Álgebra conmutativa

Bibliografía:

- Alberto del Valle Robles. *Álgebra Conmutativa Curso 2021–2022, Apuntes de Clase.* Cuarto curso del Grado en Matemáticas. Departamento de Matemáticas, Universidad de Murcia. Basado en apuntes previos de José Luis García Hernández.
- Clases de Manuel Saorín Castaño.
- Manuel Saorín Castaño. *Capítulo IV: Módulos sobre dominios de ideales principales.*
- Donald Knuth. *The Art of Computer Programming. Volume 1: Fundamental Algorithms*, 3rd. ed. (1997), pp. 45–87.

Los párrafos marcados como este proceden de ejercicios del libro.

Capítulo 1

Anillos conmutativos

Un **grupo abeliano** es un par $(A, +)$ formado por un conjunto A y una **suma** $+ : A \times A \to A$ asociativa, conmutativa, con un elemento neutro $0 \in A$ llamado **cero** y en el que cada $a \in A$ posee un simétrico u **opuesto** $-a$. Un **anillo** es una terna $(A, +, \cdot)$ formada por un grupo abeliano $(A, +)$ y un **producto** $\cdot : A \times A \to A$ asociativo y distributivo respecto a la suma $((a + b) \cdot c = (a \cdot c) + (b \cdot c)$ y $c \cdot (a + b) = (c \cdot a) + (c \cdot b))$.

El producto tiene precedencia sobre la suma, y escribimos $a - b \coloneqq a + (-b)$ y $ab \coloneqq a \cdot b$. Si A es un anillo y $a \in A$, definimos $0a = 0$, $a^0 = 1$ y, para $n \in \mathbb{N}$, $(n+1)a \coloneqq na + a$, $a^{n+1} \coloneqq a^n a$ y $(-na) \coloneqq -(na)$.

Un anillo es **conmutativo** si su producto es conmutativo, y tiene **identidad** si este tiene elemento neutro $1 \in A$ llamado **uno**. Salvo que se indique lo contrario, los anillos serán conmutativos y con identidad.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos con la suma y el producto usuales.

2. Para $c \in \mathbb{C}$, $\mathbb{Z}[c] \coloneqq \{\sum_{n=0}^{\infty} a_n c^n\}_{a \in \mathbb{Z}^{\mathbb{N}}} \subseteq \mathbb{C}$ es un anillo con la suma y el producto de complejos, y en particular lo es $\mathbb{Z}[\mathrm{i}] \coloneqq \{a + b\mathrm{i}\}_{a,b \in \mathbb{Z}}$, el **anillo de los enteros de Gauss**.

3. El conjunto de funciones $\mathbb{R} \to \mathbb{R}$ que se anulan en casi todo punto es un anillo conmutativo sin identidad con la suma y producto de funciones.

4. Si $(A_i)_{i \in I}$ es una familia de anillos, $\prod_{i \in I} A_i$ es un anillo con las operaciones componente a componente, el **anillo producto** de los A_i.

5. Dado un anillo A, $A[\![X]\!] \coloneqq A^{\mathbb{N}}$ es un anillo con la suma componente a componente y el producto $a \cdot b \coloneqq (\sum_{k=0}^{n} a_k b_{n-k})_n$, el **anillo de las series de potencias** sobre A, y un $a \in A$ se suele denotar como $\sum_n a_n X^n$.

GyA

Llamamos Y^X al conjunto de funciones de X a Y. [...]. Si A es un anillo y n es un entero positivo, [...] $\mathcal{M}_n(A)$ [...] es un anillo con la suma y el producto habituales.

Sean A un anillo y $a, b, c \in A$: [...]

3. [...] El 0 y el 1 son únicos.

4. El opuesto de a es único, y si a es invertible, el inverso es único.

5. $0a = a0 = 0$.

6. $a(-b) = (-a)b = -(ab)$.

7. $a(b - c) = ab - ac$.

[...] Dados un anillo A, $a, b \in A$ y $m, n \in \mathbb{Z}$:

1. $n(a + b) = na + nb$.

2. $(n + m)a = na + ma$.

3. $n(ma) = (nm)a$.

Dados dos anillos A y B, un **homomorfismo de anillos** es una $f : A \to B$ tal que $f(1) = 1$ y, para $x, y \in A$, $f(x + y) = f(x) + f(y)$ y $f(xy) = f(x)f(y)$.

GyA

Un **automorfismo** de A es un isomorfismo de A en A. [...] Sean $f : A \to B$ un homomorfismo de anillos y $a, b, a_1, \ldots, a_n \in A$:

1. $f(0) = 0$.

2. $f(-a) = -f(a)$.

3. $f(a - b) = f(a) - f(b)$.

5. $f(na) = nf(a)$.

[...] Ejemplos:

1. Dados anillos A y B, $f : A \to B$ dada por $f(a) = 0$ es un homomorfismo si y sólo si $B = 0$. [...]

3. Dado un anillo A, $\mu : \mathbb{Z} \to A$ dada por $\mu(n) \coloneqq n1$ es el único homomorfismo de anillos de $\mathbb{Z}$ en A.

4. Dada una familia de anillos $(A_i)_{i \in I}$ y $j \in I$, la **proyección** $p_j : \prod_{i \in I} A_i \to A_j$ dada por $p_j(a) \coloneqq a_j$ es un homomorfismo.

5. La **conjugación** de complejos, dada por $\overline{a + bi} \coloneqq a - bi$ para $a, b \in \mathbb{R}$, es un automorfismo en $\mathbb{C}$. [...] Si d es un entero que no es un cuadrado, definiendo el conjugado de $a + b\sqrt{d}$ como $a - b\sqrt{d}$ en $\mathbb{Z}[\sqrt{d}]$ o en $\mathbb{Q}[\sqrt{d}]$ tenemos un automorfismo.

Un homomorfismo $f : A \to B$ es inyectivo si y sólo si $\ker f = 0$.

$\implies$] Obvio.

$\impliedby$] $f(a) = f(b) \implies 0 = f(a) - f(b) = f(a-b) \implies a - b = 0 \implies a = b$.

Un **isomorfismo de anillos** es un homomorfismo biyectivo, y su inverso es un homomorfismo. En efecto, sea $f : A \to B$ un isomorfismo, como $f(1) = 1$, $f^{-1}(1) = 1$; si $b, b' \in B$, sean $a \coloneqq f^{-1}(b)$ y $a' \coloneqq f^{-1}(b')$, entonces $f(a + a') = f(a) + f(a') = b + b'$, luego $f^{-1}(b + b') = a + a' = f^{-1}(b) + f^{-1}(b')$, y análogamente $f^{-1}(bb') = f^{-1}(b)f^{-1}(b')$. Dos anillos A y B son **isomorfos**, $A \cong B$, si existe un isomorfismo entre ellos.

Llamamos **anillo cero** o **trivial**, 0, al único con un solo elemento, o el único con $1 = 0$, salvo isomorfismo. En efecto, todo conjunto unipuntual es un anillo con la suma y producto definidos de la única forma posible, la única función entre estos anillos es un isomorfismo y, si el anillo A cumple $1 = 0$, para $a \in A$, $a = a1 = a0 = 0$.

1.1. Elementos notables

Sea A un anillo. Un $a \in A$ es **invertible** o **unidad** si existe $b \in A$ con $ab = 1$, en cuyo caso b es único, pues $ac = 1 \implies b = bac = c$; lo llamamos **inverso** de a o a^{-1}, y $(a^{-1})^{-1} = a$. Llamamos **grupo de las unidades** de A, $U(A)$ o A^*, al grupo abeliano formado por las unidades de A con el producto. Para $x, y \in A$, $xy \in A^* \iff x, y \in A^*$, en cuyo caso $(xy)^{-1} = y^{-1}x^{-1}$. Para $n \in \mathbb{N}$ y $a \in A^*$, llamamos $a^{-n} \coloneqq (a^{-1})^n = (a^n)^{-1}$.

GyA

4. Si $n, m \geq 0$, $a^{n+m} = a^n a^m$, y si a es invertible, esto se cumple para n y m enteros arbitrarios.

5. Si [...] $n \geq 0$, $(ab)^n = a^n b^n$, y si [...] a y b son invertibles, esto se cumple para todo entero n.

6. Si [$f : A \to B$ es un homomorfismo de anillos y] a es invertible, $f(a)$ también lo es y $f(a)^{-1} = f(a^{-1})$.

Un $a \in A$ es **cancelable** si $\forall x, y \in A, (ax = ay \implies x = y)$. Toda unidad es cancelable, pues podemos cancelar multiplicando por el inverso. Si A es finito se da el recíproco, pues $x \mapsto ax$ es inyectiva y por tanto suprayectiva y existe x con $ax = 1$. Para A infinito esto no es cierto en general, pues 2 es cancelable en $\mathbb{Z}$ pero no es unidad.

Un $a \in A$ es **divisor de cero** si existe $c \in A \setminus \{0\}$ con $ac = 0$, si y sólo si no es cancelable.

$\implies$] Si es cancelable, $ac = 0 = a0 \implies c = 0$, luego no es divisor de cero.

$\impliedby$] Sean $x, y \in A$ distintos con $ax = ay$, entonces $a(x - y) = 0$, pero $x - y \neq 0$.

Un $a \in A$ es **nilpotente** si existe $n \in \mathbb{N}$ con $a^n = 0$, en cuyo caso, si A no es trivial, a es divisor de cero, pues el 0 es claramente divisor de cero y, si $a \neq 0$, tomando el menor n con $a^n = 0$, $a^{n-1} \neq 0$ y $aa^{n-1} = 0$. Llamamos **nilradical** de A, $\mathrm{Nil}(A)$, al conjunto de elementos de A nilpotentes. El 1 es invertible. El 0 es nilpotente y, si A es no trivial, es no unidad.

Un $e \in A$ es **idempotente** si $e^2 = e$, en cuyo caso $f \coloneqq 1 - e$ también lo es y $ef = 0$.

Dado un homomorfismo $f : A \to B$, si $a \in A$ es invertible, nilpotente o idempotente, también lo es $f(a) \in B$. Si además f es inyectivo, si $f(a) \in B$ es cancelable, nilpotente o idempotente, también lo es $a \in A$.

Dados anillos $A_1, \dots, A_n$, $a \in A \coloneqq A_1 \times \cdots \times A_n$ es invertible, cancelable, divisor de cero, nilpotente o idempotente en A si y sólo si lo es cada a_i en A_i.

Para $m \in \mathbb{Z}$ no cuadrado, definimos la **norma** en $\mathbb{Z}[\sqrt{m}]$ como $N : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z}$ dada por $N(a + b\sqrt{m}) \coloneqq a^2 - mb^2$ para $a, b \in \mathbb{Z}$, y entonces:

1. Las unidades de $\mathbb{Z}[\sqrt{m}]$ son los elementos de norma 1.
2. Si $m < 0$, $\mathbb{Z}[\sqrt{m}]^*$ es finito.
3. Si $m > 0$ y $|\mathbb{Z}[\sqrt{m}]^*| > 2$, $|\mathbb{Z}[\sqrt{m}]^*| = |\mathbb{N}|$.

1.2. Subanillos

Dado un anillo A, un $S \subseteq A$ es un **subanillo** de A si es un anillo con las mismas operaciones y el mismo uno que A, si y sólo si es la imagen de un homomorfismo $B \to A$, si y sólo si $1 \in S$ y para $x, y \in S$, $x - y, xy \in S$.

$1 \implies 2]$ Basta tomar el homomorfismo inclusión.

$2 \implies 3]$ Sea $f : B \to A$ el homomorfismo, $f(1) = 1$ y, si $x', y' \in B$ cumplen $x = f(x')$ e $y = f(y')$, $x - y = f(x' - y') \in S$ y $xy = f(x'y') \in S$.

$3 \implies 1]$ $1 \in S$ y por tanto $1 - 1 = 0 \in S$, y para $a, b \in S$, $-a = 0 - a \in S$, $a + b = a - (-b) \in S$ y $ab \in S$, luego S es cerrado para suma, producto y opuesto.

Ejemplos:

1. En la cadena $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, cada anillo es subanillo de los que lo contienen, como pasa en $\mathbb{Z} \subseteq \mathbb{Z}[\mathrm{i}] \subseteq \mathbb{C}$.
2. Dado un anillo A, el **anillo** de los polinomios en A, $A[X]$, es el subanillo de $A[\![X]\!]$ formado por las series con una cantidad finita de elementos no nulos, y A es un subanillo de $A[X]$ identificando $a \in A$ con $(a, 0, \dots, 0, \dots)$ por isomorfismo.

GyA

1. Todo anillo A es un subanillo de sí mismo, el **subanillo impropio**, y el resto de subanillos son **propios**. [...]
3. $\{0\}$ es subanillo de A si y sólo si $A = \{0\}$.
4. Llamamos **subanillo primo** de A a $\mathbb{Z}1 \coloneqq \{n1_A\}_{n \in \mathbb{Z}}$, el menor subanillo de A.
5. Si A y B son anillos y $B \neq 0$, $A \times \{0_B\}$ es cerrado para sumas y productos pero no es un subanillo de $A \times B$. [...]

7. Dado un espacio topológico X, $\{f \in \mathbb{R}^X \mid f \text{ continua}\}$ es un subanillo de $\mathbb{R}^X$ con la suma y el producto por elementos.

8. Dado un espacio vectorial V, $\{f \in V^V \mid f \text{ lineal}\}$ es un subanillo de $(V^V, +, \circ)$.

9. Dado un anillo A y un conjunto X, $\{f \in A^X \mid f \text{ constante}\}$ es un subanillo de A^X.

[...] Si [$f : A \to B$ es un homomorfismo y] B' es un subanillo de B, $f^{-1}(B')$ es un subanillo de A.

1.3. Ideales

Un $I \subseteq A$ es un **ideal** de A, $I \trianglelefteq A$, si es el núcleo de un homomorfismo $A \to B$, si y sólo si $0 \in I$ y, para $a \in A$ y $x, y \in I$, $x+y, ax \in I$. En concreto, definiendo la relación de equivalencia **módulo** I en A como $a \equiv b \iff a - b \in I$, el conjunto cociente $A/I \coloneqq A/\equiv$ es un anillo con la suma $\overline{a} + \overline{b} \coloneqq \overline{a+b}$, el producto $\overline{a}\,\overline{b} \coloneqq \overline{ab}$, $0 = \overline{0}$, $1 = \overline{1}$, $-\overline{a} = \overline{-a}$ y, si $a \in A^*$, $\overline{a} \in (A/I)^*$ y $\overline{a}^{-1} = \overline{a^{-1}}$, donde $\overline{a}$ es la clase de equivalencia de a, y la **proyección canónica** $p : A \to A/I$ es un homomorfismo con núcleo I.

$\Longrightarrow$] Sean $f : A \to B$ un homomorfismo, $a \in A$ y $x, y \in \ker f$. Entonces $f(ax) = f(a)f(x) = f(a)0 = 0$ y $f(x+y) = f(x) + f(y) = 0 + 0 = 0$.

$\Longleftarrow$] Sean $a \equiv a', b \equiv b' \in A$, entonces $x \coloneqq a - a', y \coloneqq b - b' \in I$, luego $a+b = a'+x+b'+y = a' + b' + (x + y)$ con $x + y \in I$ y $a + b \equiv a' + b'$. Además $ab = (a' + x)(b' + y) = a'b' + a'y + b'x + xy$ con $a'y + b'x + xy \in I$, luego $ab \equiv a' + b'$ y el producto está bien definido. Entonces es fácil ver que A/I es un anillo con los neutros y simétricos indicados. Además, $p(1) = \overline{1}$, $p(a + b) = \overline{a + b} = \overline{a} + \overline{b} = p(a) + p(b)$ y del mismo modo $p(ab) = p(a)p(b)$, y $p(x) = \overline{x} = 0 \iff x - 0 = x \in I$.

Llamamos $\mathcal{L}(A)$ al conjunto de ideales de A. Todo anillo A tiene al menos el **ideal trivial** $0 \coloneqq \{0\}$ y el **ideal impropio** A, el único que contiene una unidad. En efecto, si $I \trianglelefteq A$ y existe $u \in I \cap A^*$, para $a \in A$, $a = (au^{-1})u \in I$, luego $I = A$. $I \trianglelefteq A$ es **propio**, $I \triangleleft A$, si no es impropio.

Dados anillos $A_1, \ldots, A_n$, $\mathcal{L}(A_1 \times \cdots \times A_n) = \{I_1 \times \cdots \times I_n\}_{I_i \trianglelefteq A_i, \forall i}$.

1.4. Ideales finitamente generados

La intersección de una familia de ideales de A es un ideal de A. Dados un anillo A y un subconjunto $S \subseteq A$, el **ideal de** A **generado por** S es

$$(S) \coloneqq \bigcap \{I \trianglelefteq A \mid S \subseteq I\} = \{a_1 s_1 + \cdots + a_n s_n\}_{n \in \mathbb{N}, a \in A^n, s \in S^n},$$

y S es un **conjunto generador** de (S). En efecto, $\bigcap\{I \trianglelefteq A \mid S \subseteq I\}$ es un ideal de A que contiene a S y es el menor de ellos, pero todo ideal de A que contenga a S debe contener a las combinaciones A-lineales finitas de elementos de S, y el conjunto de estas es claramente un ideal, luego ambos conjuntos son iguales.

$I \trianglelefteq A$ es **finitamente generado** (FG) si existe $S \subseteq I$ finito tal que $I = (S)$, en cuyo caso, si $S = \{b_1, \ldots, b_n\}$, escribimos $I =: (b_1, \ldots, b_n)$. Un **ideal principal** de un anillo A es uno de la forma (b) para algún $b \in A$. Por ejemplo, $0 = (0)$ y $A = (1)$. Dados $b \in A$ e $I \trianglelefteq A$, $(b) \subseteq I$ si y sólo si $b \in I$, y en particular para $b' \in A$, $(b) \subseteq (b')$ si y sólo si b' divide a b.

> Si $a \in A$ es nilpotente entonces $1 + (a) \subseteq A^*$ y, para $u \in A^*$, $u + a \in A^*$.
>
> Dado un anillo A y $b \in A$ cancelable no invertible, (b, X) no es un ideal principal de $A[X]$, y en particular (X, Y) no es un ideal principal de $A[X, Y] \coloneqq A[X][Y]$. Si $e \in A$ es idempotente, para $a \in A$, $a \in (e) \iff a = ea$, con lo que (e) es un anillo con identidad e.

No todos los ideales son finitamente generados. En efecto, dado un anillo no trivial A, en $A^{\mathbb{N}}$ con las operaciones componente a componente, $A^{(\mathbb{N})}$ formado por los elementos de $A^{\mathbb{N}}$ con una cantidad finita de entradas no nulas es un ideal de $A^{\mathbb{N}}$, pero no es finitamente generado porque si tomamos una cantidad finita de elementos del ideal, hay un índice a partir del cual todos tienen solo ceros y no generan elementos de $A^{(\mathbb{N})}$ con un 1 después de esta posición.

1.5. Dominios

Un anillo es **reducido** si no tiene elementos nilpotentes distintos de 0, si y sólo si todo elemento no nulo tiene cuadrado no nulo.

$\Longrightarrow$] Trivial.

$\Longleftarrow$] Si hubiera $b \in \mathrm{Nil}(A) \setminus \{0\}$, sea $n > 0$ mínimo con $b^n = 0$, entonces $b^{n-1} \neq 0$ y $(b^{n-1})^2 = b^{2n-2} = b^n b^{n-2} = 0\#$.

Un anillo A es un **dominio** si no tiene divisores de cero no nulos, si y sólo si todo elemento no nulo es cancelable, y es un **cuerpo** si todo elemento no nulo es unidad.

Todo cuerpo es dominio y todo dominio es reducido. Los recíprocos no se cumplen, pues $\mathbb{Z}$ es un dominio que no es un cuerpo y $\mathbb{Z}_6$ es un anillo reducido que no es un dominio.

Todo subanillo de un dominio es dominio, y todo subanillo de un anillo reducido es reducido. No todo subanillo de un cuerpo es un cuerpo, pues $\mathbb{Z}$ es subanillo del cuerpo $\mathbb{Q}$ pero no es un cuerpo.

> Todo dominio con un número finito de ideales es un cuerpo, y en particular lo es todo dominio finito.

Dados un dominio D y $a, b \in D$, a **divide a** b, a es **divisor** de b o b es **múltiplo** de a, $a \mid b$, si existe $c \in D$ con $ac = b$. Esta relación es reflexiva y transitiva, y para $a, b, c, r, s \in D$, si $a \mid b$ y $a \mid c$, $a \mid rb + sc$. Dos elementos a y b son **asociados** si $a \mid b$ y $b \mid a$, si y sólo si existe $u \in D^*$ con $b = au$.

$\Longrightarrow$] Si $b = 0$, $a = 0$ y tomamos $u = 1$. En otro caso, sean $c, d \in D$ con $ac = b$ y $bd = a$, $b = ac = bdc$, luego $dc = 1$ y c es unidad.

$\Longleftarrow$] $a = bu^{-1}$.

GyA

Sean A un anillo [...] y $a \in A \setminus (A^* \cup \{0\})$, a es **irreducible** en A si $\forall b, c \in A, (a = bc \implies b \in A^* \vee c \in A^*)$, y es **primo** en A si $\forall b, c \in A, (a \mid bc \implies a \mid b \vee a \mid c)$.

Si A es un dominio, todo primo es irreducible.

Irreducible en un dominio no implica primo. [...]

Si A es un dominio, a es irreducible si y sólo si (a) es maximal entre los ideales principales no nulos de A, es decir, si $(a) \neq 0, A$ y $\forall b \in A, ((a) \subseteq (b) \neq A \implies (a) = (b))$. [...]

Dados un anillo conmutativo A y $S \subseteq A$, $a \in A$ es un **máximo común divisor** de S en A, $a = \text{mcd}S[= \gcd S]$, si divide a cada elemento de S y es múltiplo de cada elemento que cumple esto, y es un **mínimo común múltiplo** de S en A, $a = \text{mcm}S[= \text{lcm}S]$, si es múltiplo de cada elemento de S y divide a cada elemento que cumple esto. Para $a, b \in A$:

1. $a = \text{mcd}S$ si y solo si (a) es el menor ideal principal de A que contiene a S. En particular, si $(a) = (S)$, $a = \text{mcd}S$.

2. $a = \text{mcm}S$ si y sólo si (a) es el mayor ideal principal de A contenido en $\bigcap_{s \in S}(s)$. En particular, si $(a) = \bigcap_{s \in S}(s)$, $a = \text{mcm}S$.

3. Si $a = \text{mcd}S$, $b = \text{mcd}S$ si y sólo si a y b son asociados en A.

4. Si $a = \text{mcm}S$, $b = \text{mcm}S$ si y sólo si a y b son asociados en A.

5. Si a divide a todo elemento de S y $a \in (S)$, [...] $a = \text{mcd}S$. En tal caso llamamos **identidad de Bézout** a una expresión de la forma $a = a_1 s_1 + \cdots + a_n s_n$ con $a_1, \ldots, a_n \in A$ y $s_1, \ldots, s_n \in S$, que existe porque $a \in (S)$.

6. $\text{mcd}S = 1$ si y sólo si los únicos divisores comunes de los elementos de S son las unidades de A.

7. Si $1 \in (S)$, $\text{mcd}S = 1$.

[...] Dado un dominio D, una **factorización en producto de irreducibles** de $a \in D$ es una expresión de la forma $a = up_1 \cdots p_n$, donde u es una unidad de D y $p_1, \ldots, p_n$ son irreducibles en D. Dos factorizaciones en producto de irreducibles de $a \in D$, $a = up_1 \cdots p_m$ y $a = vq_1 \cdots q_n$, son **equivalentes** si $m = n$ y existe una permutación σ de $\mathbb{N}_n \coloneqq \{1, \ldots, n\}$ tal que para $k \in \mathbb{N}_n$, p_k y $q_{\sigma(k)}$ son asociados, en cuyo caso u y v también lo son.

D es un **dominio de factorización** (**DF**) si todo elemento no nulo de D admite una factorización en producto de irreducibles, y es un **dominio de factorización única** (**DFU** o **UFD**) si, además, todas las factorizaciones de un mismo elemento son equivalentes.

1. **Teorema Fundamental de la Aritmética:** $\mathbb{Z}$ es un DFU.

2. Dado $m \in \mathbb{Z}^+$, $\mathbb{Z}[\sqrt{m}]$ es un DF.

Un dominio D es un DFU si y sólo si todo elemento no nulo de D es producto de una unidad por primos, si y sólo si D es un dominio de factorización en el que todo elemento irreducible es primo.

Todo cuerpo es un DFU, pues no tiene elementos nulos no invertibles. También lo son los anillos de polinomios sobre un DFU.

Un **dominio de ideales principales** (DIP) es uno en el que todos los ideales son principales.

GyA

Si D es un DIP y $a \in D \setminus (D^* \cup \{0\})$, a es irreducible si y solo si (a) es un ideal maximal, si y solo si $\frac{D}{(a)}$ es un cuerpo, si y solo si a es primo, si y solo si (a) es un ideal primo, si y solo si $\frac{D}{(a)}$ es un dominio. [...] Todo DIP es un DFU.

GyA

A es un cuerpo si y sólo si los únicos ideales de A son 0 y A, si y sólo si todo homomorfismo de anillos $A \to B$ con $B \neq 0$ es inyectivo.

1.6. Aritmética modular

GyA

Dado $n \in \mathbb{Z}^+$, llamamos $\mathbb{Z}_n \coloneqq \frac{\mathbb{Z}}{n\mathbb{Z}} = \{0 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$.

Para $n \geq 2$:

1. $r \in \mathbb{Z}_n$ es unidad si y sólo si $\gcd\{r, n\} = 1$ en $\mathbb{Z}$.

   $\Longrightarrow$] Si fuera $d \coloneqq \gcd\{r, n\} > 1$, sean $r', n' \in \mathbb{Z}$ con $r = dr'$ y $n = dn'$, entonces $n' \not\equiv 0$ mód n pero $rn' = dr'n' = r'n \equiv 0$ mód n, con lo que r es divisor de cero.#

   $\Longleftarrow$] Una identidad de Bézout $ar + bn = 1$ se traduce en que $ar \equiv 1$ mód n.

2. $r \in \mathbb{Z}_n$ es nilpotente si y sólo si todos los divisores primos de n dividen a r.

   $\Longrightarrow$] Sean m con $r^m \equiv 0$ y p un divisor primo de n, como $n \mid r^m$, p divide a r^m y por tanto a r.

   $\Longleftarrow$] Sea $p_1^{k_1} \cdots p_s^{k_s}$ la descomposición prima de n, como $p_1 \cdots p_s \mid r$, llamando $m \coloneqq \text{máx}\{k_1, \dots, k_s\}$, $n \mid p_1^m \cdots p_s^m \mid r^m$.

3. $\mathbb{Z}_n$ es un cuerpo si y sólo si es un dominio, si y sólo si n es primo.

   1 $\Longrightarrow$ 2] Visto.

   2 $\Longrightarrow$ 3] Probamos el contrarrecíproco. Si existen $p, q \in \{2, \dots, n-1\}$ con $n = pq$, p es divisor de 0 en $\mathbb{Z}_n$.

   3 $\Longrightarrow$ 1] Para $r \in \mathbb{Z}_n \setminus \{0\}$, $\gcd\{r, n\} = 1$ en $\mathbb{Z}$ y por tanto r es unidad.

4. $\mathbb{Z}_n$ es reducido si y sólo si n es **libre de cuadrados**, es decir, si no tiene divisores cuadrados de primos.

   $\Longrightarrow$] Si no fuera libre de cuadrados, sea $n = p^2q$ para ciertos $p, q \in \mathbb{Z}$ con p primo, en $\mathbb{Z}_n$ $pq \neq 0$ pero $(pq)^2 = p^2q^2 = 0$.

   $\Longleftarrow$] La descomposición en primos de n es de la forma $p_1 \cdots p_s$ con los p_i distintos, y si $r \in \mathbb{Z}_n$ cumple $r^2 = 0$ entonces en $\mathbb{Z}$ cada p_i divide a r^2 y por tanto a r, luego $n \mid r$ y $r = 0$ en $\mathbb{Z}_n$.

1.7. Operaciones con ideales

Dados subconjuntos S_1 y S_2 de un anillo A, llamamos $S_1 + S_2 \coloneqq \{x + y\}_{x \in S_1, y \in S_2}$ y $S_1 \cdot S_2 \coloneqq \{xy\}_{x \in S_1, y \in S_2}$. Para $a \in A$, llamamos $a + S_2 \coloneqq \{a\} + S_2$ y $a \cdot S_2 \coloneqq \{a\} \cdot S_2$. Por ejemplo, para $I \trianglelefteq A$ y $a \in A$, $a + I$ es la clase de equivalencia de A en A/I.

Si $S_1, S_2 \subseteq A$, $(S_1)+(S_2) = (S_1 \cup S_2)$. Llamamos **ideal suma** de $I, J \trianglelefteq A$ a $I+J = (I \cup J)$.

> $I, J \trianglelefteq A$ tienen **suma directa** $K \trianglelefteq A$, $I \oplus J = K$, si $I + J = K$ e $I \cap J = 0$. $I \oplus J = A$ si y sólo si existe un idempotente $e \in A$ con $I = (e)$ y $J = (1 - e)$.

Dados $I, J \trianglelefteq A$, en general $I \cdot J$ no es un ideal. En efecto, sean $A \coloneqq \mathbb{Z}[X, Y]$ e $I \coloneqq (X, Y) \trianglelefteq A$, entonces $X^2, Y^2, XY \in I \cdot I$, y si $I \cdot I$ fuera un ideal sería $p \coloneqq X^2 + XY + Y^2 \in I \cdot I$ y por tanto habría $q = a_0X + b_0Y + \ldots, r = a_1X + b_1Y + \cdots \in I$ con $p = qr$, pero entonces $a_0a_1, b_0b_1, a_0b_1 + b_0a_1 = 1$, pero como los coeficientes son enteros las dos primeras ecuaciones implican $a_0 = a_1, b_0 = b_1 \in \{\pm 1\}$ y por tanto $a_0b_1 + b_0a_1 \in \{\pm 2\}\#$.

El **ideal producto** de $I, J \trianglelefteq A$ es

$$IJ \coloneqq (I \cdot J) = \{x_1y_1 + \cdots + x_ny_n\}_{x_i \in I, y_i \in J, \forall i} \subseteq I \cap J.$$

Llamamos $I^0 \coloneqq A$ y, para $n \in \mathbb{N}$, $I^{n+1} \coloneqq II^n$. $I \trianglelefteq A$ es **nilpotente** si existe $n \in \mathbb{N}$ tal que $I^n = 0$.

Si $S_1, S_2 \subseteq A$, $(S_1)(S_2) = (S_1 \cdot S_2)$, y en particular el producto de ideal principales es un ideal principal.

$\subseteq$] Usando combinaciones lineales, los elementos de $(S_1)(S_2)$ son sumas de elementos de la forma $a_ix_ib_jy_j$ con $a_i, b_j \in A$, $x_i \in S_1$ e $y_j \in S_2$, pero $x_iy_j \in S_1 \cdot S_2$ y por tanto $a_ib_jx_iy_j$ está en $(S_1 \cdot S_2)$, y la suma de elementos de este tipo también.

$\supseteq$] Los elementos de $(S_1 \cdot S_2)$ tienen forma $s = a_1x_1y_1 + \cdots + a_nx_ny_n$ con los $a_i \in A$, los $x_i \in S_1$ y los $y_i \in S_2$, pero $a_ix_i \in (S_1)$ e $y_i \in (S_2)$, luego cada $a_ix_iy_i \in (S_1)(S_2) = ((S_1) \cdot (S_2))$ y por tanto $s \in (S_1)(S_2)$.

> En un DIP, $(a)+(b) = (\gcd\{a, b\})$ y $(a) \cap (b) = (\operatorname{lcm}\{a, b\})$. Dados un dominio A, $a, b \in A$ e $I \trianglelefteq A$ no trivial, si $(a)I = (b)I$ entonces $(a) = (b)$. Esto no es cierto en general si se cambian (a) o (b) por ideales no principales.

Para $I, J \trianglelefteq A$, en general $IJ \neq I \cap J$, pues por ejemplo en $\mathbb{Z}$ es $(2) \cap (4) = (4)$ pero $(2)(4) = (8)$.

Un anillo A es **completamente idempotente** si todo $I \trianglelefteq A$ cumple $I = I^2$, si y sólo si para todo $I, J \trianglelefteq A$ es $I \cap J = IJ$.

1.8. Isomorfía

Dado un homomorfismo de anillos $f : A \to B$:

1. Si $J \trianglelefteq B$, la **contracción** de J es $f^{-1}(J) \trianglelefteq A$.

   Sea $\pi : B \to B/J$ la proyección canónica, $J = \ker \pi$, luego $f^{-1}(J) = f^{-1}(\pi^{-1}(0)) = \ker(\pi \circ f)$ es un ideal.

2. Si $I \trianglelefteq A$, $f(I) \trianglelefteq \mathrm{Im} f$, y llamamos **extensión** de I relativa a f a $(f(I))$.

   Sean $a \in A$ y $x, y \in I$, de modo que $f(a) \in \mathrm{Im} f$ y $f(x), f(y) \in f(I)$, $f(x) + f(y) = f(x + y) \in f(I)$ y $f(a)f(x) = f(ax) \in f(I)$.

3. En general $f(I)$ no es ideal de B.

   La inclusión $\iota : \mathbb{Z} \to \mathbb{Q}$ es un homomorfismo de anillos y $\mathbb{Z} \trianglelefteq \mathbb{Z}$, pero $\iota(\mathbb{Z}) = \mathbb{Z} \not\trianglelefteq \mathbb{Q}$.

Teorema de la correspondencia:

1. Dado un homomorfismo de anillos $f : A \to B$, la extensión es una biyección

   $$\{I \trianglelefteq A \mid \ker f \subseteq I\} \to \{J \trianglelefteq \mathrm{Im} f\},$$

   y su inversa es la contracción.

   Primero vemos que las imágenes están donde deben. Si $I \trianglelefteq A$, $f(I) \trianglelefteq \mathrm{Im} f$, y si $J \trianglelefteq \mathrm{Im} f$, $f^{-1}(J) \trianglelefteq A$ y, como $0 \in J$, $\ker f = f^{-1}(0) \subseteq f^{-1}(J)$. Veamos ahora que la extensión y la contracción son inversas una de la otra. Por teoría de conjuntos, para todo $J \subseteq \mathrm{Im} f$, $f(f^{-1}(J)) = J$, y para todo $I \subseteq A$, $I \subseteq f^{-1}(f(I))$, por lo que solo hay que ver que $f^{-1}(f(I)) \subseteq I$. Sea $x \in f^{-1}(f(I))$, $f(x) \in f(I)$, luego existe $y \in I$ con $f(x) = f(y)$, pero entonces $f(x - y) = 0$, $x - y \in \ker f \subseteq I$ y $x = y + (x - y) \in I$.

2. Si I es un ideal de A y $p : A \to A/I$ es la proyección canónica,

   $$\rho : \{J \trianglelefteq A \mid I \subseteq J\} \to \{K \trianglelefteq A/I\}$$

   dada por $\rho(J) \coloneqq J/I \coloneqq p(J) = \{x + I\}_{x \in J}$ es una biyección que conserva la inclusión de los elementos.

   Basta aplicar el punto anterior a p.

3. Sean $I, J \trianglelefteq A$ y $p : A \to A/I$ la proyección canónica, $p(J) = (J + I)/I$.

Dados $I, J, J' \trianglelefteq A$ con $I \subseteq J, J'$, $\frac{J}{I} + \frac{J'}{I} = \frac{J+J'}{I}$, $\frac{J}{I} \cap \frac{J'}{I} = \frac{J \cap J'}{I}$ y $\frac{J}{I}\frac{J'}{I} = \frac{JJ'}{I}$.

Hay tantos ideales de $\mathbb{Z}_n$ como divisores positivos de n. En efecto, como $\mathbb{Z}_n = \mathbb{Z}/(n)$, por el teorema anterior hay una biyección entre $\mathcal{L}(\mathbb{Z}_n)$ y $\{I \trianglelefteq \mathbb{Z} \mid (n) \subseteq I\}$, pero $\mathbb{Z}$ es un DIP, luego estos elementos se corresponden con los $m \in \mathbb{Z}$ con $(n) \subseteq (m)$, que son aquellos con $m \mid n$, y tomamos solo los m positivos ya que los negativos son sus asociados y $0 \nmid n$.

Teorema del factor: Sean $f : A \to B$ un homomorfismo de anillos, $I \trianglelefteq A$ y $p : A \to A/I$ la proyección canónica, existe un homomorfismo $\overline{f} : A/I \to B$ con $\overline{f} \circ p = f$ si y sólo si $I \subseteq \ker f$, en cuyo caso $\overline{f}$ es único y $\ker \overline{f} = \ker f/I$.

$\Longrightarrow$] Para $x \in I$, $f(x) = \overline{f}(p(x)) = \overline{f}(0) = 0$, luego $I \subseteq \ker f$.

$\Longleftarrow$] Sea $\overline{f} : A/I \to B$ con $\overline{f} \circ p = f$, para $a \in A$, $\overline{f}(a + I) = f(a)$, lo que prueba la unicidad. Para la existencia, si $a + I = b + I$, $f(b) = f(a + b - a) = f(a) + f(b - a) = f(a)$ porque $b - a \in I \subseteq \ker f$. Finalmente $x + I \in \ker \overline{f} \iff \overline{f}(x + I) = f(x) = 0 \iff x \in \ker f$.

Teoremas de isomorfía:

1. Para un homomorfismo de anillos $f : A \to B$, $A/\ker f \cong \mathrm{Im} f$.

   $B' \coloneqq \mathrm{Im} f$ es un subanillo de B, luego $f : A \to B'$ es un homomorfismo suprayectivo y, por el teorema del factor, existe $\overline{f} : A/\ker f \to B'$ con $\overline{f} \circ p = f$ y $\ker \overline{f} = \ker f/\ker f = 0$, que es pues inyectivo y es suprayectivo por serlo f, de modo que es un isomorfismo.

2. Sean $I \trianglelefteq A$ y S un subanillo de A, $I + S$ es un subanillo de A, $I \cap S \trianglelefteq S$, $I \trianglelefteq I + S$ y $S/(I \cap S) \cong (I + S)/I$.

   Es fácil comprobar que $I + S$ es subanillo de A y claramente $I \cap S \trianglelefteq S$ e $I \trianglelefteq I + S$. Sea ahora el homomorfismo $f : S \to (I + S)/I$ dado por $f(a) = a + I$, $f(a) = 0 \iff a \in I$, luego $\ker f = I \cap S$, e $\mathrm{Im} f = (I + S)/I$, pues un $(x + s) + I \in (I + S)/I$ arbitrario, con $x \in I$ y $s \in S$, es la imagen por f de s. Entonces, por el primer teorema de isomorfía, $S/(I \cap S) \cong (I + S)/I$.

3. Si $I, J \trianglelefteq A$ con $I \subseteq J$, $(A/I)/(J/I) \cong A/J$.

   Sea $p : A \to A/J$ la proyección canónica, como $I \subseteq J = \ker f$, el teorema del factor nos da un homomorfismo $\overline{p} : A/I \to A/J$ con $\ker \overline{p} = \ker p/I = J/I$, que es suprayectivo por serlo p, y el resultado se obtiene del primer teorema de isomorfía.

GyA

Un anillo A tiene **característica** $n \in \mathbb{Z}^{\geq 0}$ si n es el menor entero positivo con $n1_A = 0_A$, o 0 si no existe tal n. Sean A un anillo conmutativo, $f : \mathbb{Z} \to A$ el único homomorfismo de anillos ($f(n) = n1$) y $n \geq 0$, A tiene característica n si y sólo si $\ker f = n\mathbb{Z}$, si y sólo si el subanillo primo de A es isomorfo a $\mathbb{Z}_n$, si y sólo si A contiene un subanillo isomorfo a $\mathbb{Z}_n$. [...] La característica de un dominio no trivial es 0 o un número primo.

$I, J \trianglelefteq A$ son **comaximales** si $I + J = A$, si y sólo si $\exists a \in I, b \in J : a + b = 1$.

1. Si $I \trianglelefteq A$ es comaximal con $J_1, \ldots, J_n \trianglelefteq A$, lo es con $J_1 \cdots J_n$ y con $J_1 \cap \cdots \cap J_n$.

   Basta verlo para el producto, pues la intersección es más grande. Para $n \in \{0, 1\}$ es claro. Para $n = 2$, existen $a, a' \in I$, $b \in J_1$ y $b' \in J_2$ con $1 = a + b = a' + b'$, luego $1 = aa' + ab' + ba' + bb'$ con $bb' \in J_1 J_2$ y el resto de sumandos en I. Para $n > 2$ se hace inducción.

2. Si $I_1, \ldots, I_n \trianglelefteq A$ son comaximales dos a dos, $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$.

   Para $n \in \{0,1\}$ es claro. Para $n = 2$, sea $x \in I_1 \cap I_2$, como existen $a \in I_1$ y $b \in I_2$ con $a + b = 1$, $x = ax + bx$, pero $a \in I_1$ y $x \in I_2$ y por tanto $ax \in I_1 I_2$, y del mismo modo $bx \in I_1 I_2$, luego $I_1 \cap I_2 \subseteq I_1 I_2$ y ya sabíamos que $I_1 I_2 \subseteq I_1 \cap I_2$. Para $n > 2$, supuesto esto probado para n menor, por lo anterior $I_1 \cdots I_{n-1} = I_1 \cap \cdots \cap I_{n-1}$ es comaximal con I_n y basta usar el caso $n = 2$.

3. $I, J \trianglelefteq A$ son comaximales si y sólo si $\forall x, y \in A, (x + I) \cap (y + J) \neq \emptyset$, en cuyo caso para $n, m \in \mathbb{N}$, I^n y J^m son comaximales.

Teorema chino de los restos: Dados anillos $A, B_1, \ldots, B_n$ y homomorfismos $g_i : A \to B_i$ con $K_i \coloneqq \ker g_i$:

1. $\phi : A \to B_1 \times \cdots \times B_n$ dado por $\phi(x) \coloneqq (g_1(x), \ldots, g_n(x))$ es un homomorfismo con núcleo $K_1 \cap \cdots \cap K_n$.

2. Si los g_i son suprayectivos y los K_i son comaximales dos a dos, ϕ es suprayectivo, $\ker \phi = K_1 \cdots K_n$ y $A/(K_1 \cdots K_n) \cong B_1 \times \cdots \times B_n$.

   Para $n \in \{0,1\}$ es claro, por lo que suponemos $n \geq 2$. Al ser los K_i comaximales, K_1 es comaximal con $K_2 \cap \cdots \cap K_n$. Sean ahora $a \in K_1$ y $b \in K_2 \cap \cdots \cap K_n$ con $a + b = 1$, como $g_1(a) = 0$, $g_1(b) = g_1(a) + g_1(b) = g_1(a + b) = 1$, y para $j \in \{2, \ldots, n\}$, $g_j(b) = 0$. Sea ahora $x \in B_1$ arbitrario, por suprayectividad existe $u \in A$ con $g_1(u) = x$, con lo que $g_1(ub) = g_1(u)g_1(b) = x$ y, para $j \in \{2, \ldots, n\}$, $g_j(ub) = g_j(u)g_j(b) = 0$, de modo que $\phi(u) = (x, 0, \ldots, 0)$. Por simetría, para cada i y $x \in B_i$ existe u tal que $\phi(u) = (0, \ldots, 0, x, 0, \ldots, 0)$ con x en la i-ésima posición, y como todo elemento de $B_1 \times \cdots \times B_n$ es suma de elementos de esta forma, ϕ es suprayectiva. Entonces $\ker \phi = K_1 \cap \cdots \cap K_n = K_1 \cdots K_n$, y para la última afirmación basta aplicar el primer teorema de isomorfía.

1.9. Ideales maximales

$I \triangleleft A$ es **maximal** en A, $I \trianglelefteq_{\mathrm{m}} A$, si es maximal en el conjunto de ideales propios de A, si y sólo si A/I es un cuerpo. **Demostración:** Como $J \mapsto J/I$ conserva la inclusión, I es maximal si y sólo si lo es $I/I = 0$, si y sólo si A/I no es trivial y no tiene ideales propios no nulos (si tuviera alguno, contendría a 0 y 0 no sería maximal), si y sólo si es un cuerpo no trivial, pero sabemos que A/I es no trivial porque I es propio.

Llamamos **espectro maximal** de A, $\mathrm{MaxSpec}(A)$, al conjunto de ideales maximales de A. Para $I \trianglelefteq A$, la biyección $\{J \in \mathcal{L}(A) \mid I \subseteq J\} \to \mathcal{L}(A/I)$ del teorema de la correspondencia se restringe a una biyección $\{J \in \mathrm{MaxSpec}(A) \mid I \subseteq J\} \to \mathrm{MaxSpec}(A/I)$.

$I \trianglelefteq A$ es maximal en A si y sólo si $I + (X)$ lo es en $A[X]$, pero $I[X]$ nunca es maximal en $A[X]$.

Una **cadena** en un conjunto ordenado es un subconjunto que, con el mismo orden, es totalmente ordenado. Un conjunto ordenado es **inductivo** si toda cadena no vacía tiene cota superior. **Lema de Zorn:** Todo conjunto inductivo no vacío tiene un elemento maximal.

Si $I \lhd A$, existe un ideal maximal de A que contiene a I, y en particular todo anillo no trivial tiene al menos un elemento maximal. **Demostración:** Sea $\Omega \coloneqq \{J \lhd A \mid I \subseteq J\}$, $\Omega \neq \emptyset$ porque $I \in \Omega$. Considerándolo ordenado por inclusión, si $\mathcal{C}$ es una cadena no vacía en Ω, $\bigcup \mathcal{C}$ es una cota superior, pues si $x, y \in \bigcup \mathcal{C}$ y $a \in A$, sean $I, J \in \mathcal{C}$ tales que $x \in I$ e $y \in J$, entonces por ejemplo $I \subseteq J$, luego $x, y \in J \subseteq \bigcup \mathcal{C}$ y $x + y, ax, ay \in J \subseteq \bigcup \mathcal{C}$ para $a \in A$, de modo que $\bigcup \mathcal{C}$ es un ideal, contiene a I y no es propio porque ninguno de los elementos de $\mathcal{C}$ contiene a 1. Entonces, por el lema de Zorn, Ω tiene un elemento maximal J, que es un ideal propio que contiene a I y es maximal porque, para $J' \lhd A$ con $J \subseteq J'$, $J' \in \Omega$ y por tanto $J' = J$.

Llamamos **radical de Jacobson** de un anillo A a $\mathrm{Jac}(A) \coloneqq \bigcap \mathrm{MaxSpec}(A) = \{a \in A \mid 1 + (a) \subseteq A^*\}$. $\mathrm{Jac}(A)$ no contiene idempotentes no nulos.

Un anillo A tiene un único ideal maximal M si y sólo si $A \setminus A^*$ es un ideal, en cuyo caso $M = A \setminus A^*$, y entonces decimos que A, (A, M) o $(A, M, A/M)$ es un **anillo local**, y $1 + M$ es un subgrupo multiplicativo de A^*. $\mathbb{Z}_n$ es un anillo local si y sólo si n es potencia de primo.

Sean $p \in \mathbb{Z}^+$ primo y $\mathbb{Z}_{(p)}$ el subconjunto de $\mathbb{Q}$ de los racionales en cuya expresión como fracción irreducible el denominador no es múltiplo de p, entonces $(\mathbb{Z}_{(p)}, (\frac{p}{1}))$ es un subanillo local de $\mathbb{Q}$ con $\mathbb{Z}_{(p)}/(\frac{p}{1}) \cong \mathbb{Z}_p$, y es un DFU en el que p es el único irreducible salvo asociados.

Si $(A, (p))$ es un anillo local con $p \neq 0$ y $\bigcap_{n \in \mathbb{N}} (p)^n = 0$, cada $a \in A \setminus 0$ es de la forma up^n para ciertos $u \in A^*$ y $n \in \mathbb{N}$, y en particular A es un DIP con un único irreducible salvo asociados.

Dados anillos locales $A_1, \ldots, A_n$, los idempotentes de $A_1 \times \cdots \times A_n$ son las n-uplas $(e_1, \ldots, e_n)$ con cada $e_i \in \{0, 1\}$. Para $n \geq 2$ con factorización prima $p_1^{m_1} \cdots p_t^{m_t}$ (con los p_i distintos y los $t_i \geq 1$), $\mathbb{Z}_n$ tiene 2^t idempotentes dados por los sistemas de ecuaciones diofánticas

$$\begin{cases} e_I & \equiv 0 \mod \left(q \coloneqq \prod_{i \in I} p_i^{m_i}\right), \\ e_I & \equiv 1 \mod \left(r \coloneqq \prod_{i \notin I} p_i^{m_i}\right), \end{cases}$$

para $I \subseteq \{1, \ldots, t\}$. En concreto existen $s, t \in \mathbb{Z}$ con $x = 1 + qt = rs$, de modo que $rs - qt = 1$ y, como q y r son coprimos, se pueden obtener s y t con una identidad de Bézout. Para obtener una identidad de Bézout:

1. Se calcula el máximo común divisor por el algoritmo de Euclides, usando la recurrencia $r_0 \coloneqq q$, $r_1 \coloneqq r$, $r_{i+1} = r_{i-1} - q_i r_i$, con $q_i, r_{i+1} \in \mathbb{Z}$ y $0 \leq r_{i+1} < r_i$, hasta llegar a un $r_n = 1$.

2. Se va despejando hacia atrás, haciendo

$$\begin{aligned} 1 = r_n = r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2}) = \\ = -q_{n-1} r_{n-3} + (1 + q_{n-1} q_{n-2}) r_{n-2} = \cdots = r_0 t + r_1 s. \end{aligned}$$

1.10. Ideales primos

$I \lhd A$ es **primo**, $I \trianglelefteq_{\mathrm{p}} A$, si $\forall x, y \in A, (xy \in I \implies x \in I \vee y \in I)$, si y sólo si $\forall n \in \mathbb{N}^*, \forall x_1, \ldots, x_n \in A, (x_1 \cdots x_n \in I \implies \exists k : x_k \in I)$, si y sólo si A/I es un dominio, si y sólo si $\forall n \in \mathbb{N}^*, \forall J_1, \ldots, J_n \trianglelefteq A, (J_1 \cdots J_n \subseteq I \implies \exists k : J_k \subseteq I)$.

$1 \iff 2]$ Trivial.

$1 \iff 3]$ Para $x, y \in A$, $xy \in I \implies x \in I \vee y \in I$ si y sólo si, en A/I, $\overline{x}\,\overline{y} = \overline{xy} = 0 \implies \overline{x} = 0 \vee \overline{y} = 0$, y que esto se de para todo $\overline{x}, \overline{y} \in A/I$ equivale a que A/I sea un dominio.

$1 \implies 4]$ Si fuera cada $J_k \not\subseteq I$, sea $x_k \in J_k \setminus I$ para cada k, $x_1 \cdots x_n \in J_1 \cdots J_n \subseteq I$, pero si I es primo existe k con $x_j \in I\#$.

$4 \implies 1]$ Sean $a_1, a_2 \in A$ con $a_1 a_2 \in I$, $(a_1)(a_2) = (a_1 a_2) \subseteq I$, luego por hipótesis $(a_1) \subseteq J$ o $(a_2) \subseteq J$ y por tanto $a_1 \in J$ o $a_2 \in J$.

GyA

[Si A es un anillo y $a \in A$,] a es primo si y sólo si (a) es un ideal primo no nulo de A.

El **espectro primo** de A, $\operatorname{Spec}(A)$, es el conjunto de todos los ideales primos. $\operatorname{MaxSpec}(A) \subseteq \operatorname{Spec}(A)$, pues todo cuerpo es un dominio. Para $I \lhd A$, la biyección del teorema de la correspondencia se restringe a una biyección $\{J \in \operatorname{Spec}(A) \mid I \subseteq J\} \to \operatorname{Spec}(A/I)$. En efecto, para $J \in \mathcal{L}(A)$ con $I \subseteq J$, $(A/I)/(J/I) \cong A/J$ por el tercer teorema de isomorfía, con lo que J es primo si y sólo si A/J es un dominio, si y sólo si lo es $(A/I)/(J/I)$, si y sólo si J/I es primo en A/I.

En un anillo A:

1. Sean $I_1, \ldots, I_n \trianglelefteq A$ con intersección J prima, algún $I_k = J$.

   J está contenido en cada I_k y, como $I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n = J$, algún $I_k \subseteq J$.

2. Sean $I \trianglelefteq A$ y $J_1, \ldots, J_n \trianglelefteq_{\mathrm{p}} A$, si $I \subseteq J_1 \cup \cdots \cup J_n$, I está contenido en algún J_k.

   Para $n = 1$ es trivial. Si $n > 1$, suponemos esto probado para $n - 1$, y suponemos por reducción al absurdo que $I \not\subseteq J_k$ para todo k. Para cada i, como $I \subseteq J_k$ para $k \neq i$, $I \not\subseteq \bigcup_{k \neq i} J_k$ y existe $a_i \in I$ con $a_i \notin \bigcup_{k \neq i} J_k$, por lo que $a_i \in J_i$. Sea entonces $b_i \coloneqq \prod_{k \neq i} a_k$, $b_i \in I$ y $b_i \in \bigcap_{k \neq i} J_k$, pero $b_i \notin J_i$ porque es el producto de elementos fuera de J_i y J_i es primo. Entonces $b \coloneqq \sum_{k=1}^{n} b_k \in I = \bigcup_{k=1}^{n} J_k$ y debe haber un k con $b \in J_k$, pero de ser así, como $b_i \in J_k$ para $i \neq k$, sería $b - \sum_{i \neq k} b_i = b_k \in J_k\#$.

3. Si todo ideal principal de A es primo, A es un cuerpo.

4. Si $\forall x \in A, \exists k \geq 2 : x^k = x$ entonces $\operatorname{Spec}(A) = \operatorname{MaxSpec}(A)$.

5. $I \trianglelefteq A$ es primo si y sólo si lo es $I[X]$ en $A[X]$, si y sólo si lo es $I + (X)$ en $A[X]$.

Dados un homomorfismo $f : A \to B$ y $P \trianglelefteq_{\mathrm{p}} B$, $f^{-1}(P) \trianglelefteq_{\mathrm{p}} A$, y el recíproco se cumple si f es suprayectivo.

Dado un conjunto ordenado $(S, \leq)$, su **opuesto** es $(S, \leq)^{\mathrm{op}} \coloneqq (S, \geq)$. $(S, \leq)$ es **contra-inductivo** si su opuesto es inductivo, es decir, si toda subcadena no vacía tiene una cota inferior. **Lema de Zorn dual:** Todo conjunto contra-inductivo no vacío tiene al menos un elemento minimal.

Un **primo minimal** de A es un elemento minimal de $\operatorname{Spec}(A)$. Llamamos $\operatorname{MinSpec}(A)$ al conjunto de primos minimales de A. Para $I \trianglelefteq A$ y $Q \trianglelefteq_{\mathrm{p}} A$ con $I \subseteq Q$, Q contiene un **primo**

minimal sobre I, un minimal entre los ideales primos que contienen a I, y en particular todo $Q \trianglelefteq_{\mathrm{p}} A$ contiene un primo minimal. **Demostración:** Sea $\Omega \coloneqq \{P \trianglelefteq_{\mathrm{p}} A \mid I \subseteq P \subseteq Q\}$, $\Omega \neq \emptyset$ porque $Q \in \Omega$. Sea entonces $\mathcal{C}$ una cadena no vacía en Ω, $\bigcap \mathcal{C} \in \Omega$, pues es un ideal propio entre I y Q y, usando el contrarrecíproco de la definición de primo, si $x, y \notin \bigcap \mathcal{C}$, sean $J_1, J_2 \in \mathcal{C}$ con $x \notin J_1$ e $y \notin J_2$, si por ejemplo $J_1 \subseteq J_2$, $x, y \notin J_1$, luego $xy \notin J_1$ y por tanto $xy \notin \bigcap \mathcal{C}$. Entonces, por el lema de Zorn dual, Ω tiene un minimal J, que es un ideal primo de A entre I y Q, y si J' es un ideal primo de A que contiene a I con $J' \subseteq J$, entonces $J' \subseteq Q$ y $J' \in \Omega$, luego $J' = J$ y J es minimal sobre I.

1.11. Radicales

$I \trianglelefteq A$ es un **radical** de A, $I \trianglelefteq_{\mathrm{r}} A$, si $\forall x \in A, \forall n \in \mathbb{N}, (x^n \in I \implies x \in I)$, si y sólo si $\forall x \in A, (x^2 \in I \implies x \in I)$, si y sólo si A/I es reducido.

$1 \implies 2]$ Obvio.

$2 \implies 1]$ Sean $x \in A$ y $n \in \mathbb{N}$ con $x^n \in I$, si $n = 0$, $1 \in I$ y $x \in I$, y si $n = 1$ es obvio. En otro caso, si n es par, $x^{n/2} \in I$, y si es impar, $x^{n+1} = xx^n \in I$ y por tanto $x^{(n+1)/2} \in I$. En cualquier caso $x^k \in I$ para cierto k con $1 \leq k < n$, y repitiendo el proceso llegamos a que $x \in I$.

$1 \iff 3]$ $x^n \in I \implies x \in I$ es equivalente a que, en A/I, $\overline{x}^n = \overline{x^n} = 0 \implies \overline{x} = 0$.

Propiedades:

1. Todo ideal primo es radical.
2. La intersección de una familia de radicales es un radical.
3. Para $I \trianglelefteq A$, la biyección del teorema de la correspondencia se restringe a una entre los radicales de A que contienen a I y los radicales de A/I.

   Sea $J \trianglelefteq A$ con $I \subseteq J$, por el tercer teorema de isomorfía, $(A/I)/(J/I) \cong A/J$, luego J es un radical de A si y sólo si A/J es reducido, si y sólo si lo es $(A/I)/(J/I)$, si y sólo si J/I es un radical de A/I.

Un **subconjunto multiplicativo** de un anillo A es un $S \subseteq A$ cerrado para el producto y que contiene al 1.

Lema de Krull: Sean A un anillo, $S \subseteq A$ un subconjunto multiplicativo e $I \trianglelefteq A$ disjunto de S:

1. $\mathcal{L}_{I,S} \coloneqq \{J \trianglelefteq A \mid I \subseteq J, J \cap S = \emptyset\}$ es un conjunto inductivo no vacío.

   La unión de elementos de una cadena vacía de $\mathcal{L}_{I,S}$ está en $\mathcal{L}_{I,S}$.
2. Todo elemento maximal de $\mathcal{L}_{I,S}$ es un ideal primo de A.

   Sean J maximal de $\mathcal{L}_{I,S}$ y supongamos que existen $x, y \in A$ con $x, y \notin J$ pero $xy \in J$. Entonces $J \subsetneq (x) + J$, por lo que $(x) + J \notin \mathcal{L}_{I,S}$ y, como es un ideal que contiene a I, debe contener un elemento de S, $a_1 x + b_1 \in ((x) + J) \cap S$, donde $a_1 \in A$ y $b_1 \in J$, y análogamente existe $a_2 y + b_2 \in ((y) + J) \cap S$ con $a_2 \in A$ y $b_2 \in J$, pero entonces $s \coloneqq (a_1 x + b_1)(a_2 y + b_2) = a_1 a_2 xy + a_1 x b_2 + b_1 a_2 y + b_1 b_2 \in S$, pero como $xy, b_1, b_2 \in J$, $s \in J \cap S\#$.

Para $I \trianglelefteq A$, llamamos **radical** de I a

$$\sqrt{I} \coloneqq \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I\} = \bigcap\{J \trianglelefteq_{\mathrm{r}} A \mid I \subseteq J\} = \bigcap\{J \trianglelefteq_{\mathrm{p}} A \mid I \subseteq J\},$$

y en particular

$$\sqrt{0} = \mathrm{Nil}(A) = \bigcap\{J \trianglelefteq_{\mathrm{r}} A\} = \bigcap\{J \trianglelefteq_{\mathrm{p}} A\}.$$

$1 \subseteq 2]$ Sean $x \in A$, $n \in \mathbb{N}$ con $x^n \in I$ y $J \trianglelefteq_{\mathrm{r}} A$ con $I \subseteq J$, $x^n \in J$ y por tanto $x \in J$.

$2 \subseteq 3]$ Todo ideal primo es radical.

$3 \subseteq 1]$ Sea $x \in A$ tal que $\forall n \in \mathbb{N}, x^n \notin I$, y queremos ver que existe $P \trianglelefteq_{\mathrm{p}} A$ con $I \subseteq P$ y $x \notin P$. $S \coloneqq \{x^n\}_{n\in\mathbb{N}}$ es un subconjunto multiplicativo de A y por el lema de Krull existe un maximal P de $\mathcal{L}_{I,S}$ que es primo, de modo que $P \trianglelefteq_{\mathrm{p}} A$, $I \subseteq P$ y $x \notin P$ porque $x \in S$.

Así:

1. $I \subseteq \sqrt{I}$.
2. I es radical si y sólo si $I = \sqrt{I}$.
3. Si $I \trianglelefteq A$ y $J \trianglelefteq_{\mathrm{r}} A$ con $I \subseteq J$, entonces $\sqrt{I} \subseteq J$.
4. $I \triangleleft A$ es un radical si y sólo si es intersección de ideales primos.

$I \trianglelefteq A$ es **nil** si está contenido en $\mathrm{Nil}(A)$, y en tal caso:

1. $\forall a \in A, (a + I \in (A/I)^* \implies a \in A^*)$.
2. Si A/I no tiene idempotentes distintos de $\overline{0}$ y $\overline{1}$, tampoco los tiene A.
3. Si I es maximal, A es un anillo local.

Todo ideal nil finitamente generado es nilpotente.

Capítulo 2

Anillos noetherianos

2.1. Retículos

Un conjunto ordenado $(A, \leq)$ cumple la **condición de cadena ascendente** (**ACC**, *Ascending Chain Condition*) si para $\{a_n\}_n \subseteq A$ con cada $a_n \leq a_{n+1}$ existe $n_0 \in \mathbb{N}$ tal que para $n \geq n_0$ es $a_n = a_{n_0}$, si y sólo si todo $S \subseteq A$ no vacío tiene un elemento maximal.

$\Longrightarrow$] Probamos el contrarrecíproco. Si $S \subseteq A$ no tiene elementos maximales, sea $s_1 \in S$ arbitrario, como s_1 no es maximal, existe $s_2 \in S$ son $s_1 < s_2$, y por inducción se puede construir una secuencia $\{s_n\}_n \subseteq S \subseteq A$ con cada $s_n < s_{n+1}$ y A no cumple la ACC.

$\Longleftarrow$] Dada $\{a_n\}_n \subseteq A$ con cada $a_n \leq a_{n+1}$, como $\{a_n\}_n \neq \emptyset$, tiene un maximal a_{n_0}, y para $n \geq n_0$, $a_n \geq a_{n_0}$ y por tanto $a_n = a_{n_0}$.

$(A, \leq)$ cumple la **condición de cadena descendente** (**DCC**, *Descending Chain Condition*) si $(A, \geq)$ cumple la ACC, si y sólo si todo $S \subseteq A$ no vacío tiene un elemento minimal.

Un **retículo** es un conjunto parcialmente ordenado en que todo subconjunto de dos elementos tiene supremo e ínfimo, y es **completo** si todo subconjunto tiene supremo e ínfimo. $(\mathcal{L}, \leq)$ es un retículo completo si y sólo si lo es $(\mathcal{L}, \geq)$.

Sea $\mathcal{L}$ un retículo completo, para $S \subseteq \mathcal{L}$, llamamos $\bigvee S \coloneqq \sup_{\mathcal{L}} S$ y $\bigwedge S \coloneqq \inf_{\mathcal{L}} S$. Un $x \in \mathcal{L}$ es **compacto** si para $S \subseteq \mathcal{L}$ no vacío con $x = \bigvee S$ existe $F \subseteq S$ finito con $x = \bigvee F$, y es **cocompacto** si para $S \subseteq \mathcal{L}$ no vacío con $x = \bigwedge S$ existe $F \subseteq S$ finito con $x = \bigwedge F$.

Un retículo completo $(\mathcal{L}, \leq)$ cumple la ACC si y sólo si todo $x \in \mathcal{L}$ es compacto.

$\Longrightarrow$] Sean $x \in \mathcal{L}$ y $S \subseteq \mathcal{L}$ no vacío con $x = \bigvee S$, $\Sigma \coloneqq \{\bigvee F\}_{F \subseteq S \text{ finito no vacío}}$ tiene un elemento maximal $\bigvee F$ con $F \subseteq S$ finito, y queremos ver que $x = \bigvee F$. Sean $t \in S$ arbitrario y $F' \coloneqq F' \cup \{t\}$, entonces $\bigvee F \leq \bigvee F'$, pero como $\bigvee F' \in \Sigma$ y $\bigvee F$ es maximal, $\bigvee F = \bigvee F'$, de modo que $t \leq \bigvee F$. Como $t \in S$ es arbitrario, $\bigvee S \leq \bigvee F$ y por tanto $x = \bigvee S = \bigvee F$.

$\Longleftarrow$] Sean $\{s_n\}_n \subseteq \mathcal{L}$ con cada $s_n \leq s_{n+1}$ y $x \coloneqq \bigvee_n s_n$, como x es compacto, $x = \bigvee_{k=1}^{r} s_{n_k}$ para ciertos $n_1 < \cdots < n_r$, luego $x = s_{n_r}$ y, para $n \geq n_r$, $s_{n_r} \leq s_n$ y por tanto, como s_{n_r} es maximal, $s_{n_r} = s_n$.

Análogamente, $(\mathcal{L}, \leq)$ cumple la DCC si y sólo si todo $x \in \mathcal{L}$ es cocompacto.

2.2. Retículos de ideales

Dado un anillo A, $(\mathcal{L}(A), \subseteq)$ es un retículo completo con supremo $\bigvee S = \sum S = (\bigcup S)$ e ínfimo $\bigwedge S = \bigcap S$. $I \trianglelefteq A$ es compacto en $(\mathcal{L}(A), \subseteq)$ si y sólo si es finitamente generado.

$\Longrightarrow$] $I = \bigvee_{x \in I}(x)$, por lo que existen $x_1, \ldots, x_n \in I$ tales que $I = \bigvee_{i=1}^{n}(x_i) = (\{x_i\}_{i=1}^{n})$.

$\Longleftarrow$] Sean $I =: (x_1, \ldots, x_n)$ y $S \subseteq \mathcal{L}(A)$ no vacío con $I = \bigvee S$, para cada i, como $x_i \in I$, existen $J_{i1}, \ldots, J_{ik_i} \in S$ y $a_{i1} \in J_{i1}, \ldots, a_{ik_i} \in J_{ik_i}$ con $x_i = a_{i1} + \cdots + a_{ik_i}$, de modo que todo elemento de I se puede expresar como combinación lineal de los a_{ij} y por tanto $I = \bigvee_{ij} J_{ij}$.

Un anillo A es **noetheriano** si $\mathcal{L}(A)$ cumple la ACC, si y sólo si todos sus ideales son finitamente generados, y es **artiniano** si cumple la DCC. Ejemplos:

1. Si un anillo es noetheriano o artiniano, también lo es cualquier anillo cociente suyo.

   El teorema de la correspondencia establece una biyección entre los ideales de A/I y los de A que contienen a I que conserva la inclusión y por tanto las condiciones ACC y DCC.

2. Los anillos con una cantidad finita de ideales son noetherianos y artinianos, y en particular lo son los cuerpos.

3. Los DIPs son noetherianos.

   Todos sus ideales son finitamente generados.

4. Un anillo con un elemento cancelable y no invertible no es artiniano.

   Sean A el anillo y $x \in A$ el elemento, $(x) \supsetneq (x^2) \supsetneq \cdots \supsetneq (x^k) \supsetneq \ldots$.

5. Los dominios que no son cuerpos no son artinianos, y en particular los DIPs que no son cuerpos son noetherianos pero no artinianos.

   Por ser dominios todos los elementos no nulos son cancelables, y por no ser cuerpo hay un elemento no nulo no invertible.

6. Los anillos de polinomios no son artinianos.

   X es cancelable y no invertible.

7. Dado un anillo A no trivial, $A^{\mathbb{N}}$ y $A[X_1, X_2, \ldots]$ no son noetherianos ni artinianos.

   Para $A^{\mathbb{N}}$, los $I_n \coloneqq \{a \mid \forall k > n, a_k = 0\}$ cumplen $I_1 \subsetneq I_2 \subsetneq \ldots$ y los $J_n \coloneqq \{a \mid \forall k < n, a_k = 0\}$ cumplen $J_1 \supsetneq J_2 \supsetneq \ldots$. Para $A[X_1, X_2, \ldots]$ esto ocurre con los $I_n \coloneqq (X_1, \ldots, X_n)$ y los $J_n \coloneqq (X_n, X_{n+1}, \ldots)$.

8. Si un anillo es un K-espacio vectorial de dimensión finita en que todos los ideales son subespacios vectoriales entonces es noetheriano y artiniano.

   Si la dimensión es $d \in \mathbb{N}$, una cadena estricta de ideales tiene a lo sumo $d+1$ elementos.

9. Para todo cuerpo K, $\frac{K[X]}{(X^n)}$ es noetheriano y artiniano.

   Es un K-espacio vectorial con base $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$.

10. Que un anillo sea noetheriano o artiniano no implica que sus subanillos lo sean.

    $K[X_1, X_2, \ldots]$ no es noetheriano ni artiniano pero es subanillo de su cuerpo de fracciones.

2.3. Anillos noetherianos

Si A es noetheriano, todo $X \subseteq A$ admite un $X_0 \subseteq X$ finito con $(X_0) = (X)$, pues $(X) = (b_1, \ldots, b_m)$ con cada $b_i = \sum_{j=1}^{k_j} a_{ij} x_{ij}$ para ciertos $a_{ij} \in A$ y $x_{ij} \in X$ y por tanto $(X) = (x_{11}, \ldots, x_{1j_1}, \ldots, x_{m1}, \ldots, x_{mk_m})$.

Todo dominio noetheriano es un dominio de factorización. **Demostración:** Supongamos que D es noetheriano pero no es un DF, de modo que el conjunto S de elementos no nulos de D que no se factorizan, es decir, que no están en $\{up_1 \cdots p_n\}_{u \in D^*}^{p_1, \ldots, p_n \in D \text{ irreducibles}}$, no es vacío. Entonces $\Omega \coloneqq \{(a)\}_{a \in S}$ tiene un maximal (a) con $a \in S$, y como a no es nulo, invertible ni irreducible, existen $b, c \in D$ no asociados de a con $a = bc$. Entonces $(b), (c) \supsetneq (a)$ y por tanto no están en Ω, luego $b, c \notin S$, y claramente $b, c \neq 0$, de modo que b y c se factorizan y por tanto también lo hace $a\#$.

Si A es noetheriano, todo ideal contiene un producto finito de ideales primos, y en particular 0 es un producto finito de ideales primos. **Demostración:** De no ser así, el conjunto Ω de ideales que no contienen un producto finito de primos es no vacío y tiene un maximal $I \in \Omega$. Como I no es primo, existen $a, b \notin I$ con $ab \in I$, luego $I + (a), I + (b) \supsetneq I$ e $I + (a), I + (b) \notin \Omega$, con lo que existen $P_i \trianglelefteq_{\mathrm{p}} A$ y $Q_j \trianglelefteq_{\mathrm{p}} A$ con $P' \coloneqq \prod_i P_i \subseteq I + (a)$ y $Q' \coloneqq \prod_i Q_i \subseteq I + (b)$. Ahora bien, los elementos de $P'Q'$ son suma de elementos pq con $p \in P' \subseteq I + (a)$ y $q \in Q' \subseteq I + (b)$, de modo que existen $x, y \in I$ y $s, t \in A$ con $p = x + sa$ y $b = y + tb$, y entonces $pq = (x + sa)(y + tb) = xy + (tb)x + (sa)y + (st)(ab) \in I$, ya que $ab \in I$, y por tanto $P'Q' \subseteq I\#$.

Si A es noetheriano:

1. Todo ideal suyo contiene una potencia de su radical.
2. Si $b \in A$ es cancelable y no unidad, $\bigcap_{n \in \mathbb{N}} (b^n)$ puede ser no trivial, pero no contiene elementos cancelables.
3. A tiene una cantidad finita de primos minimales.

Teorema de la base de Hilbert: Un anillo A es noetheriano si y sólo si lo es $A[X]$, si y sólo si lo es cualquiera de los $A[X_1, \ldots, X_n]$.

$1 \implies 2]$ Probamos el contrarrecíproco. Sea $I \trianglelefteq A[X]$ no finitamente generado, por inducción y usando el buen orden de $\mathbb{N}$ definimos una secuencia $\{f_i\}_{i=1}^{\infty} \subseteq I$ donde cada f_i es un elemento de $I \setminus (f_1, \ldots, f_{i-1})$ de grado mínimo. Llamando n_i al grado de f_i y b_i a su coeficiente principal, $(b_1) \subseteq (b_1, b_2) \subseteq (b_1, b_2, b_3) \subseteq \ldots$ es una cadena ascendente de ideales de A, y queda ver que los contenidos son estrictos. En efecto, si fuera $b_k \in (b_1, \ldots, b_{k-1})$, digamos $b_k = \sum_{i=1}^{k-1} a_i b_i$ para ciertos $a_i \in A$, como $n_1 \leq n_2 \leq \ldots$, podemos tomar $f_k - \sum_{i=1}^{k-1} a_i f_i X^{n_k - n_i}$, que está en $I \setminus (f_1, \ldots, f_{k-1})$ y tiene grado menor que $n_k\#$.

$2 \implies 1]$ $A \cong A[X]/(X)$ es noetheriano.

$1 \iff 3]$ Por inducción en $[1 \iff 2]$.

Así, si K es un cuerpo, los anillos de la forma $K[X_1, \ldots, X_n]/I$ son noetherianos. Si A es un subanillo noetheriano de B y $b_1, \ldots, b_n \in B$, entonces $A[b_1, \ldots, b_n]$ es noetheriano, pues la evaluación $\epsilon_b : A[X_1, \ldots, X_n] \to A[b_1, \ldots, b_n]$ es un homomorfismo y por tanto $A[b_1, \ldots, b_n] \cong A[X_1, \ldots, X_n]/\ker \epsilon_b$. En particular los $\mathbb{Z}[\sqrt{m}]$ son noetherianos, aunque muchos no son DFUs.

Dados $I \trianglelefteq A$ y $S \subseteq A$, llamamos $(I : S) = \{a \in A \mid aS \subseteq I\}$. $I \subseteq (I : S)$, pues para $x \in I$, $xS \subseteq xA \subseteq I$.

Dados $I, J \trianglelefteq A$, $X, Y \subseteq A$, $\{K_\lambda\}_{\lambda\in\Lambda} \subseteq \mathcal{L}(A)$ y $\{Z_\lambda\}_{\lambda\in\Lambda} \subseteq \mathcal{P}(A)$:

1. $(I : X)$ es el mayor $L \trianglelefteq A$ con $LX \subseteq I$.
2. $I \subseteq J \implies (I : X) \subseteq (J : X)$.
3. $X \subseteq Y \implies (I : Y) \subseteq (I : X)$.
4. $(I : X) = (I : (X))$.
5. $(I : A) = I$.
6. $(I : 0) = A$.
7. $(A : X) = A$.
8. $((I : X) : Y) = (I : X \cdot Y)$.
9. $(I : \bigcup_\lambda Z_\lambda) = \bigcap_\lambda (I : Z_\lambda)$.
10. $(I : \sum_\lambda K_\lambda) = \bigcap_\lambda (I : K_\lambda)$.
11. $(\bigcap_\lambda K_\lambda : J) = \bigcap_\lambda (K_\lambda : J)$.

Si $X \neq \emptyset$, llamamos **anulador** de X en A a $\operatorname{ann}_A(X) \coloneqq (0 : X) = \{a \in A \mid aX = 0\}$, y entonces $\operatorname{ann}(X) = \operatorname{ann}((X))$, $\operatorname{ann}\left(\bigcup_\lambda Z_\lambda\right) = \bigcap_\lambda \operatorname{ann}(Z_\lambda)$ y $\operatorname{ann}\left(\sum_\lambda K_\lambda\right) = \bigcap_\lambda \operatorname{ann}(Z_\lambda)$.

Teorema de Cohen: Un anillo es noetheriano si y sólo si todos sus ideales primos son finitamente generados.

$\implies$] Obvio.

$\impliedby$] Probamos el contrarrecíproco. Sean A no noetheriano y Ω el conjunto de ideales de A no finitamente generados, la unión de una cadena de elementos de Ω está en Ω. En efecto, dada una cadena $\{I_\lambda\}_{\lambda\in\Lambda} \subseteq \Omega$, si fuera $\bigcup_\lambda I_\lambda =: (a_1, \ldots, a_n)$, por ser $\{I_\lambda\}_\lambda$ una cadena existe un $\mu \in \Lambda$ con $a_1, \ldots, a_n \in I_\mu$, luego $(a_1, \ldots, a_n) \subseteq I_\mu \subseteq (a_1, \ldots, a_n)$ e I_μ es finitamente generado.# Esto nos permite aplicar el lema de Zorn y obtener un elemento maximal P de Ω, y queda ver que P es primo. Supongamos que no lo fuera. $P \neq A$, pues $A = (1)$ es finitamente generado, luego existen $a, b \notin P$ con $ab \in P$. Entonces $P \subsetneq P + (a)$, luego $P + (a) \notin \Omega$ y existen $p_1, \ldots, p_n \in P$ y $r_1, \ldots, r_n \in A$ con $P + (a) = (p_1 + r_1 a, \ldots, p_n + r_n a) = (p_1, \ldots, p_n, a)$. Para la segunda igualdad:

$\subseteq$] Cada $p_i + r_i a \in (p_i, a) \subseteq (p_1, \ldots, p_n, a)$.

$\supseteq$] Claramente $a \in P + (a)$, y entonces cada $p_i = (p_i + r_i a) - r_i a \in P + (a)$.

$(P : (a)) = \{c \in A \mid c(a) = (ca) \subseteq P\} = \{c \in A \mid ac \in P\}$, y entonces $P \subsetneq (P : (a))$ ya que $ab \in P$ pero $b \notin P$. Por tanto $(P : (a)) = (q_1, \ldots, q_m)$ para ciertos $q_1, \ldots, q_m$ con cada $q_j a \in P$. Entonces $P = (p_1, \ldots, p_n, q_1 a, \ldots, q_m a)$:

$\subseteq]$ Para $x \in P$, $x \in P + (a) = (p_1, \ldots, p_n, a)$, luego $x = s_1p_1 + \cdots + s_np_n + ra$ para ciertos $s_j, r \in A$, y como $x \in P$ y los $p_i \in P$, $ra \in P$ y por tanto $ra \in (P : (a)) = (q_1, \ldots, q_m)$, con lo que $r = t_1q_1 + \cdots + t_mq_m$ para ciertos $t_j \in A$ y por tanto $x = s_1p_1 + \cdots + s_np_n + t_1q_1a + \cdots + t_mq_ma \in (p_1, \ldots, p_n, q_1a, \ldots, q_ma)$.

$\supseteq]$ Cada p_i y cada q_ja está en P.

Con esto P es finitamente generado.#

Como **teorema**, un anillo A es noetheriano si y sólo si lo es $A[\![X]\!]$, si y sólo si lo es cualquiera de los $A[\![X_1, \ldots, X_n]\!]$.

$1 \implies 2]$ Sea $P \trianglelefteq_{\mathrm{p}} A[\![X]\!]$ y queremos ver que P es finitamente generado. Como la evaluación en 0 $\epsilon : A[\![X]\!] \to A$ es suprayectiva, $\varepsilon(P)$ es un ideal de A y por tanto es finitamente generado, digamos $\varepsilon(P) = (b_1, \ldots, b_n)$ con cada $b_i = \varepsilon(f_i)$ para cierto $f_i \in P$. Si $X \in P$ entonces $P = (b_1, \ldots, b_n, X)$.

$\subseteq]$ Para $f \in P$, $f = gX + b$ para ciertos $g \in A[\![X]\!]$ y $b \in \varepsilon(P) = (b_1, \ldots, b_n)$.

$\supseteq]$ $X \in P$ y cada $b_i = f_i - g_iX$ para cierto $g_i \in A[\![X]\!]$, luego $b_i \in P$.

Si $X \notin P$ entonces $P = (f_1, \ldots, f_n)$.

$\subseteq]$ Sea $g \in P$, queremos ver que existen $(a_{ij})_{1 \le i \le n}^{j \in \mathbb{N}} \in A[\![X]\!]$ tales que, para $j \in \mathbb{N}$, existe $g' \in P$ con $f = a_{1j}f_1 + \cdots + a_{nj}f_n + g'X^j$, y a_{ij} y a_{kj} tienen los mismos coeficientes hasta el de grado $\min\{i, k\} - 1$. Para $j = 0$, tomamos los $a_{i0} = 0$ y $g' = g$. Para $j > 0$, probado esto para $j - 1$, $g = a_{1,k-1}f_1 + \cdots + a_{n,k-1}f_n + g'X^{j-1}$ con $g' \in P$, pero como $\epsilon(g') \in \epsilon(P)$, existen x_i con $\epsilon(g') =: \sum_{i=1}^n x_ib_i$, con lo que $h_0 \coloneqq g' - \sum_{i=1}^n x_if_i$ está en P y tiene término independiente 0, luego $h_0 = hX$ con $h \in P$ ya que $X \notin P$ y P es primo, y como $g' = hX + \sum_{i=1}^n x_if_i$, $g = (a_{1,j-1} + x_1X^{j-1})f_1 + \cdots + (a_{n,j-1} + x_nX^{j-1})f_n + hX^j$, y hacemos los $a_{ij} \coloneqq a_{i,j-1} + x_iX^{j-1}$. Con esto, para $i \in \{1, \ldots, n\}$ definimos $c_i \in A[\![X]\!]$ de modo que $c_{ik} \coloneqq a_{i,k+1,k}$, y entonces $g = \sum_{i=1}^n c_if_i$. En efecto, para el coeficiente de grado j,

$$\left(\sum_{i=1}^n c_if_i\right)_j = \sum_{i=1}^n \sum_{k=1}^j c_{ik}f_{i,j-k} = \sum_{i=1}^n \sum_{k=1}^j a_{i,k+1,k}f_{i,j-k} =$$

$$= \sum_{i=1}^n \sum_{k=1}^j a_{i,j+1,k}f_{i,j-k} = \sum_{i=1}^n (a_{i,j+1}f_i)_j = g_j.$$

$\supseteq]$ Todo $f_i \in P$.

$2 \implies 1]$ $A \cong A[\![X]\!]/(X)$, que es noetheriano.

$1 \iff 3]$ Por inducción en $[1 \iff 2]$.

2.4. Anillos artinianos

La **dimensión de Krull** de un anillo A es

$$\dim A \coloneqq \mathrm{Kdim} A \coloneqq \sup\{n \in \mathbb{N} \mid \exists P_0, \ldots, P_n \trianglelefteq_{\mathrm{p}} A \mid P_0 \subsetneq \cdots \subsetneq P_n\} \in \mathbb{N} \cup \{\infty\},$$

y se tiene $\mathrm{Spec} A = \mathrm{MaxSpec} A \iff \dim A = 0$.

$\Longrightarrow$] Si existen $P, Q \trianglelefteq_{\mathrm{p}} A$ con $P \subsetneq Q$, $P \in \mathrm{Spec} A \setminus \mathrm{MaxSpec} A$.

$\Longleftarrow$] Si existe $P \in \mathrm{Spec} A \setminus \mathrm{MaxSpec} A$, sabemos que P está contenido (estrictamente) en un maximal Q, que debe ser primo, luego $P \subsetneq Q$ y $\dim A \geq 1$.

Los DIPs que no son cuerpos tienen dimensión 1, pues el único primo que no es maximal es (0) y, para b cancelable no invertible, $(0) \subsetneq (b)$. Dado un anillo artiniano A:

1. $\dim A = 0$.

   Dado $P \trianglelefteq_{\mathrm{p}} A$, A/P es un dominio por ser P primo y es artiniano por serlo A, pero los dominios no cuerpos no son artinianos, luego A/P es un cuerpo y por tanto P es maximal y $\mathrm{Spec} A = \mathrm{MaxSpec} A$.

2. $\mathrm{Spec} A = \mathrm{MaxSpec} A$ es finito.

   $\Omega \coloneqq \{\bigcap \mathcal{M}\}_{\mathcal{M} \subseteq \mathrm{MaxSpec} A} \neq \emptyset$, pues $\emptyset \neq \mathrm{MaxSpec} A \subseteq \Omega$, con lo que tiene un minimal $I \coloneqq M_1 \cap \cdots \cap M_k \in \Omega$ con los $M_i \trianglelefteq_{\mathrm{m}} A$. Para $M \trianglelefteq_{\mathrm{m}} A$, $M \cap I = M \cap M_1 \cap \cdots \cap M_k \in \Omega$ y por tanto $M \cap I \subseteq I$, con lo que $I \subseteq M$, pero $M_1 \cdots M_k \subseteq M_1 \cap \cdots \cap M_k = I \subseteq M$ y, como M es primo, algún $M_i \subseteq M$, de modo que $M_i = M$ por ser M maximal y $\mathrm{MaxSpec}(A) = \{M_1, \ldots, M_k\}$.

3. $\mathrm{Jac}(A) = \mathrm{Nil}(A)$ es nilpotente.

   $J \coloneqq \mathrm{Jac}(A) = \bigcap \mathrm{MaxSpec}(A) = \bigcap \mathrm{Spec}(A) = \mathrm{Nil}(A)$. Como A es artiniano, la cadena $J \supseteq J^2 \supseteq J^3 \supseteq \ldots$ se estabiliza en un cierto $I = J^n$, y queremos ver que $I = 0$. Si no lo fuera, $\Omega \coloneqq \{K \trianglelefteq A \mid KI \neq 0\} \neq \emptyset$, pues $A \in \Omega$, con lo que tiene un minimal K. Como $KI \neq 0$, existe $x \in K$ con $xI = (x)I \neq 0$, luego $(x) \in \Omega$ y, como $(x) \subseteq K$, $K = (x)$. Ahora bien, $I^2 = J^{2n} = J^n = I$, luego $0 \neq xI = xI^2 = (xI)I$, con lo que $xI \in \Omega$ y está contenido en (x) y por tanto $xI = (x)$. En particular $x \in xI$, luego existe $y \in I$ con $x = xy$, y por inducción $x = xy^n$ para todo $n \in \mathbb{N}$, pues si $x = xy^{n-1}$ entonces $x = (xy)y^{n-1} = xy^n$. Ahora bien, $y \in I \subseteq J = \mathrm{Nil}(A)$, luego existe n con $y^n = 0$ y por tanto $x = xy^n = 0$, pero $xI \neq 0\#$.

4. 0 es producto finito de ideales maximales.

   $\mathrm{MaxSpec}(A)$ es finito, digamos $\mathrm{MaxSpec}(A) = \{M_1, \ldots, M_r\}$, y entonces $\mathrm{Jac}(A) = M_1 \cap \cdots \cap M_r = M_1 \cdots M_r$ por ser los M_i comaximales dos a dos, pero existe $n \in \mathbb{N}$ con $\mathrm{Jac}(A)^n = 0$, luego $0 = M_1^n \cdots M_r^n$.

Dado un anillo artiniano A, sean $\mathrm{Spec}(A) = \{M_1, \ldots, M_k\}$ y $n \in \mathbb{N}$ con $\mathrm{Jac}(A)^n = 0$, $A \cong \frac{A}{M_1^n} \times \cdots \times \frac{A}{M_k^n}$, con cada $\frac{A}{M_i^k}$ local y artiniano.

Capítulo 3

Módulos

Dado un anillo A, un **módulo** sobre A o **A-módulo** ${}_AM$ es una terna $(M, +, \cdot)$ donde $(M, +)$ es un grupo abeliano y $\cdot : A \times M \to M$ es una operación llamada **producto por escalares** tal que para $a, b \in A$ y $m, n \in M$:

1. $1m = m$.
2. $(ab)m = a(bm)$.
3. $(a + b)m = am + bm$.
4. $a(m + n) = am + an$.

> Equivalentemente, el producto currificado es un homomorfismo de anillos $A \to \mathrm{End}(M)$, donde $\mathrm{End}(M)$ es el anillo de los endomorfismos del grupo abeliano M con la suma por componentes y la composición como producto.

Propiedades:

1. $0m = 0$.
   $1m = (1 + 0)m = 1m + 0m$.
2. $a0 = 0$.
   $a0 = a(0 + 0) = a0 + a0$.
3. $-(am) = (-a)m = a(-m)$.
   $am + (-a)m = (a - a)m = 0m = 0$, $am + a(-m) = a(m - m) = a0 = 0$.

Llamamos ${}_A\mathrm{Mod}$ a la clase de los módulos sobre A.

1. Dado un cuerpo K, la clase de espacios vectoriales sobre K es ${}_K\mathrm{Vect} =_K \mathrm{Mod}$.
2. La clase de grupos abelianos es $\mathrm{GrAb} =_{\mathbb{Z}} \mathrm{Mod}$.
   Un $\mathbb{Z}$-módulo es un grupo abeliano con un producto por escalares de $\mathbb{Z}$ y este producto debe cumplir $(a + 1)m = am + a$ y $(-a)m = a(-m)$, por lo que se puede definir de una y sólo una forma.

3. Llamamos **A-módulo regular** a ${}_AA$.

4. Llamamos **anulador** de ${}_AM$ en $X \subseteq A$ a $\operatorname{ann}_M(X) \coloneqq \{m \in M \mid Xm = 0\}$.

5. Si $\{M_i\}_{i\in I}$ es una familia de A-módulos, $\prod_{i\in I} M_i$ es un A-módulo con las operaciones componente a componente, y también lo es la **suma directa** (**externa**)

$$\bigoplus_{i\in I} M_i \coloneqq \left\{ x \in \prod_{i\in I} M_i \;\middle|\; \{i \in I \mid x_i \neq 0\} \text{ finito} \right\}.$$

6. Dados un conjunto I y un A-módulo M, llamamos $M^I \coloneqq \prod_{i\in I} M$ y $M^{(I)} \coloneqq \bigoplus_{i\in I} M$. Llamamos **$A$-módulo libre de rango** n a ${}_AA^n$, que si A es un cuerpo es el espacio vectorial A^n.

3.1. Submódulos

$N \subseteq_A M$ es un **submódulo** de ${}_AM$ o un **A-submódulo** de M, $N \leq_A M$, si es un subgrupo de M cerrado para el producto por escalares, si y sólo si $0 \in N$ y N es cerrado para **combinaciones A-lineales**, en cuyo caso N es un módulo.

$\Longrightarrow$] Obvio.

$\Longleftarrow$] Claramente es cerrado para la suma y el producto, y también para el opuesto porque si $n \in N$ entonces $-n = (-1)n \in N$.

Llamamos $\mathcal{L}({}_AM)$ al conjunto de A-submódulos de M ordenado por inclusión, que es un retículo en que el ínfimo es la intersección y el supremo es la suma, definida para $\mathcal{S} \subseteq \mathcal{L}({}_AM)$ como

$$\sum \mathcal{S} \coloneqq \left\{ \sum_{N\in F} a_N \;\middle|\; F \subseteq \mathcal{S} \text{ finito}, a_N \in N \right\}.$$

Ejemplos:

1. Dado un cuerpo K, un K-submódulo es un subespacio vectorial.

2. Un $\mathbb{Z}$-submódulo es un subgrupo abeliano.

3. Todo módulo ${}_AM$ tiene al menos los submódulos 0 y ${}_AM$, y puede no haber más.
   ${}_{\mathbb{Z}}\mathbb{Z}_2$ no tiene más.

4. Los submódulos del módulo regular son los ideales, $\mathcal{L}({}_AA) = \mathcal{L}(A)$.

5. Si A es subanillo de B, B es un A-módulo tomando como producto por escalares el producto en B. En general $\mathcal{L}({}_AB) \neq \mathcal{L}({}_BB)$. Por ejemplo, $\mathbb{Q}$ solo tiene dos $\mathbb{Q}$-submódulos (sus ideales) pero tiene muchos $\mathbb{Z}$-submódulos (sus subgrupos), y dados un anillo A y $n \in \mathbb{N}$, $\{f \in A[X] \mid \operatorname{gr} f \leq n\}$ es un submódulo de ${}_AA[X]$ pero no de ${}_{A[X]}A[X]$.

6. $\operatorname{ann}_M(X) \leq_A M$, y en particular $\operatorname{ann}_A(X) \trianglelefteq A$.

7. $\bigoplus_{i\in I} M_i \leq_A \prod_{i\in I} M_i$.

8. Para $I \trianglelefteq A$ y $X \subseteq_A M$, $IX \leq_A M$, y para $m \in M$, $Im = \{bm\}_{b\in I} \leq_A M$.

9. Para $S \subseteq A$ y $N \leq_A M$, $SN \leq_A M$, y para $a \in A$, $aN = \{an\}_{n\in N} \leq_A M$.

Si $N \leq_A M$, $M/N \coloneqq \{\overline{m} \coloneqq m + N\}_{m\in M}$ es un A-módulo con la suma y el producto heredados, el **módulo cociente** de M por N. **Demostración:** Para $m, m', n, n' \in M$ y $a \in A$ con $m - m', n - n' \in N$, $\overline{m} + \overline{n} = \overline{m + n} = \overline{m + n + (m' - m + n' - n)} = \overline{m' + n'} = \overline{m'} + \overline{n'}$ y $a\overline{m} = \overline{am} = \overline{am + a(m' - m)} = \overline{am'} = a\overline{m'}$, por lo que las operaciones están bien definidas, y es fácil ver que se cumplen los axiomas de A-módulo.

1. Dado un cuerpo K, el módulo cociente de ${}_KV$ por $U \leq_K V$ es el espacio vectorial cociente.

2. El módulo cociente de ${}_{\mathbb{Z}}G$ por $H \leq_{\mathbb{Z}} G$ es el grupo cociente.

3.2. Homomorfismos

Un **homomorfismo de A-módulos**, **A-homomorfismo** o **aplicación A-lineal** entre ${}_AM$ y ${}_AN$ es un homomorfismo de grupos abelianos $f : M \to N$ que conserva el producto por escalares, y llamamos $\mathrm{Hom}_A(M, N)$ al conjunto de los A-homomorfismos de M a N, que es un grupo abeliano con la suma. El **núcleo** de un A-homomorfismo f es $\ker f \coloneqq f^{-1}(0)$. Propiedades:

1. f es inyectivo si y sólo si $\ker f = 0$.

   $\implies]\ f(x) = 0 = f(0) \implies x = 0.$
   $\impliedby]\ f(a) = f(b) \implies f(a - b) = 0 \implies a - b = 0.$

2. Si $M' \leq_A M$, $f(M') \leq_A N$, y en particular $f(M) \leq_A N$.

   $f(M')$ contiene al $0 = f(0)$ y sus combinaciones A-lineales son la imagen de combinaciones A-lineales en M', que están en M'.

3. Si $N' \leq_A N$, $f^{-1}(N') \leq_A M$.

   $f^{-1}(N')$ contiene al $0 = f^{-1}(0)$, y si $a_1, \ldots, a_k \in A$ y $m_1, \ldots, m_k \in f^{-1}(N')$, $f(a_1m_1 + \cdots + a_km_k) = a_1f(m_1) + \cdots + a_kf(m_k) \in N'$.

4. La composición de A-homomorfismos es un A-homomorfismo.

Un homomorfismo es un **monomorfismo** si es inyectivo, un **epimorfismo** si es suprayectivo y un **isomorfismo** si es biyectivo. Se suele indicar un monomorfismo con una flecha «$\rightarrowtail$» y un epimorfismo con «$\twoheadrightarrow$».

Las proyecciones canónicas $M \twoheadrightarrow M/N$ son epimorfismos. Los inversos de isomorfismos son isomorfismos, y se dice que los módulos involucrados son **isomorfos**. En efecto, si $f : M \to N$ es un A-isomorfismo, $a \in A$ y $n, n' \in N$ con imágenes por f^{-1} $m, m' \in M$, $f(m+m') = f(m)+f(m') = n+n'$ y por tanto $f^{-1}(n+n') = m+m' = f^{-1}(n)+f^{-1}(n')$, y $f(am) = af(m) = an$ y por tanto $f^{-1}(an) = am = af^{-1}(n)$.

1. En un cuerpo K, un K-homomorfismo es una aplicación lineal.

2. Un $\mathbb{Z}$-homomorfismo es un homomorfismo de grupos.

3. $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_3) = 0$.

Que dos submódulos de ${}_AM$ sean isomorfos no significa que lo sean los módulos cociente de M entre ellos, ni al revés. Por ejemplo, si ${}_{\mathbb{Z}}M := \mathbb{Z}_3 \oplus \mathbb{Z}_9$, $K := \mathbb{Z}_3 \oplus 0$, $N := 0 \oplus \mathbb{Z}_9$ y $L = ((0,6))$, $K \cong L$ pero $\frac{M}{K} \ncong \frac{M}{L}$, y $\frac{M}{K+L} \cong \frac{M}{N}$ pero $K + L \ncong N$.

Si $\phi : M \to M'$ es un A-isomorfismo, para $N \leq_A M$, $\frac{M}{N} \cong \frac{M'}{\phi(N)}$.

3.3. Restricción de escalares

Dado un homomorfismo de anillos $f : A \to B$, cada B-módulo M es un A-módulo definiendo $am := f(a)m$, lo que se conoce como **restricción de escalares**. Entonces $\mathcal{L}({}_BM) \subseteq \mathcal{L}({}_AM)$ y $\mathrm{Hom}_B(M,N) \subseteq \mathrm{Hom}_A(M,N)$ y ambos son igualdades cuando f es suprayectivo. **Demostración:** Todo B-submódulo de M es un A-submódulo, y todo B-homomorfismo $h : M \to N$ es un A-homomorfismo ya que $h(a \cdot_{{}_AM} m) = h(f(a) \cdot_{{}_BM} m) = f(a) \cdot_{{}_BN} h(m) = a \cdot_{{}_AN} h(m)$. Si f es suprayectivo y $S \leq {}_AM$, para $b \in B$ y $s \in S$, existe $a \in A$ con $f(a) = b$ y $bs = f(a)s = as \in B$, y si $h : M \to N$ es un A-homomorfismo, es un homomorfismo de grupos abelianos y, para $b \in B$ y $m \in M$, sea $a \in A$ con $f(a) = b$, $h(bm) = h(am) = ah(m) = bh(m)$.

Ejemplos:

1. Si f es el único homomorfismo de anillos $\mathbb{Z} \to A$, la restricción de escalares de un A-módulo es el grupo abeliano subyacente, y la de un A-homomorfismo es el homomorfismo de los grupos abelianos.

2. Si $\iota : A \hookrightarrow B$ es una inclusión, restringir escalares es limitarse a los escalares de A.

3. $\mathrm{Hom}_{\mathbb{R}[X]}(\mathbb{R}[X], \mathbb{R}[X]) \subsetneq \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}[X], \mathbb{R}[X])$.

   La inclusión es por restricción de escalares con la inclusión, y la derivada es un $\mathbb{R}$-homomorfismo (lleva 0 a 0 y conserva sumas y producto por escalares de $\mathbb{R}$) pero no es un $\mathbb{R}[X]$-homomorfismo (no conserva producto por X).

4. Si $I \trianglelefteq A$, ${}_{A/I}\mathrm{Mod} \equiv \{M \in_A \mathrm{Mod} \mid IM = 0\}$ por la biyección

   $$(M, +, \cdot) \mapsto (M, +, (a, m) \mapsto \overline{a}m),$$

   $\mathcal{L}({}_{A/I}M) = \mathcal{L}({}_AM)$ y $\mathrm{Hom}_{A/I}(M,N) = \mathrm{Hom}_A(M,N)$. En particular los $\mathbb{Z}_n$-módulos son grupos abelianos M con $nM = 0$, y si p es primo, los $\mathbb{Z}_p$-espacios vectoriales son grupos abelianos con $pM = 0$.

   ${}_{A/I}M$ es un A-módulo por restricción de escalares en la proyección canónica $A \to A/I$ con $am = \overline{a}m$, $IM = \overline{0}M = 0$ y las igualdades se tienen porque la proyección canónica es suprayectiva. Si ${}_AM$ cumple $IM = 0$, el producto $\overline{a}m := am$ está bien definido y convierte a M en un (A/I)-módulo. Estos procesos son uno inverso del otro.

5. Si K es un cuerpo, ${}_{K[X]}\mathrm{Mod} \equiv \prod_{V \in_K \mathrm{Vect}} \mathrm{End}_K(V)$ por la biyección

   $$(V, +, \cdot) \mapsto ((V, +, \cdot), v \mapsto Xv),$$

   y los $K[X]$-submódulos de V son sus K-subespacios vectoriales f**-invariantes** siendo $f(v) := vX$, es decir, los $W \leq V$ con $f(W) \subseteq W$. Decimos que V tiene **estructura de**

$K[X]$**-módulo asociada al endomorfismo** f, y para $p \in K[X]$, llamamos $p(f) : V \to V$ a $p(f)(v) \coloneqq \sum_i p_i f^i(v)$.

Si V es un $K[X]$-módulo, f es un $K[X]$-endomorfismo, y por restricción de escalares V es un K-módulo o K-espacio vectorial y f un $\mathbb{K}$-endomorfismo (vectorial). Y si V es un K-espacio vectorial y f un K-endomorfismo, el producto $K[X] \times V \to V$ dado por $\left(\sum_i r_i X^i\right) v \coloneqq \sum_i r_i f^i(v)$ hereda las propiedades del producto escalar (identidad en el anillo, asociatividad y distributividad por ambos lados). Todas son obvias salvo la asociatividad, pero

$$\left(\sum_i q_i X^i\right)\left(\left(\sum_i r_i X^i\right) v\right) = \left(\sum_i q_i X^i\right)\left(\sum_i r_i f^i(v)\right) =$$

$$= \sum_i q_i f^i \left(\sum_j r_j f^j(v)\right) = \sum_i \sum_j q_i r_j f^{i+j}(v) = \sum_i \sum_{k=0}^{i} q_k r_{i-k} f^i(v) =$$

$$= \left(\sum_i \sum_{k=0}^{i} q_k r_{i-k} X^i\right) v = \left(\left(\sum_i q_i X^i\right)\left(\sum_i r_i X^i\right)\right) v.$$

Finalmente, estas operaciones son inversas una de la otra, pues para $p \in K[X]$, $a \in K$ y $v \in V$, partiendo del $K[X]$-módulo, $\left(\sum_i r_i X^i\right) v = \sum_i r_i f^i(v) = \sum_i r_i X^i v = \left(\sum_i r_i X^i\right) v$ por asociatividad y distributividad del producto en el $K[X]$-módulo, y partiendo del K-espacio vectorial y endomorfismo, $a_{K[X]} v = a f^0(v) = a$ y $(v \mapsto Xv)(v) = Xv = f(v)$.

Sean V y W K-espacios vectoriales y $f : V \to V$ y $g : V \to V$ K-endomorfismos, un $K[X]$-homomorfismo entre los $K[X]$-módulos asociados a (V, f) y (W, g) es precisamente una aplicación K-lineal $\phi : V \to W$ con $\phi \circ f = g \circ \phi$.

3.4. Teoremas de isomorfía

Teorema de la correspondencia: Si $N \leq_A M$ y $p : M \to M/N$ es la proyección canónica,

$$\rho : \{K \leq_A M \mid N \subseteq K\} \to \{L \leq_A M/N\}$$

dada por $\rho(K) \coloneqq K/N \coloneqq p(K) = \{k + N\}_{k \in K}$ es una biyección que conserva la inclusión, y

$$p(K) = \frac{K + N}{N}.$$

Demostración: Que conserve la inclusión es claro, y que $p(K) = p(K + N)$ también. Si $K \leq_A M$ con $N \subseteq K$, para $a \in A$ y $k, l \in K$, $\overline{0}, \overline{k} + \overline{l} = \overline{k + l}, \overline{a}\overline{k} = \overline{ak} \in K/N$, luego $K/N \leq_A M/N$, y si $L \leq_A M/N$, para $n \in N$, $p(n) = \overline{n} = \overline{0} \in L$, con lo que $N \subseteq p^{-1}(L)$, y para $a \in A$ y $k, l \in p^{-1}(L)$, $\overline{k}, \overline{l} \in L$ y $\overline{ak} = a\overline{k}, \overline{k + l} = \overline{k} + \overline{l} \in L$, con lo que $ak, k + l \in p^{-1}(L)$. Queda ver que ρ y $L \to p^{-1}(L)$ son inversas una de la otra. Por teoría de conjuntos, para $L \subseteq M/N$, $p(p^{-1}(L)) = \{p(k) \in M \mid k \in p^{-1}(L)\} = \{p(k) \in M \mid p(k) \in L\} = L$, y para $K \subseteq M$, $p^{-1}(p(K)) = \{k \in M \mid p(k) \in p(K)\} = \{k \in M \mid \exists k' \in K : p(k) = p(k')\} \supseteq K$, y

solo hay que ver que si $K \leq_A M$ $p^{-1}(p(K)) \subseteq K$. Pero si $k \in p^{-1}(p(K))$, existe $k' \in K$ con $p(k) = p(k')$, luego $p(k-k') = 0$ y $k - k' \in N \subseteq K$, de modo que $k = k' + (k - k') \in K$.

Teoremas de isomorfía:

1. Si $f : M \to N$ es un A-homomorfismo, $\frac{M}{\ker f} \cong \mathrm{Im} f$.

   $N' \coloneqq \mathrm{Im} f \leq_A N$, luego $f : N \to N'$ es un homomorfismo suprayectivo. Sea entonces $\overline{f} : M/\ker f \to \mathrm{Im} f$ dada por $\overline{f}(\overline{a}) \coloneqq f(a)$, que está bien definida porque para $k \in \ker f$ es $\overline{f}(\overline{a+k}) = f(a) + f(k) = f(a)$, $\overline{f}(\overline{a}) = f(a) = 0 \implies a \in \ker f \implies \overline{a} = 0$, luego $\overline{f}$ es inyectiva y suprayectiva y por tanto un A-isomorfismo.

2. Si $N, K \leq_A M$, $\frac{N}{N \cap K} \cong \frac{N+K}{K}$.

   Sea $p : M \to M/K$ la proyección canónica, $p(N) = \frac{N+K}{K}$, luego $f \coloneqq p|_N : N \to \frac{N+K}{K}$ es suprayectiva y $f(a) = 0 \iff f \in K$, con lo que $\ker f = N \cap K$ y el resultado se obtiene del primer teorema de isomorfía.

3. Si $N, K \leq_A M$ con $N \subseteq K$, $\frac{M/N}{K/N} \cong \frac{M}{K}$.

   Sea $p : M \to M/K$ la proyección canónica, como $N \subseteq K = \ker p$, $\overline{p} : \frac{M}{N} \to \frac{M}{K}$ dada por $\overline{p}(\overline{a}) \coloneqq p(a)$ está bien definida, es suprayectiva y su núcleo es $\frac{K}{N}$, y el resultado se obtiene del primer teorema de isomorfía.

Una **clase de isomorfía** es una clase de equivalencia por la relación «ser isomorfos». Para $I, J \trianglelefteq A$, si $\frac{A}{I} \cong \frac{A}{J}$ como A-módulos entonces $I = J$, pero esto no es válido si el isomorfismo es de anillos.

3.5. Sistemas generadores

Si $X \subseteq_A M$, llamamos **A-submódulo de M generado por X** a

$$(X) \coloneqq AX \coloneqq \text{mín}\{N \leq_A M \mid X \subseteq N\} = \{a_1x_1 + \cdots + a_nx_n\}_{a_i \in A, x_i \in X}.$$

$\subseteq]$ El conjunto de combinaciones A-lineales de elementos de X contiene a X y es un A-submódulo de M, por lo que contiene al mínimo de los A-submódulos que cumplen esto.

$\supseteq]$ Por definición todo A-submódulo de M que contiene a X contiene a sus combinaciones A-lineales, por lo que el conjunto de estas está en el ínfimo y es en sí un A-submódulo de M que contiene a X.

Claramente $(\emptyset) = 0$ y $(x_1, \ldots, x_n) = Ax_1 + \cdots + Ax_n$, y llamamos **submódulo cíclico** generado por $m \in_A M$ a $Am \coloneqq (m) \coloneqq (\{m\})$.

Un **conjunto** o **sistema generador** de ${}_AM$ es un $X \subseteq M$ con $(X) = M$, y $(M) = M$. ${}_AM$ es **finitamente generado** si admite un conjunto generador finito, y es **cíclico** si admite uno unipuntual.

1. El A-módulo regular es cíclico, ${}_AA = (1)$.

2. Un K-espacio vectorial es finitamente generado si y sólo si es de dimensión finita, y entonces los generadores minimales son bases y tienen todos el mismo número de elementos.

3. No siempre los generadores minimales finitos tienen igual número de elementos.

   $\mathbb{Z}_{\mathbb{Z}}$ tiene generadores minimales $\{1\}$ y $\{3,5\}$.

4. Si $\{X_i\}_{i\in I} \subseteq \mathcal{P}(M)$ y $M = \sum_i (X_i)$ entonces $M = (\bigcup X_i)$.

5. Si $f : M \twoheadrightarrow N$ es un epimorfismo y $M = (X)$, $N = (f(X))$, luego si M es finitamente generado también lo es N, y en particular los cocientes de módulos finitamente generados son finitamente generados.

6. En general los submódulos de módulos finitamente generados no son finitamente generados.

   $\mathcal{L}({}_AA) = \mathcal{L}(A)$, pero $A = (1)$ y puede contener ideales no finitamente generados.

7. $A[X]$ es un $A[X]$-módulo cíclico pero no es finitamente generado como A-módulo.

   Si $S \subseteq A[X]$ es finito, $X^{\text{máx}_{f\in S}\, \text{gr} f+1} \notin AS$ y $A[X] \neq AS$.

8. $\mathbb{Q}$ es cíclico como $\mathbb{Q}$-módulo pero no es finitamente generado como $\mathbb{Z}$-módulo.

   Si $S \subseteq \mathbb{Q}$ es finito y $p \in \mathbb{Z}$ es un primo que no divide a los denominadores de los elementos de S en forma irreducible, $\frac{1}{p} \notin \mathbb{Z}S$.

9. Si $N \leq_A M$ y $\frac{M}{N}$ son finitamente generados, M es finitamente generado.

10. Si $N, K \leq_A M$, $N \cap K =: (x_1, \ldots, x_r)$ y $N + K =: (n_1 + k_1, \ldots, n_s + k_s)$ con cada $n_j \in N$ y cada $k_j \in K$, $N = (x_1, \ldots, x_r, n_1, \ldots, n_s)$ y $K = (x_1, \ldots, x_r, k_1, \ldots, k_s)$.

11. Dado un entero $q \geq 2$, $\mathbb{Z}\left[\frac{1}{q}\right] = \left\{\frac{a}{q^n}\right\}_{a\in\mathbb{Z}, n\in\mathbb{N}} \leq_{\mathbb{Z}} \mathbb{Q}$ no es finitamente generado.

12. Los epimorfismos conservan los conjuntos generadores.

Lema de Nakayama: Dados ${}_AM$ y $J \leq A$ con $J \subseteq \text{Jac}A$:

1. Si M es finitamente generado y $JM = M$ entonces $M = 0$. Esto no se cumple si ${}_AM$ no es finitamente generado, pues por ejemplo $\mathbb{Q}$ visto como $\mathbb{Z}_{(p)}$-módulo cumple $\text{Jac}(\mathbb{Z}_p(\mathbb{Q})) = \mathbb{Q}$.

2. Si M es finitamente generado, el único $N \leq_A M$ con $M = JM + N$ es M.

3. Si (A, J, K) es un anillo local, $\frac{M}{JM}$ es anulado por J ($J \subseteq \text{ann}_A(\frac{M}{JM})$), luego es un K-espacio vectorial. Si además M es finitamente generado, $\frac{M}{JM}$ es de dimensión finita, y si ${}_K\frac{M}{JM} = (\overline{m_1}, \ldots, \overline{m_n})$ entonces ${}_AM = (m_1, \ldots, m_n)$.

3.6. Sumas directas

Sean $\{N_i\}_{i\in I} \subseteq \mathcal{L}({}_AM)$ y el homomorfismo de A-módulos $\phi : \bigoplus_{i\in I} N_i \to M$ dado por $\phi(m) \coloneqq \sum_i m_i$:

1. ϕ es suprayectiva si y sólo si $M = \sum_i N_i$.

2. ϕ es inyectiva si y sólo si los elementos de $\sum_i N_i$ tienen una expresión única como $\sum_i n_i$ con cada $n_i \in N_i$ casi todos nulos, si y sólo si $\forall i, N_i \cap \sum_{j\neq i} N_j = 0$, en cuyo caso $\sum_i N_i$ es la **suma directa interna** de $(N_i)_i$, escrita $\bigoplus_i N_i$, que es isomorfa con la suma directa externa.

   $1 \iff 2]$ Por definición de ϕ.

   $2 \implies 3]$ Si $n_i = \sum_{j\neq i} n_j$, por unicidad es $n_i = 0$.

   $3 \implies 1]$ Para $n \in \sum_i N_i$ con $\phi(n) = \sum_i n_i = 0$, para $i \in I$, $n_i = -\sum_{j\neq i} n_j = 0$, luego $n = 0$.

3. M es la suma directa interna de los N_i si y sólo si ϕ es un isomorfismo, si y sólo si cada elemento de M se escribe de forma única como $\sum_i m_i$ con cada $m_i \in M_i$ y casi todos nulos.

Si $N, N' \leq_A M$, $M = N \oplus N' \iff M = N + N' \wedge N \cap N' = 0$, y entonces:

1. La **proyección** $p : M \to N$ dada por $p(x + x') \coloneqq x$ para $x \in N$ y $x' \in N'$ es un homomorfismo suprayectivo con núcleo N'.

   La unicidad garantiza que está bien definida y el resto es trivial.

2. $N \cong \frac{M}{N'}$.

   Por el primer teorema de isomorfía en p.

3. M es finitamente generado si y sólo si lo son N y N'.

   $\implies]$ Por ser isomorfos a espacios cociente del módulo finitamente generado M.

   $\impliedby]$ La unión de un conjunto generador de N y uno de N' es uno de M.

Si $J \trianglelefteq A$ y ${}_AM = \bigoplus_{i\in I} M_i$:

1. Dado un A-isomorfismo $\phi : M \to N$, $N = \bigoplus_{i\in I} f(M_i)$.
2. $\operatorname{ann}_M(J) = \bigoplus_{i\in I} \operatorname{ann}_{M_i}(J)$.
3. $\operatorname{ann}_A(M) = \bigcap_{i\in I} \operatorname{ann}_A(M_i)$.
4. Si A es un DIP, I es finito y $\operatorname{ann}_A(M_i) = (b_i)$ para cada $i \in I$, entonces $\operatorname{ann}_A(M) = (\operatorname{lcm}_{i\in I} b_i)$.

$N \leq_A M$ es un **sumando directo** de M si existe $N' \leq_A M$ con $M = N \oplus N'$ llamado **complemento directo** de N en M, si y sólo si la inclusión $\iota : N \hookrightarrow M$ tiene un inverso por la izquierda, es decir, un A-homomorfismo $h : M \to N$ con $h \circ \iota = 1_N$, que deja fijos los puntos de N.

$\implies]$ La proyección $p : M \to N$ cumple $p \circ \iota = 1_N$.

$\impliedby]$ Sea $N' \coloneqq \ker h$, para $x \in N \cap N'$, $0 = h(x) = h(\iota(x)) = x$, y para $x \in M$, $x = h(x) + (x - h(x))$ con $h(x) \in N$ y $x - h(x) \in N' = \ker h$ ya que $h(x - \iota(h(x))) = h(x) - h(x) = 0$.

En general un submódulo de M no es isomorfo a un cociente de M ni al revés, pues el cociente $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ no es isomorfo a un ideal de $\mathbb{Z}$ y $\mathbb{Z} \leq_{\mathbb{Z}} \mathbb{Q}$ no es isomorfo a un cociente de $\mathbb{Q}$ ya que todo cociente de $\mathbb{Q}$ cumple que para cada x hay un y con $x = y + y$ ($y = \frac{x}{2}$) y esto no ocurre en $\mathbb{Z}$. Si $M = \bigoplus_{i\in I} M_i$, cada M_i es un sumando directo de M con complemento directo $\bigoplus_{j\in I\setminus\{i\}} M_i$.

${}_AM$ es **indescomponible** si sus únicos sumandos directos son 0 y M.

1. Todo subespacio de un espacio vectorial tiene complementos directos (no únicos).

   Si $V \leq_K V$ con K cuerpo, una base de W se completa a una de V y el subespacio generado por los vectores que se añaden es un complemento directo de W en V.

2. Dada una familia $\{M_i\}_{i\in I} \subseteq_A \text{Mod}$, podemos identificar cada M_i con el submódulo de $\prod_i M_i$ con entradas nulas en cada componente salvo la i y entonces la familia $(M_i)_i$ es independiente y su suma directa interna coincide con la suma directa externa.

3. Si $I \triangleleft A$ tiene un elemento cancelable (no invertible), I no es un sumando directo de ${}_AA$. En particular, si A es un dominio, ${}_AA$ es indescomponible.

   Si tuviera complemento directo J, este sería no nulo por ser I propio, luego si $b \in I$ es cancelable y $c \in J \setminus \{0\}$, $0 \neq bc \in I \cap J\#$.

4. Si $p_1, \ldots, p_r \in \mathbb{Z}$ son primos distintos, $n \coloneqq \prod_{i=1}^r p_i^{m_i}$ y $q_i \coloneqq \frac{n}{p_i^{m_i}}$, $\mathbb{Z}_n = \bigoplus_{i=1}^r q_i\mathbb{Z}_n$.

   Como $\gcd\{q_1, \ldots, q_r\} = 1$, hay una identidad de Bézout $\sum_i a_iq_i = 1$ y la suma de ideales es $\mathbb{Z}_n$. Para ver que es directa, si $q_i\overline{a_i} = \sum_{j\neq i} q_j\overline{a_j}$ entonces $q_ia_i = nb + \sum_{j\neq i} q_ja_j$ en $\mathbb{Z}$ para cierto b, y como $p_i^{m_i}$ divide a la parte derecha de la igualdad, debe dividir a la izquierda y $p_i^{m_i} \mid q_ia_i$, con lo que $n = \prod_j p_j^{m_j} \mid q_ia_i$, $q_i\overline{a_i} = 0$ y la suma es directa.

5. Un A-módulo cíclico $M \neq 0$ es indescomponible si y sólo si los únicos idempotentes de $\frac{A}{\text{ann}_A(M)}$ son $\overline{0}$ y $\overline{1}$.

6. Si $M \in \text{MaxSpec}(A)$ y $n \in \mathbb{N}^*$, el A-módulo $\frac{A}{M^n}$ es indescomponible.

7. Si A es un DIP y $a \in A \setminus (A^* \cup \{0\})$, $\frac{A}{(a)}$ es indescomponible si y sólo si a es asociado a p^t para ciertos $p \in A$ irreducible y $t \in \mathbb{N}^*$.

8. Si $e \in A$ es idempotente, eM es sumando directo de M.

9. Si $f : M \to M$ es un A-endomorfismo idempotente, $M = \ker f \oplus \text{Im}f$.

3.7. Módulos libres

Dados $X \coloneqq \{m_i\}_{i\in I} \subseteq_A M$, el homomorfismo $\phi : A^{(I)} \to M$ dado por $\phi(a) \coloneqq \sum_i a_im_i$ es suprayectivo si y sólo si $M = \sum_{i\in I} Am_i$, y es inyectivo si y sólo si cada elemento de (X) se expresa de forma única como $\sum_i a_im_i$ con los $a_i \in A$ casi todos nulos, si y sólo si los submódulos $(Am_i)_{i\in I}$ son independientes y para cada $i \in I$ y $a \in A \setminus \{0\}$ es $am_i \neq 0$, en cuyo caso $(m_i)_{i\in I}$ es **linealmente independiente**.

$1 \implies 2]$ Si $\sum_i a_im_i = \sum_i a'_im_i$ entonces $\phi(a) = \phi(a')$ y $a = a'$.

$2 \implies 3]$ La expresión de elementos de (X) como $\sum_i n_i$ con cada $n_i = a_i m_i \in Am_i$ es única, luego los Am_i son independientes, y si hubiera $a \in A \setminus \{0\}$ e $i \in I$ con $am_i = 0$ habría dos expresiones $\sum_i a_i m_i$ para el $0\#$.

$3 \implies 1]$ Si $\phi(a) = \sum_i a_i m_i = 0$, por lo primero cada $a_i m_i = 0$, y por lo segundo cada $a_i = 0$, luego $a = 0$.

Una familia $\{m_i\}_{i\in I} \subseteq_A M$ es una **base** de M si es linealmente independiente y genera M, si y sólo si $\phi : A^{(I)} \to M$ dado por $\phi(a) \coloneqq \sum_i m_i$ es biyectiva, si y sólo si para cada $m \in M$ existe una única elección de coeficientes $a_i \in A$ casi todos nulos, llamados **coordenadas** de m en la base, con $m = \sum_i a_i m_i$. Un módulo es **libre** si tiene una base.

1. El módulo 0 es libre con base vacía.
2. Los $A^{(I)}$ son libres con la **base canónica** $(e_i)_{i\in I}$, donde cada e_i tiene un 1 en la entrada i y un 0 en el resto.
3. Todo espacio vectorial es libre, y las bases coinciden con los conjuntos linealmente independientes maximales y los conjuntos generadores minimales.
4. ${}_A A[X]$ es libre con base $(X^n)_{n\in\mathbb{N}}$.
5. ${}_{\mathbb{Z}}\mathbb{Z}[\mathrm{i}]$ es libre con base $\{1, \mathrm{i}\}$.
6. ${}_{\mathbb{Z}}\mathbb{Q}$ no es libre.

   Para $\frac{a}{r}, \frac{b}{s} \in \mathbb{Q}$, $br\frac{a}{r} - as\frac{b}{s} = 0$, luego los conjuntos linealmente independientes son de un elemento, pero estos no generan $\mathbb{Q}$.
7. Si M es un grupo abeliano finito no nulo, ${}_{\mathbb{Z}}M$ no es libre.

   No puede ser isomorfo a un $\mathbb{Z}^{(I)}$.

8. Los epimorfismos conservan la independencia lineal.
9. Los isomorfismos conservan bases.
10. Un $M \leq_{\mathbb{Z}} \mathbb{Q}$ es libre si y sólo si es cíclico, si y solo si es finitamente generado.
11. Un anillo A es un cuerpo si y sólo si todo A-módulo es libre.

${}_A M$ es libre si y sólo si es isomorfo a $A^{(I)}$ para cierto I, en cuyo caso, si $A \neq 0$, todas las bases tienen cardinal $|I|$, llamado el **rango** de M o $\mathrm{rg}M$. **Demostración:** Si ${}_A M$ es libre con base $(m_i)_{i\in I}$, hay un isomorfismo $\phi : A^{(I)} \to M$, y recíprocamente, si hay tal isomorfismo, M tiene la base resultante de llevar la base canónica de $A^{(I)}$ a M por el isomorfismo. Si $A \neq 0$, existe $J \trianglelefteq_{\mathrm{m}} A$ y $JM \leq_A M$, luego si $\overline{M} \coloneqq \frac{M}{JM}$, los elementos de $J\overline{M}$ son sumas de elementos de la forma $j\overline{m} = jm + JM = JM$ con $j \in J$ y $m \in M$ y por tanto $J\overline{M} = 0$. Pero un A-módulo $\overline{M}$ con $J\overline{M} = 0$ es un $\frac{A}{J}$-módulo, luego $\overline{M}$ es un $\frac{A}{J}$-módulo y por tanto es un $\frac{A}{J}$-espacio vectorial. Sea entonces $(m_i)_{i\in I}$ una base de ${}_A M$, $\{\overline{m_i}\}_{i\in I} \subseteq \overline{M}$ es un conjunto generador, y es linealmente independiente. En efecto, si $\sum_i \overline{a_i m_i} = \overline{0}$ entonces $x \coloneqq \sum_i a_i m_i \in JM$, luego $x = \sum_{j=1}^n b_j x_j$ con cada $b_j \in J$ y cada $x_j \in M$ y, escribiendo cada x_j como

$\sum_i c_{ji}m_i$, $x = \sum_j \sum_i b_j c_{ji} m_i = \sum_i \left(\sum_j b_j c_{ji}\right) m_i$, y por la independencia lineal de los m_i, cada $a_i = \sum_j b_j c_{ji} \in J$ y por tanto $\overline{a_i} = \overline{0}$. Haciendo esta operación con dos bases distintas de M con el mismo J se obtienen dos bases distintas del espacio vectorial $J\overline{M}$ que deben tener el mismo cardinal.

Un A-módulo libre es finitamente generado si y sólo si tiene rango finito, es decir, si es isomorfo a un A^n.

$\Longrightarrow$] Sean $S \subseteq_A M$ un generador finito de M, $(b_i)_{i\in I}$ una base de M y $\phi : A^{(I)} \to M$ el isomorfismo asociado a la base, si $f(a) \coloneqq \{i \in I : (\phi^{-1}(a))_i \neq 0\}$ entonces $J \coloneqq \bigcup_{a\in S} f(a)$ es finito, pero necesariamente $J = I$.

$\Longleftarrow$] Obvio.

Todo módulo es cociente de un módulo libre de rango igual al cardinal de un generador del módulo, pues si X es un generador de M existe un epimorfismo $\phi : A^{(X)} \twoheadrightarrow M$ dado por $\phi(a) \coloneqq \sum_x a_x x$ y, por el primer teorema de isomorfía, $\frac{A^{(X)}}{\ker \phi} \cong M$. En particular todo módulo finitamente generado es cociente de un módulo libre de rango finito y todo A-módulo cíclico es cociente de ${}_AA$.

Si ${}_AL = L_1 \oplus \cdots \oplus L_t$ es una suma directa interna y cada L_i es libre con base finita X_i, L tiene como base la concatenación de las X_i y $\mathrm{rg}L = \mathrm{rg}L_1 + \cdots + \mathrm{rg}L_t$. **Demostración:** Para $t \leq 1$ es obvio, y para $t > 2$ se ve por inducción. Para $t = 2$, las uniones de conjuntos generadores generan el submódulo suma, y queda ver que si $\{n_1, \ldots, n_r\} \subseteq L_1$ y $\{k_1, \ldots, k_s\} \subseteq L_2$ son linealmente independientes, la unión, que es disjunta, es linealmente independiente. Pero si $(a \coloneqq a_1 n_1 + \cdots + a_r n_r) + (b \coloneqq b_1 k_1 + \cdots + b_s k_s) = 0$ para ciertos $a_i, b_j \in A$ entonces $a, b = 0$ por ser $a \in L_1$ y $b \in L_2$, luego cada $a_i, b_j = 0$.

Sean $(m_i)_{i\in I}$ una base de ${}_AM$ y $\{n_i\}_{i\in I} \subseteq_A N$, existe un único A-homomorfismo $f : M \to N$ con cada $f(m_i) = n_i$. **Demostración:** Existe un A-isomorfismo $\phi : A^{(I)} \to M$ con $\phi(e_i) = m_i$ para cada e_i de la base canónica y un A-homomorfismo $\psi : A^{(I)} \to N$ dado por $\psi(e_i) = n_i$, y $f \coloneqq \psi \circ \phi^{-1} : M \to N$ es un A-homomorfismo con cada $f(m_i) = n_i$. Para la unicidad, como $\{m_i\}_i$ es un conjunto generador, dos A-homomorfismos que actúen igual sobre sus elementos son iguales.

3.8. Condiciones de cadena en módulos

${}_AN \in \mathcal{L}({}_AM)$ es compacto si y sólo si es finitamente generado.

$\Longrightarrow$] $N = \bigvee_{n\in N}(n)$, por lo que existen $n_1, \ldots, n_k \in N$ con $N = (n_1) \vee \cdots \vee (n_k) = (n_1, \ldots, n_k)$.

$\Longleftarrow$] Sean $N =: (x_1, \ldots, x_n)$ y $S \subseteq \mathcal{L}({}_AN)$ no vacío con $N = \bigvee S$, para cada i, como $x_i \in N$, existen $L_{i1}, \ldots, L_{ik_i} \in S$ y $p_{i1} \in L_{i1}, \ldots, p_{ik_i} \in L_{ik_i}$ con $x_i = a_{i1} + \cdots + a_{ik_i}$, de modo que todo elemento de N se puede expresar como combinación lineal de los a_{ij} y por tanto $N = \bigvee_{ij} L_{ij}$.

${}_AN \in \mathcal{L}({}_AM)$ es **finitamente cogenerado** si es cocompacto.

${}_AM$ es **noetheriano** si $(\mathcal{L}({}_AM), \subseteq)$ cumple la ACC, si y sólo si todos sus submódulos son finitamente generados, y es **artiniano** si cumple la DCC, si y sólo si todos sus submódulos son finitamente cogenerados, con lo que un anillo A es noetheriano o artiniano cuando lo es ${}_AA$.

1. Un espacio vectorial es noetheriano si y sólo si es artiniano, si y sólo si es finitamente generado, si y sólo si es de dimensión finita.

   $1 \implies 3]$ Por definición.

   $3 \implies 4 \implies 1, 2]$ Por álgebra lineal.

   $2 \implies 4]$ Probamos el contrarrecíproco. Si $(v_n)_{n\in\mathbb{N}}$ es una familia de vectores linealmente independiente y llamamos $V_n \coloneqq \operatorname{span}\{v_m\}_{m\geq n}$, $V_1 \supsetneq V_2 \supsetneq V_3 \supsetneq \dots$ viola la DCC.

2. ${}_{\mathbb{Z}}\mathbb{Q}$ no es noetheriano ni artiniano.
   $\cdots \subsetneq (4) \subsetneq (2) \subsetneq (1) \subsetneq (\frac{1}{2}) \subsetneq (\frac{1}{4}) \subsetneq \dots$.

3. Si $f : A \to B$ es un homomorfismo de anillos y vemos a un ${}_BM$ como A-módulo por restricción de escalares sobre f, si ${}_AM$ es noetheriano o artiniano también lo es ${}_BM$. En particular si A es cuerpo y ${}_AM$ tiene dimensión finita, ${}_BM$ es noetheriano y artiniano.

   $\mathcal{L}({}_BM) \subseteq \mathcal{L}({}_AM)$, por lo que si en $\mathcal{L}({}_AM)$ no hay cadenas de cierta forma, en $\mathcal{L}({}_BM)$ tampoco.

4. En el grupo $\frac{\mathbb{Q}}{\mathbb{Z}}$, para $n \geq 2$,

$$\left(\overline{\frac{1}{n}}\right) = \left\{\overline{\frac{0}{n}}, \overline{\frac{1}{n}}, \dots, \overline{\frac{n-1}{n}}\right\} \cong \mathbb{Z}_n$$

   admite como generadores unitarios los $\overline{\frac{a}{n}}$ en que la fracción es irreducible. Si $p \in \mathbb{Z}$ es primo, $\mathbb{Z}_{p^\infty} \coloneqq \left\{\overline{\frac{a}{p^n}}\right\}_{a\in\mathbb{Z}, n\in\mathbb{N}}$ es un subgrupo de $\frac{\mathbb{Q}}{\mathbb{Z}}$ que es artiniano pero no noetheriano, y que no es finitamente generado pero todos sus subgrupos propios son cíclicos de la forma $\left(\overline{\frac{1}{p^n}}\right)$ con $n \in \mathbb{N}$.

   $\mathbb{Z}_{p^\infty}$ es la unión de la cadena de subgrupos

$$0 = \left(\overline{\frac{1}{p^0}}\right) \subsetneq \left(\overline{\frac{1}{p}}\right) \subsetneq \left(\overline{\frac{1}{p^2}}\right) \subsetneq \left(\overline{\frac{1}{p^3}}\right) \subsetneq \dots,$$

   por lo que no es noetheriano. Si ${}_{\mathbb{Z}}N \leq \mathbb{Z}_{p^\infty}$ contiene una cantidad infinita de elementos $\overline{\frac{1}{p^n}}$, contiene a todos los miembros de la cadena y $N = \mathbb{Z}_{p^\infty}$, y en otro caso, sea $n \coloneqq \max\left\{n \in \mathbb{N} : \overline{\frac{1}{p^n}} \in \mathbb{N}\right\}$, $N = \left(\overline{\frac{1}{p^n}}\right)$.

   $\subseteq]$ Para $\overline{\frac{a}{p^m}} \in N$ con la fracción irreducible, a es coprimo con p^m y por tanto $\left(\overline{\frac{1}{p^m}}\right) = \left(\overline{\frac{a}{p^n}}\right) \subseteq N$, de donde $m \leq n$ y $\overline{\frac{a}{p^m}} \in \left(\overline{\frac{1}{p^n}}\right)$.

   $\supseteq]$ Obvio.

   Como todos sus subgrupos son los de esta cadena, $\mathbb{Z}_{p^\infty}$ es artiniano, y no es finitamente generado porque de serlo, como todos sus subgrupos propios lo son, sería noetheriano.

5. $\frac{\mathbb{Q}}{\mathbb{Z}} = \bigoplus_p \mathbb{Z}_{p^\infty}$.

6. Si ${}_AM$ es noetheriano, todo A-endomorfismo suprayectivo en M es inyectivo.

7. Si ${}_AM$ es artiniano, todo A-endomorfismo inyectivo en M es suprayectivo.

Una **sucesión exacta corta** es una expresión de la forma $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ en la que L, M y N son A-módulos, cada flecha es un homomorfismo y el núcleo de cada morfismo es la imagen del que le precede, lo que equivale a que f sea un monomorfismo y g un epimorfismo con $\mathrm{Im} f = \ker g$.

Toda sucesión exacta corta con término central M es isomorfa a una de la forma $0 \to K \overset{\iota}{\hookrightarrow} M \overset{\pi}{\twoheadrightarrow} \frac{M}{K} \to 0$, donde ι es la inclusión y π la proyección canónica. **Demostración:** Dada $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$, sea $K \coloneqq \mathrm{Im} f$, restringiendo $\hat{f} : L \to K$ tenemos un isomorfismo que nos permite cambiar L por K y f por ι ya que $\iota \circ \hat{f} = f$, y por el primer teorema de isomorfía en g, $\frac{M}{K} \cong N$, por lo que cambiamos N por $\frac{M}{K}$ y g por π ya que el isomorfismo de la prueba del teorema de isomorfía es $\overline{g} : \frac{M}{K} \to N$ dado por $\overline{g}(\overline{m}) \coloneqq g(m)$ y claramente $\overline{g} \circ \pi = g$.

Si $N \leq_A M$, M es noetheriano o artiniano si y sólo si lo son N y $\frac{M}{N}$.

$\Longrightarrow$] Si M es noetheriano o artiniano, como $\mathcal{L}({}_AN) \subseteq \mathcal{L}({}_AM)$, también lo es N, y como la biyección $\rho : \{K \in \mathcal{L}({}_AM) \mid N \subseteq K\} \to \mathcal{L}({}_AM/N)$ del teorema de correspondencia conserva la inclusión, $\rho^{-1}(\mathcal{L}({}_AM/N)) \subseteq \mathcal{L}({}_AM)$ y también lo es $\frac{M}{N}$.

$\Longleftarrow$] Si $P \subseteq Q$ son submódulos de M con $P \cap N = Q \cap N$ y $P + N = Q + N$, para $q \in Q$, $q \in Q + N = P + N$ y por tanto $q = p + n$ para ciertos $p \in P$ y $n \in N$, y $q - p = n \in Q \cap N = P \cap N \subseteq P$, luego $q = (q - p) + p \in P$ y se concluye $P = Q$. Si N y $\frac{M}{N}$ son noetherianos o artinianos respectivamente, sea $(P_n)_n$ una cadena ascendente o descendente de submódulos de M, los $P_n \cap N$ y los $\frac{P_n + N}{N}$ forman cadenas ascendentes o descendentes de submódulos de N y $\frac{M}{N}$ respectivamente, y por hipótesis ambas se estabilizan a partir de un n_0 que podemos suponer común, pero entonces, para $n \geq n_0$, $P_n \subseteq P_{n+1}$ con $P_n \cap N = P_{n+1} \cap N$ y $\frac{P_n \cap N}{N} = \frac{P_{n+1} + N}{N}$, por lo que $P_n = P_{n+1}$ y M es noetheriano o artiniano.

La suma directa finita de módulos noetherianos o artinianos es respectivamente noetheriana o artiniana. En efecto, para $n \leq 1$ módulos es obvio, para $n = 2$ se deduce de lo anterior y de que, si $M = N \oplus K$, $K \cong \frac{M}{N}$, y para $n > 2$ se hace inducción.

Dado un anillo A:

1. A es noetheriano o artiniano, respectivamente, si y sólo si existe $n > 0$ con ${}_AA^n$ noetheriano o noetheriano, si y sólo si todo A-módulo finitamente generado es noetheriano o artiniano.

   $1 \implies 3]$ Es fácil ver que los submódulos de ${}_AA^n$ son productos de submódulos de A, que son ideales, pero si $(M_k \coloneqq I_{k1} \times \cdots \times I_{kn})_k$ es una cadena ascendente de submódulos de A^n, cada cadena ascendente $(I_{ki})_k$ se estabiliza en un punto, que podemos suponer común, y $(M_k)_k$ se estabiliza. Entonces para ${}_AM$ finitamente generado existe un epimorfismo $\phi : A^n \twoheadrightarrow M$ y las cadenas ascendentes de M también se estabilizan.

$3 \implies 2]$ Obvio.

$2 \implies 1]$ Si A^n es noetheriano para cierto $n > 0$, sea $(I_k)_k$ una cadena ascendente de ideales de A, $(I_k, 0, \ldots, 0)_k$ es una cadena ascendente de submódulos de A^n y por tanto se estabiliza, luego $(I_k)_k$ también se estabiliza.

Para artinianos es análogo.

2. Dados un anillo A noetheriano o artiniano, respectivamente, y un homomorfismo $f : A \to B$ tal que ${}_AB$ por restricción de escalares es finitamente generado, entonces B es un anillo noetheriano o artiniano.

   Por lo anterior lo es ${}_AB$, pero $\mathcal{L}({}_BB) \subseteq \mathcal{L}({}_AB)$.

Si $A = A_1 \times \cdots \times A_n$ es un producto de anillos, todo A-módulo es isomorfo a un producto $M_1 \times \cdots \times M_n$, donde cada M_i es un A_i-módulo, y en particular $\mathcal{L}({}_AM) \cong \prod_{i=1}^m \mathcal{L}({}_{A_i}M_i)$.

Lema de Artin: En un anillo A en que 0 es producto finito de ideales maximales, un A-módulo es noetheriano si y sólo si es artiniano. **Demostración:** Si el número de ideales que hay que multiplicar es $n \leq 1$, A es un cuerpo y sabemos que se cumple. Para $n > 1$, por inducción, sean $0 = J_1J_2$ donde cada J_i es producto de menos de n maximales. Si por ejemplo $J_1 = M_1 \cdots M_k$ con los M_i maximales, en $\frac{A}{J_1}$, $0 = \frac{J_1}{J_1} = \frac{M_1 \cdots M_k}{J_1} = \frac{M_1}{J_1} \cdots \frac{M_k}{J_1}$, y como $J_1 \subseteq M_i$ para cada i, $\frac{M_i}{J_1} \trianglelefteq_{\mathrm{m}} \frac{A}{J_1}$ y, en $\frac{A}{J_1}$, 0 es producto de menos de n maximales y por tanto un $\frac{A}{J_1}$-módulo es noetheriano si y sólo si es artiniano, y análogamente para un $\frac{A}{J_2}$-módulo. Dado ${}_AM$, $N \coloneqq J_1M$ es anulado por J_2 y por tanto se puede ver como un $\frac{A}{J_2}$-módulo con $\mathcal{L}({}_{A/J_2}N) = \mathcal{L}({}_AN)$ por restricción de escalares, mientras que $\frac{M}{N} = \frac{M}{J_1M}$ es anulado por J_1 y se puede ver como un $\frac{A}{J_1}$-módulo con $\mathcal{L}({}_{A/J_1}M/N) = \mathcal{L}({}_AM/N)$. Entonces ${}_AM$ es noetheriano si y sólo si lo son ${}_AM/N$ y ${}_AN$, si y sólo si lo son ${}_{A/J_1}M/N$ y ${}_{A/J_2}N$, si y sólo si son artinianos, si y sólo si lo son ${}_AM/N$ y ${}_AN$, si y sólo si ${}_AM$ es noetheriano.

Teorema de Akizuki:

1. Un anillo es artiniano si y sólo si es noetheriano de dimensión 0.

   $\implies]$ Ya vimos que entonces es de dimensión 0 y el 0 es producto finito de maximales, luego es noetheriano por el lema de Artin.

   $\impliedby]$ Por ser noetheriano, 0 es producto finito de ideales primos, que son maximales por ser de dimensión 0, luego el anillo es artiniano por el lema de Artin.

2. Un módulo de un anillo artiniano es artiniano si y sólo si es noetheriano, si y sólo si es finitamente generado.

   $1 \iff 2]$ Por el argumento anterior el 0 es producto finito de maximales y aplica el lema de Artin.

   $2 \implies 3]$ Por definición.

   $3 \implies 1]$ Visto.

Un A-módulo es **de longitud finita** si es noetheriano y artiniano. Un anillo A es artiniano si y sólo si todo A-módulo finitamente generado es de longitud finita.

3.9. Módulos y matrices

Sean $m, n \in \mathbb{N}^*$ y $\mathcal{C}_m$ y $\mathcal{C}_n$ las bases canónicas respectivas de los A-módulos libres A^m y A^n, $(f \mapsto M_{\mathcal{C}_m\mathcal{C}_n}(f)) : \mathrm{Hom}_A(A^n, A^m) \to \mathcal{M}_{m\times n}(A)$ es un isomorfismo de A-módulos con inversa $C \mapsto v \mapsto Cv$. **Demostración:** Sean $\mathcal{C}_n =: (e_1, \dots, e_n)$ y $\mathcal{C}_m =: (f_1, \dots, f_m)$, toda $f \in \mathrm{Hom}_A(A^n, A^m)$ viene dada por los valores que le asigna a los e_i, que se pueden expresar respecto a los f_j dando lugar a $M \coloneqq M_{\mathcal{C}_m\mathcal{C}_n}(f)$ cuyas columnas son los $f(e_i)$, pero claramente Me_i es la i-ésima columna de M, y recíprocamente, si $M \in \mathcal{M}_{m\times n}(A)$ y f viene dada por $f(v) \coloneqq Mv$, las columnas de $M_{\mathcal{C}_m\mathcal{C}_n}(f)$ son los Me_i que son las columnas de M. Que es un isomorfismo es claro tomando $(b_{ij} \coloneqq \sum_k a_k e_k \mapsto a_i f_j)_{i,j}$ como base de $\mathrm{Hom}_A(A^n, A^m)$ y viendo que conserva combinaciones lineales de los b_{ij}.

$\mathrm{GL}_s(K) \coloneqq \{A \in \mathcal{M}_s(K) \mid \det A \neq 0\}$. Dada $C \in \mathcal{M}_{m\times n}(A)$, llamamos **$A$-módulo asociado a** C, $M(C)$, a $\frac{A^m}{\{Cv\}_{v\in A^n}}$. $B, C \in \mathcal{M}_{m\times n}(A)$ son **equivalentes** si existen $P \in \mathrm{GL}_m(A)$ y $Q \in \mathrm{GL}_n(A)$ con $C = PBQ$, en cuyo caso $M(B) \cong M(C)$. **Demostración:** Se tiene $PB = CQ^{-1}$, luego llamando $f_C : A^n \to A^m$ al homomorfismo $f_C(v) \coloneqq Cv$, $f_P \circ f_B = f_C \circ f_{Q^{-1}}$. Definiendo el homomorfismo $\psi : M(B) \to M(C)$ como $\psi(\overline{a}) = \overline{f_P(a)}$, ψ está bien definido porque $a \in \mathrm{Im} f_B \implies f_P(a) \in \mathrm{Im}(f_P \circ f_B) = \mathrm{Im}(f_C \circ f_{Q^{-1}}) = \mathrm{Im} f_C$, pero el homomorfismo $\phi : M(C) \to M(B)$ dado por $\phi(\overline{c}) \coloneqq \overline{f_{P^{-1}}(c)}$ también está bien definido porque $c \in \mathrm{Im} f_C \implies f_{P^{-1}}(c) \in \mathrm{Im}(f_{P^{-1}} \circ f_C) = \mathrm{Im}(f_{P^{-1}} \circ f_C \circ f_{Q^{-1}}) = \mathrm{Im}(f_P)$, y $\phi = \psi^{-1}$.

Una **operación** o **transformación elemental por filas** o **columnas** en $C \in \mathcal{M}_{m\times n}(A)$ consiste en intercambiar dos filas o columnas de C, multiplicar una por un $\alpha \in A^*$ o sumarle a una otra multiplicada por un $\alpha \in A$.

AlgL

Llamamos **matriz elemental** de tamaño n a toda matriz obtenida al efectuar una operación elemental [...] en I_n. [...] Si B se obtiene al realizar una operación elemental por filas en A y E al realizar la misma en I_m, entonces $B = EA$. [...] Si B se obtiene de aplicar una operación elemental por columnas en A y E al aplicarla a I_n, entonces $B = AE$. Así, realizar una serie de estas operaciones en una matriz equivale a multiplicarla por uno o ambos lados por un producto de matrices elementales, el cual es invertible.

Las matrices elementales son las mismas por filas que por columnas. Si $B, C \in \mathcal{M}_{m\times n}(A)$ y C se puede obtener aplicando a B una cantidad finita de transformaciones elementales por filas y por columnas, entonces B y C son equivalentes, pues aplicar transformaciones por filas y columnas a B equivale a multiplicarla a izquierda y derecha por matrices invertibles.

Capítulo 4

Módulos sobre DIPs

En adelante, salvo que se indique lo contrario, A es un DIP y $\mathcal{P} \subseteq A$ es un conjunto irredundante de representantes salvo asociados de los elementos irreducibles o primos de A. Por ejemplo, si $A = \mathbb{Z}$, $\mathcal{P}$ podría ser el conjunto de primos positivos, y cuando $A = K[X]$ con K cuerpo, $\mathcal{P}$ podría ser el conjunto de polinomios mónicos irreducibles.

Como **teorema**, si $G \leq_A F$ con F libre, entonces G es libre y $\mathrm{rg}G \leq \mathrm{rg}F$. **Demostración** cuando F tiene rango finito**:**[1] Sean $B = \{x_1, \ldots, x_n\}$ una base de F y, para $j \in \{0, \ldots, n\}$, $F_j \coloneqq \bigoplus_{i=1}^{j} Ax_i$, tenemos una cadena estrictamente ascendente $0 = F_0 \subsetneq \cdots \subsetneq F_n = F$ donde $\frac{F_j}{F_{j-1}} \cong Ax_j$ para $j \in \{1, \ldots, n\}$, pero el homomorfismo canónico $A \to Ax_j$, $a \mapsto ax_j$, es un isomorfismo (por restricción de $\phi : A^n \to F$), luego todo submódulo de $\frac{F_j}{F_{j-1}}$ es isomorfo a un ideal de A, que será principal, y es pues nulo o un A-módulo libre de rango 1. Intersecando los términos de esta cadena con G, $0 = G \cap F_0 \subseteq G \cap F_1 \subseteq \cdots \subseteq G \cap F_n = G$, y el homomorfismo $f_j : G \cap F_j \hookrightarrow F_j \xrightarrow{\pi} \frac{F_j}{F_{j-1}}$ tiene núcleo $G \cap F_{j-1}$, por lo que hay un monomorfismo $\frac{G \cap F_j}{G \cap F_{j-1}} \rightarrowtail \frac{F_j}{F_{j-1}}$ y por tanto $\frac{G \cap F_j}{G \cap F_{j-1}} = 0$ o es un A-módulo libre de rango 1. Tras eliminar términos repetidos de la cadena, existen $k_i \in \{1, \ldots, n\}$, $k_1 < \cdots < k_t$, con $0 = G \cap F_{k_0} \subsetneq G \cap F_{k_1} \subsetneq \cdots \subsetneq G \cap F_{k_t} = G$ y donde cada $\frac{G \cap F_{k_i}}{G \cap F_{k_{i-1}}}$ es un A-módulo libre de rango 1. Si $t = 0$ hemos terminado. En otro caso, sean $H_i \coloneqq G \cap F_{k_i}$, y_1 un generador de H_1 y, para $i \in \{2, \ldots, n\}$, y_i tal que $y_i + H_{i-1}$ sea un generador de $\frac{H_i}{H_{i-1}}$, entonces $(y_1, \ldots, y_i)$ es base de H_i. Para $i = 1$ esto es claro. Para $i > 1$, por inducción, para $m \in H_i$ existe $a \in A$ tal que, en $\frac{H_i}{H_{i-1}}$, $\overline{ay_i} = \overline{m}$ y por tanto $ay_i - m \in H_{i-1}$, que por inducción se puede expresar unívocamente como combinación lineal de $(y_1, \ldots, y_{i-1})$. Así, $\{y_1, \ldots, y_i\}$ es generador de H_j, y es linealmente independiente porque, al ser $\frac{H_i}{H_{i-1}} = (\overline{y_i})$ de rango 1, $\phi : A \to (\overline{y_i})$ dado por $\phi(a) \coloneqq a\overline{y_i}$ es un isomorfismo y, si $n \in H_{i-1}$ y $a \in A$ cumplen $n + ay_i = 0$, $ay_i = -n \in H_{i-1}$ y $\phi(a) = 0$, luego $a = 0$ y $n = 0$. Por tanto, para $i = t$, $H_t = G$ tiene base $(y_1, \ldots, y_t)$.

Todo epimorfismo de A-módulos $p : M \twoheadrightarrow F$ con F libre tiene inverso por la derecha, un $f : F \to M$ con $p \circ f = 1_F$, y entonces $M = \mathrm{Im}f \oplus \ker p$ y $M \cong F \times \ker p$. **Demostración:** Dada una base $X = \{x_i\}_{i \in I}$ de F, y para $i \in I$, $m_i \in M$ con $p(m_i) = x_i$, existe un único $f : F \to M$ con $f(x_i) = m_i$ para cada i, luego el homomorfismo $p \circ f$ es la identidad sobre los elementos

[1] Demostración general en *Algebra* de Thomas W. Hungerfor, IV.6.1, que usa propiedades de los números ordinales.

de X y por tanto sobre todos los de F. Para la descomposición, $\mathrm{Im} f \cap \ker p = 0$ porque sus elementos son de la forma $f(x)$ con $x \in F$ y $p(f(x)) = 0$, pero $p(f(x)) = x$, e $\mathrm{Im} f + \ker p = M$ porque, para $m \in M$, $m = m - f(p(m)) + f(p(m))$ con $f(p(m)) \in \mathrm{Im} f$ y $m - f(p(m)) \in \ker p$ ya que $p(m - f(p(m))) = p(m) - p(m) = 0$. Finalmente, como f es inyectiva, su restricción a la imagen es un isomorfismo e $\mathrm{Im} f \cong F$.

4.1. Submódulos de torsión

Un $x \in_A M$ es un **elemento de torsión** si $\mathrm{ann}_A(x) \neq 0$, y es un **elemento de p-torsión** para cierto $p \in \mathcal{P}$ si existe $t \in \mathbb{N}$ con $\mathrm{ann}_A(x) = (p^t)$, si y sólo si existe $s \in \mathbb{N}$ con $p^s x = 0$.

Llamamos **submódulo de torsión** de ${}_AM$ a

$$t(M) \coloneqq \{x \in M \mid x \text{ es de torsión}\} \leq_A M.$$

En efecto, para $a \in A$ y $x, y \in t(M)$, sean $b \in \mathrm{ann}_A(x) \setminus 0$ y $c \in \mathrm{ann}_A(y) \setminus 0$, entonces $bc(x-y) = bcx - bcy = 0 - 0 = 0$, luego $0 \neq bc \in \mathrm{ann}_A(x-y)$ y $x - y \in t(M)$, y como $abx = 0$ y $ab \neq 0$, $ax \in t(M)$.

Para $p \in \mathcal{P}$, llamamos **subgrupo de p-torsión** de ${}_AM$ a

$$M(p) \coloneqq \{x \in M \mid x \text{ es de } p\text{-torsión}\} \leq_A M.$$

En efecto, para $a \in A$ y $x, y \in M(p)$, existe $s \in \mathbb{N}$ con $p^s x = p^s y = 0$ y entonces $ap^s x = 0$ y $p^s(x+y) = 0$.

Para ${}_AM$, $t(M) = \bigoplus_{p \in \mathcal{P}} M(p)$. **Demostración:** Claramente $\sum_{p \in \mathcal{P}} M(p) \leq_A t(M)$. Para ver que la suma es directa, sean $q \in \mathcal{P}$ y $x \in M(q) \cap \sum_{p \in \mathcal{P} \setminus \{q\}} M(p)$, existen $s \in \mathbb{N}$ con $q^s x = 0$, una descomposición $x = x_1 + \cdots + x_r$ con cada $x_i \in M(p_i)$ para cierto $p_i \in \mathcal{P} \setminus \{q\}$ y, para cada i, $t_i \in \mathbb{N}$ con $p_i^{t_i} x_i = 0$, con lo que si $a \coloneqq \prod_{i=1}^r p_i^{t_i}$, $ax = 0$, pero $\gcd\{q^s, a\} = 1$, por lo que hay una identidad de Bézout $q^s b + ac = 1$ y por tanto $x = 1x = q^s bx + acx = 0$. Queda ver que $t(M) \subseteq \sum_{p \in \mathcal{P}} M(p)$. Sea $x \in t(M) \setminus 0$, $\mathrm{ann}_A(x) \triangleleft A$, pero como A es un DIP existen $(b) \in A \setminus (A^* \cup \{0\})$ con $\mathrm{ann}_A(x) = (b)$ y una factorización en irreducibles $b = up_1^{t_1} \cdots p_r^{t_r}$ con $u \in A^*$, los $p_i \in \mathcal{P}$ irreducibles distintos y los $t_i > 0$, y queremos ver que $x \in \sum_{i=1}^r M(p_i) \subseteq \sum_{p \in \mathcal{P}} M(p)$. Si $r = 1$, $x \in M(p_1)$ y hemos terminado. Si $r > 1$, por inducción, como $\gcd\{p_1^{t_1} \cdots p_{r-1}^{t_{r-1}}, p_r^{t_r}\} = 1$, existe una identidad de Bézout $p_1^{t_1} \cdots p_{r-1}^{t_{r-1}} b + p_r^{t_r} c = 1$ y $x = p_1^{t_1} \cdots p_{r-1}^{t_{r-1}} bx + p_r^{t_r} cx$, donde el primer sumando es anulado por $p_r^{t_r}$ y por tanto está en $M(p_r)$ y el segundo es anulado por $p_1^{t_1} \cdots p_{r-1}^{t_{r-1}}$ y por tanto está en $\sum_{i=1}^r M(p_i)$.

Si ${}_AM \neq 0$ es finitamente generado, existen $p_1, \ldots, p_r \in \mathcal{P}$, unívocamente determinados salvo permutación, tales que $t(M) = \bigoplus_{i=1}^r M(p_i)$ y cada $M(p_i) \neq 0$. **Demostración:** Como A es noetheriano, M es noetheriano y $t(M)$ es finitamente generado. Como $t(M) = \bigoplus_{p \in \mathcal{P}} M(p)$ es finitamente generado, digamos por $\{x_1, \ldots, x_s\}$, entendiendo la suma directa como externa, como cada x_i tiene una cantidad finita de elementos no nulos, $(x_1, \ldots, x_s)$ tiene una cantidad finita de índices no nulos y casi todo $M(p) = 0$, luego $t(M) = \bigoplus_{i=1}^r M(p_i)$ para ciertos p_i. La unicidad se sigue de que los p_i deben ser justo aquellos con $M(p_i) \neq 0$.

${}_AM$ es **de torsión** si $M = t(M)$, y es **de p-torsión** para un $p \in \mathcal{P}$ si $M = M(p)$.

Si G es un grupo abeliano, es finitamente generado de torsión si y sólo si es finito, y para p primo positivo, es de p-torsión finitamente generado si y sólo si es finito y $p^m M = 0$ para cierto $m > 0$.

Si $p \in \mathcal{P}$, $n \in \mathbb{N}^*$ y ${}_AM \coloneqq \frac{A}{(p^n)}$, para $k \in \{0, \dots, n-1\}$ es $\operatorname{ann}_M(p^k) = \frac{(p^{n-k})}{(p^n)}$ y para $k \geq n$ es $\operatorname{ann}_M(p^k) = M$, y $\operatorname{ann}_M(p)$ es un $\frac{A}{(p)}$-espacio vectorial de dimensión 1.

Si Q es el cuerpo de fracciones de A y $N \leq_A Q$ es no nulo, $\frac{Q}{N}$ es un A-módulo de torsión.

Dado un A-homomorfismo $f : M \to N$, $f(t(M)) \subseteq t(N)$, y la inclusión puede ser estricta incluso cuando f es un monomorfismo o un epimorfismo.

4.2. Parte libre de torsión

${}_AF$ es **libre de torsión** si $t(F) = 0$. Llamamos **parte libre de torsión** de ${}_AM$ a $\frac{M}{t(M)}$, que es libre de torsión. **Demostración:** Queremos ver que, para $\overline{x} \in \frac{M}{t(M)} \setminus 0$ es $\operatorname{ann}_A(\overline{x}) = 0$. Sean entonces $x \in M$ con $\operatorname{ann}_A(\overline{x}) \neq 0$ y $a \in A \setminus 0$ con $a\overline{x} = 0$, entonces $ax \in t(M)$ y existe $b \in A \setminus 0$ con $bax = 0$, luego $x \in t(M)$ y $\overline{x} = 0$.

Todo A-módulo libre es libre de torsión, pues es isomorfo a un $A^{(I)}$ y, si hubiera un $a \in A$ y un $v \in A^{(I)}$ con $av = 0$, como estamos en un dominio, $a = 0$ o $v = 0$.

Como **teorema**:

1. Un A-módulo es finitamente generado y libre de torsión si y sólo si es libre de rango finito.

   $\Longrightarrow$] Para ${}_AF = 0$ es obvio. Si ${}_AF \neq 0$, sean $X = \{x_1, \dots, x_n\}$ un generador finito de F y $S = \{x_1, \dots, x_k\}$ con $k \leq n$ un subconjunto linealmente independiente maximal, $G \coloneqq (x_1, \dots, x_k) \leq_A F$ es libre con base S. $\frac{F}{G}$ es finitamente generado, y queremos ver que es de torsión. Para $x \in X \setminus S$, $S \cup \{x\}$ no es linealmente independiente, luego existen $a_1, \dots, a_k, a \in A$ no todos nulos con $a_1x_1 + \cdots + a_kx_k = ax$, lo que implica que $a \neq 0$ y que $ax \in (X) = G$, luego $a\overline{x} = 0$ con $a \neq 0$ y $\overline{x} \in t(\frac{F}{G})$. Entonces, como $\frac{F}{G} = (\overline{X}) = (\overline{x_1}, \dots, \overline{x_n}) = (\overline{0}, \dots, \overline{0}, \overline{x_{k+1}}, \dots, \overline{x_n}) = (\overline{X \setminus S})$, $X \subseteq t(\frac{F}{G})$ y $\frac{F}{G} = t(\frac{F}{G})$. Por tanto, para $i \in \{k+1, \dots, n\}$ existe $a_i \in A \setminus 0$ con $a_i\overline{x_i} = 0$, luego $r \coloneqq a_{k+1} \cdots a_n \neq 0$ cumple $rx \in G$ para todo $x \in X$ y por tanto $rF \subseteq G$, pero $F \to rF$ dada por $z \mapsto rz$ es un A-isomorfismo ya que es un epimorfismo y, como r es libre de torsión, $z \neq 0 \implies rz \neq 0$. Entonces, como G es libre y $rF \leq_A G$, rF es libre y por tanto F también con $\operatorname{rg}F \leq \operatorname{rg}G = k$.

   $\Longleftarrow$] Es libre de torsión por ser libre y es finitamente generado por ser de rango finito.

2. Todo ${}_AM$ finitamente generado admite una descomposición en suma directa interna $M = t(M) \oplus L$ con ${}_AL$ libre de rango finito.

   $\frac{M}{t(M)}$ es finitamente generado y libre de torsión, y por el apartado anterior es libre de rango finito, luego la proyección canónica $p : M \twoheadrightarrow \frac{M}{t(M)}$ tiene inversa por la derecha $\alpha : \frac{M}{t(M)} \to M$ y si $L \coloneqq \operatorname{Im}\alpha \cong \frac{M}{t(M)}$, $M = \ker p \oplus \operatorname{Im}\alpha = t(M) \oplus F$ con F libre de rango finito.

3. Si ${}_AF$ es libre de rango finito, $|S| = \operatorname{rg}F$ para todo $S \subseteq F$ linealmente independiente maximal.

S es finito porque, de no serlo, $G \coloneqq (S)$ sería un submódulo libre de rango infinito de uno de rango finito, y como $\frac{F}{G}$ es finitamente generado con un cierto generador $\{\overline{y_1}, \ldots, \overline{y_s}\}$, $X \coloneqq S \cup \{y_1, \ldots, y_s\}$ es un generador finito de F en que S es linealmente independiente maximal. Entonces, por un argumento como el del primer apartado, existe $r \in F$ con $rF \leq_A G \leq_A F$ y $rF \cong F$, pero como G es libre, $rF \cong F$ también y $\mathrm{rg}F \leq \mathrm{rg}G$, y como ahora F es libre, $\mathrm{rg}G \leq \mathrm{rg}F$, luego $\mathrm{rg}F = \mathrm{rg}G = |S|$.

Sean $\mathcal{T}$ la clase de A-módulos de torsión y $\mathcal{F}$ la de A-módulos libres de torsión:

1. Si $N \leq_A M$ y tanto N como $\frac{N}{M}$ están en una de las clases, entonces M también.
2. Si $N \leq_A M \in \mathcal{T}$ entonces $N, \frac{N}{M} \in \mathcal{T}$, pero esto no se cumple para $\mathcal{F}$.
3. Si $K, N \leq_A M$ y $K+N$ está en una de las clases, K y N están también en la misma.
4. Si $K, N \leq_A M$ con $K, N \in \mathcal{T}$ entonces $K + N \in \mathcal{T}$, pero esto no se cumple para $\mathcal{F}$.

4.3. Módulos finitamente generados de p-torsión sobre un DIP

En un anillo conmutativo unitario A arbitrario, $N \leq_A M$ es un **submódulo esencial** de M si $\forall L \leq_A M, (L \neq 0 \implies L \cap N \neq 0)$, y un monomorfismo de A-módulos $f : L \rightarrowtail M$ es un **monomorfismo esencial** si su imagen es un submódulo esencial de M.

Si A es un anillo conmutativo unitario arbitrario:

1. Si $N \leq_A M$, un **pseudocomplemento** de N en M es un elemento maximal X de $\mathcal{C}_N(M) \coloneqq \{L \leq_A M : L \cap N = 0\}$ por inclusión, que siempre existe. El homomorfismo $f : N \hookrightarrow M \overset{\pi}{\twoheadrightarrow} \frac{M}{X}$ es un monomorfismo esencial, y es un isomorfismo si y sólo si X es complemento directo de N en M.

   La existencia es por el lema de Zorn.

2. Si A es un dominio, los ideales (A-submódulos) esenciales de A son precisamente los ideales no nulos.

3. Si A es un dominio, ${}_AF$ es libre y $N \leq_A F$ contiene un subconjunto linealmente independiente maximal de F entonces N es un submódulo esencial de F.

${}_AM$ es finitamente generado de p-torsión para cierto $p \in \mathcal{P}$, existen $r > 0$ y $0 < n_1 \leq \cdots \leq n_r$ únicos tales que $M \cong \frac{A}{(p^{n_1})} \oplus \cdots \oplus \frac{A}{(p^{n_r})}$.

Demostración: El enunciado se puede reescribir cambiando $0 < n_1 \leq \cdots \leq n_r$ por $n_1 \geq \cdots \geq n_r > 0$. Sea $X = \{x_1, \ldots, x_k\}$ un generador de M, para la existencia hacemos inducción en k.

- Si $k = 1$, $M = (x_1)$ y, como x_1 es de p-torsión, existe $n > 0$ con $\mathrm{ann}_A(x_1) = (p^n)$, luego $\frac{A}{(p^n)} = \frac{A}{\mathrm{ann}_A(x_1)} \cong (x_1) = M$ por el primer teorema de isomorfía sobre $a \mapsto ax_1$.

- Si $k > 1$, sea $n_1 > 0$ mínimo con $p^{n_1}x_i = 0$ para todo i, entonces $p^{n_1}M = 0 \neq p^{n_1-1}M$, y podemos suponer $p^{n_1-1}x_1 \neq 0$. Sean ahora Z un pseudocomplemento de (x_1) en M y $f : (x_1) \hookrightarrow M \overset{\pi}{\twoheadrightarrow} \frac{M}{Z}$ un monomorfismo esencial, $p^{n_1}\frac{M}{Z} = \{\overline{p^{n_1}m}\}_{m\in\mathbb{Z}} = 0$ y $p^{n_1-1}f(x_1) = f(p^{n_1-1}x_1) \neq 0$.

  Supongamos $(y_1 \coloneqq f(x_1)) \subsetneq \frac{M}{Z}$. Sean $\xi \in M \setminus (y_1)$ y $k \coloneqq \min\{i \in \mathbb{N}^* \mid p^i\xi \in (y_1)\}$, que existe porque $p^{n_1}\xi = 0 \in (y_1)$, entonces $p^k\xi \in (y_1)$ y $p^{k-1}\xi \notin (y_1)$, luego $z \coloneqq p^{k-1}\xi \in M \setminus (y_1)$ cumple $pz \in (y_1)$ y existe $a \in A$ con $pz = ay_1$. En la factorización $a =: p^t b$ con $t \in \mathbb{N}$ y $p \nmid b$, se tiene $t > 0$. En efecto, si no lo fuera sería $pz = bx$ con b y p coprimos, pero como $p^{n_1}\frac{M}{Z} = 0$, $\frac{M}{Z}$ se puede ver como un $\frac{A}{(p^{n_1})}$-módulo y entonces $\overline{b} = b + (p^{n_1})$ es unidad de $\frac{A}{(p^{n_1})}$ y $(\overline{y_1}) = (\overline{by_1})$, y por la correspondencia, $(y_1) = (by_1)$, con lo que existe a tal que $aby_1 = y_1$ y como $p^{n-1}y_1 = p^{n-1}aby_1 \neq 0$ es $p^n z = p^{n-1}by_1 \neq 0$, pero $p^n M = 0\#$. Por tanto $t > 0$, luego $pz = p^t by_1$ y $p(z - p^{t-1}by_1) = 0$. Sea entonces $y' \coloneqq z - p^{t-1}by_1$, $y' \notin (y_1)$ porque $z \notin (y_1)$ y $py' = 0$, pero entonces $\frac{A}{(p)} \to (y')$ dado por $a + (p) \mapsto ay'$ es un isomorfismo de A-módulos y los únicos submódulos de (y') son 0 e (y'), pero (y_1) es esencial por ser la imagen de un monomorfismo esencial, luego $(y_1) \cap (y') \neq 0$ y por tanto $(y_1) \cap (y') = (y')$ e $(y') \subseteq (y_1)$, pero $y' \notin (y_1)\#$. Por tanto $\frac{M}{Z} = (y_1)$.

  Con esto f es un isomorfismo y $M = (x_1) \oplus Z \cong \frac{A}{(p^{n_1})} \oplus Z$, pero entonces $Z \cong \frac{(x_1)\oplus Z}{(x_1)} = \frac{M}{(x_1)}$, que es un A-módulo generado por $\{\overline{x_2}, \dots, \overline{x_k}\}$, y por hipótesis de inducción, $Z \cong \frac{A}{(p^{n_2})} \oplus \cdots \oplus \frac{A}{(p^{n_r})}$ con $n_2 \geq \cdots \geq n_r > 0$ y se tiene $n_2 = \min\{s \in \mathbb{N}^* \mid p^s Z = 0\}$, pero $p^{n_1}Z \subseteq p^{n_1}M = 0$, luego $n_1 \geq n_2$.

Para la unicidad, si $M \cong \frac{A}{(p^{n_1})} \oplus \cdots \oplus \frac{A}{(p^{n_r})} \cong \frac{A}{(p^{m_1})} \oplus \cdots \oplus \frac{A}{(p^{m_s})}$ con $r, s > 0$, $0 < n_1 \leq \cdots \leq n_r$ y $0 < m_1 \leq \cdots \leq m_s$, $M \cong \frac{A}{(p^{n_1})} \times \cdots \times \frac{A}{(p^{n_r})}$ y $\frac{M}{pM} \cong \bigoplus_{i=1}^r \frac{A}{(p)} \cong \left(\frac{A}{(p)}\right)^r$, y análogamente $\frac{M}{pM} \cong \left(\frac{A}{(p)}\right)^s$, pero como (p) es maximal, $\frac{A}{(p)}$ es un cuerpo y los isomorfismos son entre $\frac{A}{(p)}$-espacios vectoriales, luego $r = s$ por la unicidad de la dimensión entre espacios vectoriales. Entonces n_1 es el mínimo $j > 0$ tal que $p^j M$ admite una descomposición en menos de r sumandos y m_1 también, luego $n_1 = m_1$. Por inducción en r:

- Si $r = 1$ hemos terminado.
- Si $r > 1$, $p^{n_1}M \cong \bigoplus_{i\geq 2} \frac{(p^{n_1})}{(p^{n_i})} \cong \bigoplus_i \frac{A}{(p^{n_i-n_1})}$ y del mismo modo $p^{n_1}M \cong \bigoplus_{i\geq 2} \frac{A}{(p^{m_i-n_1})}$, y tomando el mínimo t con $n_t > n_1$ y el mínimo t' con $n_{t'} > n_1$, por hipótesis de inducción, $(n_i - n_1)_{i\geq t} = (m_i - m_1)_{i\geq t'}$, con lo que $t = t'$ y hay exactamente $t - 1$ apariciones de $\frac{A}{(p^{n_1})}$ y de $\frac{A}{(p^{m_1})}$, pero $n_1 = m_1$, luego al final cada $n_i = m_i$.

4.4. Módulos finitamente generados sobre un DIP

Como **teorema**, si ${}_AM \neq 0$ es finitamente generado, existen un único $r \in \mathbb{N}$, el **rango libre de torsión** de M, y una familia $p_1^{n_{11}}, \dots, p_1^{n_{1r_1}}, \dots, p_k^{n_{k1}}, \dots p_k^{n_{kr_k}}$ de **divisores elementales** de M, única salvo asociados y orden de los p_i, con los p_i irreducibles no asociados dos a dos y $0 < n_{i1} \leq \cdots \leq n_{ir_i}$ para cada i, de forma que

$$M \cong A^r \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} \frac{A}{(p_i^{n_{ij}})},$$

lo que llamamos la **descomposición indescomponible** de M.

Demostración: $M \cong t(M) \oplus \frac{M}{t(M)}$ con $\frac{M}{t(M)}$ libre de rango finito r, con lo que $M \cong A^r \oplus t(M)$. Ahora bien, existen irreducibles distintos $p_1, \ldots, p_k \in \mathcal{P}$ con $t(M) = M(p_1) \oplus \cdots \oplus M(p_k)$ y cada $M(p_i) \neq 0$, pero como cada $M(p_i)$ es finitamente generado de p_i-torsión existen $0 < n_{i1} \leq \cdots \leq n_{ir_i}$ con $M(p_i) \cong \bigoplus_{j=1}^{r_i} \frac{A}{(p_i^{n_{ij}})}$. Para la unicidad, si hay otra descomposición $M \cong A^s \oplus \bigoplus_{i=1}^{l} \bigoplus_{j=1}^{s_i} \frac{A}{(q_i^{m_{ij}})}$ de la misma forma, donde podemos suponer que los $q_i \in \mathcal{P}$, la parte libre de torsión de la suma es isomorfa a A^s y por tanto $\frac{M}{t(M)} \cong A^s$, y la parte de torsión isomorfa al sumando derecho y a $t(M) = M(p_1) \oplus \cdots \oplus M(p_k) = M(q_1) \oplus \cdots \oplus M(q_l)$, luego por unicidad queda $\{p_1, \ldots, p_k\} = \{q_1, \ldots, q_l\}$, $k = l$ y, reordenando, cada $p_i = q_i$.Entonces, como cada $M(p_i)$ es de p_i-torsión, por la proposición anterior es $(n_{i1}, \ldots, n_{ir_i}) = (m_{i1}, \ldots, m_{ir_i})$.

Si ${}_AM$ es finitamente generado, existe una descomposición $M = L \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} M_{ij}$ como suma directa interna con L libre de rango igual al rango libre de torsión de M y cada $M_{ij} \cong \frac{A}{(p_i^{n_{ij}})}$, siendo los $p_i^{n_{ij}}$ los divisores elementales de M. En efecto, por el teorema hay un isomorfismo $\phi : A^r \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} \frac{A}{(p_i^{n_{ij}})} \to M$ y basta tomar $L \coloneqq \phi(A^r)$ y $M_{ij} \coloneqq \phi(\frac{A}{(p_i^{n_{ij}})})$.

Como **teorema**, si ${}_AM \neq 0$ es finitamente generado, existe un único $r \in \mathbb{N}^*$ y una única secuencia $d_1, \ldots, d_t \in A \setminus (A^* \cup \{0\})$ de **factores invariantes** de M, única salvo asociados, tal que $d_1 \mid \cdots \mid d_t$ y

$$M \cong A^r \oplus \bigoplus_{j=1}^{t} \frac{A}{(d_j)},$$

y de hecho r es el rango libre de torsión de A y si $(p_i^{n_{ij}})_{1 \leq i \leq k}^{1 \leq j \leq r_i}$ son los divisores elementales de M, $t \coloneqq \max_i r_i$ y cada $d_j = \prod_i p_i^{n_{i,r_i - t+j}}$, tomando $n_{ij} \coloneqq 0$ para $j < 0$. **Demostración:** Claramente $d_1 \mid \cdots \mid d_t$ y, como $\frac{A}{(d_j)} \cong \bigoplus_i \frac{A}{(p_i^{n_{i,r_i - t+j}})}$, $\bigoplus_{j=1}^{t} \frac{A}{(d_j)} \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} \frac{A}{(p_i^{n_{ij}})}$. Para la unicidad, la de r es como en el teorema anterior, y para la del sumando derecho queremos ver que toda descomposición $t(M) \cong \bigoplus_{j=1}^{u} \frac{A}{(\delta_j)}$ con los $\delta_j \notin A^* \cup \{0\}$ y $\delta_1 \mid \cdots \mid \delta_u$ cumple $t = u$ y $\frac{A}{(\delta_j)} \cong \frac{A}{(d_j)}$, y entonces δ_j y d_j serán asociados. Cada δ_k debe ser suma de submódulos de los $\frac{A}{(p_i^{n_{ij}})}$, pero estos submódulos son de la forma $\frac{A}{(p_i^z)}$ para ciertos z, por lo que finalmente δ_j debe ser de la forma $p_1^{m_{1j}} \cdots p_k^{m_{kj}}$ para ciertos m_{kj}, y claramente para cada i es $0 \leq m_{i1} \leq \cdots \leq m_{iu}$. Por el teorema chino de los restos, $\frac{A}{(\delta_j)} \cong \bigoplus_{i=1}^{k} \frac{A}{(p_i^{m_{ij}})}$ y por tanto $t(M) \cong \bigoplus_{i,j} \frac{A}{(p_i^{m_{ij}})}$, lo que tras eliminar los sumandos nulos y reordenar debe coincidir con la descomposición indescomponible de $t(M)$, lo que junto a que $0 \leq m_{i1} \leq \cdots \leq m_{iu}$ determina los m_{ij} y por tanto los δ_j salvo asociados.

Así, si ${}_AM \neq 0$ es finitamente generado, se puede expresar como suma directa interna de la forma $L \oplus \bigoplus_{i=1}^{t} M_i$ con L libre de rango igual al rango libre de torsión de M y cada $M_i \cong \frac{A}{(d_i)}$, siendo los d_i los factores invariantes de M.

Teoremas de estructura de los grupos abelianos finitos: Si M es un grupo abeliano finito:

1. Existen números primos $1 < p_1 < \cdots < p_k$ y enteros $0 < n_{i1} \leq \cdots \leq n_{ir_i}$ para $i \in \{1, \ldots, k\}$, únicos, con $M \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} \mathbb{Z}_{p_i^{n_{ij}}}$.

2. Existen enteros $1 < d_1 \mid \cdots \mid d_t$ únicos con $M \cong \bigoplus_{j=1}^{t} \mathbb{Z}_{d_j}$.

GyA

Un grupo cíclico $\langle a\rangle_n$ es indescomponible si y sólo si tiene orden potencia de primo.

Dado un grupo G, llamamos **exponente** o **periodo** de G, $\mathrm{Exp}(G)$, al menor $n \in \mathbb{N}^*$ tal que $\forall g \in G, g^n = 1$, o a ∞ si este no existe. [...]

Si un grupo es finito tiene periodo finito, y si tiene periodo finito es periódico. Los recíprocos no se cumplen. Todo p-grupo es periódico, pero no necesariamente finito. [...]

Si A es un grupo abeliano, $B \leq A$, $a \in A$, $n \in \mathbb{N}$ y $na = 0$, en A/B es $|a+B| \mid |a|$. En general estos órdenes no coinciden. [...]

Dados dos grupos abelianos finitos A y B, una descomposición por suma directa de A y una de B son **semejantes** si existe una biyección entre los subgrupos en la descomposición de A y la de B que a cada subgrupo de A le asocia uno de B isomorfo. [...]

Dos grupos abelianos finitos son isomorfos si y sólo si tienen descomposiciones primarias semejantes, si y sólo si tienen descomposiciones invariantes semejantes, si y sólo si tienen la misma lista de divisores elementales, si y sólo si tienen la misma lista de factores invariantes. [...]

4.5. Módulos de torsión finitamente generados

Si ${}_AM$ es finitamente generado de torsión, llamamos **divisores irreducibles** de M a los $p \in \mathcal{P}$ con $M(p) = 0$. Si además $M \neq 0$ y sus factores invariantes son $d_1 \mid \cdots \mid d_t$:

1. $\mathrm{ann}_A(M) = (d_t)$.

   $\subseteq]$ Para $a \in \mathrm{ann}_A(M)$, como $\frac{A}{(d_t)}$ es isomorfo a un sumando directo de M, $a\frac{A}{(d_t)} = 0$, pero $a\frac{A}{(d_t)} = \frac{(a)+(d_t)}{(d_t)} = 0$ y por tanto $(a) + (d_t) \subseteq (d_t)$ y $a \in (d_t)$.

   $\supseteq]$ $M \cong \bigoplus_{j=1}^{t} \frac{A}{(d_j)}$ y, como cada $d_j \mid d_t$, $d_t M = 0$, luego $(d_t) \subseteq \mathrm{ann}_A(M)$.

2. Un $p \in \mathcal{P}$ es divisor irreducible de M si y sólo si lo es de d_t, si y sólo si existe $x \in M \setminus \{0\}$ con $px = 0$.

   $1 \iff 2]$ Si $(p_{ij})_{1\leq i\leq k}^{1\leq j\leq r_i}$ son los divisores elementales de M, $d_t = p_1^{n_{1r_1}} \cdots p_k^{n_{kr_k}}$, luego los divisores irreducibles son los irreducibles de la factorización irreducible de d_t.

   $1 \implies 3]$ Si $M(p) \neq 0$, sea $z \in M(p) \setminus \{0\}$ con $\mathrm{ann}_A(z) = (p^s)$ y s mínimo, $s > 0$ ya que de lo contrario sería $(p^s) = A$ y $z = 1z = 0$, y $x := p^{s-1}z \in M \setminus \{0\}$ cumple $px = 0$.

   $3 \implies 1]$ $x \in M(p) \neq 0$.

Así, si M es un grupo abeliano finito, los divisores irreducibles de M son los $p > 0$ que dividen a $|M|$.

Sean ${}_AM \neq 0$ finitamente generado de torsión, p un divisor irreducible de M y $M(p) \cong \bigoplus_{j=0}^{r} \frac{A}{(p^{n_j})}$ con $0 < n_1 \leq \cdots \leq n_r$:

1. $0 \neq \mathrm{ann}_M(p_i) \subseteq \mathrm{ann}_M(p_i^2) \subseteq \cdots \subseteq \mathrm{ann}_M(p_i^s) \subseteq \ldots$.

2. $\{s \in \mathbb{N}^* \mid \mathrm{ann}_M(p^s) = \mathrm{ann}_M(p^{s+1})\} = \{s \in \mathbb{N}^* \mid s \geq n_r\}$.

$\supseteq]$ Para $s \geq n_r$, $M(p) \subseteq \operatorname{ann}_M(p^{n_r}) \subseteq \operatorname{ann}_M(p^s) \subseteq M(p)$ y $\operatorname{ann}_M(p^s) = \operatorname{ann}_M(p^{s+1}) = M(p)$.

$\subseteq]$ Sea X el conjunto de la izquierda, queremos ver que si $s \in X$ entonces $s+1 \in X$, de modo que si fuera $s < n_r$, por inducción sería $\operatorname{ann}_M(p^s) = \operatorname{ann}_M(p^{n_r}) = M(p)\#$. Sabemos que $\operatorname{ann}_M(p^{s+1}) \subseteq \operatorname{ann}_M(p^{s+2})$, y si $x \in \operatorname{ann}_M(p^{s+2})$, $p^{s+1}(px) = 0$ y por tanto $px \in \operatorname{ann}_M(p^{s+1}) = \operatorname{ann}_M(p^s)$, luego $p^{s+1}x = p^s(px) = 0$ y $x \in \operatorname{ann}_M(p^{s+1})$.

3. $M(p) = \operatorname{ann}_M(p^{n_r})$.

   Sean $(q_i^{m_{ij}})_{1\leq i\leq k}^{1\leq j\leq r_i}$ los divisores elementales de M con $p = q_1$ y por tanto $r = r_1$ y $n_j = m_{1j}$, hay un isomorfismo $\phi : \bigoplus_{i=1}^k \bigoplus_{j=1}^{m_{ir_i}} \frac{A}{(q_i^{m_{ij}})} \to M$, pero

$$X \coloneqq \operatorname{ann}_{\bigoplus_{i=1}^k \bigoplus_{j=1}^{m_{ir_i}} \frac{A}{(q_i^{m_{ij}})}}(p^{n_r}) = \bigoplus_{j=1}^{n_r} \frac{A}{(p^{n_j})}$$

   ya que, si $i \neq 1$, $\operatorname{ann}_{\frac{A}{(q_i^s)}}(p^{n_j}) = 0$ al ser $p^{n_j} + (q_i^s)$ una unidad de $\frac{A}{(p_h^s)}$, de modo que

$$\operatorname{ann}_M(p^{n_r}) = \phi(X) = \phi\left(\bigoplus_{j=1}^{n_r} \frac{A}{(p^{n_j})}\right) = M(p).$$

Sean ${}_AM \neq 0$ finitamente generado de torsión, $p \in \mathcal{P}$ un divisor irreducible de M y, para $h \in \mathbb{N}^*$, μ_h el número de divisores elementales de M iguales a p^h:

1. Para $h \in \mathbb{N}^*$, $\frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$ es un $\frac{A}{(p)}$-espacio vectorial.

   Como p es primo en un DIP, (p) es maximal, luego $\frac{A}{(p)}$ es un cuerpo, y el resultado se sigue de que p anula a $\frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$.

2. Para $h \in \mathbb{N}^*$, si $\delta_h \coloneqq \dim_{\frac{A}{(p)}} \frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$, $\mu_h = \delta_h - \delta_{h+1}$.

   Sea $n \coloneqq \min\{s > 0 \mid \operatorname{ann}_M(p^s) = \operatorname{ann}_M(p^{s+1})\}$. Para $h > n$, $\mu_h = 0$ y, como $\operatorname{ann}_M(p^{s-1}) = \operatorname{ann}_M(p^s) = \operatorname{ann}_M(p^{s+1})$, $\delta_h = \delta_{h+1}$.

   Sea ahora $h \leq n$. Si $\{p = p_1, \ldots, p_k\}$ son los divisores irreducibles (distintos) de M, entonces $\operatorname{ann}_M(p^h) = \bigoplus_{i=1}^k \operatorname{ann}_{M(p_i)}(p^h)$. En efecto, si $x \in \operatorname{ann}_{M(p_i)}(p^h)$, $p^h x = 0$ en $M(p_i)$ y por tanto en M, y si $x \in \operatorname{ann}_M(p^h)$, si $x =: x_1 + \cdots + x_k$ con cada $x_i \in M(p_i)$, entonces $0 = p^h x = p^h x_1 + \cdots + p^h x_k$ y cada $p^h x_i = 0$, luego $x \in \bigoplus_{i=1}^k \operatorname{ann}_{M(p_i)}(p^h)$. Pero para $i > 1$, si $x \in \operatorname{ann}_{M(p_i)}(p^h)$, $p^h x = 0$, $x \in M(p)$ y $x \in M(p) \cap M(p_i) = 0$, luego $\operatorname{ann}_{M(p_i)}(p^h) = 0$ y queda $\operatorname{ann}_M(p^h) = \operatorname{ann}_{M(p)}(p^h)$, con lo que podemos suponer $M = M(p)$.

   Para $h \in \{1, \ldots, n\}$, como

$$M \cong \bigoplus_{i=1}^n \left(\frac{A}{(p^i)}\right)^{\mu_i} =: M' \oplus \left(\frac{A}{(p^h)}\right)^{\mu_h} \oplus \cdots \oplus \left(\frac{A}{(p^n)}\right)^{\mu_n},$$

se tiene

$$\operatorname{ann}_M(p^{n-h}) = M' \oplus \left(\frac{A}{(p^h)}\right)^{\mu_h} \oplus \left(\frac{(p)}{(p^{h+1})}\right)^{\mu_{h+1}} \oplus \cdots \oplus \left(\frac{(p^{n-h})}{(p^n)}\right)^{\mu_n},$$
$$\operatorname{ann}_M(p^{n-h-1}) = M' \oplus \left(\frac{(p)}{(p^h)}\right)^{\mu_h} \oplus \left(\frac{(p^2)}{(p^{h+1})}\right)^{\mu_{h+1}} \oplus \cdots \oplus \left(\frac{(p^{n-h+1})}{(p^n)}\right)^{\mu_n}.$$

El sumando directo M'' se cancela en $\frac{\operatorname{ann}_M(p^{n-h})}{\operatorname{ann}_M(p^{n-h-1})}$ y cada

$$\frac{\left(\frac{(p^i)}{(p^{h+i})}\right)^{\mu_{h+i}}}{\left(\frac{(p^{i+1})}{(p^{h+i})}\right)^{\mu_{h+i}}} \cong \left(\frac{(p^i)}{(p^{i+1})}\right)^{\mu_{h+i}} \cong \left(\frac{A}{(p)}\right)^{\mu_{h+i}},$$

con lo que $\frac{\operatorname{ann}_M(p^{n-h})}{\operatorname{ann}_M(p^{n-h-1})} \cong \left(\frac{A}{(p)}\right)^{\mu_h+\mu_{h+1}+\cdots+\mu_n}$ y $\delta_h = \sum_{i=h}^n \mu_i$, de donde se obtiene $\mu_h = \delta_h - \delta_{h+1}$.

Sean A un anillo arbitrario, $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n$ una cadena de A-módulos y, para $i \in \{1, \ldots, n\}$, $X_i \subseteq M_i$ tal que $\frac{M_i}{M_{i-1}} = (\overline{X_i})$, entonces $M_n = (\bigcup_{i=1}^n X_i)$. **Demostración:** Si $n = 0$ es obvio. Si $n = 1$, la proyección canónica $M_1 \to \frac{M_1}{M_0}$ es un isomorfismo y ya estaría. Si $n > 1$, probado esto para $n-1$, para $x \in M_n$, $\overline{x} \in \frac{M_n}{M_{n-1}}$ se escribe como $\overline{x} = \sum_{y \in X_n} a_y \overline{y}$ con los $a_y \in A$ casi todos nulos, de modo que $x' \coloneqq x - \sum_{y \in X_n} a_y y \in M_{n-1}$ y, como $x' \in (\bigcup_{i=1}^{n-1} X_i)$, $x \in (\bigcup_{i=1}^n X_i)$.

Como **teorema**, si ${}_AM$ es finitamente generado de torsión, p es un divisor irreducible de M, $n \coloneqq \min\{s \in \mathbb{N}^* \mid \operatorname{ann}_M(p^s) = \operatorname{ann}_M(p^{s+1})\}$ y $(F_h)_{h=1}^n$ es una familia de subconjuntos de $M(p)$ tal que cada $F_h \subseteq \operatorname{ann}_M(p^h)$ y cada $F_h \cup pF_{h+1} \cup \cdots \cup p^{n-h}F_n$ es una unión disjunta que induce una base de $\frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$ como $\frac{A}{(p)}$-espacio vectorial:

1. $\forall x \in \bigcup_{i=1}^n F_h, Ax \cong \frac{A}{(p^h)} \iff x \in F_h$.

   $Ax \cong \frac{A}{(p^h)}$ si y sólo si $\operatorname{ann}_A(x) = p^h$. Ahora bien, si $x \in F_h \subseteq \operatorname{ann}_M(p^h)$, $p^h \in \operatorname{ann}_A(x)$ y $(p^h) \subseteq \operatorname{ann}_A(x)$, pero si $a \in \operatorname{ann}_A(x)$, tomando $a =: p^s b$ con $s \in \mathbb{N}$ y $b \nmid p$, si fuera $s < h$, $\overline{p^s x} \in p^s F_h$ es elemento de una base de $\frac{\operatorname{ann}_M(p^{h-s})}{\operatorname{ann}_M(p^{h-s-1})}$, y como $ax = 0$ y por tanto $\overline{bp^s x} = \overline{ax} = 0$, se tiene $\overline{b} = 0$ y $b \in (p)\#$, de modo que $s \geq h$, $a \in (p^h)$ y $\operatorname{ann}_A(x) \subseteq (p^h)$.

2. $M(p) = \bigoplus_{h=1}^n \bigoplus_{x \in F_h} Ax$.

   $0 = \operatorname{ann}_M(p^0) \subseteq \operatorname{ann}_M(p^1) \subseteq \cdots \subseteq \operatorname{ann}_M(p^n) = M(p)$, y si $X_h \coloneqq F_h \cup pF_{h+1} \cup \cdots \cup p^{n-h}F_n$, cada $\overline{X_h}$ genera $\frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$ y $X \coloneqq \bigcup_{h=1}^n X_h$ genera $M(p)$, pero $X \subseteq (\bigcup_{i=1}^n F_i) = \sum_{i=1}^n \sum_{x \in F_i} Ax$ y por tanto $M(p) = \sum_{h=1}^n \sum_{x \in F_h} Ax$. Para ver que la suma es directa, si $n = 1$, $M(p) = \operatorname{ann}_M(p)$ es un espacio vectorial con base F_1 ya que la proyección canónica $\operatorname{ann}_M(p) \to \frac{\operatorname{ann}_M(p)}{\operatorname{ann}_M(1)}$ es un isomorfismo. Si $n > 1$, probado esto para $n-1$, sea $\sum_{h=1}^n \sum_{x \in F_h} a_x x = 0$, $\sum_{x \in F_n} a_x x = -\sum_{h=1}^{n-1} \sum_{x \in F_h} a_x x \in (\bigcup_{h=1}^{n-1} F_h) \subseteq \operatorname{ann}_M(p^{n-1})$, pero F_n induce una base del $\frac{A}{(p)}$-espacio vectorial $\frac{\operatorname{ann}_M(p^n)}{\operatorname{ann}_M(p^{n-1})}$ y, como $\sum_{x \in F_n} \overline{a_x x} = 0 \in \frac{\operatorname{ann}_M(p^n)}{\operatorname{ann}_M(p^{n-1})}$, cada $a_x \in (p)$ y, llamando $a_x \coloneqq pa'_x$, $\sum_{x \in F_n} a'_x(px) + \sum_{x \in \bigcup_{h=1}^{n-1} F_h} a_x x = 0$,

pero llamando $F'_h \coloneqq F_h$ para $h < n-1$ y $F'_{n-1} \coloneqq F_{n-1} \cup pF_n$, $(F'_h)_{h=1}^{n-1}$ cumple respecto a $\operatorname{ann}_M(p^{n-1})$ las mismas propiedades de $(F_h)_{h=1}^n$ para $M(p)$, y por hipótesis de inducción los submódulos $\{Apx\}_{x\in F_n} \cup \bigcup_{h=1}^{n-1}\{Ax\}_{x\in F_h}$ son independientes, con lo que los a_x son todos nulos.

3. $|F_h|$ es el número de divisores elementales de M iguales a p^h.

   $M(p) \cong \bigoplus_{h=1}^n \bigoplus_{x\in F_h} \frac{A}{(p^h)} = \bigoplus_{h=1}^n \left(\frac{A}{(p^h)}\right)^{|F_h|}$.

4. Podemos encontrar tal familia tomando una base $(\overline{x_i})_i$ de $\frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$, haciendo $F_n \coloneqq \{x_i\}_i$ y, para h de $n-1$ hasta 1, completando el conjunto linealmente independiente de $\frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$ inducido por $pF_{h+1} \cup p^2F_{h+2} \cup \cdots \cup p^{n-h}F_n$ con vectores $(\overline{x_i})_i$ para formar una base y haciendo $F_h \coloneqq \{x_i\}_i$.

   Para $h = n$, la F_n definida cumple las propiedades. Si $h < n$ y $F_{h+1}, \ldots, F_n$ cumplen las propiedades, $pF_{h+1} \cup \cdots \cup p^{n-h}F_n$ es una unión disjunta ya que, si hubiera $i, j \in \{h+1, \ldots, n\}$ con $i < j$ y $p^{i-h}F_i \cap p^{j-h}F_j \neq \emptyset$, sean $x \in F_i$ e $y \in F_j$ con $p^{i-h}x = p^{j-h}y$, de modo que $p^{i-h}(x - p^{j-i}y) = 0$, entonces $x - p^{j-i}y \in \operatorname{ann}_M(p^{j-h}) \subseteq \operatorname{ann}_M(p^{j-1})$, pero x y $p^{j-i}y$ son elementos de una base de $\frac{\operatorname{ann}_M(p^j)}{\operatorname{ann}_M(p^{j-1})}$#. Además, $\phi : \frac{\operatorname{ann}_M(p^{h+1})}{\operatorname{ann}_M(p^h)} \rightarrowtail \frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$ dado por $\phi(\overline{z}) \coloneqq p\overline{z}$ es un monomorfismo ya que $p\overline{z} = 0 \iff pz \in \operatorname{ann}_M(p^{h-1}) \iff z \in \operatorname{ann}_M(p^h) \iff \overline{z} = 0$, y como $F_{h+1} \cup \cdots \cup p^{n-h-1}F_n$ induce una base de $\frac{\operatorname{ann}_M(p^{h+1})}{\operatorname{ann}_M(p^h)}$, $pF_{h+1} \cup \cdots \cup p^{n-h}F_n$ induce una familia linealmente independiente en $\frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})}$. Completamos esta familia para formar una base y ahora la unión sigue siendo disjunta por inducir una base.

4.6. Descomposiciones en dominios euclídeos

GyA

Dado un dominio $D \neq 0$, una función $\delta : D \setminus \{0\} \to \mathbb{N}$ es **euclídea** si cumple:

1. $\forall a, b \in D \setminus \{0\}, (a \mid b \implies \delta(a) \leq \delta(b))$.
2. $\forall a \in D, b \in D \setminus \{0\}, \exists q, r \in D \mid (a = bq + r \wedge (r = 0 \vee \delta(r) < \delta(b)))$.

Un **dominio euclídeo** es uno que admite una función euclídea.

1. El valor absoluto es una función euclídea en $\mathbb{Z}$.
2. El cuadrado del módulo complejo es una función euclídea en $\mathbb{Z}[i]$.

Sean δ una función euclídea en D, I un ideal de D y $a \in I \setminus \{0\}$, entonces

$$I = (a) \iff \forall x \in I \setminus \{0\}, \delta(a) \leq \delta(x).$$

[...] Todo dominio euclídeo es DIP. Si δ es una función euclídea en D, un elemento $a \in D$ es una unidad si y sólo si $\delta(a) = \delta(1)$, si y sólo si $\forall x \in D \setminus \{0\}, \delta(a) \leq \delta(x)$.

Como **teorema**, sean A un dominio euclídeo, $C \in \mathcal{M}_{m\times n}(A)$ y $A^r \oplus \bigoplus_{i=1}^t \frac{A}{(d_i)}$ la descomposición invariante externa de $M(C)$, C es equivalente a

$$\begin{pmatrix} \boxed{I_{m-r-t}} & & & \\ & d_1 & & \\ & & \ddots & \\ & & & d_t \\ & & & \end{pmatrix} \in \mathcal{M}_{m\times n}(A),$$

llamada **forma normal** de C y a la que se puede llegar desde C por transformaciones elementales. **Demostración:** Primero vemos que C se puede llevar a una matriz D de la forma dada con $d_1 \mid \cdots \mid d_t$ y luego que $M(D)$ tiene la descomposición invariante indicada, y el resultado se obtiene de que $M(C) \cong M(D)$ y de la unicidad de la descomposición invariante. Para lo primero, si $C = 0$, $m = 0$ o $n = 0$ no hay que hacer nada. En otro caso, sean $\mathcal{C} \subseteq \mathcal{M}_{m\times n}(A)$ el conjunto de matrices alcanzables desde C por transformaciones elementales en filas y columnas, $\delta : A \setminus \{0\} \to \mathbb{N}$ una función euclídea y $X \in \mathcal{C}$ e índices i, j con $\delta_0 \coloneqq \delta(X_{ij})$ mínimo, por intercambio de filas 1 e i y de columnas 1 y j podemos suponer $i = j = 1$. Para $j \in \{2, \ldots, n\}$, si fuera $X_{11} \nmid X_{1j}$ sería $X_{1j} =: qX_{11} + r$ con $r \neq 0$ y $\delta(r) < \delta(X_{11})$, pero restando a la columna j la primera por q_{1j} quedaría una matriz X' con $\delta(X'_{1j}) < \delta(X_{11}) = \delta_0\#$, de modo que $X_{11} \mid X_{1j}$ para todo j y, análogamente, $X_{11} \mid X_{1i}$ para todo i. Si ahora definimos q_i y s_j de modo que cada $X_{i1} = q_i X_{11}$ y cada $X_{1j} = s_j X_{11}$, restando a la fila i la primera por q_i y a la columna j la primera por s_j queda una matriz

$$Y = \left(\begin{array}{c|c} X_{11} & 0 \\ \hline 0 & B \end{array}\right),$$

pero para $i, j \geq 2$, si fuera $X_{11} \nmid Y_{ij}$, sumando a la primera fila la i-ésima quedaría una matriz Z con $Z_{11} = X_{11}$ y $Z_{1j} = Y_{1j}$, con lo que $Z_{1j} = qZ_{11} + r$ con $r \neq 0$ y $\delta(r) < \delta(Z_{11}) = \delta(X_{11}) = \delta_0$, y restando a la i-ésima fila la primera por q se obtendría una matriz Z' con $\delta(Z'_{1j}) < \delta_0\#$. Por tanto X_{11} divide a todo elemento de B, y si $B =: XB'$, por inducción B' es semejante a una matriz de la forma original y por tanto B también lo es e $Y_{11} \mid Y_{22} \mid \ldots$, pero como los Y_{ii} nulos están al final de la «diagonal» y los invertibles están al principio, si hay digamos k invertibles, multiplicando Y por $\operatorname{diag}(Y_{11}^{-1}, \ldots, Y_{kk}^{-1}, 1, \ldots, 1)$ se obtiene la matriz D. Para la segunda parte, sean $s \coloneqq m - r - t$, $(e_i)_{i=1}^n$ la base canónica de A^n y $(f_i)_{i=1}^m$ la de A^m, $f_D \coloneqq (v \mapsto Dv) : A^n \to A^m$ lleva a cada e_i a f_i para $i \in \{1, \ldots, s\}$, a cada e_{s+i} a $d_i f_{s+i}$ para $i \in \{1, \ldots, t\}$ y al resto de elementos de la base canónica a 0, luego descomponiendo $A^n = A^s \oplus A^t \oplus A^{n-s-t}$ y $A^m = A^s \oplus A^t \oplus A^r$ se puede descomponer $f_D = 1_{A^s} \oplus \left(\bigoplus_{i=1}^t (a \mapsto d_i a)\right) \oplus 0$ con $0 : A^{n-s-t} \to A^r$ y

$$\frac{A}{M(D)} = \frac{A}{\operatorname{Im} f_D} \cong \frac{A^s}{A^s} \oplus \left(\bigoplus_{i=1}^t \frac{A}{(d_i)}\right) \oplus \frac{A^r}{0} \cong A^r \oplus \bigoplus_{i=1}^t \frac{A}{(d_i)}$$

con $d_1 \mid \cdots \mid d_t$.

Si A es un dominio euclídeo:

1. La forma normal de $P \in \mathrm{GL}_k(A)$ es I_k.

   Es de la forma $\mathrm{diag}(1,\dots,1,d_1,\dots,d_t,0,\dots,0)$ con los d_i no invertibles, pero es invertible y una matriz diagonal invertible debe tener todos los elementos de la diagonal invertibles.

2. Si $C, D \in \mathcal{M}_{m\times n}(A)$ son equivalentes, es posible llegar de C a D por transformaciones elementales en filas y columnas.

   Existen matrices invertibles P y Q con $D = PCQ$, pero desde P o Q se puede llegar a su forma normal, que es la identidad, por transformaciones elementales, de modo que P y Q son productos de matrices elementales.

4.7. Presentaciones de grupos abelianos finitamente generados

Una **presentación** de un grupo abeliano finitamente generado M es una expresión

$$(x_1,\dots,x_m/\rho_1,\dots,\rho_n),$$

donde los x_i son variables o **generadores** y los $\rho_j = \sum_{i=1}^m c_{ij}x_i$ son $\mathbb{Z}$-combinaciones lineales de dichas variables o **relatores**, de forma que $M \cong \frac{F}{N}$ siendo F el grupo abeliano libre con base $\{x_1,\dots,x_n\}$ y N su subgrupo generado por los ρ_j, o equivalentemente, $M \cong M(C)$ para $C = (c_{ij}) \in \mathcal{M}_{m\times n}(\mathbb{Z})$. **Demostración:** Existe un único homomorfismo $f : \mathbb{Z}^n \to F$ que lleva cada e_j de la base canónica de $\mathbb{Z}^n$ a ρ_j, con lo que $\mathrm{Im}f = N$, y un único isomorfismo $\phi : F \to \mathbb{Z}^m$ que lleva cada x_i al elemento $\hat{e}_i$ de la base canónica de $\mathbb{Z}^m$, con lo que $\phi \circ f$ lleva cada e_j a $(c_{1j},\dots,c_{mj})$ y por tanto cada $v \in \mathbb{Z}^n$ a Cv y $M(C) = \frac{\mathbb{Z}^m}{\mathrm{Im}(\phi\circ f)} = \frac{\phi(F)}{\phi(N)} \cong \frac{F}{N}$.

Para encontrar la estructura de un grupo abeliano finitamente generado a partir de su presentación por generadores y relatores:

1. Usar transformaciones elementales sobre la matriz C asociada a la presentación hasta llegar a su forma normal $D = PCQ$.

2. Obtener el rango libre de torsión de D.

3. Obtener los factores invariantes d_j de D y usar el teorema chino de los restos para factorizar cada $\mathbb{Z}_{d_j}$ en producto finito de grupos abelianos de la forma $\mathbb{Z}_{p_i^{n_{ij}}}$.

4. Una vez obtenida de aquí la descomposición primaria externa, convertirla trivialmente en descomposición primaria interna de $M(D)$.

5. Multiplicar cada sumando directo en esta descomposición por P^{-1}, obteniendo una descomposición directa interna de $M(P^{-1}D) = M(CQ) = M(C)$.

Llamamos **determinante** del endomorfismo $g : \mathbb{Z}^n \to \mathbb{Z}^n$, $\det g$, a $\det M_{\mathcal{BB}}(g)$ para cualquier base $\mathcal{B}$ de $\mathbb{Z}^n$, que no depende de la base elegida, y entonces $\frac{\mathbb{Z}^n}{\mathrm{Im}g}$ es finito si y sólo si $\det g \neq 0$, en cuyo caso su orden es el valor absoluto de $\det g$.

Capítulo 5

Endomorfismos vectoriales en dimensión finita

Sean K un cuerpo y M el $K[X]$-módulo asociado a un par (V, f) de un espacio vectorial y un K-endomorfismo $V \to V$, M es de torsión finitamente generado si y sólo si ${}_KV$ es de dimensión finita, y si $p \in K[X]$ es irreducible, M es finitamente generado de p-torsión si y sólo si ${}_KV$ es de dimensión finita y $p(f)^m = 0 \in \mathrm{End}_K(V)$ para cierto $m > 0$.

En el resto de la sección, salvo que se indique lo contrario, K es un cuerpo, V un K-espacio vectorial de dimensión finita, $f : V \to V$ un K-endomorfismo y M el $K[X]$-módulo asociado a (V, f).

Teoremas de clasificación de endomorfismos de espacios vectoriales:

1. Existen $p_1, \ldots, p_k \in K[X]$ mónicos irreducibles distintos y $n_{ij} \in \mathbb{N}^*$ para $i \in \{1, \ldots, k\}$ y $j \in \{1, \ldots, r_i\}$, unívocamente determinados, y vectores $v_{ij} \in V$, tales que

$$\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} K\{f^s(v_{ij})\}_{s\geq 0}$$

es una descomposición de V en suma directa interna de subespacios vectoriales f-invariantes y cada $p_i(f)^{n_{ij}}(v_{ij}) = 0 \neq p_i(f)^{n_{ij}-1}(v_{ij})$.

Sean $W \leq V$ y N el $K[X]$-submódulo de M asociado a $(W, f|_W)$, basta ver que $N \cong \frac{K[X]}{(p_i^{n_{ij}})}$ si y sólo si existe $v \in V$ tal que $W = K\{f^s(v)_{s\geq 0}\}$ y $p_i(f)^{n_{ij}}(v) = 0 \neq p_i(f)^{n_{ij}-1}(v)$.

$\Longrightarrow$] Sean $\phi : \frac{K[X]}{(p_i^{n_{ij}})} \to N$ el isomorfismo y $v \coloneqq \phi(\overline{1})$, $p_i^{n_{ij}}\overline{1} = 0$ y por tanto $0 = p_i^{n_{ij}}\phi(\overline{1}) = p_i^{n_{ij}}v = p_i(f)^{n_{ij}}(v)$ por la definición del $K[X]$-módulo, pero $p_i^{n_{ij}-1}\overline{1} \neq 0$ y por tanto $p_i(f)^{n_{ij}-1}(v_{ij}) \neq 0$. Finalmente, como $\frac{K[X]}{(p_i^{n_{ij}})} = K\{\overline{1}, X\overline{1}, \ldots, X^s\overline{1}, \ldots\}$, $M = K\{f^s(v)\}_{s\geq 0}$ ya que $\phi(X^s\overline{1}) = X^s\phi(\overline{1}) = f^s(v)$.

$\Longleftarrow$] Por la hipótesis y la definición de N, $N = (v)$, pero v es anulado por $p_i(f)^{n_{ij}}$ y por tanto hay un epimorfismo $\psi : \frac{K[X]}{(p_i^{n_{ij}})} \twoheadrightarrow K[X]v = N$ con $\ker\psi \trianglelefteq \frac{K[X]}{(p_i^{n_{ij}})}$, pero los

únicos ideales de $\frac{K[X]}{(p_i^{n_{ij}})}$ son $(\overline{p_i}^k)$ con $k \in \{0, \dots, n_{ij}\}$, y como $p_i(f)^{n_{ij}-1}(v) \neq 0$, $\overline{p_i}^{n_{ij}-1} \notin \ker \psi$, con lo que $\ker \psi = 0$ y ψ es un isomorfismo.

2. Existen polinomios mónicos no constantes $d_1 \mid \cdots \mid d_t$ unívocamente determinados y vectores $v_j \in V$ tales que $\bigoplus_{i=1}^t \operatorname{span}\{f^s(v_j)\}_{s \in \mathbb{N}_{\operatorname{gr}(d_j)}}$ es una descomposición de V en subespacios f-invariantes y cada $d_j(f)(v_j) = 0$.

   Sean $W \leq V$ y N el $K[X]$-submódulo de M asociado a $(W, f|_W)$, basta ver que $N \cong \frac{K[X]}{(d_j)}$ si y sólo si existe $v \in V$ tal que $\{f^s(v)\}_{s \in \mathbb{N}_{\operatorname{gr}(d_j)}}$ es base de W como K-espacio vectorial y $d_j(f)(v) = 0$.

   $\Longrightarrow$] Sean $\phi : \frac{K[X]}{(p_i^{n_{ij}})} \to N$ el isomorfismo y $v \coloneqq \phi(\overline{1})$, $d_j\overline{1} = 0$ y por tanto $0 = d_j\phi(\overline{1}) = d_j v = d_j(f)(v)$, y como $\frac{K[X]}{(d_j)} = K\{\overline{1}, X\overline{1}, \dots, X^{\operatorname{gr} d_j - 1}\overline{1}\}$ con $(X^s\overline{1})_{s \in \mathbb{N}_{\operatorname{gr}(d_j)}}$ linealmente independiente, $N = K\{f^s(v)\}_{s \in \mathbb{N}_{\operatorname{gr}(d_j)}}$ con $(f^s(v))_{s \in \mathbb{N}_{\operatorname{gr}(d_j)}}$ linealmente independiente.

   $\Longleftarrow$] v es anulado por $p_i(f)^{n_{ij}}$ y por tanto hay un epimorfismo $\psi : \frac{K[X]}{(d_j)} \twoheadrightarrow K[X]v = K\{f^s(v)\}_{s \in \mathbb{N}} = K\{f^s(v)\}_{s \in \mathbb{N}_{\operatorname{gr}(d_j)}} = N$, pero si $p \in K[X]$ con $\operatorname{gr} p < \operatorname{gr} d_j$ cumple $\psi(\overline{p}) = p(f)(v) = \sum_i p_i f^i(v) = 0$, como los $f^i(v)$ son linealmente independiente, cada $p_i = 0$ y $p = 0$, y como cada elemento de $\frac{K[X]}{(d_j)}$ tiene un representante de grado menor que el de d_j, $\ker \psi = 0$ y ψ es un isomorfismo.

5.1. Polinomio mínimo

Sea $\varphi \in K[X]$ el polinomio característico de f:

1. **Teorema de Cayley-Hamilton:** $\varphi(f) = 0$.

   Sean $C \in \mathcal{M}_n(K)$ la matriz asociada a f bajo cualquier base de V e $I \coloneqq I_n$, queremos ver que $\varphi = \det(XI - C)$ cumple $\sum_{i=0}^n \varphi_i C^i = 0$. Por la prueba de la fórmula de la matriz inversa, para toda matriz A es $A \cdot \operatorname{adj}(A)^\intercal = |A|I$, por lo que viendo $XI - C \in \mathcal{M}_n(K[X])$ es $(XI - C)\operatorname{adj}(XI - C)^\intercal = \varphi I$. Como las entradas de $\operatorname{adj}(XI - C)^\intercal$ son polinomios de grado máximo $n-1$, podemos escribir $\operatorname{adj}(XI - C)^t =: \sum_{i=0}^{n-1} B_i X^i$ con cada $B_i \in \mathcal{M}_n(K)$ y entonces $(XI - C)\sum_{i=0}^{n-1} B_i X^i = \sum_{i=0}^n \varphi_i I$. Viendo esta igualdad en $\mathcal{M}_n(K)[X]$, igualando coeficientes,

   $$B_{n-1} = \varphi_n I, \quad B_{n-2} - CB_{n-1} = \varphi_{n-1} I, \quad \cdots, \quad B_0 - B_1 C = \varphi_1 I, \quad -B_0 C = \varphi_0 I,$$

   y multiplicando la primera igualdad por C^n, la segunda por C^{n-1}, etc.,

   $$\begin{aligned} C^n B_{n-1} &= \varphi_n C^n, & C^{n-1}B_{n-2} - C^n B_{n-1} &= \varphi_{n-1} C^{n-1}, & &\dots, \\ CB_0 - C^2 B_1 &= \varphi_1 C, & -CB_0 &= \varphi_0 I, \end{aligned}$$

   luego sumando es $0 = \varphi_n C^n + \cdots + \varphi_1 C + \varphi_0 = \varphi_C(C)$.

2. Los divisores irreducibles de M son precisamente los divisores irreducibles de φ.

$p \in K[X]$ irreducible es divisor irreducible de M si y sólo si existe $v \in M \setminus \{0\}$ con $pv = p(f)(v) = 0$, si y sólo si $\ker(p(f)) \neq 0$, si y sólo si $p(f) : V \to V$ como endomorfismo no es un isomorfismo, si y sólo si $\det(p(f)) = 0$. Sea $\overline{K}$ la clausura algebraica de K, $p = (X - \lambda_1) \cdots (X - \lambda_t) \in \overline{K}[X]$. Si $p \mid \varphi$, sea C la matriz asociada a f bajo cualquier base, los λ_i son valores propios de C en $\overline{K}$ y por tanto existen $v_i \in \overline{K}^n \setminus \{0\}$ con $Cv_i = \lambda v_i$ y $(C - \lambda_i I) = 0$. Pero $(C - \lambda_i I)(C - \lambda_j I) = C^2 - \lambda_i I - \lambda_j I + \lambda_i \lambda_j I = (C - \lambda_j I)(C - \lambda_i I)$, por lo que $(C - \lambda_i I)(C - \lambda_j I)(v_i) = 0$ y $p(C)(v) = \left(\prod_j (C - \lambda_j I)\right)(v_i) = 0$, de modo que $\ker_{\overline{K}}(p(C)) \neq 0$ y $\det(p(C)) = 0$, lo que no depende de si consideramos $p(C)$ sobre K o sobre $\overline{K}$ y por tanto p es divisor irreducible de M. Si p es divisor irreducible de M, divide al mayor factor invariante de M, d_t, pero para $v \in M$, $\varphi v = \varphi(f)(v) = 0$, con lo que $\varphi \in \operatorname{ann}_A(M) = (d_t)$ y $p \mid d_t \mid \varphi$.

AlgL

$A, B \in \mathcal{M}_n(K)$ son **semejantes** si $\exists P \in \mathcal{M}_n(K) : B = P^{-1}AP$.

Sean $\mathcal{B}$ una base de V, $C \coloneqq M_{\mathcal{B}}(f)$ y $f_C : K^n \to K^n$ dado por $f_C(y) \coloneqq Cy$:

1. El isomorfismo $\phi : V \to K^n$ que lleva $\mathcal{B}$ a la base canónica induce un isomorfismo entre el $K[X]$-módulo asociado a (V, f) y el asociado a (K^n, f_C).

   Claramente la biyección $\hat{\phi}$ inducida conserva la suma y el producto por escalares de K, y $\hat{\phi}(Xv) = \phi(f(v)) = \phi((\phi^{-1} \circ f_C \circ \phi)(v)) = f_C(\phi(v)) = X\phi(v)$.

2. Sean W otro K-espacio vectorial, $g : W \to W$ un K-endomorfismo, $\phi : V \to W$ un K-isomorfismo con $\phi \circ f = g \circ \phi$, $\mathcal{B}$ una base de V y $\mathcal{B}'$ la base correspondiente de W por ϕ, se tiene$M_{\mathcal{B}}(f) = M_{\mathcal{B}'}(g)$.

   Si $\mathcal{B} =: (b_i)_i$, $\mathcal{B}' = (\phi(b_i))_i$, pero $M_{\mathcal{B}}(f)$ tiene como columnas los $f(b_i)$ respecto de $\mathcal{B}$ y $M_{\mathcal{B}'}(g)$ tiene como columnas los $g(\phi(b_i)) = \phi(f(b_i))$ respecto de $\mathcal{B}'$, por lo que $M_{\mathcal{B}}(f) = M_{\mathcal{B}'}(g)$.

3. Si W es otro K-espacio vectorial de dimensión finita y $g : W \to W$ un K-endomorfismo, los $K[X]$-módulos asociados a (V, f) y (W, g) son isomorfos si y sólo si $\dim V = \dim W$ y existen bases respectivas $\mathcal{B}$ y $\mathcal{B}'$ de V y W tales que $M_{\mathcal{B}}(f)$ y $M_{\mathcal{B}'}(g)$ son semejantes.

   $\Longrightarrow$] Sea $\phi : M \to N$ el isomorfismo, claramente $\phi : V \to W$ es un K-isomorfismo y por tanto $\dim_K V = \dim_K W$, y basta tomar una base $\mathcal{B}$ de V y, como $\phi(f(v)) = \phi(Xv) = X\phi(v) = g(\phi(v))$, estamos en las condiciones del anterior apartado.

   $\Longleftarrow$] Por cambio de base podemos suponer $M_{\mathcal{B}}(f) = M_{\mathcal{B}'}(g) =: (a_{ij})_{1 \leq i,j \leq n}$, y si $\mathcal{B} = (b_1, \ldots, b_n)$ y $\mathcal{B}' = (b'_1, \ldots, b'_n)$, tomando el isomorfismo vectorial $\phi : V \to W$ que lleva cada b_i a b'_i y viéndolo como un $K[X]$-isomorfismo $\phi : M \to N$, $\phi(Xb_i) = \phi(f(b_i)) = \phi(\sum_j a_{ji} b_j) = \sum_j a_{ji} b'_j = g(b'_i) = X\phi(b_i)$.

Si A es una matriz cuadrada, llamamos $\operatorname{rk} A$ al rango de A, y si $f : V \to V$ es un endomorfismo, $\operatorname{rk} f \coloneqq \operatorname{rk} M_{\mathcal{B}}(f)$ para cualquier base $\mathcal{B}$ de V.

Llamamos **polinomio mínimo** de M a su mayor factor invariante, elegido mónico.

1. Para $G \in K[X]$ y $j \in \mathbb{N}$,$\operatorname{ann}_M(G^j) = \ker(G^j(f))$, y $G^j \in \operatorname{ann}_{K[X]}(M) \iff G^j(f) = 0$.
   $G^j \in \operatorname{ann}_{K[X]}(M) \iff \operatorname{ann}_M(G^j) = \ker(G^j(f)) = M \iff G^j(f) = 0$.

2. El polinomio mínimo de M es el menor $d_t \in K[X]$ (por divisibilidad) con $d_t(f) = 0$.
   Si este es d_t, $(d_t) = \operatorname{ann}_{K[X]}(M)$, y basta aplicar el apartado anterior.

3. Si φ es el polinomio característico de f, $d_t \mid \varphi$.
   $\varphi(f) = 0$.

4. Si p es divisor irreducible de M y $n \coloneqq \min\{s \in \mathbb{N} \mid \ker(p(f)^s) = \ker(p(f)^{s+1})\} = \min\{s \in \mathbb{N} \mid \operatorname{rk}(p(f)^s) = \operatorname{rk}(p(f)^{s+1})\}$, entonces $M(p) = \ker(p(f)^n)$.
   $\ker(p(f)^s) = \ker(p(f)^{s+1})$ implica $\operatorname{rk}(p(f)^s) = \operatorname{rk}(p(f)^{s+1})$, y el recíproco se cumple porque entonces $\dim\ker(p(f)^s) = \dim\ker(p(f)^{s+1})$ con $p(f)^s \subseteq p(f)^{s+1}$. Pero sabemos que $M(p) = \operatorname{ann}_M(p^{n_r}) = \ker(p(f)^{n_r})$ siendo $n_r = \min\{s \in \mathbb{N} \mid \operatorname{ann}_M(p^s) = \operatorname{ann}_M(p^{s+1})\} = n$.

5. La multiplicidad de p como factor irreducible de φ es $m \geq n$ y cumple $M(p) = \ker(p(f)^m)$.
   Sea $\varphi =: p^m G$ con $p \nmid G$, la identidad de Bézout $1 = p^m R + GS$ implica, evaluando en f sobre un $v \in V$, que

$$v = p(f)^m(R(f)(v)) + G(f)(S(f)(v)) = R(f)(p(f)^m(v)) + S(f)(G(f)(v)),$$

   y por el teorema de Cayley-Hamilton, $(p^m G)(f) = p^m(f) \circ G(f) = G(f) \circ p^m(f) = 0$ y entonces $p(f)^m(R(f)(v)) \in \ker(G(f))$ y $G(f)(S(f)(v)) \in \ker(p(f)^m)$, luego $V = \ker(p(f)^m) + \ker(G(f))$ y si $v \in \ker(p(f)^m) \cap \ker(G(f))$ la igualdad anterior nos da $v = 0 + 0 = 0$, con lo que la suma es directa y $V = \operatorname{ann}_M(p^m) \oplus \operatorname{ann}_M(G)$, de donde $M(p) = \operatorname{ann}_M(p^m) = \ker(p(f)^m)$ y, por la afirmación anterior, $m \geq n$.

6. Sea $V = V_1 \oplus \cdots \oplus V_t$ con los V_i f-invariantes, el polinomio mínimo de f es el mínimo común múltiplo de los polinomios mínimos de los $f|_{V_i} : V_i \to V_i$.
   Sean $\hat{f}_i \coloneqq f|_{V_i} : V_i \to V_i$, P el polinomio mínimo de f y Q_i el de $\hat{f}_i$, como $P(\hat{f}_i) = P(f)|_{V_i} = 0$, $Q_i \mid P$, y si $F \in K[X]$ es tal que $Q_1, \ldots, Q_t \mid F$, para $v \in V$, sea $v =: v_1 + \cdots + v_t$ con cada $v_i \in V_i$, entonces $f(v) = f(v_1) + \cdots + f(v_t) = \hat{f}_1(v_1) + \cdots + \hat{f}_t(v_t) = 0$, luego $F(f) = 0$ y $P \mid F$.

7. Si f es nilpotente, su polinomio característico es X^n con $n \coloneqq \dim V$.

8. Dados $f, g \in \operatorname{End}_K V$, las matrices asociadas a f y g son semejantes si y solo si f y g tienen el mismo polinomio característico con factorización irreducible $\varphi = p_1^{m_1} \cdots p_k^{m_k}$ y $\operatorname{rk}(p_i(f)^s) = \operatorname{rk}(p_i(g)^s)$ para todo i y $s \in \mathbb{N}^*$, si y sólo si tienen el mismo polinomio mínimo con factorización irreducible $d = p_1^{n_1} \cdots p_k^{n_k}$ y $\operatorname{rk}(p_i(f)^s) = \operatorname{rk}(p_i(g)^s)$ para todo i y $s \in \mathbb{N}^*$.

Que dos endomorfismos tengan el mismo polinomio característico y el mismo polinomio mínimo no implica que sus matrices asociadas bajo alguna base sean semejantes.

5.2. Formas canónicas

Para $F \in K[X]$ mónico de grado $n > 0$, llamamos **matriz compañera** de F a

$$C(F) \coloneqq \begin{pmatrix} & & & -F_0 \\ 1 & & & -F_1 \\ & \ddots & & \vdots \\ & & 1 & -F_{n-1} \end{pmatrix} \in \mathcal{M}_n(K),$$

y para $r > 0$ escribimos

$$C_r(F) = \begin{pmatrix} \boxed{C(F)} & \boxed{U} & & \\ & \ddots & \ddots & \\ & & \ddots & \boxed{U} \\ & & & \boxed{C(F)} \end{pmatrix} \in \mathcal{M}_{rn}(K),$$

donde

$$U \coloneqq \begin{pmatrix} & & 1 \\ & & \\ & & \end{pmatrix} \in \mathcal{M}_n(K).$$

El polinomio característico de un $C_r(F)$ es F^r. **Demostración:** Primero vemos que el de $C(F)$ es F. Para $n \coloneqq \mathrm{gr}F = 1$, $C(F) = (-F_0) \in \mathcal{M}_1(K)$ y $\det(XI - C(F)) = X + F_0 = F$. Para $n > 1$,

$$\begin{aligned} \det(XI - C(F)) &= \begin{vmatrix} X & & & F_0 \\ -1 & \ddots & & \vdots \\ & \ddots & X & F_{n-2} \\ & & -1 & X + F_{n-1} \end{vmatrix} = \\ &= X \begin{vmatrix} X & & & F_1 \\ -1 & \ddots & & \vdots \\ & \ddots & X & F_{n-2} \\ & & -1 & X + F_{n-1} \end{vmatrix} + (-1)^{n+1} F_0 \begin{vmatrix} -1 & X & & \\ & \ddots & \ddots & \\ & & \ddots & X \\ & & & -1 \end{vmatrix} = \\ &= X(F_1 + XF_2 + \cdots + X^{n-2}F_{n-1} + X^{n-1}F_n) + (-1)^{n+1}(-1)^{n-1}F_0 = F, \end{aligned}$$

donde para el primer sumando hemos usado la hipótesis de inducción. Para C_rF, el caso $r = 1$ está hecho, y para $r > 1$,

$$\det(XI - C_r(F)) = \begin{vmatrix} \boxed{C(F)} & \boxed{U} & & \\ & \ddots & \ddots & \\ & & \ddots & \boxed{U} \\ & & & \boxed{C(F)} \end{vmatrix} = \det(C(F)) \det(C_{r-1}(F)) = FF^{r-1} = F^r.$$

Sean $p \in K[X]$ un divisor irreducible del polinomio característico de f, $h \in \mathbb{N}^*$ y $\{v_1, \dots, v_t\} \subseteq \ker(p(f)^h)$, $(\overline{v_1}, \dots, \overline{v_t})$ es base de $\frac{\ker(p(f)^h)}{\ker(p(f)^{h-1})}$ como $\frac{K[X]}{(p)}$-espacio vectorial si y sólo si $\left(\overline{f^i(v_j)}\right)_{0\le i<d}^{1\le j\le t}$ es base de $\frac{\ker(p(f)^h)}{\ker(p(f)^{h-1})}$ como K-espacio vectorial. En particular, si $p \in K[X]$ es mónico irreducible con $p(f) = 0$ y $\{v_1, \dots, v_t\} \subseteq V$, $(v_1, \dots, v_t)$ es base de M como $\frac{K[X]}{(p)}$-espacio vectorial si y sólo si $(f^i(v_j))_{0\le i<d}^{1\le j\le t}$ es base del K-espacio vectorial V.

Sean $F \in K[X]$ un polinomio mónico de grado $n > 0$ y $r \in \mathbb{N}^*$, $M \cong \frac{K[X]}{(F^r)}$ si y sólo si existe $v \in V$ tal que $(f^s(v))_{s=0}^{rn-1}$ es base de v y $F(f)^r(v) = 0$, si y sólo si existe una base $\mathcal{B}$ de V con $M_{\mathcal{B}}(f) = C_r(F)$, en cuyo caso el polinomio mínimo de M coincide con el polinomio característico de f y es F^r.

$1 \implies 3]$ Sea $\tilde{\mathcal{B}}_j \coloneqq (\overline{F^j}, \overline{XF^j}, \dots, \overline{X^{n-1}F^j})$ para $j \in \{0, \dots, r-1\}$ y «$\star$» la concatenación de secuencias, $\tilde{\mathcal{B}} \coloneqq \tilde{\mathcal{B}}_{r-1} \star \cdots \star \tilde{\mathcal{B}}_1 \star \tilde{\mathcal{B}}_0$ es base de $\frac{K[X]}{(F^r)}$ como K-espacio vectorial. Para verlo, como $|\tilde{\mathcal{B}}| = rn = \dim \frac{K[X]}{(F^r)}$, basta ver que $\tilde{\mathcal{B}}$ es linealmente independiente. Si $r = 1$, $\tilde{\mathcal{B}} = (\overline{1}, \overline{X}, \dots, \overline{X}^{n-1})$ y el resultado es claro. Si $r > 1$, sea $\sum_{i=0}^{n-1}\sum_{j=0}^{r-1} \lambda_{ij} X^i F^j = 0 \in \frac{K[X]}{(F^r)}$ para ciertos $\lambda_{ij} \in K$, entonces $\sum_{ij} \lambda_{ij} X^i F^j = F^r G \in K[X]$ para cierto $G \in K[X]$, pero $\sum_{ij} \lambda_{ij} X^i F^j = \sum_{i=0}^{n-1} \lambda_{i0} X^i + F(\sum_{i=0}^{n-1}\sum_{j=1}^{r-1} \lambda_{ij} X^i F^j)$, luego debe ser $F \mid \sum_{i=0}^{n-1} \lambda_{i0} X^i$ y, como $\operatorname{gr} F = n$, $\sum_{i=0}^{n-1} \lambda_{i0} X^i = 0$ y cada $\lambda_{i0} = 0$. Pero entonces, dividiendo por F, $\sum_{i=0}^{n-1}\sum_{j=1}^{r-1} \lambda_{ij} X^i F^{j-1} = F^{r-1} G$ y por hipótesis de inducción todos los $\lambda_{ij} = 0$. Sea $g : \frac{K[X]}{(F^r)} \to \frac{K[X]}{(F^r)}$ el endomorfismo $G \mapsto XG$, queremos ver que $C \coloneqq M_{\mathcal{B}}(g) = C_r(F)$. Para $j \in \{0, \dots, r-1\}$, $g(\tilde{\mathcal{B}}_j) = (\overline{XF^j}, \overline{X^2F^j}, \dots, \overline{X^nF^j})$, pero

$$\overline{F^{j+1}} - \overline{X^nF^j} = \overline{(F - X^n)F^j} = \left(\sum_{i=0}^{n-1} F_i \overline{X^i}\right)\overline{F^j} = \sum_{i=0}^{n-1} F_i \overline{X^iF^j}$$

y por tanto

$$\overline{X^nF^j} = \overline{F^{j+1}} - \sum_{i=0}^{n-1} F_i \overline{X^iF^j}.$$

Entonces, para $j = r-1$, $\overline{F^{r+1}} = 0$ y las primeras n columnas de C solo tienen entradas no nulas en las primeras n filas y estas entradas son

$$\begin{pmatrix} & & -F_0 \\ 1 & & -F_1 \\ & \ddots & \vdots \\ & 1 & -F_{n-1} \end{pmatrix} = C(F),$$

mientras que para $j < r-1$, $\overline{F^{j+1}}$ es un elemento de la base y las columnas de C correspondientes a $\tilde{\mathcal{B}}_j$ solo tienen entradas no nulas en las filas de $\tilde{\mathcal{B}}_j$, formando la submatriz $C(F)$, y en la columna de $\overline{X^{n-1}F^j}$ con la fila de $\overline{F^{j+1}}$, dando la submatriz U

de la definición de $C_r(F)$. Finalmente, el $K[X]$-módulo generado por $(\frac{K[X]}{(F^r)}, g)$ es claramente $\frac{K[X]}{(F^r)}$, y si $\phi : M \to \frac{K[X]}{(F^r)}$ es el isomorfismo de la hipótesis, como $\phi(f(v)) = \phi(Xv) = X\phi(v) = g(\phi(v))$, tomando la base $\mathcal{B}$ de V inducida por $\tilde{\mathcal{B}}$ mediante ϕ^{-1} queda $M_{\mathcal{B}}(f) = M_{\tilde{\mathcal{B}}}(g) = C_r(F)$, y el polinomio característico de f es el de $C_r(F)$ que es F^r.

$3 \implies 1]$ Tomando g y $\tilde{\mathcal{B}}$ de la parte anterior de la prueba, $M_{\mathcal{B}}(f) = C_r(f) = M_{\tilde{B}}(g)$ y, como esto también significa que $\dim V = \dim \frac{K[X]}{(F^r)}$, queda el isomorfismo $M \to \frac{K[X]}{(F^r)}$ deseado, y como $\operatorname{ann}_{K[X]}(M) = \operatorname{ann}_{K[X]} \frac{K[X]}{(F^r)} = (F^r)$ y F^r es mónico, F^r es el polinomio mínimo de M.

$1 \implies 2]$ Sea $\phi : \frac{K[X]}{(F^r)} \to M$ un $K[X]$-isomorfismo, que induce un K-isomorfismo $\phi : \frac{K[X]}{(F^r)} \to V$, como $(\overline{1}, \overline{X}, \ldots, \overline{X}^{rn-1})$ es base de $\frac{K[X]}{(F^r)}$, tomando $v \coloneqq \phi(\overline{1})$, $(\overline{v}, \overline{f(v)}, \ldots, \overline{f^{rn-1}(v)})$ es base de V y $F(f)^r(v) = F^r(f)(v) = \overline{F^r} = 0$.

$2 \implies 1]$ Para $w \in M = V$, existen $b_s \in K$ con $w = \sum_{s=0}^{rn-1} b_s f^s(v) = (\sum_{s=0}^{rn-1} b_s X^s)v$, luego $M = (v)$ y $\pi : K[X] \twoheadrightarrow M$ dada por $\pi(G) \coloneqq Gv$ es un epimorfismo, pero $F^r \in \ker \pi$, por lo que π induce un epimorfismo $\hat{\pi} : \frac{K[X]}{(F^r)} \twoheadrightarrow M$, y como $\dim_K \frac{K[X]}{(F^r)} = rn = \dim_K M$, $\hat{\pi}$ es un isomorfismo.

Teorema de clasificación de endomorfismos: Existen una base $\mathcal{B}$ de V, $h_1, \ldots, h_t \in \mathbb{N}^*$ y $p_1, \ldots, p_t \in K[X]$ irreducibles tales que

$$M_{\mathcal{B}}(f) = \begin{pmatrix} \boxed{C_{h_1}(p_1)} & & \\ & \ddots & \\ & & \boxed{C_{h_t}(p_t)} \end{pmatrix},$$

siendo esta matriz, llamada **forma canónica** de f, unívocamente determinada por f salvo reordenación de bloques y formada, exactamente, por

$$\frac{\operatorname{rk}(p(f)^{h-1}) + \operatorname{rk}(p(f)^{h+1}) - 2\operatorname{rk}(p(f)^h)}{\operatorname{rg} p}$$

bloques $C_h(p)$ para cada divisor irreducible mónico p del polinomio característico de f y cada $h \leq \min\{s \in \mathbb{N}^* \mid \operatorname{rk}(p(f)^s) = \operatorname{rk}(p(f)^{s+1})\}$.

Demostración: Sea $M = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} N_{ij}$ una descomposición canónica con cada $N_{ij} \cong \frac{K[X]}{(p_i^{n_{ij}})}$, cada N_{ij} es un subespacio f-invariante de V, por lo que existe una base $\mathcal{B}_{ij}$ de N_{ij} como K-espacio vectorial con $M_{\mathcal{B}_{ij}}(f|_{N_{ij}}) = C_{n_{ij}}(p_i)$, y uniendo las bases se obtiene una base $\mathcal{B}$ con $M_{\mathcal{B}}(f)$ de la forma buscada.

Si ahora $\mathcal{B}'$ es otra base tal que $M_{\mathcal{B}}(f)$ está formada por bloques diagonales $(C_{h_s}(q_s))_{s=1}^{u}$, V se puede descomponer en suma directa interna de subespacios f-invariantes W_s con bases $\mathcal{B}_s$ tales que, si $\hat{f}_s \coloneqq f|_{W_s} : W_s \to W_S$, $M_{\mathcal{B}_s}(\hat{f}_s) = C_{h_s}(q_s)$, con lo que el módulo generado por $(W_s, \hat{f}_s)$ es un submódulo no nulo de M isomorfo a $\frac{K[X]}{(q_s^{h_s})}$, de modo que $M = \bigoplus_{s=1}^{u} \frac{K[X]}{(q_s^{h_s})}$ y, como las descomposiciones de esta forma son únicas, los bloques son los mismos que en la descomposición que hemos encontrado y los irreducibles que aparecen son los divisores irreducibles de f.

Para la última parte, otra forma de obtener la forma canónica de cada $M(p)$ es usando los $(F_h)_{h=1}^n$ con $n := \max_i r_i = \min\{s \in \mathbb{N}^* \mid \operatorname{ann}_{M(p)}(p^s) = \operatorname{ann}_{M(p)}(p^{s+1})\}$, cada $F_h \subseteq \operatorname{ann}_M(p^h)$ y tales que cada $F_h \dot\cup pF_{h+1} \dot\cup \ldots \dot\cup p^{n-h}F_n$ induce una base de $\frac{\operatorname{ann}_M(p^h)}{\operatorname{ann}_M(p^{h-1})} = \frac{\ker(p(f)^h)}{\ker(p(f)^{h-1})}$ como $\frac{K[X]}{(p)}$-espacio vectorial. Si $\hat f := f|_{M(p)} : M(p) \to M(p)$, $\operatorname{ann}_{M(p)}(p^s) = \ker(p(\hat f)^s) = \ker(p(f)^s)$ ya que $p(f)^s(v) = 0 \implies p^s v = 0 \implies v \in \operatorname{ann}_M(p^s) \subseteq M(p)$, de modo que $n = \min\{s \in \mathbb{N}^* \mid \operatorname{rk}(p(f)^s) = \operatorname{rk}(p(f)^{s+1})\}$. Además, el número de apariciones de p^s como divisor elemental de M es $\mu_h = \delta_h - \delta_{h+1} := \dim_{\frac{K[X]}{(p)}} \frac{\ker(p(f)^h)}{\ker(p(f)^{h-1})} - \dim_{\frac{K[X]}{(p)}} \frac{\ker(p(f)^{h+1})}{\ker(p(f)^h)}$, pero es fácil ver que todo $\frac{K[X]}{(p)}$-espacio vectorial U es un K-espacio vectorial y $\dim_{\frac{K[X]}{(p)}}(U) = \frac{\dim_K(U)}{\operatorname{gr} p}$, luego $\mu_h = \frac{1}{\operatorname{gr} p}(\dim_K \ker(p(f)^h) - \dim_K \ker(p(f)^{h-1}) - \dim_K \ker(p(f)^{h+1}) + \dim_K \ker(p(f)^h))$ y el resultado sale de que $\dim_K \ker(p(f)^h) = \dim_K V - \operatorname{rk}(p(f)^h)$.

Como **teorema**, toda $C \in \mathcal{M}_n(K)$ es semejante a una de la forma

$$\begin{pmatrix} \boxed{C_{h_1}(p_1)} & & \\ & \ddots & \\ & & \boxed{C_{h_t}(p_t)} \end{pmatrix}$$

con los $p_i \in K[X]$ irreducibles, siendo esta matriz, llamada **forma canónica** de C, unívocamente determinada por C salvo reordenación de bloques y formada, exactamente, por

$$\frac{\operatorname{rk}(p(C)^{h-1}) + \operatorname{rk}(p(C)^{h+1}) - 2\operatorname{rk}(p(C)^h)}{\operatorname{gr} p}$$

bloques $C_h(p)$ para cada divisor irreducible mónico p del polinomio característico de p y cada $h \le \min\{s \in \mathbb{N}^* \mid \operatorname{rk}(p(f)^s) = \operatorname{rk}(p(f)^{s+1})\}$.

Si $F \in K[X]$ es no constante con factorización irreducible $F = p_1^{m_1} \cdots p_k^{m_k}$ con los p_i mónicos irreducibles distintos, la forma canónica de la matriz compañera C de F es

$$\begin{pmatrix} \boxed{C_{m_1}(p_1)} & & \\ & \ddots & \\ & & \boxed{C_{m_k}(p_k)} \end{pmatrix},$$

y en particular C tiene un único divisor elemental asociado a cada divisor mónico irreducible de F.

5.3. Formas de Jordan

Un **valor propio** de f es un $\lambda \in K$ tal que $X - \lambda$ divide al polinomio característico de f, y su **multiplicidad geométrica** es $\nu_g(\lambda) := \dim_K \ker(f - \lambda 1_V) > 0$.

Para $\lambda \in K$, $C(X - \lambda) = (\lambda) \in \mathcal{M}_1(K)$ y, para $r > 0$, llamamos **bloque de Jordan** de tamaño r asociado al valor propio λ a $J_r(\lambda) := C_r(X - \lambda)$.

Teorema de Jordan:

1. Si el polinomio característico de f se descompone completamente en $K[X]$, existe una base $\mathcal{B}$ de V tal que

$$M_{\mathcal{B}}(f) = \begin{pmatrix} \boxed{J_{h_1}(\lambda_1)} & & \\ & \ddots & \\ & & \boxed{J_{h_t}(\lambda_t)} \end{pmatrix}$$

   para ciertos $h_i > 0$ y $\lambda_i \in K$, siendo esta matriz unívocamente determinada por f salvo reordenación de bloques y formada por $\mathrm{rk}((f-\lambda 1_V)^{h-1}) + \mathrm{rk}((f-\lambda 1_V)^{h+1}) - 2\mathrm{rk}((f-\lambda 1_V)^h)$ bloques $J_h(\lambda)$ para cada valor propio λ de f y cada $h \in \mathbb{N}^*$.

   Por el teorema de clasificación de endomorfismos usando que los irreducibles del polinomio característico son los $X-\lambda$ con λ valor propio de f y que el grado de estos es 1.

2. Si $C \in \mathcal{M}_n(K)$ es una matriz cuadrada cuyo polinomio característico se descompone completamente en $K[X]$, C es semejante a una matriz como la del apartado anterior, única salvo reordenación de bloques y formada por $\mathrm{rk}((C-\lambda I)^{h-1}) + \mathrm{rk}((C-\lambda I)^{h+1}) - 2\mathrm{rk}((C-\lambda I)^h)$ bloques $J_h(\lambda)$ para cada valor propio λ de C y cada $h \in \mathbb{N}^*$.

Sean φ el polinomio característico de f y p un divisor mónico irreducible de grado d y multiplicidad 1:

1. $M(p) = \ker(p(f)) \cong \frac{K[X]}{(p)}$.

   Claramente $\ker(p(f)) \subseteq M(p)$, y si $x \in M(p)$, existe $s > 0$ con $p^s x = 0$ y $x \in \ker(p(f)^s)$, pero como la multiplicidad de p en φ es 1, $\ker(p(f)) = \ker(p(f)^s)$.

2. Para todo $v \in M(p) \setminus \{0\}$, $\mathcal{B} \coloneqq \{f^s(v)\}_{s \in \mathbb{N}_d}$ es una base de $\ker(p(f))$ y $M_{\mathcal{B}}(f|_{M(p)} : M(p) \to M(p)) = C_1(p)$.

   Sean $\phi_0 : \frac{K[X]}{(p)} \to M(p)$ un isomorfismo, $\overline{q} \coloneqq (\phi_0)^{-1}(v) \neq 0$ y $\pi : \frac{K[X]}{(p)} \twoheadrightarrow \frac{K[X]}{(p)}$ el epimorfismo $\pi(\overline{F}) \coloneqq \overline{qF}$, como $\gcd\{p,q\} = 1$, existe una identidad de Bézout $1 = pR + qS$, luego $\overline{1} = \overline{qS} \in \mathrm{Im}\pi$ y π es un isomorfismo. Por tanto $\phi \coloneqq \phi_0 \circ \pi L \frac{K[X]}{(p)} \to M(p)$ es un isomorfismo con $\phi(\overline{1}) = v$ y, como $(X^s)_{s \in \mathbb{N}_d}$ es base de $\frac{K[X]}{(p)}$ como K-espacio vectorial, $\mathcal{B} \coloneqq (f^s(v))_{s \in \mathbb{N}_d}$ es base de $M(p)$ como K-espacio vectorial. Ahora bien, si $b_i \coloneqq f^i(v)$, para $i \in \{0, \ldots, d-2\}$, $f(b_i) = f(f^i(v)) = f^{i+1}(v) = b_{i+1}$, y para $d-1$,

$$f(b_{d-1}) = f^d(v) = \phi(X^d) = \phi(X^d - p) = \phi\left(-\sum_{i=0}^{d-1} p_i X^i\right) = \sum_{i=0}^{d-1} -p_i b_i,$$

   lo que nos da $M_{\mathcal{B}}(f) = C(p)$.

Análogamente, si $C \in \mathcal{M}_n(K)$ y $p \in K[X]$ es un irreducible con multiplicidad 1 en el polinomio característico de C, la forma canónica de C tiene exactamente un bloque de la forma $C_h(p)$ que es precisamente $C(p)$.

Un $\lambda \in \mathbb{R}$ es un **valor propio simple** de f o de $C \in \mathcal{M}_n(K)$ si $X - \lambda$ es divisor de su polinomio característico con multiplicidad 1, en cuyo caso:

1. $M(X-\lambda) = \ker((X-\lambda)(f)) = \{v \in V \mid f(v) = \lambda v\} \cong \frac{K[X]}{(X-\lambda)}$ es el subespacio propio de V asociado al valor propio λ de f.
2. Para todo $v \in M(X-\lambda) \setminus \{0\}$, $M(X-\lambda) = (v)$ y $f|_{(v)}$ es el producto por λ.
3. La forma canónica de C tiene un único bloque de la forma $J_h(\lambda)$, que es $J(\lambda)$.

5.4. Anillos de polinomios y matrices

Si $B \in \mathrm{GL}_s(K)$ y

$$C \coloneqq \begin{pmatrix} \boxed{B} & \boxed{I_s} & & \\ & \ddots & \ddots & \\ & & \ddots & \boxed{I_s} \\ & & & \boxed{B} \end{pmatrix} \in \mathcal{M}_{rs}(K),$$

para $k \in \{1, \dots, r-1\}$, viendo C^k por bloques como elemento de $\mathcal{M}_r(\mathcal{M}_s(K))$, su k-ésima diagonal por encima de la principal está formada por copias de B^k y las de debajo de dicha diagonal son nulas, y $C^r = 0 \neq C^{r-1}$. **Demostración:** $\phi : \mathcal{M}_{rs}(K) \to \mathcal{M}_r(\mathcal{M}_s(K))$ que agrupa las matrices en bloques es un isomorfismo de anillos, pues claramente conserva la suma y la identidad y, para el producto, haciendo los índices de matrices empezar por 0 por simplicidad,[1] si $A, B \in \mathcal{M}_{rs}(K)$, para $i, j \in \{0, \dots, r-1\}$ y $k, l \in \{1, \dots, s\}$,

$$\begin{aligned}(\phi(A)\phi(B))_{ijkl} &= \left(\sum_{p \in \mathbb{N}_r} \phi(A)_{ir}\phi(B)_{rj}\right)_{kl} = \sum_{p \in \mathbb{N}_r} (\phi(A)_{ip}\phi(B)_{pj})_{kl} = \\ &= \sum_{p \in \mathbb{N}_r} \sum_{q \in \mathbb{N}_s} \phi(A)_{ipkq}\phi(B)_{pjql} = \sum_{p \in \mathbb{N}_r} \sum_{q \in \mathbb{N}_s} A_{is+k,ps+q}B_{ps+q,js+l} = \\ &= \sum_{z \in \mathbb{N}_{rs}} A_{is+k,z}B_{z,js+l} = (AB)_{is+k,js+l} = \phi(AB)_{ijkl}.\end{aligned}$$

Entonces, si $C \in \mathcal{M}_r(\mathcal{M}_s(K))$, queremos ver que cada $(C^k)_{ij} = \binom{k}{2k+i-j}B^{2k+i-j}$, con lo que $(C^k)_{i,i+k} = \binom{k}{k}B^k = B^k$ y, para $j < i+k$, $2k+i-j > k$ y $\binom{k}{2k+i-j} = 0$. Por inducción, para $k = 1$, $C_{i,i+1} = B = \binom{1}{1}B^1$, $C_{i,i+2} = I_s = \binom{1}{0}B^0$ y el resto de entradas son nulas, y para $k > 1$,

$$\begin{aligned}(C^k)_{ij} &= \sum_{l=1}^{r} (C^{k-1})_{il}C_{lj} = \sum_{l=1}^{r} \binom{k-1}{2k-2+i-l}\binom{1}{2+l-j}B^{2k-2+i-l+2-j+l} = \\ &= \sum_{l} \binom{k-1}{(1-k-i)+l}\binom{1}{(2-j)+l}B^{2k+i-j} = \binom{k}{2k+i-j}B^{2k+i-j},\end{aligned}$$

[1] Como debería ser siempre.

donde en la última igualdad hemos usado que $\sum_k \binom{r}{m+k}\binom{s}{n+k} = \binom{r+s}{r-m+n}$ y en la penúltima hemos usado que $(k-1)-(2k-2+i-l) = 1-k-i+l$ y que podemos expandir el rango del sumatorio ya que, si el producto de los dos coeficientes no se anula, entonces $2+l-j \in \{0,1\} \implies l \leq j-1 < r$ y $0 \leq 1-k-i+l \leq k-1 \implies k-1 \leq l-i \leq 2(k-1) \implies l \geq k+i-1 > 1$.

Sean $C \in \mathcal{M}_n(K)$, $P \in \mathrm{GL}_n(K)$ y $C' \coloneqq PCP^{-1}$:

1. Para $F \in K[X]$, $F(C') = PF(C)P^{-1}$.

   Para $k \in \mathbb{N}$, $(PCP^{-1})^k = PC^kP^{-1}$, con lo que $F(PCP^{-1}) = \sum_k F_k PC^kP^{-1} \overset{F_k \in K}{=} P(\sum_k F_k C^k)P^{-1} = PF(C)P^{-1}$.

2. C y C' tienen el mismo polinomio mínimo.

   Por lo anterior, usando que el polinomio mínimo de una matriz C es el menor d_t con $d_t(C) = 0$ y que $F(C') = PF(C)P^{-1} = 0 \iff F(C) = 0$.

5.5. Formas canónicas reales

Si $(a,b) \in \mathbb{R} \times \mathbb{R}^*$ y $r > 0$, llamamos

$$J(a,b) \coloneqq \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

con polinomio característico irreducible $p \coloneqq (X-a)^2 + b^2$, pues $p = X^2 - 2aX + a^2 + b^2$ y $(-2a)^2 - 4(a^2+b^2) = -b^2 < 0$. Entonces, para $r \in \mathbb{N}^*$, llamamos **bloque de Jordan real** de tamaño r asociado a (a,b) o a p a

$$J_r(a,b) \coloneqq \begin{pmatrix} \boxed{J(a,b)} & \boxed{I_2} & & \\ & \ddots & \ddots & \\ & & \ddots & \boxed{I_2} \\ & & & \boxed{J(a,b)} \end{pmatrix} \in \mathcal{M}_{2r}(\mathbb{R}).$$

Toda $C \in \mathcal{M}_n(\mathbb{R})$ es semejante a una matriz de la forma

$$\begin{pmatrix} \boxed{J_{r_1}(a_1,b_1)} & & & & & \\ & \ddots & & & & \\ & & \boxed{J_{r_t}(a_t,b_t)} & & & \\ & & & \boxed{J_{h_1}(\lambda_1)} & & \\ & & & & \ddots & \\ & & & & & \boxed{J_{h_s}(\lambda_s)} \end{pmatrix},$$

única salvo reordenación de bloques, formada por

$$\mathrm{rk}((C-\lambda I)^{h-1}) + \mathrm{rk}((C-\lambda I)^{h+1}) - 2\mathrm{rk}((C-\lambda I)^h)$$

bloques $J_h(\lambda)$ para cada $h \in \mathbb{N}^*$ y λ valor propio real de C y

$$\frac{1}{2}(\mathrm{rk}(p(C)^{r-1}) + \mathrm{rk}(p(C)^{r+1}) - 2\mathrm{rk}(p(C)^r)$$

bloques $J_r(a,b)$ para cada $r \in \mathbb{N}^*$ y $p = (X-a)^2 + b^2$ divisor irreducible cuadrático del polinomio característico de C. **Demostración:** Por el teorema de clasificación de matrices cuadradas y el hecho de que todos los irreducibles en $\mathbb{R}[X]$ son de grado 1 o 2, solo hay que ver que $J_r(a,b)$ es semejante a $C_r(p)$, ambas con polinomio característico p^r. Pero si $J \coloneqq J_r(a,b)$, $(J - aI) = J_r(0,b)$ y, viendo $J_r(0,b) \in \mathcal{M}_r(\mathcal{M}_2(K))$,

$$J_r(0,b)_{ij} = \begin{cases} J(0,b), & j = i; \\ I_2, & j = i+1; \\ 0, & \text{en otro caso,} \end{cases}$$

y como además $J(0,b)^2 = -b^2 I_2 \in \mathrm{GL}_2(\mathbb{R})$,

$$(J_r(0,b)^2)_{ij} = \begin{cases} J(0,b)^2 = -b^2 I_2, & j = i; \\ 2J(0,b), & j = i+1; \\ I_2, & j = i+2; \\ 0, & \text{en otro caso,} \end{cases}$$

con lo que $p(J) = (J-aI)^2 + b^2$ tiene la forma de la matriz del resultado anterior y $p(J)^r = 0 \neq p(J)^{r-1}$. Entonces el $\mathbb{R}[X]$-módulo M asociado a $(\mathbb{R}^{2r}, v \mapsto Jv)$ tiene un sumando directo isomorfo a $\frac{\mathbb{R}[X]}{(p^r)}$, y como $\dim_{\mathbb{R}} \frac{\mathbb{R}[X]}{(p^r)} = 2h = \dim_{\mathbb{R}} M$, $M \cong \frac{\mathbb{R}[X]}{(p^r)}$. Pero por el teorema de clasificación de endomorfismos, $v \mapsto Jv$ se expresa como $C_r(p)$ en alguna base de $\mathbb{R}^{2r}$ y por tanto en alguna de M.

5.6. Series de Taylor pero en álgebra y son un porro[2]

Sean $\lambda \in K$, $r, k \in \mathbb{N}^*$ y $J \coloneqq J_r(\lambda)$, si $k < r$, $(J - \lambda I_r)^k$ tiene a 1 las celdas de la diagonal k-ésima por encima de la diagonal principal y a 0 el resto, y si $k \geq r$, $(J - \lambda I_r)^k = 0$. **Demostración:** Esto equivale a que, en cualquier caso, $((J - \lambda I_r)^k)_{ij} \equiv \delta_{i-j,k}$. Para $k = 1$ esto es claro, y para $k > 1$, $((J - \lambda I_r)^k)_{ij} = \sum_{l=1}^{r} \delta_{i-l,k-1}\delta_{l-j,1} = \delta_{i-j,k}$, pues lo de dentro del sumatorio vale 1 si y sólo si $i - l = k - 1$ y $l - j = 1$, si y sólo si $l = j + 1$ e $i = j + k$, pero si $j + k \leq r$, $l \leq r$ está dentro de rango y hay exactamente un sumando en que se da esto, y si $j + k > r$, esto no se da en ningún sumando pero tampoco se da $i - j = k$ porque entonces sería $i > r$.

Sean $\mathbb{K}$ igual a $\mathbb{R}$ o $\mathbb{C}$, $D \subseteq \mathbb{K}$ abierto, $\psi : D \to \mathbb{K}$ infinitamente derivable, $\lambda \in D$ y $J \coloneqq J_r(\lambda)$, llamamos **valor** o **evaluación** de ψ en J a $\psi(J)$, que es un polinomio en J. En efecto, ψ tiene una serie de Taylor $\psi(x) = \sum_{n\geq 0} \frac{\psi^{(n)}(\lambda)}{n!}(x-\lambda)^n$ y entonces $\psi(J) = \sum_{n\geq 0} \frac{\psi^{(n)}(\lambda)}{n!}(J-\lambda I)^n$, pero para $n \geq r$ es $(J - \lambda I)^n = 0$, por lo que queda una suma finita que es un polinomio en J. Además:

[2]En realidad el porro es todo lo de antes.

1. Para $k \in \{1, \dots, r-1\}$,
$$(J^k)_{ij} = \binom{k}{j-i} \lambda^{k-j+i},$$
tomando el criterio $0 \cdot \infty = 0$.

   Para $k = 1$ es claro, pues para $j = i$ es $J_{ij} = \lambda = \binom{1}{0}\lambda^1$, para $j = i+1$ es $J_{ij} = 1 = \binom{1}{1}\lambda^0$ y en otro caso la fórmula da 0, usando el criterio si fuese necesario. Para $k > 1$, por inducción,
$$(J^k)_{ij} = \sum_{l=1}^{r} (J^{k-1})_{il} J_{lj} = \sum_{l=1}^{r} \binom{k-1}{l-i}\binom{1}{j-l} \lambda^{(k-1-l+i)+(1-j+l)} =$$
$$= \sum_{l} \binom{k-1}{l-i}\binom{1}{(j-i)-(l-i)} \lambda^{k+i-j} = \binom{k}{j-i}\lambda^{k+i-j},$$
   donde justificamos expandir el rango del sumatorio viendo que, si $0 \le l-i \le k-1$ y $0 \le j-l \le 1$, entonces por lo primero $i \le l$ y por lo segundo $l \le j$, luego $l \in \{1, \dots, r\}$.

2.
$$(\psi(J))_{ij} = \begin{cases} \frac{\psi^{(j-i)}(\lambda)}{(j-i)!}, & j \ge i; \\ 0, & \text{en otro caso.} \end{cases}$$
   $\psi(J) = \sum_{n \ge 0} \frac{\psi^{(n)}(\lambda)}{n!}(J - \lambda I)^n$, con lo que
$$(\psi(J))_{ij} = \sum_{n \ge 0} \frac{\psi^{(n)}(\lambda)}{n!}\delta_{j-i,n} = \begin{cases} \frac{\psi^{(n)}(\lambda)}{n!}, & n \coloneqq j-i \ge 0; \\ 0, & \text{en otro caso.} \end{cases}$$

Sean $C \in \mathcal{M}_n(\mathbb{K})$ y $P \in \mathrm{GL}_n(\mathbb{K})$ son tales que $P^{-1}CP =: \mathrm{diag}(J_1, \dots, J_t)$ con los J_i bloques de Jordan, $D \subseteq \mathbb{K}$ es un abierto que contiene a todos los valores propios de C y $\psi : D \to \mathbb{K}$ es infinitamente derivable, llamamos **valor** o **evaluación** de ψ en C a $\psi(C) \coloneqq P(\psi(J_1) \oplus \cdots \oplus \psi(J_t))P^{-1}$, que no depende de la P elegida.

Apéndice A

Grupos

GyA

Llamamos **orden** de [un grupo] G al cardinal del conjunto. [...]

Si A es un anillo, $(A, +)$ es su **grupo aditivo**, que es abeliano, y $(A^*, \cdot)$ es su **grupo de unidades**, que es abeliano cuando el anillo es conmutativo. [...]

Llamamos **orden** de $a \in G$ al orden de $\langle a \rangle$, $|a| \coloneqq |\langle a \rangle|$, y escribimos $\langle a \rangle_n$ para referirnos a $\langle a \rangle$ indicando que tiene orden n. El orden de a divide al de G.

Sea $f : \mathbb{Z} \to G$ el homomorfismo dado por $f(n) \coloneqq a^n$, $\ker f = n\mathbb{Z}$ para algún $n \geq 0$. Si $n = 0$, f es inyectivo y $(\mathbb{Z}, +) \cong \langle a \rangle$, y en otro caso $\mathbb{Z}_n \cong \langle a \rangle$, con lo que $n = |a|$ y $a^n = 1 \iff |a| \mid n$. De aquí, $a^k = a^l \iff k \equiv l \text{ mód } n$, con lo que $|a|$ es el menor entero positivo con $a^n = 1$.

Si a tiene orden finito y $n > 0$,

$$|a^n| = \frac{|a|}{\text{mcd}\{|a|, n\}}.$$

Si $G = \langle a \rangle$:

1. Si G tiene orden infinito, $G \cong (\mathbb{Z}, +) \cong C_\infty$ y los subgrupos de G son los $\langle a^n \rangle$ con $n \in \mathbb{N}$.

2. Si $|G| = n$, $G \cong (\mathbb{Z}_n, +) \cong C_n$ y los subgrupos de G son exactamente uno de orden d por cada $d \mid n$, $\langle a^{n/d} \rangle_d$.

3. Todos los subgrupos y grupos cociente de G son cíclicos.

Así, si $p \in \mathbb{N}$ es primo, todos los grupos de orden p son isomorfos a $(\mathbb{Z}_p, +)$. Si $G = \langle g_1, \ldots, g_n \rangle$ y $N \trianglelefteq G$, $G/N = \langle g_1 N, \ldots, g_n N \rangle$.

Teorema chino de los restos para grupos:

1. Si G y H son subgrupos cíclicos de órdenes respectivos n y m, $G \times H$ es cíclico si y sólo si n y m son coprimos. [...]

2. Si $g, h \in G$ tienen órdenes respectivos n y m coprimos y $gh = hg$, entonces $\langle g, h \rangle$ es cíclico de orden nm. [...]

Dados un grupo G y $a \in G$, llamamos **conjugado** de $g \in G$ por a a $g^a := a^{-1}ga$, y conjugado de $X \subseteq G$ por a a $X^a := \{x^a\}_{x \in X}$. Dos elementos $x, y \in G$ o conjuntos $x, y \subseteq G$ son **conjugados** en G si existe $a \in G$ con $x^a = y$.

Si $a \in G$, llamamos **automorfismo interno** definido por a al automorfismo $\iota_a : G \to G$ dado por $\iota_a(x) := x^a$. Su inverso es $\iota_{a^{-1}}$. El conjugado por a de un subgrupo de G es otro subgrupo de G del mismo orden. [...]

$\forall g, a, b \in G, g^{ab} = (g^a)^b$, y [...] la relación de ser conjugados es de equivalencia. Las clases de equivalencia se llaman **clases de conjugación** de G, y llamamos $a^G := [a] = \{a^g\}_{g \in G}$.

Sea X un conjunto. Una **acción por la izquierda** de G en X es una función $\cdot : G \times X \to X$ tal que $\forall x \in X, (\forall g, h \in G, (gh) \cdot x = g \cdot (h \cdot x) \wedge 1 \cdot x = x)$, y una **acción por la derecha** de G en X es una función $\cdot : X \times G \to X$ tal que $\forall x \in X, (\forall g, h \in G, x \cdot (gh) = (x \cdot g) \cdot h \wedge x \cdot 1 = x)$.

Si $\cdot : G \times X \to X$ es una acción por la izquierda de G en X y $x \in X$, llamamos **órbita** de x en G a $G \cdot x := \{g \cdot x\}_{g \in G}$ y **estabilizador** de x en G a $\mathrm{Estab}_G(x) := \{g \in G \mid g \cdot x = x\}$. Si $\cdot : X \times G \to X$ es una acción por la derecha de G en X y $x \in X$, llamamos órbita de x en G a $x \cdot G := \{x \cdot g\}_{g \in G}$ y estabilizador de x en G a $\mathrm{Estab}_G(x) := \{g \in G \mid x \cdot g = x\}$. Las órbitas forman una partición de G.

1. Llamamos **acción por traslación a la izquierda** a la acción por la izquierda de G en G/H dada por $g \cdot xH = gxH$. Entonces $G \cdot xH = G/H$ y

$$\mathrm{Estab}_G(xH) = [...] = H^{x^{-1}}.$$

   Análogamente llamamos **acción por traslación a la derecha** a la acción por la derecha de G en $H \backslash G$ dada por $Hx \cdot g = Hxg$.

2. Cuando $H = 1$, la acción de traslación es de G en G, con $G \cdot x = G$ y $\mathrm{Estab}_G(x) = 1$.

3. La **acción por conjugación** de G en G es la acción por la derecha $x \cdot g := x^g$. Entonces $x \cdot G = x^G$ y $\mathrm{Estab}_G(x) = C_G(x)$.

4. Si S es el conjunto de subgrupos de G, la **acción por conjugación de G en sus subgrupos** es la acción por la derecha de G en S $H \cdot g = H^g$. [...]

5. Si $n \in \mathbb{N}$ y X es un conjunto, $\cdot : S_n \times X^n \to X^n$ dada por $\sigma \cdot (x_1, \ldots, x_n) := (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ es una acción por la izquierda.

6. Sean $\cdot : G \times X \to X$ una acción por la izquierda, $H \leq G$ e $Y \subseteq X$, si $\forall h \in H, y \in Y, h \cdot y \in Y$, $\cdot|_{H \times Y}$ es una acción por la izquierda de H en Y.

Sean G un grupo actuando sobre un conjunto X, $x \in X$ y $g \in G$:

1. $\mathrm{Estab}_G(x) \leq G$.

2. $[G : \mathrm{Estab}_G(x)] = |G \cdot x|$. En particular, si G es finito, $|G \cdot x| \mid |G|$.

3. Si la acción es por la izquierda, $\mathrm{Estab}_G(g \cdot x) = \mathrm{Estab}_G(x)^{g^{-1}}$, y si es por la derecha, $\mathrm{Estab}_G(x \cdot g) = \mathrm{Estab}_G(x)^g$. En particular, si $x, g \in G$ y $H \leq G$, $C_G(x^g) = C_G(x)^g$ y $N_G(H^g) = N_G(H)^g$.

4. Si R es un conjunto irredundante de representantes de las órbitas, $|X| = \sum_{r \in R} |G \cdot r| = \sum_{r \in R} [G : \mathrm{Estab}_G(r)]$.

Así, si G es un grupo y $a \in G$, $|a^G| = [G : C_G(a)]$, y en particular a^G es unipuntual si y sólo si $a \in Z(G)$. **Ecuación de clases:** Si G es finito y $X \subseteq G$ contiene exactamente un elemento de cada clase de conjugación con al menos dos elementos, entonces $|G| = |Z(G)| + \sum_{x \in X} [G : C_G(x)]$.

Dado un número primo p, un **p-grupo** es un grupo en que todo elemento tiene orden potencia de p, y un grupo finito es un p-grupo si y sólo si su orden es potencia de p. [...]

Teorema de Cauchy: Si G es un grupo finito con orden múltiplo de un primo p, G tiene un elemento de orden p. [...]

Dados un grupo finito G y un número primo p, $H \leq G$ es un **p-subgrupo de Sylow** de G si es un p-grupo y $[G : H]$ es coprimo con p, si y sólo si es un p-grupo y $|H|$ es la mayor potencia de p que divide a $|G|$. Llamamos $s_p(G)$ al número de p-subgrupos de Sylow de G.

Teoremas de Sylow: Sean p un número primo y G un grupo finito de orden $n := p^k m$ para ciertos $k, m \in \mathbb{N}$ con $p \nmid m$. Entonces:

1. G tiene al menos un p-subgrupo de Sylow, que tendrá orden p^k.

2. Si P es un p-subgrupo de Sylow de G y Q es un p-subgrupo de G, existe $g \in G$ tal que $Q \subseteq P^g$. En particular, todos los p-subgrupos de Sylow de G son conjugados en G.

3. $s_p(G) \mid m$ y $s_p(G) \equiv 1 \bmod p$. [...]

Apéndice B

Anillos de polinomios

B.1. Cuerpos de fracciones

GyA

Sean $D \neq 0$ un dominio y $X \coloneqq D \times (D \setminus \{0\})$, definimos la relación binaria

$$(a_1, s_1) \sim (a_2, s_2) : \iff a_1 s_2 = a_2 s_1.$$

Esta relación es de equivalencia. Llamamos $a/s \coloneqq \frac{a}{s} \coloneqq [(a, s)] \in Q(D) \coloneqq X/\sim$, y las operaciones

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} \coloneqq \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \qquad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \coloneqq \frac{a_1 a_2}{s_1 s_2},$$

están bien definidas.

Para $a, b \in D$ y $s, t \in D \setminus \{0\}$:

1. $\frac{a}{s} = \frac{0}{1} \iff a = 0$.
2. $\frac{a}{s} = \frac{1}{1} \iff a = s$.
3. $\frac{at}{st} = \frac{a}{s}$.
4. $\frac{a}{s} = \frac{b}{s} \iff a = b$.
5. $\frac{a}{s} + \frac{b}{s} = \frac{a+b}{s}$.

[...] $(Q(D), +, \cdot)$ es un cuerpo llamado **cuerpo de fracciones** o **de cocientes** de D cuyo cero es $\frac{0}{1}$ y cuyo uno es $\frac{1}{1}$.

$\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$. [...] $u : D \to Q(D)$ dada por $u(a) \coloneqq a/1$ es un homomorfismo inyectivo, por lo que podemos ver a D como un subdominio de $Q(D)$ identificando a cada $a \in D$ con $a/1 \in Q(D)$.

Propiedad universal del cuerpo de fracciones: Dados un dominio D y $u : D \to Q(D)$ dada por $u(a) \coloneqq a/1$:

1. Sean K un cuerpo y $f : D \to K$ un homomorfismo inyectivo, el único homomorfismo de cuerpos $\tilde{f} : Q(D) \to K$ con $\tilde{f} \circ u = f$ viene dado por $\tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$.

2. Sean K un cuerpo no trivial y $g, h : Q(D) \to K$ homomorfismos que coinciden en D, entonces $g = h$.

3. Sean F un cuerpo no trivial y $v : D \to F$ un homomorfismo inyectivo tal que para todo cuerpo K y homomorfismo inyectivo $f : D \to K$ existe un único homomorfismo $\tilde{f} : F \to K$ con $\tilde{f} \circ v = f$, entonces existe un isomorfismo $\phi : F \to Q(D)$ con $\phi \circ v = u$.

Sean D un dominio, K un cuerpo no trivial y $f : D \to K$ un homomorfismo inyectivo, K contiene un subcuerpo isomorfo a $Q(D)$.

De aquí, para $m \in \mathbb{Z}$, $Q(\mathbb{Z}[\sqrt{m}]) \cong \mathbb{Q}[\sqrt{m}]$, lo que nos permite identificar los elementos de $Q(\mathbb{Z}[\sqrt{m}])$ con los de $\mathbb{Q}[\sqrt{m}]$.

Sea K un cuerpo no trivial, existe un subcuerpo K' de K llamado **subcuerpo primo** de K contenido en cualquier subcuerpo de K, y este es isomorfo a $\mathbb{Z}_p$ si la característica de K es un entero primo p o a $\mathbb{Q}$ en caso contrario.

B.2. Polinomios

GyA

A es un subanillo de $A[X]$ identificando los elementos de A con los **polinomios constantes**, de la forma $P(X) = a_0$. Dado un ideal I de A, $\{a_0 + a_1X + \cdots + a_nX^n \in A[X] \mid a_0 \in I\}$ e $I[X] \coloneqq \{a_0 + a_1X + \cdots + a_nX^n \in A[X] \mid a_0, \ldots, a_n \in I\}$ son ideales de $A[X]$.

Dado $p \coloneqq \sum_{k\in\mathbb{N}} p_k X^k \in A[X] \setminus \{0\}$, llamamos **grado** de p a $\operatorname{gr}(p) \coloneqq \operatorname{máx}\{k \in \mathbb{N} \mid p_k \neq 0\}$, **coeficiente** de **grado** k de p a p_k, **coeficiente independiente** al de grado 0 y **coeficiente principal** al de grado $\operatorname{gr}(p)$. Un polinomio es **mónico** si su coeficiente principal es 1. El polinomio 0 tiene grado $-\infty$ por convención.

Un **monomio** es un polinomio de la forma aX^n con $a \in A$ y $n \in \mathbb{N}$. Todo polinomio en $A[X]$ se escribe como suma finita de monomios de distinto grado de forma única salvo orden.

Si $P, Q \in A[X] \setminus \{0\}$ tienen coeficientes principales respectivos p y q:

1. $\operatorname{gr}(P + Q) \leq \operatorname{máx}\{\operatorname{gr}(P), \operatorname{gr}(Q)\}$, con desigualdad estricta si y sólo si $\operatorname{gr}(P) = \operatorname{gr}(Q)$ y $p + q = 0$.

2. $\operatorname{gr}(PQ) \leq \operatorname{gr}(P) + \operatorname{gr}(Q)$, con igualdad si y sólo si $pq \neq 0$.

$A[X]$ no es un cuerpo. Es un dominio si y sólo si lo es A, en cuyo caso llamamos **cuerpo de las funciones racionales** sobre A al cuerpo de fracciones de $A[X]$.

[...] **Propiedad universal del anillo de polinomios (PUAP):** Sean A un anillo y $u : A \to A[X]$ el homomorfismo inclusión:

1. Para cada homomorfismo de anillos conmutativos $f : A \to B$ y $b \in B$, el único

homomorfismo $\tilde{f} : A[X] \to B$ tal que $\tilde{f}(X) = b$ y $\tilde{f} \circ u = f$ es

$$\tilde{f}\left(\sum_n p_n X^n\right) := \sum_n f(p_n) b^n.$$

2. $A[X]$ y u están determinados salvo isomorfismos por la propiedad universal: dados un homomorfismo de anillos $v : A \to P$ y $t \in P$ tales que, para cada homomorfismo de anillos $f : A \to B$ y $b \in B$, existe un único $\tilde{f} : P \to B$ tal que $\tilde{f} \circ v = f$ y $\tilde{f}(t) = b$, existe un isomorfismo $\phi : A[X] \to P$ tal que $\phi \circ u = v$ y $\phi(X) = t$.

Así:

1. Si A es un subanillo de B y $b \in B$, el **homomorfismo de sustitución** o **de evaluación** en b es $S_b : A[X] \to B$ dado por

$$S_b(p) := p(b) := \sum_n p_n b^n,$$

y su imagen es el subanillo generado por $A \cup \{b\}$, llamado $A[b]$. Todo $p \in A[X]$ induce una **función polinómica** $\hat{p} : B \to B$ dada por $\hat{p}(b) := S_b(p)$.

2. Dado $a \in A$, el homomorfismo de sustitución S_{X+a} es un automorfismo de $A[X]$ con inverso S_{X-a}.

3. Si A es un anillo conmutativo, $\frac{A[X]}{(X)} \cong A$.

4. Todo homomorfismo de anillos $f : A \to B$ induce un homomorfismo $\hat{f} : A[X] \to B[X]$ dado por

$$\hat{f}(p) = \sum_n f(p_n) X^n,$$

que es inyectivo o suprayectivo si lo es f.

5. Si A es un subanillo de B, $A[X]$ lo es de $B[X]$.

6. Si I es un ideal de A, el **homomorfismo de reducción de coeficientes módulo** I es $\tilde{\pi} : A[X] \to (A/I)[X]$ dado por

$$\tilde{\pi}(p) := \sum_n (p_n + I) X^n.$$

Su núcleo es $I[X]$, por lo que $(A/I)[X] \cong \frac{A[X]}{I[X]}$.

B.3. Descomposiciones de polinomios en dominios

GyA

Sean $f, g \in A[X]$, si el coeficiente principal de g es invertible en A, existen dos únicos polinomios $q, r \in A[X]$, llamados respectivamente **cociente** y **resto** de la **división** de f entre g, tales que $f = gq + r$ y $\text{gr}(r) < \text{gr}(g)$ [...]. En particular, el grado es una función euclídea.

Teorema del resto: Dados $f \in A[X]$ y $a \in A$, el resto de f entre $X - a$ es $f(a)$. De aquí se obtiene el **teorema de Ruffini**, que dice que f es divisible por $X - a$ si y sólo si $f(a) = 0$, en cuyo caso a es una **raíz** de f.

Para $f \in A[X] \setminus \{0\}$ y $a \in A$, existe $m \coloneqq \text{máx}\{k \in \mathbb{N} \mid (X-a)^k \mid f\}$. Llamamos a m **multiplicidad** de a en f, y a es raíz de f si y sólo si $m \geq 1$. Decimos que a es una **raíz simple** de f si $m = 1$ y que es una **raíz compuesta** si $m > 1$.

La multiplicidad de a en f es el único natural m tal que $f = (X-a)^m g$ para algún $g \in A[X]$ del que a no es raíz.

Si D es un dominio, $f \in D[X] \setminus \{0\}$, $a_1, \ldots, a_n$ son n elementos de D y $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}^{>0}$ con $(X - a_k)^{\alpha_k} \mid f$ para cada k, entonces $(X-a_1)^{\alpha_1} \cdots (X-a_n)^{\alpha_n} \mid f$, por lo que $\sum_{k=1}^{n} \alpha_k \leq \text{gr}(f)$ y, en particular, la suma de las multiplicidades de las raíces de f, y el número de raíces, no son superiores a $\text{gr}(f)$.

Principio de las identidades polinómicas: Sea D un dominio:

1. Para $f, g \in D[X]$, si las funciones polinómicas $f, g : D \to D$ coinciden en m elementos de D con $m > \text{gr}(f), \text{gr}(g)$, los polinomios f y g son iguales.

2. D es infinito si y sólo si cualquier par de polinomios distintos en $D[X]$ define dos funciones polinómicas distintas en D.

Como ejemplo de lo anterior, por el teorema pequeño de Fermat, dado un primo p, todos los elementos de $\mathbb{Z}_p$ son raíces de 0 y $X^p - X$.

Dado un anillo conmutativo A, definimos la **derivada** de $P \coloneqq \sum_k a_k X^k \in A[X]$ como $P' \coloneqq D(P) \coloneqq \sum_{k \geq 1} k a_k X^{k-1}$, y escribimos $P^{(0)} \coloneqq P$ y $P^{(n+1)} \coloneqq P^{(n)\prime}$. Dados $a, b \in A$ y $P, Q \in A[X]$:

1. $(aP + bQ)' = aP' + bQ'$.

2. $(PQ)' = P'Q + PQ'$.

3. $(P^n)' = nP^{n-1}P'$.

Dados un dominio D de característica 0, $P \in D[X] \setminus \{0\}$ y $a \in D$, la multiplicidad de a en P es el menor $m \in \mathbb{N}_0$ con $P^{(m)}(a) \neq 0$. [...]

Dado un anillo A, $A[X]$ es un dominio euclídeo si y sólo si es un DIP, si y sólo si A es un cuerpo.

Sean D un dominio y $p \in D$:

1. p es irreducible en D si y sólo si lo es en $D[X]$. [...]

2. Si p es primo en $D[X]$, lo es en D. [...]

3. Si D es un DFU, p es irreducible en D si y sólo si lo es en $D[X]$, si y sólo si es primo en D, si y sólo si lo es en $D[X]$. [...]

Sea D un DFU, definimos $\varphi : D \setminus 0 \to \mathbb{N}$ tal que $\varphi(a)$ es el número de factores irreducibles en la factorización por irreducibles de a en D, contando repetidos, y para $a, b \in D \setminus \{0\}$, $\varphi(ab) = \varphi(a) + \varphi(b)$ y $\varphi(a) = 0 \iff a \in D^*$.

Si D es un DFU, K es su cuerpo de fracciones y $f \in D[X]$ es irreducible en $D[X]$, es irreducible en $K[X]$. [...] D es un DFU si y sólo si lo es $D[X]$.

[...] Si D es un DFU y K es su cuerpo de fracciones, definimos la relación de equivalencia en K $x \sim y :\iff \exists u \in D^* : y = ux$, con lo que $[x] = xD^*$ y, en particular, si $x \in D$, $[x]$ es el conjunto de los asociados de x en D. Definimos $\cdot : K \times (K/\sim) \to K/\sim$ como $a(bD^*) = (ab)D^*$. Esto está bien definido. Además, $a(b(cD^*)) = (ab)(cD^*)$.

Definimos $c : K[X] \to K/\sim$ tal que, para $p \coloneqq \sum_{k\geq 0} p_k X^k \in D[X]$, $c(p) \coloneqq \{x \mid x = \operatorname{mcd}_{k\geq 0} p_k\}$, y para $p \in K[X]$, si $a \in D \setminus \{0\}$ cumple $ap \in D[X]$, $c(p) \coloneqq a^{-1}c(ap)$. Esto está bien definido. Si $c(p) = aD^*$, a es el **contenido** de p ($a = c(p)$).

Para $a \in K$ y $p \in K[X]$:

1. Si $a \in D$ y $p \in D[X]$, $a \mid p$ en $D[X]$ si y sólo si $a \mid c(p)$ en D.

2. $c(ap) = ac(p)$.

3. $p \in D[X] \iff c(p) \in D$.

Un polinomio p es **primitivo** si $c(p) = 1$, esto es, si $p \in D[X]$ y $\operatorname{mcd}_k p_k = 1$.

Lema de Gauss: Para $f, g \in D[X]$, $c(fg) = c(f)c(g)$, y en particular fg es primitivo si y sólo si f y g lo son. [...]

Dado $f \in D[X] \setminus D$ primitivo, f es irreducible en $D[X]$ si y sólo si lo es en $K[X]$, si y sólo si $\forall G, H \in K[X], (f = GH \implies \operatorname{gr}(G) = 0 \vee \operatorname{gr}(H) = 0)$, si y sólo si $\forall g, h \in D[X], (f = gh \implies \operatorname{gr}(g) = 0 \vee \operatorname{gr}(h) = 0)$. [...]

De aquí que si D es un DFU con cuerpo de fracciones K, los irreducibles de $D[X]$ son precisamente los de D y los polinomios primitivos de $D[X] \setminus D$ irreducibles en $K[X]$.

[...] Sean K un cuerpo y $f \in K[X]$:

1. Si $\operatorname{gr}(f) = 1$, f es irreducible en $K[X]$.

2. Si $\operatorname{gr}(f) > 1$ y f tiene una raíz en K, f no es irreducible en $K[X]$.

3. Si $\operatorname{gr}(f) \in \{2, 3\}$, f es irreducible en $K[X]$ si y sólo si no tiene raíces en K.

Si D es un DFU con cuerpo de fracciones K, $f \coloneqq \sum_k a_k X^k \in D[X]$ y $n \coloneqq \operatorname{gr}(f)$, todas las raíces de f en K son de la forma $\frac{r}{s}$ con $r \mid a_0$ y $s \mid a_n$.

Criterio de reducción: Sean $\phi : D \to K$ un homomorfismo de anillos donde D es un DFU y K es un cuerpo, $\hat{\phi} : D[X] \to K[X]$ el homomorfismo inducido por ϕ y f un polinomio primitivo de $D[X] \setminus D$, si $\hat{\phi}(f)$ es irreducible en $K[X]$ y $\operatorname{gr}(\hat{\phi}(f)) = \operatorname{gr}(f)$, entonces f es irreducible en $D[X]$.

En particular, si $p \in \mathbb{Z}$ es primo, $f \coloneqq \sum_k a_k X^k \in \mathbb{Z}[X]$ es primitivo, $n \coloneqq \mathrm{gr}(f)$, $p \nmid a_n$ y f es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Z}[X]$.

Criterio de Eisenstein: Sean D un DFU, $f \coloneqq \sum_k a_k X^k \in D[X]$ primitivo y $n \coloneqq \mathrm{gr} f$, si existe un irreducible $p \in D$ tal que $\forall k \in \{0, \dots, n-1\}, p \mid a_k$ y $p^2 \nmid a_0$, entonces f es irreducible en $D[X]$.

Así:

1. Si $a \in \mathbb{Z}$ y existe $p \in \mathbb{Z}$ cuya multiplicidad en a es 1, $X^n - a$ es irreducible.

2. Para $n \geq 3$, llamamos **raíces n-ésimas de la unidad** o **de 1** a las raíces de $X^n - 1$ en $\mathbb{C}$, que son los n vértices del n-ágono regular inscrito en el círculo unidad de $\mathbb{C}$ con un vértice en el 1. $X^n - 1 = (X-1)\Phi_n(X)$, donde $\Phi_n(X) \coloneqq X^{n-1} + X^{n-2} + \cdots + X + 1$ es el **n-ésimo polinomio ciclotómico** y sus raíces en $\mathbb{C}$ son las raíces n-ésimas de 1 distintas de 1. En $\mathbb{Q}$, $X + 1 \mid \Phi_4(X)$, pero si n es primo, $\Phi_n(X)$ es irreducible.

B.4. Polinomios en varias indeterminadas

GyA

Dados un anillo conmutativo A y $n \geq 2$, definimos el **anillo de polinomios** en n indeterminadas con coeficientes en A como $A[X_1, \dots, X_n] \coloneqq A[X_1, \dots, X_{n-1}][X_n]$. Llamamos **indeterminadas** a los símbolos $X_1, \dots, X_n$ y **polinomios en n indeterminadas** a los elementos de $A[X_1, \dots, X_n]$. Dados un anillo conmutativo A y $n \in \mathbb{N}^*$:

1. $A[X_1, \dots, X_n]$ no es un cuerpo.

2. $A[X_1, \dots, X_n]$ es un dominio si y sólo si lo es A.

3. Si A es un dominio, $A[X_1, \dots, X_n]^* = A^*$.

4. $A[X_1, \dots, X_n]$ es un DFU si y sólo si lo es A.

5. $A[X_1, \dots, X_n]$ es un DIP si y sólo si $n = 1$ y A es un cuerpo.

Dados $a \in A$ e $i \coloneqq (i_1, \dots, i_n) \in \mathbb{N}^n$, llamamos a $aX_1^{i_1} \cdots X_n^{i_n} \in A[X_1, \dots, X_n]$ **monomio** de **tipo** i y coeficiente a. Todo $p \in A[X_1, \dots, X_n]$ se escribe de forma única como suma de monomios de distinto tipo,

$$p \coloneqq \sum_{i \in \mathbb{N}^n} p_i X_1^{i_1} \cdots X_n^{i_n},$$

con $p_i = 0$ para casi todo $i \in \mathbb{N}^n$.

PUAP en n indeterminadas: Sean A un anillo conmutativo, $n \in \mathbb{N}^*$ y $u : A \to A[X_1, \dots, X_n]$ la inclusión:

1. Dados un homomorfismo de anillos $f : A \to B$ y $b_1, \dots, b_n \in B$, existe un único homomorfismo de anillos $\tilde{f} : A[X_1, \dots, X_n] \to B$ tal que $\tilde{f} \circ u = f$ y $\tilde{f}(X_k) = b_k$ para $k \in \{1, \dots, n\}$.

2. Dados un anillo conmutativo P, $T_1, \ldots, T_n \in P$ y un homomorfismo $v : A \to P$ tales que, dados un homomorfismo de anillos $f : A \to B$ y $b_1, \ldots, b_n \in B$, existe un único homomorfismo $\tilde{f} : P \to B$ tal que $\tilde{f} \circ v = f$ y $\tilde{f}(T_k) = b_k$ para $k \in \{1, \ldots, n\}$, existe un isomorfismo $\phi : A[X_1, \ldots, X_n] \to P$ tal que $\phi \circ u = v$ y $\phi(X_k) = T_k$ para cada $k \in \{1, \ldots, n\}$.

Así:

1. Dados dos anillos conmutativos $A \subseteq B$ y $b_1, \ldots, b_n \in B$, el **homomorfismo de sustitución** $S : A[X_1, \ldots, X_n] \to B$ viene dado por $p(b_1, \ldots, b_n) := S(p) := \sum_{i \in \mathbb{N}^n} p_i b_1^{i_1} \cdots b_n^{i_n}$. Su imagen es el subanillo de B generado por $A \cup \{b_1, \ldots, b_n\}$, $A[b_1, \ldots, b_n]$, y dados dos homomorfismos de anillos $f, g : A[b_1, \ldots, b_n] \to C$, $f = g$ si y sólo si $f|_A = g|_A$ y $f(b_k) = g(b_k)$ para todo k.

2. Sean A un anillo y σ una permutación de $\mathbb{N}_n$ con inversa $\tau := \sigma^{-1}$, tomando $B = A[X_1, \ldots, X_n]$ y $b_k = X_{\sigma(k)}$ en el punto anterior obtenemos un automorfismo $\hat{\sigma}$ en $A[X_1, \ldots, X_n]$ con inversa $\hat{\tau}$ que permuta las indeterminadas.

3. $A[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \cong A[X_1, \ldots, X_n][Y_1, \ldots, Y_m] \cong A[Y_1, \ldots, Y_m][X_1, \ldots, X_n]$, por lo que en la práctica no distinguimos entre estos anillos.

4. Todo homomorfismo de anillos conmutativos $f : A \to B$ induce un homomorfismo $\hat{f} : A[X_1, \ldots, X_n] \to B[X_1, \ldots, X_n]$ dado por $\hat{f}(p) := \sum_{i \in \mathbb{N}^n} f(p_i) X_1^{i_1} \cdots X_n^{i_n}$.

Llamamos **grado** de un monomio $aX_1^{i_1} \cdots X_n^{i_n}$ a $i_1 + \cdots + i_n$, y grado de $p \in A[X_1, \ldots, X_n] \setminus 0$, $\operatorname{gr}(p)$, al mayor de los grados de los monomios no nulos en la expresión por monomios de p. Entonces $\operatorname{gr}(p+q) \leq \max\{\operatorname{gr}(p), \operatorname{gr}(q)\}$ y $\operatorname{gr}(pq) \leq \operatorname{gr}(p) + \operatorname{gr}(q)$.

Un polinomio es **homogéneo** de grado n si es suma de monomios de grado n. Todo polinomio se escribe de modo único como suma de polinomios homogéneos de distintos grados, sin más que agrupar los monomios de igual grado en la expresión como suma de monomios. Así, si D es un dominio, $\operatorname{gr}(pq) = \operatorname{gr}(p) + \operatorname{gr}(q)$ para cualesquiera $p, q \in D[X_1, \ldots, X_n]$.

Apéndice C

Coeficientes binomiales

$$\binom{n}{k} = \binom{n}{n-k}; \qquad \binom{r}{k} = (-1)^k \binom{k-r-1}{k};$$

$$\binom{r}{k} = \frac{r}{k}\binom{r-1}{k-1}, \qquad k \neq 0; \qquad \binom{n}{m} = (-1)^{n-m}\binom{-(m+1)}{n-m}, \qquad n \geq 0;$$

$$\binom{r}{k} = \frac{r}{r-k}\binom{r-1}{k}, \qquad k \neq r; \qquad \sum_{k=0}^{n}\binom{r+k}{k} = \binom{r+n+1}{n}, \qquad n \geq 0;$$

$$\binom{r}{k} = \binom{r-1}{k} + \binom{r-1}{k-1}; \qquad \sum_{k=0}^{n}\binom{k}{m} = \binom{n+1}{m+1}, \qquad m, n \geq 0;$$

$$\binom{r}{m}\binom{m}{k} = \binom{r}{k}\binom{r-k}{m-k}, \qquad \sum_{k}\binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n};$$

$$\sum_{k}\binom{r}{m+k}\binom{s}{n+k} = \binom{r+s}{r-m+n}, \quad \sum_{k}\binom{r}{k}\binom{s+k}{n}(-1)^{r-k} = \binom{s}{n-r}, \quad r \geq 0;$$

$$\sum_{k=0}^{r}\binom{r-k}{m}\binom{s}{k-t}(-1)^{k-t} = \binom{r-t-s}{r-t-m}, \qquad t, r, m \geq 0;$$

$$\sum_{k=0}^{r}\binom{r-k}{m}\binom{s+k}{n} = \binom{r+s+1}{m+n+1}, \qquad n \geq s \geq 0,\ m, r \geq 0;$$

$$\sum_{k\geq 0}\binom{r-tk}{k}\binom{s-t(n-k)}{n-k}\frac{r}{r-tk} = \binom{r+s-tn}{n};$$

$$\sum_{k}\binom{n}{k}x(x-kz)^{k-1}(y+kz)^{n-k} = (x+y)^n, \qquad x \neq 0;$$

$$\sum_{k}\binom{r}{k}x^k y^{r-k} = (x+y)^r, \qquad r \geq 0; \qquad \sum_{k}\binom{r}{k}x^k = (1+x)^r, \qquad r \geq 0 \text{ o } |x| < 1;$$