Álgebra

José Cuevas Barrientos

8 de mayo de 2022

Índice general

Introducción

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

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

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

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

Parte I.

Álgebra abstracta

1

Teoría de grupos

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

1.1. Estructuras algebraicas

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

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

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

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

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

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

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

Semigrupo Si $\cdot$ es asociativa.

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

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

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

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

Ejemplo. Son grupos:

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

Los cuatro primeros incisos son grupos abelianos.

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

1. Si posee elemento neutro es único.

Si es semigrupo:

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

Si es grupo entonces:

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

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

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

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

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

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

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

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

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

Pista: Se hace por inducción. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$x = x_1 x_2 \cdots x_n$$

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

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

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

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

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

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

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

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

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

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

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

Corolario 1.15: Se cumplen:

1. Los grupos cíclicos son abelianos.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ejemplo.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ahora veamos que f es inyectiva: Si

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

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

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

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

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

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

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

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

1.2. Ejemplos de grupos

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

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

Proposición 1.34: Se cumple:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Teorema 1.37: Se cumplen:

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

Demostración:

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

Signo de una permutación.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proposición 1.42: Se cumple:

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

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

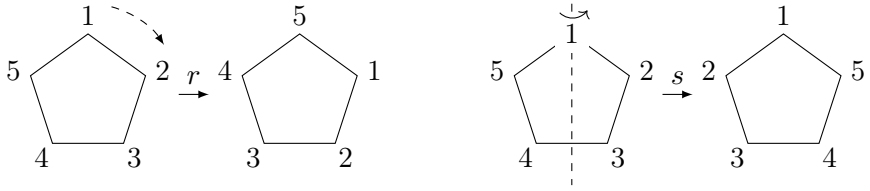


Figura 1.1. Ejemplo con un pentágono.

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

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

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

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

Proposición 1.44: Para todo grupo diedral se cumple:

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

1.3. Representaciones de grupos finitos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

conjugación, i.e.,

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

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

Proposición 1.51: Se cumple:

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

Teorema 1.52: Todo subgrupo de índice dos es normal.

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

Proposición 1.53: Se cumple:

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

3. El orden se preserva bajo conjugados.

Demostración:

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

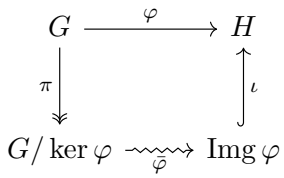
2. Sea $a \in G$ y $c \in G$ arbitrario, de forma que $b := c^{-1}ac$, luego por la propiedad anterior se cumple que $b^k = c^{-1}a^kc$, por lo que si $n := \operatorname{ord} a$, entonces $b^n = c^{-1}a^nc = c^{-1}ec = e$. Por lo que $\operatorname{ord} b \leq \operatorname{ord} a$. Pero notemos que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

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

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

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

En figura de diagrama conmutativo:



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

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

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

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

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

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

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

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

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

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

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

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

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

Proposición 1.60: Se cumple:

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

3. Si $H \trianglelefteq G$, entonces

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

es una sucesión exacta corta.

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

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

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

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

conmuta.

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

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

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

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

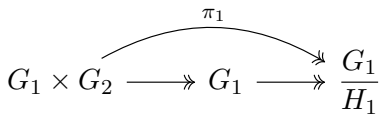
Luego se cumple que

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

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

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

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



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

Teorema 1.63 – *Cuarto teorema de isomorfismos*: Si $\varphi\colon G \twoheadrightarrow H$, entonces

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

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

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

Demostración:

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

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

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

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

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

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

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

§1.3.2 Productos directos y semidirectos de grupos.

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

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

Demostración:

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

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

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

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

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

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

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

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

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

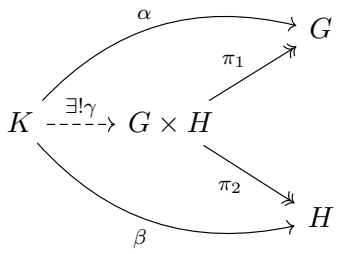
Demostración: Notemos que $[n, m] = (n^{-1}m^{-1}n)m = n^{-1}(m^{-1}nm)$, donde $n^{-1}mn \in M$ y $m^{-1}nm \in N$ por ser normales. Como $[n, m] \in N \cap M = \{1\}$, entonces $[n, m] = 1$, luego conmutan. □

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

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

Proposición 1.68: Sean G, H grupos, entonces:

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



conmuta.

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

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

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

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

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

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

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

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

En particular, se cumple para grupos abelianos finitos.

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

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

Finalmente agrupando todo nos da el enunciado. □

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

Veamos dos aplicaciones de ésto:

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

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

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

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

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

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

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

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

es un grupo.

Demostración: Veamos que se cumplen las propiedades:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a los que llamamos órbita y estabilizador de a resp.

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

Ejemplos. Son acciones:

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

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

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

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

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

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

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

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

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

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

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

Corolario 1.87: Se cumplen:

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

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

1.4. Teoremas de Sylow

§1.4.1 Acciones.

Teorema 1.88: Si G actúa sobre S, entonces:

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

Demostración:

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

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

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

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

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

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

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

Demostración: Por la ecuación de órbitas se cumple que

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ejemplo. Los grupos cíclicos de orden primo son simples.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.5. Otros tópicos de grupos

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

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

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

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

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

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

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

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

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

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

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

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

forma por definición de ser libre. Si $g \neq 1$ y se tienen las dos siguientes representaciones:

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

Luego se cumple que

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

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

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

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

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

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

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

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

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

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

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

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

Y si $y_1 \neq x_n$ es trivial.

Luego el caso inductivo queda al lector.

$\Longrightarrow$. Sea X una base de G que genera el subgrupo H. Luego sea $\iota \colon X \to H$ la función inclusión, con lo que se extiende a un homomorfismo $f \colon G \to H$. Pero además, como $H \leq G$ se cumple que la inclusión $g \colon H \to G$

es un homomorfismo. Así $(f \circ g)\colon G \to G$ es una extensión de la inclusión $X \to G$ que es la identidad por unicidad y que implica que g es suprayectiva (que era la inclusión), así que $H = G$.

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

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

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

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

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

Demostración:

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

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

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

   lo que comprueba el caso finito.

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

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

Una aplicación de los grupos libres como tal son las demostraciones de la paradoja de Banach-Tarski (véase [31, §A.1.2.]).

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

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

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

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

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

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

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

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

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

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

conmuta, del que se deriva el epimorfismo deseado. □

§1.5.2 Grupos resolubles.

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

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

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

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

Proposición 1.115: Se cumplen:

1. Todo grupo finito posee una serie de composición.

2. Toda serie normal estricta puede extenderse a una serie de composición.

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

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

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

□

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

Proposición 1.117: Se cumplen:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Teorema 1.121: Se cumple:

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

Demostración:

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

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

es una serie abeliana. Nótese que

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

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

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

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

es una serie abeliana pues

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

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

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

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

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

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

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

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

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

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

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

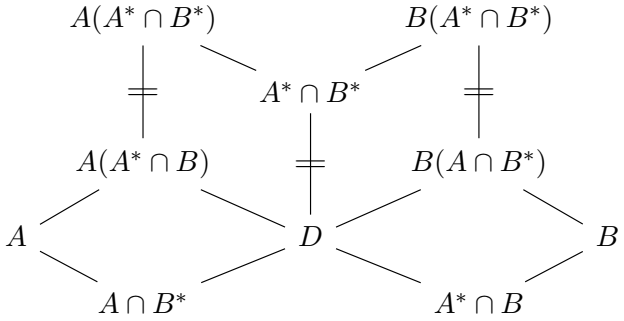
1. $A(A^* \cap B) \trianglelefteq A(A^* \cap B^*)$.
2. $B(B^* \cap A) \trianglelefteq B(B^* \cap A^*)$.
3. $\dfrac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \dfrac{B(B^* \cap A^*)}{B(B^* \cap A)}$.

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

Formalmente probaremos que:

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

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



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

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

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

Demostración: Sean

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

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

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

[4]Éste diagrama fue introducido por Lang en [6] y fue la razón de que él le nombrara el «lema de la mariposa».

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Demostración:

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

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

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

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

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

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

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

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

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

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

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

2

Anillos y cuerpos

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

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

2.1. Definiciones elementales

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

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

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

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

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

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

Si $x, y \in A$ son no nulos y $xy = 0$ entonces diremos que x, y son *divisores de cero* y, en particular, x es 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 $\Bbbk$ representa un cuerpo con operaciones $+, \cdot$, neutro aditivo 0 y multiplicativo 1.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Teorema 2.26: Todo dominio euclídeo es un DIP.

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

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

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

(1) Todo ideal de A está finitamente generado.

(2) Para toda cadena ascendente de ideales de A

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

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

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

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

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

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

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

Corolario 2.29: Todo DIP es noetherinao.

[1] Véase [30, Def. 2.3]

§2.1.1 Teorema del binomio.

Definición 2.30: Dado n natural se define por recursividad:

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

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

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

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

Proposición 2.31: Se cumple:

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

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

3. Si $m < n$, entonces

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

(regla de Pascal).

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

Demostración:

3.

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

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

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

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

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

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

Lo que completa la demostración. □

§2.1.2 Característica.

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

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

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

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

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

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

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

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

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

Teorema 2.38 (Sueño del aprendiz): Si $\operatorname{car} \Bbbk = p \neq 0$, entonces para todo $x, y \in \Bbbk$ se cumple que

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

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

2.2. Divisibilidad en anillos

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

Definición 2.39 – *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 2.40 – *Irreducibles y primos*: Sea A un dominio. Diremos que un elemento es *irreducible* syss es es no nulo, no es inversible, y no posee divisores propios. Un elemento que no sea nulo ni inversible y que no sea irreducible se dice *reducible*.

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

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

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

Teorema 2.41: En un dominio íntegro A todo primo es irreducible.

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

Definición 2.42: Un dominio A se dice que posee la:

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

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

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

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

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

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

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

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

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

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

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

Teorema 2.43: En un DFU un elemento es primo syss es irreducible.

Teorema 2.44: Todo anillo noetheriano A posee la propiedad de factorización. Si además todo irreducible es primo, entonces A es DFU.

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

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

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

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

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

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

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

Definición 2.45: 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) 2.46 (Cohen): Un dominio A es noetheriano syss todo ideal primo de A es finitamente generado.

Demostración: $\Longrightarrow$. Trivial.

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

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

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

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

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

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

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

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

Proposición 2.47: Sea $\varphi\colon A \to B$ un homomorfismo de anillos. Si $\mathfrak{p}$ es un ideal primo de B, entonces $\varphi^{-1}[\mathfrak{p}]$ es un ideal primo de A.

Teorema 2.48: Un ideal $\mathfrak{p}$ en un dominio A es primo syss $A/\mathfrak{p}$ es un dominio íntegro.

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

$\Longleftarrow$. Es análogo. □

Teorema 2.49: Un ideal $\mathfrak{m}$ en un dominio A es maximal syss $A/\mathfrak{m}$ es un cuerpo.

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

$\Longleftarrow$. Es análogo. □

Corolario 2.50: 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 2.77).

Lema 2.51: Sea A un dominio íntegro y $a, p \in A$ no nulo, entonces:

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

Como un DIP es un dominio, vemos que efectivamente todo irreductible es primo. Lo que sumado al teorema 2.44 nos da:

Teorema 2.52: Todo DIP es un DFU.

Definición 2.53: 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 2.54 (Identidad de Bézout): Sea A un DIP con $a_0, \ldots, a_n \in A$; luego sea m un mcd, entonces

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

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

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

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

Nótese que conceptos como los de ser coprimos se mantienen.

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

Definición 2.55: 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 2.56: 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 2.57: Se cumplen:

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

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

Demostración:

1. Probaremos por inducción la contrarrecíproca, vale decir:

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

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

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

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

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

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

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

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

Teorema 2.58 – *Teorema chino del resto*: Si A es un dominio y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq A$, entonces

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

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

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

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

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

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

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

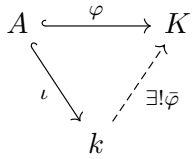
Luego, para todo $(b + \mathfrak{a}_1, c + \mathfrak{a}_2)$ se cumple que $ba_1 + ca_2$ es una preimagen. La otra implicancia es claramente deducible de manera similar.

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

Corolario 2.59: Si A es un dominio y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \trianglelefteq A$, entonces el homomorfismo φ del teorema anterior se restringe a un homomorfismo de grupos

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

Teorema 2.60: Todo dominio íntegro A está contenido en un cuerpo k, tal que si $\varphi : A \hookrightarrow K$ con K cuerpo, entonces existe un único homomorfismo $\bar{\varphi} : k \hookrightarrow K$. Es decir, se satisface el siguiente diagrama:



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

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

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

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

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

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

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

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

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

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

Corolario 2.61: 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 2.62: Por el corolario anterior se denota por $\mathrm{Frac}(A)$ al cuerpo dado en la demostración del teorema, al que llamamos *cuerpo de fracciones* de A.

El lector atento habrá notado dos cosas: La primera es que la construcción de $\mathrm{Frac}(A)$ es exactamente la misma que de $\mathbb{Q}$ desde $\mathbb{Z}$, es decir, podríamos definir $\mathbb{Q} := \mathrm{Frac}(\mathbb{Z})$. La segunda es que la condición segunda del teorema es una condición minimal propia de las categorías, de hecho, podríamos construir una categoría de los cuerpos que extienden a A y lo que nos dice el teorema es que dicha categoría posee un objeto inicial; en este sentido el corolario es trivial.

2.3. Polinomios

Un polinomio viene a representar objetos de la forma

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

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

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

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

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

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

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

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

Definición 2.63 – *Polinomio*: Finalmente, dado un anillo A y un conjunto de indeterminadas S, denotaremos $A[S]$ al conjunto de todas las aplicaciones $f\colon M \to A$ tal que $M \setminus f^{-1}[0]$ es finito, es decir, tal que tan sólo finitos monomios poseen coeficientes no nulos. En definitiva f representa a la expresión

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

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

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

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 *lider*. 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

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

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

Teorema 2.64: Sea A un anillo, entonces $(A[x], +, \cdot)$ lo es. Si A es unitario, $A[x]$ también lo es. Si A es conmutativo, $A[x]$ también lo es.

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

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

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

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

Teorema 2.65: 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

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

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

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

Notemos que si $f \in A[x_1, \ldots, x_n]$ entonces se escribe como prosigue

$$f(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n};$$

evidentemente, $A[x_1, \ldots, x_n]$ es siempre un anillo por inducción.

Teorema 2.66: Sea A un dominio íntegro, entonces $A[x_1, \ldots, x_n]$ es un dominio íntegro.

Demostración: Por el teorema anterior, sabemos que multiplicar dos polinomios no nulos incrementa su grado y por definición de grado en polinomios de múltiples variables este siempre crece, por tanto, no puede ser nulo a menos que uno de ellos sea nulo, osea, es un dominio íntegro. Para formalismos, el argumento se aplica con inducción. □

Teorema 2.67: Todas las unidades de un dominio íntegro A lo son también de $A[x_1, \ldots, x_n]$.

Demostración: Por el teorema 2.65 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. □

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

Teorema 2.68 – *Algoritmo de división polinómica*: Sea A un anillo con $\alpha \in A[x]$ un polinomio no nulo cuyo coeficiente director es una unidad de A y $\beta \in A[x]$ cualquiera. Existen unos únicos polinomios $q, r \in A[x]$ tales que

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

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

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

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

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

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

que

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

que satisface todas nuestras restricciones.

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

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

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

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

Corolario 2.69: Si A es un cuerpo, entonces $A[x]$ es un dominio euclídeo cuya norma es el grado.

Teorema 2.70: Si A es un dominio íntegro, entonces $A[x]$ es un DIP syss A es un cuerpo.

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

Teorema 2.71 – *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 2.72: Sea A un anillo con $p(x) \in A[x]$ de grado n, entonces p tiene, a lo sumo, n raíces.

Teorema 2.73 (Wilson): Si p es primo, entonces

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

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

Figura 2.1. Aplicación del algoritmo de Horner-Ruffini.

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

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

Teorema 2.74 (Algoritmo de Horner-Ruffini): Sean A un dominio íntegro con $x_0 \in R$ y $p(x) \in A[x]$ un polinomio de la forma $p(x) = a_0 + \cdots + a_n x^n$. Defínase la secuencia, de forma inductiva (a la inversa):

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

entonces se cumple que

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

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

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

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

Podemos ver que es correcto, pues

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

Teorema 2.75 – *Polinomio de interpolación de Lagrange*: Sea A un cuerpo con $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$. Existe un único polinomio $f \in A[x]$ de grado menor a n tal que $f(a_i) = b_i$ para todo $i = 1, \ldots, n$; y está dado por la fórmula[a]

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

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

Demostración: Es fácil ver que $P_i(a_j) = 0$ cuando $i \neq j$, por lo que, el polinomio de Lagrange efectivamente cumple con las condiciones indicadas. Para ver que es el único de grado menor a n, consideremos que $g(x) \in A[x]$ también cumpliese con las condiciones, luego $(f-g)(x)$ sería un polinomio de grado menor que n con n raíces, lo que es imposible por el teorema 2.72. □

Teorema 2.76 – *Teorema de bases de Hilbert*: Si A es un anillo noetheriano, entonces $A[x_1, \ldots, x_n]$ lo es.

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

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

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

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

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

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

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

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

Ejemplo. Tomemos a $\mathbb{R}$ que es cuerpo y por ende noetheriano. Luego si $S := \{x_1, x_2, x_3, \dots\}$ 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 2.77: Son equivalentes:

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

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

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

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

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

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

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

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

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

Consideremos $R \cdot U^{-1} \leq \mathrm{Frac}(R)$, es decir, $R \cdot U^{-1}$ como subanillo del cuerpo de fracciones de R. Entonces $R \cdot U^{-1}$ es un dominio y por el teorema

de Krull posee un ideal maximal $\mathfrak{m}$. Luego $\mathfrak{a} := \mathfrak{m} \cap R$ es claramente un ideal de R, y además es maximal y disjunto de U; en consecuencia $\mathfrak{a} \subseteq T$.

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

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

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

2.4. Divisibilidad de polinomios

Definición 2.78 – *Contenido*: Sea A un DFU, definimos la aplicación $c\colon A[x] \to \mathcal{P}(A)$, llamada *contenido del polinomio*, como aquella tal que sea d el mcd de los coeficientes no-nulos de $f \in A[x]$, entonces $c(f) = (d)$. Definimos que $c(0) = (0)$.

Decimos que un polinomio es *primitivo* syss $c(f) = (1)$, es decir, si sus coeficientes no nulos son coprimos. En particular, todo polinomio mónico es primitivo.

Teorema 2.79 – *Teorema de las raíces racionales*: Sea A un DFU, $K := \mathrm{Frac}(A)$ y $p(x) \in A[x]$ un polinomio no-constante:

$$p(x) = \sum_{i=0}^{n} c_i x^i.$$

Si $\alpha = a/b$, con $a, b \in A$ coprimos, es una raíz de $p(x)$, entonces $a \mid c_0$ y $b \mid c_n$.

Demostración: Como $\alpha = a/b$ es una solución

$$\sum_{i=0}^{n} \frac{a^i}{b^i} c_i = 0,$$

multiplicando por b^n y aplicando técnicas de despeje obtenemos las dos ecuaciones siguientes:

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

en las cuales, evidentemente los factores resultan ser elementos de A, por lo que, $b \mid a^n c_n$ y $a \mid b^n c_0$, pero como a, b son coprimos, nos resulta que $b \mid c_n$ y $a \mid c_0$ tal como lo indica el enunciado. □

Esto es útil tanto para buscar raíces racionales que con aplicar la regla de Ruffini simplifican los polinomios, como para comprobar la irracionalidad de ciertas raíces; en particular para otorgar otra demostración que $\sqrt{2} \notin \mathbb{Q}$, pero que se generaliza a que para todo primo p se cumple que $\sqrt{p} \notin \mathbb{Q}$.

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

Lema 2.81 (de primitividad de Gauss): Sea A un DFU con $f, g \in A[x]$ primitivos, entonces $f \cdot g$ es primitivo.

Demostración: Sean $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ y $g(x) = b_0 + \cdots + b_m x^m$, entonces $f \cdot g(x) = c_0 + \cdots + c_{n+m} x^{n+m}$. Sea p un número primo y digamos

que divide a todos los a_i con $i < u$ y los b_i con $i < v$, entonces

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

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

Teorema 2.82: Sean $f, g \in A[x]$ y $k \in A$, entonces

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

Demostración:

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

Lema 2.83: Sea A un DFU con K su cuerpo de cocientes y $f, g \in A[x]$ polinomios primitivos no-constantes. f y g son asociados en $K[x]$ syss lo son en $A[x]$.

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

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

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

Teorema 2.84: Si $f \in \Bbbk[x]$ es de grado 2 o 3, entonces es irreductible syss no posee raíces.

Demostración: Por regla de Ruffini es claro que si es irreductible no posee raíces. Para el caso recíproco basta considerar que toda posible factorización incluye un término de grado 1. □

Teorema 2.85 – *Criterio de Irreducibilidad de Gauss*: Sea A un DFU, $K := \mathrm{Frac}(A)$ y $f \in A[x]$ un polinomio primitivo no constante. f es irreducible en $A[x]$ syss lo es en $K[x]$.

Demostración: $\Longleftarrow$. Éste caso es trivial.

$\Longrightarrow$. Supongamos que f es reducible en $K[x]$, pero no en $A(x)$, por lo que $f = gh$ con $g, h \in K[x]$. Esto significa que

$$g(x) = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i, \quad h(x) = \sum_{i=0}^{m} \frac{c_i}{d_i} x^i$$

con b_i, c_i no-nulos. Definamos $b := \prod_{i=0}^{n} b_i$ y $\tilde{b}_i := b/b_i$ con lo que $g_1(x) = \sum_{i=1}^{n} a_i \tilde{b}_i x^i$ de contenido u, por lo que $g_2 := g_1/u$. Por lo que $g = (b/u)g_2$ y $h = (d/v)h_2$, es decir,

$$f = \frac{bd}{uv} g_2 h_2$$

como u, v son no nulos, f y $g_2 h_2$ son primitivos asociados en $K[x]$, luego lo son en $A[x]$. □

Teorema 2.86: 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 $K := \mathrm{Frac}(A)$; pero $K[x]$ es un DFU, luego las factorizaciones son equivalentes en $K[x]$ y claramente también lo son en $A[x]$.

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

Teorema 2.87 – *Criterio de Irreducibilidad de Eisenstein*: Sean A un DFU, $K := \mathrm{Frac}(A)$ y $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ no-constante. Sea $p \in A$ un primo, luego f es irreducible en K si:

1. $p \nmid a_n$.
2. $p \mid a_i$ para $i = 0, 1, \ldots, n-1$.
3. $p^2 \nmid a_0$.

Demostración: Supondremos que $f = af^*$ con f^* primitiva (a es una unidad en K), de modo que si fuese reducible en K existirían $g = \sum_{i=0}^{r} b_i x^i, h = \sum_{i=0}^{s} c_i x^i \in A[x]$ primitivos, no constantes, tales que $f^* = gh$. Nótese que $a_0^* = b_0 c_0$, por lo que $p \mid b_0$ o $p \mid c_0$, pero no ambos (restricción por construcción), por ello supondremos el primer caso.

p no puede dividir todos los b_i por ser g primitiva, así que digamos que sea k el primer índice tal que $p \nmid b_k$ con $0 < k \leq r < n$. Sabemos que $p \mid a_k = \sum_{i+j=k} b_i c_j$, además de dividir todos los términos individualmente a excepción del último, por lo que, p divide a la resta (que da como resultado $b_k c_0$), pero $p \nmid b_k$ y $p \nmid c_0$, lo que sería absurdo. □

Teorema 2.88: Sea A un dominio con $a \in A$ invertible y $b \in A$ cualquiera, entonces $p(x)$ es irreductible syss $p(ax+b)$ lo es.

Demostración: Para demostrarlo veremos que $f : A[x] \to A[x]$ donde $f(p(x)) = p(ax+b)$ es un isomorfismo de anillos. Es claro que es un homomorfismo, y como $g(x) = ax + b$ es una biyección, comprobamos el enunciado. □

Ejemplo 1 (polinomios ciclotómicos): Para todo p primo, llamamos polinomio ciclotómico p-ésimo a

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

veamos que son irreductibles en $\mathbb{Q}[x]$: Es una aplicación directa del criterio de Eisenstein usando la composición

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k.$$

Nótese que el polinomio es mónico, así que p no divide al coeficiente director, mientras que el término constante es p así que $p^2 \nmid p$, y para el resto basta

notar que el denominador es de la forma $n!$ con $n < p$, así que no «cancela» el término con p, luego $p \mid \binom{p}{n}$.

Usualmente se suelen aplicar en conjunto el criterio de Eisenstein con el teorema anterior para demostrar la irreductibilidad de un polinomio. Por ejemplo, utilizando el mismo polinomio que en la aplicación del algoritmo de Horner-Ruffini, $p(x) = 3x^2 + 2x + 1$, probaremos que es irreductible en $\mathbb{Q}$, primero multiplicamos todos los términos por 3 para obtener $3p(x) = 9x^2 + 6x + 3$, luego consideremos el polinomio

$$3p\left(\frac{x+1}{3}\right) = (x+1)^2 + 2(x+1) + 3 = x^2 + 4x + 6.$$

que es irreductible por criterio de Eisenstein. Recuerde que 3 es una unidad de $\mathbb{Q}$ y como el polinomio original es primitivo, entonces es irreductible también en $\mathbb{Z}$.

Teorema 2.89 (criterio de irreducibilidad por reducción): Sea $\sigma\colon A \to B$ un homomorfismo entre dominios íntegros. Sean $K := \operatorname{Frac}(A)$ y $L := \operatorname{Frac}(B)$. Sea $f \in A[x]$ un polinomio tal que $\sigma(f) \neq 0$ y $\deg \sigma(f) = \deg f$. Entonces si $\sigma(f)$ es irreducible en $L[x]$, entonces $f \neq g \cdot h$ con $g, h \in A[x]$ y $\deg g, \deg h \geq 1$.

Demostración: Por contrarrecíproca: si $f = g \cdot h$ con $g, h \in A[x]$ y $\deg g, \deg h \geq 1$, entonces $\sigma(f) = \sigma(g)\sigma(h)$. Ahora bien, es claro que $\deg \sigma(g) \leq \deg g$ y $\deg \sigma(h) \leq \deg h$, pero como $\deg \sigma(f) = f$, entonces se concluye la igualdad en el caso anterior. Y sabemos que $L[x]^\times = L^\times$, por lo que $\sigma(g), \sigma(h)$ no son inversibles y por ende son divisores propios de $\sigma(f)$, es decir, $\sigma(f)$ es reducible. □

Ejemplo. Veamos que el polinomio $p(x) := x^3 + x + 1 \in \mathbb{Z}[x]$ es irreducible. Consideremos $\pi\colon \mathbb{Z} \to \mathbb{F}_2$ que es un homomorfismo, y recordemos que $\mathbb{F}_2$ es un cuerpo. Luego veamos que $\pi(p(x)) = x^3 + x + 1 = p(x) \in \mathbb{F}_2$ es irreducible. Como $p(x)$ es cúbico basta ver que no tiene raíces y $p(0) \equiv 1$ y $p(1) \equiv 1$ (mód 2), así que efectivamente es irreducible en $\mathbb{F}_2$; luego es irreducible en $\mathbb{Z}[x]$ por el criterio por reducción.

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

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

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

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

(a) Si $-1 = a^2$ (incluye a $p = 2$): Entonces
$$x^4 + 1 = x^4 - a^2 = (x^2 - a)(x^2 + a).$$

(b) Si $p \neq 2$ y $2 = b^2$: Entonces
$$x^4 + 1 = (x^2 + 1)^2 - (bx)^2 = (x^2 + 1 - bx)(x^2 + 1 + bx).$$

(c) En otro caso: Si -1 y 2 no son cuadrados, como $\mathbb{F}_p^\times$ es cíclico, se concluye que -2 ha de ser un cuadrado. En particular $-2 = c^2$ y:
$$x^4 + 1 = (x^2 + 1)^2 - (cx)^2 = (x^2 + 1 - cx)(x^2 + 1 + cx).$$

Corolario 2.90: Sea A un DFU, $K := \mathrm{Frac}(A)$ y $p(x) \in A[x]$ un polinomio no-constante mónico, entonces $\alpha \in K$ es una raíz de p syss $\alpha \in A$.

§2.4.1 Raíces básicas.

Definición 2.91: Dado $\alpha \in \Bbbk$, decimos que β es una n-ésima raíz de α si $\beta^n = \alpha$ o alternativamente si β es raíz del polinomio $x^n - \alpha$.

Lema 2.92: Si β es una raíz cuadrada de α, entonces $-\beta$ y β son todas las raíces cuadradas de α.

Teorema 2.93 (Fórmula cuadrática): Si $p(x) = x^2 + rx + s$, entonces llamamos definimos $\Delta := r^2 - 4s$ como el *discriminante* de $p(x)$. Finalmente p tiene raíces syss existe α raíz cuadrada de Δ, en cuyo caso las raíces de p son
$$\frac{-r + \alpha}{2}, \quad \frac{-r - \alpha}{2}.$$

Demostración: Es fácil comprobar que éste es el caso, pero la deducción viene de que si
$$\begin{aligned} x^2 + rx + s = 0 &\iff x^2 + 2x \cdot \frac{r}{2} = -s \\ &\iff x^2 + 2x \cdot \frac{r}{2} + \frac{r^2}{4} = \left(x - \frac{r}{2}\right)^2 = \frac{r^2}{4} - s = \frac{\Delta}{4} \end{aligned}$$
Luego si α es raíz de Δ, entonces $\pm\alpha/2 = x - r/2$ y así se deduce el enunciado. □

Corolario 2.94: Un polinomio de grado 2 es irreductible syss su discriminante no posee raíces cuadradas.

2.5. Números complejos

Rigurosamente los números complejos emergen por las llamadas extensiones de Kronecker, que se ven más adelante, de modo que se introduce la unidad imaginaria i como raíz del polinomio real irreductible x^2+1. Aquí haremos una definición alternativa de los números complejos que permitirá al lector acostumbrarse a ellos.

Definición 2.95 – *Números complejos*: Se define $\mathbb{C}$ como el conjunto $\mathbb{R}^2$ con las operaciones:

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

Usualmente denotamos $(a,b) = a+\mathrm{i}b$. Pues $(1,0)$ se comporta como el neutro multiplicativo, $(0,0)$ como el neutro aditivo e $\mathrm{i}^2 = (0,1)^2 = (-1,0) = -1$. También se definen las funciones $\mathrm{Re}, \mathrm{Im} : \mathbb{C} \to \mathbb{R}$ como

$$\mathrm{Re}(a+\mathrm{i}b) = a, \quad \mathrm{Im}(a+\mathrm{i}b) = b,$$

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

También, denotamos

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

donde a $|z|$ se le dice el *módulo*[a] de z y a $\overline{z}$ el *conjugado* de z.

[a] Algunos textos prefieren usar $\|\,\|$ para los complejos y dejar $|\,|$ para los reales. Mi convenio es usar $\|\,\|$ para sus espacios vectoriales.

Proposición 2.96: Para todo $z, w \in \mathbb{C}$ se cumple:

1. $|z| = 0$ syss $z = 0$.
2. $\overline{\overline{z}} = z$.
3. $|\overline{z}| = |z|$.
4. $z + \overline{z} = 2\,\mathrm{Re}\,z$ y $z - \overline{z} = 2\,\mathrm{Im}\,z$.
5. $\overline{z+w} = \overline{z} + \overline{w}$ y $\overline{z\cdot w} = \overline{z}\cdot\overline{w}$. En otras palabras, $\overline{\cdot}$ es un automorfismo de cuerpos.

6. $x \in \mathbb{R}$ syss $\overline{x} = x$ syss $\overline{\mathrm{i}x} = -x$.
7. $z \cdot \overline{z} = |z|^2$.
8. $|zw| = |z|\,|w|$.

Teorema 2.97: $(\mathbb{C}, +, \cdot)$ es un cuerpo.

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

Teorema 2.98: 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 2.99: Todo complejo tiene raíz cuadrada. En consecuencia, todo polinomio cuadrático es reductible en los complejos.

Proposición 2.100: Si $P, Q \in \mathbb{C}[x]$, entonces:

1. Para todo $z \in \mathbb{C}$ que $\overline{P}(\overline{z}) = \overline{P(z)}$.
2. $P \in \mathbb{R}[x]$ syss $P(z) = \overline{P}(z)$.
3. Si $R := P \cdot Q$, entonces $\overline{R} = \overline{P} \cdot \overline{Q}$.
4. Si $P \in \mathbb{R}[x]$ tiene raíz compleja z, entonces $\overline{z}$ también es raíz.
5. $P \cdot \overline{P} \in \mathbb{R}[x]$.

Definición 2.101: Se define la función $\operatorname{cis} : \mathbb{R} \to \mathbb{C}$ tal que

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

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

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

Proposición 2.102: Si $z \in \mathbb{C}_{\neq 0}$, entonces $z = |z| \operatorname{cis}(\arg z)$.

Teorema 2.103 – *Teorema de De Moivre*: Si $u = r \operatorname{cis} \alpha$ y $v = s \operatorname{cis} \beta$, entonces

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

En particular

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

Demostración: Basta notar que

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

como se quería probar. □

Corolario 2.104: 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 2.105: Sea $n > 1$, entonces se le llaman *raíces n-ésimas de la unidad* a los $z \in \mathbb{C}$ tales que $z^n = 1$. Se denota también

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

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

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

Lema 2.106: Si $f \in \mathbb{C}[x]$ es no constante, entonces $|f(z)| \to \infty$ si $|z| \to \infty$. Dicho de otro modo, para todo $R > 0$ existe $r > 0$ tal que para todo $|z| \geq r$ se cumple que $|f(z)| \geq R$.

Demostración: En particular probaremos que

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

Esto se cumple pues si

$$f(z) = c_n z^n + \cdots + c_1 z + c_0$$

entonces

$$\frac{|f(z)|}{|z|^n} \geq |c_n| + |c_{n-1}|\,|z|^{-1} + \cdots + |c_0|\,|z|^{-n}$$

lo que converge a $|c_n|$ y que

$$|f(z)| \geq |c_n|\,|z|^n - |z|^{n-1}(|c_{n-1}| + \cdots + |c_0|\,|z|^{1-n})$$

Luego, basta exigir que $|z| > 1$ para ver que

$$\frac{|f(z)|}{|z|^n} \geq |c_n| - \frac{1}{|z|}(|c_{n-1}| + \cdots + |c_1| + |c_0|)$$

de lo que se concluye el enunciado. □

Lema 2.107: Para todo $f \in \mathbb{C}[x]$ no constante, existe x_0 que minimiza $|f(x_0)|$.

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

Teorema 2.108 – *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 $g(0) = 1$. □

Parte II.

Álgebra lineal

3

Módulos

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 y vectores

Definición 3.1 – *Módulos y vectores*: Dado un anillo unitario A, diremos que una terna $(M, +, \cdot)$ es un A-módulo (izquierdo) si $+\colon M^2 \to M$ y $\cdot\colon A \times M \to M$ tales que $(M, +)$ es un grupo abeliano (de neutro $\vec{0}$) y para todo $\boldsymbol{u}, \boldsymbol{v} \in M$ y $\alpha, \beta \in A$ se cumple:

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

Si A es un anillo de división entonces diremos que M es un A-espacio vectorial y a los elementos de M les diremos *vectores* y a los de A *escalares*.

En general, denotaremos los elementos de los A-módulos con letras negritas,

a los escalares con fuente normal y como excepción al $\vec{0}$ con una flechita.

Proposición 3.2: Si M es un A-módulo, entonces:

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

Ejemplo 3: Son A-módulos:

- A^n con la suma y el producto por escalar coordenada a coordenada.
- $\mathrm{Func}(S; A)$ con $(f+g)(s) := f(s) + g(s)$ y $(\alpha f)(s) := \alpha \cdot f(s)$ para $\alpha \in A$ y $s \in S$.
- $A[S]$ de forma análoga a $\mathrm{Func}(S; A)$.
- I con la suma y el producto, donde I es ideal de A.
- B, donde B es un anillo tal que A es subanillo de B.

Ejemplo 4: Todo grupo abeliano es un $\mathbb{Z}$-módulo: Sea G abeliano, entonces consideramos $\boldsymbol{u} + \boldsymbol{v} := \boldsymbol{u} * \boldsymbol{v}$ (donde $*$ es la operación de grupo de G) y $n\boldsymbol{u} := (\boldsymbol{u})^n$. La notación engorrosa es solamente para ilustrar el sentido de ésta afirmación. Claramente «$(G, +)$» es un grupo abeliano de neutro «$\vec{0}$» y nótese que ya hemos probado en el primer capítulo que todos los axiomas son ciertos; ésto es lo que motiva el uso de «notación aditiva» al tratarse de grupos abelianos.

Definición 3.3 – *Morfismos de módulos*: Una aplicación $f\colon M \to N$ se dice un morfismo de A-módulos si para todo $\boldsymbol{u}, \boldsymbol{v} \in M$ y $\lambda \in A$ se comprueba

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

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

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

Proposición 3.4: Sea M un A-módulo. Entonces:

1. $\mathrm{Id}_M \colon M \to M$ es un morfismo de A-módulos.

2. La composición de morfismos de A-módulos es también un morfismo de A-módulos.

En consecuencia, los A-módulos (como objetos) y los morfismos de A-módulos (como flechas) conforman una categoría, denotada Mod_A. Ésto también aplica para k-espacios vectoriales, cuya categoría se denota Vect_k.

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

Proposición 3.5: Dados X, Y no vacíos se cumple que $\mathrm{Func}(X; A) \cong \mathrm{Func}(Y; A)$ syss $|X| = |Y|$. Luego, dado un cardinal κ denotamos A^κ a un A-módulo $\mathrm{Func}(S; A)$ genérico[1] con $|S| = \kappa$.

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

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

Lema 3.8: La intersección de submódulos es un submódulo.

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

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

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

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

Proposición 3.10: Se cumple que

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

Proposición 3.11: Si N es un submódulo del A-módulo M, entonces $\boldsymbol{x} \equiv \boldsymbol{y}$ (mód N) definido porque $\boldsymbol{x} - \boldsymbol{y} \in N$ es una relación de equivalencia, bajo la cuál se denota por M/N al conjunto cociente que también resulta ser un A-módulo.

Teorema 3.12 – *Teoremas de isomorfismos*: Se cumple:

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

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

II Si S, T son submódulos del A-módulo M, entonces

$$\frac{S}{S \cap T} \cong \frac{S+T}{T}.$$

III Si $S \leq T \leq M$, entonces

$$\frac{M}{T} \cong \frac{M/S}{T/S}.$$

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

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

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

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

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

a) $M = \bigoplus_{i\in I} N_i$.

b) Si $\sum_{i\in I} \boldsymbol{m}_i = \vec{0}$ con $\boldsymbol{m}_i \in N_i$ para todo $i \in I$, entonces $\boldsymbol{m}_i = \vec{0}$.

c) Para todo $\boldsymbol{m} \in M$ existen unos únicos $\boldsymbol{m}_i \in N_i$ para cada $i \in I$ tales que

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

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

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

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

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

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

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

por construcción, sabemos que corresponde a un epimorfismo, y la propiedad *b*) nos asegura que $\ker f = (\vec{0})_{i\in I}$, por ende es un monomorfismo.

c) $\implies$ *a*). También por contradicción, sea $\boldsymbol{m} \in M$ con dos descomposiciones

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

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

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

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

3.2. La categoría de módulos*

Definición 3.15: Sean M, N un par de A-módulos, se define $M \times N$ con

$$(\boldsymbol{x}, \boldsymbol{y}) + (\boldsymbol{z}, \boldsymbol{w}) := (\boldsymbol{x} + \boldsymbol{z}, \boldsymbol{y} + \boldsymbol{w}), \quad \lambda(\boldsymbol{x}, \boldsymbol{y}) := (\lambda\boldsymbol{x}, \lambda\boldsymbol{y}).$$

para todo $\boldsymbol{x}, \boldsymbol{z} \in M$, $\boldsymbol{y}, \boldsymbol{w} \in N$ y $\lambda \in A$.

El producto directo se puede generalizar a una familia $\{M_i\}_{i\in I}$ de A-módulos, cuyos elementos son:

$$(\boldsymbol{m}_i)_{i\in I} \in \prod_{i\in I} M_i \iff \forall i \in I\ \boldsymbol{m}_i \in M_i$$

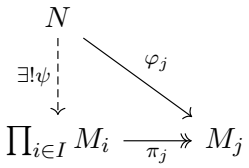
y cuyas operaciones son:

$$(\boldsymbol{m}_i)_{i\in I} + (\boldsymbol{n}_i)_{i\in I} := (\boldsymbol{m}_i + \boldsymbol{n}_i)_{i\in I}, \qquad \lambda \cdot (\boldsymbol{m}_i)_{i\in I} := (\lambda\boldsymbol{m}_i)_{i\in I}.$$

Proposición 3.16: Sea $\{M_i\}_{i\in I}$ una familia de A-módulos, entonces:

1. Las proyecciones $\pi_j \colon \prod_{i\in I} M_i \to M_j$ son morfismos de A-módulos para todo $j \in I$.

2. Si $\{\varphi_i \colon T \to M_i\}$ es una familia de morfismos de A-módulos, entonces $\psi := \Delta_{i\in I}\, \varphi_i \colon T \to \prod_{i\in I} M_i$ es el único morfismo de A-módulos tal que el siguiente diagrama: $\psi := \Delta_{i\in I}\, \varphi_i \colon T \to \prod_{i\in I} M_i$ es el único morfismo de A-módulos tal que el siguiente diagrama:



   conmuta para todo $j \in I$.

En consecuencia, el producto de A-módulos es un producto categorial. El resultado también aplica para k-espacios vectoriales.

Definición 3.17: Sea $\{M_i\}_{i\in I}$ una familia de A-módulos, entonces su suma directa se define como:

$$\coprod_{i\in I} M_i := \bigoplus_{i\in I} M_i \subseteq \prod_{i\in I} M_i.$$

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 $\coprod_{i\in I} M_i$ 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:

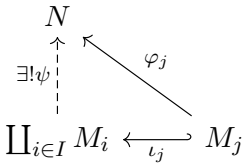
$$k[x] \cong \coprod_{n\in\mathbb{N}} \langle x^n \rangle.$$

Proposición 3.18: Sea $\{M_i\}_{i\in I}$ una familia de A-módulos, entonces:

1. Las inclusiones canónicas $\iota_j \colon M_j \to \coprod_{i\in I} M_i$ son morfismos de A-módulos para todo $j \in I$.
2. Si $\{\varphi_i \colon M_i \to N\}$ es una familia de morfismos de A-módulos, entonces

$$\begin{aligned} \psi := \left(\textstyle\sum_{i\in I} \varphi_i\right) \colon \coprod_{i\in I} M_i &\longrightarrow N \\ \sum_{i\in I} \boldsymbol{m}_i &\longmapsto \sum_{i\in I} \varphi_i(\boldsymbol{m}_i) \end{aligned}$$

   es el único morfismo de A-módulos tal que el siguiente diagrama:



   conmuta para todo $j \in I$.

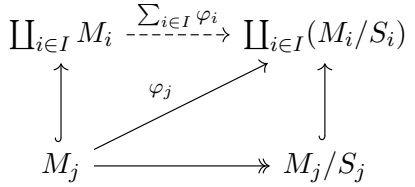
   (Nótese que ψ está bien definido ya que sólo finitos de los $\boldsymbol{m}_i$'s son no nulos.)

En consecuencia, la suma directa de A-módulos es un coproducto categorial. El resultado también aplica para k-espacios vectoriales.

Proposición 3.19: 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:

$$\coprod_{i\in I} \left(\frac{M_i}{S_i}\right) \cong \frac{\coprod_{i\in I} M_i}{\coprod_{i\in I} S_i}.$$

Demostración: Considere el siguiente diagrama conmutativo:



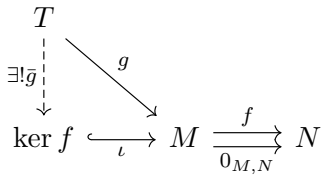
Donde la flecha punteada existe por propiedad universal del coproducto. Finalmente, es claro que $\psi := \sum_{i\in I}\varphi_i$ es suprayectiva, así que basta notar que $\ker\psi = \coprod_{i\in I} S_i$ para concluir el teorema. □

Proposición 3.20: $A^n \times A^m \cong A^n \amalg A^m \cong A^{n+m}$.

Una ventaja del lenguaje categórico es una mejor descripción del (co)núcleo:

Proposición 3.21: Sea $f\colon M \to N$ un morfismo de A-módulos. Entonces:

1. $\iota\colon \ker f \to M$ es un morfismo de A-módulos tal que $\iota \circ f = \iota \circ 0_{M,N}$, donde $0_{M,N}\colon M \to N$ es el morfismo nulo.
2. Si existe otro morfismo $g\colon T \to M$ tal que $g \circ f = g \circ 0_{M,N}$, entonces existe un único morfismo $\bar{g}\colon T \to \ker f$ tal que el siguiente diagrama conmuta:



En consecuencia, $\ker f$ es un núcleo categorial.

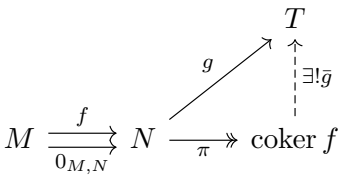
Definición 3.22: Sea $f\colon M \to N$ un morfismo de A-módulos. Puesto que $\operatorname{Img} f$ es submódulo de N se define $\operatorname{coker} f := N/\operatorname{Img} f$.

Ésto nos permite construir el siguiente objeto:

Proposición 3.23: Sea $f\colon M \to N$ un morfismo de A-módulos. Entonces:

1. $\pi\colon N \to \operatorname{coker} f$ es un morfismo de A-módulos tal que $f \circ \pi = 0_{M,N} \circ \pi$.

2. Si existe otro morfismo $g\colon N \to T$ tal que $f \circ g = 0_{M,N} \circ g$, entonces existe un único morfismo $\bar{g}\colon \operatorname{coker} f \to T$ tal que el siguiente diagrama conmuta:



En consecuencia, $\operatorname{coker} f$ es un conúcleo categorial.

El conúcleo no solo dualiza la propiedad universal del núcleo sino que también dualiza una caracterización usual de módulos:

Proposición 3.24: Sea $f\colon M \to N$ un morfismo de A-módulos. Entonces f es suprayectiva syss $\operatorname{coker} f$ es nulo.

Al igual que en Grp, es útil trabajar con las herramientas de sucesiones exactas:

Proposición 3.25: Sean M, N un par de A-módulos y $f\colon M \to N$ un morfismo de A-módulos. Entonces:

1. f es inyectiva syss $0 \longrightarrow M \xrightarrow{f} N$ es una sucesión exacta.

2. f es suprayectiva syss $M \xrightarrow{f} N \longrightarrow 0$ es una sucesión exacta.

3. f es isomorfismo syss $0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$ es una sucesión exacta.

4. Para todo $T \leq M$ submódulo se cumple que

$$0 \longrightarrow T \xrightarrow{\iota} M \xrightarrow{\pi} M/T \longrightarrow 0$$

es una sucesión exacta.

Podemos reescribir los teoremas de isomorfismos en lenguaje de sucesiones exactas:

Teorema 3.26: Se cumplen:

1. Si $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ es una sucesión exacta, entonces

$$M \cong \operatorname{Img} f = \ker g, \qquad T \cong N/\operatorname{Img} f = \operatorname{coker} f.$$

2. Sean S, T submódulos de M, entonces el siguiente diagrama conmuta y las filas son exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S \cap T & \longrightarrow & S & \longrightarrow & \dfrac{S}{S \cap T} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} & & \downarrow & & \\ 0 & \longrightarrow & T & \longrightarrow & S+T & \longrightarrow & \dfrac{S+T}{T} & \longrightarrow & 0 \end{array}$$

3. Si $S \leq T \leq M$, entonces existe una sucesión exacta:

$$0 \longrightarrow S/T \longrightarrow M/T \longrightarrow M/S \longrightarrow 0$$

Definición 3.27: Se dice que una sucesión exacta

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

se escinde si existe un $h\colon T \to N$ tal que $h \circ g = \mathrm{Id}_T$. A veces se emplea como una flecha punteada en el mismo diagrama de la sucesión exacta.

Proposición 3.28: Si una sucesión exacta

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

se escinde, entonces $N \cong M \oplus T = \ker g \oplus \operatorname{coker} f$.

Demostración: Sea $h\colon T \to N$ tal que $h \circ g = \mathrm{Id}_T$, veremos que $N = \operatorname{Img} f \oplus \operatorname{Img} h$.

Sea $\boldsymbol{n} \in N$, luego $g(\boldsymbol{n}) \in C$ y además se cumple que $\boldsymbol{n} - h(g(\boldsymbol{n})) \in \ker g$. Luego como $\ker g = \operatorname{Img} f$, existe $\boldsymbol{m} \in M$ tal que $f(\boldsymbol{m}) = \boldsymbol{n} - h(g(\boldsymbol{n}))$, así que claramente $N = \operatorname{Img} f + \operatorname{Img} h$. Más aún, sea $\boldsymbol{n} := f(\boldsymbol{m}) = h(\boldsymbol{t})$, luego $g(\boldsymbol{n}) = g(f(\boldsymbol{m})) = \boldsymbol{t} = \vec{0}$ dado que $f \circ g = 0$, pero entonces $\boldsymbol{n} = h(\vec{0}) = \vec{0}$, así que $\operatorname{Img} f \cap \operatorname{Img} h = \{\vec{0}\}$ como se quería probar. □

Ya vimos que $\mathrm{Hom}_A(X,Y)$ es un A-módulo, así pues podemos establecer el siguiente resultado:

Proposición 3.29: Sea M un A-módulo y $f\colon X \to Y$ un morfismo de A-módulos, entonces:

$$\begin{aligned} h^f\colon \mathrm{Hom}_A(M,X) &\longrightarrow \mathrm{Hom}_A(M,Y) \\ g &\longmapsto g\circ f \end{aligned}$$

y

$$\begin{aligned} h_f\colon \mathrm{Hom}_A(Y,M) &\longrightarrow \mathrm{Hom}_A(X,M) \\ g &\longmapsto f\circ g \end{aligned}$$

son también morfismos de A-módulos.

Demostración: Sea $\boldsymbol{m}\in M$, entonces:

$$\begin{aligned} \big((g+h)\circ f\big)(\boldsymbol{m}) &= f\big((g+h)(\boldsymbol{m})\big) = f\big(g(\boldsymbol{m})+h(\boldsymbol{m})\big) \\ &= f\big(g(\boldsymbol{m})\big)+f\big(h(\boldsymbol{m})\big) = (g\circ f)(\boldsymbol{m})+(h\circ f)(\boldsymbol{m}). \end{aligned}$$

Y el producto escalar se demuestra análogamente. El resto de resultados queda al lector. □

Corolario 3.30: Para todo A-módulo M se satisface que el siguiente

$$\begin{array}{ccc} X & & \mathrm{Hom}_A(M,X) \\ {\scriptstyle f}\big\downarrow & \xRightarrow{\mathrm{Hom}_A(M,-)} & \big\downarrow{\scriptstyle h^f} \\ Y & & \mathrm{Hom}_A(M,Y) \end{array}$$

es un funtor covariante en Mod_A; y el siguiente:

$$\begin{array}{ccc} X & & \mathrm{Hom}_A(X,M) \\ {\scriptstyle f}\big\downarrow & \xRightarrow{\mathrm{Hom}_A(-,M)} & \big\uparrow{\scriptstyle h_f} \\ Y & & \mathrm{Hom}_A(Y,M) \end{array}$$

es un funtor contravariante en Mod_A. Éstos funtores se llaman *funtores de representación*.

En la teoría de conjuntos se demuestra que los funtores de representación siempre existen y están bien definidos; la sorpresa radica en que, en general, los conjuntos Hom's no suelen ser elementos de la categoría y los funtores de representación tampoco suelen traducirse en flechas de la categoría; ésto indica que la categoría Mod_A es bastante especial.

Proposición 3.31: Sean X, Y, Z un trío de A-módulos. Son equivalentes:

1. La siguiente secuencia es exacta:

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

2. La siguiente secuencia es exacta para todo M:

$$\mathrm{Hom}_A(M, X) \xrightarrow{h^f} \mathrm{Hom}_A(M, Y) \xrightarrow{h^g} \mathrm{Hom}_A(M, Z)$$

3. La siguiente secuencia es exacta para todo M:

$$\mathrm{Hom}_A(X, M) \xleftarrow{h_f} \mathrm{Hom}_A(Y, M) \xleftarrow{h_g} \mathrm{Hom}_A(Z, M)$$

Demostración: $1 \implies 2$. Sea $j \in \mathrm{Hom}_A(M, Y)$, se cumple que $j \in \ker(h^g)$ syss $j \circ g = 0$, es decir para todo $\boldsymbol{m} \in M$ se cumple que $g(j(\boldsymbol{m})) = \vec{0}$, o lo que es equivalente, $\mathrm{Img}\, j \subseteq \ker g$. Por otro lado $j \in \mathrm{Img}(h^f)$ syss $j = k \circ f$, luego $j(\boldsymbol{m}) = f(k(\boldsymbol{m}))$, por lo que $\mathrm{Img}\, j \subseteq \mathrm{Img}\, f = \ker g$, es decir, $\mathrm{Img}(h^f) = \ker(h^g)$ como se quería probar.

$2 \implies 1$. Fijemos $M = X$, entonces $h^f(\mathrm{Id}_X) = f \in \ker(h^g)$, es decir, $f \circ g = 0$ y $\mathrm{Img}\, f \subseteq \ker g$. Ahora fijemos $M = \ker g$, entonces como $\ker g \subseteq Y$ existe $\iota \in \mathrm{Hom}_A(\ker g, Y)$ y claramente $\iota \circ g = 0$ por lo que $\iota \in \ker(h^g) = \mathrm{Img}(h^f)$, luego $\iota = j \circ f$, es decir, para todo $\boldsymbol{y} \in \ker g$ se cumple que $\boldsymbol{y} \in \mathrm{Img}\, f$.

El resto son análogas. □

Proposición 3.32: Sean M_1, M_2, N un trío de A-módulos. Entonces $\mathrm{Hom}_A(M_1 \oplus M_2, N) \cong \mathrm{Hom}_A(M_1, N) \times \mathrm{Hom}_A(M_2, N)$ y $\mathrm{Hom}_A(N, M_1 \times M_2) \cong \mathrm{Hom}_A(N, M_1) \oplus \mathrm{Hom}_A(N, M_2)$ como grupos abelianos.

Demostración: Sea $\psi \in \mathrm{Hom}_A(M_1 \oplus M_2, N)$, de modo que para todo $\boldsymbol{m}_1 \in M_1, \boldsymbol{m}_2 \in M_2$ se cumple que $\psi(\boldsymbol{m}_1 + \boldsymbol{m}_2) = \psi(\boldsymbol{m}_1) + \psi(\boldsymbol{m}_2)$. Definamos $\varphi_i \colon M_i \to N$ como $\varphi_i(\boldsymbol{m}_i) := \psi(\boldsymbol{m}_i)$. Finalmente, nótese que por definición se cumple que $\psi = \varphi_1 + \varphi_2$, y así es fácil notar que son isomorfos como grupos. □

3.3. Módulos libres y bases

Definición 3.33: Sea M un A-módulo con $X \subseteq M$. Diremos que X es *libre* o que sus elementos son *linealmente independientes* syss la ecuación

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

se da con $\boldsymbol{x}_i \in X$ distintos dos a dos y $\lambda_i \in A$ siempre que $\lambda_i = 0$ para todo $i = 0, \ldots, n$. De lo contrario decimos que el conjunto está *ligado* o que hay elementos que son *linealmente dependientes* entre sí.

Si, X es un conjunto libre y además es un sistema generador, diremos que X es una *base* de dicho módulo. Si M posee alguna base, entonces, se dice que es *libre*.

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

§3.3.1 Finitamente generados.

Definición 3.34: Se dice que un A-módulo M es *finitamente generado* si posee un sistema generador finito. Otra manera de decir lo mismo, pero que será útil más adelante, es que existe alguna tupla $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ tal que el morfismo de módulos

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

es suprayectivo.

Ejemplo. Consideremos $\mathbb{Q}[x]$ que, como ya vimos, corresponde a un $\mathbb{Q}$-espacio vectorial o un $\mathbb{Q}$-módulo. Nótese sin embargo que no está finitamente generado, puesto que si $\{p_1(x), \ldots, p_n(x)\}$ es un subconjunto finito de polinomios sobre $\mathbb{Q}$ basta tomar d como el grado máximo entre ellos y notar que $x^{d+1} \in \mathbb{Q}[x]$ no está generado por ellos.

Teorema 3.35: Sea M un A-módulo, entonces $M \cong A^n$ syss posee una base de cardinal n.

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

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

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

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

Lema 3.36: Si S es ligado en un espacio vectorial, entonces existe un $\boldsymbol{v} \in S$ que es generado por el resto, es decir, tal que $\boldsymbol{v} \in \langle S \setminus \{\boldsymbol{v}\}\rangle$.

Teorema 3.37: Si G es un sistema generador ligado, entonces $\boldsymbol{v} \in G$ está generado por el resto de G syss $G \setminus \{\boldsymbol{v}\}$ es un sistema generador. Si S es libre en un espacio vectorial y $\boldsymbol{v}$ no es generado por S, entonces $S \cup \{\boldsymbol{v}\}$ es libre.

Corolario 3.38: Todo sistema generador finito en un espacio vectorial contiene una base. En consecuencia, todo espacio vectorial finitamente generado es libre.

Teorema 3.39: Todo par de bases de un espacio vectorial finitamente generado posee el mismo cardinal.

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

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

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

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

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

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

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

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

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

de modo que si $B_2 := B_1 \setminus \{\boldsymbol{x}_2\} \cup \{\boldsymbol{y}_2\}$ entonces B_2 es base.

Iterando el proceso anterior, B_n resulta ser base y estar formado solamente a partir de elementos de Y, luego $Y = B_n$ pues de tener elementos aparte sería ligado y es claro que B_n posee n elementos. □

Corolario 3.40: Todo conjunto libre en un espacio vectorial finitamente generado se puede extender a una base.

Definición 3.41 – *Dimensión*: Si V es un $\Bbbk$-espacio vectorial y sus bases son equipotentes, entonces denotamos por $\dim_{\Bbbk} V$ al cardinal de cualquiera de ellas.

Corolario 3.42: Si S es libre en un espacio vectorial de dimensión finita n y S posee n elementos, entonces S es base.

Teorema 3.43: Si V, W son $\Bbbk$-espacios vectoriales que comparten dimensión finita, entonces son isomorfos. En consecuencia si $n := \dim_{\Bbbk} V$, entonces $V \cong \Bbbk^n$.

Definición 3.44 – *Base canónica*: Se le llama *base canónica* de $\Bbbk^n$ como $\Bbbk$-espacio vectorial a la base ordenada $(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$ donde

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

Por ejemplo, la base canónica de $\Bbbk^2$ es

$$\boldsymbol{e}_1 := (1, 0), \qquad \boldsymbol{e}_2 := (0, 1).$$

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

§3.3.2 Espacios de dimensión infinita. Es sencillo notar que para todo cuerpo $\Bbbk$ se cumple que $\Bbbk[x]$ es un $\Bbbk$-espacio vectorial y que $\{1, x, x^2, \dots\}$ es una base, sin embargo, generalizar sus propiedades es mucho más difícil que en el caso finito e inevitablemente hay que recurrir al axioma de elección.

Teorema 3.45: Son equivalentes:

1. **El axioma de elección.**
2. Todo conjunto libre en un espacio vectorial está contenido en una base.
3. Todo espacio vectorial es un módulo libre.

Demostración: (1) $\implies$ (2). Aplicamos el lema de Zorn: Sea S un conjunto libre, luego se define $\mathcal{F}$ como la familia de conjuntos libres que contienen a S, es claro que $\mathcal{F}$ está parcialmente ordenado por la inclusión, y por el lema anterior un elemento maximal de $\mathcal{F}$ sería una base que conteniera a S. Sea $\mathcal{C}$ una cadena de $\mathcal{F}$ hay que probar que $T := \bigcup \mathcal{C} \in \mathcal{F}$ para poder aplicar el lema de Zorn, y es claro que $S \subseteq T$, luego sólo falta probar que T es libre, lo que queda al lector (Hint: Use prueba por contradicción).

(2) $\implies$ (3). Trivial.

(3) $\implies$ (1). Probaremos que implica el axioma de elecciones múltiples, que es equivalente al AE: Sea $\{X_i : i \in I\}$ una familia de conjuntos no vacíos, hemos de probar que existe $\{F_i : i \in I\}$ tal que $F_i \subseteq X_i$ y los F_is son finitos. Definamos $X := \bigcup_{i\in I} X_i$, si $\Bbbk$ es un cuerpo arbitrario, entonces $\Bbbk(X)$ es el cuerpo de polinomios con indeterminadas en X. Se le llama i-grado de un monomio a la suma de exponentes de las indeterminadas de X_i. Se dice que una función racional $f \in \Bbbk(X)$ es i-homogéneo de grado d si todos los monomios del denominador tienen un i-grado común de n y los del numerador un i-grado común de $n+d$. Denotamos K al subconjunto de $\Bbbk(X)$ conformado por las funciones racionales i-homogéneas de grado 0 para todo $i \in I$; K resulta ser un subcuerpo estricto de $\Bbbk(X)$ (¿por qué?), luego $\Bbbk(X)$ es un K-espacio vectorial. Finalmente denotamos por V al K-subespacio de $\Bbbk(X)$ generado por X, y por B a una base de V.
Por definición de B y en particular para $x \in X_i$ existe un subconjunto finito $B(x)$ de B tal que

$$x = \sum_{v\in B(x)} \lambda_{v,x} v$$

donde $\lambda_{v,x} \in K_{\neq 0}$. Nótese que si $y \in X_i$ es distinto de x, entonces

$$y = (y/x)\, x = \sum_{v \in B(x)} (y/x \cdot \lambda_{v,x}) v$$

donde $y/x \cdot \lambda_{v,x} \in K_{\neq 0}$, luego los $B(x)$ y los $\lambda_{v,x}/x$ son fijos para un X_i fijo, por lo que le denotamos por B_i y $\beta_{v,i}$ resp.
Finalmente $\beta_{v,i}$ es i-homogéneo de grado -1 y j-homogéneo de grado 0 para todo $j \neq i$. Así que $\beta_{v,i}$ debe tener finitos términos de X_i, luego llamamos F_i al subconjunto de X_i que tienen términos en algún $\beta_{v,i}$ para algún $v \in B_i$. □

Teorema 3.46: Son equivalentes:

1. **El axioma de elección**.

2. En un espacio vectorial, todo generador contiene una base.

Pista: Siga la prueba anterior. □

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) 3.47: 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 $f : Y \to X \times \mathbb{N}$ tal que $f(y)$ es un par (x, i) donde y es el i-ésimo elemento de Y_x. Nótese que f es inyectiva, para finalizar, como X es infinito y se asume AE se cumple que $\aleph_0 \leq |X|$ de modo que $|X \times \mathbb{N}| = |X|$ y existe una biyección $g : X \times \mathbb{N} \to X$, luego $f \circ g : Y \to X$ es una inyección, y análogamente se construye otra inyección desde X a Y. Finalmente, por el

teorema de Cantor-Schröder-Bernstein, existe una biyección entre X e Y, que es lo que se quería probar. □

Observe que, al contrario del caso finito, un conjunto libre puede tener cardinal la dimensión y no ser base. En efecto, basta tomar una base de cardinal infinito y quitarle un elemento cualquiera como ejemplo.

§3.3.3 Fórmulas con la dimensión.

Teorema 3.48: Si V es un espacio vectorial y $W \leq V$, entonces:

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

Demostración:

1. Sea B_W una base de W, sabemos que se puede extender a una base B_V de V, simplemente basta ver que $B := \{[\boldsymbol{v}] : \boldsymbol{v} \in B_V \setminus B_W\}$ conserva el cardinal deseado y que es base de V/W. Sean $\boldsymbol{u}, \boldsymbol{v} \in B_V \setminus B_W$, si $[\boldsymbol{u}] = [\boldsymbol{v}]$ entonces $\boldsymbol{u} - \boldsymbol{v} \in W$, luego B_V sería ligado lo que es absurdo, análogamente se prueba que B es libre. Para notar que B es un sistema generador, basta considerar que todo $[\boldsymbol{v}] \in V/W$ se escribe como

$$\boldsymbol{v} = \sum_{i=1}^{n} \lambda_i \boldsymbol{e}_i$$

donde $e_i \in B_V$, luego

$$[\boldsymbol{v}] = \sum_{i=1}^{n} \lambda_i [\boldsymbol{e}_i],$$

donde $[\boldsymbol{e}_i]$ o pertenece a B, o es nulo, en cuyo caso podemos omitirle. De este modo, es claro que B es base.

2. Si B es base de W y tiene el mismo cardinal de $\dim V$ que es finito, entonces es base de V, de modo que $V = \langle B \rangle = W$. □

Teorema 3.49 – *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 3.50: Si $f : V \to W$ es lineal, entonces

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

3.4. Matrices y transformaciones lineales

Teorema 3.51: Sea $f : X \to N$ donde X es base de un A-módulo M y N es otro A-módulo. Entonces existe un único homomorfismo de módulos $\bar{f} : M \to N$ tal que $\bar{f}|_X = f$.

Teorema 3.52: Si $f \in L(V, W)$, entonces:

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

Corolario 3.53: Dos espacios vectoriales son isomorfos syss comparten dimensión.

Definición 3.54: Si $B := (e_i)_{i \in I}$ es una base (ordenada) de un A-módulo M, entonces $\pi_i^B : M \to A$ son la serie de aplicaciones tal que para todo $v \in M$ se cumple que

$$v = \sum_{i \in I} \pi_i^B(v) e_i.$$

Sabemos que para cada $i \in I$, las proyecciones π_i^B están bien definidas. Se define $\pi^B : M \to A^I$ la función tal que $\pi^B(v) := (\pi_i^B(v))_{i \in I}$.

De este modo si $v = 2e_1 + 3e_2 - 1e_3$ donde $B := (e_1, e_2, e_3)$ es una base ordenada de un módulo que contiene a v, entonces $\pi^B(v) = (2, 3, -1)$.

Proposición 3.55: Si $X := (x_1, \ldots, x_n)$ es base ordenada de M, entonces

1. Para todo i se cumple que π_i^X es un funcional.

2. Para todo i, j se cumple que $\pi_i^X(x_j) = \delta_{ij}$.

3. π^X es un isomorfismo con A^n.

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

Supongamos entonces que si $f : M \to N$ es un morfismo de módulos y M es libre, entonces f queda completamente determinado por una tupla de N correspondiente a la imagen de la base. Si además N es libre, entonces cada vector de N puede escribirse como una tupla de valores del anillo A. En sintesis, si el dominio y codominio son libres todo el homomorfismo se reduce a tuplas de tuplas de valores de A. Esto sucede más fácilmente si nos restringimos a espacios vectoriales, y en particular si éstos son de dimensión finita, en cuyo caso se cumple que toda la transformación lineal puede reducirse a $n \cdot m$ escalares, donde n es la dimensión del dominio y m la del codominio.

Definición 3.56 – *Matrices*: Una matriz M sobre un anillo unitario A de orden $n \times m$ es una función $M : \{1, \ldots, n\} \times \{1, \ldots, m\} \to A$, donde solemos denotar $M(i, j)$ como M_{ij}. A éstos últimos valores les decimos sus *coeficientes*. El conjunto de matrices sobre A de $n \times m$ se denota $\mathrm{Mat}_{n\times m}(A)$. El conjunto $\mathrm{Mat}_{n\times m}(A)$ es un A-módulo, en donde:

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

2. $(\lambda B)_{ij} := \lambda B_{ij}$ para todo $B \in \mathrm{Mat}_{n\times m}(A)$ y $\lambda \in A$.

La diagonal de una matriz se le llama al conjunto de coeficientes de coordenadas (i, i).

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

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

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

Se les llama matrices:

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

Simétricas A las matrices cuadradas B tal que $B = B^t$.

Antisimétricas A las matrices cuadradas B tal que $B = -B^t$.

Diagonales A las que tienen coeficientes nulos en todas las coordenadas exceptuando tal vez la diagonal.

Escalares A las matrices diagonales que en la diagonal sólo contienen un valor escalar.

Identidad A la matriz escalar con valor 1. La matriz identidad de orden $n \times n$ se denota I_n.

Nula A la matriz escalar con valor 0.

Por lo general, denotaremos los valores de la matriz en una tabla, por ejemplo

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

donde $M_{2,1} = 4$.

Cabe destacar que si

$$B_{ij} = f(i,j)$$

para todo i, j; entonces también denotaremos

$$B = [f(i,j)]_{ij}$$

de modo que, por ejemplo

$$I_n = [\delta_{ij}]_{ij}.$$

En general admitiremos que A^n corresponde a $\mathrm{Mat}_{1\times n}(A)$, de modo que $\pi^X(\boldsymbol{v}) \in \mathrm{Mat}_{1\times n}(A)$.

Proposición 3.57: $\mathrm{Mat}_{n\times m}(A)$ es un A-módulo libre de rango nm.

Proposición 3.58: Si B, C, D son matrices de orden apropiado en cada caso, se cumple:

1. $B \cdot (C \cdot D) = (B \cdot C) \cdot D$ (asociatividad).
2. $B \cdot (C + D) = B \cdot C + B \cdot D$ (distributividad izquierda).
3. $(B + C) \cdot D = B \cdot D + C \cdot D$ (distributividad derecha).
4. Si B es de orden $n \times m$, entonces $I_n \cdot B = B \cdot I_m = B$ (neutro).

5. $\mathrm{Mat}_n(A)$ es un anillo unitario de neutro aditivo la matriz nula y neutro multiplicativo la matriz identidad.

Proposición 3.59: 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 3.60: Si $f \in L(\mathbb{k}^n, \mathbb{k}^m)$, y $X := (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n), Y := (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ son bases ordenadas de $\mathbb{k}^n$ y $\mathbb{k}^m$ resp., entonces denotamos $\mathrm{M}_X^Y(f)$ a la matriz de orden $n \times m$ a aquella tal que sus columnas son las imagenes ordenadas de la base X, dicho de otro modo que $\mathrm{M}_X^Y(f) := \left[\pi_j^Y\left(f(\boldsymbol{x}_i)\right)\right]_{ij}$.

Teorema 3.61: 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 $B = \mathrm{M}_X^Y(f)$ syss para todo $\boldsymbol{v} \in \mathbb{k}^n$ se cumple:

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

Demostración: $\Longrightarrow$. Sea $X = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$, $\boldsymbol{v} = \sum_{i=1}^n v_i \boldsymbol{x}_i$ y $B := \mathrm{M}_X^Y(f)$, luego como f es lineal se cumple que

$$f(\boldsymbol{v}) = \sum_{i=1}^n v_i f(\boldsymbol{x}_i).$$

Las proyecciones son también lineales, luego

$$\pi_j^Y(f(\boldsymbol{v})) = \sum_{i=1}^n v_i \pi_j^Y[f(\boldsymbol{x}_i)] = \sum_{i=1}^n v_i b_{ij} = (\pi^X(\boldsymbol{v}) \cdot B)_{1j},$$

como se quería probar.

$\Longleftarrow$. Si se cumple para todo vector, en particular se cumple para los vectores de la base X y claramente

$$\left(\mathrm{M}_X^Y(f)\right)_{ij} = \pi_j^Y(f(\boldsymbol{x}_i)) = \sum_{k=1}^n \delta_{ik} b_{kj} = b_{ij}$$

ergo $B = \mathrm{M}_X^Y(f)$. □

Ejemplo (matriz cambio de base). Sea V un $\Bbbk$-espacio vectorial de dimensión n. Sean $X, Y = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ bases ordenadas de V, luego

$$\pi^X(\boldsymbol{v}_i) = \pi^X(\mathrm{Id}(\boldsymbol{v}_i)) = \pi^Y(\boldsymbol{v}_i) \cdot \mathrm{M}_Y^X(\mathrm{Id}) = \boldsymbol{e}_i \, \mathrm{M}_Y^X(\mathrm{Id}) = [\mathrm{M}_X^Y(\mathrm{Id})]_{i,*}.$$

Teorema 3.62: Si f, g son funciones lineales y X, Y, Z son bases ordenadas adecuadas a las dimensiones en cada caso, se cumple:

1. $\mathrm{M}_X^X(\mathrm{Id}) = I_n$, donde $n = |X|$.
2. Para todo λ escalar se cumple $\mathrm{M}_X^Y(\lambda f) = \lambda \, \mathrm{M}_X^Y(f)$.
3. $\mathrm{M}_X^Y(f + g) = \mathrm{M}_X^Y(f) + \mathrm{M}_X^Y(g)$.
4. $\mathrm{M}_X^Z(f \circ g) = \mathrm{M}_X^Y(f) \cdot \mathrm{M}_Y^Z(g)$.
5. Son equivalentes:
   a) f es invertible.
   b) Para algún par de bases ordenadas X, Y se da que $\mathrm{M}_X^Y(f)$ es invertible.
   c) Para todo par de bases ordenadas X, Y se da que $\mathrm{M}_X^Y(f)$ es invertible.
6. $L(\Bbbk^n, \Bbbk^m) \cong \mathrm{Mat}_{n \times m}(\Bbbk) \cong \Bbbk^{nm}$. En particular, $L(\Bbbk^n, \Bbbk) \cong \Bbbk^n$.

Los últimos dos son los que justifican la definición de matrices.

Ejemplo. Si X, Y son bases ordenadas de $\Bbbk^n$, entonces

$$I_n = \mathrm{M}_X^X(\mathrm{Id}) = \mathrm{M}_X^Y(\mathrm{Id}) \cdot \mathrm{M}_Y^X(\mathrm{Id}).$$

Luego si $B \in \mathrm{Mat}_n(\Bbbk)$ es invertible, entonces representa a una única matriz de cambio de base. De hecho, todo endomorfismo $f \in L(\Bbbk^n)$ está representado por la familia

$$\mathrm{M}_Y^Y(f) = \mathrm{M}_Y^X(\mathrm{Id}) \cdot \mathrm{M}_X^X(f) \cdot \mathrm{M}_X^Y(\mathrm{Id}).$$

Teorema 3.63: Si $B \in \mathrm{Mat}_n(\Bbbk)$, entonces son equivalentes:

1. B es invertible.

2. Para todo $\boldsymbol{v} \in \mathbb{k}^n$ se cumple que $\boldsymbol{v} \cdot B = 0$ implica $\boldsymbol{v} = 0$.

DEMOSTRACIÓN: $\Longrightarrow$. Si B es invertible entonces sea B^{-1} su inversa, luego $v = (v \cdot B)B^{-1} = 0 \cdot B^{-1} = 0$.

$\Longleftarrow$. Si X es la base canónica, entonces $f(\boldsymbol{v}) := \boldsymbol{v} \cdot B$ claramente es lineal y cumple que $B = \mathrm{M}_X^X(f)$ (¿por qué?). Si $f^{-1}(\mathbf{0}) = \{\mathbf{0}\}$, entonces $\dim \ker f = 0$, luego $\dim \operatorname{Img} f = n$ y f es una biyección, luego es invertible, y por el teorema anterior, cualquiera de sus representaciones matriciales (en particular, B) lo son. □

3.5. Determinante

Definición 3.64 – *Forma multilineal*: Se dice que una función $f : (A^n)^n \to A$ es una *forma multilineal* si es lineal coordenada a coordenada, es decir, si para todo $v_1, \ldots, v_n, v \in A^n$ y todo $\lambda \in A$ se cumple que

$$f(v_1, \ldots, \underset{(i)}{v_i + \lambda v}, \ldots, v_n) = f(v_1, \ldots, v_n) + \lambda f(v_1, \ldots, \underset{(i)}{v}, \ldots, v_n).$$

Además, una forma multilineal se dice *antisimétrica* si intercambiar dos vectores de coordenadas cambia el signo, es decir si

$$f(v_1, \ldots, \underset{(i)}{v_i}, \ldots, \underset{(j)}{v_j}, \ldots, v_n) = -f(v_1, \ldots, \underset{(i)}{v_j}, \ldots, \underset{(j)}{v_i}, \ldots, v_n).$$

Y también se dice *alternada* si es nula si un vector aparece en más de una coordenada, es decir si

$$f(v_1, \ldots, \underset{(i)}{v}, \ldots, \underset{(j)}{v}, \ldots, v_n) = 0.$$

Proposición 3.65: 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:
$$f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = (\operatorname{sgn}\sigma) \cdot f(v_1, \dots, v_n).$$

Teorema 3.66: 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
$$f(v_1, \dots, v_n) = a \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \cdot v_{1\sigma(1)} \cdots v_{n\sigma(n)}.$$

Demostración: Utilizando la notación del enunciado $v_i = \sum_{j=1}^n v_{ij} e_j$, luego
$$\begin{aligned} f(v_1, \dots, v_n) &= \sum_{j=1}^n v_{1j} f(e_j, v_2, \dots, v_n) \\ &= \sum_{j_1=1}^n \sum_{j_2=1}^n v_{1j_1} v_{2j_2} f(e_{j_1}, e_{j_2}, v_3, \dots, v_n) \\ &= \sum_{j_1=1}^n \cdots \sum_{j_n=1}^n v_{1j_1} \cdots v_{nj_n} f(e_{j_1}, \dots, e_{j_n}). \end{aligned}$$

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:
$$\begin{aligned} f(v_1, \dots, v_n) &= \sum_{\sigma \in S_n} v_{1\sigma(1)} \cdots v_{n\sigma(n)} f(e_{\sigma(1)}, \dots, e_{\sigma(n)}) \\ &= a \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \cdot v_{1\sigma(1)} \cdots v_{n\sigma(n)} \end{aligned}$$
□

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 3.67 – *Determinante*: Se define la función determinante $\det : \operatorname{Mat}_n(A) \to A$ como la única forma multilineal tal que $\det(I_n) = 1$.

Algunos textos usan $|B|$, pero éste **no**, para evitar confusiones.

Algo que destacar es que el cálculo de matrices se vuelve, en casos generales, exponencialmente más complejo de acuerdo a las dimensiones de las matrices, ésto es fácil de ver ya que $|S_n| = 2^n$, luego el determinante comprende una herramienta sólo en casos particulares, en matrices pequeñas o en contextos teóricos.

Proposición 3.68 (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 3.69: Para toda matriz B cuadrada se cumple $\det(B^t) = \det(B)$.

Teorema 3.70: Para todos $B, C \in \mathrm{Mat}_n(\mathbb{k})$ 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, $B = (B_1, \ldots, B_n)$ donde $B_1 = (b_{11}, \ldots, b_{1n})$. Luego si $B' := (B_1, \ldots, B_u + \lambda \boldsymbol{v}, \ldots, B_n)$, $D := BC$ y $D' := B'C$, entonces

$$D'_{ij} = \sum_{k=1}^{n} B'_{ik} C_{kj}$$

luego si $i \neq u$, entonces $D'_{ij} = D_{ij}$. Si $i = u$, entonces $D'_{u,*} = D_{u,*} + \lambda(\boldsymbol{v}C)_*$, y como el determinante es multilineal sobre columnas y filas (por traspuesta) se comprueba también la multilinealidad de f.
Para ver que es alternada notamos que si B repite columnas, D repite filas, luego como el determinante es alternado también por filas, f toma valor nulo.

Finalmente para calcular la constante a evaluamos en I_n lo que da $\det C$ y comprueba el enunciado. □

Definición 3.71 (Menor complemento): Dada una matriz $B \in \mathrm{Mat}_n(A)$ con $n > 1$, se le llama *menor complemento*, denotado $M_{ij}(B)$, de la coordenada (i, j) al determinante de la matriz resultante de eliminar la i-ésima fila y j-ésima columna de B.

Proposición 3.72: Si $B \in \mathrm{Mat}_n(A)$ con $n > 1$, entonces para todo $i, j \leq n$ se cumple que

$$\det B = \sum_{k=1}^{n} (-1)^{i+k} b_{ik} M_{ik}(B) = \sum_{k=1}^{n} (-1)^{k+j} b_{kj} M_{kj}(B). \tag{3.1}$$

Definición 3.73 (Matriz adjunta): Dada una matriz $B \in \mathrm{Mat}_n(A)$ con $n > 1$, se le llama *matriz adjunta*, denotado $\operatorname{adj} B$, a la matriz

$$\operatorname{adj} B := \left[(-1)^{i+j} M_{ji}(B)\right]_{ij}.$$

Teorema 3.74: Para todo $B \in \mathrm{Mat}_n(D)$ con $n > 1$ se cumple que

$$B \cdot \operatorname{adj} B = \operatorname{adj} B \cdot B = (\det B) \cdot I_n. \tag{3.2}$$

En consecuencia, B es invertible syss $\det B$ es invertible, en cuyo caso, $B^{-1} = \frac{1}{\det B} \operatorname{adj} B$. Si D es un cuerpo, la condición se reduce a notar que las matrices invertibles son las de determinante no nula.

Proposición 3.75: Se cumple:

1. $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$
2. $\operatorname{adj} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$
3. $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = aei + bfg + cdh - (afh + bdi + ceg)$ (regla de Sarrus).

Una técnica de mnemotecnia se basa en la fig. 3.1, donde las diagonales verdes se suman y las rojas se restan.

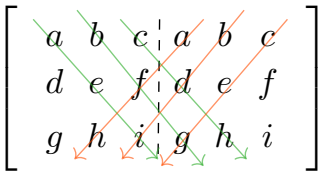


Figura 3.1. Regla de Sarrus.

§3.5.1 Rango de matrices.

Definición 3.76: Dada $A \in \mathrm{Mat}_{n\times m}(\mathbb{k})$ se le dice *rango por filas* (resp. por columnas) a la dimensión del subespacio generado por sus vectores fila (resp. vectores columna).

Lema 3.77: El rango por filas, el rango por columnas y la dimensión de la imagen de una matriz concuerdan.

DEMOSTRACIÓN: Sean r_f y r_c el rango por filas y por columnas resp. de una matriz fijada $A \in \mathrm{Mat}_{n\times m}(\mathbb{k})$. Sin perdida de generalidad supongamos que las filas están ordenadas de tal manera que las primeras r_f son linealmente independientes, luego para todo i se cumple que

$$A_{i,*} = \sum_{k=1}^{r_f} \lambda_{ik} A_{k,*}$$

es decir que para todo i, j:

$$A_{ij} = \sum_{k=1}^{r_f} \lambda_{ik} A_{kj}.$$

Donde $\lambda_{ij} = \delta_{ij}$ si $i \leq r_f$; en definitiva si $B := [\lambda_{ij}]_{ij}^t$ que es una matriz de $r_f \times n$ vemos que se cumple que

$$A = B^t A \iff A^t = A^t B \iff A_{*,j} = \sum_{k=1}^{r_f} A_{jk}^t B_{k,*}$$

Luego $(B_{k,*})_{k=1}^{r_f}$ es un sistema generador de las columnas de A, es decir, $r_c \leq r_f$. Análogamente se deduce la otra desigualdad. □

Definición 3.78: Se le dice *rango*, denotado $\operatorname{rank}(A)$, de una de una matriz A al rango por filas o columnas.

Corolario 3.79: Para toda matriz A se cumple que $\operatorname{rank}(A) = \operatorname{rank}(A^t)$.

Teorema 3.80: Dada $A \in \operatorname{Mat}_{n\times m}(\Bbbk)$ cualquiera, y sean $B \in \operatorname{Mat}_n(\Bbbk)$ y $C \in \operatorname{Mat}_m(\Bbbk)$ invertibles. Entonces $\operatorname{rank}(A) = \operatorname{rank}(BA) = \operatorname{rank}(AC)$.

De éste modo también podemos definir el rango para transformaciones lineales ya que sería independiente de la base.

Proposición 3.81: Una matriz de $n \times n$ es invertible syss tiene rango n.

Teorema 3.82: Si $A \in \operatorname{Mat}_{n\times m}(\Bbbk)$ y $B \in \operatorname{Mat}_{m\times p}(\Bbbk)$, entonces

$$\operatorname{rank}(AB) \leq \operatorname{rank}(A), \qquad \operatorname{rank}(AB) \leq \operatorname{rank}(B).$$

Nótese que en este sentido el rango de una matriz sirve como indicador de qué tan «invertible» es.

Definición 3.83: Dada una matriz $A \in \operatorname{Mat}_{n\times m}(R)$. Una submatriz B está dado por un par de inyecciones $\sigma\colon \{1,\dots,n'\} \to \{1,\dots,n\}$ y $\tau\colon \{1,\dots,m'\} \to \{1,\dots,m\}$ tal que $B = [A_{\sigma(i),\tau(j)}]_{ij} \in \operatorname{Mat}_{n'\times m'}(R)$.

Por ejemplo, si consideramos

$$A := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

entonces algunas de sus submatrices son:

$$\begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 3 \\ 8 & 9 \end{bmatrix}.$$

Ésta definición puede parecer extraña, pero es útil para lo siguiente:

Proposición 3.84: El rango de una matriz A, es el mayor n tal que existe una submatriz de A de tamaño $n \times n$ inversible.

Demostración: Sea A de dimensiones $u \times v$. Claramente si A posee una submatriz de $n \times n$ inversible, entonces necesariamente $\operatorname{rank} A \geq n$. Por otro lado, si $\operatorname{rank} A = m$, 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 $\operatorname{rank} A \leq n$. □

4

Extensiones de cuerpo

4.1. Extensiones algebraicas

Definición 4.1 – *Extensión de cuerpos*: Dado un cuerpo k se dice que K es una *extensión de cuerpos* de k si K tiene un subcuerpo isomorfo a k, lo que abreviamos diciendo que K/k es una extensión.

Si K es una extensión de cuerpo, entonces con las operaciones usuales se puede ver como un k-espacio vectorial, de modo que llamamos su *grado* a $[K : k] := \dim_k(K)$. Si $g = [K : k]$, entonces podemos expresarlo empleando el siguiente *diagrama de retículos*:

$$\begin{array}{c} K \\ {\scriptstyle \cdot\, g}\,\big| \\ k \end{array}$$

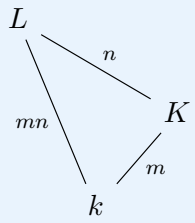
Dada una extensión K del cuerpo k, un elemento $\alpha \in K$ se dice k-*algebraico* si existe $p \in k[x]$ tal que $p(\alpha) = 0$, de lo contrario se dice k-*trascendente*. Una extensión K se dice k-algebraica si todos sus elementos lo son, de lo contrario, K se dice k-trascendente. De no haber ambigüedad 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 $S := \{1, \alpha, \ldots, \alpha^n\}$.
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

$$\sum_{i=0}^{n} c_i \alpha^i = c_n \alpha^n + \cdots + c_1 \alpha + c_0 = 0,$$

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. □

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 irreductibles 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. □

Cabe destacar que diremos que un elemento es una *raíz cuadrada* de a syss es la raíz de $x^2 - a$. Asimismo diremos que es *raíz cúbica* cuando es raíz de $x^3 - a$ y, en general, que es una *n-ésima raíz* cuando es raíz de $x^n - a$. **Ojo** que ésto no tiene nada que ver con la función real $\sqrt[n]{x}$, pues se define de otra manera (ver def. 1.50 de [Top]).

Definición 4.6: Sea k un cuerpo con $p(x) \in k[x]$ 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 irreductible $p(x) \in k[x]$ 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. $\mathrm{ev}_\alpha\left[k[x]\right] = \mathrm{ev}_\alpha\left[k(x)\right] = \{r(\alpha) : r(x) \in k[x] \wedge \deg r < \deg p\}$
4. $k(\alpha)/k$ es una extensión finita, de hecho $[k(\alpha) : k] = \deg p =: n$ y $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es base para $k(\alpha)$.

Demostración:

1. Consideremos $\pi := \mathrm{ev}_\alpha : k[x] \to k(\alpha)$ 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 irreductible.
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 irreductible, 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 $p(x)$. □

El teorema anterior nos dice que en un sentido $k(\alpha)$ es la *mínima* extensión de cuerpos que contiene a α. En el teorema 4.13 veremos una generalización del teorema anterior que no depende del cuerpo base.

Corolario 4.8: Sea K/k una extensión de cuerpos y sean $\alpha, \beta \in K$ algebraicos, entonces

$$[k(\alpha, \beta) : k] \leq [k(\alpha) : k] \cdot [k(\beta) : k].$$

En consecuencia si $S \subseteq K$ es finito y algebraico, entonces $k(S)/k$ es una extensión finita.

Demostración: Por transitividad de grados sabemos que

$$[k(\alpha, \beta) : k] = [k(\beta)(\alpha) : k(\beta)] \cdot [k(\beta) : k],$$

por ende basta notar que $[k(\beta)(\alpha) : k(\beta)] \leq [k(\alpha) : k]$. Para ello, el teorema anterior demuestra que $[k(\alpha) : k] = \deg f$, donde $f(x) \in k[x]$ es el polinomio

minimal de α. Pero $f(x) \in k(\beta)[x]$, así que por el teorema anterior se cumple que es múltiplo del polinomio minimal $g(x)$ en $k(\beta)$, por lo que $[k(\beta)(\alpha) : k(\beta)] = \deg g \leq \deg f = [k(\alpha) : k]$. □

Ejemplo. Considere $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Primero nótese que el $\mathbb{Q}$-polinomio minimal de $\sqrt{2}$ y $\sqrt{3}$ son resp.:

$$p(x) = x^2 - 2, \quad q(x) = x^2 - 3.$$

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

$$q(a + b\sqrt{2}) = a^2 + 2ab\sqrt{2} + 2b^2 - 3$$

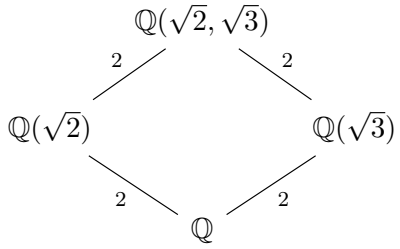
como $\mathbb{Q}(\sqrt{2})$ es un $\mathbb{Q}$-espacio vectorial de base $\{1, \sqrt{2}\}$ se concluye que

$$\begin{aligned} a^2 + 2b^2 - 3 &= 0, \\ 2ab &= 0. \end{aligned}$$

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

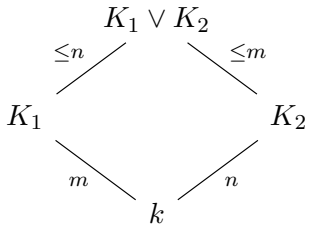
$$r(x) := 2x^2 - 3 = 0$$

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.

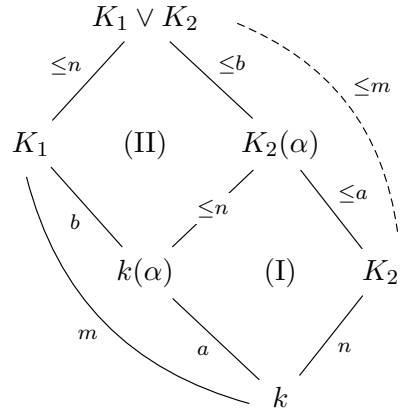
Proposición 4.10: Sean $L/K_1/k$ y $L/K_2/k$ extensiones de cuerpo con K_1, K_2 finitas. Entonces se satisface el siguiente diagrama de retículos:



Demostración: Lo demostraremos por inducción fuerte sobre $n + m$: El caso base $1 + 1$ es trivial, ya que $K_1 = K_2 = k$ y $K_1 \vee K_2 = k$.

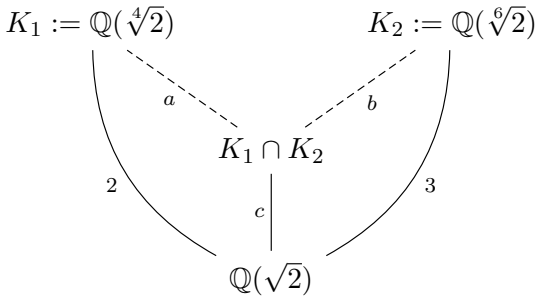
Hagamos la siguiente observación: Si $K_1 = k(\alpha)$, entonces el enunciado se satisface. La demostración es la misma del corolario 4.8, se toma el polinomio minimal de α y se nota que es también tiene raíz en $K_1 \vee K_2 = K_2(\alpha)$ como polinomio de K_2.

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:



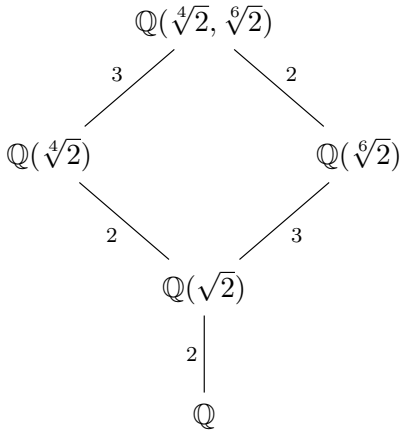
donde el diamante (I) sale de la observación, mientras que el diamante (II) sale por hipótesis inductiva. □

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 $Q(\sqrt[6]{2})$ 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 $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4n = 6$ y no existe un n entero que la satisfaga. Luego $[\mathbb{Q}(\sqrt[6]{2}, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] > 1$ y por el corolario es ≤ 2. Por ende el diagrama de retículos se ve así:



y en conclusión $[\mathbb{Q}(\sqrt[6]{2}, \sqrt[4]{2}) : \mathbb{Q}] = 12$

Teorema 4.11: Si $L/K/k$ son extensiones de cuerpos, entonces L/k es algebraica syss L/K y K/k lo son.

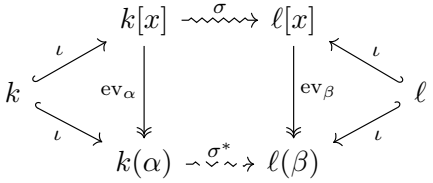
Demostración: $\Longrightarrow$. Si L/k es algebraica, claramente K/k lo es y como k es subcuerpo de K se comprueba que L/K lo es.

$\Longleftarrow$. Si $\alpha \in L$ entonces α es K-algebraico, luego sean $\beta_1, \ldots, \beta_n$ los coeficientes de su polinomio minimal, luego α es algebraico sobre $k(\beta_1, \ldots, \beta_n)$, por ende $k(\beta_1, \ldots, \beta_n)[\alpha]/k(\beta_1, \ldots, \beta_n)$ es finita, y como los β_i son k-algebraicos, entonces $k(\beta_1, \ldots, \beta_n)/k$ es finito, finalmente $k(\beta_1, \ldots, \beta_n, \alpha)/k$ es finito y luego algebraico. $\square$

Corolario 4.12: Si K/k es una extensión de cuerpos, entonces el conjunto de elementos algebraicos de K es un cuerpo.

Demostración: Basta notar que si α, β son algebraicos sobre K, entonces $k(\alpha, \beta)/k$ es finita, luego algebraica y por ende $\alpha + \beta$, $\alpha \cdot \beta$ y α/β (si $\beta \neq 0$) lo son. □

Teorema 4.13: Sean K/k y L/ℓ extensiones de cuerpo con $\sigma : k \to \ell$ un isomorfismo de cuerpo, que induce un morfismo de anillos $\sigma : k[x] \to \ell[x]$. 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 $\sigma^* : k(\alpha) \to \ell(\beta)$ con $\sigma^*(\alpha) = \beta$, es decir, existe un σ^* tal que el siguiente diagrama



conmuta (en Ring).

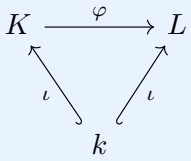
Demostración: Sea $\phi : k[x] \to k[\alpha]$ el morfismo de evaluación, i.e., tal que $\phi(g) = g(\alpha)$. Es claro que $\ker \phi$ es el ideal $(p(x))$, luego por el primer teorema de isomorfismos $k[x]/(p(x)) \cong k[\alpha]$.

En primer lugar veamos que $\sigma p(x)$ ha de ser el polinomio minimal de β en l. Luego, análogamente $l[x]/(\sigma p(x)) \cong l[\alpha]$.

Finalmente $\omega : k[x] \to l[x]$ que fija a la identidad induce un isomorfismo $k[x]/(p(x)) \cong l[x]/(\sigma p(x))$, de lo que se concluye que $k[\alpha] \cong l[\beta]$. □

Ésto nos motiva a formular la siguiente definición:

Definición 4.14: Sean K/k y L/k extensiones de cuerpo. Entonces decimos que una función $\varphi : K \to L$ es un un *k-morfismo* si es un homomorfismo de anillos tal que $\varphi(\alpha) = \alpha$ para todo $\alpha \in k$, es decir, si el siguiente diagrama



conmuta (en Ring). Las extensiones de cuerpos sobre k, como objetos, y los k-morfismos, como flechas, conforman una categoría denotada por Ext_k.

Se le llama *grupo de Galois* de K, denotado por $\mathrm{Gal}(K/k)$, al conjunto $\mathrm{Aut}_{\mathsf{Ext}_k}(K)$; vale decir, $\mathrm{Gal}(K/k)$ son los k-automorfismos de K.

Corolario 4.15: Sea K/k una extensión de cuerpo, donde $K = k(\alpha)$ y $p(x) \in k[x]$ es el polinomio minimal de α. Entonces $|\operatorname{Gal}(K/k)|$ es la cantidad de raíces distintas de $p(x)$; en particular,

$$|\operatorname{Gal}(K/k)| \leq [K : k],$$

donde $|\operatorname{Gal}(K/k)| = [K : k]$ syss $p(x)$ se factoriza en distintos polinomios lineales.

Demostración: Sean $\alpha_1, \ldots, \alpha_n$ todas las raíces de $p(x)$ en K. Por el teorema anterior siempre existe un único k-automorfismo $\sigma_{ij} : k(\alpha_i) \to k(\alpha_j)$ tal que $\sigma_{ij}(\alpha_i) = \alpha_j$. Así pues, para cada j notemos que σ_{1j} es un k-automorfismo distinto, por lo que $|\operatorname{Gal}(K/k)| \geq n$. Al mismo tiempo si σ es un k-automorfismo, entonces $p\big(\sigma(\alpha)\big) = \sigma\big(p(\alpha)\big) = 0$, de modo que $\sigma(\alpha) = \alpha_i$, pero el teorema anterior prueba la unicidad de σ, con lo que $|\operatorname{Gal}(K/k)| = n$. Como $n \leq \deg p$ se comprueba la desigualdad.

Ya vimos que $|\operatorname{Gal}(K/k)|$ es la cantidad de raíces de $p(x)$, así que la equivalencia es clara. □

Definición 4.16 (k-conjugados): Dados α, β algebraicos sobre k, se dice que son k-conjugados si comparten el polinomio minimal.

Teorema 4.17: Dados α, β algebraicos sobre k, entonces son k-conjugados syss existe un k-isomorfismo $\sigma\colon k(\alpha) \to k(\beta)$ tal que $\sigma(\alpha) = \beta$. Más aún, $\sigma(\alpha)$ siempre es un k-conjugado de α.

Ejemplo. El polinomio ciclotómico p-ésimo, con $p > 2$, es irreducible luego carece de raíces, así que construyamos $\mathbb{Q}(\omega)$ donde ω es una raíz.

Como $\Phi_p(x) \cdot (x-1) = x^p - 1$, entonces todas las raíces del polinomio son raíces p-ésimas de la unidad, ergo $\omega^p = 1$, luego $(\omega^2)^p = 1^2 = 1$, por lo que ω^2 también es raíz de $\Phi_p(x)$. De hecho, se concluye que todas las raíces de $\Phi_p(x)$ son $\omega^1, \omega^2, \ldots, \omega^{p-1}$; luego ellos son k-conjugados.

Teorema 4.18: Si K/k es finito, entonces $\mathrm{Gal}(K/k)$ también.

Demostración: Sea $S := \{\alpha_1, \ldots, \alpha_n\}$ tal que $K = k(S)$. Sea $\sigma \in \mathrm{Gal}(K/k)$ y $p \in k[S]$, como σ es un k-automorfismo se cumple $\sigma(p(\alpha_1, \ldots, \alpha_n)) = p(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$. Notemos que todo elemento en K es de la forma $p(\alpha_1, \ldots, \alpha_n)$, luego dos k-automorfismos coinciden syss 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 $\mathrm{Gal}(K/k)$ es finito. □

4.2. Extensiones normales y separables

§4.2.1 Cuerpos de escisión.

Definición 4.19: Se dice que un polinomio $p \in k[x]$ *se escinde* (en inglés, *split*) en una extensión de cuerpos K/k, si existen $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$ 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 $K = k(\alpha_1, \ldots, \alpha_n)$.

Teorema 4.20: Si $\sigma : k \to k'$ 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 $\bar{\sigma} : K \to K'$ como isomorfismo. En consecuencia, todo par de cuerpos de escisión de un mismo polinomio son k-isomorfos.

Demostración: No perdemos generalidad al suponer que p es irreductible. 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 $\sigma^* : k(\alpha_{n+1}) \to k'(\beta_{n+1})$ 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 $\bar{\sigma} : K \to K'$ es un isomorfismo de cuerpos. □

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. □

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 syss su discriminante tiene raíces, el cual es

$$\sqrt[6]{2}^2 - 4\sqrt[3]{2} = -3\sqrt[3]{2}.$$

Como $\sqrt[6]{2} \in \mathbb{R}$ se tiene que $\mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{R}$ y $\mathbb{R}$ no posee raíces de números negativos, así que $\mathbb{Q}(\sqrt[6]{2})$ tampoco; y por tanto el polinomio no se escinde.

Definición 4.22 – *Extensión normal*: Se dice que una extensión de cuerpos K/k es *normal* si para todo $p \in k[x]$ irreductible con alguna raíz en K se escinde en K.

Lema 4.23: Si $L/F/K/k$ son extensiones algebraicas de cuerpo de modo que F es un cuerpo de escisión de algún polinomio $p(x) \in k[x]$. Entonces si $\sigma : K \to L$ es un k-monomorfismo se cumple que $\sigma[K] \subseteq F$ y σ se extiende a un k-automorfismo de F, y en consecuencia, se extiende a un k-automorfismo de L. En diagramas conmutativos:

$$\begin{array}{ccc} F & \overset{\sigma^*}{\rightsquigarrow} & F \\ \uparrow & & \uparrow \mathrm{Id} \\ K & \xrightarrow{\sigma} & F \\ \uparrow & & \uparrow \\ k & \xrightarrow[\mathrm{Id}]{} & k \end{array}$$

Demostración: Supongamos que $p(x) = \alpha_0(x - \alpha_1) \cdots (x - \alpha_n)$ de modo que $F = k(\alpha_1, \ldots, \alpha_n)$. Sea $K' := \sigma[K]$ y $F' := K'(\alpha_1, \ldots, \alpha_n)$. Notemos que por definición K, K' son isomorfos, así que por el teorema anterior $\bar{\sigma} : F \to F'$ es un k-isomorfismo que exitiende a σ.

Sea $\beta \in K$, como $F = K(\alpha_1, \ldots, \alpha_n)$, entonces existe $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ tal que $g(\alpha_1, \ldots, \alpha_n) = \beta$, pero como los α_is son k-conjugados, entonces

$$\bar{\sigma}(\beta) = \bar{\sigma}(h(\alpha_1, \ldots, \alpha_n)) = h(\bar{\sigma}(\alpha_1), \ldots, \bar{\sigma}(\alpha_n)),$$

donde $\bar{\sigma}$ es una permutación de los α_i, de modo que $F' = \bar{\sigma}(F) \subseteq F$. En consecuencia $F' = F$ y $\bar{\sigma}$ es un k-automorfismo. □

Teorema 4.24: Una extensión finita K/k es normal syss es el cuerpo de escisción de algún polinomio.

Demostración: $\Longleftarrow$. Sea $p(x) \in k[x]$ el polinomio tal que K es su cuerpo de escisión. Sea $q(x) \in k[x]$ irreductible 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 $\alpha_1, \ldots, \alpha_n$, entonces $L = K(\alpha_1, \ldots, \alpha_n)$. Como α_i y α son k-conjugados, existe $\sigma : k(\alpha) \to k(\alpha_i) \subseteq L$ un k-isomorfismo, luego por el lema $k(\alpha_i) \subseteq K$, y como los $\alpha_i \in K$, $q(x)$ se escinde en K.

$\Longrightarrow$. Sea K/k normal. Como K/k es finita, existen $\alpha_1, \ldots, \alpha_n$ tales que $K = k(\alpha_1, \ldots, \alpha_n)$. 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. □

Definición 4.25: Sea K/k una extensión finita. Entonces N se dice una *clausura normal* de K si $N/K/k$ es extensión y si $N/N'/K/k$ es tal que N' es normal, entonces $N' = N$.

Proposición 4.26: Toda extensión finita posee una clausura normal que es única salvo isomorfismo.

Demostración: Sea $K = k(\alpha_1, \ldots, \alpha_n)$ y $p_i(x) \in k[x]$ 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. □

§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. $(p/q)' = \dfrac{p'q - pq'}{q^2}$.

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. □

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 $\mathrm{Frob}_k(a) = a^p$ 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 $\mathrm{car}\, D = 0$, entonces $p'(x) \neq 0$.
2. Si $\mathrm{car}\, D = p$, 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 car $k = p$, entonces k es perfecto syss Frob_k es un automorfismo.
3. Todo cuerpo finito es perfecto.

Demostración:

1. Sea $\alpha \in K$ algebraico, cuyo polinomio minimal es $p(x)$. 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. $\Longleftarrow$. 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 irreductible, contradicción.

   $\Longrightarrow$. Sea k perfecto y sea $a \in k$ arbitrario. Luego sea b una raíz p-ésima de a, es decir, un elemento tal que b es raíz de $x^p - a$. Construyamos $k(b)$, luego sea $p(x)$ 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 $p(x) := x^{p^n} - x \in \mathbb{F}_x$, luego su polinomio derivado es $p'(x) = -1 \neq 0$. Luego sea $k/\mathbb{F}_p$ el cuerpo de escisión de $\mathbb{F}_p$, entonces k tiene al menos p^n elementos por ser separable. Además, $(\mathrm{Frob}_k)^n(x) = x^{p^n} = x$ por el sueño del aprendiz, así que todo elemento en k es raíz de $p(x)$; 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 $L \cong K$. □

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 $\mathrm{Gal}(K/k)$. En el teorema 4.18 vimos que ha de ser finito en extensiones finitas y el teorema 4.17 nos caracteriza los k-automorfismos en términos de las raíces de un polinomio minimal. Sin embargo, podrían darse varias situaciones desfavorables: podría ser que las raíces se repitan y, por lo tanto, que el grupo esté más restringido, o podría darse que un polinomio no se escinda y luego no podamos conjugar las raíces a causa de no tenerlas. Por ello, reorientaremos el problema:

Definición 4.36: Sea K/k una extensión finita, entonces se denota por $\mathrm{N}(K/k)$ a la cantidad de k-monomorfismos desde K hasta su clausura normal.

Proposición 4.37: Sea α algebraico, entonces $\mathrm{N}(k(\alpha)/k) = [k(\alpha) : k]$ si α es separable y $\mathrm{N}(k(\alpha)/k) < [k(\alpha) : k]$ si no.

En general nos enfocaremos en cuerpos separables, pero aún así le dedicaremos un par de teoremas al caso inseparable:

Proposición 4.38: Sea K/k una extensión de cuerpos y $\alpha \in K$ algebraico. Si $\operatorname{car} k = p$, entonces existe algún $n \in \mathbb{N}$ tal que

$$[k(\alpha) : k] = p^n \,\mathrm{N}(k(\alpha)/k)$$

y que α^{p^n} es separable. En consecuencia, $\mathrm{N}(k(\alpha)/k) \mid [k(\alpha) : k]$.

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 raices distintas de $f(x)$, $m_i > 0$ y $\alpha_1 = \alpha$. Sea $\sigma \in \mathrm{Gal}(N/k)$, 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, $\mathrm{N}(k(\alpha^{p^n})/k) = r$. Y de hecho, por la correspondencia entre raíces de f y de h se concluye una correspondencia entre los k-morfismos, de modo que $\mathrm{N}(k(\alpha^{p^n})/k) = \mathrm{N}(k(\alpha)/k)$ y, en síntesis,

$$[k(\alpha) : k] = [k(\alpha) : k(\alpha^{p^n})][k(\alpha^{p^n}) : k] = p^n \,\mathrm{N}(k(\alpha)/k). \qquad \square$$

Definición 4.39 – *Extensión de Galois*: Se dice que K/k es una extensión de Galois si es normal y separable.

Sea $H \leq \mathrm{Gal}(K/k)$, 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

$$H_L := \{\sigma \in \mathrm{Gal}(K/k) : \forall a \in L\ \sigma(a) = a\}.$$

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 $\mathrm{N}(L/k) = \mathrm{N}(L/K)\,\mathrm{N}(K/k)$.

Demostración: En ésta demostración N representa la clausura normal de K, de modo que $\mathrm{N}(K/k) := |\operatorname{Hom}_k(K, N)|$. Nótese que L/K y L/k son normales, de modo que $\mathrm{N}(L/K) = |\mathrm{Gal}(L/K)|$.

Sea $\sigma \in \operatorname{Hom}_k(K, N)$, por el lema 4.23 se ha de cumplir que σ se extiende a un k-automorfismo $\sigma^* \in \mathrm{Gal}(L/k)$, por lo tanto, el problema se reduce a ver que hay $\mathrm{N}(L/K)$ posibles extensiones.

Sean τ_1, τ_2 dos posibles extensiones de σ. Es decir, τ_1, τ_2 son k-automorfismos de L, pero entonces $\tau_1 \circ \tau_2^{-1} \colon L \to L$ es un k-automorfismo que de hecho fija a K, es decir, $\tau_1 \circ \tau_2^{-1} \in \mathrm{Gal}(L/K)$. Y así podemos concluir. □

Teorema 4.41: Sea K/k una extensión finita. Entonces:

1. $|\mathrm{Gal}(K/k)| \leq \mathrm{N}(K/k)$.
2. Si K/k es separable, entonces $\mathrm{N}(K/k) = [K : k]$.
3. Si K/k no es separable, entonces $\mathrm{N}(K/k) \mid [K : k]$.
4. Si K/k es de Galois, entonces $|\mathrm{Gal}(K/k)| = [K : k]$.

Demostración: Si K es de Galois, entonces sea $K = k(\alpha_1, \ldots, \alpha_n)$. Luego aplicando el teorema anterior se tiene que

$$\begin{aligned}
\mathrm{N}(K/k) &= \mathrm{N}(K/k(\alpha_1, \alpha_2))\,\mathrm{N}(k(\alpha_1, \alpha_2), k) \\
&= \mathrm{N}(K/k(\alpha_1, \alpha_2))\,\mathrm{N}(k(\alpha_1, \alpha_2), k(\alpha_1))\,\mathrm{N}(k(\alpha_1), k) \\
&= \mathrm{N}(K/k(\alpha_1, \alpha_2))[k(\alpha_1, \alpha_2) : k(\alpha_1)][k(\alpha_1) : k] \\
&= \mathrm{N}(K/k(\alpha_1, \alpha_2))[k(\alpha_1, \alpha_2) : k].
\end{aligned}$$

luego podemos seguir iterando y aplicar la transitividad de grados para concluir que el enunciado aplica. Si K no es separable se reemplazan las igualdades por divisibilidades y el mismo razonamiento aplica.

Si K no es normal, entonces sea N su clausura normal. Por el teorema anterior y el caso normal se cumple que

$$[N : k] = \mathrm{N}(N/k) = \mathrm{N}(N/K)\,\mathrm{N}(K/k) \leq [N : K]\,\mathrm{N}(K/k),$$

por lo que se concluye que también aplica. □

Una pregunta curiosa sería ver si el converso es cierto. La respuesta es que sí y la veremos en un teorema más adelante.

Teorema 4.42 – *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 lo que tiene un generador γ y claramente $K = k(\gamma)$. Insertar referencia

Si k es infinito: Por inducción basta probar el caso cuando K/k está generado por dos elementos. Así pues, sea $K = k(\alpha, \beta)$, queremos probar que $K = k(\gamma)$. Sea A el conjunto de todos los pares (α', β'), donde α', β' son k-conjugados de α y β resp. Si $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in A$, entonces existe a lo más un $u \in k$ tal que $\alpha_1 + u\beta_1 = \alpha_2 + u\beta_2$. Como A es finito y k infinito, entonces existe un $v \in k$ tal que $\alpha_1 + v\beta_1 \neq \alpha_2 + v\beta_2$ para todo $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in A$.

Sea $\gamma := \alpha + v\beta$ y sean σ, τ dos k-monomorfismos de K en una clausura normal de K. Luego, como $(\sigma(\alpha), \sigma(\beta)), (\tau(\alpha), \tau(\beta)) \in A$, entonces

$$\sigma(\gamma) = \sigma(\alpha) + v\sigma(\beta) \neq \tau(\alpha) + v\tau(\beta) = \tau(\gamma).$$

Es decir, γ posee $\mathrm{N}(K/k)$ conjugados. Pero como K es separable, entonces vemos que

$$[k(\gamma) : k] = \mathrm{N}(k(\gamma)/k) = \mathrm{N}(K/k) = [K : k].$$

Luego, como $K/k(\gamma)$ es una extensión de cuerpos de dimensión 1 se concluye la igualdad. □

Proposición 4.43: Para toda extensión K/k y todo $H \leq \mathrm{Gal}(K/k)$ se cumple que $F(H)$ es un cuerpo y $k \leq F(H) \leq K$.

Teorema 4.44: Una extensión finita K/k es de Galois syss

$$F(\mathrm{Gal}(K/k)) = k.$$

Demostración: $\Longrightarrow$. Sea $\alpha \in K$, hemos de probar que existe un k-isomorfismo de K que mueve a α. Sea $p(x)$ 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 $\alpha \in k$.

$\Longleftarrow$. Sea $\alpha \in K \setminus k$ de polinomio minimal $p(x)$. Sean $\alpha_1, \ldots, \alpha_n$ 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 $\sigma \in \mathrm{Gal}(K/k)$. 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). □

Lema 4.45 (de independencia de Dedekind): Sean $\sigma_1, \ldots, \sigma_n$ automorfismos de un cuerpo K. Si $\sum_{i=1}^{n} c_i\sigma_i(a) = 0$ para todo $a \in K$, entonces $c_1 = c_2 = \cdots = c_n = 0$.

Demostración: Lo demostraremos por inducción sobre n. El caso base es trivial pues $c_1\sigma_1(1) = c_1 = 0$. Supongamos que $\sum_{i=1}^{n} c_i\sigma_i(a) = 0$ para todo a, si algún c_i es nulo, el resto lo son por inducción. Como $\sigma_1 \neq \sigma_n$, entonces existe $b \in K$ no nulo tal que $\sigma_1(b) \neq \sigma_n(b)$. Nótese que como b es invertible se cumple que el enunciado equivale a que para todo $a \in K$ se cumple que

$$\sum_{i=1}^{n} c_i\sigma_i(ba) = \sum_{i=1}^{n} c_i\sigma_i(b) \cdot \sigma_i(a) = 0.$$

Como $\sigma_i(b) \neq 0$, entonces todos los coeficientes que acompañan a $\sigma_i(a)$ siguen siendo no nulos. Luego se cumple que

$$\sum_{i=1}^{n} c_i(1 - \sigma_n(b^{-1})\sigma_i(b))\sigma_i(a) = \sum_{i=1}^{n} c_i\sigma_i(a) + \sum_{i=1}^{n} c_i\sigma_n(b^{-1})\sigma_i(b)\sigma_i(a) = 0,$$

sin embargo, $c_i(1-\sigma_n(b^{-1})\sigma_i(b))$ tiene un coeficiente nulo en el índice $i = n$, por lo que, por hipótesis de inducción se cumple que $1 - \sigma_n(b^{-1})\sigma_i(b) = 0$ para todo i, lo que implica que $\sigma_1(b) = \sigma_n(b)$ que es absurdo. □

Teorema 4.46: Sea K/k una extensión de cuerpos con $H \leq \mathrm{Gal}(K/k)$ entonces

$$[K : F(H)] = |H|.$$

En consecuncia, K/k finita es de Galois syss $|\mathrm{Gal}(K/k)| = [K : k]$.

Demostración: Lo haremos por contradicción suponiendo que $\{a_1, \ldots, a_m\}$ es una $F(H)$-base de K, y $H = \{\sigma_1, \ldots, \sigma_n\}$. Supongamos que $m < n$: Entonces la aplicación

$$\begin{aligned} f : K^n &\longrightarrow K^m \\ (x_1, \ldots, x_n) &\longmapsto \left(\sum_{i=1}^{n} x_i \sigma_i(a_1), \sum_{i=1}^{n} x_i \sigma_i(a_2), \ldots, \sum_{i=1}^{n} x_i \sigma_i(a_m) \right) \end{aligned}$$

es lineal y $n = \dim_K(K^n) = \dim(\ker f) + \dim(\mathrm{Img}\, f) \leq \dim(\ker f) + m$, de modo que $\dim(\ker f) \neq 0$ y el kernel es no vacío y por ende posee un elemento $(c_1, \ldots, c_n) \neq \vec{0}$. Nótese que por definición de base todo $\beta \in K$ se escribe como $\beta = \sum_{i=1}^{m} \lambda_i a_i$ con $\lambda_i \in F(H)$, luego como los λ_i están fijos bajo los k-automorfismos, se cumple que

$$\sum_{j=1}^{n} c_j \sigma_j(\beta) = \sum_{j=1}^{n} \sum_{i=1}^{m} c_j \lambda_i \sigma_j(a_i) = \sum_{i=1}^{m} \lambda_i \left(\sum_{j=1}^{n} c_j \sigma_j(a_i) \right) = 0$$

que es nulo, pues los términos en rojo lo son por definición de $(c_1, \ldots, c_n)$. Pero por el lema de independencia de Dedekind se cumple que los c_j's son nulos lo que es absurdo.

Supongamos que $m > n$: Considerando un truco similar al anterior construimos:

$$\begin{aligned} f : K^{n+1} &\longrightarrow K^n \\ (x_1, \ldots, x_{n+1}) &\longmapsto \left(\sum_{i=1}^{n+1} x_i \sigma_1(a_i), \ldots, \sum_{i=1}^{n+1} x_i \sigma_n(a_i) \right) \end{aligned}$$

tal que posee kernel no vacío y Elegimos $(c_1, \ldots, c_{n+1}) \neq \vec{0}$ que pertenezca al kernel tal que posea la máxima cantidad de coordenadas nulas, podemos elegirlas de tal modo que $c_1, \ldots, c_p$ sean no nulos y $c_{p+1}, \ldots, c_{n+1}$ lo sean, aunque nótese que $p > 1$.

Como H es subgrupo, entonces contiene a la identidad, y supongamos que ésta ocupa el j-ésimo lugar; luego como $\sum_{i=1}^{n+1} c_i a_i = 0$ se concluye que no

todos los c_i's están en $F(H)$ (pues los a_i's son linealmente independientes). Luego, como $c_p \neq 0$ multiplicamos por c_p^{-1} para asumir que $c_p = 1$. También podemos reordenar los c_i's de tal modo que $c_1 \notin F(H)$; por lo que existe algún σ_h tal que $\sigma_h(c_1) \neq c_1$. Nótese que como H es grupo, el producto $\tau \mapsto \tau \circ \sigma_h$ es una permutación, de modo que al aplicar σ_h a las n-tuplas, de modo que

$$\forall j \in \{1, \dots, n\} \quad \sum_{i=1}^{n+1} \sigma_h(c_i)\sigma_j(a_i) = 0$$

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 $(c_1, \dots, c_{n+1})$. □

Teorema 4.47 – *Teorema fundamental de la teoría de Galois*: Sea K/k una extensión finita de Galois. Denotando $G := \mathrm{Gal}(K/k)$ y

$$\{L : K/L/k \text{ extensiones}\} \underset{F(H)}{\overset{\mathrm{Gal}(K/L)}{\rightleftarrows}} \{H : H \leq G\}$$

entonces:

1. $F(H)$ y H_L son biyecciones, la una la inversa de la otra. Más aún, si $H_1 < H_2 \leq G$, entonces $K \supseteq F(H_2) \supset F(H_1)$, y si $k \subseteq L_1 \subset L_2 \subseteq K$, entonces $\mathrm{Gal}(K/L_1) > \mathrm{Gal}(K/L_2)$. En consecuencia, F es un funtor contravariante biyectivo:

$$\begin{array}{ccc} L_2 & & H_2 \\ \uparrow & \underset{F(H)}{\overset{\mathrm{Gal}(K/L)}{\rightleftarrows}} & \downarrow \\ L_1 & & H_1 \end{array}$$

2. Si $K/L/k$, entonces K/L es de Galois.
3. Si $K/L/k$, entonces L/k es de Galois syss $\mathrm{Gal}(K/L) \trianglelefteq G$.

4. Si $K/L/k$ y L/k es de Galois, entonces

$$\begin{aligned} r\colon \operatorname{Gal}(K/k) &\longrightarrow \operatorname{Gal}(L/k) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

es un epimorfismo de grupos y $\ker r = \operatorname{Gal}(K/L)$. En consecuencia, $\operatorname{Gal}(K/k)/\operatorname{Gal}(K/L) \cong \operatorname{Gal}(L/k)$.

5. Si $H_1, H_2 \leq \operatorname{Gal}(K/k)$, 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 $F(\operatorname{Gal}(K/L)) = L$.

   Por otro lado, sea $H \leq \operatorname{Gal}(K/k)$, entonces claramente $H \leq \operatorname{Gal}(K/F(H))$. Más aún $K/F(H)$ es de Galois, por lo que $|H| = [K : F(H)] = |\operatorname{Gal}(K/F(H))|$, y como H es finito, se da que $\operatorname{Gal}(K/F(H)) = H$.

3. $\implies$. Si L/k es de Galois, entonces es normal. Sea $\sigma \in \operatorname{Gal}(K/L)$ y $\tau \in \operatorname{Gal}(K/k)$, entonces $\tau^{-1} \in \operatorname{Gal}(K/k)$. Sea $\alpha \in L$, nótese que τ^{-1} manda α a sus k-conjugados, luego $\tau^{-1}(\alpha) \in L$. Como σ fija a L se cumple que $\sigma\big(\tau^{-1}(\alpha)\big) = \tau^{-1}(\alpha)$ y en consecuente, $\tau\big(\sigma(\tau^{-1}(\alpha))\big) = \alpha$, por lo que $\tau^{-1}\sigma\tau \in \operatorname{Gal}(K/L)$. Es decir, $\operatorname{Gal}(K/L) \trianglelefteq \operatorname{Gal}(K/k)$ 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 $\tau \in \operatorname{Gal}(K/k)$ tal que $\tau^{-1}(\alpha) = \beta$.

   Como $F(\operatorname{Gal}(K/L)) = L$, basta ver que todo σ fija a β. Sea $\sigma \in \operatorname{Gal}(K/L)$, entonces

$$\tau\big(\sigma(\tau^{-1}(\alpha))\big) = \tau(\sigma(\beta)) = \alpha \iff \sigma(\beta) = \tau^{-1}(\alpha) = \beta.$$

4. Ejercicio para el lector.

5. Basta notar que $\langle H_1, H_2\rangle$ es el mínimo subgrupo que contiene a H_1, H_2 y que $F(H_1) \cap F(H_2)$ es el máximo subcuerpo contenido en $F(H_1)$ y $F(H_2)$. □

4.4. Cuerpos algebraicamente cerrados

Lema 4.48: 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 irreductibles de K son de grado 1.
4. Todo polinomio de K se escinde.
5. K contiene un subcuerpo tal que la extensión K/k es algebraica y todo polinomio de $k[x]$ se escinde en K.

Demostración: 1 $\implies$ 2. Sea $p(x) \in K[x]$ un polinomio no constante, luego éste posee un factor irreductible $q(x)$ 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 irreductible.

3 $\implies$ 4. Basta notar que K es un DFU y aplicar descomposición en factores irreducibles.

4 $\implies$ 5. Basta tomar $K = k$.

5 $\implies$ 1. Sea L/K una extensión y $\alpha \in L$ un elemento algebraico, probaremos que $\alpha \in K$. Por definición existe un polinomio $p(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$ tal que α es raíz de $p(x)$. Como K/k es algebraico, entonces $K(c_0, \ldots, c_n)$ es una extensión finita y claramente $[K(c_0, \ldots, c_n; \alpha) : K(c_0, \ldots, c_n)] < \infty$ de modo que α es k-algebraico y, por lo tanto, es raíz de un polinomio $q(x) \in k[x]$. 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 $L = K$. □

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. □

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 $k = \{\alpha_1, \ldots, \alpha_n\}$, 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. □

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 $y_- : \mathcal{P} \to S$ 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:

$$\mathfrak{a} := \big(p(y_p) : p(x) \in \mathcal{P}\big).$$

1. $\mathfrak{a}$ es un ideal propio, es decir, $1 \notin \mathfrak{a}$: Procedamos por contradicción: supongamos que $1 \in \mathfrak{a}$, entonces existen $\lambda_i \in k[S]$ y $p_i \in \mathcal{P}$ 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 $F := \{y_{p_1}, y_{p_2}, \ldots, y_{p_n}, z_1, z_2, \ldots, z_m\}$.

Luego, la combinación lineal también vale en $k[F]$, pero he aquí un truco: Como hay finitos polinomios 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

$$\lambda_1(\alpha_1, \ldots, \alpha_n, 0, \ldots, 0)p_1(\alpha_1) + \cdots + \lambda_n(\alpha_1, \ldots, \alpha_n, 0, \ldots, 0)p_n(\alpha_n) = 1$$

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, $K_0 := \mathrm{Frac}(k[S]/\mathfrak{p})$ es una extensión de cuerpos de k.

3. Veamos que cada polinomio en k no constante posee una raíz en K_0: En efecto, sea $p(x) \in \mathcal{P}$, 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 $\alpha \in K_{n+1} \subseteq K$.

[1] Ésta idea fue propuesta por Banaschewski (véase [22]).

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. □

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

$$\mathcal{F} := \{(L, \tau) : K_1/L/k \text{ extensión y } \tau\colon L \to K_2 \ k\text{-morfismo}\},$$

y también definamos la relación $\preceq$ sobre $\mathcal{F}$:

$$(L_1, \sigma_1) \preceq (L_2, \sigma_2) \iff L_1 \subseteq L_2 \wedge \sigma_2|_{L_1} = \sigma_1.$$

Nótese que $\preceq$ es un orden parcial. Tenemos que comprobar que toda $\preceq$-cadena C está acotada superiormente, para ello nótese que

$$L := \bigcup_{(K_i,\sigma_i)\in C} K_i$$

y $\sigma\colon L \to K_2$ dado por $\sigma(\alpha) = \tau_i(\alpha)$ donde $\alpha \in K_i$ donde $(K_i, \sigma_i) \in C$. Así pues (L, σ) es una cota superior de C (¿por qué?).

Luego, por el lema de Zorn se cumple que $\mathcal{F}$ tiene un elemento $\subseteq$-maximal (M, σ). Veamos que $M = K_1$: Sea $\alpha \in K_1$, entonces α es k-algebraico, luego es la raíz de un polinomio $p(x)$. 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

$$\begin{array}{ccc} M(\alpha) & \overset{\sigma^*}{\rightsquigarrow} & M'(\beta) \\ \uparrow & & \uparrow \\ M & \underset{\sigma}{\rightsquigarrow} & M' \end{array}$$

por lo que $(M, \sigma) \preceq \big(M(\alpha), \sigma^*\big)$. Pero como M es maximal se da la igualdad y $\alpha \in M$.

Finalmente, veamos que $\sigma\colon K_1 \to K_2$ es suprayectiva: Sea $\beta \in K_2$, luego β es k-algebraico así que es la raíz de $p(x) \in k[x]$. 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. □

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 $K_1 = k(\alpha_1, \ldots, \alpha_n)$ 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. □

Definición 4.55: En consecuencia de los teoremas anteriores se denota por $\overline{k}$ 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 $|\operatorname{Gal}(L/R)| = [L : R] = 2^n m$ con m impar.

Por el primer teorema de Sylow, existe H un 2-subgrupo de Sylow de modo que $[L : F(H)] = |H| = 2^n$ y $[F(H) : R] = m$. Como $F(H)/R$ es de grado impar, entonces sus elementos son algebraicos de grado impar, i.e., cuyos polinomios minimales son de grado impar, lo cual es absurdo pues sabemos que tiene raíces en R. En conclusión L debe ser de grado una potencia de 2.

Como $[L : R] = 2^n$, se tiene que posee un subgrupo H tal que $[L : F(H)] = |H| = 2^{n-1}$ y $[F(H) : R] = 2$, luego $F(H) = K$. Así L es extensión de cuerpos de K. Luego, existe H' tal que $[L : F(H')] = 2^{n-2}$ y $[F(H') : K] = 2$ lo cual es imposible pues todo polinomio cuadrático de K es reducible. □

4.5. Otras aplicaciones

§4.5.1 Norma y traza. Ya vimos en las secciones anteriores que más que trabajar en extensiones normales, podemos sustituir los k-automorfismos por k-morfismos hasta su clausura normal. De éste modo se obtiene lo siguiente:

Definición 4.57: Dada una extensión finita separable K/k y N la clausura normal de K, sea $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_k(K, N)$. Entonces para todo $\alpha \in K$ se define

$$\mathrm{Nm}_k^K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{Tr}_k^K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Corolario 4.58: Sea K/k finita separable de grado g. Entonces para todo $\alpha \in k$ se cumple que

$$\mathrm{Nm}_k^K(\alpha) = \alpha^g, \qquad \mathrm{Tr}_k^K(\alpha) = g \cdot \alpha.$$

Ejemplo. En la extensión $\mathbb{C}/\mathbb{R}$, la norma y traza son:

$$\mathrm{Nm}_{\mathbb{R}}^{\mathbb{C}}(z) = z \cdot \overline{z} = |z|^2, \qquad \mathrm{Tr}_{\mathbb{R}}^{\mathbb{C}}(z) = z + \overline{z} = 2\,\mathrm{Re}(z).$$

Teorema 4.59 (transitividad de la norma y de la traza): Sean $L/K/k$ extensiones finitas y separables, entonces:

$$\mathrm{Nm}_k^L = \mathrm{Nm}_K^L \circ \mathrm{Nm}_k^K, \qquad \mathrm{Tr}_k^L = \mathrm{Tr}_K^L \circ \mathrm{Tr}_k^K.$$

§4.5.2 Raíces de la unidad y extensiones ciclotómicas. Ya hemos visto que Φ_p (el polinomio ciclotómico p-ésimo) es irreducible, pero podemos mejorar las condiciones. Para ello vayamos re-introduciendo varios conceptos antiguos: Se dice que un número complejo ω es una raíz n-ésima de la unidad si $\omega^n = 1$, por ejemplo, el 1 es una raíz n-ésima trivial de la unidad para todo $n > 0$. En particular ya vimos que todas las raíces n-ésimas de la unidad pueden ser generadas a partir de la siguiente:

$$\zeta_n := \mathrm{cis}\left(\frac{2\pi}{n}\right)$$

vale decir, ζ_n^j son todas las raíces n-ésimas de la unidad. A una raíz n-ésima de la unidad ω se le dice *primitiva* si ω^j son todas las raíces n-ésimas de la unidad. Por ejemplo, claramente el 1 no es una raíz n-ésima de la unidad

primitiva, excepto para $n = 1$. En particular ζ_n^j es primitiva syss j y n son coprimos.

Definición 4.60: 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 4.61: 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 4.62: 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. □

§4.5.3 La insolubilidad de la quíntica. Éste es tal vez uno de los temas más conocidos y una de las motivaciones para el estudio de la teoría de Galois. Aquí le dejamos al final para ser la «cereza sobre el pastel» de todo el trabajo de éste capítulo y es obligatoria la lectura de la sección §1.5.2.

Definición 4.63: 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 4.64: Una extensión es *resoluble (por radicales)* si está contenida en otra extensión radical.

Proposición 4.65: Se cumplen:

1. $\mathrm{Gal}(k(\zeta_n)/k)$ es abeliano.
2. Sea α raíz del polinomio irreducible $x^n - \beta \in k[x]$ y supongamos que $\zeta_n \in k$. Entonces $\mathrm{Gal}(k(\alpha)/k)$ es abeliano.
3. Toda extensión normal radical tiene grupo de Galois resoluble.
4. Toda extensión normal resoluble tiene grupo de Galois resoluble.

Demostración:

1. Nótese que como todas las raíces primitivas n-ésimas de la unidad son potencias de ζ_n, un $\mathbb{Q}$-automorfismo σ está completamente determinado por su valor en ζ_n, en particular denotemos $\sigma_j(\zeta_n) = \zeta_n^j$. Nótese que σ_j determina un automorfismo syss $(j;n) = 1$. Luego $(\sigma_j \circ \sigma_k)(\zeta_n) = \sigma_k(\zeta_n^j) = (\zeta_n^j)^k = (\zeta_n^k)^j = (\sigma_k \circ \sigma_j)(\zeta_n)$, lo que basta para comprobar que el grupo es abeliano.
2. γ es otra raíz de $x^n - \beta$ syss $(\gamma/\alpha)^n = \beta/\beta = 1$, vale decir, si γ/α es una raíz n-ésima de la unidad. Pero por hipótesis k posee a todas las raíces n-ésimas de la unidad, luego $k(\alpha)/k$ es una extensión normal.

Más aún, es claro que el grupo de automorfismos es abeliano puesto que todos son de la forma $\sigma_j(\alpha) = \alpha\zeta_m^j$. □

3. Supongamos que $K := k(\alpha_1, \ldots, \alpha_n)$ es radical, de modo que $\alpha_{i+1}^{m_{i+1}} \in k(\alpha_1, \ldots, \alpha_i)$ para todo i. Luego consideremos a la clausura normal N de K, la cual ha de ser de la forma

$$N = k(\zeta_{m_1}, \cdots, \zeta_{m_n}, \alpha_1, \ldots, \alpha_n).$$

Finalmente definamos $N_j := k(\zeta_{m_1}, \ldots, \zeta_{m_j})$ para $j \leq n$ y $N_j := k(\zeta_{m_1}, \ldots, \zeta_{m_n}, \alpha_1, \ldots, \alpha_{n-j})$ para $j > n$. Entonces claramente N_{i+1} es una extensión normal de N_i, por lo que se obtiene la siguiente serie normal de $\mathrm{Gal}(N/k)$:

$$\mathrm{Gal}(N/k) = \mathrm{Gal}(N/N_0) \trianglerighteq \mathrm{Gal}(N/N_1) \trianglerighteq \cdots \trianglerighteq \mathrm{Gal}(N/N_{2n}) = \{1\}.$$

Pero aún mejor, $\mathrm{Gal}(N/N_i)/\mathrm{Gal}(N/N_{i+1}) \cong \mathrm{Gal}(N_{i+1}/N_i)$ (por el teorema fundamental de la teoría de Galois) el cual es abeliano por los incisos anteriores. Finalmente, hemos construido una serie abeliana de $\mathrm{Gal}(N/k)$, por lo que $\mathrm{Gal}(N/k)$ es un grupo resoluble.

Además, $\mathrm{Gal}(N/k)/\mathrm{Gal}(N/K) \cong \mathrm{Gal}(K/k)$, por el teorema fundamental de la teoría de Galois, y sabemos que todo cociente de un grupo resoluble es también resoluble.

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 Einsenstein se concluye que $p(x)$ es irreducible, veamos lo siguiente: $p(x)$ debe tener tres raíces reales y dos complejas: ésto debido a que $\lim_{x\to\pm\infty} p(x) = \pm\infty$, 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 $\mathrm{Gal}(\mathbb{Q}/K) \leq S_5$, dado que cada automorfismo de K permuta las cinco raíces. ...

5

Álgebra lineal avanzada

5.1. 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 5.1: Sea $\{G_i\}_{i\in I}$ una familia de grupos, entonces definimos su producto como

$$\prod_{i\in I} G_i := \{(g_i)_{i\in I} : \forall i \in I \; g_i \in G_i\}$$

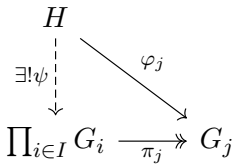
con la operación

$$(g_i)_{i\in I} \cdot (h_i)_{i\in I} := (g_i \cdot h_i)_{i\in I}.$$

Proposición 5.2: Sea $\{G_i\}_{i\in I}$ una familia de grupos, entonces:

1. $\prod_{i\in I} G_i$ es también un grupo, y las proyecciones $\pi_j \colon \prod_{i\in I} G_i \to G_j$ son homomorfismos de grupos.

2. Si H es un grupo y $\{\varphi_i \colon H \to G_i\}_{i\in I}$ es una familia de homomorfismos de grupos, entonces existe un único homomorfismo $\psi := \Delta_{i\in I}\, \varphi_i \colon H \to \prod_{i\in I} G_i$ tal que el siguiente entonces existe un único homomorfismo $\psi := \Delta_{i\in I}\, \varphi_i \colon H \to \prod_{i\in I} G_i$ tal que el siguiente diagrama:



conmuta. En consecuencia, $\prod_{i\in I} G_i$ es un producto categorial en Grp.

3. $\prod_{i\in I} G_i$ es abeliano syss todos los G_i's lo son.

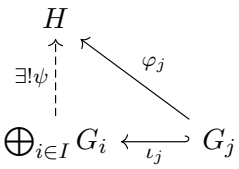
Definición 5.3: Dada una familia de grupos $\{G_i\}_{i\in I}$ se denota:

$$\bigoplus_{i\in I} G_i := \{(g_i)_{i\in I} : \{i : g_i \neq 1\} \text{ es finito}\} \subseteq \prod_{i\in I} G_i.$$

Proposición 5.4: Sea $\{G_i\}_{i\in I}$ una familia de grupos, entonces:

1. $\bigoplus_{i\in I} G_i$ es un subgrupo de $\prod_{i\in I} G_i$, y las inclusiones $\iota_j \colon G_j \to \bigoplus_{i\in I} G_i$ son homomorfismos de grupos.

2. Si H es un grupo y $\{\varphi_i \colon G_i \to H\}_{i\in I}$ es una familia de homomorfismos de grupos, entonces existe un único homomorfismo $\psi := \sum_{i\in I} \varphi_i \colon \bigoplus_{i\in I} G_i \to H$ tal que el siguiente diagrama:



conmuta. En consecuencia, $\bigoplus_{i\in I} G_i$ es un coproducto categorial en Grp.

3. $\bigoplus_{i\in I} G_i$ es abeliano syss todos los G_i's lo son.

Reiteramos que éstas propiedades no deben de sorprender a nadie, puesto que son absolutamente análogas al caso de módulos. En ésta sección hicimos énfasis en el hecho de que los (co)productos existen en Ab, ésto permite definir lo siguiente:

Definición 5.5: 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 5.6: Sea G un grupo abeliano, entonces para todo $n > 0$ natural:

$$nG := \{ng : g \in G\}$$

es un subgrupo de G. Más aún, si p es un número primo, entonces G/pG es un $\mathbb{F}_p$-espacio vectorial.

Demostración: Sea $[r] \in \mathbb{F}_p$ y sea $g \in G$, luego definamos

$$[r] \cdot (a + pG) := ra + pG.$$

Nótese que está bien definido dado que si $r' = r + pm$, entonces

$$r'a + pG = ra + pma + pG = ra + pG,$$

dado que $p(ma) \in pG$. También es fácil probar el resto de axiomas de un espacio vectorial. □

Corolario 5.7: Se cumplen:

1. Todo grupo abeliano libre finitamente generado es isomorfo a $\mathbb{Z}^n$ para algún n. Más generalmente, definiendo $\mathbb{Z}^{\oplus\kappa} := \bigoplus_{\alpha=1}^{\kappa} \mathbb{Z}$, se cumple que todo grupo abeliano libre es isomorfo a $\mathbb{Z}^{\oplus\kappa}$ para algún número cardinal κ.

2. Más aún, $\mathbb{Z}^n \cong \mathbb{Z}^m$ syss $n = m$. De modo que todo par de bases de un grupo abeliano libre finitamente generado son de igual cardinalidad.

3. (AE) $\mathbb{Z}^{\oplus\kappa} \cong \mathbb{Z}^{\oplus\mu}$ syss $\kappa = \mu$. De modo que todo par de bases de un grupo abeliano libre son de igual cardinalidad.

Demostración: Para probar la segunda y la tercera basta tomar un grupo abeliano libre G y considerar a $G/2G$ como $\mathbb{F}_2$-espacio vectorial. Luego la unicidad de cardinalidad de bases de un espacio vectorial induce la unicidad de cardinalidad de bases como grupo abeliano libre. □

Definición 5.8: Dado un grupo abeliano libre G, se denota por $\operatorname{rank} G$ a la cardinalidad de cualquiera de sus bases.

Proposición 5.9: Sea G un grupo abeliano con un conjunto X tal que satisface lo siguiente: Para todo grupo abeliano H y toda aplicación $f\colon X \to H$, existe una única extensión $f^*\colon G \to H$ que es un homomorfismo de grupos. Entonces G es un grupo abeliano libre de base X.

Demostración: Sea H un grupo abeliano libre de base Y tal que existe una biyección $q\colon X \to Y$ de inversa $p\colon Y \to X$. Luego, por ser libres, ambas funciones se extienden a $f\colon G \to H$ y $g\colon H \to G$, homomorfismos de grupos. Nótese que además $p \circ q = \mathrm{Id}_X\colon X \to X \subseteq G$ es una aplicación que posee una extensión $\mathrm{Id}_G\colon G \to G$ que es única, y lo mismo vale para Id_H como extensión única de $q \circ p$. Finalmente, $p \circ q$ también se extiende a $f \circ g$ y $q \circ p$ se extiende a $g \circ f$, luego se comprueba que f, g son homomorfismos de grupos y además son una la inversa de la otra. □

Proposición (AE) 5.10: Sea M un A-módulo y $N \leq M$ tal que M/N es un módulo libre. Entonces existe $F \leq M$ tal que $M/N \cong F$ y $M = N \oplus F$.

Demostración: Si N es un submódulo de M, entonces la siguiente sucesión:

$$0 \longrightarrow N \longrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$$

es exacta. Como M/N es libre entonces posee una base $X = \{[x_i]\}_{i \in I}$, por tanto, la aplicación $g\colon X \to M$ dada por $g([x_i]) := x_i$ admite una extensión única $g\colon M/N \to M$, tal que $g \circ \pi$ fija a la base, luego por unicidad, se cumple que $g \circ \pi = \mathrm{Id}_{M/N}$. Es decir, la sucesión exacta se escinde y por la proposición 3.28 se cumple el enunciado. □

Como ejercicio en la demostración anterior ubique el uso de elección.

Teorema (AE) 5.11: Sea A un DIP, entonces todo A-submódulo M de un módulo libre F es también libre; y de hecho $\operatorname{rank} M \leq \operatorname{rank} F$.

Demostración: Como F es libre, entonces posee una base, que por el teorema del buen orden (AE) admite un buen orden $X = \{x_\alpha : \alpha < \kappa\}$ (aquí los subíndices son ordinales). Luego definamos

$$F'_\beta := \langle\{x_\alpha : \alpha < \beta\}\rangle, \qquad F_\beta := F'_\beta \oplus \langle x_\beta\rangle.$$

Y definamos $M'_\beta := M \cap F'_\beta$ y $M_\beta := M \cap F_\beta$. Nótese que

$$\frac{M_\beta}{M'_\beta} = \frac{M_\beta}{M_\beta \cap F'_\beta} \cong \frac{M_\beta + F'_\beta}{M_\beta} \subseteq \frac{F'_\beta}{F_\beta} \cong A,$$

donde hemos empleado el tercer teorema de isomorfismos (para módulos). Así que M_β/M'_β es isomorfo a un ideal de A, pero todos los ideales de A son principales, luego o son el ideal nulo o son isomorfos (como A-módulos) a A. Si el ideal no es nulo, entonces por la proposición anterior se cumple que $M_\beta \cong M'_\beta \oplus \langle \boldsymbol{m}_\beta\rangle$ para algún $\boldsymbol{m}_\beta \in M_\beta$ tal que $\langle \boldsymbol{m}_\beta\rangle \cong A$; si el ideal es nulo entonces $\boldsymbol{m}_\beta := \vec{0}$. Claramente, eliminando los $\boldsymbol{m}_\beta$'s nulos se tiene que éstos elementos son linealmente independientes (por construcción, de hecho), de modo que simplemente bastaría probar que generan a M para concluir el enunciado.

Para ello, definamos $M^* := \mathrm{Span}\{\boldsymbol{m}_\beta\}_{\beta<\kappa}$ y definamos:

$$\mu(\boldsymbol{m}) := \text{mín}\{\alpha : \boldsymbol{m} \in F_\alpha\}.$$

Supongamos que $M^* < M$, entonces definamos γ como el mínimo índice tal que $\gamma = \mu(\boldsymbol{m})$ para algún $\boldsymbol{m} \in M \setminus M^*$ y sea $\tilde{\boldsymbol{m}}$ un elemento que cumpla lo anterior, luego se cumple que

$$\tilde{\boldsymbol{m}} = \boldsymbol{a} + \lambda \boldsymbol{m}_\gamma \in M_\gamma$$

para unos únicos $\boldsymbol{a} \in M'_\gamma$ y $\lambda \in A$. Luego como $\boldsymbol{m}_\gamma \in M^*$ y $\tilde{\boldsymbol{m}} \notin M^*$ necesariamente se tiene que $\boldsymbol{a} \notin M^*$. Pero $\boldsymbol{a} \in F'_\gamma$, luego $\mu(\boldsymbol{a}) < \gamma$ contradiciendo la minimalidad de γ. □

Nótese que su F es finitamente generado, entonces no hay uso de elección.

Proposición 5.12: Sea A un anillo, F un A-módulo libre de base X y M otro A-módulo. Toda aplicación $f\colon X \to M$ admite una única extensión $f^*\colon F \to M$ en un morfismo de A-módulos.

Definición 5.13: Sea G un grupo abeliano, definimos su *subgrupo de torsión* como

$$\mathsf{T}(G) := \{x \in G : \operatorname{ord} x \neq 0\},$$

o equivalentemente es el subgrupo de los x tales que alguna potencia no nula sea el neutro. G se dice un *grupo de torsión* si $\mathsf{T}(G) = G$; y se dice *libre de torsión* si $\mathsf{T}(G) = \{1\}$.

Ejemplo. Todo grupo abeliano finito es un grupo de torsión. $(\mathbb{Z}, +)$ es libre de torsión. $(\mathbb{R}^\times, \cdot)$ es tal que $\mathsf{T}(\mathbb{R}^\times) = \{\pm 1\}$, así que ni es de torsión ni es libre de torsión.

Proposición 5.14: Para todo G, H abelianos, se cumplen:

1. $G/\mathsf{T}(G)$ es libre de torsión.
2. Si $G \cong H$, entonces $\mathsf{T}(G) \cong \mathsf{T}(H)$ y $G/\mathsf{T}(G) \cong H/\mathsf{T}(H)$.

Teorema 5.15: Se cumplen las siguientes:

1. Todo grupo abeliano finitamente generado y libre de torsión es un grupo abeliano libre. En consecuencia dicho grupo será isomorfo a $\mathbb{Z}^n$ para algún n.
2. Todo subgrupo H de un grupo abeliano libre finitamente generado G es también abeliano libre y además $\operatorname{rank} H \leq \operatorname{rank} G$.
3. (AE) Todo subgrupo H de un grupo abeliano libre G es también abeliano libre y además $\operatorname{rank} H \leq \operatorname{rank} G$.

Demostración:

1. La demostración es por inducción sobre la cantidad de generadores $\langle x_1, \ldots, x_n\rangle$ del grupo G. Claramente se satisface el caso base $n = 1$.

   Para el caso inductivo, sea $G := \langle x_1, \ldots, x_n, x_{n+1}\rangle$ y sea

   $$H := \{g \in G : \exists m \in \mathbb{Z}_{\neq 0}\ mg \in \langle x_{n+1}\rangle\}.$$

   Claramente $H \leq G$, y G/H es un grupo abeliano, libre de torsión (¿por qué?) que está generado por $\{[x_1], \ldots, [x_n]\}$, por lo que, por hipótesis inductiva, es un grupo abeliano libre. En consecuencia, basta probar que H sea también abeliano libre.

Sea $g \in H$, y sea $m \in \mathbb{Z}_{\neq 0}$ tal que $mg \in \langle x_{n+1} \rangle$, de modo que existe $r \in \mathbb{Z}$ tal que $rx_{n+1} = mg$; definamos $\varphi\colon H \to \mathbb{Q}$ dado por $\varphi(g) := r/m$. Nótese que φ está bien definido: En efecto, si $r'x_{n+1} = m'g$ con r', m' distintos, entonces $r'rx_{n+1} = m'mg$, pero x_{n+1}, g tienen orden 0, así que necesariamente $r'r = m'm$ y $r'/m' = r/m$. Además φ es un homomorfismo de grupos inyectivo (¿por qué?), así que basta probar que todo subgrupo finitamente generado F de $\mathbb{Q}$ sea abeliano libre para poder concluir éste inciso.

Sea $F := \langle a_1/b_1, \ldots, a_r/b_r \rangle \leq \mathbb{Q}$. Y sea $d := \prod_{i=1}^{n} b_i$, entonces $f\colon D \to \mathbb{Z}$ dado por $f(x) := dx$ es un homomorfismo de grupos bien definido, dado que d «limpia todos los denominadores», pero más aún, como D es libre de torsión, entonces $\ker f$ es trivial y, por lo tanto, f es inyectivo; luego f es un encaje, i.e., un isomorfismo con un subgrupo de $\mathbb{Z}$. Pero todos los subgrupos de $\mathbb{Z}$ son ideales de $\mathbb{Z}$ que son además principales, por lo que $U \cong \{0\}$ o $U \cong n\mathbb{Z} \cong \mathbb{Z}$.

2. Basta notar que todo grupo abeliano libre puede verse como un $\mathbb{Z}$-módulo libre y que $\mathbb{Z}$ es un DIP para aplicar el teorema 5.11. □

Corolario 5.16: Se cumplen:

1. Todo grupo abeliano finitamente generado G puede escribirse como
$$G = \mathsf{T}(G) \oplus F$$
donde F es un grupo abeliano libre finitamente generado.

2. Dados G, H abelianos y finitamente generados. Entonces $G \cong H$ syss $\mathsf{T}(G) \cong \mathsf{T}(H)$ y $\operatorname{rank}(G/\mathsf{T}(G)) \cong \operatorname{rank}(H/\mathsf{T}(H))$.

5.2. Formas canónicas

En ésta sección trabajaremos exclusivamente con espacios vectoriales de dimensión finita.

Daremos varias definiciones para endomorfismos lineales, y nos daremos la libertad de asumir que las definiciones también aplicar singularmente a matrices mediante el endomorfismo $\boldsymbol{v} \mapsto \boldsymbol{v} \cdot B$.

Definición 5.17: Sea $T\colon V \to V$ una función lineal, si existe $\boldsymbol{v} \in V_{\neq \vec{0}}$ tal que $T(\boldsymbol{v}) = \lambda \boldsymbol{v}$ para algún $\lambda \in k$, entonces se dice que $\boldsymbol{v}$ es un *autovector* y λ es su *autovalor* asociado.

Denotamos por $\sigma(T)$ al conjunto de los autovalores de T.

Teorema 5.18: Dado $A \in \mathrm{Mat}_n(k)$, se cumple que λ es autovalor de A syss $\det(\lambda I_n - A) = 0$.

Demostración: Sea λ el autovalor asociado a $\boldsymbol{v} \in V_{\neq \vec{0}}$, es decir, $\boldsymbol{v}A = \lambda \boldsymbol{v}$. Luego $\boldsymbol{v} \cdot (\lambda I_n - A) = \vec{0}$, por lo que $\lambda I_n - A$ no es inversible y $\det(\lambda I_n - A) = 0$. El recíproco es análogo. □

Definición 5.19: Dado $A \in \mathrm{Mat}_n(k)$, se define

$$\psi_A(x) := \det(xI_n - A) \in k[x]$$

llamado el *polinomio característico* de A.

Ahora el teorema anterior se reescribe como que λ es autovalor de A syss λ es raíz de ψ_A.

Corolario 5.20: Toda matriz de $n \times n$ posee a lo más n autovalores.

Teorema 5.21: Son equivalentes:

1. k es algebraicamente cerrado.
2. Toda matriz cuadrada con coeficientes en k tiene un autovector.

Demostración: Claramente $1 \implies 2$, veremos la recíproca: Para ello basta probar por inducción que todo polinomio está asociado al polinomio característico de una matriz. En particular el polinomio característico de

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

es

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0. \qquad \square$$

Lema 5.22: Sea $A \in \mathrm{Mat}_n(k)$, entonces $\psi_A(x)$ es un polinomio mónico y el coeficiente que acompaña al monomio x^{n-1} es $-(a_{11} + a_{22} + \cdots + a_{nn}) = -\operatorname{tr}(A)$.

Proposición 5.23: Sea $A \in \mathrm{Mat}_n(\overline{k})$, tal que sus autovalores son $\alpha_1, \ldots, \alpha_n$ (contando multiplicidades), entonces

$$\mathrm{tr}(A) = -\sum_{i=1}^{n} \alpha_i, \qquad \det(A) = \prod_{i=1}^{n} \alpha_i.$$

Definición 5.24: Se dice que dos matrices $A, B \in \mathrm{Mat}_n(k)$ son *similares* si existe $C \in \mathrm{GL}(n,k)$ tal que $A = C^{-1}BC$.

Proposición 5.25: Dadas dos matrices $A, B \in \mathrm{Mat}_n(k)$ que son similares se cumple que $\psi_A = \psi_B$.

Demostración: Sea $C \in \mathrm{GL}(n,k)$ tal que $A = C^{-1}BC$, luego $\det(xI - A) = \det(xC^{-1}IC - C^{-1}BC) = \det(C^{-1})\det(xI - B)\det(C)$. □

Definición 5.26: Se dice que una matriz $A \in \mathrm{Mat}_n(k)$ es *diagonalizable* si es similar a una matriz diagonal. Equivalentemente, un endomorfismo es diagonalizable si su representación matricial en alguna base es diagonal.

Teorema 5.27: Una matriz A es diagonalizable syss el conjunto de sus autovectores genera el espacio. En cuyo caso, A es similar a $\mathrm{diag}(\alpha_1, \ldots, \alpha_n)$, donde los α_i's son los autovalores (contando multiplicidad) de la matriz.

Demostración: $\Longleftarrow$. Sean S los autovectores de A. Si $\mathrm{Span}\, S = V$, entonces existe $B \subseteq S$ base y claramente $\mathrm{M}_B^B(A) = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$.

$\Longrightarrow$. Sea $B := C^{-1}AC = \mathrm{diag}(\beta_1, \ldots, \beta_n)$, entonces $\boldsymbol{e}_1 B = \beta_1 \boldsymbol{e}_1$, $\boldsymbol{e}_2 B = \beta_2 \boldsymbol{e}_2$ y así. Por lo que, definiendo $\boldsymbol{v}_i := \boldsymbol{e}_i C^{-1}$ se obtiene que $\boldsymbol{v}_i$ son autovectores de A que generan el espacio y que los β_i's eran efectivamente los autovalores de A. □

5.3. Productos tensoriales

Definición 5.28: Sean M, N, T un trío de A-módulos. Una aplicación $\varphi\colon M \times N \to T$ es *A-bilineal* si es un morfismo en cada coordenada, formalmente:

1. Si para todo $\boldsymbol{n}_0 \in N$ se cumple que la aplicación $\boldsymbol{m} \to \varphi(\boldsymbol{m}, \boldsymbol{n}_0)$ es un morfismo de A-módulos.

2. Si para todo $\boldsymbol{m}_0 \in M$ se cumple que la aplicación $\boldsymbol{n} \to \varphi(\boldsymbol{m}_0, \boldsymbol{n})$ es un morfismo de A-módulos.

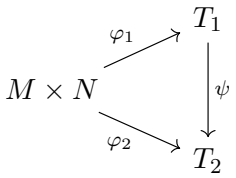
Ejemplo. En el capítulo sobre módulos ya vimos un primer ejemplo clásico: el determinante. La aplicación $\det\colon k^2 \times k^2 \to k$ es claramente k-bilineal (por definición, de hecho), pero no es k-lineal en sí misma, de hecho, si $\operatorname{car} k \neq 2$, entonces

$$\det\big((2,0),(0,2)\big) = 4 \neq 2 = 2\det\big((1,0),(0,1)\big).$$

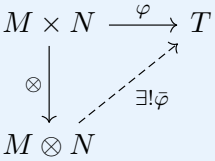
En general las aplicaciones bilineales no suelen ser lineales y ejemplos análogos al anterior aplican.

En ésta sección pretendemos definir el producto tensorial, sin embargo hay dos posibilidades: una es comenzar definiéndolo de manera concreta y concluir la propiedad universal categórica que le define, o la otra es comenzar por definir la propiedad categórica y concluir por otorgar una construcción concreta. En éste libro hemos en general optado por la primera, pero ahora lo haremos de manera inversa.

Sean M, N un par de A-módulos, definimos la categoría $\operatorname{Bil}(M \times N)$ 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 $\operatorname{Bil}(M \times N)$ syss $\varphi_i\colon M \times N \to T_i$ es bilineal, $\psi\colon T_1 \to T_2$ es un morfismo de A-módulos y el siguiente diagrama conmuta:



Definición 5.29: Un producto tensorial $M \otimes N$ es un objeto inicial de $\operatorname{Bil}(M \times N)$; es decir, es tal que para toda aplicación A-bilineal $\varphi\colon M \times N \to T$ se cumple que el siguiente diagrama conmuta:



Teorema 5.30: Los productos tensoriales existen.

Demostración: Sean M, N un par de A-módulos. Entonces comencemos por definir $F(M \times N) := A^{\oplus(M\times N)}$, es decir, el A-módulo libre que tiene por base a $M \times N$, queremos que la función $j\colon M \times N \to F(M \times N)$ que manda cada objeto en sí mismo sea bilineal. Sea K el submódulo generado por todos los elementos de la forma

$$j(\alpha \boldsymbol{m}_1 + \beta \boldsymbol{m}_2, \boldsymbol{n}) - \alpha j(\boldsymbol{m}_1, \boldsymbol{n}) - \beta j(\boldsymbol{m}_2, \boldsymbol{n})$$

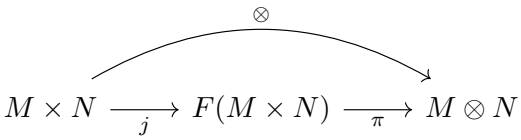
con $\alpha, \beta \in A$, $\boldsymbol{m}_1, \boldsymbol{m}_2 \in M$ y $\boldsymbol{n} \in N$; y los elementos de la forma

$$j(\boldsymbol{m}, \alpha \boldsymbol{n}_1 + \beta \boldsymbol{n}_2) - \alpha j(\boldsymbol{m}, \boldsymbol{n}_1) - \beta j(\boldsymbol{m}, \boldsymbol{n}_2)$$

con $\alpha, \beta \in A$, $\boldsymbol{m} \in M$ y $\boldsymbol{n}_1, \boldsymbol{n}_2 \in N$. Finalmente definamos

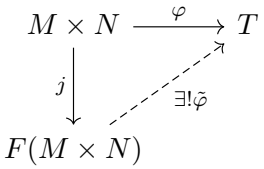
$$M \otimes N := \frac{F(M \times N)}{K},$$

junto a la aplicación:



Nótese de que por construcción de K se cumple que $\otimes$ resulte bilineal.

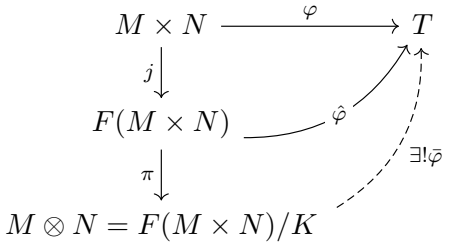
Luego hay que verificar que se satisfaga la propiedad universal. Sea $\varphi\colon M \times N \to T$ bilineal, entonces por definición de módulo libre se cumple que existe:



tal que el diagrama conmuta, donde $\hat{\varphi}$ es un morfismo de A-módulos. Basta probar que $\hat{\varphi}$ se anula en K:

$$\begin{aligned}
&\hat{\varphi}\big(j(\alpha\boldsymbol{m}_1+\beta\boldsymbol{m}_2,\boldsymbol{n})-\alpha j(\boldsymbol{m}_1,\boldsymbol{n})-\beta j(\boldsymbol{m}_2,\boldsymbol{n})\big)\\
&\quad=\hat{\varphi}\big(j(\alpha\boldsymbol{m}_1+\beta\boldsymbol{m}_2,\boldsymbol{n})\big)-\alpha\hat{\varphi}\big(j(\boldsymbol{m}_1,\boldsymbol{n})\big)-\beta\hat{\varphi}\big(j(\boldsymbol{m}_2,\boldsymbol{n})\big)\\
&\quad=\varphi(\alpha\boldsymbol{m}_1+\beta\boldsymbol{m}_2,\boldsymbol{n})-\alpha\varphi(\boldsymbol{m}_1,\boldsymbol{n})-\beta\varphi(\boldsymbol{m}_2,\boldsymbol{n})\\
&\quad=\vec{0}.
\end{aligned}$$

De lo cual se sigue que el siguiente diagrama necesariamente conmuta:



□

Definición 5.31: 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

$$\boldsymbol{m}_1\otimes\boldsymbol{n}_1+\boldsymbol{m}_2\otimes\boldsymbol{n}_2+\cdots+\boldsymbol{m}_s\otimes\boldsymbol{n}_s,$$

con $s>0$, $\boldsymbol{m}_i\in M$ y $\boldsymbol{n}_i\in N$ (aquí suprimimos los coeficientes dados que por bilinealidad se pueden «meter» dentro del producto y dado que los objetos de los módulos son cerrados bajo producto escalar).

A los tensores de la forma $\boldsymbol{m}\otimes\boldsymbol{n}$ se le dicen *tensores puros*. Nótese que los tensores puros generan al resto de tensores, pero ellos no constituyen necesariamente todos los tensores.

Proposición 5.32: Si $M=\mathrm{Span}_A(B)$ y $N=\mathrm{Span}_A(C)$, entonces

$$M\otimes N=\mathrm{Span}_A(\{\boldsymbol{b}\otimes\boldsymbol{c}:\boldsymbol{b}\in B,\boldsymbol{c}\in C\}).$$

Demostración: Basta notar que si

$$\boldsymbol{m}=\lambda_1\boldsymbol{b}_1+\cdots+\lambda_s\boldsymbol{b}_s$$

entonces $\boldsymbol{m}\otimes\boldsymbol{n}=\sum_{i=1}^{s}\lambda_i(\boldsymbol{b}_i\otimes\boldsymbol{n}_i)$. □

En consecuencia diríamos que si V, W son k-espacios vectoriales, entonces $\dim_k(V \otimes W) \leq \dim_k(V) \cdot \dim_k(W)$. Pero ésta afirmación se puede mejorar.

Primero comenzaremos con la siguiente observación:

Teorema 5.33: Sean M, N, T un trío de A-módulos, entonces $\mathrm{Hom}_A(M \otimes N, T) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, T))$ (como A-módulos).

Demostración: Sea $\alpha \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, T))$, eso quiere decir que $\alpha(\boldsymbol{m}) \in \mathrm{Hom}_A(N, T)$. Luego la siguiente aplicación:

$$\begin{aligned} \varphi\colon M \times N &\longrightarrow T \\ (\boldsymbol{m}, \boldsymbol{n}) &\longmapsto \alpha(\boldsymbol{m})(\boldsymbol{n}) \end{aligned}$$

es A-bilineal, y por ende admite una única factorización $\overline{\alpha}\colon M \otimes N \to T$ (que es un morfismo de A-módulos) tal que $\otimes \circ \overline{\alpha} = \alpha$. Queda al lector comprobar que la aplicación $\alpha \mapsto \overline{\alpha}$ es el isomorfismo de A-módulos deseado. □

Ésto puede parecer un resultado parcialmente inofensivo, pero demuestra una intrínseca dualidad especial entre los tensores y los conjuntos Hom's.

Proposición 5.34: Sean M, N, T un trío de A-módulos, entonces:

1. $M \otimes N \cong N \otimes M$.
2. $(M \oplus N) \otimes T \cong (M \oplus T) \otimes (N \oplus T)$.
3. En general, si $\{M_i\}_{i \in I}$ es una familia de A-módulos, entonces
$$\left(\bigoplus_{i \in I} M_i \right) \otimes T \cong \bigoplus_{i \in I} (M_i \otimes T).$$
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. Si
$$M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$
es una sucesión exacta, entonces

$$M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0$$

también lo es. En consecuencia, $- \otimes N$ es un funtor exacto por la derecha.

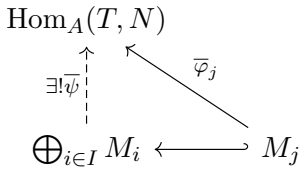
8. Sea $\mathfrak{a}$ un ideal de A, entonces
$$\frac{A}{\mathfrak{a}} \otimes M \cong \frac{M}{\mathfrak{a}M}.$$

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 $\{\varphi_i \colon M_i \otimes T \to N\}_{i\in I}$ una familia de morfismos de A-módulos. Vale decir,

$$\varphi_i \in \mathrm{Hom}_A(M_i \otimes T, N) \iff \overline{\varphi}_i \in \mathrm{Hom}_A(M_i, \mathrm{Hom}_A(T, N));$$

luego existe una única extensión tal que el siguiente diagrama conmuta:



finalmente consideramos que $\overline{\psi} \in \mathrm{Hom}\left(\bigoplus_{i\in I} M_i, \mathrm{Hom}_A(T,N)\right)$ lo devolvemos a $\psi \in \mathrm{Hom}\left(\left(\bigoplus_{i\in I} M_i\right) \otimes T, N\right)$. Queda al lector comprobar que ψ es una extensión única.

Para la sexta emplee $\otimes \colon (a, \boldsymbol{m}) \mapsto a\boldsymbol{m}$ y note que toda aplicación bilineal desde $0 \times M$ es necesariamente el morfismo nulo. Para la séptima basta aplicar el mismo truco anterior y recordar que Hom preservaba sucesiones exactas.

Para la octava considere la sucesión exacta

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0$$

la cual se traduce en

$$\mathfrak{a} \otimes M \longrightarrow A \otimes M \cong M \longrightarrow A/\mathfrak{a} \otimes M \longrightarrow 0 \otimes M \cong 0$$

Nótese además que $\mathfrak{a} \otimes M \cong \mathfrak{a}M$. Luego existe una transformación canónica que completa el que $A/\mathfrak{a} \otimes M \cong M/\mathfrak{a}M$. □

Ejemplo. Consideraremos los siguientes productos tensoriales en $\mathbb{Z}$. Considere la siguiente sucesión exacta

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z}$$

donde $f(n) = 2n$ y tensoricemos los factores por $\mathbb{Z}/2\mathbb{Z}$: luego considere

$$\bar{f} := f \otimes \mathbb{Z}/2\mathbb{Z} \colon \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

que nótese que manda el [0] en el cero y el [1] en el cero. De modo que $\bar{f} = 0$, por lo que la sucesión

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\bar{f}} \mathbb{Z}/2\mathbb{Z}$$

no es exacta.

Definición 5.35: Se dice que el A-módulo N es *plano* si $- \otimes N$ es un funtor exacto.

6

Teoría espectral

6.1. 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 6.1 – *Subespacio f-invariante*:** Dado un módulo M, $f \in \mathrm{End}(M)$ y un subespacio S de M, se dice que S es f-invariante si $f[S] \subseteq S$.

Proposición 6.2: Para todo $f \in \mathrm{End}(M)$ se cumple que son subespacios f-invariantes:

1. El subespacio nulo $\{\mathbf{0}\}$.
2. Todo subespacio de $\ker f$.
3. Todo subespacio que contenga a $\mathrm{Img}\, f$.

Lema 6.3: Si $f \in \mathrm{End}(\Bbbk^n)$ y X, Y son bases ordenadas cualesquiera de $\Bbbk^n$, entonces para todo $x \in \Bbbk$

$$\det(xI_n - \mathrm{M}_X^X(f)) = \det(xI_n - \mathrm{M}_Y^Y(f))$$

Demostración: Como hemos visto

$$\mathrm{M}_Y^Y(f) = \mathrm{M}_Y^X(\mathrm{Id})\,\mathrm{M}_X^X(f)\,\mathrm{M}_X^Y(\mathrm{Id}),$$

luego si llamamos $B := \mathrm{M}_X^Y(\mathrm{Id})$ (que es invertible), cumple que

$$\mathrm{M}_Y^Y(f) = B^{-1}\,\mathrm{M}_X^X(f)B,$$

luego

$$\begin{aligned}\det(xI_n - \mathrm{M}_Y^Y(f)) &= \det(xI_n - B^{-1}\,\mathrm{M}_X^X(f)B)\\ &= \det(B^{-1}(xI_n - \mathrm{M}_X^X(f))B) = \det(xI_n - \mathrm{M}_X^X(f)).\end{aligned}$$

□

Definición 6.4 – *Polinomio característico*: Si $f \in \mathrm{End}(\Bbbk^n)$, entonces dada una base X cualquiera se define

$$p_f(x) := \det(xI_n - \mathrm{M}_X^X(f))$$

conocido como el *polinomio característico* de f.

Definición 6.5: Si M es un A-módulo y $f \in \mathrm{End}(M)$, entonces $v \in M_{\neq 0}$ se dice un *autovector* de f si $\mathrm{Span}\{v\}$ es f-invariante, o tradicionalmente, si existe $\alpha \in M$ tal que $f(v) = \alpha v$, en cuyo caso se dice que α es el *autovalor* asociado a v de f. Si $M = A^n$ y $B \in \mathrm{Mat}_n(A)$, entonces se definen los autovalores y autovectores de B a aquellos correspondientes a la función $f(v) := Bv$.
Una transformación lineal f se dice *diagonalizable* si existe una base ordenada X tal que $\mathrm{M}_X^X(f)$ es una matriz diagonal.
Se le llama *espectro* de f, denotado por $\sigma(f)$ al conjunto de sus autovalores.

Teorema 6.6: Un escalar $\lambda \in \sigma(f)$ syss $p_f(\lambda) = 0$.

Definición 6.7: Sea $f \in \mathrm{End}(V)$. Si $\alpha \in \Bbbk$, entonces se les llaman *autoespacio* y *autoespacio generalizado* generado por α de f a:

$$V_\alpha^f := \{v \in V : f(v) = \alpha v\}, N_\alpha^f := \{v \in V : \exists r \geq 0\ (f - \alpha\,\mathrm{Id})^r v = 0\};$$

de no haber ambigüedad se obvia el "f".

Para un $\alpha \in \Bbbk$ se le dice *multiplicidad geométrica* y *algebraíca* resp., a $\dim V_\alpha$ y $\dim N_\alpha$.

Proposición 6.8: Para todo $f \in \mathrm{End}(\Bbbk^n)$ y todo $\alpha \in \Bbbk$ se cumple:

1. V_α y N_α son submódulos o subespacios vectoriales de $\Bbbk^n$.
2. $V_\alpha \leq N_\alpha$.
3. V_α y N_α son f-invariantes.
4. La multiplicidad geométrica de α siempre es menor o igual a su multiplicidad algebraíca.
5. α es autovalor syss tiene multiplicidad geométrica no nula syss tiene multiplicidad algebraíca no nula.

Definición 6.9 – *Endomorfismo nilpotente*: Se dice que $f \in \mathrm{End}(V)$ es *nilpotente de grado* n si $f^{n-1} \neq 0$ y $f^n = 0$. Análogo para matrices cuadradas.

El estudio de endomorfismos nilpotentes es relevante pues si λ es autovalor de f, entonces $f - \lambda \,\mathrm{Id}$ restringido al autoespacio N_λ es nilpotente.

Proposición 6.10: Sea $f \in \mathrm{End}(V)$:

1. Si f es nilpotente y su campo escalar es un dominio íntegro, entonces todos sus autovalores son nulos.
2. Si $\lambda \in \sigma(f)$, entonces $(f - \lambda \,\mathrm{Id})$ es nilpotente en N_λ.

Proposición 6.11: Sea V un módulo sobre un dominio íntegro y $f \in \mathrm{End}(V)$. Si $\alpha \neq \beta$, entonces $f - \alpha \,\mathrm{Id}$ es inyectiva en N_β. Y si el último es de dimensión finita, entonces $f - \alpha \,\mathrm{Id}$ es biyección.

Demostración: Sea $v \in N_\beta$ tal que $(f - \alpha \,\mathrm{Id})v = 0$, luego se cumple que

$$(f - \beta \,\mathrm{Id})v = (\alpha - \beta)v.$$

Si $v = 0$ entonces $f - \alpha \,\mathrm{Id}$ es inyectiva, como se quería probar. Si $v \neq 0$, entonces v es autovector de $(f - \beta \,\mathrm{Id})$ con autovalor $\alpha - \beta \neq 0$. Pero $(f - \beta \,\mathrm{Id})$ es nilpotente en N_β, luego sólo posee autovalores nulos, contradicción. □

Teorema 6.12: Sea V un módulo sobre un dominio íntegro y $f \in \mathrm{End}(V)$. Si $\alpha_1, \ldots, \alpha_n$ son escalares distintos, entonces sus autoespacios generalizados son independientes. En consecuencia, sus autoespacios comúnes también lo son.

DEMOSTRACIÓN: La demostración es por inducción sobre n. El caso base $n = 1$ es trivial. Sean $v_i \in N_{\alpha_i}$ tales que

$$v_1 + \cdots + v_n + v_{n+1} = 0,$$

por definición existe $r > 0$ tal que

$$(f - \alpha_{n+1} \operatorname{Id})^r v_{n+1} = 0,$$

luego aplicando la función al resto de v_is se obtiene que

$$(f - \alpha_{n+1} \operatorname{Id})^r v_1 + \cdots + (f - \alpha_{n+1} \operatorname{Id})^r v_n = 0,$$

que corresponde al paso inductivo, puesto que N_{α_i} son invariantes; por lo tanto para todo $i \in \{1, \ldots, n\}$:

$$(f - \alpha_{n+1} \operatorname{Id})^r v_i = 0.$$

Finalmente aplicamos la proposición anterior que dice que $(f - \alpha_{n+1} \operatorname{Id})^r$ es biyección en N_{α_i} para deducir que $v_i = 0$. □

Corolario 6.13: Sea $f \in \mathrm{End}(\Bbbk^n)$. Si f posee n autovalores distintos, entonces es diagonalizable.

Teorema 6.14: Un endomorfismo es diagonalizable syss existe una base formada por sus autovectores.

Teorema 6.15: Son equivalentes:

1. $\Bbbk$ es algebraicamente cerrado.

2. Toda matriz cuadrada con coeficientes en $\Bbbk$ tiene un autovector.

DEMOSTRACIÓN: Claramente 1 $\implies$ 2, veremos la recíproca: Para ello basta probar por inducción que todo polinomio está asociado al polinomio

característico de una matriz. En particular el polinomio característico de

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

es

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

□

Definición 6.16: Se dice que un endomorfismo $f \in L(\mathbb{k}^n)$ es *triangularizable* syss existe una base ordenada X tal que su representación matricial es triangular. En el caso de matrices cuadradas, si existe $C \in \mathrm{Mat}_n(\mathbb{k})$ tal que $C^{-1}BC$ es triangular.

Teorema 6.17: Para un endomorfismo sobre V, son equivalentes:

1. f es triangularizable.
2. Existe una cadena maximal de subespacios f-invariantes:

$$0 =: V_0 \subset V_1 \subset \cdots \subset V_n := V$$

Demostración: 1) $\implies$ 2). Si f es triangularizable, entonces sea $X := (x_1, \ldots, x_n)$ la base para la que f es triangular. Luego la cadena viene dada por $V_k := \langle x_1, \ldots, x_k \rangle$.
2) $\implies$ 1). Basta ir formando la base a partir de puntos en los V_k, tomamos un vector no nulo en V_1, luego $x_2 \in V_2 \setminus V_1$ y así. □

Ejemplo (matriz triangular no diagonalizable). Consideremos

$$B = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$$

para que B sea diagonalizable ha de existir C invertible tal que $C^{-1}BC$ sea diagonal, es decir:

$$C^{-1}BC = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{\det C}\begin{bmatrix} ad+dc-bc & d^2 \\ -c^2 & ad-bc-cd \end{bmatrix}.$$

luego $c = d = 0$, pero en éste caso $\det C = 0$ lo que es una contradicción.

§6.1.1 El teorema fundamental del álgebra II. Ésta demostración hace uso de cierta noción muy básica de análisis. Aquí aplicaremos una inducción extraña para la cual admitimos la siguiente definición:

> $P(\Bbbk, d, r)$: Todo conjunto $A_1, \ldots, A_r$ de matrices cuyo producto conmuta sobre $\Bbbk^n$ con $d \nmid n$ posee un autovector en común.

Lema 6.18: Si $P(\Bbbk, d, 1)$, entonces para todo $r \geq 1$ se cumple que $P(\Bbbk, d, r)$.

Demostración: Probaremos la propiedad $P(\Bbbk, d, r+1)$ por inducción fuerte sobre la dimensión n del espacio vectorial: El caso $n = 1$ es trivial. Sean $A_1, \ldots, A_r, A_{r+1}$ matrices conmutativas en $\Bbbk^{n+1}$ con $d \nmid n+1$. Como $P(\Bbbk, d, 1)$ se cumple, entonces A_{r+1} tiene un autovalor λ, luego se define $B := A_{r+1} - \lambda I$ y se definen

$$U := \ker(B), \qquad W := \operatorname{Img}(B),$$

que por conmutatividad de los endomorfismos son invariantes para todo A_i (¿por qué?).

Si $U = V$, entonces $A_{r+1} = \lambda v$ para todo $v \in V$, luego todos son autovectores de V, así que cualqueir autovector común de $A_1, \ldots, A_r$ lo es con A_{r+1}.

Si $U \neq V$, entonces como $\dim W + \dim Z = \dim V$ hay alguno que tiene dimensión no divisible por d, sin perdida de generalidad supongamos que es U. Luego, por inducción, $A_1, \ldots, A_{r+1}$ tienen un autovector común en $W \subseteq V$. □

Proposición 6.19: Se cumple que $P(\mathbb{R}, 2, r)$ para todo $r \in \mathbb{N}_{\neq 0}$

Demostración: Para ésto basta ver que $P(\mathbb{R}, 2, 1)$, lo que equivale a ver que toda matriz $B \in \operatorname{Mat}_n(\mathbb{R})$ tiene autovectores para n impar. En este caso, el polinomio característico de B es de grado impar, y todo polinomio de grado impar sobre $\mathbb{R}$ tiene raíces. □

Definición 6.20 – *Matriz hermitiana*: Dada $B \in \operatorname{Mat}_n(\mathbb{C})$, se denota por $B^* := \overline{B}^t$. Se dice que B es *hermitiana* (o *auto-adjunta* en algunos libros) si $B = B^*$.

Corolario 6.21: El conjunto de las matrices hermitianas de $n \times n$ es un $\mathbb{R}$-espacio vectorial de dimensión n^2.

Pista: Recuerde que en la diagonal de una matriz hermitiana sólo pueden ir números reales. □

Lema 6.22: Se cumple que $P(\mathbb{C}, 2, 1)$.

Demostración: Sea $A \in \mathrm{Mat}_n(\mathbb{C})$ con n impar. Sea V el $\mathbb{R}$-espacio vectorial de las matrices hermitianas de $\mathrm{Mat}_n(\mathbb{C})$. Se definen los endomorfismos sobre V:

$$L_1(B) := \frac{AB + BA^*}{2}, \quad L_2(B) := \frac{AB - BA^*}{2i}.$$

Ésta elección deriva de que

$$AB = \frac{AB + B^*A^*}{2} + \mathrm{i} \cdot \frac{AB - B^*A^*}{2i},$$

aplicando el hecho de que B es hermitiana.
Como V tiene dimensión n^2 impar, y L_1, L_2 son operadores que conmutan (¿por qué?), entonces comparten un autovector $B \in V$ en común, con lo que luego

$$AB = L_1(B) + \mathrm{i}L_2(B) = (\mu + \mathrm{i}\lambda)B,$$

osea B es autovector de A que es lo que se quería probar. □

Teorema 6.23: Para todo $k > 0$ se cumple que $P(\mathbb{C}, 2^k, 1)$. En consecuencia, toda matriz tiene autovalores en $\mathbb{C}$, y $\mathbb{C}$ resulta ser algebraícamente cerrado.

Demostración: Lo probaremos por inducción fuerte sobre k, habiendo ya probado el caso base. Sea $A \in \mathrm{Mat}_n(\mathbb{C})$ con $2^{k-1} \mid n$ y $2^k \nmid n$. Sea V el conjunto de matrices anti-simétricas complejas de orden $n \times n$ (i.e., $B \in V$ syss $B^t = -B$). Se definen los endomorfismos sobre V:

$$L_1(B) := AB - BA^t, \quad L_2(B) := ABA^t$$

que conmutan (¡demuéstrelo!). Nótese que $\dim V = \frac{n(n-1)}{2}$ y cumple que $2^{k-1} \nmid \dim V$, luego por hipótesis inductiva existe B autovector común, de modo que

$$L_2(B) = \mu B = A(BA^t) = A(AB - L_1(B)) = A(AB - \lambda B)$$

luego despejando B se obtiene que

$$(A^2 - \lambda A + \mu I)B = 0,$$

tomando alguna columna no nula $\boldsymbol{v}$ de B se tiene que

$$(A^2 - \lambda A + \mu I)\boldsymbol{v} = 0.$$

Como en $\mathbb{C}$ todo polinomio cuadrático se escinde se tiene que existen $\alpha, \beta \in \mathbb{C}$ tales que $x^2 - \lambda x - \mu = (x - \alpha)(x - \beta)$. Por lo que, en conclusión:

$$(A - \alpha I)(A - \beta I)\boldsymbol{v} = 0$$

Luego o $(A - \beta I)v = 0$ con lo que v es autovector de A, o $(A - \beta I)v$ es autovector de A. □

§6.1.2 Teorema de Cayley-Hamilton. Si A es un dominio, entonces hemos probado que $A[x]$ también lo es. Usando ésto realizaremos comparaciones entre dos tipos de espacios cursiosos: $\mathrm{Mat}_n(A[x])$, es decir, el conjunto de matrices del anillo $A[x]$ de los polinomios de A; y $(\mathrm{Mat}_n A)[x]$, es decir, el conjunto de polinomios con coeficientes matrices de A.

Por ejemplo, un elemento de $\mathrm{Mat}_2(\mathbb{Z}[x])$ podría ser

$$\begin{bmatrix} x^2 + 1 & 3x \\ x^3 - 2x & 0 \end{bmatrix}$$

y un elemento de $(\mathrm{Mat}_2 \mathbb{Z})[x]$ podría ser

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 3 \\ -2 & 0 \end{bmatrix} X + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} X^2 + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} X^3.$$

Queremos probar que son isomorfos. Para ello admitimos el convenio de que $r_p(f)$ es el coeficiente que acompaña a la x, o que si f es de grado n, entonces $f(x) = \sum_{p=0}^{n} r_p(f)x^p$. Si $F \in \mathrm{Mat}_n(A[x])$ entonces convenimos que $[r_p(F)]_{i,j} := r_p(F_{i,j})$ (en general denotaremos elementos de $\mathrm{Mat}_n(A[x])$ con letras mayúsculas).

Proposición 6.24: Sean $F, G \in \mathrm{Mat}_n(A[x])$, entonces para todo k:

1. $r_p(F + G) = r_p(F) + r_p(G)$.
2. $r_p(F \cdot G) = \sum_{\ell=0}^{p} r_\ell(F) r_{p-\ell}(G)$

Demostración: La primera es trivial, la segunda tiene la misma forma que los coeficientes del producto de polinomios y es el resultado de una manipulación algebraíca:

$$(r_p(F \cdot G))_{ij} = r_p((F \cdot G)_{ij}) = r_p\left(\sum_{k=1}^{n} F_{ik} G_{kj}\right)$$

$$= \sum_{k=1}^{n} r_p(F_{ik}G_{kj}) = \sum_{k=1}^{n}\sum_{\ell=0}^{p} r_\ell(F_{ik})r_{p-\ell}(G_{kj})$$
$$= \sum_{\ell=0}^{p}\sum_{k=1}^{n}[r_\ell(F)]_{ik}[r_{p-\ell}(G)]_{kj} = \sum_{\ell=0}^{p} r_\ell(F)r_{p-\ell}(G).$$

□

Teorema 6.25:

$$\mathrm{Mat}_n(A[x]) \cong (\mathrm{Mat}_n\, A)[x]$$

Teorema 6.26 – *Teorema de Cayley-Hamilton*: Si B es una matriz cuadrada de polinomio característico $p_B(x) = a_0 + a_1x + \cdots + a_nx^n$, entonces

$$p_B(B) = a_0I + a_1B + \cdots + a_nB^n = 0.$$

Demostración: Sea $\varphi : \mathrm{Mat}_n(A[x]) \to (\mathrm{Mat}_n\, A)[x]$ el isomorfismo canónico. Sabemos que se define

$$p_B(x) := \det(xI - B),$$

y que

$$(\mathrm{adj}\, B)B = \det(B)I$$

de modo que

$$\mathrm{adj}(xI - B)(xI - B) = p_B(x)I$$

notemos que ésta es una relación sobre $\mathrm{Mat}_n(A[x])$ (pues la matriz a la derecha tiene por coordenadas polinomios), luego por el teorema anterior se cumple que se traduce a $(\mathrm{Mat}_n\, A)[X]$:

$$\mathrm{adj}(X - B)(X - B) = p_B(X),$$

finalmente por regla de Ruffini como $X - B$ divide a $p_B(X)$ se cumple que $X = B$ es raíz de $p_B(X)$. □

6.2. Espacios duales

Dado un $\Bbbk$-espacio vectorial V, entonces $V^* := L(V, \Bbbk)$ es el espacio formado por funcionales lineales desde V.

Ésta demostración es de [25].

Proposición 6.27: Se cumple:

1. Si $\dim V < \infty$ entonces $\dim V = \dim V^*$.
2. Existe un monomorfismo canónico $\iota : V \to V^*$ tal que establece un isomorfismo entre V y $\iota[V]$.
3. (AEN) Si $\dim V$ es infinito, entonces $\dim V < \dim V^*$.

Demostración: La primera es trivial, probaremos la segunda: Consideremos que $\{\boldsymbol{e}_i\}_{i\in I}$ es base de V, de modo que $\dim V = |I|$. Para construir el monomorfismo, definimos $\iota(\boldsymbol{e}_i)$ como el funcional tal que $[\iota(\boldsymbol{e}_i)](\boldsymbol{e}_j) = \delta_{ij}$. Luego al extender linealmente a ι le definimos sobre todo V y vemos que la imágen sobre la base genera un conjunto linealmente independiente en V^*. Claramente ι es inyectiva y prueba que $\dim V \leq \dim V^*$ en todo caso.

Para probar la tercera probaremos varios pasos:

1. **Si $\Bbbk \leq \aleph_0$, entonces $|V| = |I|$:**
   Claramente $|V| \geq |I|$, así que veremos la otra implicancia. Veamos que V puede ser visto como un subconjunto de S, donde S es la familia de subconjuntos finitos de $\Bbbk \times I$, por lo que,
   $$|V| \leq |S| = \left|[\Bbbk \times I]^{<\aleph_0}\right| = |\aleph_0| \cdot |\Bbbk \times I| = |I|.$$
2. **Si $\Bbbk \leq \aleph_0$, entonces $\dim V < \dim V^*$:**
   Simple: como toda función lineal viene determinada exclusivamente por los valores en la base, se cumple que
   $$|V| = |\operatorname{Func}(I;\Bbbk)| = |\Bbbk|^{|I|} \geq 2^{|I|} > |I| = |V|$$
   donde la última desigualdad es el teorema de cardinalidad de Cantor.
3. **Caso arbitrario:**
   Notemos que $\Bbbk$, por ser un cuerpo, siempre contiene a otro cuerpo
   $$F := \begin{cases} \mathbb{Q}, & \operatorname{car}\Bbbk = 0 \\ \mathbb{F}_p, & \operatorname{car}\Bbbk = p \end{cases}$$
   Luego si $W := \operatorname{Span}_F(\boldsymbol{e}_i)_{i\in I}$ vemos que $\dim_F W = \dim_\Bbbk V$, y sabemos que $\dim_F W < \dim_k W^*$, así que basta probar que $\dim_F W^* \leq \dim_\Bbbk V^*$.

   Sea $G \in L_F(W^*, V^*)$ definida así: Sea $\varphi \in W^*$, es decir, $\varphi : W \to F$ es F-lineal y queremos que $G(\varphi) : V \to \Bbbk$ sea $\Bbbk$-lineal. Sea $\boldsymbol{v} \in V$, existe

$(\lambda_i)_{i\in I} \in \Bbbk$ tal que es nula excepto en finitos índices y $\boldsymbol{v} = \sum_{i\in I} \lambda_i \boldsymbol{e}_i$. Luego se define

$$[G(\varphi)](\boldsymbol{v}) = \sum_{i\in I} \lambda_i \varphi(\boldsymbol{e}_i)$$

el cual está bien definido y veamos que todo cumple las condiciones esperadas, dados

$$\boldsymbol{u} = \sum_{i\in I} \alpha_i \boldsymbol{e}_i, \quad \boldsymbol{v} = \sum_{i\in I} \beta_i \boldsymbol{e}_i$$

y dados $\lambda \in \Bbbk$ se cumple

a) Fijada $\varphi \in W^*$ vemos que

$$\begin{aligned}[G(\varphi)](\boldsymbol{u}+\boldsymbol{v}) &= \sum_{i\in I} (\alpha_i + \beta_i)\varphi(\boldsymbol{e}_i) \\ &= \sum_{i\in I} \alpha_i \varphi(\boldsymbol{e}_i) + \sum_{i\in I} \beta_i \varphi(\boldsymbol{e}_i) = [G(\varphi)](\boldsymbol{u}) + [G(\varphi)](\boldsymbol{v}).\end{aligned}$$

Y claramente $[G(\varphi)](\lambda \boldsymbol{v}) = \lambda [G(\varphi)](\boldsymbol{v})$ de modo que $G(\varphi)$ efectivamente es un elemento de V^*.

b) G es efectivamente una aplicación F-lineal (¿por qué?).

c) Si $\boldsymbol{u} \in W$, entonces $\alpha_i \in F$ y se cumple que

$$\varphi(\boldsymbol{u}) = \varphi\left(\sum_{i\in I} \alpha_i \boldsymbol{e}_i\right) = \sum_{i\in I} \alpha_i \varphi(\boldsymbol{e}_i) = [G(\varphi)](\boldsymbol{u})$$

De ésto se deduce que G es inyectiva.

Por ende G comprueba que $\dim_F W^* \leq \dim_F V^*$, pero queremos ver algo más fuerte ...

□

6.3. Formas bilineales

Cuando definimos el determinante nos topamos con la noción de forma multilineal, en este capítulo la retomamos pero sólo admitiendo dos coordenadas.

§6.3.1 Formas bilineales.

Definición 6.28 – *Forma bilineal*: Una forma bilineal $F \in L(V, V; \Bbbk)$ es una forma multilineal de $V \times V$ a $\Bbbk$, donde V es un $\Bbbk$-espacio vectorial. En general también exigiremos que F sea simétrica, es decir, que $F(\boldsymbol{u}, \boldsymbol{v}) = F(\boldsymbol{v}, \boldsymbol{u})$ para todo $\boldsymbol{u}, \boldsymbol{v} \in V$.
Si $\boldsymbol{u}, \boldsymbol{v}$ cumplen que $F(\boldsymbol{u}, \boldsymbol{v}) = 0$ para una forma bilineal simétrica, entonces diremos que son *ortogonales* respecto a F, lo que denotaremos por $\boldsymbol{u} \perp \boldsymbol{v}$.

Sea $B := (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ una base de V, entonces se le llama representación matricial de la forma bilineal F según B a

$$\mathrm{M}_B(F) := [F(\boldsymbol{x}_i, \boldsymbol{x}_j)]_{ij}$$

Si F es una forma bilineal simétrica, decimos que $q : V \to \Bbbk$ definido por $q(\boldsymbol{v}) := F(\boldsymbol{v}, \boldsymbol{v})$ es su *forma cuadrática* asociada.

Proposición 6.29: Dada una forma bilineal F sobre $\Bbbk^n$ con base ordenada B, se cumple que una matriz $M = \mathrm{M}_B(F)$ syss para todo $\boldsymbol{u}, \boldsymbol{v} \in \Bbbk^n$ se cumple que

$$F(\boldsymbol{u}, \boldsymbol{v}) = \pi_B(\boldsymbol{u}) M \pi_B(\boldsymbol{v})^t.$$

Luego si denotamos $(\boldsymbol{u}, \boldsymbol{v}) := \pi_B(\boldsymbol{u})\pi_B(\boldsymbol{v})^t$ para alguna base fijada, como la canónica, entonces toda forma bilineal F corresponde a

$$F(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}A, \boldsymbol{v}) = (\boldsymbol{u}, \boldsymbol{v}A^t)$$

con una matriz A.

Proposición 6.30: Si F es una forma bilineal simétrica, entonces su representación matricial bajo cualquier base también lo es.

Teorema 6.31: Si V es un $\Bbbk$-espacio vectorial con $\operatorname{car} \Bbbk \neq 2$ y $\dim V < \infty$, entonces si F es una forma bilineal simétrica sobre V, V posee una base ortogonal respecto a F.

Demostración: La demostración es por inducción sobre n, la dimensión de V. El caso base es trivial.
Si F es nula, entonces toda base es ortogonal. De lo contrario, sean $\boldsymbol{u}, \boldsymbol{v}$ tales que $F(\boldsymbol{u}, \boldsymbol{v}) \neq 0$, luego si q es su forma cuadrática, entonces

$$q(\boldsymbol{u} + \boldsymbol{v}) = q(\boldsymbol{u}) + 2F(\boldsymbol{u}, \boldsymbol{v}) + q(\boldsymbol{v})$$

de modo que q es no nulo para al menos alguno entre $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{u}+\boldsymbol{v}$; sea $\boldsymbol{e}_1$ alguno de ellos. Sea

$$W := \{\boldsymbol{x} \in V : \boldsymbol{x} \perp \boldsymbol{e}_1\}.$$

Vamos a probar que $V = \operatorname{Span}(\boldsymbol{e}_1) \oplus W$: Sea $\boldsymbol{x} \in \operatorname{Span}(\boldsymbol{e}_1) \cap W$, entonces $\boldsymbol{x} = \alpha \boldsymbol{e}_1 \perp \boldsymbol{e}_1$ satisface que $F(\boldsymbol{x}, \boldsymbol{e}_1) = 0 = \alpha F(\boldsymbol{e}_1, \boldsymbol{e}_1)$ de modo que $\alpha = 0$ y $\boldsymbol{x} = \vec{0}$.
Notemos que $\boldsymbol{x} \mapsto F(\boldsymbol{x}, \boldsymbol{e}_1)$ es un funcional lineal (por definición de forma bilineal) suprayectivo y cuyo kernel es W, de modo que por fórmula de dimensiones se cumple que $\dim W = n - 1$, de modo que $\dim(\operatorname{Span}(\boldsymbol{e}_1) \oplus W) = n$ y se comprueba nuestra hipótesis.

Finalmente como W tiene dimensión menor, por hipótesis inductiva, posee base ortogonal $\boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ y añadirle $\boldsymbol{e}_1$ genera una base ortogonal para V. □

Supongamos que sea $(\boldsymbol{e}_i)_i$ una base ortogonal de V según una forma bilineal simétrica F de representación matricial A, entonces si M es la matriz cambio de base a ella, entonces se cumple que

$$F(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}A, \boldsymbol{v}) = ((\boldsymbol{u}M)B, \boldsymbol{v}M) = (\boldsymbol{u}(MBM^t), \boldsymbol{v})$$

De modo que $A = MBM^t$.

Definición 6.32: Se dice que dos matrices A, B son *congruentes* si existe M invertible tal que $A = MBM^t$.

Por ende hemos probado:

Teorema 6.33: Toda matriz simétrica sobre un campo escalar de característica distinta de 2 es congruente a una matriz diagonal.

Sea F una forma bilineal simétrica con base ortonormal $(\boldsymbol{x}_i)_i$, entonces si B es la representación diagonal de F por el teorema anterior, B tiene por diagonal $\alpha_i^2 \lambda_i$ donde $\lambda_i := F(\boldsymbol{x}_i, \boldsymbol{x}_i)$ y α_i es un escalar que multiplicamos por $\boldsymbol{x}_i$ a conveniencia, luego es claro que:

Teorema 6.34: Si $\operatorname{car} \Bbbk \neq 2$ y todo elemento de $\Bbbk$ posee raíz cuadrada, entonces toda matriz simétrica es congruente a una única matriz $[\underbrace{1, \ldots, 1}_{r}, 0, \ldots, 0]$.

En $\mathbb{C}$ ésto es claro, pero en $\mathbb{R}$ no sucede. Lo mejor que tenemos en $\mathbb{R}$ es una matriz diagonal con 1s, (-1)s y 0s.

Proposición 6.35: Si $\operatorname{car}\mathbb{k} \neq 2$, entonces si F es una forma bilineal simétrica sobre V con forma cuadrática asociada q, entonces F está completamente determinada por

$$F(u,v) = \frac{q(u+v) - q(u) - q(v)}{2}.$$

De éste modo podemos definir una forma cuadrática de tal modo que la función descrita cumpla ser una forma bilineal simétrica.

Definición 6.36: Dada una forma cuadrática q sobre V, se dice que posee alguna de las siguientes propiedades si para todo $\boldsymbol{v} \in V$:

Definida positiva Si $\boldsymbol{x} \neq 0$ implica $q(\boldsymbol{x}) > 0$.

Semidefinida positiva Si $q(\boldsymbol{x}) \geq 0$.

Definida negativa Si $\boldsymbol{x} \neq 0$ implica $q(\boldsymbol{x}) < 0$.

Semidefinida negativa Si $q(\boldsymbol{x}) \leq 0$.

§6.3.2 Formas sesquilineales, producto interno y "geometría euclídea".

Definición 6.37 – *Forma sesquilineal*: Sea H un $\mathbb{K}$-espacio vectorial, se dice que $F : H^2 \to \mathbb{K}$ es una forma sesquilineal si para todo $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in H$ y $\alpha \in \mathbb{K}$ se cumple:

1. $F(\boldsymbol{u}, \boldsymbol{v}) = \overline{F(\boldsymbol{v}, \boldsymbol{u})}$ (simetría hermitiana).
2. $F(\boldsymbol{u} + \boldsymbol{v}, \boldsymbol{w}) = F(\boldsymbol{u}, \boldsymbol{w}) + F(\boldsymbol{v}, \boldsymbol{w})$ (linealidad).
3. $F(\alpha\boldsymbol{u}, \boldsymbol{v}) = \alpha F(\boldsymbol{u}, \boldsymbol{v})$.

Las mismas nociones de representación matricial y formas cuadráticas (ahora llamadas *hermitianas*) aplica.

Proposición 6.38: Si F es una forma sesquilineal, entonces para todo $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^n$ y todo $\alpha \in \mathbb{K}$ se cumple:

1. $F(\boldsymbol{u}, \alpha\boldsymbol{v}) = \bar{\alpha} F(\boldsymbol{u}, \boldsymbol{v})$.
2. $F(\boldsymbol{u}, \boldsymbol{u}) \in \mathbb{R}$.

El resultado anterior permite conservar las definiciones para forma cuadrática en $\mathbb{R}$ y nos permite ver un análogo para la representación matricial:

Teorema 6.39: Dada una forma sesquilineal F sobre $\mathbb{K}^n$ con base ordenada B, se cumple que una matriz $A := \mathrm{M}_B(F)$ syss para todo $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^n$ se cumple que

$$F(\boldsymbol{u}, \boldsymbol{v}) = \pi_B(\boldsymbol{u}) A \pi_B(\boldsymbol{v})^*$$

Luego si denotamos $(\boldsymbol{u}, \boldsymbol{v}) := \pi_B(\boldsymbol{u})\pi_B(\boldsymbol{v})^*$, entonces toda forma sesquilineal corresponde a

$$F(\boldsymbol{u}, \boldsymbol{v}) = (\boldsymbol{u}A, \boldsymbol{v}) = (\boldsymbol{u}, \boldsymbol{v}A^*).$$

Definición 6.40 – *Producto interno*: Se dice que una forma sesquilineal $(,) : H^2 \to \mathbb{K}$ es un *producto interno* si su forma cuadrática asociada es definida positiva. Un par $(H, (,))$ se dice un *espacio vectorial con producto interno* o un *espacio prehilbertiano*. En éste capítulo, H siempre representará un espacio prehilbertiano.

Denotamos $\| \| : H \to [0, \infty)$ a la aplicación

$$\|\boldsymbol{x}\| := \sqrt{(\boldsymbol{x}, \boldsymbol{x})},$$

que ésta bien definida y sólo toma 0 en el $\vec{0}$.

§6.3.3 Formas hermitianas y espacios de producto interno.

Definición 6.41 – *Forma hermitiana*: Sea H un $\mathbb{K}$-espacio vectorial, se dice que $f : H^2 \to \mathbb{K}$ es una forma hermitiana si para todo $u, v, w \in H$ y $\alpha \in \mathbb{K}$ se cumple:

1. $f(u, v) = \overline{f(v, u)}$ (simetría hermitiana).
2. $f(u + v, w) = f(u, w) + f(v, w)$ (linealidad).
3. $f(\alpha u, v) = \alpha f(u, v)$.

Se dice que $\langle , \rangle : H^2 \to \mathbb{K}$ es un *producto interno* si es una forma hermitiana que satisface que $f(u, u) = 0$ syss $u = \mathbf{0}$, y que $f(u, u) \geq 0$. Un par $(H, \langle , \rangle)$ se dice un *espacio prehilbertiano*.

Si H es prehilbertiano, entonces se define

$$\|x\| := \sqrt{\langle x, x\rangle}.$$

En este capítulo, H siempre denotara un espacio prehilbertiano.

Proposición 6.42: Si f es una forma hermitiana sobre H, entonces, para todo $u, v \in H$ y $\alpha \in \mathbb{K}$:

1. $f(u, \alpha v) = \overline{\alpha} f(u, v)$.
2. $f(u, u) \in \mathbb{R}$.

DEMOSTRACIÓN: Para probar el segundo veamos primero que por simetría hermitiana $f(u, u)$ ha de ser real. □

Lema 6.43: 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 6.44: 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 6.45: Sean $A, B \in \mathrm{End}(H)$. Se cumple que $A = B$ syss para todo $x, y \in H$ se cumple que $\langle Ax, y\rangle = \langle Bx, y\rangle$.

DEMOSTRACIÓN: Basta fijar un x cualquiera para que variar el y concluya que $Ax = Bx$ para dicho x. Luego variando todo x se cumple que $Ax = Bx$ para todo $x \in H$, i.e., $A = B$. □

Teorema 6.46 – *Desigualdad de Cauchy-Schwarz*: Para todo $x, y \in H$ se cumple:

$$|\langle x, y\rangle| \leq \|x\| \, \|y\|$$

DEMOSTRACIÓN: Supongamos que $y \neq 0$ (pues $y = 0$ es trivial), entonces notemos que

$$\begin{aligned} 0 \leq \langle x - \alpha y, x - \alpha y\rangle &= \langle x, x\rangle - \alpha \langle y, x\rangle - \overline{\alpha} \langle x, y\rangle + |\alpha|^2 \langle y, y\rangle \\ &= \|x\|^2 - 2\,\mathrm{Re}(\alpha \langle y, x\rangle) + |\alpha|^2 \|y\|^2. \end{aligned}$$

para todo $\alpha \in \mathbb{k}$, luego sea $\alpha := \frac{\langle x,y\rangle}{\|y\|^2}$ y despejemos un poco:

$$0 \leq \|x\|^2 - 2\frac{\langle x,y\rangle \langle y,x\rangle}{\|y\|^2} + \frac{|\langle x,y\rangle|^2}{\|y\|^2} = \|x\|^2 - \frac{|\langle x,y\rangle|^2}{\|y\|^2},$$

de lo que se concluye el resultado. □

Teorema 6.47 (Desigualdad traingular): Para todo $x, y \in H$ se cumple que

$$\|x+y\| \leq \|x\| + \|y\|,$$

luego, $\|\,\| : H^2 \to \mathbb{R}$ es una norma.

Demostración: Basta aplicar el siguiente procedimiento:

$$\begin{aligned}
\|x+y\|^2 &= \langle x+y, x+y\rangle \\
&= \langle x,x\rangle + \langle x,y\rangle + \langle y,x\rangle + \langle y,y\rangle \\
&= \|x\|^2 + 2\,\mathrm{Re}(\langle x,y\rangle) + \|y\|^2 \\
&\leq \|x\|^2 + 2|\langle x,y\rangle| + \|y\|^2 \\
&\leq \|x\|^2 + 2\|x\|\cdot\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2.
\end{aligned}$$

□

Llamaremos *unitarios* a los vectores de norma 1.

Definición 6.48 – *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 6.49: Se cumple:

1. $\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2$ (ley del paralelogramo).
2. $x \perp y$ syss $\|x+y\|^2 = \|x\|^2 + \|y\|^2$ (teorema de Pitágoras I).
3. Si $\{x_i\}_{i=1}^n$ es una sucesión ortonormal, entonces para todo $i \leq n$ se cumple $x_i \perp \sum_{j\neq i} x_j$.

4. Si $\{x_i\}_{i=1}^n$ es una sucesión ortonormal, entonces para todo $x \in H$ se cumple
$$\|x\|^2 = \sum_{i=1}^n |\alpha_i|^2 + \left\| x - \sum_{i=1}^n \alpha_i x_i \right\|^2,$$
donde $\alpha_i := \langle x, x_i \rangle$ (teorema de Pitágoras II).

Demostración:

4. Obsérvese que
$$x = \sum_{i=1}^n \alpha_i x_i + \left(x - \sum_{i=1}^n \alpha_i x_i \right).$$
Donde hay $n+1$ vectores, hemos de probar que todos son ortogonales entre sí para aplicar el teorema de Pitágoras. Es claro que $x_i \perp x_j$ con $i \neq j$, por ende, basta notar que
$$\begin{aligned} \left\langle x_k, x - \sum_{i=1}^n \alpha_i x_i \right\rangle &= \langle x_k, x \rangle - \sum_{i=1}^n \langle x_k, \alpha_i x_i \rangle \\ &= \langle x_k, x \rangle - \overline{\alpha_k} \cancelto{1}{\langle x_k, x_k \rangle} = 0. \end{aligned}$$

□

Teorema 6.50 – *Ortogonalización de Gram-Schmidt*: Si $\dim H \leq \aleph_0$ tiene una base $\{x_i\}_i$, entonces posee una base ortonormal $\{z_i\}_i$ que satisface que para todo $k > 0$:
$$\operatorname{Span}\{x_1, \ldots, x_k\} = \operatorname{Span}\{y_1, \ldots, y_k\}$$

Demostración: Sea $\{x_i\}$ una base cualquiera de H. Para el proceso de Gram-Schmidt primero definiremos $y_1 := x_1$. Luego queremos que $y_2 \perp y_1$ y que $\operatorname{Span}(x_1, x_2) = \operatorname{Span}(y_1, y_2)$, para lo cual
$$y_2 := x_2 - \frac{\langle x_2, y_1 \rangle}{\|y_1\|^2} y_1$$
que comprueba cumplir nuestras condiciones (¿por qué?). Así se define por recursión
$$y_{n+1} := x_{n+1} - \sum_{k=1}^n \frac{\langle x_{n+1}, y_k \rangle}{\|y_k\|^2} y_k$$
Finalmente se normaliza $\{y_i\}$ en $\{z_i\}$ y ya está. □

Proposición 6.51: Se cumple:

1. Si $S \subseteq H$, entonces $S^\perp \leq H$.
2. Para todo $S \subseteq H$ se cumple que $S \subseteq (S^\perp)^\perp$.

Si exigimos que $\dim H \leq \aleph_0$, entonces para todo $E \leq H$ se cumple que:

3. Existe una única transformación lineal $\pi_E : H \to E$ tal que $\pi_E(v) = v$ si $v \in E$ y $\pi_E(v) = 0$ si $v \notin E$, a la que llamamos *proyección ortogonal* sobre E.
4. $E \oplus E^\perp = H$.
5. $(E^\perp)^\perp = E$.

Demostración: Se elige $\{x_i\}_i$ base ortonormal de H que contiene una subsucesión $\{y_i\}_i$ que es base (también ortonormal) de E. Finalmente π_E lo que hace es anular los coeficientes de $\{x_i\}_i$ que no están en $\{y_i\}_i$. □

¿Y cómo se ve el producto interno? Sea $\{x_i\}$ una base ortonormal de H y sean $\boldsymbol{u}, \boldsymbol{v} \in H$. Por definición de base existen unas sucesiones de escalares $(\alpha_i)_i$ y $(\beta_i)_i$ tales que

$$\boldsymbol{u} = \sum_{i=1} \alpha_i x_i, \quad \boldsymbol{v} = \sum_{i=1} \beta_i x_i$$

luego

$$\begin{aligned}\langle \boldsymbol{u}, \boldsymbol{v} \rangle &= \left\langle \sum_{i=1} \alpha_i x_i, \boldsymbol{v} \right\rangle = \sum_{i=1} \alpha_i \langle x_i, \boldsymbol{v} \rangle \\ &= \sum_{i=1} \alpha_i \left\langle x_i, \sum_{j=1} \beta_j x_j \right\rangle = \sum_{i=1} \alpha_i \sum_{j=1} \bar{\beta}_j \langle x_i, x_j \rangle \\ &= \sum_{i=1} \alpha_i \sum_{j=1} \bar{\beta}_j \delta_{ij} = \sum_{i=1} \alpha_i \bar{\beta}_i.\end{aligned}$$

Luego, todo el producto interno queda completamente determinado por una base ortonormal. Si exigimos que la base canónica sea ortonormal por definición, entonces se tiene que

$$\langle (u_1, \ldots, u_n), (v_1, \ldots, v_n) \rangle = \sum_{i=1}^{n} u_i \bar{v}_i.$$

Es más, si identificamos $H := \mathrm{Mat}_{n\times 1}(\mathbb{C})$, entonces tenemos que para todo $\boldsymbol{u}, \boldsymbol{v} \in H$ se cumple que

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \overline{\boldsymbol{v}}^t \boldsymbol{u}.$$

Corolario 6.52 (Desigualdad de Bessel): Sea $\{x_i\}$ una sucesión[1] ortonormal, entonces para todo $x \in H$ se cumple

$$\sum_i |\alpha_i|^2 \leq \|x\|^2,$$

donde $\alpha_i := \langle x, x_i \rangle$.

Pista: Para probar el caso de un conjunto ortonormal infinito, basta notar que para todo n se cumple por el teorema de Pitágoras, por ende, la sucesión dada por las sumas parciales es creciente y acotada, ergo, converge. □

Teorema 6.53: Sea $\{x_i\}_{i=0}^n$ una sucesión finita ortonormal y $x \in H$. Entonces, los escalares $\lambda_i \in \Bbbk$ que minimizan el valor de

$$\left\| x - \sum_{i=0}^{n} \lambda_i x_i \right\|$$

son únicos y son $\lambda_i = \langle x, x_i \rangle$.

Demostración: Observe que

$$\begin{aligned}
\left\| x - \sum_{i=0}^{n} \lambda_i x_i \right\|^2 &= \|x\|^2 - \sum_{i=0}^{n} (\overline{\lambda_i} \langle x, x_i \rangle + \lambda_i \overline{\langle x, x_i \rangle}) + \left\| \sum_{i=0}^{n} \lambda_i x_i \right\|^2 \\
&= \|x\|^2 + \sum_{i=0}^{n} |\lambda_i|^2 - \sum_{i=0}^{n} (\overline{\lambda_i} \langle x, x_i \rangle + \lambda_i \overline{\langle x, x_i \rangle}) \\
&\quad + \sum_{i=0}^{n} |\langle x, x_i \rangle|^2 - \sum_{i=0}^{n} |\langle x, x_i \rangle|^2 \\
&= \|x\|^2 + \sum_{i=0}^{n} |\lambda - \langle x, x_i \rangle|^2 - \sum_{i=0}^{n} |\langle x, x_i \rangle|^2,
\end{aligned}$$

de aquí es fácil deducir el enunciado. □

[1] Aquí se obvian los límites de los índices pues el resultado es válido tanto para sucesiones finitas como infinitas.

Corolario 6.54: 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 6.55 (Identidad de Parseval): Una sucesión ortonormal $\{x_i\}$ es base de H syss para todo $x \in H$ se cumple

$$\|x\|^2 = \sum_i |\langle x, x_i \rangle \, x_i|^2.$$

§6.3.4 Formas cuadráticas.

Definición 6.56 – *Formas bilineales y cuadráticas*: Sea V un $\Bbbk$-espacio vectorial. Se dice que $F : V^2 \to \Bbbk$ es una *forma bilineal* si para todo $u, v, w \in V$ y todo $\alpha, \beta \in \Bbbk$ se cumple:

1. $F(\alpha u + \beta v, w) = \alpha F(u, w) + \beta F(v, w)$.
2. $F(u, \alpha v + \beta w) = \alpha F(u, v) + \beta F(u, w)$.

y se dice que una forma bilineal es *simétrica* si $F(u, v) = F(v, u)$.
Dada una forma bilineal F, se le dice la *forma cuadrática* asociada a F a $q : V \to \Bbbk$ es $q(v) := F(v, v)$.

Proposición 6.57: 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.

Parte III.

Álgebra Conmutativa y Geometría Algebraica

7

Introducción al álgebra conmutativa

7.1. Anillos locales y radicales

Definición 7.1: Se dice que un anillo unitario A es un *anillo local* si sólo posee un ideal maximal.

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 7.2: Todo elemento no inversible está contenido en un ideal maximal.

Demostración: Basta notar que $(a) \neq (1)$ si a no es inversible. □

Proposición 7.3: 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 $(ax)^{-1}a = x^{-1}$. □

Definición 7.4: 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 7.5: Sea S un sistema multiplicativo, entonces la relación $\sim$ sobre $A \times S$ dada por

$$(a, s) \sim (b, t) \iff \exists r \in S \quad r(at - bs) = 0$$

es de equivalencia.

Demostración: La reflexividad y simetría son triviales. Veamos la transitividad: sean $(a, s) \sim (b, t)$ y $(b, t) \sim (c, u)$. Por definición sean $r_1, r_2 \in S$ tales que

$$r_1(at - bs) = r_2(bu - ct) = 0$$

luego, nótese que $r_2, t, s \in S$ de modo que

$$r_1 r_2(uat - ubs) = r_1 r_2(sbu - sct) = 0$$

sumando ambas ecuaciones se obtiene que

$$r_1 r_2(uat - sct) = r_1 r_2 t(au - cs) = 0$$

con $r_1 r_2 t \in S$ como se quería probar. □

Definición 7.6: 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 7.7: $(S^{-1}A, +, \cdot)$ es un dominio de neutro aditivo $0/1$, neutro multiplicativo $1/1$, donde

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

y la función $\lambda_S \colon A \to S^{-1}A$ dada por $\lambda_S(a) = a/1$ es un morfismo de anillos. Más aún, $S^{-1}A$ es un A-módulo, λ_S un morfismo de módulos y todo elemento de S es inversible en $S^{-1}A$.

Demostración: Hay que ver primero que las operaciones están bien definidas: Para ello sean $a_1/s_1 = a_2/s_2$ tales que $r(a_1s_2 - a_2s_1) = 0$ con $r \in S$. Nótese que basta ver que

$$\frac{a_1t + bs_1}{s_1t} = \frac{a_2t + bs_2}{s_2t}, \quad \frac{a_1b}{s_1t} = \frac{a_2b}{s_2t}.$$

Para ello nótese que

$$r\big((a_1t + b\cancel{s_1})s_2t - (a_2t + b\cancel{s_2})s_1t\big) = t^2 \cdot r(a_1s_2 - a_2s_1) = 0,$$
$$r\big(a_1bs_2t - a_2bs_1t\big) = bt \cdot r(a_1s_2 - a_2s_1) = 0.$$

Probar que es un anillo es análogo a las demostraciones de que $\mathrm{Frac}(A)$ lo es. Lo mismo para notar que λ_S es morfismo. □

Proposición 7.8: Sea $\mathfrak{p} \lhd A$ primo. Luego $S := A \setminus \mathfrak{p}$ es un sistema multiplicativo tal que $S^{-1}A$ 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. □

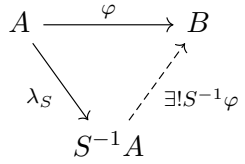
Lema 7.9: El morfismo λ_S es inyectivo syss S no posee divisores de cero.

Demostración: $\Longrightarrow$. Por contrarrecíproca: si $a \in S$ es divisor de cero, es decir, si $ab = 0$ con $b \neq 0$, entonces $\lambda_S(b) = \lambda_S(0)$.

$\Longleftarrow$. Sean $a, b \in A$ tales que $\lambda_S(a) = \lambda_S(b)$ lo que se traduce en que existe $r \in S$ tal que $r(a-b) = 0$; pero como r no es divisor de cero, entonces necesariamente $a - b = 0$ y $a = b$. $\square$

Teorema 7.10: Sean A, B dominios y S un sistema multiplicativo de A. Sea $\varphi\colon A \to B$ un morfismo tal que $\varphi[S] \subseteq B^\times$, entonces el siguiente diagrama conmuta:

$$\begin{aligned} S^{-1}\varphi\colon S^{-1}A &\longrightarrow B \\ a/s &\longmapsto \varphi(a)/s \end{aligned}$$



Demostración:

i) Veamos que dicho morfismo está bien definido: En primer lugar $\varphi(s)$ es inversible pues $\varphi[S] \subseteq B^\times$ y además si $a/s = b/t$ existe $r \in S$ tal que $r(at - bs) = 0$ y

$$0 = \varphi(r)\big(\varphi(at) - \varphi(bs)\big) = \varphi(a)\varphi(t) - \varphi(b)\varphi(s)$$

donde cancelamos a $\varphi(r)$ pues es inversible. Y así nos queda que $\bar{\varphi}(a/s) = \bar{\varphi}(b/t)$.

Ver que es morfismo de anillos y que el diagrama conmuta queda al lector.

ii) Veamos que es único: Supongamos que α, β hacen conmutar al diagrama y sea $a/s \in S^{-1}A$, entonces

$$\alpha(a/s) = \alpha(a/1)\alpha(1/s) = \varphi(a)\varphi(s)^{-1} = \beta(a/1)\beta(1/s) = \beta(a/s). \qquad \square$$

Así pues, queremos extender las construcciones anteriores para A-módulos, así que similarmente establecemos los siguientes resultados análogos:

Lema 7.11: Sea S un sistema multiplicativo de A y sea M un A-módulo, entonces la relación $\sim$ sobre $M \times S$ dada por

$$(\boldsymbol{u}, s) \sim (\boldsymbol{v}, t) \iff \exists r \in S \quad r(\boldsymbol{u}t - \boldsymbol{v}s) = \vec{0}$$

es de equivalencia.

Proposición 7.12: $S^{-1}M$ es un A-módulo (y un $S^{-1}A$-módulo también) y la función $\lambda_S\colon M \to S^{-1}M$ dada por $\lambda_S(\boldsymbol{m}) = \boldsymbol{m}/1$ es un morfismo de módulos. Más aún, λ_S es inyectiva syss S no posee al cero ni a divisores de cero.

Proposición 7.13: Sea S un sistema multiplicativo de A. Entonces determina un funtor entre los A-módulos:

$$\begin{aligned} S^{-1}f\colon S^{-1}M_1 &\longrightarrow S^{-1}M_2 \\ \boldsymbol{m}/s &\longmapsto f(\boldsymbol{m})/s \end{aligned} \qquad\qquad \begin{array}{ccc} M_2 & & S^{-1}M_2 \\ {\scriptstyle f}\uparrow & \xRightarrow{S^{-1}-} & \uparrow{\scriptstyle S^{-1}f} \\ M_1 & & S^{-1}M_1 \end{array}$$

que, de hecho, preserva exactitud, es decir, dada la siguiente sucesión exacta:

$$M_1 \xrightarrow{\ f\ } M_2 \xrightarrow{\ g\ } M_3$$

Entonces la siguiente sucesión también es exacta:

$$S^{-1}M_1 \xrightarrow{\ S^{-1}f\ } S^{-1}M_2 \xrightarrow{\ S^{-1}g\ } S^{-1}M_3$$

Proposición 7.14: Sea M un A-módulo y S un sistema multiplicativo de A. Entonces, para todo par N, T de submódulos de M se cumplen:

1. $S^{-1}N$ es un submódulo de $S^{-1}M$.
2. $S^{-1}(N+T) = S^{-1}N + S^{-1}T$.
3. $S^{-1}(N \cap T) = S^{-1}N \cap S^{-1}T$.
4. $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.
5. Si $\mathfrak{a}, \mathfrak{b}$ son ideales de A, entonces $S^{-1}(\mathfrak{a}\cdot\mathfrak{b}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$.

Proposición 7.15: Sea M un A-módulo. Entonces

$$\begin{gathered} f\colon S^{-1}A \otimes M \longrightarrow S^{-1}M \\ \sum_{k=1}^{n}(a_k/s_k)\otimes \boldsymbol{m}_k \longmapsto \sum_{k=1}^{n} a_k\boldsymbol{m}_k/s_k. \end{gathered}$$

es un isomorfismo, y más aún es el único entre dichos dominios.

Demostración: Consideremos la aplicación

$$\begin{aligned}\varphi\colon S^{-1}A \times M &\longrightarrow S^{-1}M\\ (a/s, \boldsymbol{m}) &\longmapsto a\boldsymbol{m}/s.\end{aligned}$$

Claramente φ es A-bilineal y por definición de producto tensorial se cumple que existe una única $\bar{\varphi}\colon S^{-1}A \otimes M \to S^{-1}M$ tal que $\varphi = \otimes \circ \bar{\varphi}$. Luego definimos $f := \bar{\varphi}$ que concuerda con el enunciado.

Claramente f es suprayectiva y para ver que es inyectiva. Primero veamos que todo tensor en $S^{-1}A \otimes M$ es puro: Para ello, definamos $s := \prod_{k=1}^{n} s_k$ y $t_i := \prod_{\substack{k=1\\k\neq i}}^{n} s_k$, luego:

$$\sum_{k=1}^{n} \frac{a_k}{s_k} \otimes \boldsymbol{m}_k = \sum_{k=1}^{n} \frac{a_k t_k}{s} \otimes \boldsymbol{m}_k = \sum_{k=1}^{n} \frac{1}{s} \otimes a_k t_k \boldsymbol{m} = \frac{1}{s} \otimes \left(\sum_{k=1}^{n} a_k t_k \boldsymbol{m} \right).$$

Luego, como $1/s$ es inversible, se cumple que $f(1/s \otimes \boldsymbol{m}) = \boldsymbol{m}/s = 0$ syss $\boldsymbol{m} = \vec{0}$. □

Corolario 7.16: $S^{-1}A$ es un A-módulo plano.

Definición 7.17: Sea A un dominio, entonces un elemento $a \in A$ es *nilpotente* si existe $n \geq 1$ tal que $x^n = 0$.

Proposición (AE) 7.18: Si S es un sistema multiplicativo que no contiene al 0, entonces existe el conjunto de los ideales contenidos en S^c posee un $\subseteq$-maximal que es de hecho un ideal primo del anillo.

Demostración: Sea $\mathcal{F} := \{\mathfrak{a} : \mathfrak{a} \trianglelefteq A, \mathfrak{a} \subseteq S^c\}$, y sea $\{\mathfrak{a}_i\}_{i\in I}$ una $\subseteq$-cadena de $\mathcal{F}$; ya sabemos que $\mathfrak{b} := \bigcup_{i\in I} \mathfrak{a}_i$ es también un ideal y claramente está también contenido en S^c. Luego por lema de Zorn $\mathcal{F}$ posee un elemento $\subseteq$-maximal $\mathfrak{p}$.

Probaremos que $\mathfrak{p}$ es primo por contradicción: Sea $ab \in \mathfrak{p}$ tales que $a, b \notin \mathfrak{p}$, entonces como $(a, \mathfrak{p}) \supset \mathfrak{p}$ se ha de cumplir que $(a, \mathfrak{p})$ y $(b, \mathfrak{p})$ poseen elementos de S, digamos:

$$s = r_1 a + p, \qquad s' = r_2 b + p'$$

con $s, s' \in S$, $r_1, r_2 \in A$ y $p, p' \in \mathfrak{p}$. Luego

$$s \cdot s' = r_1 r_2 ab + p'(r_1 a) + ps'$$

pero $s \cdot s' \in S$ y $ab, p, p' \in \mathfrak{p}$ lo que es absurdo puesto que $\mathfrak{p}$ no posee elementos de S. □

Corolario 7.19: 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 7.20: Dado un ideal $\mathfrak{a}$ se define su radical como

$$\mathrm{Rad}(\mathfrak{a}) = \{a \in A : \exists n\ a^n \in \mathfrak{a}\}.$$

Se dice que $\mathfrak{a}$ es *radical* si $\mathfrak{a} = \mathrm{Rad}(\mathfrak{a})$.

Se le llama el *nilradical* de A a $\mathrm{Rad}(0)$, es decir, al conjunto de los elementos nilpotentes.

El corolario anterior entonces se puede reescribir así:

$$\mathrm{Rad}(0) = \bigcap \{\mathfrak{p} : \mathfrak{p} \trianglelefteq A \text{ primo}\}.$$

El lector creerá que es un caso particular del radical, pero engloba a todo el resto haciendo la siguiente observación: Sea $\mathfrak{a}$ un ideal arbitrario de A, entonces el nilradical de $A/\mathfrak{a}$, bajo el teorema de la correspondencia, nos otorga el siguiente teorema:

Teorema (AE) 7.21: Si $\mathfrak{a}$ es un ideal de A, entonces

$$\mathrm{Rad}(\mathfrak{a}) = \bigcap \{\mathfrak{p} : \mathfrak{a} \subseteq \mathfrak{p} \trianglelefteq A,\ \mathfrak{p} \text{ primo}\}.$$

Corolario 7.22: 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 7.23: Para todo par de ideales $\mathfrak{a}, \mathfrak{b}$ en A se cumple:

1. Para todo $\mathfrak{a} \trianglelefteq A$ se cumple que $\mathfrak{a} \subseteq \mathrm{Rad}(\mathfrak{a}) \trianglelefteq A$.
2. $\mathrm{Rad}(\mathrm{Rad}(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a})$, es decir, todo radical de un ideal es un ideal radical.

3. $\mathrm{Rad}(\mathfrak{a}\cdot\mathfrak{b}) = \mathrm{Rad}(\mathfrak{a}\cap\mathfrak{b}) = \mathrm{Rad}(\mathfrak{a})\cap\mathrm{Rad}(\mathfrak{b})$.
4. $\mathrm{Rad}(\mathfrak{a}) = (1)$ syss $\mathfrak{a} = (1)$.
5. $\mathrm{Rad}(\mathfrak{a}+\mathfrak{b}) = \mathrm{Rad}(\mathrm{Rad}(\mathfrak{a}) + \mathrm{Rad}(\mathfrak{b}))$.
6. Si $\mathfrak{p}$ es primo, entonces $\mathrm{Rad}(\mathfrak{p}^n) = \mathfrak{p}$ para todo $n > 0$.
7. $\mathfrak{a}+\mathfrak{b} = (1)$ syss $\mathrm{Rad}(\mathfrak{a}) + \mathrm{Rad}(\mathfrak{b}) = (1)$.

Demostración: Probaremos las primeras dos:

1. Definamos $\mathfrak{r} := \mathrm{Rad}(\mathfrak{a})$. Claramente se cumple que $\mathfrak{a}\subseteq\mathrm{Rad}(\mathfrak{a})$, así que veamos que es un ideal. Para ello consideremos $a, b\in\mathfrak{r}$, de modo que $a^n, b^m\in\mathfrak{a}$ para algunos n, m:
   i) Para todo $\lambda\in A$ se da que $(\lambda a)^n = \lambda^n a^n\in\mathfrak{a}$, dado que $\mathfrak{a}$ es ideal.
   ii) Se cumple que $a+b\in\mathfrak{r}$: En efecto, basta notar que
   $$\begin{aligned}(a+b)^{n+m} &= \sum_{j=0}^{n+m}\binom{n+m}{j}a^j b^{n+m-j}\\ &= b^m\sum_{j=0}^{n}\binom{n+m}{j}a^j b^{n-j} + a^n\sum_{j=0}^{m}\binom{n+m}{n+j}a^j b^{m-j}.\end{aligned}$$
   iii) Claramente $a\cdot b\in\mathfrak{r}$ puesto que si $N := \mín\{n, m\}$, entonces $(ab)^N = a^N b^N$, donde alguno de los dos factores está en $\mathfrak{a}$, luego el producto también.
2. Por la proposición anterior claramente se da que $\mathrm{Rad}(\mathfrak{a})\subseteq\mathrm{Rad}(\mathrm{Rad}(\mathfrak{a}))$. Sea $a\in\mathrm{Rad}(\mathrm{Rad}(\mathfrak{a}))$, entonces $a^n\in\mathrm{Rad}(\mathfrak{a})$ y entonces $(a^n)^m\in\mathfrak{a}$ para algunos n, m. Pero entonces $(a^n)^m = a^{nm}\in\mathfrak{a}$, luego $a\in\mathrm{Rad}(\mathfrak{a})$. □

Definición 7.24: Sean S, T submódulos de un A-módulo M, entonces denotamos:
$$(S : T) := \{a\in A : aT\subseteq S\}.$$
Más aún, se define el *aniquilador* o *anulador* de T como
$$\mathrm{Ann}(T) := (0 : T).$$

Proposición 7.25: Sean $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ideales de A. Entonces:

1. $(\mathfrak{a} : \mathfrak{b})$ es un ideal.
2. Más generalmente, si S, T son submódulos de un A-módulo M, entonces $(S : T)$ es un ideal de A.
3. $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.
4. $\big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big) = (\mathfrak{a} : \mathfrak{bc}) = \big(\mathfrak{a} : \mathfrak{c} : \mathfrak{b}\big)$.
5. $\big(\bigcap_{i\in I} \mathfrak{a}_i : \mathfrak{b}\big) = \bigcap_{i\in I}(\mathfrak{a}_i : \mathfrak{b})$.
6. $\big(\mathfrak{a} : \sum_{i\in I} \mathfrak{b}_i\big) = \bigcap_{i\in I}(\mathfrak{a} : \mathfrak{b}_i)$.

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 $x \in \big(\mathfrak{a} : \sum_{i\in I} \mathfrak{b}_i\big)$, luego, nótese que como $0 \in \mathfrak{b}_i$ para todo ideal en general, se tiene que para todo $y \in \mathfrak{b}_i$ se cumple que $xy \in \mathfrak{a}$, luego $x \in (\mathfrak{a} : \mathfrak{b}_i)$ para todo $i \in I$. En particular x está en la intersección.

   La otra inclusión viene dada por que si $x \in \bigcap_{i\in I}(\mathfrak{a} : \mathfrak{b}_i)$, entonces para todo $y_i \in \mathfrak{b}_i$ se cumple que $xy_i \in \mathfrak{a}$, luego $x \sum_{i\in I} y_i \in \mathfrak{a}$. □

Proposición 7.26: Denotemos D el conjunto de los divisores de cero de A. Entonces

$$D = \bigcup_{x\neq 0} \mathrm{Rad}(\mathrm{Ann}(x)) = \bigcup_{x\neq 0} \mathrm{Ann}(x).$$

Proposición 7.27: Sea M un A-módulo. Entonces las siguientes son equivalentes:

1. $M = 0$.
2. $M_{\mathfrak{p}} = 0$ para todo $\mathfrak{p} \trianglelefteq A$ primo.
3. $M_{\mathfrak{m}} = 0$ para todo $\mathfrak{m} \trianglelefteq A$ maximal.

Demostración: Claramente $1 \implies 2 \implies 3$. Veamos $3 \implies 1$ por contrarrecíproca: Si $M \neq 0$ sea $\boldsymbol{m} \neq \vec{0} \in M$. Luego sea $\mathfrak{a} := \mathrm{Ann}(\boldsymbol{m}) \neq (1)$. Por el teorema de Krull, se cumple que $\mathfrak{a} \subseteq \mathfrak{m}$ maximal. Luego $\boldsymbol{m}/1 \in M_{\mathfrak{m}}$ y $\boldsymbol{m}/1 \neq \vec{0}$, puesto que si lo fuera entonces $s\boldsymbol{m} = \vec{0}$ con $s \in A \setminus \mathfrak{m} \subseteq A \setminus \mathfrak{a}$, lo que es absurdo. □

Definición 7.28 (Extensión y contracción): Sea $\varphi\colon A \to B$ un morfismo de anillos, y sean $\mathfrak{a}, \mathfrak{b}$ ideales de A y B resp. Entonces se define la *contracción* de $\mathfrak{b}$ y la *extensión* de $\mathfrak{a}$ como:

$$\mathfrak{b}^c := \varphi^{-1}[\mathfrak{b}], \qquad \mathfrak{a}^e := \big(\varphi[\mathfrak{a}]\big).$$

Nótese que si $A \subseteq B$, entonces $\mathfrak{b}^c = \mathfrak{b} \cap A$.

La idea de éstas definiciones está en forzar de manera natural una correspondencia entre ideales bajo el morfismo. Así pues, ya hemos visto que la contracción de ideales primos es primo, pero la extensión no necesariamente.

Ejemplo. Sea $\iota\colon \mathbb{Z} \to \mathbb{Q}$, entonces $(p)^e = \mathbb{Q}$ para todo p primo; de modo que la extensión de todo ideal primo no nulo es no primo. Reemplazando $\mathbb{Z}$ por cualquier dominio íntegro y $\mathbb{Q}$ por su cuerpo de fracciones vemos que esta misma situación siempre se replica.

La siguiente proposición justifica la terminología:

Proposición 7.29: Sea $\varphi\colon A \to B$ un morfismo de anillos y sean $\mathfrak{a}, \mathfrak{b}$ ideales de A y B resp. Entonces:

1. Si $\mathfrak{a} \subseteq \mathfrak{a}' \trianglelefteq A$, entonces $\mathfrak{a}^e \subseteq \mathfrak{a}'^e$. Si $\mathfrak{b} \subseteq \mathfrak{b}' \trianglelefteq B$, entonces $\mathfrak{b}^c \subseteq \mathfrak{b}'^c$.
2. $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ y $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$.
3. $\mathfrak{a}^e = \mathfrak{a}^{ece}$ y $\mathfrak{b}^c = \mathfrak{b}^{cec}$.
4. Las siguientes aplicaciones:

$$\{\mathfrak{a} \trianglelefteq A : \mathfrak{a}^{ec} = \mathfrak{a}\} \underset{()^c}{\overset{()^e}{\rightleftarrows}} \{\mathfrak{b} \trianglelefteq B : \mathfrak{b}^{ce} = \mathfrak{b}\}$$

son biyecciones y son la una la inversa de la otra.

Proposición 7.30: Sea S un sistema multiplicativo de A, $\mathfrak{a} \trianglelefteq A$ y consideremos el morfismo $\lambda_S\colon A \to S^{-1}A$. Entonces:

1. Todo ideal de $S^{-1}A$ es una extensión de un ideal en A.
2. $\mathfrak{a}^{ec} = \bigcup_{s \in S}(\mathfrak{a} : s)$. En consecuencia, $\mathfrak{a}^e = (1)$ syss $\mathfrak{a} \cap S \neq \varnothing$.

3. $\mathfrak{a}$ es una contracción syss ningún elemento de S es divisor de cero en $A/\mathfrak{a}$.

4. Las siguientes aplicaciones:

$$\{\mathfrak{p} \lhd A : \mathfrak{p} \text{ primo}, \mathfrak{p} \cap S \neq \varnothing\} \underset{()^c}{\overset{S^{-1}-}{\rightleftarrows}} \{\mathfrak{q} \lhd S^{-1}A : \mathfrak{q} \text{ primo}\}$$

son biyecciones y son la una la inversa de la otra.

Demostración:

1. Sea $\mathfrak{b} \trianglelefteq S^{-1}A$, hay que probar que $\mathfrak{b}^{ce} = \mathfrak{b}$. Para ello, sea $x/s \in \mathfrak{b}$, entonces $x/1 \in \mathfrak{b}$, por ende $x \in \mathfrak{b}^c$ y luego $x/s \in \mathfrak{b}^{ce}$; es decir, hemos probado que $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$ y se concluye por doble contención.

2. Siga la siguiente cadena de equivalencias:

$$\begin{aligned} x \in \mathfrak{a}^{ec} = (S^{-1}\mathfrak{a})^c &\iff \exists a \in \mathfrak{a}, s \in S \quad x/1 = a/s \\ &\iff \exists a \in \mathfrak{a}, s \in S, t \in S \quad (xs - a)t = 0 \\ &\iff \exists s \in S, t \in S \quad xst \in \mathfrak{a} \\ &\iff \exists s \in S \quad x \in (\mathfrak{a} : s). \end{aligned}$$

3. $\mathfrak{a}$ es contracción syss $\mathfrak{a}^{ec} \subseteq \mathfrak{a}$ y luego emplee el inciso anterior.

4. Ejercicio para el lector. □

7.2. Descomposición primaria de anillos

Definición 7.31: Un ideal $\mathfrak{q} \lhd A$ (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 syss $A/\mathfrak{q}$ es no nulo y no posee nilpotentes no nulos.

Proposición 7.32: Si $\mathfrak{q}$ es primario, entonces $\operatorname{Rad}\mathfrak{q}$ es el mínimo ideal primo que contiene a $\mathfrak{q}$.

Pista: Sólo basta probar que $\operatorname{Rad}\mathfrak{q}$ es primo. □

Definición 7.33: Si $\mathfrak{q}$ es primario y $\mathfrak{p} = \operatorname{Rad}\mathfrak{q}$, entonces $\mathfrak{q}$ se dice $\mathfrak{p}$-primario.

Proposición 7.34: Si $\operatorname{Rad}\mathfrak{a}$ es maximal, entonces $\mathfrak{a}$ es primario. En particular, las potencias de un ideal maximal $\mathfrak{m}$ son ideales $\mathfrak{m}$-primarios.

Lema 7.35: Sean $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ 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

$$\operatorname{Rad}\left(\bigcap_{i=1}^{n} \mathfrak{q}_i\right) = \bigcap_{i=1}^{n} \operatorname{Rad}(\mathfrak{q}_i) = \mathfrak{p}.$$

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 $y \notin \mathfrak{q}_\mathrm{i}$, 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. □

Definición 7.36: 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 $\operatorname{Rad}\mathfrak{q}_i$'s son todos distintos. $\mathfrak{a}$ se dice *decomposible* si posee alguna descomposición primaria.

Por el lema anterior toda descomposición primaria se puede reducir a una descomposición minimal, de ahí dicho concepto.

Lema 7.37: 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, $\operatorname{Rad}(\mathfrak{q} : x) = \mathfrak{p}$.
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 $\operatorname{Rad}\mathfrak{q} \subseteq \operatorname{Rad}(\mathfrak{q} : x)$; veremos la otra inclusión: Sea $t \in \operatorname{Rad}(\mathfrak{q} : x)$, 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, $t \in \operatorname{Rad}\mathfrak{q}$.

3. Ejercicio para el lector. □

Definición 7.38: 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 $\operatorname{As}\mathfrak{a}$ al conjunto de los ideales primos asociados a $\mathfrak{a}$.

Teorema 7.39: Sea $\mathfrak{a} \lhd A$ un ideal decomposible, con descomposición primaria minimal $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$. Entonces $\operatorname{As}(\mathfrak{a}) = \{\operatorname{Rad}\mathfrak{q}_i\}_{i=1}^{n}$. En consecuencia, toda descomposición primaria minimal posee los mismos radicales y tiene la misma longitud.

Demostración: Sea $x \in A$, luego

$$\operatorname{Rad}(\mathfrak{a} : x) = \operatorname{Rad}\left(\bigcap_{i=1}^{n} \mathfrak{q}_i : x\right) = \bigcap_{i=1}^{n} \operatorname{Rad}(\mathfrak{q}_i : x) = \bigcap_{i=1}^{n} \mathfrak{p}_i.$$

Luego si $\operatorname{Rad}(\mathfrak{a} : x)$ 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:

$$\operatorname{Rad}(\mathfrak{a} : x) = \bigcap_{\substack{i=1 \\ i \neq j}}^{n} \operatorname{Rad}(\mathfrak{q}_i : x) \cap \operatorname{Rad}(\mathfrak{q}_j : x) = \operatorname{Rad}(1) \cap \operatorname{Rad}\mathfrak{q}_j = \mathfrak{p}_j. \qquad \square$$

Proposición 7.40: Sea $\mathfrak{a}$ un ideal decomposible 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 $\operatorname{As}\mathfrak{a}$.

Demostración: Basta notar que

$$\mathfrak{p} = \operatorname{Rad}\mathfrak{p} \subseteq \operatorname{Rad}\mathfrak{a} = \bigcap_{i=1}^{n} \operatorname{Rad}\mathfrak{q}_i = \bigcap_{i=1}^{n} \mathfrak{p}_i,$$

y recordar que como $\mathfrak{p}$ es primo, entonces $\mathfrak{p} \supseteq \mathfrak{p}_j$ para algún j por la proposición 2.57. □

Proposición 7.41: Si $\mathfrak{a} \lhd A$ es decomposible y $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ es una descomposición minimal con $\mathfrak{p}_i := \operatorname{Rad} \mathfrak{q}_i$, entonces:

$$\bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A : (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

Proposición 7.42: Sea S un sistema multiplicativo de A y $\mathfrak{q}$ un ideal $\mathfrak{p}$-primario. Entonces:

1. $S \cap \mathfrak{p} \neq \varnothing$, entonces $S^{-1}\mathfrak{q} = S^{-1}A$.
2. $S \cap \mathfrak{p} = \varnothing$, 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. □

Proposición 7.43: Sea S un sistema multiplicativo y $\mathfrak{a}$ un ideal decomposible con descomposición minimal $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ tal que $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ son disjuntos de S y $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ cortan a S. Entonces:

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i, \qquad S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i.$$

Demostración: Sabemos que S^{-1} distribuye uniones y el resto es aplicar la proposición anterior. □

Definición 7.44: 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 7.45: Sea $\mathfrak{a}$ un ideal decomposible con descomposición minimal $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ y con $\mathfrak{p}_i := \operatorname{Rad} \mathfrak{q}_i$. Si $\mathcal{F} := \{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_j}\}$ es una familia aislada, entonces $\bigcap_{j=1}^{m} \mathfrak{q}_{i_j}$ es independiente de la descomposición.

Demostración: Definamos $S := A \setminus \bigcup_{j=1}^{m} \mathfrak{p}_{i_j}$ y nótese que es un sistema multiplicativo. Más aún, sea $\mathfrak{p}$ un ideal primo asociado a $\mathfrak{a}$: Si $\mathfrak{p} \in \mathcal{F}$, entonces por definición se cumple que $\mathfrak{p} \cap S = \varnothing$. Si $\mathfrak{p} \notin \mathcal{F}$, entonces $\mathfrak{p} \not\subseteq \bigcup_{j=1}^{m} \mathfrak{p}_{i_j}$ por la proposición 2.57, por lo que $\mathfrak{p} \cap S \neq \varnothing$.

Finalmente basta aplicar el resultado anterior para obtener el enunciado. □

7.3. Módulos noetherianos y artinianos

Existe una larga discusión que implica traducir varios de los conceptos y propiedades de anillos a módulos. Varios libros lo hacen al instante de definir módulos, para realizar el paralelo con anillos, no obstante, en éste libro se optó por no hacerlo para enfocar la discusión en módulos libres y particularmente en espacios vectoriales. En particular, todo nace de la siguiente observación vital:

Proposición 7.46: Sea A un dominio. Entonces los submódulos de A (visto como un A-módulo) son precisamente los ideales de A.

Proposición 7.47: Sea M un A-módulo. M es finitamente generado syss M es isomorfo a un cociente de A^n.

Demostración: Recordemos que ser finitamente generado significa que existen $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in M$ tales que el morfismo

$$\begin{aligned} \varphi\colon A^n &\longrightarrow M \\ (\lambda_1, \ldots, \lambda_n) &\longmapsto \lambda_1 \boldsymbol{x}_1 + \cdots + \lambda_n \boldsymbol{x}_n \end{aligned}$$

es suprayectivo. Luego por el primer teorema de isomorfismos se cumple que $A^n / \ker \varphi \cong M$. □

Definición 7.48: Dado un anillo A, se le llama su *radical de Jacobson* a

$$\mathfrak{J}(A) := \bigcap \{\mathfrak{m} : \mathfrak{m} \lhd A,\ \mathfrak{m} \text{ maximal}\}$$

Proposición 7.49: Se cumplen:

1. El radical de Jacobson es un ideal radical.
2. Si A es un anillo local, $\mathfrak{J}(A)$ es su único ideal maximal.

3. $y \in \mathfrak{J}(A)$ syss para todo $x \in A$ se cumple que $1 - xy \in A^\times$.

Demostración: La primera y segunda quedan al lector. La tercera: $y \in \mathfrak{J}(A)$ syss $y \in \mathfrak{m}$ para todo $\mathfrak{m} \lhd A$ maximal. Como $1 \notin \mathfrak{m}$, entonces $1-xy \notin \mathfrak{m}$ para todo $x \in A$. Pero todo elemento no inversible está contenido en algún ideal maximal (por teorema de Krull), de modo que $1 - xy$ es inversible. □

Proposición 7.50: Sea M un A-módulo finitamente generado, $\varphi\colon M \to M$ 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: Nótese que éste lema es una generalización del teorema de Cayley-Hamilton, y de hecho la demostración es bastante similar. En primer lugar, si M es finitamente generado sea $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ un sistema generador finito y luego se ha de cumplir que $\varphi(\boldsymbol{x}_i) = \sum_{j=1}^n c_{ij}\boldsymbol{x}_j$ con $c_{ij} \in \mathfrak{a}$, o equivalentemente

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - c_{ij})\boldsymbol{x}_j = \vec{0}$$

para todo i. Luego formando la matriz $B := [\delta_{ij}\varphi - c_{ij}]_{ij}$, nos damos cuenta de que B aplicado sobre todo $\boldsymbol{x}_i$ se anula, por lo que, multiplicando por $\operatorname{adj} B$ también los anula y se comprueba que $\det(B) = 0$. Expandiendo el determinante se obtiene un polinomio como el del enunciado; en el caso de elegir una base para un k-espacio vectorial ésto no es más que el polinomio característico de la matriz. □

Ésta proposición será empleada para el siguiente resultado y más adelante en la sección de dependencia íntegra.

Ahora procedemos a probar un famoso resultado de álgebra conmutativa. El lema de Nakayama posee varias versiones y aquí enlisté todas las que encontré. El mismo Nakayama sugiere que se le llame «teorema de Krull-Azumaya», pero el nombre de «lema de Nakayama» es mucho más estándar.

Teorema 7.51 (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 $x \equiv 1$ (mód $\mathfrak{a}$) 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 $M/\mathfrak{J}(A)M = \mathrm{Span}_A\{[\boldsymbol{x}_1], \ldots, [\boldsymbol{x}_n]\}$, entonces $M = \mathrm{Span}_A\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$.

Demostración:

1. Considere el lema anterior con $\varphi = \mathrm{Id}$ y sea $x := 1 + a_{n-1} + \cdots + a_1 + a_0$.

2. Sea x como en el inciso 1, entonces $x - 1 = y \in \mathfrak{J}(A)$, pero $1 - y = x$ es inversible, luego $xM = M = \{\vec{0}\}$.

3. Basta aplicar el inciso anterior con M/N.

4. Basta aplicar el inciso anterior con $N = \mathrm{Span}_A\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$. □

Lema 7.52: 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 7.53: Se dice que un A-módulo M es *noetheriano* si satisface las condiciones del lema anterior.

Corolario 7.54: Sea A un dominio. Entonces si consideramos a A como A-módulo, sus submódulos son, efectivamente, los ideales de A.

La siguiente definición permite un elegante paralelo con la noción de noetheriano:

Definición 7.55: Se dice que un A-módulo M es *artiniano* si para toda cadena descendiente de submódulos

$$N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots$$

existe un n tal que para todo $m \geq n$ se cumple que $N_n = N_m$.

Ejemplo. Todo cuerpo es noetheriano y artiniano. Ya vimos también que todo DIP es noetheriano.

Ejemplo. $\mathbb{Z}$ es un dominio euclídeo, luego es un DIP y luego es noetheriano. Sin embargo, no es artiniano puesto que

$$\mathbb{Z} \supseteq (2) \supseteq (2^2) \supseteq (2^3) \supseteq \cdots$$

es una cadena $\subseteq$-descendiente de ideales sin $\subseteq$-minimal.

Ejemplo 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 artiniano. Pero no es noetheriano puesto que la siguiente cadena no posee $\subseteq$-maximal:

$$\langle p^{-1} \rangle \subset \langle p^{-2} \rangle \subset \langle p^3 \rangle \subset \cdots$$

En el ejemplo anterior construimos un objeto que desafía varios de nuestros convenios algebraicos, principalmente no es unitario lo que a simple vista parece un requisito bastante razonable. Se puede probar (aunque no es nada sencillo) que todo anillo noetheriano unitario es artiniano, y en susodicha prueba es importante distinguir entre anillos conmutativos y no.

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 7.56: Sea M un A-módulo noetheriano (resp. artiniano). Entonces todo submódulo N y todo módulo cociente M/N es noetheriano (resp. artiniano).

Demostración: Como todo submódulo T de N es un submódulo de M, entonces está finitamente generado. Más aún, por el teorema de la correspondencia, todo submódulo de M/N es de la forma $(T+N)/N$ con $T \leq M$; luego como T es finitamente generado, se sigue que $(T+N)/N$ también lo es. □

Corolario 7.57: Sea A un anillo noetheriano (resp. artiniano) y sea $\mathfrak{a}$ un ideal de A. Entonces $A/\mathfrak{a}$ también es noetheriano (resp. artiniano).

Corolario 7.58: Si $\varphi\colon M \to N$ es un morfismo de A-módulos suprayectivo y M es noetheriano (resp. artiniano), entonces N también.

Proposición 7.59: Si A es noetheriano y S es un sistema multiplicativo de A, entonces $S^{-1}A$ también es noetheriano.

Teorema 7.60: Sea M un A-módulo y N un submódulo de M. Si N y M/N son noetherianos (resp. artinianos), entonces M también es noetheriano (resp. artiniano).

Demostración: En primer lugar construyamos la siguiente aplicación:

$$\Phi\colon \{T : T \leq M\} \longrightarrow \{L : L \neq N\} \times \{S : S \leq M/N\}$$
$$T \longmapsto \left(T \cap N, \frac{T+N}{N}\right)$$

Sean $E \leq T \leq M$ tales que $\Phi(E) = \Phi(T)$, queremos probar que si eso ocurre entonces $E = T$: Basta notar que si $\boldsymbol{x} \in T \setminus E$, entonces como $E \cap N = T \cap N$ se ha de cumplir que $\boldsymbol{x} \notin N$ y luego $[\boldsymbol{x}] \neq [\boldsymbol{y}]$ para todo $\boldsymbol{y} \in E$, puesto que de lo contrario $\boldsymbol{x} - \boldsymbol{y} = \boldsymbol{n} \in N$, pero entonces $\boldsymbol{n} \in T \cap N = E \cap N$, por lo que $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{n} \in E$; lo que es absurdo.

Luego sea

$$E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots$$

una cadena de submódulos de M. Nótese que $E_i \cap N$ es una cadena de submódulos de N y que $(E_i + N)/N$ es una cadena de submódulos de M/N, luego ambas se estabilizan digamos en un n suficientemente grande. Pero por la observación anterior, ésto implica que los E_i's también se estabilizan desde dicho n; luego M es noetheriano. □

Corolario 7.61: La suma de A-módulos noetherianos (resp. artinianos) es también noetheriano (resp. artiniano).

Reescribiendo el último teorema en lenguaje de sucesiones exactas:

Proposición 7.62: Si $0 \longrightarrow N \longrightarrow M \longrightarrow T \longrightarrow 0$ es una sucesión exacta de A-módulos, entonces M es noetheriano (resp. artiniano) syss N, T lo son.

Corolario 7.63: Sea $M = \bigoplus_{i=1}^{n} M_i$ un A-módulo. Entonces M es noetheriano (resp. artiniano) syss cada M_i lo es.

Demostración: Basta considerar la siguiente sucesión exacta y aplicar inducción:

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0 \qquad \square$$

Proposición 7.64: Sea A un anillo noetheriano (resp. artiniano). Entonces todo A-módulo M finitamente generado también es noetheriano (resp. artiniano).

Demostración: Ya vimos que todo módulo finitamente generado es un cociente de A^n para algún n y todo cociente de un noetheriano (resp. artiniano) sigue siendo noetheriano (resp. artiniano). $\square$

Desde aquí en adelante podemos hacer una discusión análoga a la de grupos resolubles y las series normales (véase §1.5.2).

Lema 7.65 (de Zassenhaus): Sean $B \leq B^*$ y $C \leq C^*$ submódulos de M. Entonces:

1. $B + (B^* \cap C)$ es submódulo de $B + (B^* \cap C^*)$.
2. $C + (C^* \cap B)$ es submódulo de $C + (C^* \cap B^*)$.
3. $\dfrac{B + (B^* \cap C^*)}{B + (B^* \cap C)} \cong \dfrac{C + (C^* \cap B^*)}{C + (C^* \cap B)}$.

Definición 7.66: 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.

Teorema 7.67 (de refinamiento de Schreier): Dos series de un mismo A-módulo poseen al menos un refinamiento equivalente.

Teorema 7.68 – *Teorema de Jordan-Hölder*: Todas las series de composición de un A-módulo son equivalentes.

Definición 7.69: 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 7.70: Un A-módulo posee una serie de composición syss es noetheriano y artiniano.

Proposición (AEN) 7.71: Para un k-espacio vectorial V, las siguientes condiciones son equivalentes:

1. V tiene dimensión finita.
2. V tiene longitud finita.
3. V es noetheriano.
4. V es artiniano.

Más aún, si ese es el caso, entonces $\ell(V) = \dim_k(V)$.

Demostración: Es claro que 1 $\implies$ 2, y 2 $\implies$ 3 y 2 $\implies$ 4. Para ver que 3 $\implies$ 1, veamos la contrarrecíproca: Si V tiene dimensión infinita, entonces sea $\{\boldsymbol{x}_n : n \in \mathbb{N}\}$ un conjunto linealmente independiente, luego la cadena ascendente:

$$\mathrm{Span}_k\{\boldsymbol{x}_1\} \subset \mathrm{Span}_k\{\boldsymbol{x}_1, \boldsymbol{x}_2\} \subset \mathrm{Span}_k\{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3\} \subset \cdots$$

no posee $\subseteq$-maximal, por lo que V no es noetheriano.

La implicancia 4 $\implies$ 1 es análoga. □

Proposición 7.72: Todo dominio íntegro artiniano es un cuerpo.

Demostración: Sea $x \in D$ y no es inversible, entonces la siguiente cadena de ideales no posee $\subseteq$-minimal:

$$(x) \supset (x^2) \supset (x^3) \supset \cdots \qquad \square$$

Teorema 7.73 (Akizuki): Todo dominio noetheriano es artiniano.

Demostración: Procedemos por contradicción: Supongamos que existe un dominio artiniano A que no sea noetheriano. Necesariamente A debe ser infinito y debe poseer ideales infinitamente generados, luego podemos elegir $\mathfrak{a}$ un ideal $\subseteq$-minimal entre la familia de los infinitamente generados (puesto que A es artiniano). Nótese que $\mathfrak{a}$ satisface que todo ideal propio contenido en $\mathfrak{a}$ es finitamente generado.

Luego, veamos que para todo $r \in A$ se cumple que $r\mathfrak{a} = 0$ ó $r\mathfrak{a} = \mathfrak{a}$: Si $r\mathfrak{a} \neq \mathfrak{a}$, entonces consideremos el epimorfismo $\varphi\colon x \mapsto rx$, del cual concluimos que como $r\mathfrak{a}$ es finitamente generado y

$$\frac{\mathfrak{a}}{\ker \varphi} \cong r\mathfrak{a},$$

entonces $\ker \varphi \subseteq \mathfrak{a}$ es un ideal infinitamente generado y, en consecuencia, $\ker \varphi = \mathfrak{a}$.

Sea $\mathfrak{p} := \operatorname{Ann}(\mathfrak{a})$. Nótese que si $r, s \notin \mathfrak{p}$, ha de ser porque $r\mathfrak{a} = s\mathfrak{a} = \mathfrak{a}$; luego $rs\mathfrak{a} = \mathfrak{a}$ y $rs \notin \mathfrak{p}$; en consecuencia, $\mathfrak{p}$ es un ideal primo. Por lo tanto, $k := A/\mathfrak{p}$ es un dominio íntegro artiniano, y por la proposición anterior, es un cuerpo.

Nótese que $\mathfrak{a}$ es un k-espacio vectorial con el producto escalar $[r] \cdot x = rx$ el cual está bien definido. Como $\mathfrak{a}$ no está finitamente generado en A, y todos sus ideales propios sí, entonces $\mathfrak{a}$ es un k-espacio vectorial artiniano de dimensión infinita; lo cual es absurdo. $\square$

El caso no conmutativo aparece bajo el nombre del teorema de Hopkins-Levitzki.

8

Anillos de valuación discreta y teoría de la dimensión

8.1. Dependencia íntegra

Definición 8.1: Dado un dominio A, se dice que una aplicación $\alpha\colon A \to B$ es una *A-álgebra* si es un homomorfismo de anillos y $\operatorname{Img}\alpha$ 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 $\alpha\colon A \to B$ 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 $\operatorname{Func}(X; A)/A$ es una extensión de anillos.

- Si D es un dominio íntegro, $\mathrm{Frac}(D)/D$ 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 $\mathrm{Mat}_n(A)/A$ es una extensión de anillos.
- Si $\mathfrak{a} \lhd A$ 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 8.2: Dado un par de A-álgebras $\alpha\colon A \to B$ y $\beta\colon A \to C$, una aplicación $\varphi\colon B \to C$ es un A-morfismo si el siguiente diagrama

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & C \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\beta} \\ A & \xrightarrow[\mathrm{Id}_R]{} & A \end{array}$$

conmuta (en Ring).

Proposición 8.3: Sea A un dominio y B un A-álgebra. Entonces:

1. $\mathrm{Id}_B\colon B \to B$ 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 8.4: 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 8.5: Sea B un A-álgebra. Una base X de B es un subconjunto tal que toda aplicación $f\colon X \to C$, donde C es otro A-álgebra admita una única extensión $\bar{f}\colon B \to C$ a un morfismo de A-álgebras. Si B posee una base X, entonces se dice que es un A-*álgebra libre* sobre X.

Teorema 8.6: 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 $f\colon S \to B$. 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:

$$\begin{aligned} \bar{f}\colon A[S] &\longrightarrow B \\ p(x_{i_1},\ldots,x_{i_n}) &\longmapsto p(t_{i_1},\ldots,t_{i_n}) \end{aligned}$$

donde la aplicación está bien definida en el sentido de que todo polinomio en $A[S]$ sólo contiene finitas indeterminadas. □

En éste capítulo, emplearemos $A^F[S]$ para denotar al anillo de polinomios con indeterminadas en S, ésto para evitar futuras confusiones.

Corolario 8.7: 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 $\mathrm{Func}(S;A) \cong A^F[S]$ 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 8.8: Dado un A-álgebra $\alpha\colon A \to B$. Se dice que $S \subseteq B$ es una subálgebra si es un subanillo y $\operatorname{Img}\alpha \subseteq S$. Equivalentemente, $\bar{\alpha}\colon A \to S$ es un subálgebra si el siguiente diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle \mathrm{Id}}\uparrow & & \uparrow{\scriptstyle \iota} \\ A & \xrightarrow[\bar{\alpha}]{} & S \end{array}$$

conmuta (en Alg_A).

Proposición 8.9: La intersección de subálgebras es una subálgebra.

Definición 8.10: 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 posee 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 $\{1, x, x^2, \ldots, x^n\}$ siempre es un conjunto linealmente independiente.

Proposición 8.11: Una A-álgebra B es finitamente generada syss existe $S \subseteq B$ finito, con una biyección $S \mapsto \{x_1, x_2, \ldots, x_n\}$ a un conjunto de indeterminadas tal que la aplicación:

$$\mathrm{ev}_S \colon A[x_1, \ldots, x_n] \to A[S]$$

es suprayectiva. En consecuencia, toda A-álgebra finita es un cociente de algún anillo de polinomios con finitas indeterminadas.

Demostración: La parte de «en consecuencia» sigue del primer teorema de isomorfismos. □

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 aleman, el *Nullstellensatz*.

Teorema 8.12: Si L/k es una extensión de cuerpos donde L es un 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 9.11. Daremos dos demostraciones:

Demostración (Rabinowitsch): En esta demostración supondremos que k no es numerable.

Si L es un k-álgebra de tipo finito, entonces viene generado por una m-tupla finita $\boldsymbol{a}$. Para ver que L es una extensión finita, basta ver que cada uno de los elementos es algebraico. Para ello sea $\mathrm{ev}_{\boldsymbol{a}} \colon k[x_1, \ldots, x_m] \to L$

el morfismo suprayectiva, entonces viene generado, como k-espacio vectorial, por todos los monomios de $k[x_1, \dots, x_m]$ evaluados en $\boldsymbol{a}$ que son numerables.

Sea $\alpha \in L \setminus k$, para ver que es algebraica entonces nótese que el conjunto

$$\left\{ \frac{1}{\alpha - \beta} : \beta \in k \right\}$$

es no numerable, luego no puede ser base así que ha de ser linealmente dependiente y existe

$$\frac{\lambda_1}{\alpha - \beta_1} + \cdots + \frac{\lambda_n}{\alpha - \beta_n} = \frac{p(\alpha)}{q(\alpha)} = 0$$

para algunos λ_i no nulos. Sustituyendo α por una variable x arbitraria se obtienen los polinomios $p(x), q(x) \in k[x]$, donde $q(x) = (x - \beta_1) \cdots (x - \beta_n)$ es no nulo en α, así que $p(\alpha) = 0$.

Ésto prueba que L es algebraico, y como viene generado por finitos elementos, es una extensión finita. □

Teorema 8.13 – *Teorema débil de ceros de Hilbert*: Si k es algebraicamente cerrado, entonces un ideal $\mathfrak{a} \lhd k[x_1, \dots, x_n]$ 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 $k \to k[x_1, \dots, x_n]/\mathfrak{m} =: L$, 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 $\pi \colon k[x_1, \dots, x_n] \to k$ es un epimorfismo de anillos con $\mathfrak{m} = \ker \pi$. Definiendo $\alpha_i := \pi(x_i)$ se cumple que

$$(x_1 - \alpha_1, \dots, x_n - \alpha_n) \subseteq \mathfrak{m} \neq k[x_1, \dots, x_n]$$

y por maximalidad del conjunto de la izquierda se da la igualdad buscada. □

Definición 8.14: Se dice que un R-módulo M es *fiel* si para todos $\lambda_1, \lambda_2 \in R$ distintos existe un $\boldsymbol{m} \in M$ tal que $\lambda_1 \boldsymbol{m} \neq \lambda_2 \boldsymbol{m}$. Equivalentemente, un R-módulo M es fiel si no existe $a \in R$ tal que $aM = 0$.

Lema 8.15: Sea B un A-álgebra y $\alpha \in B$. Son equivalentes:

1. α es raíz de un polinomio mónico $p(x) \in A[x]$ no constante.
2. El subálgebra $A[\alpha]$ es un A-módulo finitamente generado.
3. $A[\alpha]$ está contenido en un subálgebra C que es un A-módulo finitamente generado.
4. Existe un $A[\alpha]$-módulo fiel sobre que es un A-módulo finitamente generado.

Demostración: $1 \implies 2$. Supongamos que α es raíz de

$$x^{n+1} + c_n x^n + \cdots + c_1 x + c_0.$$

Sabemos que como R-módulo se satisface que $A[\alpha] = \mathrm{Span}_A\{1, \alpha^1, \alpha^2, \dots\}$, pero por el polinomio arriba descrito se tiene que $\alpha^{n+1} \in \mathrm{Span}\{1, \alpha, \dots, \alpha^n\}$ y así también con las potencias superiores de α; de modo que está generado por $\{1, \alpha, \dots, \alpha^n\}$ que es finito.

$2 \implies 3 \implies 4$. Trivial.

$4 \implies 1$. Sea M dicho $A[\alpha]$-módulo fiel que está generado sobre A por $\boldsymbol{m}_1, \dots, \boldsymbol{m}_n$. Luego como $\alpha M \subseteq M$, entonces $x \mapsto \alpha x$ es una morfismo de A-módulos y por la proposición 7.50 se obtiene el polinomio mónico deseado. □

Definición 8.16: Sea B un 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 2.80 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 8.17: 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. □

Proposición 8.18: Sea A un dominio íntegro, sea $k := \operatorname{Frac} A$ y sea L/k una extensión de anillos. Sea $\alpha \in L$ algebraico sobre k, entonces existe $c \in A$ tal que $c\alpha \neq 0$ es entero sobre A.

Teorema 8.19: Sean $C/B/A$ extensiones de anillos. Entonces C/A es una extensión entera syss C/B y B/A son extensiones enteras.

Proposición 8.20: Si B es una A-álgebra entera de tipo-finita, entonces es un A-módulo finitamente generado.

Demostración: Sea $\{\alpha_1, \ldots, \alpha_n\}$ un sistema generador de B como A-álgebra. Luego se tiene que

$$A[\alpha_1] \subseteq A[\alpha_1, \alpha_2] \subseteq \cdots \subseteq B$$

es una cadena finita, tal que cada término es un álgebra de tipo-finito, finitamente generada como módulo del anterior. □

Proposición 8.21: Sea $\sigma\colon B \to C$ un homomorfismo de anillos. Si B es un A-álgebra entera, entonces $\sigma[B]$ es entera sobre $\sigma[A]$. Si σ es inyectivo y B/A es extensión anillos, entonces $\sigma[B]/\sigma[A]$ también.

Proposición 8.22: Sea B/A una extensión de anillos, y sea C el conjunto de elementos enteros de B. Entonces C/A es una extensión de anillos.

Demostración: Claramente todo elemento de A es entero sobre A, pues basta considerar el polinomio $x - a$. Ahora hay que probar que C es cerrado bajo sumas y productos. Sean $\alpha, \beta \in B$ enteros. Luego $A[\alpha]$ es finitamente generado como A-módulo y siendo $p(x) \in A[x]$ mónico tal que $p(\beta) = 0$, como $p(x) \in A[\alpha][x]$, entonces $A[\alpha, \beta]$ es entero sobre $A[\alpha]$ y finitamente generado como $A[\alpha]$-módulo. Sean $S, T \subseteq B$ tales que $A[\alpha] = \operatorname{Span}_A S$ y $A[\alpha, \beta] = \operatorname{Span}_{A[\alpha]} T$. Sea

$$U := \{st : s \in S, t \in T\}$$

luego es claro que U es finito y queda al lector comprobar que $A[\alpha, \beta] = \operatorname{Span}_A U$. Como $\alpha + \beta, \alpha \cdot \beta \in A[\alpha, \beta]$, entonces son enteros. □

Definición 8.23: El subanillo C construido en la proposición anterior se le dice la *clausura íntegra* de B. Si $C = A$, entonces se dice que A es *íntegramente cerrado* sobre B. En particular, decimos que un dominio íntegro A es *íntegramente cerrado* (a secas) si lo es sobre $\mathrm{Frac}(A)$.

Proposición 8.24: Sean $C/B/A$ extensiones de anillos. Si C/B y B/A son extensiones enteras, entonces C/A también lo es.

Proposición 8.25: Sea A un dominio íntegro y un DFU, entonces A es íntegramente cerrado.

Demostración: Al igual que en el caso $\mathbb{Q}/\mathbb{Z}$, se reduce a una aplicación del teorema de las raíces racionales. □

Teorema 8.26: 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 8.27: Sean B/A una extensión entera de dominios íntegros. Entonces A es un cuerpo syss B es un cuerpo.

Demostración: $\Longrightarrow$. Sea $y \in B$ no nulo, entonces existen $a_i \in A$ tales que

$$y^{n+1} + a_n y^n + \cdots + a_1 y + a_0 = 0,$$

luego, como y no es divisor de cero entonces $a_0 \neq 0$, y luego, con un despeje algebraico se obtiene que

$$y^{-1} = -a_0^{-1}(y^n + a_n y^{n-1} + \cdots + a_1) \in B.$$

$\Longleftarrow$. Sea $a \in A_{\neq 0}$, como $a \in B$ y B es cuerpo, entonces $a^{-1} \in B$, luego

$$(a^{-1})^{m+1} + c_n a^{-m} + \cdots + c_1 a^{-1} + c_0 = 0$$

con $c_i \in A$, por lo que, multiplicando por a^m se obtiene que $a^{-1} = -(c_n + \cdots + c_1 a^{m-1} + c_0 a^m) \in A$. □

Corolario 8.28: Sea B/A una extensión entera de anillos, y sean $\mathfrak{q} \trianglelefteq B$ y $\mathfrak{p} := \mathfrak{q} \cap A \trianglelefteq A$. Entonces $\mathfrak{q}$ es maximal syss $\mathfrak{p}$ es maximal.

Teorema 8.29: Sea B/A una extensión entera de anillos, y sea $\mathfrak{p} \trianglelefteq A$ primo. Entonces existe un ideal $\mathfrak{q} \trianglelefteq B$ primo tal que $\mathfrak{p} = \mathfrak{q} \cap A$.

Demostración: Sea $\mathfrak{p} \trianglelefteq A$, consideremos el siguiente diagrama conmutativo dado por la localización:

$$\begin{array}{ccc} A & \xhookrightarrow{\iota} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A_{\mathfrak{p}} & \xhookrightarrow[\iota]{} & B_{\mathfrak{p}} \end{array}$$

Sea $\mathfrak{n} \lhd B_{\mathfrak{p}}$ un ideal maximal, luego $\mathfrak{m} := \mathfrak{n} \cap A_{\mathfrak{p}}$ ha de ser el único ideal maximal de $A_{\mathfrak{p}}$ y luego definamos $\mathfrak{q} := \beta^{-1}[\mathfrak{n}]$. Pero por la conmutatividad del diagrama se cumple que

$$\mathfrak{q} \cap A = \iota^{-1}[\mathfrak{q}] = (\iota \circ \beta)^{-1}[\mathfrak{n}] = (\alpha \circ \iota)^{-1}[\mathfrak{n}] = \alpha^{-1}[\mathfrak{m}] = \mathfrak{p}. \qquad \square$$

Culminamos ésta sección con los dos teoremas de Cohen y Seidenberg bajo el nombre de «teorema del ascenso» y «del descenso».

Teorema 8.30 – *Teorema del ascenso*: Sea B/A una extensión entera de anillos, y sean

$$\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_n \lhd A,$$
$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m \lhd B,$$

dos cadenas de ideales primos, tales que $m < n$ y $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $1 \leq i \leq m$. Luego se puede extender la segunda cadena a

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m \subseteq \cdots \subseteq \mathfrak{q}_n \lhd B$$

con $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $1 \leq i \leq n$.

Demostración: Por inducción basta probar el caso $m = 1 < 2 = n$. Sea $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \lhd A$, y sea $\mathfrak{q}_1 \lhd B$ con las condiciones del enunciado. Luego $\mathfrak{p}_2/\mathfrak{p}_1 \lhd A/\mathfrak{p}_1$ es un ideal primo, y $B/\mathfrak{q}_1$ es una extensión entera de $A/\mathfrak{p}_1$; luego por el teorema anterior, existe $\mathfrak{r} \cap (A/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1$, con $\mathfrak{r} \lhd B/\mathfrak{q}_1$. Para entender el proceso, vea el siguiente diagrama conmutativo:

$$\begin{array}{ccc} A & \xhookrightarrow{\iota_1} & B \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ A/\mathfrak{p}_1 & \xhookrightarrow[\iota_2]{} & B/\mathfrak{q}_1 \end{array}$$

Luego definamos $\mathfrak{q}_2 := \pi_2^{-1}[\mathfrak{r}]$ y se satisface que

$$\begin{aligned} \mathfrak{p}_2 &= \pi_1^{-1}[\mathfrak{p}_2/\mathfrak{p}_1] = \pi_1^{-1}\left[\iota_2^{-1}[\mathfrak{r}]\right] = (\pi_1 \circ \iota_2)^{-1}[\mathfrak{r}] \\ &= (\iota_1 \circ \pi_2)^{-1}[\mathfrak{r}] = \iota_1^{-1}\left[\pi_2^{-1}[\mathfrak{r}]\right] = \iota_1^{-1}[\mathfrak{q}_2] = \mathfrak{q}_2 \cap A. \end{aligned}$$ □

Proposición 8.31: Sea A un dominio íntegro. Son equivalentes:

1. A es íntegramente cerrado.
2. $A_\mathfrak{p}$ es íntegramente cerrado para todo $\mathfrak{p} \lhd A$ primo.
3. $A_\mathfrak{m}$ es íntegramente cerrado para todo $\mathfrak{m} \lhd A$ maximal.

Teorema 8.32 – *Teorema del descenso*: Sea B/A una extensión entera de anillos, y sean

$$\begin{aligned} A \rhd \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_n, \\ B \rhd \mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m, \end{aligned}$$

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

$$B \rhd \mathfrak{q}_1 \supseteq \mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_m \supseteq \cdots \supseteq \mathfrak{q}_n$$

con $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $1 \leq i \leq n$.

9

Variedades afines y proyectivas

En el capítulo sobre extensiones de cuerpo y teoría de Galois vimos técnicas para encontrar raíces de polinomios con una variable. En geometría algebraica veremos cómo encontrar raíces a polinomios multivariable, aunque naturalmente varios otros problemas se abrirán durante el camino.

Dependencias del capítulo: §2, §4 y del libro de topología §2 [espacios topológicos].

Dado una extensión de cuerpos K/k, en éste capítulo siempre asumiremos que K es algebraicamente cerrado. La mayoría de ejemplos se reducirán al estudio de $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$ y $\overline{\mathbb{Q}}/\mathbb{Q}$.

9.1. Variedades afines

Desde ahora en adelante se asume que k siempre representa un cuerpo algebraicamente cerrado.

Definición 9.1: Denotaremos por $\mathbb{A}^n_k := k^n$ al *espacio afín* de dimensión n sobre k.

Además de ello, en éste capítulo denotaremos por $A := k[x_1, \ldots, x_n]$ 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 9.2 – *Conjunto algebraico*: Sea $\mathbb{A}^n$ un espacio afín, entonces dado un conjunto de polinomios $T \subseteq A$ se define

$$\mathbf{V}(T) := \{\boldsymbol{p} \in \mathbb{A}^n : \forall f \in T\ f(\boldsymbol{p}) = 0\}.$$

Si $T = \{f_1, \ldots, f_m\}$ nos permitimos denotar $\mathbf{V}(f_1, \ldots, f_m)$. Los conjuntos de ésta forma son llamados *algebraicos afínes*.

Otro convenio es denotar por $\boldsymbol{x}$ a una variable y $\boldsymbol{p}$ a un punto específico.

Primero veamos la conexión con álgebra:

Lema 9.3: 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 $\mathbf{V}(1) = \varnothing$.

Proposición 9.4: 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 $\boldsymbol{a} \in \mathbf{V}(T)$ nos basta ver que para cualquier $f \in \mathfrak{a}$ se cumpla que $f(\boldsymbol{a}) = 0$. Para ello notemos que si $f \in (T)$, entonces existen polinomios $\lambda_i(\boldsymbol{x}) \in A$ y $g_i(\boldsymbol{x}) \in T$ tales que

$$f(\boldsymbol{x}) = \sum_{i=1}^{m} \lambda_i(\boldsymbol{x}) g_i(\boldsymbol{x})$$

pero como $g_i(\boldsymbol{a}) = 0$ para todo $g_i \in T$ (por definición de estar en $\mathbf{V}(T)$) se concluye que $f(\boldsymbol{a}) = 0$. □

Corolario 9.5: Si el conjunto $Z \subseteq \mathbb{A}^n$ es algebraico, entonces existen finitos polinomios $p_1, \ldots, p_m \in A$ tales que $Z = \mathbf{V}(p_1, \ldots, p_m)$.

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 $J = (p_1, \ldots, p_m)$ que hacen cumplir el enunciado. □

Lema 9.6: 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 afínes 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 $\mathbf{V}(\mathfrak{a}\cdot\mathfrak{b}) \subseteq \mathbf{V}(\mathfrak{a})\cup\mathbf{V}(\mathfrak{b})$ por contrarrecíproca: Sea $\boldsymbol{a} \notin \mathbf{V}(\mathfrak{a})\cup\mathbf{V}(\mathfrak{b})$, por definición existe $f\in\mathfrak{a}, g\in\mathfrak{b}$ tales que $f(\boldsymbol{a})\neq 0\boldsymbol{g}(\boldsymbol{a})$. Luego $f(\boldsymbol{a})g(\boldsymbol{a}) = (f\cdot g)(\boldsymbol{a}) \neq 0$ donde $f\cdot g\in\mathfrak{a}\cdot\mathfrak{b}$, por lo que $\boldsymbol{a}\notin\mathbf{V}(\mathfrak{a}\cdot\mathfrak{b})$.

   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 $\mathbf{V}_k(\mathfrak{a}\cap\mathfrak{b}) \supseteq \mathbf{V}(\mathfrak{a})$ (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. 9.4 induce la primera igualdad.

   La segunda se deduce de lo siguiente:
$$\begin{aligned}\bigcap_{j\in J}\mathbf{V}_k(\mathfrak{a}_j) &= \{\boldsymbol{a}\in\mathbb{A}^n : \forall j\ \boldsymbol{a}\in\mathbf{V}(\mathfrak{a}_j)\}\\ &= \{\boldsymbol{a}\in\mathbb{A}^n : \forall j\forall f\in\mathfrak{a}_j\ f(\boldsymbol{a})=0\}\\ &= \left\{\boldsymbol{a}\in\mathbb{A}^n : \forall f\in\left(\bigcup_{j\in J}\mathfrak{a}_j\right)\ f(\boldsymbol{a})=0\right\}\\ &= \mathbf{V}\left(\bigcup_{j\in J}\mathfrak{a}_j\right).\end{aligned}$$
□

Definición 9.7: 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 $\mathbb{A}^1, \varnothing$ 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 9.8: Sea $X \subseteq \mathbb{A}^n$, se define:

$$\mathbf{I}(X) := \{f \in A : \forall \boldsymbol{a} \in X \ f(\boldsymbol{a}) = 0\}.$$

Lema 9.9: Para todo $X \subseteq \mathbb{A}^n$ se cumple que $\mathbf{I}(X)$ es un ideal.

Proposición 9.10: Si $X \subseteq \mathbb{A}^n$, entonces $\mathbf{I}(X)$ es un ideal radical.

DEMOSTRACIÓN: Sea $f^n \in \mathbf{I}(X)$, entonces $f(\boldsymbol{a})^n = 0$ para todo $\boldsymbol{a}$. Luego, como k es un cuerpo y, por ende, un dominio íntegro se cumple que $f(\boldsymbol{a}) = 0$ y $f \in \mathbf{I}(X)$. □

Ahora veremos uno de los resultados principales de la geometría algebraica:

Teorema 9.11 – *Teorema de ceros de Hilbert*: Sea k algebraicamente cerrado. Entonces:

1. Si $\mathfrak{a} \trianglelefteq k[x_1, \ldots, x_n]$ es un ideal, entonces $\mathbf{V}(\mathfrak{a}) = \varnothing$ syss $\mathfrak{a} = (1)$ (débil).
2. Dado un ideal $\mathfrak{a} \trianglelefteq k[x_1, \ldots, x_n]$ se cumple que $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a})$ (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 $\mathbf{V}(1) = \varnothing$. Recíprocamente y por contradicción sea $\mathfrak{a} \neq A$ tal que $\mathbf{V}(\mathfrak{a}) = \varnothing$, por el teorema de Krull está contenido en un ideal maximal $\mathfrak{m}$ que por el Nullstellensatz algebraico es de la forma $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. Pero claramente $(\alpha_1, \ldots, \alpha_n) \in \mathbf{V}(\mathfrak{m}) \subseteq \mathbf{V}(\mathfrak{a})$, así que $\mathbf{V}(\mathfrak{a}) \neq \varnothing$.

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 $\mathrm{Rad}(\mathfrak{a}) \subseteq \mathbf{I}(\mathbf{V}(\mathfrak{a}))$.

   Sea $F \in \mathbf{I}(\mathbf{V}(\mathfrak{a}))$, es decir, $F(\boldsymbol{p}) = 0$ para todo $\boldsymbol{p} \in \mathbf{V}(\mathfrak{a})$, la cual satisface que $H(\boldsymbol{p})$ 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 $\mathfrak{a} = (G_1, \ldots, G_m)$. Para probar lo que queremos emplearemos un truco atribuido a Rabinowitsch: Añadamos una variable extra z a $K[x_1, \ldots, x_n; z]$ y definamos $\mathfrak{b} := (G_1, \ldots, G_m; 1 - Fz)$.

Veamos que $\mathbf{V}(\mathfrak{b}) = \varnothing$: Por contradicción, si no lo fuese tendría algún punto $(p_1, \ldots, p_n; q) \in \mathbb{A}_K^{n+1}$. Luego para todo i se cumple que $G_i(p_1, \ldots, p_n) = 0$ y además $1 - F(p_1, \ldots, p_n) \cdot q = 0$; pero claramente $(p_1, \ldots, p_n) \in \mathbf{V}(\mathfrak{a})$ así que $F(p_1, \ldots, p_n) = 0$ por construcción lo que es contradictorio.

En consecuencia, por el Nullstellensatz geométrico se tiene que $\mathfrak{b} = (1)$, es decir, existen $H_i, L \in K[x_1, \ldots, x_n, z]$ 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

$$H_i(x_1, \ldots, x_n, 1/F) = \frac{H_i'(x_1, \ldots, x_n)}{F(x_1, \ldots, x_n)^r}$$

donde r es el grado máximo entre los H_i's. De modo que se obtiene que

$$\sum_{i=1}^{m} \frac{H_i'}{F^r} G_i = 1 \iff F^r = H_1' G_1 + \cdots + H_m' G_m$$

Ésto 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. □

Proposición 9.12: 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, $\mathbf{V}(\mathbf{I}(X)) = \overline{X}$. □

Corolario 9.13: Se cumple que

$$\{X \subseteq \mathbb{A}^n : X \text{ algebraico}\} \underset{\mathbf{V}}{\overset{\mathbf{I}}{\rightleftarrows}} \{\mathfrak{a} \subseteq A : \mathfrak{a} \text{ ideal radical}\}$$

son biyecciones y son la inversa la una de la otra.

Definición 9.14: 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 9.15: En un espacio topológico X son equivalentes:

1. X es irreducible.
2. Si U_1, U_2 son abiertos no vacíos, entonces $U_1 \cap U_2 \neq \varnothing$.
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. □

Lema 9.16: Sea $Y \subseteq X$ es no vacío, entonces Y es irreducible syss 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

$$\varnothing \neq U_1 \cap U_2 \cap Y \subseteq U_1 \cap U_2 \cap \overline{Y},$$

lo que demuestra que $\overline{Y}$ es □

Definición 9.17: Una *componente irreducible* es un subconjunto irreducible $\subseteq$-maximal.

Teorema 9.18: 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 componenetes irreducibles.

Definición 9.19: Se dice que un espacio topológico X es *noetheriano* si para toda sucesión $(F_n)_{n\in\mathbb{N}}$ de cerrados tal que

$$F_1 \supseteq F_2 \supseteq F_3 \supseteq \cdots$$

se cumple que existe un n tal que para todo $m > n$ se da que $F_m = F_n$.

Proposición 9.20: 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 $F = F_1 \cup \cdots \cup F_n$, donde los F_i's son irreducibles distintos. Si $F = F'_1 \cup \cdots \cup F'_m$, entonces $F'_j \subseteq F_1 \cup \cdots \cup F_n$ 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. □

Definición 9.21 – *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 9.22: 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 afínes.

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. □

Teorema 9.23: 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 9.24: 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 $\mathbf{V}_{\mathbb{C}}(y^2 - x(x^2 - 1))$ es una variedad afín, puesto que el polinomio $y^2 - x(x^2 - 1)$ es irreductible en $\mathbb{C}[x, y]$. Lo interesante es que su gráfico (fig. 9.1) 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.

9.2. Variedades proyectivas

Lema 9.25: En $k^{n+1} \setminus \{\vec{0}\}$, la relación:

$$\boldsymbol{u} \sim \boldsymbol{v} \iff \exists \lambda \in k \; \boldsymbol{u} = \lambda \boldsymbol{v}$$

es de equivalencia.

Definición 9.26: Se define el *espacio proyectivo* $\mathbb{P}^n := (k^{n+1} \setminus \{\vec{0}\})/\sim$. Cuyos elementos se denotan por

$$[a_0 : a_1 : \cdots : a_n] := [(a_0, a_1, \ldots, a_n)]_\sim.$$

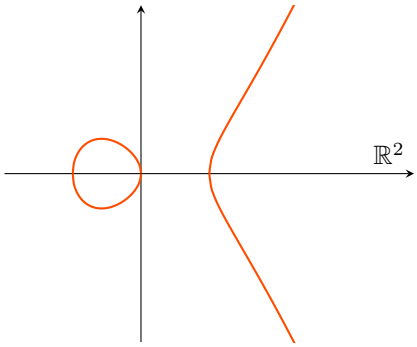


Figura 9.1

(Ésta notación debe entenderse como que la tupla es una «proporción», de ahí los «:».)

Para $0 \leq j \leq n$ se denota:

$$U_j := \{[a_0 : a_1 : \cdots : a_n] \in \mathbb{P}^n : a_j \neq 0\}.$$

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 9.27: Un polinomio $p \in k[x_0, \ldots, x_n]$ se dice *homogéneo* si todos sus monomios son de igual grado.

Antes de seguir necesitaremos la siguiente definición:

Definición 9.28: Se dice que un anillo R es *graduado* si admite una descomposición $\bigoplus_{d\in\mathbb{N}} R_d$, donde:

1. Cada R_i es un subanillo y un grupo abeliano bajo la suma.
2. Cada R_i es un R_0-módulo.
3. Para cada $d, e \geq 0$ se satisface que $R_d \cdot R_e \subseteq R_{d+e}$.

Dicha descomposición se dice una *graduación*, y cada $f \in R_d$ se dice un elemento *homogéneo de grado d*. Un ideal $\mathfrak{a} \trianglelefteq R$ se dice *homogéneo* si $\mathfrak{a} = \bigoplus_{d\in\mathbb{N}}(\mathfrak{a} \cap R_d)$.

Consecuencia de la tercera propiedad es que el producto de elementos homogéneos es homogéneo.

Proposición 9.29: Un ideal $\mathfrak{a} \trianglelefteq R$ es homogéneo syss posee un generador mediante elementos homogéneos.

DEMOSTRACIÓN: $\Longleftarrow$. Sea T tal que $\mathfrak{a} = (T)$ y tal que los elementos de T son homogéneos. Luego, sea $f \in \mathfrak{a}$, por definición

$$f = g_1 f_1 + \cdots g_n f_n$$

donde $f_i \in T$ y $g_i \in R$. Como R 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 $\lambda_{ji} \in R_0$. 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, $f \in \bigoplus_{d\in\mathbb{R}} (\mathfrak{a} \cap R_d)$. La otra inclusión es trivial.

$\Longrightarrow$. Basta notar que por definición $\mathfrak{a} = \left(\bigcup_{d\in\mathbb{N}} (\mathfrak{a} \cap R_d)\right)$. □

Proposición 9.30: Sean $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ homogéneos. Entonces:

1. $R/\mathfrak{a} = \bigoplus_{d\in\mathbb{N}} R_d/\mathfrak{a}$. En consecuente, $R/\mathfrak{a}$ es un anillo graduado.
2. $\mathfrak{a}$ es primo syss para todos $f, g \in R$ 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. (AE) $\mathrm{Rad}(\mathfrak{a})$ es homogéneo.

DEMOSTRACIÓN:

1. Es claro ver que $R/\mathfrak{a} = \sum_{d\in\mathbb{N}} R_d/\mathfrak{a}$ en general (vale incluso si $\mathfrak{a}$ no es homogéneo). Así que queda probar que están en suma directa, para ello sean $f \in R_d/\mathfrak{a} \cap R_e/\mathfrak{a}$ con $d \neq e$. Es decir, $f = f_d + g_d = f_e + g_e \in R$, donde $f_d \in R_d, f_e \in R_e$ 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 $f = 0 \in R/\mathfrak{a}$ como se quería probar.

2. Claramente se cumple « $\Longrightarrow$ », veamos la otra implicancia: En primer lugar, como $f', g' \in R$ se ha de cumplir que

$$f' = \sum_{i=0}^{n} f_i, \quad g' = \sum_{j=0}^{m} g_j$$

con f_d, g_d homogéneos de grado d (posiblemente nulos). Luego sea $f'g' = \sum_{d=0}^{n+m} \sum_{i+j=d} f_i g_j \in \mathfrak{a}$. Por construcción, se debe cumplir que cada término homogéneo $h_d := \sum_{i+j=d} f_i g_j \in \mathfrak{a}$. Luego haremos la demostración por inducción sobre la cantidad de términos homogéneos de $f'g'$:

El caso base: un solo término, es trivial ya que $f' = f_i$ y $g' = g_j$, donde cada término es homogéneo. Y el caso inductivo se ve así:

$$f'g' = h_0 + h_1 + \cdots + h_{n+m}.$$

Donde $h_{n+m} \neq 0$. Como $\mathfrak{a}$ es un ideal homogéneo ha de cumplirse que cada $h_d \in \mathfrak{a}$. Además, $h_{n+m} = f_n g_m \in \mathfrak{a}$ necesariamente. Luego, $f_n \in \mathfrak{a}$ o $g_m \in \mathfrak{a}$, sin perdida de generalidad supongamos la primera. Luego

$$(f' - f_n)g' = h_0 + \cdots + h_{n-1} + h'_n + \cdots + h'_{n+m-1}$$

donde cada $h'_{n+i} = f_{n-1}g_{i+1} + \cdots = h_{n+i} - f_n g_i$. Sin embargo, como $f_n \in \mathfrak{a}$ se cumple que $h'_{n+i} \in \mathfrak{a}$, por lo que $(f' - f_n)g' \in \mathfrak{a}$ y tiene menos términos que el original, así que, por hipótesis inductiva, se cumple que $(f' - f_n) \in \mathfrak{a}$ o $g' \in \mathfrak{a}$; lo que concluye el caso inductivo.

3. La intersección es trivial. Sean T_a, T_b son generadores por homogéneos de $\mathfrak{a}, \mathfrak{b}$ resp. Para la suma, basta notar que $T_a \cup T_b$ es un generador por homogéneos de $\mathfrak{a} + \mathfrak{b}$, y para el producto basta notar que $T_a \cdot T_b = \{fg : f \in T_a, g \in T_b\}$ es generador por homogéneos de $\mathfrak{a} \cdot \mathfrak{b}$.

4. Emplearemos la caracterización del radical como intersección de ideales primos, notando que si $\mathfrak{a} \subseteq \mathfrak{p}$, con $\mathfrak{p} \trianglelefteq R$ primo, entonces existe $\mathfrak{a} \subseteq \mathfrak{p}_h \subseteq \mathfrak{p}$, donde $\mathfrak{p}_h$ es primo y homogéneo. Para ello definamos

$$\mathfrak{p}_h := \big(\{f \in \mathfrak{p} : f \text{ homogéneo}\}\big),$$

por el inciso anterior se concluye que $\mathfrak{p}_h$ es primo y claramente $\mathfrak{a} \subseteq \mathfrak{p}_h$. Luego, hemos probado que

$$\operatorname{Rad}(\mathfrak{a}) = \bigcap \{\mathfrak{p} : \mathfrak{a} \subseteq \mathfrak{p} \trianglelefteq R \text{ primo y homogéneo}\}$$

de modo que $\operatorname{Rad}(\mathfrak{a})$ es homogéneo por el inciso anterior. □

El ejemplo vital es $R = k[x_0, x_1, \ldots, x_n]$ como anillo graduado, donde sus elementos homogéneos de grado d son los polinomios homogéneos de grado d.

Proposición 9.31: Si $p \in k[x_0, \ldots, x_n]$ es homogéneo, entonces para todo $\boldsymbol{x} \in k^{n+1}$ y todo $\lambda \in k$ se cumple que

$$p(\lambda \boldsymbol{x}) = \lambda^d p(\boldsymbol{x}),$$

donde $d = \deg p$. En consecuente, la expresión «$f(\boldsymbol{u}) = 0$» para $\boldsymbol{u} \in \mathbb{P}^n$ está bien definida.

Definición 9.32: Sean $T \subseteq k[x_0, \ldots, x_n]$ un conjunto de polinomios homogéneos, entonces se define

$$\mathbf{V}(T) := \{\boldsymbol{a} \in \mathbb{P}^n : \forall f \in T \ f(\boldsymbol{a}) = 0\}.$$

Los conjuntos de ésta forma son llamados *algebraicos proyectivos*. Así mismo, dado $Z \subseteq \mathcal{P}^n$ se define

$$\mathbf{I}(Z) := \big(\{f \in k[x_0, \ldots, x_n] \text{ homogéneo} : \forall \boldsymbol{p} \in Z \ f(\boldsymbol{p}) = 0\}\big).$$

Y ahora varios de los resultados de los conjuntos algebraicos afínes aplican también con demostraciones análogas:

Teorema 9.33: Los conjuntos algebraicos proyectivos forman los cerrados de una única topología en $\mathbb{P}^n$.

Definición 9.34: Dicha topología, es llamada la *topología de Zariski* sobre $\mathbb{P}^n$.

Corolario 9.35: 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 8 (ideal irrelevante): Sea $\mathfrak{a} := (x_0, x_1, \ldots, x_n) \trianglelefteq k[x_0, \ldots, x_n]$. Por definición es un ideal y es homogéneo por ser generado por homogéneos. Sin embargo, nótese que $\mathbf{V}(\mathfrak{a}) = \varnothing$, 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, $[0 : 0 : \cdots : 0] \notin \mathbb{P}^n$. A $\mathfrak{a}$ le decimos el *ideal irrelevante*. Nótese que el ideal irrelevante es de hecho un ideal primo, así que $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = (1) \neq \mathfrak{a} = \mathrm{Rad}(\mathfrak{a})$.

Y otro caso del teorema de ceros de Hilbert para el espacio proyectivo:

Teorema 9.36: Sea $\mathfrak{a} \trianglelefteq k[x_0, \ldots, x_n]$ un ideal homogéneo no irrelevante. Entonces $\mathbf{I}(\mathbf{V}(\mathfrak{a})) = \mathrm{Rad}(\mathfrak{a})$.

Y como corolarios:

Corolario 9.37: Se cumple que:

1. Si $T \subseteq k[x_0, \ldots, x_n]$ 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 $k[x_0, \ldots, x_n]$.

Definición 9.38: Admitimos las siguientes funciones:

$$\begin{aligned} \phi\colon \mathbb{A}^n &\longrightarrow U_0 \\ (x_1, \ldots, x_n) &\longmapsto [1 : x_1 : \cdots : x_n] \end{aligned}$$

$$\begin{aligned} \alpha\colon k[x_0, \ldots, x_n] &\longrightarrow k[x_1, \ldots, x_n] \qquad \beta\colon k[x_1, \ldots, x_n] \longrightarrow k[x_0, \ldots, x_n] \\ p(x_0, x_1, \ldots, x_n) &\longmapsto p(1, x_1, \ldots, x_n) \qquad q(x_1, \ldots, x_n) \longmapsto x_0^{\deg q} q\left(\frac{x_1}{x_0}, \ldots \frac{x_n}{x_0}\right) \end{aligned}$$

ϕ es una biyección, el resto no.

Proposición 9.39: Algunas propiedades:

1. ϕ es una biyección.
2. $\beta \circ \alpha = \mathrm{Id}$.
3. Si $p \in k[x_0, \ldots, x_n]$ 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

$$(\alpha \circ \beta)(x_0x_1 + x_0^2) = \beta(x_1 + 1) = x_1 + x_0.$$

Lema 9.40: Sea $Z := \mathbf{V}_{\mathbb{P}^n}(T)$, donde T son polinomios homogéneos. Entonces $\phi^{-1}[Z \cap U_0] = \mathbf{V}_{\mathbb{A}^n}\big(\alpha[T]\big)$.

Demostración: Sea $[1 : x_1 : \cdots : x_n] \in Z \cap U_0$. Por definición, para todo $f \in T$ se cumple que $\alpha(f)(x_1, \ldots, x_n) = f(1, x_1, \ldots, x_n) = 0$. Por lo que $(x_1, \ldots, x_n) \in \mathbf{V}_{\mathbb{A}^n}\big(\alpha[T]\big)$.

La demostración es análoga. □

Definición 9.41: Definamos $\pi\colon \mathbb{A}^{n+1} \setminus \{\vec{0}\} \to \mathbb{P}^n$ la proyección canónica (puesto que es un conjunto cociente). Además si Z es un conjunto algebraico proyectivo, definimos

$$\mathrm{C}_{\mathrm{af}}(Z) := \pi^{-1}[Z] \cup \{\vec{0}\}.$$

Lema 9.42: Si $T \subseteq k[x_0, \ldots, x_n]$ está formado por homogéneos, entonces $\mathrm{C}_{\mathrm{af}}\big(\mathbf{V}_{\mathbb{P}^n}(T)\big) = \mathbf{V}_{\mathbb{A}^{n+1}}(T)$.

Definición 9.43: Sea $Z \subseteq \mathbb{A}^n$ un conjunto algebraico afín, entonces

$$\overline{Z}_{\mathrm{proy}} := \overline{\phi[Z]} \subseteq \mathbb{P}^n.$$

(Nótese que Z ya es $\mathbb{A}^n$-cerrado, por lo que la notación no debería confundir.)

Teorema 9.44: Sea $Z \subseteq \mathbb{A}^n$ algebraico afín y sea $\mathfrak{a} := \mathbf{I}_{\mathbb{A}^n}(Z)$. Entonces

$$\overline{Z}_{\mathrm{proy}} = \mathbf{V}_{\mathbb{P}^n}\big(\beta[\mathfrak{a}]\big), \qquad \overline{Z}_{\mathrm{proy}} \cap U_0 = \phi[Z].$$

Demostración: Sea $Z' := \mathbf{V}_{\mathbb{P}^n}\big(\beta[\mathfrak{a}]\big)$, probaremos el enunciado por doble contención. Como $\overline{Z}_{\mathrm{proy}}$ es el menor cerrado que contiene a $\phi[Z]$ y Z' es cerrado, basta notar que para todo $[1 : a_1 : \cdots : a_n] \in \phi[Z]$ se cumple que para todo $f \in \mathfrak{a}$ se satisface

$$\beta(f)(1, a_1, \ldots, a_n) = 1^r f\left(\frac{a_1}{1}, \ldots, \frac{a_n}{1}\right) = f(a_1, \ldots, a_n) = 0.$$

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,

$$(\alpha \circ \beta)(f) \in \mathbf{I}_{\mathbb{P}^n}\left(\mathbf{V}_{\mathbb{P}^n}(\beta[\mathfrak{a}])\right) = \mathbf{I}_{\mathbb{P}^n}(Z').$$

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 $\boldsymbol{p} := [1 : p_1 : \cdots : p_n] \in \overline{Z}_{\text{proy}} \cap U_0$, entonces $f(\boldsymbol{p}) = 0$ para todo $\beta(f) \in \beta[\mathfrak{a}]$, luego

$$0 = \beta(f)(1, p_1, \ldots, p_n) = [(\beta \circ \alpha)(f)](p_1, \ldots, p_n) = f(p_1, \ldots, p_n)$$

es decir, $(p_1, \ldots, p_n) \in Z$ como se quería probar. □

Corolario 9.45: $\phi\colon \mathbb{A}^n \to U_0$ es un homeomorfismo.

Definición 9.46: 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 9.47: Un cerrado $F \subseteq \mathbb{P}^n$ es una variedad proyectiva syss $\mathbf{I}(F)$ es un ideal primo homogéneo no irrelevante.

Teorema 9.48: 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 $\mathfrak{a} := \mathbf{I}_{\mathbb{P}^n}\left(\overline{W}_{\text{proy}}\right)$ es primo y no irrelevante. Como $\varnothing \neq W \subseteq \overline{W}_{\text{proy}}$, entonces su ideal no es irrelevante. Así pues, falta ver que es primo: Sean $f, g \in k[x_0, \ldots, x_n]$ 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 perdida 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. □

9.3. Funciones polinómicas y regulares

Definición 9.49: Sea $X \subseteq \mathbb{A}^n$ un conjunto cerrado. Se denota por

$$k[X] := \{f \colon X \to \mathbb{A}^1 : f \text{ es polinómica}\}.$$

Claramente $k[X]$ es una subálgebra de $\text{Func}(X; \mathbb{A}^1)$. A $k[X]$ le llamamos el *anillo de coordenadas afínes* de X.

Claramente existe un k-homomorfismo desde $r \colon k[\mathbb{A}^n] \to k[X]$ dado por la restricción. Nótese que $f \in \ker r$ syss $f(\boldsymbol{p}) = 0$ para todo $\boldsymbol{p} \in X$, 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 9.50: Sea X una variedad cuasi-afín. Una aplicación $\phi \colon X \to k$ se dice *regular* en $\boldsymbol{p} \in X$ si existe un entorno abierto U de $\boldsymbol{p}$, 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 $\phi \colon Y \to k$ se dice *regular* en $\boldsymbol{p} \in Y$ si existe un entorno abierto U de $\boldsymbol{p}$, 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 9.51: $\mathcal{O}(X)$ es un k-álgebra en un sentido canónico.

Proposición 9.52: Para todo $\phi \in \mathcal{O}(X)$, viéndolo como aplicación $\phi\colon X \to \mathbb{A}^1$, se cumple que f 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. □

Definición 9.53: Sean X, Y variedades y sea $\varphi\colon X \to Y$. Entonces φ es un *morfismo* si:

1. φ es continua.
2. Para todo $U \subseteq Y$ abierto no vacío y todo $f \in \mathcal{O}(U)$ se cumple que $\varphi \circ f\colon \varphi^{-1}[U] \to k$ es regular.

Lema 9.54: Sean X, Y variedades, y sea $f\colon X \to Y$ continua. Entonces f es un morfismo syss 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 $(f \circ \psi) \in \mathcal{O}\big(f^{-1}[U]\big)$.

Demostración: $\Longrightarrow$. Trivial.

$\Longleftarrow$. 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 $f \circ \psi \in \mathcal{O}\big(f^{-1}[V]\big)$. 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 $f \circ \psi \restriction V_q = g/h$ con $g, h \in k[\mathbb{A}^n]$; es decir, $f \circ \psi$ es regular como se quería probar. □

Proposición 9.55: Sea X una variedad. Entonces:

1. $\mathrm{Id}_X\colon X \to X$ 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 Var.

Demostración: Sean $\alpha\colon X \to Y$ y $\beta\colon Y \to Z$ morfismos. Fijemos $p \in Z$, entonces, como β es morfismo, existe un entorno abierto U_p de p tal que para todo $\psi \in \mathcal{O}(U)$ se cumple que $\beta \circ \psi \in \mathcal{O}\big(\beta^{-1}[U_p]\big)$. Como $\beta^{-1}[U_p]$ es abierto en Y y $\beta \circ \psi$ es regular, entonces

$$\alpha \circ (\beta \circ \psi) = (\alpha \circ \beta) \circ \psi \in \mathcal{O}\left(\alpha^{-1}\big[\beta^{-1}[U_p]\big]\right) = \mathcal{O}\big((\alpha \circ \beta)^{-1}[U_p]\big). \qquad \square$$

Teorema 9.56: Sea $f\colon X \to Y$ un morfismo de variedades, entonces la pre-composición:

$$\begin{aligned} h_f\colon \mathcal{O}(Y) &\longrightarrow \mathcal{O}(X) \\ \phi &\longmapsto f \circ \phi \end{aligned}$$

es un morfismo de k-álgebras. En consecuencia el siguiente es un funtor contravariante desde Var a Alg_k:

$$\begin{array}{ccc} X & & \mathcal{O}(X) \\ {\scriptstyle f}\big\downarrow & \overset{h_-}{\Longrightarrow} & \big\uparrow{\scriptstyle h_f} \\ Y & & \mathcal{O}(Y) \end{array}$$

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 9.57: 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 $(U, f) \sim (V, g)$ y $(W, h) \in C$, entonces:

1. $(U \cap W, f + h) \sim (V \cap W, g + h)$.
2. $(U \cap W, f \cdot h) \sim (V \cap W, g \cdot h)$.
3. $(U, \lambda f) \sim (V, \lambda g)$ para todo $\lambda \in k$.

Definición 9.58: 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 9.59: $\mathcal{O}_{p,X}$ es un anillo local, cuyo único ideal maximal es

$$\mathfrak{m}_{p,X} := \{\langle U, \phi \rangle : \phi(p) \neq 0\}.$$

Proposición 9.60: Considerando a $\mathscr{D}$ 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 $\mathscr{D}$ a Alg_k:

$$\begin{aligned} r \colon \mathcal{O}(V) &\longrightarrow \mathcal{O}(U) \\ \phi &\longmapsto \phi|_U \end{aligned} \qquad \begin{array}{ccc} U & & \mathcal{O}(U) \\ \subseteq \downarrow & \overset{F}{\Longrightarrow} & \uparrow r \\ V & & \mathcal{O}(V) \end{array}$$

Y se cumple que $\mathcal{O}_{p,X} = \varinjlim_{U \in \mathscr{D}} F(U)$.

9.4. Dimensión

Definición 9.61: 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

$$\varnothing \neq X_0 \subset X_1 \subset \cdots \subset X_d$$

de cerrados irreducibles en X.

Ejemplo. Se cumple que $n\text{-dim}\{\boldsymbol{p}\} = 0$ 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.
$\Longrightarrow$	Implica, entonces.
$\Longleftrightarrow$	Si y sólo si.
$\forall, \exists$	Para todo, existe respectivamente.
$\in$	Pertenencia.
$\subseteq, \subset$	Subconjunto, subconjunto propio resp.
$\cup, \cap$	Unión e intersección binaria respectivamente.
$A \setminus B$	Resta conjuntista, A menos B.
A^c	Complemento de A (respecto a un universo relativo).
$A \times B$	Producto cartesiano de A por B.
$A_{\neq x}$	Abreviación de $A \setminus \{x\}$.
$f : A \to B$	Función f de dominio A y codominio B.
$f \circ g$	Composición de f con g. $(f \circ g)(x) = g(f(x))$.
$\mathcal{P}(A)$	Conjunto potencia de A.
resp.	Respectivamente.

syss	Si y sólo si.
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$	Conjuntos de números naturales, enteros y racionales resp.
$\aleph_0$	Cardinal numerable, cardinalidad de $\mathbb{N}$.
AE	Axioma de elección.
DE, AEN	Axioma de elecciones dependientes, y de elecciones numerables resp.
ZF(C)	Teoría de Zermelo-Fraenkel. La C representa el axioma de elección.
a^{-1}	Inversa de un elemento invertible en un grupo, p. 4.
$S \leq G$	S es subgrupo (anillo o espacio) de G, p. 6.
$\langle S \rangle$	Subgrupo, cuerpo o espacio generado por S, p. 6.
$\operatorname{ord} x$	Orden de un elemento x, p. 7.
$G \cong H$	G y H son estructuras isomorfas, p. 9.
$\mathbb{Z}_n^\times$	Grupo multiplicativo o de las unidades de n, aquél formado por los coprimos de n, p. 11.
$\phi(n)$	Función indicatriz de Euler de n, esto es, la cantidad de coprimos positivos menores a n, p. 11.
S_n	Grupo simétrico sobre $\{1, 2, \ldots, n\}$, p. 13.
$\operatorname{sgn} \sigma$	Signo de la permutación σ, p. 15.
A_n	Grupo alternante en S_n, p. 16.
D_{2n}	Grupo diedral de cardinal $2n$, p. 17.
$N \trianglelefteq G$	N es subgrupo de G, p. 18.
$Z(S), Z(G)$	Centralizador de S, centro de G resp., p. 18.
$\mathrm{N}_G(S)$	Normalizador de S, p. 19.
$C_G(S)$	Clase de conjugación de S, p. 19.
K_4	Grupo de Klein de 4 elementos, $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, p. 26.

$N \rtimes_\alpha A$	Producto semidirecto de N con A, donde A actúa sobre N, p. 28.
Orb_a	Órbita de a, osea, los $\alpha_g(a)$ para todo $g \in G$, p. 29.
Stab_a	Estabilizador de a, osea, los $g \in G$ que dejan a a fijo, p. 29.
$\mathrm{Fix}_g(S)$	Puntos fijos de la acción α_g sobre S, p. 32.
$\mathrm{Fix}_G(S)$	Puntos fijos de todas las acciones sobre S, p. 32.
$\mathrm{Syl}_p(G)$	El conjunto de p-subgrupos de Sylow de G, p. 33.
$A^\times$	El conjunto de elementos invertibles de un anillo unitario A, p. 50.
$\Bbbk$	Un cuerpo general, p. 51.
$\mathrm{Frac}(A)$	Cuerpo de fracciones de un dominio íntegro A, p. 67.
$A[S]$	Conjunto de polinomios con coeficientes en A y con indeterminadas de S, p. 69.
$\deg f$	Grado del polinomio f, p. 69.
$c(f)$	Contenido del polinomio f, p. 76.
$\mathbb{C}$	Conjunto de números complejos, p. 83.
$\mathrm{Re}\, z, \mathrm{Im}\, z$	Parte real e imaginaria de z resp., p. 83.
ζ_n	$= \mathrm{cis}(2\pi/n)$, raíz primitiva canónica n-ésima de la unidad, p. 85.
$\mathrm{Hom}_A(M, N)$	Espacio de morfismos de A-módulos desde M a N, p. 92.
$\det B$	Determinante de la matriz B, p. 116.
$\mathrm{adj}\, B$	Matriz adjunta de B, p. 117.
$\mathrm{rank}(A)$	Rango de una matriz o de una transformación lineal, p. 119.
$[K : k]$	Grado de la extensión K de k. Su dimensión como k-espacio vectorial, p. 121.
$\mathrm{Gal}(K/k)$	El conjunto de los k-automorfismos de K, donde K/k es una extensión de cuerpos, p. 129.

$\overline{k}$	La clausura algebraica de k, p. 148.
$\psi_A(x)$	$= \det(xI_n - A)$, el polinomio característico de A, p. 162.
$p_f(x), p_B(x)$	Polinomio característico de un endomorfismo o una matriz, p. 172.
$\sigma(f)$	Espectro de un endomorfismo lineal, o de una matriz cuadrada, p. 172.
B^*	$= \overline{B}^t$, p. 176.
$x \perp y$	x e y son ortogonales, p. 187.
$A^\perp$	Complemento ortogonal de A, p. 187.
$\mathfrak{a}^e$	$= \big(\varphi[\mathfrak{a}]\big)$, la extensión del ideal $\mathfrak{a}$, p. 204.
$\mathfrak{b}^c$	$= \varphi^{-1}[\mathfrak{b}]$, la contracción del ideal $\mathfrak{b}$, p. 204.
$\operatorname{As}\mathfrak{a}$	El conjunto de los ideales asociados a $\mathfrak{a}$, p. 207.
$\mathbf{V}(T)$	Espacio de ceros de los polinomios en T, p. 228.

Índice alfabético

Bibliografía

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. Fine, B. y Rosenberger, G. *The Fundamental Theorem of Algebra* (Springer-Verlag New York, 1997).
4. Garrett, P. *Abstract Algebra* `http://www-users.math.umn.edu/~garrett/m/algebra/` (2007).
5. Jacobson, N. *Lectures in Abstract Algebra* (Springer-Verlag, 1951).
6. Lang, S. *Algebra* (Springer-Verlag New York, 2002).
7. Lee, G. T. *Abstract Algebra. An Introductory Course* (Springer International, Switzerland, 2018).
8. Rotman, J. J. *Advanced Modern Algebra* 3.ª ed. 2 vols. (American Mathematical Society, 2015).

Álgebra lineal

9. Curtis, M. L. *Abstract Linear Algebra* (Springer-Verlag New York Inc., 1990).

10. GUIMERÁ, S. *Apuntes para una Licenciatura. Algebra y Geometría* (ed. NAVARRO GONZÁLEZ, J. A.) matematicas.unex.es/~navarro/licenciatura.pdf (2017).

11. IBORT, A. y RODRÍGUEZ, M. A. *Notas de Álgebra Lineal* http://mimosa.pntic.mec.es/jgomez53/matema/docums/ibort-algebra_lineal.pdf (2014).

12. KATZNELSON, Y. y KATZNELSON, Y. R. *A (Terse) Introduction to Linear Algebra* (American Mathematical Society, 2008).

Álgebra conmutativa

13. ATIYAH, M. F. y MCDONALD, I. G. *Introduction to Commutative Algebra* (Addison-Wesley, 1969).

14. CASTILLO, C. I. *Álgebra Homológica y Álgebra Conmutativa* https://www.uv.es/ivorra/Libros/Algcom.pdf (2020).

15. MILNE, J. S. *A Primer of Commutative Algebra* https://www.jmilne.org/math/xnotes/CA.pdf (2020).

16. SANCHO DE SALAS, C. y SANCHO DE SALAS, P. *Álgebra Conmutativa. Geometría Algebraica* http://hdl.handle.net/10662/4439 (Universidad de Extremadura, 2013).

Geometría algebraica

17. CASTILLO, C. I. *Geometría Algebraica* https://www.uv.es/ivorra/Libros/GA.pdf (2020).

18. CUTKOSKY, S. D. *Introduction to Algebraic Geometry* (American Mathematical Society, 2018).

19. HARTSHORNE, R. *Algebraic Geometry* (Springer-Verlag New York, 1977).

20. MILNE, J. S. *Algebraic Geometry* https://www.jmilne.org/math/CourseNotes/ag.html (2017).

21. SHAFAREVICH, I. *Basic Algebraic Geometry* 2 vols. (Springer-Verlag Berlin Heidelberg, 2013).

Artículos

22. Banaschewski, B. Algebraic Closure without Choice. *Mathematical Logic Quarterly.* doi:10.1002/malq.19920380136 (1992).

23. Banaschewski, B. A New Proof that "Krull implies Zorn". *Mathematical Logic Quarterly.* doi:10.1002/malq.19940400405 (1994).

24. Blass, A. Existence of Basis implies the Axiom of Choice. *Contemporary Mathematics* **31.** http://www.math.lsa.umich.edu/~ablass/bases-AC.pdf (1984).

25. Conrad, K. Infinite-dimensional Dual Spaces. https://kconrad.math.uconn.edu/blurbs/linmultialg/dualspaceinfinite.pdf (2018).

26. Conrad, K. Simplicity of A_n. https://kconrad.math.uconn.edu/blurbs/grouptheory/Ansimple.pdf (2018).

27. Conrad, K. The Sylow Theorems. https://kconrad.math.uconn.edu/blurbs/grouptheory/sylowpf.pdf (2018).

28. Conrad, K. Zorn's Lemma and some applications. https://kconrad.math.uconn.edu/blurbs/zorn1.pdf (2018).

29. Derksen, H. The Fundamental Theorem of Algebra and Linear Algebra. *The American Mathematical Monthly.* doi:10.2307/3647746 (2003).

Libros de autoría propia

30. Cuevas, J. *Teoría de Conjuntos* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/conjuntos/conjuntos.pdf (2022).

31. Cuevas, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).