: \dots \longrightarrow 0 \longrightarrow 0 \longrightarrow K^0 \xrightarrow{\delta^0} K^1 \xrightarrow{\delta^1} K^2 \longrightarrow \dots$$

Las co-cadenas de complejos también conforman una categoría, denotada $\text{CoCh}(\mathcal{C})$

Definición 11.27: Dada una cadena de complejos K_\bullet de R -módulos y dado un R -módulo G se induce una co-cadena de complejos:

$$\text{Hom}^\bullet(K, G): \dots \longrightarrow \text{Hom}(K_n, G) \xrightarrow{\delta^n} \text{Hom}(K_{n+1}, G) \longrightarrow \dots$$

donde se define:

$$\begin{aligned} \delta^n: \text{Hom}(K_n, G) &\longrightarrow \text{Hom}(K_{n+1}, G) \\ f &\longmapsto (-1)^{n+1} \cdot (\partial_{n+1} \circ f) \end{aligned}$$

Como $\text{Hom}^\bullet(K, G)$ es una co-cadena, denotamos $\text{Hom}^n(K, G) := \text{Hom}(K_n, G)$. Se define:

1. Los elementos de $\ker(\delta^{n+1})$ se dicen n -cociclos.
2. Los elementos de $\text{Img}(\delta^n)$ se dicen n -cofronteras.

3. El módulo

$$H^n(K, G) := \frac{\ker(\delta^n)}{\text{Img}(\delta^{n-1})}$$

se denomina la *cohomología* n -dimensional de K_\bullet con coeficientes en G .

Dados K_\bullet, L_\bullet dos cadenas de complejos, se induce una cadena

$$\text{Hom}_n(K, L) := \prod_{p \in \mathbb{Z}} \text{Hom}(K_p, L_{p+n}),$$

de modo que un elemento es una tupla $(f_p)_{p \in \mathbb{Z}}$. Definimos el operador de borde sobre la cadena como $\partial_H f$ que corresponde a una tupla $(\partial_H f_p)_p$ dado por:

$$\begin{aligned} \partial_H f_p: K_p &\longrightarrow L_{p+n-1} \\ \mathbf{k} &\longmapsto \partial_L(f_p(\mathbf{k})) + (-1)^{n+1} f_{p-1}(\partial_K(\mathbf{k})) \end{aligned}$$

donde ∂_K, ∂_L son los operadores de borde de K_\bullet, L_\bullet resp. Queda de ejercicio verificar que efectivamente ∂_H es un operador de borde.

Proposición 11.28: Dados K_\bullet, L_\bullet un par de cadenas de complejos. Un 0-ciclo $(f_p)_p$ de $\text{Hom}_\bullet(K, L)$ es de hecho una transformación de cadenas $f: K_\bullet \rightarrow L_\bullet$. Más aún, $(f_p)_p$ es la frontera de un $s \in \text{Hom}_1(K, L)$ syss s es una homotopía tal que $s: f \simeq 0$.

DEMOSTRACIÓN: $(f_p)_p$ es un 0-ciclo syss

$$\partial_H f_p = f_p \circ \partial_L - \partial_K \circ f_{p-1} = 0,$$

lo que equivale a ser una transformación de cadenas. Por otro lado, si $(s_p: K_p \rightarrow L_{p+1})$ satisface que:

$$\partial_H s_p = s_p \circ \partial_L + \partial_K \circ s_{p-1} = f_p$$

ésto es literalmente que $s: f \simeq 0$. □

Corolario 11.29: Dados K_\bullet, L_\bullet un par de cadenas de complejos. $H_0(\text{Hom}_\bullet(K, L))$ es el grupo abeliano de clases de equivalencia de transformaciones de cadenas salvo homotopías.

Considere la siguiente sucesión exacta:

$$E: \quad 0 \longrightarrow K_{\bullet} \xrightarrow{\psi} L_{\bullet} \xrightarrow{\phi} M_{\bullet} \longrightarrow 0 \quad (11.1)$$

Dado $(n+1)$ -ciclo m de M , por definición $\partial m = 0$. Como $\phi_{n+1}: L_{n+1} \rightarrow M_{n+1}$ es epimorfismo, entonces existe $l \in L_{n+1}$ con $\phi(l) = m$, y luego $\phi(\partial l) = 0$; nótese que ∂l sólo depende de m . Como $\psi_n: K_n \rightarrow L_n$ es monomorfismo, entonces existe un único $k \in K_n$ tal que $\psi(k) = \partial l$. Luego, $\text{cls}(k)$ depende exclusivamente de $\text{cls}(m)$, por lo que podemos definir:

$$\partial_E: H_{n+1}(M) \longrightarrow H_n(K)$$

como el único homomorfismo de grupos abelianos tal que $\partial_E(\text{cls } m) = \text{cls } k$. A veces se escribe que $\partial_E = \partial_M \circ (\phi_*)^{-1} \circ (\psi_*)^{-1}$, pese a que las funciones no poseen inversa. Visualmente:

$$\begin{array}{ccc} l & \xrightarrow{\quad} & m \\ \downarrow & & \downarrow \\ c & \xrightarrow{\quad} & \partial l \end{array} \xrightarrow{\quad} 0 \quad \text{en} \quad \begin{array}{ccc} L_{n+1} & \xrightarrow{\quad} & M_{n+1} \\ \downarrow & & \downarrow \\ K_n & \xrightarrow{\quad} & L_n \xrightarrow{\quad} M_n \end{array} \quad (11.2)$$

A éste ∂_E le llamamos el *homomorfismo conector*.

Teorema 11.30: Dada la sucesión exacta de cadenas de complejos (11.1), entonces induce la siguiente sucesión exacta de homología:

$$\begin{array}{ccccccc} & & \cdots & \longrightarrow & H_{n+1}(M) & & \\ & & & & \downarrow \partial_E & & \\ & \xrightarrow{\quad} & H_n(K) & \xrightarrow{\psi_*} & H_n(L) & \xrightarrow{\phi_*} & H_n(M) \\ & & & & \downarrow \partial_E & & \\ & \xrightarrow{\quad} & H_{n-1}(K) & \longrightarrow & \cdots & & \end{array}$$

donde $\psi_* := H_n(\psi)$ y $\phi_* := H_n(\phi)$.

DEMOSTRACIÓN: Es claro que la sucesión descrita es un complejo de cadenas. Para completar la exactitud aún hay que ver tres detalles más:

- 1) $\ker(\psi_*) \subseteq \partial_E[H_{n+1}(M)]$: Ésto se deduce de la exposición preliminar al teorema.

- II) $\ker(\phi_*) \subseteq \psi_*[H_n(K)]$: Sea $c \in L_n$ un n -ciclo, con $\phi_*(\text{cls } c) = \text{cls } 0$, luego $\phi(c) = \partial m$ para algún $m \in M_{n+1}$. Como ϕ es un epimorfismo existe un $l \in L_{n+1}$ con $\phi(l) = m$. Luego $\phi(c - \partial l) = 0$, por lo que $c - \partial l = \psi(k)$ para algún $k \in K_n$ y $\partial k = 0$. Finalmente

$$\text{cls } c = \text{cls}(c - \partial l) = \psi_*(\text{cls } k).$$

- III) $\ker(\partial_E) \subseteq \phi_*[H_n(M)]$: Sea $m \in \ker(\partial_E)$, luego siguiendo la situación en (11.2) tenemos que $c = \partial k$ con $k \in K_{n+1}$ pues $\text{cls } c = 0$. Como $\psi(\partial k) = \partial l$, entonces $\phi(l - \psi(k)) = \phi(l) = m$, de modo que $m \in \phi_*[H_n(L)]$. \square

Proposición 11.31: Las sucesiones exactas cortas en \mathcal{Ch} y las flechas que hacen al diagrama conmutar conforman una categoría \mathcal{E} . Visualmente:

$$\begin{array}{ccccccc} E: & 0 & \longrightarrow & K_\bullet & \longrightarrow & L_\bullet & \longrightarrow & M_\bullet & \longrightarrow & 0 \\ f \downarrow & \longleftarrow & & \downarrow f_K & & \downarrow f_L & & \downarrow f_M & & \\ E': & 0 & \longrightarrow & K'_\bullet & \longrightarrow & L'_\bullet & \longrightarrow & M'_\bullet & \longrightarrow & 0 \end{array}$$

Para todo $n \in \mathbb{Z}$, $H_n(K), H_n(L), H_n(M)$ determinan funtores sobre \mathcal{E} . Finalmente, el homomorfismo conector $\partial_E: H_{n+1}(M) \Rightarrow H_n(K)$ es una transformación natural.

Definición 11.32: Dada una transformación de cadenas $f: K_\bullet \rightarrow K'_\bullet$ se define el *cono de mapas*² como la cadena de complejos $M_\bullet(f)$ dada por:

$$M_n(f) := K_{n-1} \oplus K'_n, \quad \partial_M(k, k') := (-\partial k, \partial k' + f(k)).$$

Dado K_\bullet , denotamos K_\bullet^+ con $K_n^+ := K_{n-1}$ y $\partial_{K^+} := -\partial_K$.

Como ejercicio, demuestre que efectivamente se trata de una cadena de complejos.

Proposición 11.33: Dada una transformación de cadenas $f: K_\bullet \rightarrow K'_\bullet$, entonces la siguiente sucesión es exacta:

$$E_f: \quad 0 \longrightarrow K'_\bullet \xrightarrow{\iota} M_\bullet(f) \xrightarrow{\pi} K_\bullet^+ \longrightarrow 0 \quad (11.3)$$

²eng. *mapping cone*.

Proposición 11.34: Sea $f: K_\bullet \rightarrow K'_\bullet$ una transformación de cadenas y sea M_\bullet su cono de mapas, entonces induce la siguiente sucesión exacta:

$$\cdots \rightarrow H_n(K) \xrightarrow{\partial_E f} H_n(K') \xrightarrow{\iota_*} H_n(M) \xrightarrow{\pi_*} H_{n-1}(K) \rightarrow \cdots$$

Así pues, $M_\bullet(f)$ nos ayuda a «arreglar el error» de la exactitud del diagrama.

Teorema 11.35: Sea G un R -módulo y considere la sucesión exacta de cadenas de complejos (11.1), entonces existe un homomorfismo conector $\delta_E: H^n(K, G) \rightarrow H^{n+1}(M, G)$ tal que:

$$\cdots \leftarrow H^{n-1}(M, G) \xleftarrow{\delta_E} H^n(K, G) \xleftarrow{\psi_*} H^n(L, G) \xleftarrow{\phi_*} H^n(M, G) \leftarrow \cdots$$

Teorema 11.36: Sea K_\bullet una cadena de complejos. Ésto determina los siguientes funtores:

$$\begin{array}{ccc} G & \text{Hom}^\bullet(K, G) & G \\ f \downarrow & \xrightarrow{F} \downarrow f_* & f \downarrow \\ G' & \text{Hom}^\bullet(K, G') & G' \end{array} \quad \begin{array}{ccc} G & H^n(K, G) & \\ f \downarrow & \xrightarrow{G} \downarrow f_* & \\ G' & H^n(K, G') & \end{array}$$

donde $F: \text{Mod}_R \rightarrow \text{CoCh}(\text{Mod}_R)$ y $G: \text{Mod}_R \rightarrow \text{Mod}_R$.

Más aún, dada la siguiente sucesión exacta (en Mod_R):

$$S: \quad 0 \longrightarrow G' \xrightarrow{\lambda} G \xrightarrow{\tau} G'' \longrightarrow 0$$

entonces podemos considerar \mathcal{S} la categoría de sucesiones exactas cortas en Mod_R con las flechas correspondientes y considerar al homomorfismo conector $\delta_S: H^n(K, G'') \Rightarrow H^{n+1}(K, G')$ como una transformación natural que además induce la siguiente sucesión exacta larga:

$$\cdots \rightarrow H^n(K, G') \xrightarrow{\lambda_*} H^n(K, G) \xrightarrow{\tau_*} H^n(K, G'') \xrightarrow{\delta_S} H^{n+1}(K, G') \rightarrow \cdots$$

§11.2.1 Aplicación: El lema de la serpiente. Las homologías nos permiten demostrar facilmente dos lemas clásicos. También se pueden probar sin homologías mediante un poco de *persecuimiento de diagramas* (cf. [40, lema 4.29] y [40, teo. 4.34]).

Lema 11.37 (de 3×3): Dado el siguiente diagrama conmutativo de R -módulos:

$$\begin{array}{ccccccc}
& 0 & & 0 & & 0 & \\
& \downarrow & & \downarrow & & \downarrow & \\
0 & \rightarrow & A_3 & \xrightarrow{\alpha_3} & A_2 & \xrightarrow{\alpha_2} & A_1 \rightarrow 0 \\
& \psi \downarrow & & \downarrow & & \downarrow \psi' & \\
0 & \rightarrow & B_3 & \xrightarrow{\beta_3} & B_2 & \xrightarrow{\beta_2} & B_1 \rightarrow 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 & \rightarrow & C_3 & \xrightarrow{\gamma_3} & C_2 & \xrightarrow{\gamma_2} & C_1 \rightarrow 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
& 0 & & 0 & & 0 &
\end{array}$$

donde las columnas y la fila central son exactas. Entonces la fila superior es exacta y la fila inferior lo es.

DEMOSTRACIÓN: En primer lugar, nótese que la exactitud de B_\bullet induce que A_\bullet es una cadena de complejos: En efecto, $\alpha_2 \circ \alpha_1 \circ \psi' = \psi \circ \beta_2 \circ \beta_1 = 0$ y ψ' es monomorfismo, luego $\alpha_2 \circ \alpha_1 = 0$. Luego podemos construir la sucesión exacta:

$$\cdots \longrightarrow H_{n+1}(C) \longrightarrow H_n(A) \longrightarrow H_n(B) \longrightarrow \cdots$$

y si B_\bullet y C_\bullet son exactos, sus homologías son nulas y así las de A_\bullet también por lo que es exacto. Análogamente se deduce la otra implicancia. \square

Teorema 11.38 – Lema de la serpiente: Dado el siguiente diagrama de R -módulos con filas exactas:

$$\begin{array}{ccccccc}
A & \xrightarrow{\psi} & B & \xrightarrow{\phi} & C & \longrightarrow & 0 \\
\downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\
0 & \longrightarrow & A' & \xrightarrow{\psi'} & B' & \xrightarrow{\phi'} & C'
\end{array}$$

se induce la siguiente sucesión exacta:

$$\ker \alpha \rightarrow \ker \beta \rightarrow \ker \gamma \xrightarrow{\partial} \operatorname{coker} \alpha \rightarrow \operatorname{coker} \beta \rightarrow \operatorname{coker} \gamma$$

DEMOSTRACIÓN: Es claro que la sucesión es de hecho una cadena de complejos. Empleando la fórmula del homomorfismo conector, se define:

$$\partial := \iota \circ \phi^{-1} \circ \beta \circ (\psi')^{-1} \circ \pi.$$

Luego veamos que la sucesión es exacta en $\operatorname{coker} \alpha$: Sea $\psi'_*(a' + \alpha[A]) = \bar{0}$ con $a' \in A'$, vale decir, $\psi'(a') = \beta(b)$ para algún $b \in B$, por lo que

$$0 = \phi'(\psi'(a')) = \phi'(\beta(b)) = \gamma(\phi(b)).$$

Así $\phi(b) \in \ker \gamma$ y $\partial(\phi(b)) = a' + \alpha[A]$, es decir, $a' + \alpha[A] \in \partial[\ker \gamma]$. \square

11.3 Extensiones y resoluciones

Definición 11.39: Dado un anillo R y un par de R -módulos A, C ; se dice que una *extensión* de A sobre C es una sucesión exacta corta de R -módulos:

$$E: \quad 0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$$

Una *morfismo* de extensiones $\Gamma: E \rightarrow E'$ es una terna (α, β, γ) de homomorfismos de R -módulos de modo que el siguiente diagrama conmuta:

$$\begin{array}{ccccccccc} E: & 0 & \longrightarrow & A & \xrightarrow{\psi} & B & \xrightarrow{\phi} & C & \longrightarrow & 0 \\ \Gamma \downarrow & & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ E': & 0 & \longrightarrow & A' & \xrightarrow{\psi'} & B' & \xrightarrow{\phi'} & C & \longrightarrow & 0 \end{array} \quad (11.4)$$

Dos extensiones E, E' se dicen *congruentes* si existe un morfismo $\Gamma: E \rightarrow E'$, donde $\Gamma = (1_A, \beta, 1_C)$, en cuyo caso denotamos $E \equiv E'$; nótese que por el lema corto de los cinco β tiene que ser necesariamente un isomorfismo. Se denota por $\text{Ext}_R(C, A)$ a las clases de congruencia de extensiones de A sobre C .

Proposición 11.40: Sea A un grupo abeliano (un \mathbb{Z} -módulo) y $m \in \mathbb{N}_{\neq 0}$, entonces existe una biyección:

$$\eta: \text{Ext}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \longrightarrow A/mA.$$

DEMOSTRACIÓN: Dadas las extensiones de A como en (11.4), donde $C = \mathbb{Z}/m\mathbb{Z}$, entonces como ϕ es epimorfismo se cumple que existe $u \in B$ tal que $\phi(u) = [1] \in \mathbb{Z}/m\mathbb{Z}$. Luego todo $b \in B$ se escribe de forma única como $b = \psi(a) + nu$ donde $n \in \{0, 1, \dots, m-1\}$. Nótese que $\phi(mu) = m \cdot [1] = [0]$, por lo que $mu = \psi(g)$ para un único $g \in A$. Nótese que g determina la aritmética sobre B puesto que

$$\begin{aligned} (\psi a + nu) + (\psi a' + n'u) &= \psi(a + a') + (n + n')u \\ &= \psi(a + a' + g) + (n + n' - m)u \end{aligned}$$

así que en B la aritmética parece comportarse como cíclica en u compensando con g . Si bien el g es único en términos de u , el u no es único en el sentido de

que puede reemplazarse por $u' := u + \psi d$ para $d \in A$, y por tanto, $g' = g + md$, así pues, si bien g no es único, la clase lateral $g + mA = [g] \in A/mA$ sí es única. Definiendo $\eta(E) := [g]$ se nota que $E \equiv E'$ implica que $\eta(E) = \eta(E')$. Análogamente para todo $[g] \in A/mA$ definamos $B := A \times \mathbb{Z}/m\mathbb{Z}$ (como conjunto), con la operación dada por la fórmula anterior y así se obtiene una extensión con $\eta(E) = [g]$. \square

11.4 Hom y \otimes

Ahora, por un momento, quitemos las restricciones de conmutatividad y volvamos a ver qué es lo que hace al funtor \otimes tan útil.

Definición 11.41: Sean R, S anillos. Será útil denotar ${}_R M$ (resp. M_S) para decir que M es un R -módulo izquierdo (resp. un S -módulo derecho). Se dice que M es un R - S -bimódulo si es un R -módulo izquierdo y un S -módulo derecho, lo cuál puede abreviarse como ${}_R M_S$.

Definición 11.42: Sea R un anillo y sean M_R y ${}_R N$ módulos. Se dice que una aplicación $f: M \times N \rightarrow G$, donde G es un grupo abeliano, es R -biaditiva si:

$$\text{BA1. } f(\mathbf{m}_1 + \mathbf{m}_2, \mathbf{n}) = f(\mathbf{m}_1, \mathbf{n}) + f(\mathbf{m}_2, \mathbf{n}).$$

$$\text{BA2. } f(\mathbf{m}, \mathbf{n}_1 + \mathbf{n}_2) = f(\mathbf{m}, \mathbf{n}_1) + f(\mathbf{m}, \mathbf{n}_2).$$

$$\text{BA3. } f(\mathbf{m}r, \mathbf{n}) = f(\mathbf{m}, r\mathbf{n}).$$

Se dice que $M \otimes_R N$ es un producto tensorial de M, N si para todo grupo abeliano G y toda aplicación R -biaditiva $f: M \times N \rightarrow G$, se cumple que existe un único $\hat{f}: M \otimes_R N \rightarrow G$ homomorfismo de grupos tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} M \times N & \xrightarrow{\quad \otimes \quad} & M \otimes_R N \\ & \searrow f & \swarrow \exists! \hat{f} \\ & G & \end{array}$$

La misma demostración aquí vale:

Teorema 11.43: El producto tensorial de R -módulos existe y es único salvo isomorfismo.

Teorema 11.44: Sean R, S anillos y $M_R, {}_R N_S$ módulos. Entonces $M \otimes_R N$ es un S -módulo derecho con

$$(\mathbf{m} \otimes \mathbf{n})s = \mathbf{m} \otimes (\mathbf{n}s).$$

Similarmente si ${}_S M_R, {}_R N$ son módulos, entonces $M \otimes_R N$ es un S -módulo izquierdo con

$$s(\mathbf{m} \otimes \mathbf{n}) = (s\mathbf{m}) \otimes \mathbf{n}.$$

Corolario 11.45: Sean R, S anillos y ${}_R M_S$ un módulo, entonces $- \otimes_R M: \text{Mod}_R \rightarrow \text{Mod}_S$ y $M \otimes_S -: {}_S \text{Mod} \rightarrow {}_R \text{Mod}$ son funtores covariantes.

Naturalmente la historia se simplificaba en los anillos conmutativos pues todo módulo puede verse como un bimódulo.

Teorema 11.46: Sean R, S anillos. Entonces:

1. Dados ${}_R M_S, {}_R N$ módulos, entonces $\text{Hom}_R(M, N)$ es un S -módulo izquierdo con $(sf)(\mathbf{m}) = f(\mathbf{m}s)$.
2. Dados ${}_R M_S, N_S$ módulos, entonces $\text{Hom}_S(M, N)$ es un R -módulo derecho con $(fr)(\mathbf{m}) = f(r\mathbf{m})$.
3. Dados $M_R, {}_S N_R$ módulos, entonces $\text{Hom}_R(M, N)$ es un S -módulo izquierdo con $(sf)(\mathbf{m}) = f(s\mathbf{m})$.
4. Dados ${}_S M, {}_S N_R$ módulos, entonces $\text{Hom}_S(M, N)$ es un R -módulo derecho con $(fr)(\mathbf{m}) = f(\mathbf{m}r)$.

Parte III.

GEOMETRÍA ALGEBRAICA

12

Teoría de valuación

12.1 Dependencia íntegra

Definición 12.1: Dado un dominio A , se dice que una aplicación $\alpha: A \rightarrow B$ es una A -álgebra si es un homomorfismo de anillos y $\text{Img } \alpha$ está contenido en el centro de B . De no haber ambigüedad en los signos diremos simplemente que « B es un A -álgebra».

Se dice que B/A es una extensión de anillos si $\alpha: A \rightarrow B$ es una A -álgebra y α es inyectivo.

Nótese que ahora hemos dado la definición pura, análoga al tema de cuerpos. Aquí la A -álgebra es el homomorfismo, pues éste contiene toda la información involucrada. El pedir que α sea inyectivo es para subentenderse que A «está contenida» en B .

Ejemplo. • Sea k un cuerpo y sea K/k una extensión de cuerpos. Entonces K/k es una extensión de anillos.

- Para todo dominio A , se cumple que $A[x]$ es una extensión de anillos. Y más generalmente para cualquier conjunto S de indeterminadas $A[S]$ es una extensión de anillos.
- Sea X un conjunto cualquiera, entonces $\text{Func}(X; A)/A$ es una extensión de anillos.

- Si D es un dominio íntegro, $\text{Frac}(D)/D$ es una extensión de anillos. En particular, \mathbb{Q}/\mathbb{Z} y $k(x)/k[x]$ son extensiones de anillos.
- Sea $n \in \mathbb{N}_{\neq 0}$, entonces $\text{Mat}_n(A)/A$ es una extensión de anillos.
- Si $\mathfrak{a} \triangleleft A$ es un ideal propio, entonces A/\mathfrak{a} un A -álgebra que no es una extensión de anillos. $\mathbb{Z}/n\mathbb{Z}$ es una \mathbb{Z} -álgebra que no es una extensión de \mathbb{Z} .

Definición 12.2: Dado un par de A -álgebras $\alpha: A \rightarrow B$ y $\beta: A \rightarrow C$, una aplicación $\varphi: B \rightarrow C$ es un A -morfismo si el siguiente diagrama

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & C \\ \alpha \uparrow & & \uparrow \beta \\ A & \xrightarrow{\text{Id}_A} & A \end{array}$$

conmuta (en Ring).

Proposición 12.3: Sea A un dominio y B un A -álgebra. Entonces:

1. $\text{Id}_B: B \rightarrow B$ es un morfismo de A -álgebras.
2. La composición de A -morfismos también es un A -morfismo.

En consecuencia, las A -álgebras (como objetos) y los A -morfismos (como flechas) conforman una categoría, denotada Alg_A .

Proposición 12.4: Toda A -álgebra es también un A -módulo y, de hecho, todo A -morfismo es también un morfismo de A -módulos. En consecuencia, Alg_A es una subcategoría de Mod_A .

Del mismo modo en que tenemos una noción de *módulo libre* y de *grupo libre*, podemos dar una definición de *álgebra libre*:

Definición 12.5: Sea B un A -álgebra. Una base X de B es un subconjunto tal que toda aplicación $f: X \rightarrow C$, donde C es otra A -álgebra admita una única extensión $\bar{f}: B \rightarrow C$ a un morfismo de A -álgebras. Si B posee una base X , entonces se dice que es un A -álgebra libre sobre X .

Teorema 12.6: Dado un conjunto cualquiera S , entonces el anillo de polinomios $A[S]$ es un A -álgebra libre sobre S .

DEMOSTRACIÓN: Sea B un A -álgebra arbitraria y $f: S \rightarrow B$. Podemos ver a S como una tupla de indeterminadas $(x_i)_{i \in I}$, y entonces definir $t_i := f(x_i)$. Finalmente \bar{f} es la evaluación de los polinomios en $(t_i)_{i \in I}$, vale decir:

$$\begin{aligned} \bar{f}: A[S] &\longrightarrow B \\ p(x_{i_1}, \dots, x_{i_n}) &\longmapsto p(t_{i_1}, \dots, t_{i_n}) \end{aligned}$$

donde la aplicación está bien definida en el sentido de que todo polinomio en $A[S]$ sólo contiene finitas indeterminadas. \square

En éste capítulo, emplearemos $A^F[S]$ para denotar al anillo de polinomios con indeterminadas en S , ésto para evitar futuras confusiones.

Corolario 12.7: Todo A -álgebra libre de base X es isomorfa (como A -álgebra) a $A^F[X]$. Más aún, dos A -álgebras libres son isomorfas syss poseen bases de igual cardinalidad.

Ejemplo. Por el corolario anterior si S es un conjunto finito de indeterminadas, entonces $\text{Func}(S; A) \cong A^F[S]$ como A -álgebras.

Ésto nos da un buen vistazo a la categoría de álgebras. Ahora procedemos a dar una definición de ser un «sistema generador» y, en particular, de ser finitamente generado.

Definición 12.8: Dado un A -álgebra $\alpha: A \rightarrow B$. Se dice que $S \subseteq B$ es una subálgebra si es un subanillo y $\text{Im } \alpha \subseteq S$. Equivalentemente, $\bar{\alpha}: A \rightarrow S$ es un subálgebra si el siguiente diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \uparrow \text{Id} & & \uparrow \iota \\ A & \xrightarrow{\bar{\alpha}} & S \end{array}$$

conmuta (en Alg_A).

Proposición 12.9: La intersección de subálgebras es una subálgebra.

Definición 12.10: Dada una A -álgebra B y un subconjunto S cualquiera, llamamos la subálgebra generada por S , denotada por $A[S]$, como la mínima subálgebra de B que contiene a S .

B se dice una A -álgebra de *tipo finito* si está generada (como álgebra) por un conjunto finito.

La expresión «de tipo finito» es para diferenciarlo de «finitamente generado» como módulo. Nótese que ser generado en un módulo significa serlo por combinaciones lineales, mientras que ser generado en un álgebra significa serlo por expresiones polinómicas; ésto marca una diferencia sustancial.

Ejemplo. $\mathbb{Q}[x]$ es una \mathbb{Q} -álgebra de tipo finito que no es finitamente generada como \mathbb{Q} -módulo. En efecto, basta notar que $\{1, x, x^2, \dots, x^n\}$ siempre es un conjunto linealmente independiente.

Proposición 12.11: Una A -álgebra B es de tipo finito si y sólo si existe $S \subseteq B$ finito, con una biyección $S \mapsto \{x_1, x_2, \dots, x_n\}$ a un conjunto de indeterminadas tal que la aplicación:

$$\text{ev}_S: A[x_1, \dots, x_n] \rightarrow A[S]$$

es suprayectiva. En consecuencia, toda A -álgebra de tipo finito es un cociente de algún anillo de polinomios con finitas indeterminadas.

DEMOSTRACIÓN: La parte de «en consecuencia» sigue del primer teorema de isomorfismos. \square

Ahora veremos una aplicación crucial de la teoría de extensiones de cuerpos para dar una primera demostración del teorema (*satz*) de ubicación (*stellen*) de ceros (*null*) de Hilbert, o por su nombre en alemán, el *Nullstellensatz*.

Teorema 12.12: Si L/k es una extensión de cuerpos donde L es una k -álgebra de tipo finito, entonces L es una extensión finita.

Éste primer resultado es llamado el «Nullstellensatz fuerte» en el libro de Aluffi [1, p. 405]; sin embargo, dicho nombre lo reservamos para el teorema 14.11. 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 $k[x_1, \dots, x_n]$ 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 λ_i no nulos. Sustituyendo α por una variable x arbitraria se obtienen los polinomios $p(x), q(x) \in k[x]$, donde $q(x) = (x - \beta_1) \cdots (x - \beta_n)$ es no nulo en α , así que $p(\alpha) = 0$.

Ésto prueba que L es algebraico, y como viene generado por finitos elementos, es una extensión finita. \square

Damos otra demostración en la proposición 12.23 y el corolario 12.51.

Teorema 12.13 – 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 syss $\mathfrak{a} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ 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 $\mathfrak{m} \trianglelefteq k[x_1, \dots, x_n]$ 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 del conjunto de la izquierda se da la igualdad buscada. \square

Definición 12.14: Se dice que un R -módulo M es *fiel* si para todos $\lambda_1, \lambda_2 \in R$ distintos existe un $\mathbf{m} \in M$ tal que $\lambda_1 \mathbf{m} \neq \lambda_2 \mathbf{m}$. Equivalentemente, un R -módulo M es fiel si no existe $a \in R$ tal que $aM = 0$.

Lema 12.15: Sea B una A -álgebra y $\alpha \in B$. Son equivalentes:

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

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

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

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

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

$4 \implies 1$. Sea M dicho $A[\alpha]$ -módulo fiel que está generado sobre A por $\mathbf{m}_1, \dots, \mathbf{m}_n$. Luego como $\alpha M \subseteq M$, entonces $x \mapsto \alpha x$ es un morfismo de A -módulos y por la proposición 6.41 se obtiene el polinomio mónico deseado. \square

Definición 12.16: Sea B una A -álgebra. Un elemento $\alpha \in B$ se dice *entero* sobre A . B se dice una A -álgebra *entera* si todo elemento de B es entero.

Ejemplo. Consideremos la extensión de anillos \mathbb{Q}/\mathbb{Z} y supongamos que $a/b \in \mathbb{Q}$ es entero. Luego a/b es la raíz de un polinomio de $\mathbb{Z}[x]$ mónico, por el corolario 2.81 al teorema de la raíz racional se cumple que necesariamente $b = \pm 1$ y que por ende $a/b \in \mathbb{Z}$.

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

Proposición 12.17: Sea B es una A -álgebra. Si $\alpha \in B$ es entero, entonces $A[\alpha]$ es una extensión entera.

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

Proposición 12.18: Sea A un dominio íntegro, sea $k := \text{Frac } A$ y sea L/k una extensión de anillos. Sea $\alpha \in L$ algebraico sobre k , entonces existe $c \in A$ tal que $c\alpha \neq 0$ es entero sobre A .

Corolario 12.19: Sea A un dominio íntegro, sea $k := \text{Frac } A$ y sea L/k una extensión de anillos. Sea B la clausura íntegra de L/A , entonces $L = \text{Frac } B$.

Teorema 12.20: Sean $C/B/A$ extensiones de anillos. Entonces C/A es una extensión entera syss C/B y B/A son extensiones enteras.

Proposición 12.21: Sea B una A -álgebra. Entonces B es de tipo finito syss es entera y un A -módulo finitamente generado.

DEMOSTRACIÓN: \Leftarrow . Es claro, pues ser A -módulo finitamente generado implica ser A -álgebra de tipo finito.

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

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

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

Proposición 12.22: Sean $C/B/A$ extensiones de anillos, con A noetheriano. Si C es una A -álgebra de tipo finito y se cumple alguno de los siguientes:

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

Entonces B es una A -álgebra de tipo finito.

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

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

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

He aquí la segunda prueba del lema del teorema de ceros de Hilbert:

Proposición 12.23: Si L/k es una extensión de cuerpos donde L es una k -álgebra de tipo finito, entonces L/k es una extensión finita.

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

Proposición 12.24: Sea $\sigma: B \rightarrow C$ un homomorfismo de anillos. Si B es un A -álgebra entera, entonces $\sigma[B]$ es entera sobre $\sigma[A]$. Si σ es inyectivo y B/A es extensión anillos, entonces $\sigma[B]/\sigma[A]$ también.

Proposición 12.25: Sea B/A una extensión de anillos, y sea C el conjunto de elementos enteros de B . Entonces C/A es una extensión de anillos.

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

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

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

Definición 12.26: El subanillo C construido en la proposición anterior se le dice la *clausura íntegra* de B . Si $C = A$, entonces se dice que A es *íntegramente cerrado* sobre B . En particular, decimos que un dominio íntegro A es *íntegramente cerrado* (a secas) si lo es sobre $\text{Frac}(A)$.

Proposición 12.27: Sea A un dominio íntegro y un DFU, entonces A es íntegramente cerrado.

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

Teorema 12.28: Sea B/A una extensión entera de anillos. Entonces:

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

Proposición 12.29: Sean B/A una extensión entera de dominios íntegros. Entonces A es un cuerpo syss B es un cuerpo.

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

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

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

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

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

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

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

Proposición 12.30: Sea A un dominio íntegramente cerrado con $k := \text{Frac } A$, y sea L/k una extensión finita de cuerpos. Entonces $\alpha \in L$ es entero sobre A si y sólo si su polinomio minimal tiene coeficientes en A .

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

Lema 12.31: Sea B una A -álgebra. Sean $f, g \in B[x]$ mónicos tales que $g \mid f$ y f tiene coeficientes enteros sobre A , entonces g también tiene coeficientes enteros sobre A .

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

Proposición 12.32: Sea B una A -álgebra. Si un polinomio en $B[x]$ es entero sobre $A[x]$, entonces sus coeficientes son enteros sobre A .

DEMOSTRACIÓN: Sea

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

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

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

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

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

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

Proposición 12.33: Sea A un dominio íntegramente cerrado, entonces $A[x]$ es íntegramente cerrado.

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

Corolario 12.34: Sea B/A una extensión entera de anillos, y sean $\mathfrak{q} \trianglelefteq B$ y $\mathfrak{p} := \mathfrak{q} \cap A \trianglelefteq A$. Entonces \mathfrak{q} es maximal si y sólo si \mathfrak{p} es maximal.

Corolario 12.35: Sea B/A una extensión entera de anillos, y sean $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \trianglelefteq B$ primos tales que $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$. Entonces $\mathfrak{q}_1 = \mathfrak{q}_2$.

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

Teorema 12.36: Sea B/A una extensión entera de anillos, y sea $\mathfrak{p} \trianglelefteq A$ primo. Entonces existe un ideal $\mathfrak{q} \trianglelefteq B$ primo tal que $\mathfrak{p} = \mathfrak{q} \cap A$.

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

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

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

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

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

Teorema 12.37 – Teorema del ascenso: Sea B/A una extensión entera de anillos, y sean

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n \triangleleft A,$$

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m \triangleleft B,$$

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

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

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

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

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

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

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

Proposición 12.38: Sea A un dominio íntegro. Son equivalentes:

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

Lema 12.39: Sea B/A una extensión de anillos, sea $\mathfrak{a} \triangleleft A$ y sea C la clausura íntegra de B en A . Considerando $\iota: A \rightarrow C$, entonces la clausura íntegra de \mathfrak{a} en B es $\text{Rad}(\mathfrak{a}^e)$.

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

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

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

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

Proposición 12.40: Sea B/A una extensión de dominios íntegros, A íntegramente cerrado y $\alpha \in B$ entero sobre $\mathfrak{a} \trianglelefteq A$. Si α es algebraico sobre $k := \text{Frac}(A)$ y su polinomio minimal es

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

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

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

Teorema 12.41 – Teorema del descenso: Sea B/A una extensión entera de anillos, y sean

$$\begin{aligned} A \triangleright \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \dots \supseteq \mathfrak{p}_n, \\ B \triangleright \mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \dots \supseteq \mathfrak{q}_m, \end{aligned}$$

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

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

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

DEMOSTRACIÓN: Por inducción basta probar el caso $m = 1 < 2 = n$. Hay que probar que \mathfrak{p}_2 es la contracción de un ideal primo en $B_{\mathfrak{q}_1}$, lo que por la proposición 6.38 se reduce a ver que $\mathfrak{p}_2^{ec} = B_{\mathfrak{q}_1} \mathfrak{p}_2 \cap A \subseteq \mathfrak{p}_2$.

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

en $k := \text{Frac } A$ es

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

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

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

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

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

12.2 Valores absolutos y valuaciones

Definición 12.42: Sea k un cuerpo, una función $||: k \rightarrow \mathbb{R}$ se dice una aplicación *valor absoluto* si:

VA1. $|x| > 0$ para todo $x \neq 0$ y $|0| = 0$.

VA2. $|xy| = |x| |y|$.

VA3. $|x + y| \leq |x| + |y|$.

Si además, satisface que $|x + y| \leq \max\{|x|, |y|\}$, entonces $||$ se dice un *valor absoluto no-arquimediano*.

Nótese que todo valor absoluto induce una métrica $d(x, y) := |x - y|$ sobre k , y por ende, una topología. Se dice que dos valores absolutos son *equivalentes* si inducen la misma topología sobre k .

Ejemplo. • Sea k un cuerpo arbitrario. Entonces $||: k \rightarrow \mathbb{R}$ dado por

$$|x| = \chi_{k^\times}(x) = \begin{cases} 0, & x = 0 \\ 1, & x \neq 0 \end{cases}$$

es un valor absoluto no-arquimediano, llamado el valor absoluto *trivial*. Nótese que el valor absoluto induce la topología discreta sobre el cuerpo.

- El valor absoluto estándar sobre \mathbb{R} y sobre \mathbb{C} son, efectivamente, aplicaciones «valor absoluto» e inducen las topologías usuales resp.

Nótese que para todo valor absoluto se cumple que

$$|1| = |1^2| = |(-1)^2| = |1|^2 \implies |1| = |(-1)| = 1.$$

Y además $|-x| = |x|$ y $|x^{-1}| = |x|^{-1}$ para todo $x \neq 0$.

Proposición 12.43: Sean $|\cdot|_1, |\cdot|_2$ dos valores absolutos no triviales sobre k . Entonces las siguientes afirmaciones son equivalentes:

1. $|\cdot|_1$ y $|\cdot|_2$ son valores absolutos equivalentes.
2. $|x|_1 < 1$ implica $|x|_2 < 1$ para todo $x \in k$.
3. Existe un $\lambda > 0$ real tal que $|x|_1 = |x|_2^\lambda$ para todo $x \in k$.

DEMOSTRACIÓN: $1 \implies 2$. Si $|x|_1 < 1$, entonces $\lim_n |x|_1^n = 0$, por lo que $\lim_n x = 0$. Como las topologías son la misma, la convergencia se da para ambos valores absolutos, luego $\lim_n |x|_2^n = 0$, por lo que $|x|_2 < 1$.

$2 \implies 3$. Nótese que si $|x|_1 < 1$ implica $|x|_2 < 1$, luego si $|x|_1 > 1$ elijamos x^{-1} luego $|x^{-1}|_1 < 1$ implica $|x^{-1}|_2 < 1$. Como $|\cdot|_1$ y $|\cdot|_2$ son no triviales, elijamos x_0 tal que $a := |x_0|_1 > 1$ y $b := |x_0|_2 > 1$. Sea

$$\lambda := \frac{\ln b}{\ln a} > 0,$$

y claramente se satisface que $|x_0|_1 = |x_0|_2^\lambda$. Sea $x \in k^\times$, entonces sea $\alpha > 0$ tal que $|x|_1 = |x_0|_1^\alpha$. Luego sean m, n enteros tales que $m/n > \alpha$, luego

$$|x|_1 < |x_0|_1^{m/n} \iff |x^n/x_0^m|_1 < 1 \iff |x^n/x_0^m|_2 < 1 \iff |x|_2 < |x_0|_2^{m/n}$$

como ello aplica para todo racional, entonces $|x|_2 \leq |x_0|_2^\alpha$. De manera análoga se comprueba que $|x|_2 \geq |x_0|_2^\alpha$. Finalmente se establece que $|x|_1 = |x_0|_1^\alpha = |x_0|_2^{\lambda\alpha} = |x|_2^\lambda$.

$3 \implies 1$. Trivial. □

Definición 12.44: Un dominio A se dice *de valuación* si para todo $a \in \text{Frac}(A)^\times$ se cumple que $a \in A$ o $a^{-1} \in A$.

Ejemplo. • Todo cuerpo es un anillo de valuación.

- \mathbb{Z} no es de valuación, puesto que $2/3 \in \mathbb{Q}$ satisface que $2/3 \notin \mathbb{Z}$ y $3/2 \notin \mathbb{Z}$.
- Sea $S := \mathbb{Z} \setminus (2)$, entonces considere

$$R := S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \in \mathbb{Q} : \text{mcm}(a, b) = 1, 2 \nmid b \right\},$$

luego R es de valuación.

Proposición 12.45: Sea A un anillo de valuación con $K := \text{Frac}(A)$, entonces:

1. A es un anillo local.
2. Si $A \subseteq B \subseteq K$, entonces B también es de valuación.
3. A es íntegramente cerrado.

DEMOSTRACIÓN:

1. Sea $\mathfrak{m} := A \setminus A^\times$, es decir, el conjunto de los elementos no inversibles de A . Sea $r \in A$, entonces $rx \in \mathfrak{m}$, pues de lo contrario $x = r(rx)^{-1} \in A^\times$. Sean $x, y \in \mathfrak{m}$ no nulos, sin pérdida de generalidad supongamos que $xy^{-1} \in A$, luego $x + y = (1 + xy^{-1})y \in \mathfrak{m}$. En conclusión, \mathfrak{m} es un ideal, luego debe ser un ideal maximal y el único de A .
2. Trivial.
3. Sea $x \in K$ no nulo y entero sobre A , es decir,

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

con $c_i \in A$. Si $x \in A$ entonces no hay nada que probar. Si $x^{-1} \in A$, entonces como $x = -(c_n + c_{n-1}x^{-1} + \cdots + c_0x^{-n}) \in A$. \square

Lema 12.46: Sea K un cuerpo, con $A \subseteq K$ de valuación y sea $\alpha \in K^\times$. Sea \mathfrak{m} el ideal maximal de A , entonces $\mathfrak{m}[\alpha] \neq A[\alpha]$ o $\mathfrak{m}[\alpha^{-1}] \neq A[\alpha^{-1}]$.

DEMOSTRACIÓN: Procedamos por contradicción: Si $\mathfrak{m}[\alpha] = A[\alpha]$ y $\mathfrak{m}[\alpha^{-1}] = A[\alpha^{-1}]$, entonces se cumple que $1 \in \mathfrak{m}[\alpha] \cap \mathfrak{m}[\alpha^{-1}]$, vale decir

$$\begin{aligned} u_0 + u_1\alpha + \cdots + u_n\alpha^n &= 1 \\ v_0 + v_1\alpha^{-1} + \cdots + v_m\alpha^{-m} &= 1 \end{aligned} \tag{12.1}$$

para algunos $u_i, v_i \in \mathfrak{m}$. Podemos asumir que n, m son los mínimos exponentes para los que se cumple lo anterior y que $n \geq m$ (de lo contrario, sustituimos « α » por « α^{-1} ») luego podemos reescribir la segunda fórmula a que

$$(1 - v_0)\alpha^m = v_1\alpha^{m-1} + \cdots + v_{m-1}\alpha + v_m,$$

como \mathfrak{m} es el único anillo maximal de A , entonces $1 - v_0 \in A^\times$, luego dividiendo por dicho término y multiplicando por α^{n-m} se obtiene que:

$$\alpha^n = w_0\alpha^{n-m} + w_1\alpha^{n-m+1} + \cdots + w_m\alpha^{n-1},$$

sustituyendo en (12.1) se obtiene una expresión con grado menor, lo que contradice la minimalidad de n . \square

Lema (AE) 12.47: Sea K un cuerpo y L un cuerpo algebraicamente cerrado. Entonces K posee un subanillo propio A con un homomorfismo $f: A \rightarrow L$ tal que A es de valuación y es un subanillo maximal que satisface éstas propiedades.

DEMOSTRACIÓN: Emplearemos el lema de Zorn: sea \mathcal{F} la familia de los pares (B, g) donde $g: B \rightarrow L$ es un homomorfismo. Se denota que

$$(B_1, g_1) \preceq (B_2, g_2) \iff B_1 \subseteq B_2 \wedge g_2 \upharpoonright B_1 = g_1.$$

Sea $\{(B_i, g_i)\}_{i \in I}$ una \preceq -cadena, luego nótese que

$$B := \bigcup_{i \in I} B_i, \quad g := \bigcup_{i \in I} g_i.$$

la cual está bien definida pues los g_i 's son compatibles por ser cadena, y además claramente es un homomorfismo desde B a L , como se quería comprobar.

Finalmente, por lema de Zorn, \mathcal{F} posee un elemento \preceq -maximal (A, f) . Nótese que $f[A]$ es un subanillo de L , luego es un dominio íntegro; definiendo $\mathfrak{m} := \ker f$, por el primer teorema de isomorfismos se cumple que $f[A] \cong A/\mathfrak{m}$, luego \mathfrak{m} es un ideal primo. Por la propiedad universal de la localización se satisface que $\bar{f}: A_{\mathfrak{m}} \rightarrow L$ con $A_{\mathfrak{m}} \subseteq K$, pero por maximalidad de A se concluye que $A = A_{\mathfrak{m}}$, luego A es local y \mathfrak{m} es su ideal maximal. \square

Teorema (AE) 12.48: Sea K un cuerpo, entonces existe $A \subset K$ anillo de valuación con $\text{Frac}(A) = K$.

DEMOSTRACIÓN: Por el lema anterior, sea A el anillo construido y sea \mathfrak{m} su anillo maximal. Hay que probar que $\text{Frac}(A) = K$: Sea $\alpha \in K^\times$, entonces por el lema previo al anterior y sin pérdida de generalidad se satisface que

$$\mathfrak{m}[\alpha] \subset A[\alpha] =: A'.$$

Por teorema de Krull se cumple que $\mathfrak{m}[\alpha] \subseteq \mathfrak{m}' \triangleleft A'$. Definamos $k := A/\mathfrak{m}$ y $k' := A'/\mathfrak{m}'$ los cuales son cuerpos; nótese que $k' = k[\bar{\alpha}]$, donde $\bar{\alpha}$ es la proyección de α en k (por ser un cociente); más aún, como los anillos de valuación son íntegramente cerrados, entonces k'/k es una extensión finita.

Por el primer teorema de isomorfismos, y recordando que $\mathfrak{m} = \ker f$ se tiene que el siguiente diagrama conmuta:

$$\begin{array}{ccc} A & \xrightarrow{f} & L \\ & \searrow & \nearrow f^* \\ & k & \end{array}$$

así mismo, como k'/k es finita y L es normal, entonces:

$$\begin{array}{ccc} k' & \xrightarrow{\bar{f}} & L \\ \uparrow & & \uparrow \text{Id} \\ k & \xrightarrow{f^*} & L \end{array}$$

Pre-componiendo \bar{f} con la proyección obtenemos $\pi \circ \bar{f}: A' \rightarrow L$ la cual extiende a $f: A \rightarrow L$, lo que, por maximalidad, implica que $A = A'$ y por ende $\alpha \in A$ como se quería probar. \square

Corolario (AE) 12.49: Sea K un cuerpo, y $A \subseteq K$ un subanillo. Entonces, la clausura íntegra C de A en K es la intersección de todos los anillos de valuación contenidos en K que contienen a A .

DEMOSTRACIÓN: Sea $A \subseteq V \subseteq K$ con V de valuación, luego como V es íntegramente cerrado, entonces $C \subseteq V$.

Sea $\alpha \notin C$, luego como α no es entero sobre A , se cumple que $\alpha \notin A[\alpha^{-1}] =: A'$; es decir, α^{-1} no es inversible en A' , por lo que, por el teorema de Krull está contenido en un ideal maximal $\mathfrak{m} \triangleleft A'$. Definamos $k := A'/\mathfrak{m}$, luego podemos definir L como la clausura algebraica de k y luego tenemos el siguiente homomorfismo de anillos:

$$\begin{array}{ccccc}
 & & \varphi & & \\
 & \curvearrowright & & \curvearrowleft & \\
 A & \hookrightarrow & A' & \twoheadrightarrow & k & \hookrightarrow & L
 \end{array}$$

Siguiendo el proceso del lema y teorema anteriores podemos extender $A \subseteq V$ y $\varphi^*: V \rightarrow L$ tal que V es de valuación. Como $\varphi(\alpha^{-1}) = 0$, entonces $\alpha \notin V$. \square

Proposición (AE) 12.50: Sea B/A una extensión de dominios íntegros con B una A -álgebra de tipo finito. Sea $v \in B_{\neq 0}$ existe un $u \in A_{\neq 0}$ tal que todo homomorfismo de anillos $f: A \rightarrow L$ con L un cuerpo algebraicamente cerrado y con $f(u) \neq 0$ se puede extender a $g: B \rightarrow L$ tal que $g(v) \neq 0$.

DEMOSTRACIÓN: Por inducción sobre la cantidad minimal de generadores de B como A -álgebra podemos reducirlo al caso $B = A[\alpha]$.

- (a) α es trascendente: Sea $v = c_n \alpha^n + \cdots + c_1 \alpha + c_0$ con $c_i \in A$; definamos $u := c_n$. Como L es algebraicamente cerrado, entonces es infinito y así existe β tal que

$$f(c_n)\beta^n + \cdots + f(c_1)\beta + f(c_0) \neq 0.$$

Como $B \cong A[x]$ (el anillo de polinomios), entonces considere el siguiente diagrama:

$$\begin{array}{ccccc}
 & & g & & \\
 & \curvearrowright & & \curvearrowleft & \\
 B \cong A[x] & \xrightarrow{f^*} & L[x] & \xrightarrow{\text{ev}_\beta} & L \\
 \uparrow & & \uparrow & & \\
 A & \xrightarrow{f} & L & &
 \end{array}$$

Luego g satisface lo requerido.

- (b) α es algebraico: Luego tomando $k := \text{Frac}(A)$, entonces como α es algebraico, se cumple que $\alpha, v^{-1} \in k(\alpha)$ son algebraicos. Por la proposición 12.18 se satisface que $c\alpha, c'v^{-1}$ son enteros sobre A para algunos $c, c' \in A$, luego:

$$\begin{aligned}
 a_n \alpha^n + \cdots + a_1 \alpha + c_0 &= 0 \\
 b_m v^{-m} + \cdots + b_1 v^{-1} + b_0 &= 0
 \end{aligned}$$

definamos $u := a_n b_m$. Si $f: A \rightarrow L$ es un homomorfismo de anillos con $f(u) \neq 0$, entonces podemos extender la función a $f_1: A[u^{-1}] \rightarrow L$. Más aún, por el teorema anterior se puede extender a $f_2: V \rightarrow L$, donde V es de valuación. Como $a_n^{-1} = a_n u^{-1} \in A[u^{-1}]$, entonces α es entero en $A[u^{-1}]$, análogamente v^{-1} también. Como V es íntegramente cerrado, entonces $\alpha, v^{-1} \in V$. Además como B/A es entero, entonces $v \in V$, luego $v \in V^\times$ y por tanto $f_2(v) \neq 0$. \square

Aquí damos la tercera demostración del lema del teorema (débil) de ceros de Hilbert:

Corolario (AE) 12.51: Sea L/k una extensión de cuerpos con L una k -álgebra de tipo finito. Entonces L/k es una extensión finita.

12.3 Dominios de valuación discreta y de Dedekind

Proposición 12.52: Sea A un dominio íntegro noetheriano de $k\text{-dim } A = 1$. Entonces todo ideal no nulo puede expresarse de manera única como producto de ideales primarios de radicales distintos.

DEMOSTRACIÓN: Sea $\mathfrak{a} \triangleleft A$ un ideal impropio, por el teorema 6.75 se cumple que $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$, donde \mathfrak{q}_i es \mathfrak{p}_i -primario. Como $k\text{-dim } A = 1$ y A es un dominio íntegro, entonces todo ideal primo es maximal, luego los \mathfrak{p}_i 's son ideales maximales distintos, y por ende, son coprimos. Luego, como los radicales de los \mathfrak{q}_i 's son coprimos, entonces ellos lo son y por el teorema chino del resto se cumple que

$$\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i = \prod_{i=1}^n \mathfrak{q}_i.$$

Para ver la unicidad, supongamos que $\mathfrak{a} = \prod_{i=1}^m \mathfrak{r}_i$, de modo que por el mismo argumento, $\mathfrak{a} = \bigcap_{i=1}^m \mathfrak{r}_i$, donde los \mathfrak{r}_i 's conforman una familia aislada, luego se concluye por unicidad de la representación (teorema 6.63). \square

Definición 12.53: Sea K un cuerpo. Una *valuación discreta* es una aplicación $v: K^\times \rightarrow \mathbb{Z}$ tal que:

VD1. $v(xy) = v(x) + v(y)$, i.e., v es un homomorfismo de grupos.

VD2. $v(x + y) \geq \min\{v(x), v(y)\}$.

Y a veces se añade que:

$$3. v(0) = \infty.$$

Con los convenios usuales para ∞ .

Dada una valuación discreta v sobre K se le llama su *anillo de valuación* a

$$A := \{x \in K : v(x) \geq 0\}$$

(queda al lector ver que efectivamente es un anillo de valuación).

Un dominio íntegro D se dice un *dominio de valuación discreta* si existe una valuación discreta v sobre $\text{Frac}(D)$ tal que D sea el anillo de valuación de v .

En una valuación discreta v se cumple que $v(1) = 0$, y en su anillo de valuación, $v(x) = 0$ si y sólo si x es inversible. Con ésto se puede concluir lo siguiente:

Corolario 12.54: Sea A un dominio de valuación discreta v . Entonces:

1. Todos los ideales impropios de A son de la forma:

$$\mathfrak{a}_n = \{x \in A : v(x) \geq n\}.$$

2. A es noetheriano.
3. A es local y su único ideal maximal es \mathfrak{a}_1 .

DEMOSTRACIÓN: Es claro que de la primera se sigue el resto. Supongamos que $v(x) = v(y)$, entonces supongamos que $xy^{-1} \in A$ (por ser anillo de valuación), luego $v(xy^{-1}) = 0$, por lo que es inversible y luego $(x) = (y)$. Si $\mathfrak{b} \triangleleft A$ es un ideal impropio, entonces $v[\mathfrak{b}] \subseteq \mathbb{N}$, por lo que posee un mínimo n y un $x \in \mathfrak{b}$ con $v(x) = n$, luego es fácil concluir que $\mathfrak{b} = (x) = \mathfrak{a}_n$. \square

Proposición 12.55: Sea A un dominio íntegro, local, noetheriano de dimensión 1, cuyo ideal maximal es \mathfrak{m} y con $k := A/\mathfrak{m}$. Las siguientes son equivalentes:

1. A es un dominio de valuación discreta.
2. A es íntegramente cerrado.
3. \mathfrak{m} es un ideal principal.
4. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

5. Todo ideal impropio es una potencia de \mathfrak{m} .
6. Existe un $x \in A$ tal que todo ideal impropio es de la forma (x^n) .

DEMOSTRACIÓN: 1 \implies 2. Puesto que

dominio de valuación discreta
 \Downarrow
 anillo de valuación
 \Downarrow
 íntegramente cerrado

2 \implies 3. Sea $a \in \mathfrak{m}$ no nulo, entonces (a) es un ideal impropio. Como A es decomponible y el único ideal primo de A es \mathfrak{m} , entonces (por ser dominio íntegro local de dimensión 1) (a) es \mathfrak{m} -primario y existe un n tal que $\mathfrak{m}^{n+1} \subseteq (a)$ y $\mathfrak{m}^n \not\subseteq (a)$. Sea $b \in \mathfrak{m}^n \setminus (a)$, y sea $x = a/b \in K := \text{Frac}(A)$, luego nótese que $x^{-1} \notin A$ (de lo contrario $b = ax^{-1} \in (a)$), por lo que x^{-1} no es entero sobre A y luego $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$, puesto que de lo contrario \mathfrak{m} sería un $A[x^{-1}]$ -módulo fiel finitamente generado y x^{-1} sería entero. Finalmente $x^{-1}\mathfrak{m} \subseteq A$, pero entonces $\mathfrak{m} \subseteq x^{-1}\mathfrak{m}$, por lo que $x^{-1}\mathfrak{m} = A$ y $\mathfrak{m} = Ax = (x)$.

¿Por qué?

3 \implies 4. Nótese que por el lema de Nakayama, $\mathfrak{m}/\mathfrak{m}^2$ está generado por a lo más un elemento, y las potencias de \mathfrak{m} son distintas, de lo contrario sería nilpotente y entonces sería artiniiano y de dimensión cero.

4 \implies 5. Si $\mathfrak{a} \triangleleft A$ es impropio, entonces existe un n tal que $\mathfrak{m}^n \subseteq \mathfrak{a}$, luego A/\mathfrak{m}^n es artiniiano, por lo que la extensión de \mathfrak{a} es potencia del maximal, luego \mathfrak{a} mismo también debe de serlo.

5 \implies 6. Ya vimos que las potencias del maximal son distintas. Sea $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, luego $(x) = \mathfrak{m}^r$ para algún r , y dicho r tiene necesariamente que ser 1, luego $\mathfrak{m}^n = (x^n)$.

6 \implies 1. Sea $\mathfrak{m} = (x)$, entonces para todo $a \in A$ ya vimos que $(a) = (x^n)$ para un único n , por lo que definamos $v: A_{\neq 0} \rightarrow \mathbb{Z}$ como $v(a) = n$, y extendamos $v: K^\times \rightarrow \mathbb{Z}$ por $v(a/b) = v(a) - v(b)$. Queda al lector comprobar que efectivamente se trata de una valuación discreta. \square

Lema 12.56: Sea A un dominio íntegro noetheriano de dimensión 1. Entonces son equivalentes:

1. A es íntegramente cerrado.
2. Todo ideal \mathfrak{p} -primario es de la forma \mathfrak{p}^n .
3. Toda localización $A_{\mathfrak{p}}$, con $\mathfrak{p} \neq (0)$, es un dominio de valuación discreta.

DEMOSTRACIÓN: $1 \iff 3$. Por el teorema anterior y la proposición 12.45.

$2 \iff 3$. Aplicar el teorema anterior, y el hecho de que hay una correspondencia entre ideales primos tras localizar, y \mathfrak{p} -primarios. \square

Definición 12.57: Se le llama un *dominio de Dedekind* a un dominio que satisfaga cualquiera de las condiciones del lema anterior.

Ejemplo. \mathbb{Z} es un dominio de Dedekind y más generalmente todo DIP es de Dedekind. Nótese que los cuerpos *no* son dominios de Dedekind, puesto que tienen dimensión 0.

Corolario 12.58: En un dominio de valuación discreta, todo ideal puede escribirse de manera única como producto de ideales primos.

Definición 12.59: Un *cuerpo de números* es una extensión finita K/\mathbb{Q} , y su *anillo de enteros* es la clausura íntegra de \mathbb{Z} en K .

Teorema 12.60: El anillo de enteros A de un cuerpo de números algebraicos K es un dominio de Dedekind.

DEMOSTRACIÓN: Como $A \subseteq K$ que es un cuerpo, entonces A es un dominio íntegro. Sea $\{\alpha_1, \dots, \alpha_n\}$ una \mathbb{Q} -base de K , entonces $A \subseteq \sum_{i=1}^n \mathbb{Z}\alpha_i$, de modo que A es un \mathbb{Z} -módulo finitamente generado, por tanto es noetheriano. Finalmente, sea $\mathfrak{p} \triangleleft A$ primo no nulo, luego $\mathfrak{p}^c \subseteq \mathbb{Z}$ es primo y por el corolario 12.35 se satisface que es no vacío en \mathbb{Z} , luego su contracción es maximal, así que por el corolario 12.34 se cumple que \mathfrak{p} es maximal. \square

Definición 12.61: Sea A un dominio íntegro y $K := \text{Frac } A$. Se dice que un A -submódulo M de K es un *ideal fraccionario* si existe algún $x \in A_{\neq 0}$ tal que $xM \subseteq A$. A los ideales de A (en sentido usual) les diremos *ideales enteros*. Si $M = yA$ para algún $y \in K$, entonces M se dice un *ideal principal*. Para un A -submódulo M se define:

$$(A : M) := \{x \in A : xM \subseteq A\}.$$

(Nótese que M es fraccionario si $(A : M) = (0)$.)

Un A -submódulo M se dice *invertible* si existe otro A -submódulo N tal que $MN = A$.

Nótese que si M es inversible y N es una inversa, entonces:

$$N \subseteq (A : M) = (A : M)MN \subseteq AN = N,$$

de modo que $N = (A : M)$. Además si M es inversible, entonces es claro que es finitamente generado (¿por qué?).

Proposición 12.62: Sea A un dominio íntegro, $K := \text{Frac } A$ y $M \subseteq K$ un A -submódulo. Entonces son equivalentes:

1. M es inversible.
2. M es finitamente generado y para todo $\mathfrak{p} \triangleleft A$ primo, $M_{\mathfrak{p}}$ es inversible.
3. M es finitamente generado y para todo $\mathfrak{m} \triangleleft A$ maximal, $M_{\mathfrak{m}}$ es inversible.

DEMOSTRACIÓN: 1 \implies 2. Basta notar que $A_{\mathfrak{p}} = (M \cdot (A : M))_{\mathfrak{p}} = M_{\mathfrak{p}} \cdot (A : M)_{\mathfrak{p}}$.

2 \implies 3. Trivial.

3 \implies 1. Definamos $\mathfrak{a} := M \cdot (A : M)$ el cual es un ideal entero sobre A . Como $M_{\mathfrak{m}}$ es inversible, entonces

$$\mathfrak{a}_{\mathfrak{m}} = (M \cdot (A : M))_{\mathfrak{m}} = M_{\mathfrak{m}} \cdot (A : M)_{\mathfrak{m}} = M_{\mathfrak{m}} \cdot (A_{\mathfrak{m}} : M_{\mathfrak{m}}) = A_{\mathfrak{m}},$$

por lo que $\mathfrak{a} \not\subseteq \mathfrak{m}$ y ésto aplica para todo ideal maximal, por lo que $\mathfrak{a} = A$. \square

Proposición 12.63: Sea A un dominio íntegro local. Entonces A es un dominio de valuación discreta syss todo ideal fraccionario no nulo es inversible.

DEMOSTRACIÓN: \implies . Sea $\mathfrak{m} \triangleleft A$ maximal, luego $\mathfrak{m} = (x)$. Sea $M \neq (0)$ un ideal fraccionario, como $(A : M)$ es un ideal entero, entonces $(A : M) = (y)$ y $M \cdot (A : M) \subseteq A$ el cual también es un ideal entero, entonces sea $(x^r) = M \cdot (A : M)$. También sea $v(y) = s$, entonces finalmente $M = (x^{r-s})$.

\Leftarrow . Si todo ideal fraccionario fuese inversible, entonces sería finitamente generado, luego A es noetheriano. Hay que probar que todo ideal entero es potencia de \mathfrak{m} maximal. De lo contrario, empleando el lema de Zorn, existiría \mathfrak{a} maximal en la familia de los que no son una potencia de \mathfrak{m} . Luego $\mathfrak{a} \subset \mathfrak{m}$ y

$$\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{m} = A,$$

por lo que $\mathfrak{m}^{-1}\mathfrak{a}$ es un ideal impropio entero y $\mathfrak{m}^{-1}\mathfrak{a} \supset \mathfrak{a}$. Si $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a}$, entonces $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$ y por el lema de Nakayama $\mathfrak{a} = (0)$. Si no, $\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{a}$ y entonces $\mathfrak{m}^{-1}\mathfrak{a}$ es una potencia de \mathfrak{m} lo que es absurdo. \square

Teorema 12.64: Sea A un dominio íntegro. Entonces A es de Dedekind syss todo ideal fraccionario no nulo es inversible.

DEMOSTRACIÓN: \implies . Sea M un ideal fraccionario no nulo y sea $\mathfrak{m} \triangleleft A$ maximal. Luego $A_{\mathfrak{m}}$ es un dominio de valuación discreta y $M_{\mathfrak{m}}$ es inversible. Finalmente, como A es noetheriano, se concluye que M es inversible.

\impliedby . Si todo ideal entero es inversible, entonces es finitamente generado, por lo que A es noetheriano. Sea $A_{\mathfrak{p}}$ y sea $(0) \neq \mathfrak{b} \triangleleft A_{\mathfrak{p}}$. Luego $\mathfrak{a} := \mathfrak{b}^c = \mathfrak{b} \cap A$ es inversible, luego $\mathfrak{b} = \mathfrak{a}_{\mathfrak{p}}$ también y por la proposición anterior, $A_{\mathfrak{p}}$ es un dominio de valuación discreta, y por tanto, A es de Dedekind. \square

Corolario 12.65: Sea A un dominio de Dedekind. Entonces los ideales fraccionarios no nulos de A forman un grupo.

13

Compleciones y teoría de la dimensión

13.1 Series de potencias

Definición 13.1 (Notación de multi-índice): Un *multi-índice* α es una tupla de números naturales $\alpha = (\alpha_1, \dots, \alpha_n)$. Si $\mathbf{x} = (x_1, \dots, x_n)$ es una tupla de indeterminadas, entonces se admiten las siguientes notaciones:

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

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

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

Ésta notación será útil para la siguiente definición:

Definición 13.2: Sea A un dominio. Una *serie formal de potencias* es un objeto de la forma

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots = \sum_{n \geq 0} a_n x^n,$$

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

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

$$\begin{aligned} f(\mathbf{x}) &:= \sum_{\alpha} c_{\alpha} \mathbf{x}^{\alpha}, & g(\mathbf{x}) &:= \sum_{\alpha} d_{\alpha} \mathbf{x}^{\alpha} \\ f(\mathbf{x}) + g(\mathbf{x}) &:= \sum_{\alpha} (c_{\alpha} + d_{\alpha}) \mathbf{x}^{\alpha}, \\ f(\mathbf{x}) \cdot g(\mathbf{x}) &:= \sum_{\alpha} \left(\sum_{\beta+\gamma=\alpha} c_{\beta} d_{\gamma} \right) \mathbf{x}^{\alpha}, \end{aligned}$$

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

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

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

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

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

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

Ahora, nótese que

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

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

Una primera pista de como encontrar inversibles es lo siguiente:

Proposición 13.3: Sea A un dominio.

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

Esto conlleva a la siguiente generalización:

Proposición 13.4: $f(x) \in A[[x]]$ es inversible syss $f(x) = a + xg(x)$ con $g(x) \in A[[x]]$ y $a \in A^\times$. En particular, si A es un cuerpo, entonces los inversibles son exactamente las series de orden cero.

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

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

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

Proposición 13.5: Sea S un conjunto de indeterminadas, A un dominio y k un cuerpo. Entonces:

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

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

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

13.2 Compleciones

Se recuerda que un *grupo topológico* es tal que la operación de grupo y la inversa son continuas. En particular, si G es un grupo abeliano (con notación aditiva), se dice que es un grupo topológico si las aplicaciones $(g, h) \mapsto g + h$ y $g \mapsto -g$ son continuas en dicho espacio topológico. Una de las ventajas de una definición aparentemente tan sencilla es que toda la topología está completamente determinada por el comportamiento cerca del 0.

Lema 13.6: Sea

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

entonces:

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

DEMOSTRACIÓN:

Completar demostración.

1. Sea $x, y \in H$, entonces x, y están en todos los entornos del 0.
2. Nótese que $x \in H$ syss todo entorno del 0 corta a x , es decir, syss x es de acumulación de $\{0\}$.

□

Definición 13.7: Si G es un grupo topológico 1AN,¹ entonces una sucesión $(x_n)_{n \in \mathbb{N}} \subseteq G$ se dice *de Cauchy* si para todo entorno básico U del 0 existe un $n_0 \in \mathbb{N}$ tal que para todo $n, m \geq n_0$ se satisface que $x_n - x_m \in U$.

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

¹Abreviación de «primer axioma de numerabilidad» (cf. [42, Def. 2.30, p. 43]).

Proposición 13.8: Sea G un grupo topológico 1AN, entonces la relación de «ser equivalentes» en el conjunto de sucesiones de Cauchy de G es una relación de equivalencia. El conjunto cociente dado por dicha relación se denota por \hat{G} . Entonces, \hat{G} es un grupo en un sentido canónico, y la aplicación

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

es un homomorfismo de grupos. Más aún, G es de Hausdorff si y sólo si φ es inyectiva.

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

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

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

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

$$G/G_0 \xleftarrow{\theta_1} G/G_1 \xleftarrow{\theta_2} G/G_2 \xleftarrow{\quad} \dots$$

Donde $\theta_i: G/G_i \rightarrow G/G_{i-1}$ es la típica proyección. Intuitivamente los G/G_n 's se van haciendo cada vez más grandes y en el límite debería ser \hat{G} , pero eso hay que demostrarlo.

Definición 13.9: Se dice que $(A_n)_{n \in \mathbb{N}}$ es un *sistema inverso* si corresponde a un diagrama de la forma:

$$A_0 \xleftarrow{\alpha_1} A_1 \xleftarrow{\alpha_2} A_2 \xleftarrow{\quad} \dots$$

tal que posee un límite inverso.

Definición 13.10: Se dice que una cadena $(G_n)_{n \in \mathbb{N}}$ descendiente de subgrupos de un grupo topológico G induce su topología si para todo entorno U del 0 se satisface que existe $n \in \mathbb{N}$ tal que $G_n \subseteq U$.

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

Proposición 13.11: Sea G un grupo topológico 1AN. Dada una cadena descendiente $(G_n)_{n \in \mathbb{N}}$ de subgrupos de G tal que para todo entorno U del 0 exista un n con $G_n \subseteq U$, entonces $\varprojlim_{n \in \mathbb{N}} G/G_n \cong \hat{G}$ (en \mathbf{Ab}).

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

Finalmente, supongamos que existe otro grupo abeliano L con homomorfismos $\psi_n \in \text{Hom}_{\mathbf{Ab}}(L, G/G_n)$ tales que $\psi_{n+1} \circ \theta_{n+1} = \psi_n$. Luego a cada $g \in L$ podemos asignarle una sucesión de Cauchy eligiendo elementos de la clase de equivalencia de $\psi_n(g) \in G/G_n$ en la n -ésima coordenada. Nótese que ésta sucesión es efectivamente de Cauchy puesto que se estabiliza trivialmente para todo G_n , y naturalmente, queda al lector ver que ésta aplicación está bien definida y es homomorfismo. \square

Proposición 13.12: Sean $(A_n)_n, (B_n)_n, (C_n)_n$ sistemas inversos de \mathbf{Ab} , dotados de flechas:

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

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

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

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

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

es exacta.

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

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

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

$$\begin{aligned}
 d^A: A &\longrightarrow A \\
 (a_n)_n &\longmapsto (a_n - \alpha_{n+1}(a_{n+1}))_n
 \end{aligned}$$

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

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

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

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

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

Corolario 13.13: Dada una sucesión exacta:

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

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

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

Corolario 13.14: $\hat{G}/\hat{G}_n \cong G/G_n$ y de hecho $\hat{\hat{G}} = G$.

Definición 13.15: Un grupo topológico G se dice *completo* si $G \cong \hat{G}$.

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

Definición 13.16: Sea M un A -módulo. Una cadena descendente de submódulos

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

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

Lema 13.17: Sean $(M_n)_{n \in \mathbb{N}}$ y $(M'_n)_{n \in \mathbb{N}}$ dos \mathfrak{a} -filtraciones estables de M . Entonces poseen diferencia acotada, es decir, existe n_0 tal que $M_{n+n_0} \subseteq M'_n$ y $M'_{n+n_0} \subseteq M_n$. En consecuencia $\varprojlim_n M/M_n \cong \varprojlim_n M/M'_n$ (en **Top**).

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

Definición 13.18: La topología sobre \hat{M} tal que $\hat{M} \cong \varprojlim_n M/\mathfrak{a}^n M$ se dice la *topología \mathfrak{a} -ádica*.

13.3 Anillos y módulos graduados

Definición 13.19: Se dice que un anillo A es *graduado* si existe una familia $(A_d)_{d \in \mathbb{N}}$, donde:

AG1. Cada A_i es un subgrupo abeliano bajo la suma.

AG2. $A = \bigoplus_{d \in \mathbb{N}} A_d$.

AG3. Para cada $d, e \geq 0$ se satisface que $A_d \cdot A_e \subseteq A_{d+e}$.

En consecuencia de AG3., se satisface que cada A_d es un A_0 -módulo y A también. Dicha descomposición se dice una *graduación*, y cada $f \in A_d$ se dice un elemento *homogéneo de grado d* . Un ideal $\mathfrak{a} \trianglelefteq A$ se dice *homogéneo* si $\mathfrak{a} = \bigoplus_{d \in \mathbb{N}} (\mathfrak{a} \cap A_d)$. Un ejemplo de ideal homogéneo impropio es $A^+ := \bigoplus_{d > 0} A_d$ llamado el *ideal irrelevante*.

Consecuencia de AG3. es que el producto de elementos homogéneos es homogéneo. Nótese que por AG2., todo elemento $x \neq 0$ de A se puede escribir de manera única como suma de homogéneos no nulos de distinto grado, a dichos factores les llamaremos *componentes homogéneas* de x . Un ideal es entonces homogéneo cuando siempre que contenga a un elemento, entonces posee sus componentes homogéneas.

El principal ejemplo de un anillo graduado es el siguiente:

Ejemplo. Sea A un dominio, entonces el anillo de polinomios $P := A[x_1, \dots, x_n]$ es un anillo graduado, donde los elementos homogéneos de grado d son los polinomios que se escriben como suma de monomios de grado d (incluyendo al cero).

Proposición 13.20: Un ideal $\mathfrak{a} \trianglelefteq A$ es homogéneo si y sólo si posee un generador mediante elementos homogéneos.

DEMOSTRACIÓN: \Leftarrow . Sea T tal que $\mathfrak{a} = (T)$ y tal que los elementos de T son homogéneos. Luego, sea $f \in \mathfrak{a}$, por definición

$$f = g_1 f_1 + \cdots + g_n f_n$$

donde $f_i \in T$ y $g_i \in A$. Como A es graduado, y los g_i 's son finitos, podemos encontrar suficientes h_j 's homogéneos tales que

$$g_i = \lambda_{1i} h_1 + \cdots + \lambda_{mi} h_m,$$

donde $\lambda_{ji} \in A_0$. Por lo tanto,

$$f = \lambda_{11} h_1 f_1 + \lambda_{21} h_2 f_1 + \cdots + \lambda_{mn} h_m f_n.$$

donde cada $h_j f_i$ es homogéneo. Es decir, $f \in \bigoplus_{d \in \mathbb{N}} (\mathfrak{a} \cap A_d)$. La otra inclusión es trivial.

\Rightarrow . Basta notar que por definición $\mathfrak{a} = (\bigcup_{d \in \mathbb{N}} (\mathfrak{a} \cap A_d))$. □

Proposición 13.21: Sean $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$ homogéneos. Entonces:

1. $A/\mathfrak{a} = \bigoplus_{d \in \mathbb{N}} A_d/\mathfrak{a}$. 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. $\mathfrak{a} + \mathfrak{b}, \mathfrak{a} \cdot \mathfrak{b}, \mathfrak{a} \cap \mathfrak{b}$ 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 $\mathfrak{p} \trianglelefteq R$ primo, entonces existe $\mathfrak{a} \subseteq \mathfrak{p}_h \subseteq \mathfrak{p}$, donde \mathfrak{p}_h es primo y homogéneo. Para ello definamos

$$\mathfrak{p}_h := (\{f \in \mathfrak{p} : f \text{ homogéneo}\}),$$

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 6.26), queda al lector proponerla.

Proposición 13.22: Sea A un dominio graduado. Entonces son equivalentes:

1. A es noetheriano.
2. A_0 es noetheriano y A es una A_0 -álgebra de tipo finito.

DEMOSTRACIÓN: 1 \implies 2. Primero, se tiene que $A_0 \cong A/A^+$ es noetheriano.

Como $A^+ \triangleleft A$, entonces $A^+ = (\alpha_1, \dots, \alpha_s)$ con α_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 λ_i tal que sea homogéneo de grado $n - k_i < n$. Por hipótesis inductiva $\lambda_i \in A'$, luego $y \in A'$ como se quería ver.

2 \implies 1. Ver teorema de bases de Hilbert. \square

Definición 13.23: Dado un anillo graduado A como ántes, se dice que M es un A -módulo graduado si existe una familia $(M_n)_{n \in \mathbb{N}}$ de subgrupos de M tales que:

$$\text{MG1. } M = \bigoplus_{n \in \mathbb{N}} M_n.$$

$$\text{MG2. } A_n \cdot M_m \subseteq M_{n+m} \text{ para todo } n, m \in \mathbb{N}.$$

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 $\varphi[M_n] \subseteq N_n$.

Definición 13.24: Sea \mathfrak{a} un ideal de A , entonces definamos $A^* := \bigoplus_{n \in \mathbb{N}} \mathfrak{a}^n$. Sea $(M_n)_n$ una \mathfrak{a} -filtración de M , entonces se denota $M^* := \bigoplus_{n \in \mathbb{N}} M_n$.

Nótese que M^* es un A^* -módulo graduado. Además, si A es noetheriano, entonces $\mathfrak{a} = (\alpha_1, \dots, \alpha_s)$ y por tanto $A^* = A[\alpha_1, \dots, \alpha_s]$, luego por bases de Hilbert es noetheriano.

Lema 13.25: Sea A un dominio noetheriano, \mathfrak{a} un ideal de A , M un A -módulo finitamente generado y $(M_n)_{n \in \mathbb{N}}$ una \mathfrak{a} -filtración de M . Son equivalentes:

1. M^* es un A^* -módulo finitamente generado.
2. La filtración $(M_n)_n$ es \mathfrak{a} -estable.

DEMOSTRACIÓN: Sea $Q_n := \bigoplus_{i=0}^n M_i$ y sea

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

el cual es un A^* -módulo graduado finitamente generado. Como $M^* = \bigcup_{n \in \mathbb{N}} Q_n = \bigcup_{n \in \mathbb{N}} M_n^*$, entonces se satisface que M^* es noetheriano syss la cadena M_n^* se estabiliza, es decir, syss $M_n^* = M_{n+1}^* = \dots = M^*$ desde algún n en adelante. \square

Proposición 13.26 (lema de Artin-Rees): Sea A un dominio noetheriano, \mathfrak{a} un ideal de A , M un A -módulo finitamente generado y $(M_n)_{n \in \mathbb{N}}$ una \mathfrak{a} -filtración estable de M . Si M' es submódulo de M , entonces $(M' \cap M_n)_n$ es una \mathfrak{a} -filtración estable de M' .

DEMOSTRACIÓN: Basta notar que:

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

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

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

Corolario 13.27: Sea A un dominio noetheriano, \mathfrak{a} un ideal de A , M un A -módulo finitamente generado y M' un submódulo de M . Existe un entero r tal que para todo $n \geq r$ se satisface que

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

Algunos textos le llaman a éste corolario el lema de Artin-Rees.

Otra consecuencia es la siguiente:

Teorema 13.28: Sea A un dominio noetheriano, \mathfrak{a} un ideal de A , M un A -módulo finitamente generado y M' un submódulo de M . Entonces las filtraciones $(\mathfrak{a}^n M')_n$ y $((\mathfrak{a}^n M) \cap M')_n$ tienen diferencia acotada. En particular, la \mathfrak{a} -topología sobre M' es la topología subespacio de la \mathfrak{a} -topología sobre M .

Proposición 13.29: Sean A un dominio noetheriano y M_1, M_2, M_3 un trío de A -módulos finitamente generados. Dada la siguiente sucesión exacta

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

entonces se induce la siguiente sucesión exacta

$$0 \longrightarrow \hat{M}_1 \longrightarrow \hat{M}_2 \longrightarrow \hat{M}_3 \longrightarrow 0$$

Proposición 13.30: Sea A un dominio y M un A -módulo finitamente generado. Sea

$$\begin{array}{ccccc} & & \varphi & & \\ & \searrow & & \swarrow & \\ \hat{A} \otimes_A M & \hookrightarrow & \hat{A} \otimes_A \hat{M} & \longrightarrow & \hat{A} \otimes_{\hat{A}} \hat{M} = \hat{M} \end{array}$$

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

DEMOSTRACIÓN: Por la proposición anterior se induce:

$$\begin{array}{ccccccc} 0 & \rightarrow & M & \rightarrow & M \otimes N & \rightarrow & N \rightarrow 0 \\ & & & & \Downarrow & & \\ 0 & \rightarrow & \hat{M} & \rightarrow & \widehat{M \otimes N} & \rightarrow & \hat{N} \rightarrow 0 \end{array}$$

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

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

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

Si A es noetheriano, entonces ahí la segunda fila sí está en $A\text{-Mod}$ y por lema de la serpiente:

$$\begin{array}{ccccc} & & 0 = \ker \beta & \longrightarrow & \ker \alpha \\ & & \downarrow & & \downarrow \\ \hat{A} \otimes_A N & \cdots \longrightarrow & \hat{F} & \cdots \longrightarrow & \hat{A} \otimes_A M \\ \downarrow \gamma & & \downarrow & & \downarrow \\ \hat{N} & \cdots \longrightarrow & \hat{F} & \cdots \longrightarrow & \hat{M} \\ & & \downarrow & & \\ & & \text{coker } \gamma = 0 & & \end{array}$$

(A red curved arrow connects $\ker \alpha$ to $\text{coker } \gamma = 0$.)

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

Proposición 13.31: Sea A un dominio noetheriano, \mathfrak{a} un ideal de A , y \hat{A} la completación \mathfrak{a} -ádica de A . Entonces se cumplen:

1. \hat{A} es una A -álgebra plana.
2. $\mathfrak{a} = \mathfrak{a}\hat{A} \cong \hat{A} \otimes_A \mathfrak{a}$.

3. $\widehat{(\mathfrak{a}^n)} = (\hat{\mathfrak{a}})^n$.
4. $\mathfrak{a}^n / \mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n / \hat{\mathfrak{a}}^{n+1}$.
5. $\mathfrak{a} \subseteq \mathfrak{J}(\hat{A})$.

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

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

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

Corolario 13.32: Sea (A, \mathfrak{m}, k) noetheriano local, y sea \hat{A} su completión \mathfrak{m} -ádica. Entonces $(\hat{A}, \hat{\mathfrak{m}}, k)$ es local.

Proposición 13.33: Sea A un dominio noetheriano, \mathfrak{a} un ideal de A , M un A -módulo finitamente generado y \hat{M} la completión \mathfrak{a} -ádica de M . Entonces:

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

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

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

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

Corolario 13.34: Sea A es un dominio noetheriano íntegro y \mathfrak{a} un ideal de A . Entonces

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

Corolario 13.35: Sea A un dominio noetheriano, \mathfrak{a} un ideal contenido en $\mathfrak{J}(A)$ y M un A -módulo finitamente generado. Entonces la \mathfrak{a} -topología sobre M es de Hausdorff.

Corolario 13.36: Sea (A, \mathfrak{m}) un dominio noetheriano local y M un A -módulo finitamente generado. Entonces la \mathfrak{m} -topología sobre M es de Hausdorff. En particular, la \mathfrak{m} -topología sobre A es de Hausdorff.

Corolario 13.37: Sea A un dominio noetheriano y \mathfrak{p} un ideal primo. Entonces el $\ker(A \rightarrow A_{\mathfrak{p}})$ es la intersección de todos los ideales \mathfrak{p} -primarios.

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

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

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

Definición 13.38: Sea \mathfrak{a} un ideal de A , se define:

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

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

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

$$G(M) := \bigoplus_{n \in \mathbb{N}} M_n / M_{n+1},$$

el cual es un $G(A)$ -módulo graduado, con componentes homogéneas $\mathrm{gr}_n(M) := M_n / M_{n+1}$.

Proposición 13.39: Sea A un dominio noetheriano, \mathfrak{a} un ideal de A . Entonces:

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

DEMOSTRACIÓN:

1. Como A es noetheriano, \mathfrak{a} es finitamente generado, luego $\mathfrak{a} = (\alpha_1, \dots, \alpha_s)$. Sea $\bar{\alpha}_i$ la proyección de α_i en $\mathfrak{a}/\mathfrak{a}^2$. Luego $G(A) = (A/\mathfrak{a})[\bar{\alpha}_1, \dots, \bar{\alpha}_s]$. A/\mathfrak{a} es noetheriano y $G(A)$ es una (A/\mathfrak{a}) -álgebra de tipo finito, luego es noetheriana.
2. Basta recordar que $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$.
3. Nótese que cada $\text{gr}_n(M)$ es noetheriano, luego es finitamente generado y como $(M_n)_n$ es estable, entonces $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ para algún $n_0 \geq 0$ y luego $\text{gr}_{n_0+r}(M) = 0$ en (A/\mathfrak{a}) . Por lo que, $G(M) = \bigoplus_{n=0}^{n_0} \text{gr}_n(M)$, el cual es una suma directa finita de módulos finitamente generados, luego es también finitamente generada como $G(A)$ -módulo. \square

Lema 13.40: Sean A, B grupos abelianos con filtraciones $(A_n)_n, (B_n)_n$ resp., que inducen su topología. Sea $\phi: A \rightarrow B$ un homomorfismo de grupos tal que $\phi[A_n] \subseteq B_n$, y sean $G(\phi): G(A) \rightarrow G(B)$ y $\hat{\phi}: \hat{A} \rightarrow \hat{B}$ los homomorfismos inducidos. Entonces si $G(\phi)$ es inyectivo (resp. suprayectivo, isomorfismo), entonces ϕ también lo es.

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

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

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

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \ker(\text{gr}_n(\phi)) & \longrightarrow & \ker(f_{n+1}) & \longrightarrow & \ker(f_n) \\
 & & & & & \searrow & \\
 & & & & & & \text{coker}(\text{gr}_n(\phi)) \longrightarrow \text{coker}(f_{n+1}) \longrightarrow \text{coker}(f_n) \longrightarrow 0
 \end{array}$$

Recordando que $f_0 = 0$, se concluye que por inducción si $\ker(\text{gr}_n(\phi)) = 0$ ($G(\phi)$ inyectivo), entonces $\ker(f_n) = 0$ y si $\text{coker}(\text{gr}_n(\phi)) = 0$, entonces $\text{coker}(f_n) = 0$. Finalmente, se concluye por la proposición 13.12. \square

Proposición 13.41: Sea A un dominio, \mathfrak{a} un ideal de A , M un A -módulo y $(M_n)_{n \in \mathbb{N}}$ una \mathfrak{a} -filtración de M . Si A es completo en la topología \mathfrak{a} -ádica,

M es Hausdorff en la topología inducida por la filtración y $G(M)$ es un $G(A)$ -módulo finitamente generado, entonces M es finitamente generado.

DEMOSTRACIÓN: Elija un sistema generador de $G(M)$ y sean $\mathbf{h}_1, \dots, \mathbf{h}_s$ sus componentes homogéneas de grado n_1, \dots, n_s resp. Como $\mathbf{h}_i \in \text{gr}_{n_i}(M)$, entonces $\mathbf{h}_i = [\mathbf{m}_i]$ con $\mathbf{m}_i \in M_{n_i}$. Sea $F_i = A$ el módulo con la \mathfrak{a} -filtración estable $(\mathfrak{a}^{n_i+r})_{r=0}^\infty$, y sea $F := \bigoplus_{i=1}^s F_i$, luego, cada F_i es un A -módulo libre generado por 1, por lo que podemos mandar $\mathbf{e}_i \mapsto \mathbf{m}_i$ para obtener un homomorfismo $\phi: F \rightarrow M$ de módulos (en particular, de grupos abelianos) filtrados. Luego, ϕ induce un homomorfismo $G(\phi): G(F) \rightarrow G(M)$ que es suprayectivo, luego por la proposición anterior, $\hat{\phi}$ es suprayectivo y como el siguiente diagrama conmuta:

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

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

Corolario 13.42: Sea A un dominio, \mathfrak{a} un ideal de A , M un A -módulo y $(M_n)_{n \in \mathbb{N}}$ una \mathfrak{a} -filtración de M . Si A es completo en la topología \mathfrak{a} -ádica, M es Hausdorff en la topología inducida por la filtración y $G(M)$ es un $G(A)$ -módulo noetheriano, entonces M es noetheriano.

Teorema 13.43: Si A es un dominio noetheriano, \mathfrak{a} es un ideal de A , entonces su completión \mathfrak{a} -ádica \hat{A} también es noetheriana.

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

Teorema 13.44: Sea A un dominio noetheriano, entonces su anillo de potencias $A[[x_1, \dots, x_n]]$ también es noetheriano.

DEMOSTRACIÓN: Basta probarlo para $A[[x_1]]$ por inducción, para lo cuál nótese que $A[[x_1]]$ es la completión (x_1) -ádica de $A[x_1]$ que es noetheriano por bases de Hilbert. \square

13.4 Teoría de la dimensión

Definición 13.45: Sea C una clase de A -módulos y sea G un grupo abeliano. Una función $\lambda: C \rightarrow G$ se dice *aditiva* si para toda sucesión exacta

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

en C , se satisface que:

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

Ejemplo. • Sea C la clase de A -módulos finitamente generados libres. Entonces $\text{rank}: C \rightarrow \mathbb{Z}$ es una función aditiva.

- Sea A un dominio artiniiano, entonces por Akizuki es noetheriano, luego todo módulo finitamente generado es noetheriano, y por tanto, también es artiniiano. Luego posee longitud finita, finalmente por la proposición 5.43 se concluye que la longitud $\ell: C \rightarrow \mathbb{Z}$, donde C son los A -módulos finitamente generados, es una función aditiva.

Éste segundo ejemplo será importante.

Definición 13.46: Sea C la clase de A -módulos finitamente generados y $\lambda: C \rightarrow \mathbb{Z}$ una función aditiva. Entonces, para todo A -módulo graduado finitamente generado M se define su *serie de Poincaré-Hilbert* como

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

Teorema 13.47 (Hilbert-Serre): Sea A un anillo graduado noetheriano, tal que $A = A_0[\alpha_1, \dots, \alpha_s]$ donde α_i es homogéneo de grado n_i ; y sea M un A_0 -módulo graduado finitamente generado. Entonces, existe $f(t) \in \mathbb{Z}[t]$ tal que

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

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

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

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

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

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

Sumando sobre n se obtiene que:

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

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

Definición 13.48: Sea A un anillo graduado noetheriano y sea M un A_0 -módulo finitamente generado. Se denota por $d(M)$ al orden del polo de $\text{Poin}(M, t)$ en 1, es decir, al máximo n tal que

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

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

Corolario 13.49: Sea A un anillo graduado noetheriano con $A = A_0[\alpha_1, \dots, \alpha_s]$ donde cada α_i es homogéneo de grado 1. Sea M un A_0 -módulo graduado finitamente generado, entonces $\lambda(M_n) = p(n)$ para n suficientemente grande, con $p(x) \in \mathbb{Q}[x]$ y $\deg(p) = d(M) - 1$.

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

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

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

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

para todo $n \geq N$, que es lo que buscábamos. \square

Ejemplo 8: Sea $A = A_0[x_1, \dots, x_s]$ el anillo de polinomios sobre un dominio artinianiano A_0 . Luego cada componente homogénea A_n es un A_0 -módulo libre generado por los monomios de la forma $x_1^{\eta_1} \cdots x_s^{\eta_s}$, donde $\sum_{i=1}^s \eta_i = n$, por lo que, por un problema de combinatoria se satisface que

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

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

Proposición 13.50: Sea A un anillo graduado noetheriano y M un A_0 -módulo graduado finitamente generado. Si $\beta \in A$ es homogéneo y no es divisor de cero en M , entonces $d(M/\beta M) = d(M) - 1$.

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

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

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

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

Proposición 13.51: Sea (A, \mathfrak{m}) un dominio noetheriano local, \mathfrak{q} un ideal \mathfrak{m} -primario, M un A -módulo finitamente generado y $(M_n)_{n \in \mathbb{N}}$ una \mathfrak{q} -filtración estable. Entonces:

1. M/M_n es de longitud finita.
2. Si \mathfrak{q} está generado por al menos s elementos, entonces $\ell(M/M_n) = p(n)$ con $p(x) \in \mathbb{Q}[x]$ y $\deg(p) \leq s$ para n suficientemente grande.
3. El coeficiente líder de p depende exclusivamente de M y de \mathfrak{q} , no de la filtración escogida.

DEMOSTRACIÓN:

1. Sea $G(A) := \bigoplus_{n \in \mathbb{N}} \mathfrak{q}^n / \mathfrak{q}^{n+1}$ y $G(M) := \bigoplus_{n \in \mathbb{N}} M_n / M_{n+1}$. Como A es noetheriano, $G(A)$ también y luego $G(M)$ es un $G(A)$ -módulo graduado finitamente generado. Nótese además que en $\text{gr}_0(A) = A/\mathfrak{q}$ el maximal es nilpotente y es noetheriano, por lo tanto, es artinianiano. Como

$(M_n)_n$ es una \mathfrak{q} -filtración, entonces $\text{gr}_n(M)$ es un A -módulo noetheriano y se anula por \mathfrak{q} , luego es un (A/\mathfrak{q}) -módulo noetheriano, por lo tanto, tiene longitud finita. Por inducción se concluye que M/M_n tiene longitud finita y que

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

2. Recordando el ejemplo vemos que ℓ es una función aditiva sobre los (A/\mathfrak{q}) -módulos finitamente generados. Sea $\mathfrak{q} = (\alpha_1, \dots, \alpha_s)$, y sea $\bar{\alpha}_i$ la proyección de α_i en $\mathfrak{q}/\mathfrak{q}^2$, luego se sigue que $G(A) = (A/\mathfrak{q})[\bar{\alpha}_1, \dots, \bar{\alpha}_s]$ con $\bar{\alpha}_i$ homogéneo de grado 1. Luego $\lambda(\text{gr}_n(M)) = \ell(M_n/M_{n+1}) = p(n)$ para n suficientemente grande y $\deg(p) \leq s$ (¿por qué?).
3. Sea $(M'_n)_n$ otra \mathfrak{q} -filtración estable. Por el inciso anterior, $\ell(M/M'_n) = q(n)$ para n suficientemente grande. Luego tienen diferencia acotada, i.e., $M_{n+n_0} \subseteq M'_n$ y $M'_{n+n_0} \subseteq M_n$, por lo que $p(n+n_0) \geq q(n)$ y $q(n+n_0) \geq p(n)$. De ello se concluye que

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

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

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

Corolario 13.52: Sea (A, \mathfrak{m}) un dominio noetheriano local, y \mathfrak{q} un ideal \mathfrak{m} -primario generado por s elementos. Entonces $\ell(A/\mathfrak{q}^n) = p(n)$, donde $p(x) \in \mathbb{Q}[x]$ y $\deg(p) \leq s$.

Definición 13.53: Dado un A -módulo M , considerando la filtración $(\mathfrak{q}^n M)_n$ definimos su polinomio de Hilbert-Samuel, denotado $\chi_{\mathfrak{q}}^M(n)$, como el polinomio de $\ell(M/M_n)$ para n suficientemente grande. Si $M = A$, entonces obviamos el superíndice, i.e., $\chi_{\mathfrak{q}}(n) := \chi_{\mathfrak{q}}^A(n)$.

Proposición 13.54: Sea (A, \mathfrak{m}) un dominio noetheriano local y \mathfrak{q} un ideal \mathfrak{m} -primario. Entonces $\deg(\chi_{\mathfrak{q}}) = \deg(\chi_{\mathfrak{m}})$.

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

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

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

Definición 13.55: Sea (A, \mathfrak{m}) un dominio noetheriano local. Denotaremos por $d(A) := \deg(\chi_{\mathfrak{q}})$, donde \mathfrak{q} es cualquier ideal \mathfrak{m} -primario. En particular, $d(A) = d(\text{gr}_{\mathfrak{m}}(A))$, donde aquí $d(\text{gr}_{\mathfrak{m}}(A))$ representa (en sentido viejo) el orden del polo de $\text{Poin}(\text{gr}_{\mathfrak{m}}(A), t)$ en $t = 1$.

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

Corolario 13.56: $\delta(A) \geq d(A)$.

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

Proposición 13.57: Sea (A, \mathfrak{m}) un dominio noetheriano local, \mathfrak{q} un ideal \mathfrak{m} -primario y M un A -módulo finitamente generado. Si $\alpha \in A$ no es divisor de cero en M y $M' := M/\alpha M$, entonces $\deg(\chi_{\mathfrak{q}}^{M'}) \leq \deg(\chi_{\mathfrak{q}}^M) - 1$.

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

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

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

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

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

Corolario 13.58: Sea (A, \mathfrak{m}) un dominio noetheriano local y $x \in A$ un elemento que no es divisor de cero. Entonces $d(A/(x)) \leq d(A) - 1$.

Proposición 13.59: $d(A) \geq k\text{-dim}(A)$.

DEMOSTRACIÓN: Procedemos por inducción sobre $d := d(A)$: Si $d = 0$, entonces $\ell(A/\mathfrak{m}^n)$ es constante para n suficientemente grande, luego, por

correspondencia, $\ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 0$ y $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, por lo que A es artinian y $k\text{-dim } A = 0$.

Si $d > 0$: Si $k\text{-dim}(A) = 0$, entonces claramente vale el enunciado, sino sea

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

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

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

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

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

Corolario 13.60: Si A es un dominio noetheriano local, entonces posee dimensión de Krull finita.

Definición 13.61: Sea $\mathfrak{p} \triangleleft A$ primo, entonces definimos su *altura*, denotada $n := \text{alt } \mathfrak{p} \geq 0$, como el máximo natural tal que existe una cadena

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$

de ideales primos de A . La dimensión de Krull de A corresponde entonces al supremo de las alturas de sus ideales primos.

Además por correspondencia se puede ver que $\text{alt } \mathfrak{p} = k\text{-dim}(A_{\mathfrak{p}})$.

Corolario 13.62: En un dominio noetheriano local todo ideal primo posee altura finita. Luego toda cadena descendiente de ideales primos posee minimal.

Proposición 13.63: Sea (A, \mathfrak{m}) un dominio noetheriano local de dimensión d . Entonces existe un ideal \mathfrak{m} -primario generado por d elementos. En consecuencia, $k\text{-dim}(A) \geq \delta(A)$.

DEMOSTRACIÓN: Construiremos, por inducción, un ideal (x_1, \dots, x_d) tal que para todo $\mathfrak{p} \supseteq (x_1, \dots, x_i)$ primo se cumple que $\text{alt } \mathfrak{p} \geq i$. Claramente aplica para $i = 0$. Sea $i > 0$ y sean \mathfrak{p}_j , con $1 \leq j \leq s$, los ideales primos

minimales que contienen a (x_1, \dots, x_{i-1}) tales que $\text{alt } \mathfrak{p}_j = i - 1$ (nótese que s podría ser 0). Como $i - 1 < d = \text{alt } \mathfrak{m}$, entonces $\mathfrak{p}_j \neq \mathfrak{m}$ para todo j y luego $\mathfrak{m} \neq \bigcup_{j=1}^s \mathfrak{p}_j$ por la proposición 2.58, luego sea $x_i \in \mathfrak{m} \setminus \bigcup_{j=1}^s \mathfrak{p}_j$. Sea \mathfrak{q} un ideal primo que contiene a (x_1, \dots, x_i) , luego contiene a un ideal minimal \mathfrak{p} de (x_1, \dots, x_{i-1}) ; si $\mathfrak{p} = \mathfrak{p}_j$ para algún j , entonces como $x_i \in \mathfrak{q} \setminus \mathfrak{p}$ se cumple que $\mathfrak{p} \subset \mathfrak{q}$ y $\text{alt } \mathfrak{q} > \text{alt } \mathfrak{p}$. Si \mathfrak{p} es otro ideal, entonces $\text{alt } \mathfrak{p} \geq i$ y $\text{alt } \mathfrak{q} \geq i$.

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

Teorema 13.64 – Teorema fundamental de la dimensión: En un dominio noetheriano local (A, \mathfrak{m}) son iguales:

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

Definición 13.65: Sea (A, \mathfrak{m}) un dominio noetheriano local, y sea $d = k\text{-dim}(A)$. A un conjunto $\alpha_1, \dots, \alpha_d$ de elementos tales que generan un ideal \mathfrak{m} -primario se les dice un *sistema de parámetros*.

De él se extraen varios corolarios:

Corolario 13.66: Sea (A, \mathfrak{m}) un dominio noetheriano local y $k := A/\mathfrak{m}$. Entonces:

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

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

Corolario 13.67: Sea A un dominio noetheriano y sean $\alpha_1, \dots, \alpha_r \in A$. Luego todo ideal primo \mathfrak{p} asociado a $(\alpha_1, \dots, \alpha_r)$ tiene altura $\leq r$.

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

Teorema 13.68 (de los ideales principales de Krull): Sea A un dominio noetheriano y sea $\alpha \in A$ tal que no es ni divisor de cero ni inversible. Entonces todo ideal primo minimal \mathfrak{p} que contiene a α tiene altura 1.

DEMOSTRACIÓN: Por el corolario anterior se cumple que $\text{alt } \mathfrak{p} \leq 1$. Si $\text{alt } \mathfrak{p} = 0$, entonces, por la proposición 6.59 se cumple que \mathfrak{p} está asociado al cero y que sus elementos son divisores de cero, pero $\alpha \in \mathfrak{p}$ lo que sería absurdo. En consecuencia, necesariamente $\text{alt } \mathfrak{p} = 1$. \square

Corolario 13.69: Sea (A, \mathfrak{m}) un dominio noetheriano local. Para todo $\beta \in \mathfrak{m}$ se cumple que $k\text{-dim}(A/(\beta)) = k\text{-dim}(A) - 1$.

DEMOSTRACIÓN: Sea $d := k\text{-dim}(A/(\beta))$, por el corolario 13.58 se satisface que $d \leq k\text{-dim}(A) - 1$. Por otro lado, sean $\bar{\alpha}_1, \dots, \bar{\alpha}_d$ un sistema de parámetros de $A/(\beta)$, luego $(\alpha_1, \dots, \alpha_d, \beta)$ es un ideal \mathfrak{m} -primario en A y luego $d + 1 \geq k\text{-dim}(A)$. \square

Corolario 13.70: Sea (A, \mathfrak{m}) un dominio noetheriano local y \hat{A} la completación \mathfrak{m} -ádica de A . Entonces $k\text{-dim}(A) = k\text{-dim}(\hat{A})$.

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

Proposición 13.71: Sea (A, \mathfrak{m}) un dominio noetheriano local, $\{\alpha_1, \dots, \alpha_d\}$ un sistema de parámetros de A y $\mathfrak{q} := (\alpha_1, \dots, \alpha_d)$. Sea $f \in A[t_1, \dots, t_d]$ un polinomio homogéneo de grado $s > 0$ tal que

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

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

DEMOSTRACIÓN: Considere el siguiente epimorfismo:

$$\varphi := \text{ev}_{(\bar{\alpha}_1, \dots, \bar{\alpha}_d)} : (A/\mathfrak{q})[t_1, \dots, t_d] \longrightarrow \text{gr}_{\mathfrak{q}}(A).$$

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

$$d(\text{gr}_{\mathfrak{q}}(A)) \leq d((A/\mathfrak{q})[t_1, \dots, t_d]/(\bar{f}))$$

$$\begin{aligned}
&= d((A/\mathfrak{q})[t_1, \dots, t_d]) - 1 \\
&= d - 1,
\end{aligned}$$

donde la última igualdad se deduce de lo dicho en el ejemplo 8. Pero $d(\operatorname{gr}_{\mathfrak{q}}(A)) = d$, por lo que el último resultado es absurdo. \square

Corolario 13.72: Si k es un cuerpo, $A \supseteq k$ es un dominio noetheriano local de maximal \mathfrak{m} tal que $k \cong A/\mathfrak{m}$ y $\alpha_1, \dots, \alpha_d$ son un sistema de parámetros de A , entonces son algebraicamente independientes sobre k .

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

Teorema 13.73: Sea (A, \mathfrak{m}) un dominio noetheriano local de dimensión d y sea $k := A/\mathfrak{m}$. Entonces son equivalentes:

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

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

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

$$\operatorname{ev}_{(\alpha_1, \dots, \alpha_d)}: k[t_1, \dots, t_d] \longrightarrow \operatorname{gr}_{\mathfrak{m}}(A)$$

es un isomorfismo. \square

Definición 13.74: Un dominio noetheriano local A se dice *regular* si satisface cualquiera de las condiciones del teorema anterior.

Lema 13.75: Sea A un dominio, \mathfrak{a} un ideal de A tal que $\bigcap_{n \in \mathbb{N}} \mathfrak{a}^n = (0)$. Si $\operatorname{gr}_{\mathfrak{a}}(A)$ es un dominio íntegro, entonces A también lo es.

DEMOSTRACIÓN: Sean α, β no nulos. Como $\bigcap_{n \in \mathbb{N}} \mathfrak{a}^n$, entonces existen m, r naturales tales que $\alpha \in \mathfrak{a}^m \setminus \mathfrak{a}^{m+1}$ y $\beta \in \mathfrak{a}^r \setminus \mathfrak{a}^{r+1}$, luego sus proyecciones $\bar{\alpha}, \bar{\beta}$ tienen componentes homogéneas no nulas en $\operatorname{gr}_m(A), \operatorname{gr}_r(A)$ resp., por lo que $\bar{\alpha} \cdot \bar{\beta} \neq 0$ y luego $\alpha \cdot \beta \neq 0$ en A . \square

Corolario 13.76: Un dominio regular de dimensión 1 es un dominio de valuación discreta.

Proposición 13.77: Sea A un dominio noetheriano local. Entonces A es regular syss \hat{A} es regular.

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

Variedades algebraicas

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

—Carlos Ivorra Castillo [17]

No suelo abrir con citas textuales, no obstante amerita hacerlo en éste capítulo, pues se abre la puerta a una de las transiciones más curiosas de las matemáticas. «Los geómetras se imaginan las matemáticas» es una frase que es tan acertada que hasta asusta; en última instancia casi la totalidad de las matemáticas se reduce a geometría, pero decir «geometría» no quiere significar que se regresen a las construcciones por regla y compás de Euclides, sino que, introduciendo toda la maquinaria de la topología, para contestar a problemas algebraicos se necesita primero transformarlos en problemas geométricos, o más precisamente, en problemas de espacios topológicos especiales.

Usualmente suelo dejar las sorpresas para el lector, pero le prometo que en éste capítulo y los subsiguientes encontrará la salsa de la cuestión.

14.1 Variedades afines

Desde ahora en adelante se asume que k siempre representa un cuerpo *algebraicamente cerrado*.

Definición 14.1: Denotaremos por $\mathbb{A}_k^n := k^n$ al *espacio afín* de dimensión n sobre k .

Además de ello, en éste capítulo denotaremos por $A := k[x_1, \dots, x_n]$ cuando no haya ambigüedad sobre la cantidad de variables.

La notación de \mathbb{A}^n en lugar de K^n es porque lo que buscamos es constituir una categoría, en la que la estructura de espacio vectorial no tiene ningún rol; otro detalle es que en K^n hay vectores especiales, como el $\vec{0}$ y la base canónica, mientras que \mathbb{A}^n , al igual que un espacio geométrico (afín), carece de puntos de referencia estándares.

Definición 14.2 – Conjunto algebraico: Sea \mathbb{A}^n un espacio afín, entonces dado un conjunto de polinomios $T \subseteq A$ se define

$$\mathbf{V}(T) := \{\mathbf{p} \in \mathbb{A}^n : \forall f \in T \ f(\mathbf{p}) = 0\}.$$

Si $T = \{f_1, \dots, f_m\}$ nos permitimos denotar $\mathbf{V}(f_1, \dots, f_m)$. Los conjuntos de ésta forma son llamados *algebraicos afines*.

Otro convenio es denotar por \mathbf{x} a una variable y \mathbf{p} a un punto específico.

Primero veamos la conexión con álgebra:

Lema 14.3: Si $T_1 \subseteq T_2 \subseteq A$, entonces $\mathbf{V}(T_1) \supseteq \mathbf{V}(T_2)$. Además $\mathbf{V}(0) = \mathbb{A}^n$ y $\mathbf{V}(1) = \emptyset$.

Proposición 14.4: Sean $T \subseteq A$ y $\mathfrak{a} := (T)$ (el ideal generado por T), entonces $\mathbf{V}(T) = \mathbf{V}(\mathfrak{a})$.

DEMOSTRACIÓN: Por la proposición anterior es claro que $\mathbf{V}(T) \supseteq \mathbf{V}(\mathfrak{a})$. Veamos que $\mathbf{V}(T) \subseteq \mathbf{V}(\mathfrak{a})$: Sea $\mathbf{a} \in \mathbf{V}(T)$ nos basta ver que para cualquier $f \in \mathfrak{a}$ se cumpla que $f(\mathbf{a}) = 0$. Para ello notemos que si $f \in (T)$, entonces existen polinomios $\lambda_i(\mathbf{x}) \in A$ y $g_i(\mathbf{x}) \in T$ tales que

$$f(\mathbf{x}) = \sum_{i=1}^m \lambda_i(\mathbf{x}) g_i(\mathbf{x})$$

pero como $g_i(\mathbf{a}) = 0$ para todo $g_i \in T$ (por definición de estar en $\mathbf{V}(T)$) se concluye que $f(\mathbf{a}) = 0$. \square

Corolario 14.5: Si el conjunto $Z \subseteq \mathbb{A}^n$ es algebraico, entonces existen finitos polinomios $p_1, \dots, p_m \in A$ tales que $Z = \mathbf{V}(p_1, \dots, p_m)$.

DEMOSTRACIÓN: Por definición $Z = \mathbf{V}(T)$ y por el lema se da que $Z = \mathbf{V}(J)$ con $J = (T)$. Por el teorema de bases de Hilbert A es un anillo noetheriano, luego $J = (p_1, \dots, p_m)$ que hacen cumplir el enunciado. \square

Lema 14.6: Se cumplen:

1. Sean $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$ ideales, entonces:

$$\mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbf{V}(\mathfrak{a} \cdot \mathfrak{b}) = \mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}).$$

2. Sean $(\mathfrak{a}_j)_{j \in J} \trianglelefteq A$ ideales. Entonces:

$$\mathbf{V}\left(\sum_{j \in J} \mathfrak{a}_j\right) = \mathbf{V}\left(\bigcup_{j \in J} \mathfrak{a}_j\right) = \bigcap_{j \in J} \mathbf{V}(\mathfrak{a}_j).$$

En consecuencia, los conjuntos algebraicos afines conforman los cerrados de una topología.

DEMOSTRACIÓN:

1. Como $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, entonces $\mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathbf{V}(\mathfrak{a} \cdot \mathfrak{b})$.

Veamos que $\mathbf{V}(\mathfrak{a} \cdot \mathfrak{b}) \subseteq \mathbf{V}(\mathfrak{a} \cap \mathfrak{b})$ por contrarrecíproca: Sea $\mathbf{a} \notin \mathbf{V}(\mathfrak{a} \cap \mathfrak{b})$, por definición existe $f \in \mathfrak{a}, g \in \mathfrak{b}$ tales que $f(\mathbf{a}) \neq 0, g(\mathbf{a}) \neq 0$. Luego $f(\mathbf{a})g(\mathbf{a}) = (f \cdot g)(\mathbf{a}) \neq 0$ donde $f \cdot g \in \mathfrak{a} \cdot \mathfrak{b}$, por lo que $\mathbf{a} \notin \mathbf{V}(\mathfrak{a} \cdot \mathfrak{b})$.

Veamos que $\mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) \subseteq \mathbf{V}(\mathfrak{a} \cap \mathfrak{b})$: Basta notar que $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$ (resp. $\subseteq \mathfrak{b}$), luego $\mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) \supseteq \mathbf{V}(\mathfrak{a})$ (resp. $\supseteq \mathbf{V}(\mathfrak{b})$). En consecuencia $\mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) \subseteq \mathbf{V}(\mathfrak{a} \cap \mathfrak{b})$ como se quería probar.

2. En primer lugar, nótese que $\sum_{j \in J} \mathfrak{a}_j = \left(\bigcup_{j \in J} \mathfrak{a}_j\right)$, lo que por la prop. 14.4 induce la primera igualdad.

La segunda se deduce de lo siguiente:

$$\bigcap_{j \in J} \mathbf{V}(\mathfrak{a}_j) = \{\mathbf{a} \in \mathbb{A}^n : \forall j \mathbf{a} \in \mathbf{V}(\mathfrak{a}_j)\}$$

$$\begin{aligned}
&= \{\mathbf{a} \in \mathbb{A}^n : \forall j \forall f \in \mathfrak{a}_j \ f(\mathbf{a}) = 0\} \\
&= \{\mathbf{a} \in \mathbb{A}^n : \forall f \in \left(\bigcup_{j \in J} \mathfrak{a}_j\right) \ f(\mathbf{a}) = 0\} \\
&= \mathbf{V}\left(\bigcup_{j \in J} \mathfrak{a}_j\right). \quad \square
\end{aligned}$$

Definición 14.7: Dado el espacio afín \mathbb{A}^n se le llama *topología de Zariski* a la topología que tiene como cerrados a los conjuntos algebraicos.

A pesar de que de ésta manera obtenemos de manera bastante directa una topología, ésta no es para nada conveniente. En \mathbb{A}^1 se da que los cerrados son \mathbb{A}^1, \emptyset y todos los conjuntos finitos; como \mathbb{A}^1 es infinito (pues k es algebraicamente cerrado) se concluye que \mathbb{A}^1 siempre es un espacio T_1 que no es de Hausdorff.

De momento tenemos una función que transforma conjuntos desde A en cerrados de \mathbb{A}^n , veamos la inversa:

Definición 14.8: Sea $X \subseteq \mathbb{A}^n$, se define:

$$\mathbf{I}(X) := \{f \in A : \forall \mathbf{a} \in X \ f(\mathbf{a}) = 0\}.$$

Lema 14.9: Para todo $X \subseteq \mathbb{A}^n$ se cumple que $\mathbf{I}(X)$ es un ideal.

Proposición 14.10: Si $X \subseteq \mathbb{A}^n$, entonces $\mathbf{I}(X)$ es un ideal radical.

DEMOSTRACIÓN: Sea $f^n \in \mathbf{I}(X)$, entonces $f(\mathbf{a})^n = 0$ para todo \mathbf{a} . Luego, como k es un cuerpo y, por ende, un dominio íntegro se cumple que $f(\mathbf{a}) = 0$ y $f \in \mathbf{I}(X)$. \square

Ahora veremos uno de los resultados principales de la geometría algebraica:

Teorema 14.11 – Teorema de ceros de Hilbert: Sea k algebraicamente cerrado. Entonces:

1. Si $\mathfrak{a} \trianglelefteq k[x_1, \dots, x_n]$ es un ideal, entonces $\mathbf{V}(\mathfrak{a}) = \emptyset$ syss $\mathfrak{a} = (1)$ (débil).

2. Dado un ideal $\mathfrak{a} \leq k[x_1, \dots, x_n]$ se cumple que $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \text{Rad}(\mathfrak{a})$ (fuerte).

DEMOSTRACIÓN: En éste teorema nos referiremos al antiguo teorema de ceros de Hilbert como el Nullstellensatz *algebraico*, en contraste con el presente como el *geométrico*.

1. Ya vimos que $\mathbf{V}(1) = \emptyset$. Recíprocamente y por contradicción sea $\mathfrak{a} \neq A$ tal que $\mathbf{V}(\mathfrak{a}) = \emptyset$, por el teorema de Krull está contenido en un ideal maximal \mathfrak{m} que por el Nullstellensatz algebraico es de la forma $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$. Pero claramente $(\alpha_1, \dots, \alpha_n) \in \mathbf{V}(\mathfrak{m}) \subseteq \mathbf{V}(\mathfrak{a})$, así que $\mathbf{V}(\mathfrak{a}) \neq \emptyset$.
2. En ésta demostración, las letras mayúsculas denotaran polinomios para no confundirse con las variables. Es claro que $\mathfrak{a} \subseteq \mathbf{I}(\mathbf{V}(\mathfrak{a}))$ y por la proposición anterior se tiene que $\text{Rad}(\mathfrak{a}) \subseteq \mathbf{I}(\mathbf{V}(\mathfrak{a}))$.

Sea $F \in \mathbf{I}(\mathbf{V}(\mathfrak{a}))$, es decir, $F(\mathbf{p}) = 0$ para todo $\mathbf{p} \in \mathbf{V}(\mathfrak{a})$, la cual satisface que $H(\mathbf{p})$ para todo $H \in \mathfrak{a}$. Lo que queremos ver es que para algún r se cumpla que $F^r \in \mathfrak{a}$.

Primero, por teorema de las bases de Hilbert sea $\mathfrak{a} = (G_1, \dots, G_m)$. Para probar lo que queremos emplearemos un truco atribuido a Rabinowitsch: Añadamos una variable extra z a $K[x_1, \dots, x_n; z]$ y definamos $\mathfrak{b} := (G_1, \dots, G_m; 1 - Fz)$.

Veamos que $\mathbf{V}(\mathfrak{b}) = \emptyset$: Por contradicción, si no lo fuese tendría algún punto $(p_1, \dots, p_n; q) \in \mathbb{A}_K^{n+1}$. Luego para todo i se cumple que $G_i(p_1, \dots, p_n) = 0$ y además $1 - F(p_1, \dots, p_n) \cdot q = 0$; pero claramente $(p_1, \dots, p_n) \in \mathbf{V}(\mathfrak{a})$ así que $F(p_1, \dots, p_n) = 0$ por construcción lo que es contradictorio.

En consecuencia, por el Nullstellensatz geométrico se tiene que $\mathfrak{b} = (1)$, es decir, existen $H_i, L \in K[x_1, \dots, x_n, z]$ tales que

$$\sum_{i=1}^m H_i \cdot G_i + L \cdot (1 - Fz) = 1.$$

Ojo: ésta es una igualdad entre polinomios. Luego nos permitimos pasar ésta igualdad al *cuerpo* de polinomios, ya que es una extensión de anillos, así pues si $z = 1/F$ se obtiene que

$$H_i(x_1, \dots, x_n, 1/F) = \frac{H'_i(x_1, \dots, x_n)}{F(x_1, \dots, x_n)^r}$$

donde r es el grado máximo entre los H_i 's. De modo que se obtiene que

$$\sum_{i=1}^m \frac{H'_i}{F^r} G_i = 1 \iff F^r = H'_1 G_1 + \cdots + H'_m G_m$$

Esto es una proposición en el cuerpo de funciones racionales, luego es también cierta en el anillo de polinomios. Finalmente, como los G_i 's están en \mathfrak{a} , se cumple que $F^r \in \mathfrak{a}$ tal como se quería probar. \square

Proposición 14.12: Se cumple que:

1. Si $T \subseteq A$, entonces $T \subseteq \mathbf{I}(\mathbf{V}(T))$. Así mismo, si $X \subseteq \mathbb{A}^n$, entonces $X \subseteq \mathbf{V}(\mathbf{I}(X))$.
2. Si $X \subseteq Y \subseteq \mathbb{A}^n$, entonces $\mathbf{I}(X) \supseteq \mathbf{I}(Y)$.
3. Sea $X \subseteq \mathbb{A}^n$, entonces $\mathbf{V}(\mathbf{I}(X)) = \overline{X}$, es decir, es la clausura de X en la topología de Zariski.

DEMOSTRACIÓN: Probaremos la 3: Claramente $\mathbf{V}(\mathbf{I}(X))$ es un conjunto cerrado así que $\overline{X} \subseteq \mathbf{V}(\mathbf{I}(X))$. Además sea $F \supseteq X$ cerrado, entonces $\mathbf{I}(F) \subseteq \mathbf{I}(X)$. Como F es cerrado, entonces $F = \mathbf{V}(\mathfrak{a})$ para algún ideal \mathfrak{a} ; es decir, $\mathbf{I}(\mathbf{V}(\mathfrak{a})) \subseteq \mathbf{I}(X)$, pero por el inciso 1 se tiene que $\mathfrak{a} \subseteq \mathbf{I}(X)$, luego $F = \mathbf{V}(\mathfrak{a}) \supseteq \mathbf{V}(\mathbf{I}(X))$. En consecuencia, $\mathbf{V}(\mathbf{I}(X))$ es el mínimo cerrado que contiene a X , osea, $\mathbf{V}(\mathbf{I}(X)) = \overline{X}$. \square

Corolario 14.13: Se cumple que

$$\{X \subseteq \mathbb{A}^n : X \text{ algebraico}\} \xleftrightarrow[\mathbf{V}]{\mathbf{I}} \{\mathfrak{a} \subseteq A : \mathfrak{a} \text{ ideal radical}\}$$

son biyecciones y son la inversa la una de la otra.

Definición 14.14: Un espacio topológico X se dice *reducible* si existen $F_1, F_2 \subset X$ cerrados tales que $F_1 \cup F_2 = X$, de lo contrario se dice *irreducible*. Un subconjunto $Y \subseteq X$ no vacío es irreducible si lo es como subespacio.

Teorema 14.15: En un espacio topológico X son equivalentes:

1. X es irreducible.
2. Si U_1, U_2 son abiertos no vacíos, entonces $U_1 \cap U_2 \neq \emptyset$.

3. Todo abierto no vacío es denso en X .

En consecuencia, todo espacio topológico irreducible **no** es de Hausdorff.

DEMOSTRACIÓN: Para el último inciso basta notar que si U es abierto, entonces $\overline{U} \cup U^c = X$, donde \overline{U}, U^c son cerrados. \square

Lema 14.16: Sea $Y \subseteq X$ es no vacío, entonces Y es irreducible si y sólo si su clausura, \overline{Y} , lo es.

DEMOSTRACIÓN: Si Y es irreducible, queremos ver que \overline{Y} también lo es. Dados dos abiertos no vacíos $U_1 \cap \overline{Y}, U_2 \cap \overline{Y}$ en \overline{Y} se cumple que

$$\emptyset \neq U_1 \cap U_2 \cap Y \subseteq U_1 \cap U_2 \cap \overline{Y},$$

lo que demuestra que \overline{Y} es \square

Definición 14.17: Una *componente irreducible* es un subconjunto irreducible \subseteq -maximal.

Teorema 14.18: Se cumplen:

1. Las componentes irreducibles son cerradas.
2. Todo conjunto irreducible está contenido en una componente irreducible.
3. Todo espacio topológico es la unión de sus componentes irreducibles.

Definición 14.19: Se dice que un espacio topológico X es *noetheriano* si para toda sucesión $(F_n)_{n \in \mathbb{N}}$ de cerrados tal que

$$F_1 \supseteq F_2 \supseteq F_3 \supseteq \dots$$

se cumple que existe un n tal que para todo $m > n$ se da que $F_m = F_n$.

Proposición 14.20: En un espacio noetheriano todo cerrado se escribe de forma única como unión de finitos irreducibles.

DEMOSTRACIÓN: Ésto implica demostrar dos cosas:

- i) Todo cerrado se escribe como unión de finitos irreducibles: Sea I la familia de cerrados que no admiten dicha escritura. Como X es noetheriano, entonces si I fuese no vacío contendría un cerrado F que sea \subseteq -minimal. Luego F no puede ser irreducible, por ende $F = F_1 \cup F_2$, donde F_1, F_2 son subconjuntos propios cerrados. Como $F_1, F_2 \notin I$ (por minimalidad de F), entonces F_1, F_2 se escriben como finitos irreducibles y en consecuencia F también.
- ii) Dicha escritura es única: Supongamos que $F = F_1 \cup \dots \cup F_n$, donde los F_i 's son irreducibles distintos. Si $F = F'_1 \cup \dots \cup F'_m$, entonces $F'_j \subseteq F_1 \cup \dots \cup F_n$ y luego

$$F'_j = \bigcup_{i=1}^n (F_i \cap F'_j),$$

pero cada $F_i \cap F'_j$ es cerrado, así que o es vacío o es el espacio; y no pueden ser todos vacíos, así que $F_i \cap F'_j = F'_j$ para algún i , y por irreductibilidad, $F_i = F'_j$. Así se procede por inducción. \square

Definición 14.21 – Variedad afín: Se dice que $V \subseteq \mathbb{A}^n$ es una *variedad afín* si es un conjunto algebraico afín irreducible en la topología de Zariski.

Corolario 14.22: Un espacio afín con la topología de Zariski es un espacio noetheriano. Por ende, todo conjunto algebraico se escribe de forma única como unión finita de variedades afines.

DEMOSTRACIÓN: Sea $(F_n)_{n \in \mathbb{N}}$ una sucesión \subseteq -descendiente de cerrados en \mathbb{A}^n . Luego $F_i = \mathbf{V}(I_i)$ para un único ideal radical I_i . Si $F_i \supseteq F_{i+1}$, entonces $I_i \subseteq I_{i+1}$, es decir, a la cadena de cerrados le corresponde una cadena ascendente de ideales en A que es un anillo noetheriano por el teorema de bases de Hilbert. \square

Teorema 14.23: Para todo cerrado $F \subseteq \mathbb{A}^n$ se cumple que:

1. F es variedad afín syss $\mathbf{I}(F)$ es un ideal primo.
2. F es singular syss $\mathbf{I}(F)$ es un ideal maximal.

Proposición 14.24: Si k es infinito, entonces \mathbb{A}^n es una variedad afín. En consecuencia, \mathbb{A}^n es un espacio topológico que es T_1 , pero no es de Hausdorff.

Ejemplo. Sea $k = \mathbb{C}$, entonces nótese que $V_{\mathbb{C}}(y^2 - x(x^2 - 1))$ es una variedad afín, puesto que el polinomio $y^2 - x(x^2 - 1)$ es irreducible en $\mathbb{C}[x, y]$. Lo interesante es que su gráfico (fig. 14.1) parece sugerir que la figura se forme a partir de dos conjuntos algebraicos más pequeños cuando no es el caso. Por ello, pese a que se llama «geometría algebraica» no se recomienda confiar en los diagramas.

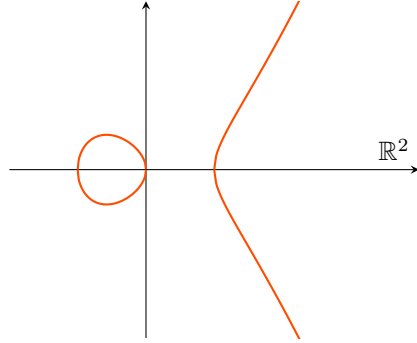


Figura 14.1

14.2 Variedades proyectivas

Lema 14.25: En $k^{n+1} \setminus \{\vec{0}\}$, la relación:

$$\mathbf{u} \sim \mathbf{v} \iff \exists \lambda \in k \ \mathbf{u} = \lambda \mathbf{v}$$

es de equivalencia.

Definición 14.26: Se define el *espacio proyectivo* $\mathbb{P}^n := (k^{n+1} \setminus \{\vec{0}\})/\sim$. Cuyos elementos se denotan por

$$[a_0 : a_1 : \dots : a_n] := [(a_0, a_1, \dots, a_n)]_{\sim}.$$

(Ésta notación debe entenderse como que la tupla es una «proporción», de ahí los «:».)

Para $0 \leq j \leq n$ se denota:

$$U_j := \{[a_0 : a_1 : \dots : a_n] \in \mathbb{P}^n : a_j \neq 0\}.$$

A éstos conjuntos les llamaremos *cartas afines* de \mathbb{P}^n .

A uno le gustaría poder tener, al igual que con el espacio afín, una noción de «lugar de ceros» para el espacio proyectivo, sin embargo, como sus elementos son clases de equivalencia y no simplemente puntos, la cuestión es más difícil, para lo cual hay que introducir el siguiente concepto:

Definición 14.27: Un polinomio $p \in k[x_0, \dots, x_n]$ se dice *homogéneo* si todos sus monomios son de igual grado.

Proposición 14.28: Si $p \in k[x_0, \dots, x_n]$ es homogéneo, entonces para todo $\mathbf{x} \in k^{n+1}$ y todo $\lambda \in k$ se cumple que

$$p(\lambda \mathbf{x}) = \lambda^d p(\mathbf{x}),$$

donde $d = \deg p$. En consecuencia, la expresión « $f(\mathbf{u}) = 0$ » para $\mathbf{u} \in \mathbb{P}^n$ está bien definida.

Definición 14.29: Sean $T \subseteq k[x_0, \dots, x_n]$ un conjunto de polinomios homogéneos, entonces se define

$$\mathbf{V}(T) := \{\mathbf{a} \in \mathbb{P}^n : \forall f \in T \ f(\mathbf{a}) = 0\}.$$

Los conjuntos de ésta forma son llamados *algebraicos proyectivos*. Así mismo, dado $Z \subseteq \mathcal{P}^n$ se define

$$\mathbf{I}(Z) := (\{f \in k[x_0, \dots, x_n] \text{ homogéneo} : \forall \mathbf{p} \in Z \ f(\mathbf{p}) = 0\}).$$

Y ahora varios de los resultados de los conjuntos algebraicos afines aplican también con demostraciones análogas:

Teorema 14.30: Los conjuntos algebraicos proyectivos forman los cerrados de una única topología en \mathbb{P}^n .

Definición 14.31: Dicha topología, es llamada la *topología de Zariski* sobre \mathbb{P}^n .

Corolario 14.32: Las cartas afines forman un cubrimiento abierto de \mathbb{P}^n (con la topología de Zariski).

Además, los conjuntos algebraicos proyectivos y los ideales homogéneos forman *casi* la misma correspondencia que en el espacio afín, con una excepción:

Ejemplo 9 (ideal irrelevante): Sea $\mathfrak{a} := (x_0, x_1, \dots, x_n) \leq k[x_0, \dots, x_n]$. Por definición es un ideal y es homogéneo por ser generado por homogéneos. Sin embargo, nótese que $\mathbf{V}(\mathfrak{a}) = \emptyset$, puesto que para que un punto se anule en \mathfrak{a} debe darse que $x_0 = 0$, $x_1 = 0$, y así hasta $x_n = 0$; no obstante, $[0 : 0 : \dots : 0] \notin \mathbb{P}^n$. A \mathfrak{a} le decimos el *ideal irrelevante*. Nótese que el ideal irrelevante es de hecho un ideal primo, así que $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = (1) \neq \mathfrak{a} = \text{Rad}(\mathfrak{a})$.

Y otro caso del teorema de ceros de Hilbert para el espacio proyectivo:

Teorema 14.33: Sea $\mathfrak{a} \leq k[x_0, \dots, x_n]$ un ideal homogéneo no irrelevante. Entonces $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \text{Rad}(\mathfrak{a})$.

Y como corolarios:

Corolario 14.34: Se cumple que:

1. Si $T \subseteq k[x_0, \dots, x_n]$ está formado por homogéneos, entonces $T \subseteq \mathbf{I}(\mathbf{V}(T))$. Así mismo, si $X \subseteq \mathbb{P}^n$, entonces $X \subseteq \mathbf{V}(\mathbf{I}(X))$.
2. Si $X \subseteq Y \subseteq \mathbb{P}^n$, entonces $\mathbf{I}(X) \supseteq \mathbf{I}(Y)$.
3. Sea $X \subseteq \mathbb{P}^n$, entonces $\mathbf{V}(\mathbf{I}(X)) = \overline{X}$.
4. Las aplicaciones \mathbf{I}, \mathbf{V} forman biyecciones entre los conjuntos algebraicos proyectivos de \mathbb{P}^n y los ideales radicales homogéneos no irrelevantes de $k[x_0, \dots, x_n]$.

Definición 14.35: Admitimos las siguientes funciones:

$$\begin{aligned} \phi: \mathbb{A}^n &\longrightarrow U_0 \\ (x_1, \dots, x_n) &\longmapsto [1 : x_1 : \dots : x_n] \\ \alpha: k[x_0, \dots, x_n] &\longrightarrow k[x_1, \dots, x_n] & \beta: k[x_1, \dots, x_n] &\longrightarrow k[x_0, \dots, x_n] \\ p(x_0, x_1, \dots, x_n) &\longmapsto p(1, x_1, \dots, x_n) & q(x_1, \dots, x_n) &\longmapsto x_0^{\deg q} q\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \end{aligned}$$

ϕ es una biyección, el resto no.

Proposición 14.36: Algunas propiedades:

1. ϕ es una biyección.
2. $\beta \circ \alpha = \text{Id}$.

3. Si $p \in k[x_0, \dots, x_n]$ es homogéneo, entonces $p = x_0^r \beta(\alpha(p))$ para algún $r \geq 0$.

En particular, con respecto a la propiedad 3, obsérvese que

$$(\alpha \circ \beta)(x_0 x_1 + x_0^2) = \beta(x_1 + 1) = x_1 + x_0.$$

Lema 14.37: Sea $Z := \mathbf{V}_{\mathbb{P}^n}(T)$, donde T son polinomios homogéneos. Entonces $\phi^{-1}[Z \cap U_0] = \mathbf{V}_{\mathbb{A}^n}(\alpha[T])$.

DEMOSTRACIÓN: Sea $[1 : x_1 : \dots : x_n] \in Z \cap U_0$. Por definición, para todo $f \in T$ se cumple que $\alpha(f)(x_1, \dots, x_n) = f(1, x_1, \dots, x_n) = 0$. Por lo que $(x_1, \dots, x_n) \in \mathbf{V}_{\mathbb{A}^n}(\alpha[T])$.

La demostración es análoga. \square

Definición 14.38: Definamos $\pi: \mathbb{A}^{n+1} \setminus \{\vec{0}\} \rightarrow \mathbb{P}^n$ la proyección canónica (puesto que es un conjunto cociente). Además si Z es un conjunto algebraico proyectivo, definimos

$$C_{\text{af}}(Z) := \pi^{-1}[Z] \cup \{\vec{0}\}.$$

Lema 14.39: Si $T \subseteq k[x_0, \dots, x_n]$ está formado por homogéneos, entonces $C_{\text{af}}(\mathbf{V}_{\mathbb{P}^n}(T)) = \mathbf{V}_{\mathbb{A}^{n+1}}(T)$.

Definición 14.40: Sea $Z \subseteq \mathbb{A}^n$ un conjunto algebraico afín, entonces

$$\overline{Z}_{\text{proy}} := \overline{\phi[Z]} \subseteq \mathbb{P}^n.$$

(Nótese que Z ya es \mathbb{A}^n -cerrado, por lo que la notación no debería confundir.)

Teorema 14.41: Sea $Z \subseteq \mathbb{A}^n$ algebraico afín y sea $\mathfrak{a} := \mathbf{I}_{\mathbb{A}^n}(Z)$. Entonces

$$\overline{Z}_{\text{proy}} = \mathbf{V}_{\mathbb{P}^n}(\beta[\mathfrak{a}]), \quad \overline{Z}_{\text{proy}} \cap U_0 = \phi[Z].$$

DEMOSTRACIÓN: Sea $Z' := \mathbf{V}_{\mathbb{P}^n}(\beta[\mathfrak{a}])$, probaremos el enunciado por doble contención. Como $\overline{Z}_{\text{proy}}$ es el menor cerrado que contiene a $\phi[Z]$ y Z' es cerrado, basta notar que para todo $[1 : a_1 : \dots : a_n] \in \phi[Z]$ se cumple que para todo $f \in \mathfrak{a}$ se satisface

$$\beta(f)(1, a_1, \dots, a_n) = 1^r f\left(\frac{a_1}{1}, \dots, \frac{a_n}{1}\right) = f(a_1, \dots, a_n) = 0.$$

De modo que $\overline{Z}_{\text{proy}} \subseteq Z'$.

Notese que probar que $\overline{Z}_{\text{proy}} \supseteq Z'$ equivale a ver que $\mathbf{I}_{\mathbb{P}^n}(\overline{Z}_{\text{proy}}) \subseteq \mathbf{I}_{\mathbb{P}^n}(Z')$. Ésto es un caso particular de ver que si $\phi[Z] \subseteq W$ cerrado, entonces $\mathbf{I}_{\mathbb{P}^n}(W) \subseteq \mathbf{I}_{\mathbb{P}^n}(Z')$. Si $f \in \mathbf{I}_{\mathbb{P}^n}(W)$ es homogéneo, entonces f se anula en W , luego $\alpha(f)$ se anula en $W \cap U_0 \supseteq \phi[Z]$. Por ende $\alpha(f) \in \mathbf{I}_{\mathbb{A}^n}(Z) = \mathfrak{a}$ y $\beta(\alpha(f)) \in \beta[\mathfrak{a}]$. Es decir,

$$(\alpha \circ \beta)(f) \in \mathbf{I}_{\mathbb{P}^n}(\mathbf{V}_{\mathbb{P}^n}(\beta[\mathfrak{a}])) = \mathbf{I}_{\mathbb{P}^n}(Z').$$

Pero como $f = x_0^r(\alpha \circ \beta)(f)$ para algún r , se ha de cumplir que $f \in \mathbf{I}_{\mathbb{P}^n}(Z')$ como se quería probar.

Para la segunda afirmación claramente $\phi[Z] \subseteq \overline{Z}_{\text{proy}} \cap U_0$. Y si $\mathbf{p} := [1 : p_1 : \dots : p_n] \in \overline{Z}_{\text{proy}} \cap U_0$, entonces $f(\mathbf{p}) = 0$ para todo $\beta(f) \in \beta[\mathfrak{a}]$, luego

$$0 = \beta(f)(1, p_1, \dots, p_n) = [(\beta \circ \alpha)(f)](p_1, \dots, p_n) = f(p_1, \dots, p_n)$$

es decir, $(p_1, \dots, p_n) \in Z$ como se quería probar. \square

Corolario 14.42: $\phi: \mathbb{A}^n \rightarrow U_0$ es un homeomorfismo.

Definición 14.43: Se dice que $V \subseteq \mathbb{P}^n$ es una *variedad proyectiva* si es un conjunto algebraico proyectivo irreducible. Si $U \subseteq V$ es un abierto no vacío de una variedad proyectiva, entonces a U se le dice una *variedad cuasi-proyectiva*.

Bajo ésta definición, \mathbb{A}^n se identifica con una variedad cuasi-proyectiva.

Teorema 14.44: Un cerrado $F \subseteq \mathbb{P}^n$ es una variedad proyectiva syss $\mathbf{I}(F)$ es un ideal primo homogéneo no irrelevante.

Teorema 14.45: Identificando \mathbb{A}^n con U_0 por medio de ϕ se cumplen:

1. Si $V \subseteq \mathbb{P}^n$ es una variedad proyectiva que se corta con U_0 , entonces $V \cap U_0$ es una variedad afín.
2. Si $W \subseteq \mathbb{A}^n$ es una variedad afín, entonces $\overline{W}_{\text{proy}} \subseteq \mathbb{P}^n$ es una variedad proyectiva.

DEMOSTRACIÓN:

1. $V \cap U_0$ es un abierto en V , luego es denso e irreducible como subespacio, pero ϕ es homeomorfismo.

2. Basta ver que $\mathfrak{a} := \mathbf{I}_{\mathbb{P}^n}(\overline{W}_{\text{proy}})$ es primo y no irrelevante. Como $\emptyset \neq W \subseteq \overline{W}_{\text{proy}}$, entonces su ideal no es irrelevante. Así pues, falta ver que es primo: Sean $f, g \in k[x_0, \dots, x_n]$ homogéneos con $f \cdot g \in \mathfrak{a}$. Luego

$$\alpha(f)\alpha(g) = \alpha(fg) \in \alpha[\mathfrak{a}] = \mathbf{I}_{\mathbb{A}^n}(W)$$

pero $\mathbf{I}_{\mathbb{A}^n}(W)$ es primo, luego, sin pérdida de generalidad, supongamos que $\alpha(f) \in \mathbf{I}_{\mathbb{A}^n}(W)$. Luego $\beta(\alpha(f)) \in \mathfrak{a}$ y $f = x_0^r \cdot \beta(\alpha(f)) \in \mathfrak{a}$. Por ende, \mathfrak{a} es primo y $\overline{W}_{\text{proy}}$ es variedad proyectiva. \square

14.3 Funciones polinómicas y regulares

Definición 14.46: Sea $X \subseteq \mathbb{A}^n$ un conjunto cerrado. Se denota por

$$k[X] := \{f: X \rightarrow \mathbb{A}^1 : f \text{ es polinómica}\}.$$

Claramente $k[X]$ es una subálgebra de $\text{Func}(X; \mathbb{A}^1)$. A $k[X]$ le llamamos el *anillo de coordenadas afines* de X .

Claramente existe un k -homomorfismo desde $r: k[\mathbb{A}^n] \rightarrow k[X]$ dado por la restricción. Nótese que $f \in \ker r$ syss $f(\mathbf{p}) = 0$ para todo $\mathbf{p} \in X$, lo que sucede syss $f \in \mathbf{I}(X)$. Luego

$$k[X] \cong \frac{k[\mathbb{A}^n]}{\mathbf{I}(X)}.$$

(Algunos libros definen $k[X]$ de ésta forma.)

Definición 14.47: Sea X una variedad cuasi-afín. Una aplicación $\phi: X \rightarrow k$ se dice *regular* en $\mathbf{p} \in X$ si existe un entorno abierto U de \mathbf{p} , y existen $f, g \in k[U]$ tales que g no se anula en U y $\phi|_U = f/g$.

Análogamente sea Y una variedad cuasi-proyectiva. Una aplicación $\phi: Y \rightarrow k$ se dice *regular* en $\mathbf{p} \in Y$ si existe un entorno abierto U de \mathbf{p} , y existen $f, g \in k[U]$ homogéneos del mismo grado tales que g no se anula en U y $\phi|_U = f/g$.

En ambos casos se dice que una función es *regular* (a secas) si lo es en todos los puntos de su dominio. Se denota por $\mathcal{O}(X)$ al conjunto de funciones regulares desde X a k .

Podría resumirse la definición en que una función regular es una función «localmente racional».

Proposición 14.48: $\mathcal{O}(X)$ es un k -álgebra en un sentido canónico.

Proposición 14.49: Para todo $\phi \in \mathcal{O}(X)$, viéndolo como aplicación $\phi: X \rightarrow \mathbb{A}^1$, se cumple que ϕ es continua.

DEMOSTRACIÓN: Asumamos que $X \subseteq \mathbb{A}^n$. Veremos que la preimagen de cerrados es cerrada. Nótese que los cerrados de \mathbb{A}^1 son conjuntos finitos, así que basta ver que para todo $a \in \mathbb{A}^1$ se cumpla que $\phi^{-1}[\{a\}]$ sea cerrado. Más aún, como X es variedad, se puede cubrir por finitos abiertos U tales que $\phi|_U = f/g$ con $f, g \in k[\mathbb{A}^n]$ de modo que $\phi^{-1}[\{a\}] \cap U = \mathbf{V}(f - ag)$ que es cerrado. En consecuencia, $\phi^{-1}[\{a\}]$ es la unión de finitos cerrados.

El caso $X \subseteq \mathbb{P}^n$ es análogo, empleando f, g homogéneos. \square

Definición 14.50: Sean X, Y variedades y sea $\varphi: X \rightarrow Y$. Entonces φ es un *morfismo* si:

1. φ es continua.
2. Para todo $U \subseteq Y$ abierto no vacío y todo $\phi \in \mathcal{O}(U)$ se cumple que $\phi \circ \varphi: \varphi^{-1}[U] \rightarrow k$ es regular.

Proposición 14.51: Sea X una variedad, y sean $U, V \subseteq X$ abiertos no vacíos. Si $\phi \in \mathcal{O}(U), \psi \in \mathcal{O}(V)$ son tales que $\phi|_{U \cap V} = \psi|_{U \cap V}$, entonces existe $\theta \in \mathcal{O}(U \cup V)$ tal que $\theta|_U = \phi$ y $\theta|_V = \psi$.

Lema 14.52: Sean X, Y variedades, y sea $f: X \rightarrow Y$ continua. Entonces f es un morfismo si y sólo si para todo $p \in Y$, existe un entorno abierto $U \subseteq Y$ de p tal que para todo $\psi \in \mathcal{O}(U)$ se cumple que $(f \circ \psi) \in \mathcal{O}(f^{-1}[U])$.

DEMOSTRACIÓN: \implies . Trivial.

\impliedby . Denotemos por U_p a un entorno como en el enunciado. Sea $V \subseteq Y$ un abierto no vacío y sea $\psi \in \mathcal{O}(V)$, queremos probar que $f \circ \psi \in \mathcal{O}(f^{-1}[V])$. Sea $q \in f^{-1}[V]$, por el enunciado, $q \in f^{-1}[V] \cap f^{-1}[U_q]$; luego, se cumple que existe $V_q \subseteq f^{-1}[V] \cap f^{-1}[U_q]$ tal que $f \circ \psi|_{V_q} = g/h$ con $g, h \in k[\mathbb{A}^n]$; es decir, $f \circ \psi$ es regular como se quería probar. \square

Corolario 14.53: Toda función regular, vista como función $f: X \rightarrow \mathbb{A}^1$, es un morfismo.

Proposición 14.54: Sea X una variedad. Entonces:

1. $\text{Id}_X: X \rightarrow X$ es un morfismo.
2. La composición de morfismos es un morfismo.

En consecuencia, las variedades (como objetos) y los morfismos (como flechas) constituyen una categoría, denotada \mathbf{Var} .

Proposición 14.55: Sea $f: X \rightarrow Y$ un morfismo de variedades, entonces la pre-composición:

$$\begin{aligned} h_f: \mathcal{O}(Y) &\longrightarrow \mathcal{O}(X) \\ \phi &\longmapsto f^* \circ \phi \end{aligned}$$

es un morfismo de k -álgebras. Luego se tiene el siguiente funtor contravariante desde \mathbf{Var} a \mathbf{Alg}_k :

$$\begin{array}{ccc} X & & \mathcal{O}(X) \\ f \downarrow & \xRightarrow{h_-} & \uparrow h_f \\ Y & & \mathcal{O}(Y) \end{array}$$

En consecuencia, si X e Y son variedades isomorfas, entonces sus anillos de coordenadas regulares son isomorfos.

En paralelo al concepto de «gérmenes de funciones diferenciables», que son clases de equivalencia definidas localmente en un punto, podemos establecer el concepto de «gérmenes de funciones regulares».

Lema 14.56: Sea X una variedad y $p \in X$ un punto. Definamos $C := \bigcup_{p \in U} \{U\} \times \mathcal{O}(U)$, donde U recorre todos los abiertos en X que contienen al punto. Entonces sea \sim la relación sobre C dada por:

$$(U, \phi) \sim (V, \psi) \iff \phi|_{U \cap V} = \psi|_{U \cap V},$$

es una relación de equivalencia. Más aún, si $(U, \phi) \sim (V, \psi)$ y $(W, \theta) \in C$, entonces:

1. $(U \cap W, \phi + \theta) \sim (V \cap W, \psi + \theta)$.
2. $(U \cap W, \phi \cdot \theta) \sim (V \cap W, \psi \cdot \theta)$.
3. $(U, \lambda \phi) \sim (V, \lambda \psi)$ para todo $\lambda \in k$.

Definición 14.57: Sea X una variedad y $p \in X$, entonces se define el anillo local $\mathcal{O}_{p,X}$ como el conjunto cociente dado por el lema anterior. Se denota $\langle U, \phi \rangle := [(U, \phi)]_{\sim}$.

Proposición 14.58: $\mathcal{O}_{p,X}$ es un anillo local, cuyo único ideal maximal es

$$\mathfrak{m}_{p,X} := \{\langle U, \phi \rangle : \phi(p) \neq 0\}.$$

Proposición 14.59: Considerando a \mathcal{D} como la categoría conformada por los entornos abiertos de p con las flechas dadas por las inclusiones; entonces el siguiente es un funtor contravariante desde \mathcal{D} a \mathbf{Alg}_k :

$$\begin{array}{ccc} r: \mathcal{O}(V) & \longrightarrow & \mathcal{O}(U) \\ \phi \longmapsto \phi|_U & & \end{array} \quad \begin{array}{ccc} U & & \mathcal{O}(U) \\ \downarrow \subseteq & \xrightarrow{F} & \uparrow r \\ V & & \mathcal{O}(V) \end{array}$$

Y se cumple que $\mathcal{O}_{p,X} = \varinjlim_{U \in \mathcal{D}} \mathcal{O}(U)$.

DEMOSTRACIÓN: Sea A un co-cono del diagrama, vale decir, $(\varphi_U: \mathcal{O}(U) \rightarrow A)_{U \in \mathcal{D}}$, entonces el morfismo deseado es el siguiente:

$$\begin{aligned} \phi: \mathcal{O}_{p,X} &\longrightarrow A \\ \langle U, f \rangle &\longmapsto \varphi_U(f) \end{aligned}$$

ϕ está bien definido, y es único, por la conmutatividad del siguiente diagrama:

$$\begin{array}{ccccc} \mathcal{O}(U) & & \xrightarrow{\varphi_U} & & A \\ & \searrow \langle U, - \rangle & & \nearrow \phi & \\ & \mathcal{O}_{p,X} & & & \\ & \nearrow \langle V, - \rangle & & \nwarrow \varphi_V & \\ \mathcal{O}(V) & & \xrightarrow{\varphi_V} & & A \end{array}$$

Y queda al lector comprobar que es un morfismo de k -álgebras. \square

Corolario 14.60: Sea X una variedad, $p \in X$, y U un entorno abierto de p . Entonces $\mathcal{O}_{p,X} = \mathcal{O}_{p,U}$.

Proposición 14.61: Se tiene el siguiente funtor contravariante:

$$\begin{array}{ccc}
h_f: \mathcal{O}_{q,Y} \longrightarrow \mathcal{O}_{p,X} & & \begin{array}{ccc} (X, p) & & \mathcal{O}_{p,X} \\ f \downarrow & \xRightarrow{\quad} & \uparrow h_f \\ (Y, q) & & \mathcal{O}_{q,Y} \end{array} \\
\langle \phi, U \rangle \longmapsto \langle f \circ \phi, f^{-1}[U] \rangle & &
\end{array}$$

En particular, si f es un isomorfismo, entonces $\mathcal{O}_{p,X}$ y $\mathcal{O}_{q,Y}$ son anillos isomorfos.

14.4 Dimensión

Definición 14.62: Dado un espacio topológico X no vacío, se define su *dimensión de Noether* $d := n\text{-dim } X \geq 0$ como el natural máximo tal que existe una cadena

$$\emptyset \neq X_0 \subset X_1 \subset \cdots \subset X_d$$

de cerrados irreducibles en X .

Ejemplo. Se cumple que $n\text{-dim}\{\mathbf{p}\} = 0$ y $n\text{-dim } \mathbb{A}^1 = 1$. En efecto, ya que sabemos que todo cerrado irreducible de \mathbb{A}^1 es una variedad, y las variedades sólo son los puntos y \mathbb{A}^1 mismo.

Índice de notación

\vee, \wedge	Disyuntor, “o lógico” y conjuntor, “y lógico” respectivamente.
\implies	Implica, entonces.
\iff	Si y sólo si.
\forall, \exists	Para todo, existe respectivamente.
\in	Pertenencia.
\subseteq, \subset	Subconjunto, subconjunto propio resp.
\cup, \cap	Unión e intersección binaria respectivamente.
$A \setminus B$	Resta conjuntista, A menos B .
A^c	Complemento de A (respecto a un universo relativo).
$A \times B$	Producto cartesiano de A por B .
$A_{\neq x}$	Abreviación de $A \setminus \{x\}$.
$f : A \rightarrow B$	Función f de dominio A y codominio B .
$f \circ g$	Composición de f con g . $(f \circ g)(x) = g(f(x))$.
$\mathcal{P}(A)$	Conjunto potencia de A .
resp.	Respectivamente.

syss	Si y sólo si.
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$	Conjuntos de números naturales, enteros y racionales resp.
\aleph_0	Cardinal numerable, cardinalidad de \mathbb{N} .
AE	Axioma de elección.
DE, AEN	Axioma de elecciones dependientes, y de elecciones numerables resp.
ZF(C)	Teoría de Zermelo-Fraenkel. La C representa el axioma de elección.
a^{-1}	Inversa de un elemento invertible en un grupo, p. 4.
$S \leq G$	S es subgrupo (anillo o espacio) de G , p. 6.
$\langle S \rangle$	Subgrupo, cuerpo o espacio generado por S , p. 6.
$\text{ord } x$	Orden de un elemento x , p. 7.
$G \cong H$	G y H son estructuras isomorfas, p. 9.
\mathbb{Z}_n^\times	Grupo multiplicativo o de las unidades de n , aquél formado por los coprimos de n , p. 11.
$\phi(n)$	Función indicatriz de Euler de n , esto es, la cantidad de coprimos positivos menores a n , p. 11.
S_n	Grupo simétrico sobre $\{1, 2, \dots, n\}$, p. 13.
$\text{sgn } \sigma$	Signo de la permutación σ , p. 15.
A_n	Grupo alternante en S_n , p. 16.
D_{2n}	Grupo diedral de cardinal $2n$, p. 17.
$N \trianglelefteq G$	N es subgrupo de G , p. 18.
$Z(S), Z(G)$	Centralizador de S , centro de G resp., p. 18.
$N_G(S)$	Normalizador de S , p. 19.
$C_G(S)$	Clase de conjugación de S , p. 19.
K_4	Grupo de Klein de 4 elementos, $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, p. 26.

$N \rtimes_{\alpha} A$	Producto semidirecto de N con A , donde A actúa sobre N , p. 28.
Orb_a	Órbita de a , osea, los $\alpha_g(a)$ para todo $g \in G$, p. 29.
Stab_a	Estabilizador de a , osea, los $g \in G$ que dejan a a fijo, p. 29.
$\text{Fix}_g(S)$	Puntos fijos de la acción α_g sobre S , p. 32.
$\text{Fix}_G(S)$	Puntos fijos de todas las acciones sobre S , p. 32.
$\text{Syl}_p(G)$	El conjunto de p -subgrupos de Sylow de G , p. 33.
A^{\times}	El conjunto de elementos invertibles de un anillo unitario A , p. 50.
\mathbb{k}	Un cuerpo general, p. 51.
$\text{Frac}(A)$	Cuerpo de fracciones de un dominio íntegro A , p. 67.
$A[S]$	Conjunto de polinomios con coeficientes en A y con indeterminadas de S , p. 69.
$\deg f$	Grado del polinomio f , p. 69.
$\text{ev}_{\alpha_1, \dots, \alpha_n}$	Homomorfismo de evaluación de un anillo de polinomios $A[x_1, \dots, x_n]$ sustituyendo $x_i = \alpha_i$, p. 72.
$c(f)$	Contenido del polinomio f , p. 78.
\mathbb{C}	Conjunto de números complejos, p. 84.
$\text{Re } z, \text{Im } z$	Parte real e imaginaria de z resp., p. 84.
ζ_n	$= \text{cis}(2\pi/n)$, raíz primitiva canónica n -ésima de la unidad, p. 86.
$\text{Hom}_A(M, N)$	Espacio de morfismos de A -módulos desde M a N , p. 90.
$\det B$	Determinante de la matriz B , p. 107.
$\text{adj } B$	Matriz adjunta de B , p. 108.
$\text{tr } B$	$= \sum_{k=1}^n b_{kk}$, traza de una matriz, p. 111.
$\psi_B(x)$	$= \det(x \cdot I_n - B)$, polinomio característico de una matriz, p. 111.

$\text{rank}(A)$	Rango de una matriz o de una transformación lineal, p. 113.
$[K : k]$	Grado de la extensión K de k . Su dimensión como k -espacio vectorial, p. 117.
$\text{Gal}(K/k)$	El conjunto de los k -automorfismos de K , donde K/k es una extensión de cuerpos, p. 125.
\bar{k}	La clausura algebraica de k , p. 144.
$\text{Tr}_{K/k}(\alpha)$	$= \text{tr}(m_\alpha)$, traza de $\alpha \in K$, p. 145.
$\text{Nm}_{K/k}(\alpha)$	$= \det(m_\alpha)$, norma de $\alpha \in K$, p. 145.
$\psi_{\alpha, K/k}(t)$	$= \psi_{m_\alpha}(t) \in k[t]$, polinomio característico de $\alpha \in K$, p. 145.
$\chi(V_\bullet)$	$= \sum_{i=0}^N (-1)^i \dim(V_i)$. Característica de Euler de un complejo corto de cadenas V_\bullet , p. 192.
$A_{\mathfrak{p}}$	Localización del anillo A en su ideal primo \mathfrak{p} , p. 198.
$(S : T)$	$= \{a \in A : aT \subseteq S\}$, donde S, T son submódulos de un A -módulo M , p. 204.
$\text{Ann}(T)$	$= (0 : T)$, p. 204.
\mathfrak{a}^e	$= (\varphi[\mathfrak{a}])$, la extensión del ideal \mathfrak{a} , p. 205.
\mathfrak{b}^c	$= \varphi^{-1}[\mathfrak{b}]$, la contracción del ideal \mathfrak{b} , p. 205.
$\text{As } \mathfrak{a}$	El conjunto de los ideales asociados a \mathfrak{a} , p. 213.
$k\text{-dim } A$	Dimensión de Krull de un anillo A , p. 221.
$\psi_A(x)$	$= \det(xI_n - A)$, el polinomio característico de A , p. 232.
$p_f(x), p_B(x)$	Polinomio característico de un endomorfismo o una matriz, p. 236.
$\sigma(f)$	Espectro de un endomorfismo lineal, o de una matriz cuadrada, p. 236.
B^*	$= \overline{B}^t$, p. 240.
$x \perp y$	x e y son ortogonales, p. 251.
A^\perp	Complemento ortogonal de A , p. 251.

$\text{Obj } \mathcal{C}, \text{Mor } \mathcal{C}$	Objetos, morfismos de la categoría \mathcal{C} , resp., p. 257.
$\text{Hom}_{\mathcal{C}}(A, B)$	Morfismos de \mathcal{C} con dominio en A y codominio en B , p. 257.
$\text{End}_{\mathcal{C}}(A)$	Endomorfismos de \mathcal{C} sobre A , p. 257.
$Z_n(K_{\bullet})$	$= \ker(\partial_n: K_n \rightarrow K_{n-1})$, el conjunto de n -ciclos de K_{\bullet} , p. 266.
$Z_n(K_{\bullet})$	$= \text{Img}(\partial_{n+1}: K_{n+1} \rightarrow K_n)$, el conjunto de n -fronteras de K_{\bullet} , p. 266.
$H_n(K)$	$= Z_n/B_n$, la homología n -dimensional de K_{\bullet} , p. 266.
$\text{Ch}(\mathcal{C})$	La categoría de cadenas de complejos sobre una categoría abeliana \mathcal{C} , usualmente Mod_R , p. 267.
$s: f \simeq g$	f, g son homotópicas bajo s , p. 267.
$E \equiv E'$	Dos extensiones son congruentes, i.e., existe un morfismo de la forma $(\text{Id}_A, \beta, \text{Id}_C)$ entre ellos, p. 275.
$A[[S]]$	Anillo de series formales de potencias con coeficientes en A e indeterminadas en S , p. 306.
$\text{ord } f$	$= \min\{m : a_m \neq 0\}$, orden de una serie formal de potencias, p. 306.
$\text{gr}_{\mathfrak{a}}(A)$	$= \bigoplus_{n \in \mathbb{N}} \mathfrak{a}^n / \mathfrak{a}^{n+1}$, p. 320.
$G(M)$	$= \bigoplus_{n \in \mathbb{N}} M_n / M_{n+1}$, p. 320.
$\text{Poin}(M, t)$	$= \sum_{n \in \mathbb{N}} \lambda(M_n) t^n$, serie de Poincaré-Hilbert de un A -módulo graduado finitamente generado, p. 323.
$\chi_{\mathfrak{q}}^M$	Polinomio de Hilbert-Samuel, el polinomio tal que $\chi_{\mathfrak{q}}^M(n) = \ell(M/\mathfrak{q}^n M)$ para n suficientemente grande, p. 326.
$\mathbf{V}(T)$	Espacio de ceros de los polinomios en T , p. 334.

Bibliografía

Las fechas empleadas son aquellas de la primera publicación o del primer registro de Copyright.

Álgebra abstracta

1. ALUFFI, P. *Algebra. Chapter 0* (American Mathematical Society, 1960).
2. CASTILLO, C. I. *Álgebra* <https://www.uv.es/ivorra/Libros/Al.pdf> (2020).
3. CHEVALLEY, C. *The Construction and Study of Certain Important Algebras* (The Mathematical Society of Japan, 1955).
4. CHEVALLEY, C. *Fundamental Concepts of Algebra* (Academic Press, 1956).
5. FINE, B. y ROSENBERGER, G. *The Fundamental Theorem of Algebra* (Springer-Verlag New York, 1997).
6. JACOBSON, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
7. LANG, S. *Algebra* (Springer-Verlag New York, 2002).
8. NAGATA, M. *Theory of Commutative Fields* (American Mathematical Society, 1967).
9. PRESTEL, A. *Lectures on Formally Real Fields* (American Mathematical Society, 1975).
10. RAJWADE, A. R. *Squares* (Cambridge University Press, 1993).
11. ROTMAN, J. J. *Advanced Modern Algebra* 3.^a ed. 2 vols. (American Mathematical Society, 2015).

Álgebra lineal

12. CURTIS, M. L. *Abstract Linear Algebra* (Springer-Verlag New York Inc., 1990).
13. GUIMERÁ, S. *Apuntes para una Licenciatura. Álgebra y Geometría* (ed. NAVARRO GONZÁLEZ, J. A.) matematicas.unex.es/~navarro/licenciatura.pdf (2017).
14. IBORT, A. y RODRÍGUEZ, M. A. *Notas de Álgebra Lineal* http://mimosa.pntic.mec.es/jgomez53/matema/docums/ibort-algebra_lineal.pdf (2014).
15. KATZNELSON, Y. y KATZNELSON, Y. R. *A (Terse) Introduction to Linear Algebra* (American Mathematical Society, 2008).
16. MILNOR, J. y HUSEMOLLER, D. *Symmetric Bilinear Forms* (Springer-Verlag Berlin Heidelberg, 1973).

Álgebra homológica

17. CASTILLO, C. I. *Álgebra Homológica y Álgebra Conmutativa* <https://www.uv.es/ivorra/Libros/Algcom.pdf> (2020).
18. MAC LANE, S. *Homology* (Springer-Verlag Berlin, 1967).
19. ROTMAN, J. J. *An Introduction to Homological Algebra* (Academic Press, 1979).

Álgebra conmutativa

20. ATIYAH, M. F. y McDONALD, I. G. *Introduction to Commutative Algebra* (Addison-Wesley, 1969).
21. EISENBUD, D. *Commutative Algebra with a View Toward Algebraic Geometry* (Springer Science+Business Media, 1994).
22. MATSUMURA, H. *Commutative Ring Theory* (Cambridge University Press, 1986).
23. MILNE, J. S. *A Primer of Commutative Algebra* <https://www.jmilne.org/math/xnotes/CA.pdf> (2020).
24. NAGATA, M. *Local Rings* (Interscience, 1962).

Geometría algebraica

25. CASTILLO, C. I. *Geometría Algebraica* <https://www.uv.es/ivorra/Libros/GA.pdf> (2020).
26. CUTKOSKY, S. D. *Introduction to Algebraic Geometry* (American Mathematical Society, 2018).
27. HARTSHORNE, R. *Algebraic Geometry* (Springer-Verlag New York, 1977).
28. MILNE, J. S. *Algebraic Geometry* ver. 6.02. <https://www.jmilne.org/math/CourseNotes/ag.html>.
29. SANCHO DE SALAS, F. y SANCHO DE SALAS, P. *Geometría Algebraica* <http://matematicas.unex.es/~sancho/LibroGeometriaAlgebraica/geometria0.pdf> (2012).
30. SHAFAREVICH, I. *Basic Algebraic Geometry* 2 vols. (Springer-Verlag Berlin Heidelberg, 2013).

Artículos

31. BANASCHEWSKI, B. Algebraic Closure without Choice. *Mathematical Logic Quarterly*. doi:10.1002/malq.19920380136 (1992).
32. BANASCHEWSKI, B. A New Proof that “Krull implies Zorn”. *Mathematical Logic Quarterly*. doi:10.1002/malq.19940400405 (1994).
33. BLASS, A. Existence of Basis implies the Axiom of Choice. *Contemporary Mathematics* **31**. <http://www.math.lsa.umich.edu/~ablass/bases-AC.pdf> (1984).
34. CONRAD, K. Infinite-dimensional Dual Spaces. <https://kconrad.math.uconn.edu/blurbs/linmultialg/dualspaceinfinite.pdf> (2018).
35. CONRAD, K. Simplicity of A_n . <https://kconrad.math.uconn.edu/blurbs/grouptheory/Ansimple.pdf> (2018).
36. CONRAD, K. The Sylow Theorems. <https://kconrad.math.uconn.edu/blurbs/grouptheory/sylowpf.pdf> (2018).
37. CONRAD, K. Zorn’s Lemma and some applications. <https://kconrad.math.uconn.edu/blurbs/zorn1.pdf> (2018).
38. DERKSEN, H. The Fundamental Theorem of Algebra and Linear Algebra. *The American Mathematical Monthly*. doi:10.2307/3647746 (2003).

39. KNEBUSCH, M., ROSENBERG, A. y WARE, R. Structure of Witttrings and Quotients of Abelian Group Rings. *American Journal of Mathematics* **94**, 119. doi:10.2307/2373597 (1972).

Libros de autoría propia

40. CUEVAS, J. *Teoría de Conjuntos* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/conjuntos/conjuntos.pdf> (2022).
41. CUEVAS, J. *Teoría de Números* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/teo-numeros/main.pdf> (2022).
42. CUEVAS, J. *Topología y Análisis* <https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf> (2022).

Índice alfabético

- α -filtración, 378
- acción, 28
 - fiel, 29
 - transitiva, 29
- aditiva (función), 389
- álgebra, 291, 345
 - alternativa, 313
 - anticonmutativa, 301
 - asociativa, 291
 - conmutativa, 291
 - de composición, 311
 - de tipo finito, 294
 - exterior, 302
 - graduada, 297
 - libre, 346
 - tensorial, 298
- algebraicamente dependientes
 - (elementos), 157
- algebraico (elemento, extensión), 119
- algoritmo
 - de Horner-Ruffini, 74
 - división polinómica, 72
- altura, 394
- anillo, 49
 - de división, 50
 - de enteros, 367
 - de valuación, 359
 - graduado, 296, 378
 - local, 203
 - noetheriano, 56
 - ordenado, 51
- asociatividad, 3
- automorfismo, 9
- autovalor, 257
- autovector, 257
- base, 96
 - (álgebra), 295
 - canónica, 98
 - de trascendencia, 158
 - minimal, 217
 - ortogonal, 263
- bilineal (función), 182
- bimódulo, 340
- cadena
 - de complejos, 330
- cancelación, 5

- categoría, 321
- c -duplicado (álgebra), 315
- centralizador, 18
- centro, 18
- ciclo, 13
- clausura
 - algebraica, 143
 - íntegra, 353
 - normal, 131
- co-cadena
 - de complejos, 333
- coeficiente
 - director, 69
 - polinomio, 68
- complejo de cadenas, 200
- complemento
 - ortogonal, 285
- completo (grupo topológico), 378
- congruentes
 - (matrices), 281
- congruentes (extensiones de módulos), 339
- conjunto
 - algebraico, 400
 - libre, 96, 295
 - ligado, 96
- conmutador, 25
- conmutatividad, 3
- cono
 - de mapas, 336
- cono positivo, 234
- criterio
 - de irreducibilidad
 - de Eisenstein, 82
 - de Gauss, 80
 - de subgrupos, 6
- cuerpo, 50
 - algebraicamente cerrado, 142
 - de escisión, 128
 - de fracciones, 67
 - de números, 367
 - de residuos, 203
 - formalmente real, 233
 - ordenado, 233
 - primo, 59
 - realmente cerrado, 236
- decomposable (ideal), 221
- descomposición
 - primaria, 221
- desigualdad
 - de Bessel, 288
 - de Cauchy-Schwarz, 284
- determinante, 109
- diagonalizable, 259
- dimensión
 - de Noether (espacio topológico), 416
- divisible (módulo), 192
- divisor
 - propio, impropio, 60
- dominio
 - de Dedekind, 367
 - de factorización única (DFU), 61
 - de ideales principales (DIP), 52
 - de valuación discreta, 365
- euclídeo, 55
- íntegro, 50
- ecuación
 - de clases, 30
- elemento
 - irreducible, 60
 - neutro, 3
 - primo, 60
- endomorfismo, 9
 - nilpotente, 271
- entera (álgebra), 350

- entero (elemento), 350
- epimorfismo, 9
- equivalencia
 - de cadenas, 332
- equivalentes (valores absolutos), 358
- escalar, 91
- esencial (homomorfismo), 194
- espacio
 - de producto interno, 260
 - metabólico, 266
 - prehilbertiano, 283
 - vectorial, 91
- estable (filtración), 378
- exacto
 - (functor), 173
 - por la derecha (functor), 172
 - por la izquierda (functor), 172
- extensión
 - abeliana, 150
 - ciclotómica, 150
 - cíclica, 150
 - de cuerpos, 119
 - de Galois, 135
 - de módulos, 339
 - normal, 129
 - trascendente simple, 161
- fiel (módulo), 213, 349
- filtración, 378
- forma
 - bilineal, 280
 - hermitiana, 283
 - multilineal, 107
 - sesquilineal, 282
- fórmula
 - de Grassman, 102
- fuertemente indecomponible (módulo), 179
- función
 - indicatriz de Euler, 11
 - lineal, 92
 - homogénea, 298
- functor
 - (categorías), 323
 - aditivo, 172
 - contravariante, 323
- grado
 - de un polinomio, 69
- grande (submódulo), 194
- grupo, 4
 - abeliano, 4
 - libre, 253
 - cíclico, 7
 - de Galois, 127
 - de torsión, 256
 - diedral, 17
 - finitamente generado, 7
 - libre, 36
 - multiplicativo de n , 11
 - resoluble, 43
 - simple, 35
 - trivial, 4
- homología, 330
- homomorfismo, 9
 - conector, 335
- homotopía
 - de cadenas, 331
- homólogos (ciclos), 331
- ideal, 52
 - entero, 367
 - fraccionario, 367
 - homogéneo, 297, 379
 - impropio, 52
 - irrelevante, 297, 379, 409
 - maximal, 56, 62
 - primo, 62
 - principal, 52, 367

- ideal (álgebra), 293
- identidad
 - de Parseval, 289
- indecomponible (módulo), 179
- índice (subgrupo), 11
- íntegramente cerrado (subanillo), 353
- inversa
 - homotópica, 332
- invertible (módulo), 367
- invertible (elemento), 4, 50
- irreducible (ideal), 227
- isomorfías (estructuras), 9
- isomorfismo, 9
- k -conjugados (elementos), 127
- lema
 - de Artin-Rees, 382
 - de Cassels, 244
 - de descomposición ortogonal, 262
 - de Gauss, 79
 - de la serpiente, 338
 - de Nakayama, 217
- ley
 - del paralelogramo, 285
- libre
 - de torsión (grupo), 256
- límite
 - directo, 327
 - inverso, 327
- matriz
 - adjunta, 110
 - de Vandermonde, 111
 - hermitiana, 274
- máximo
 - común divisor, 64
- menor
 - complemento, 110
- minimal (ideal), 176
- mínimo
 - común múltiplo, 64
- módulo
 - artiniano, 173
 - inyectivo, 191
 - libre, 96
 - noetheriano, 173
 - plano, 187
 - proyectivo, 187
- monoide, 4
- monomio, 68
- monomorfismo, 9
- morfismo (de variedades), 413
- multiplicidad (raíz), 131
- módulo
 - graduado, 382
- nilpotente (elemento), 209
- nilradical, 210
- norma
 - euclídea, 55
- normalizador, 18
- número
 - complejo, 86
- operador
 - de borde, 330
- órbita, 13
- ortogonales (vectores), 285
- ortonormal, 285
- p -grupo, 30
- p -subgrupo, 30
 - de Sylow, 33
- polinomio
 - característico, 113, 270
 - ciclotómico, 83, 151
 - de interpolación de Lagrange, 75
 - derivado, 131

- homogéneo, 408
- minimal, 121
- mónico, 69
- primitivo, 78
- positiva (co-cadena de complejos), 333
- precono positivo, 234
- primario (ideal), 221
- producto
 - directo, 25
 - interno, 260, 283
 - semidirecto, 28
- punto
 - fijo, 13
- puramente trascendente (extensión), 157
- radical (ideal), 210
- rango (matriz), 115
- raíz
 - n -ésima, 121
 - cuadrada, 121
 - cúbica, 121
 - de un polinomio, 69
- reducido (anillo), 210
- reflexión, 264
- regla
 - de Ruffini, 74
- regular (anillo), 397
- regular (función), 412
- semigrupo, 4
- semisimple (anillo), 176
- semisimple (módulo), 174
- separable (elemento, extensión), 132
- similares (matrices), 112, 259
- simple (módulo), 174
- sistema
 - de parámetros, 395
 - generador, 93
 - inverso, 375
- subálgebra, 293
 - homogénea, 297
- subanillo, 52
- subcadena, 332
- subespacio
 - f -invariante, 269
- subgrupo, 6
 - derivado, 42
 - normal, 18
- submódulo, 93
 - impropio, 93
- sucesión
 - de Cauchy (grupo topológico), 374
 - exacta, 21
- sueño del aprendiz, 59
- suma
 - ortogonal, 262
- sumando directo, 175
- tensor, 184
 - puro, 185
- teorema
 - chino del resto, 11, 66
 - de Akizuki, 229
 - de bases de Hilbert, 75
 - de Cauchy, 33
 - de Cayley, 13
 - de Cayley-Hamilton, 277
 - de ceros de Hilbert, 349, 402
 - de De Moivre, 87
 - de extensión de Kronecker, 120
 - de Frobenius, 318
 - de Hurwitz, 317
 - de isomorfismos (primero), 20

- (segundo), 21
- (tercero), 21
- de Jordan-Hölder, 46
- de Krull, 76
- de la correspondencia, 23
- de Lagrange, 11
- de Lüroth, 162
- de Maschke, 177
- de Pitágoras, 285
- de Sylow
 - (cuarto), 35
 - (primero), 33
 - (segundo), 34
 - (tercero), 35
- de Wedderburn, 320
- de Witt, 265
- del ascenso, 355
- del binomio de Newton, 58
- del descenso, 357
- del elemento primitivo, 137
- fundamental
 - de la dimensión, 395
 - de la teoría de Galois, 140
 - de los grupos abelianos, 26
 - del álgebra, 89
- tipo finito (álgebra), 348
- topología
 - α -ádica, 378
- transformación
 - lineal fraccionaria, 161
- trasposición, 14
- valor
 - absoluto, 358
 - no-arquimédiano, 358
- valuación
 - discreta, 364
- variedad
 - afín, 406
 - cuasi-proyectiva, 411
 - proyectiva, 411
- vector, 91
 - unitario, 285

Lista de tareas pendientes

Completar demostración de que su grupo de Galois no es soluble. . . .	156
Probar que si un grupo no es cíclico y posee dos subgrupos de orden 2, entonces	241
Revisar bien el ejercicio.	264
Teoremas pendientes.	302
Probar caso característica = 2.	314
¿Por qué?	364
Completar demostración.	372