Anillos y Módulos

Notas para el curso de Anillos y Módulos 2021, dictado por
Mariana Haim y Paula Verdugo.
(Extraído y adaptado de las notas del curso de Álgebra I 2011)
Centro de Matemática.
Facultad de Ciencias - UdelaR

Índice general

Capítulo 1

Grupos

1.1. Generalidades

Definición 1.1.1 (Grupo)**.** Un *grupo* es una terna $(G, *, e)$, donde

- G es un conjunto,
- $* : G \times G \to G$ es una función
- $e \in G$

tal que se verifica:

(G1) $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$,

(G2) $a * e = e * a = a \quad \forall a \in G$,

(G3) para cada $a \in G$ existe $b \in G$ tal que $a * b = b * a = e$.

La función $*$ se dice la *operación* del grupo y el elemento e se dice *elemento neutro*, en virtud de la propiedad $(G2)$ (ver proposición 1.1.1.1).

La propiedad $(G1)$ se conoce como *asociatividad* del grupo y el elemento b que verifica $(G3)$ se dice *inverso*, a veces *opuesto* de a (ver proposición 1.1.1.2).

Una terna $(G, *, e)$ que verifica las propiedades $(G1)$ y $(G2)$ se dice *monoide*.

Cuando la operación y el neutro se sobreentienden, notamos el grupo o monoide G en lugar de $(G, *, e)$.

Muchas de las propiedades que probaremos para grupos valen también en el contexto de monoides, pero no es de interés para este curso generalizar la teoría a este nivel. La noción de monoide fue presentada porque nos será de utilidad en el capítulo siguiente.

Ejemplos 1.1.1 (Grupos)**.**

1. Los enteros con la suma $(\mathbb{Z}, +, 0)$.
2. Los racionales no nulos con el producto $(\mathbb{Q}^*, \cdot, 1)$.
3. Las matrices cuadradas invertibles con coeficientes reales con el producto $(\mathrm{GL}_n(\mathbb{R}), \cdot, I_n)$.
4. Las funciones biyectivas de un conjunto en sí mismo con la composición $(\mathrm{Biy}(A), \circ, \mathrm{Id}_A)$.

Proposición-Definición 1.1.1.

1. **Unicidad del neutro:** Si $e' \in G$ verifica $e' * a = a * e' = a$, entonces $e = e'$.

2. **Unicidad del inverso de un elemento dado:** Dados $a, b, c \in G$, si tenemos $a * b = b * a = e$ y $a * c = c * a = e$, entonces $b = c$. Esto nos permite notar a^{-1} al (único) inverso de a.

3. **Propiedad cancelativa:** Dados $a, b, c \in G$ si $a * b = a * c$ entonces $b = c$.

Demostración. 1. Si $e' * a = a$, por $(G2)$ se tiene $e' * a = e * a$ y para $b \in G$ se tiene $(e' * a) * b = (e * a) * b$. Aplicando $(G1)$ se deduce $e' * (a * b) = e * (a * b)$. Tomando b como en $(G3)$ obtenemos $e' * e = e * e$ de donde $e' = e$ por $(G2)$.

2. Es claro poniendo $b = b * e = b * (a * c) = (b * a) * c = e * c = c$ (a partir de ahora queda como ejercicio para el lector verificar qué axiomas o propiedades de los grupos se usan en cada paso de las demostraciones).

3. Se deduce como sigue:

$$b = e * b = (-a * a) * b = -a * (a * b) = -a * (a * c) = (-a * a) * c = e * c = c$$

□

Definición 1.1.2 (Subgrupo)**.** Un subconjunto $H \subseteq G$ se dice *subgrupo* de G si

- $a * b \in H \quad \forall a, b \in H$,
- $0 \in H$,
- $-a \in H \quad \forall a \in H$.

Si H es un subgrupo de G notamos $H \leqslant G$.

Definición 1.1.3 (Submonoide)**.** Si G es un monoide y H es un subconjunto de G. Decimos que H es un submonoide si verifica las primeras dos condiciones de la definición anterior.

Observación 1.1.1. Todo subgrupo es un grupo.
Todo submonoide es un monoide.

Ejemplos 1.1.2 (Subgrupos)**.** 1. Si tomamos el grupo de los complejos con la suma usual $(\mathbb{C}, +, 0)$, tenemos:

$$\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$$

y para todo $n \in \mathbb{N}$, $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} \leqslant Z$.

2. Además $0 := \{e\} \leqslant G$ y $G \leqslant G$. Decimos que 0 y G son los subgrupos triviales de G.

En la siguiente proposición, presentamos dos construcciones clásicas de la Teoría de Grupos.

Proposición 1.1.1. *1. Sea G un grupo. Si H y K son subgrupos de G entonces también lo es $H \cap K$.*

2. Si H, K son grupos, el producto cartesiano $H \times K$ tiene estructura de grupo definiendo $(h, k) * (h', k') := (h * h', k * k')$.
Notamos $H \times K := (H \times K, *, (e, e))$ y lo llamamos producto directo *de H y K.*

Demostración. A cargo del lector. □

1.2. Grupos abelianos

En este curso trabajaremos únicamente con grupos cuya operación es conmutativa, reciben el nombre de Grupos Abelianos.

Definición 1.2.1 (Grupo abeliano)**.** Un grupo $(G, +, 0)$ se dice *abeliano* si se verifica:

(G4) $a + b = b + a \quad \forall a, b \in G$.

La propiedad (G4) se conoce como *conmutatividad.*

En el caso abeliano, la operación suele notarse $+$ y llamarse *suma* del grupo. Además el neutro suele notarse 0, y el inverso de $a \in G$ suele llamarse *opuesto* y notarse $-a$.

Observaciones 1.2.1.

1. Los grupos de los ejemplos 1.1.1.1 y 1.1.1.2 son abelianos. Los de los ejemplos 1.1.1.3 y 1.1.1.4 no lo son.
2. Todo subgrupo de un grupo abeliano es un grupo abeliano.

Proposición 1.2.1 (Suma de subgrupos)**.** *Si H y K son subgrupos de G y G es abeliano, entonces:*

- $H + K := \{h + k \mid h \in H, k \in K\}$ *es un subgrupo de G.*
- *Son equivalentes:*
  - *(i)* $H \cap K = \{0\}$,
  - *(ii) Si $h, h' \in H, k, k' \in K$ son tales que $h + k = h' + k'$ entonces $h = h', k = k'$.*

  En este caso se dice que la suma de H y K es directa *y se nota $H \oplus K$ en lugar de $H + K$.*

Demostración.

- Tenemos que $0 = 0 + 0 \in H + K$. Si $h + k, h' + k' \in H + K$, se tiene:

$$\begin{aligned}(h + k) - (h' + k') &= h + (k - h') - k' \\ &= h + (-h' + k) - k' \\ &= h - h' + k - k' \\ &= (h - h') + (k - k') \in H + K\end{aligned}$$

- Si $h + k = h' + k'$, entonces $h - h' = k' - k \in H \cap K = \{0\}$. Por lo tanto $h - h' = 0$ y $k - k' = 0$, de donde $h = h'$, $k = k'$.

  Recíprocamente, sea $g \in H \cap K$. Como $g, 0 \in H$, $0, g \in K$ cumplen $g + 0 = 0 + g$ se deduce que $g = 0$. □

1.3. Morfismos de grupos

En esta sección nos referimos a grupos generales (no necesariamente abelianos) pero mantenemos la notación utilizada en el contexto abeliano.

Definición 1.3.1 (Morfismo de grupos)**.** Sean $(A, *, 0_A)$ y $(B, *, 0_B)$ grupos y $f : A \to B$ una función. Decimos que f es un *morfismo de grupos*, si:

$$f(x * y) = f(x) * f(y) \quad \forall x, y \in A$$

Proposición 1.3.1. *Sea $f : A \to B$ morfismo de grupos.*

1. $f(0_A) = 0_B$,
2. $f(-x) = -f(x) \ \forall x \in A$,

Demostración. A cargo del lector. □

Para $X \subseteq A, Y \subseteq B$ y $f : A \to B$ una función, recordamos que

$$f(X) = \{f(x) \mid x \in X\}, \quad f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Proposición 1.3.2.
1. *Si $f : A \to B$ y $g : B \to C$ son morfismos de grupos, entonces $g \circ f : A \to C$ es morfismo de grupos.*
2. *Si A es un grupo, entonces $\mathrm{id}_A : A \to A$ es un morfismo de grupos.*
3. *Sea $f : A \to B$ morfismo de grupos.*
   Si $K \leqslant A$, entonces $f(K) \leqslant B$. Si $H \leqslant B$, entonces $f^{-1}(H) \leqslant A$.

Demostración. A cargo del lector. □

Recordamos que todo grupo tiene como subgrupo al conjunto formado únicamente por el elemento neutro. Dicho subgrupo lo notamos siembre 0.

Definición 1.3.2 (Núcleo e imagen)**.** Sea $f : A \to B$ morfismo de grupos. El *núcleo* y la *imagen* de f son respectivamente:

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = e_B\}, \quad \mathrm{Im}\,(f) = \{b \in B \mid \exists a \in A : f(a) = b\}.$$

Proposición 1.3.3.
1. $\mathrm{Ker}(f) \leqslant A, \mathrm{Im}\,(f) \leqslant B$.
2. *f es inyectiva si y sólo si $\mathrm{Ker}(f) = 0$, f es sobreyectiva si y sólo si $\mathrm{Im}\,(f) = B$.*
3. *La función $O : A \to B$ definida por $O(x) = e_B, \forall x \in B$ es un morfismo de grupos con núcleo A e imagen el grupo 0.*

Dem. A cargo del lector.

Definición 1.3.3. Un morfismo de grupos inyectivo se dice *monomorfismo de grupos.*

Un morfismo de grupos sobreyectivo se dice *epimorfismo de grupos.*

Un morfismo de grupos biyectivo se dice *isomorfismo de grupos.* Además si existe un isomorfismo de grupos $f : A \to B$ decimos que A y B son grupos *isomorfos* (o *isomorfos via f* si queremos explicitar el isomorfismo) y notamos $A \cong B$ (o $A \cong_f B$).

Un morfismo $G \to G$ se dice *endomorfismo* de G.

Un isomorfismo $G \to G$ se dice *automorfismo* de G.

Proposición 1.3.4.
1. *Si $f : A \to B$ es un isomorfismo de grupos, entonces $f^{-1} : B \to A$ es un (iso)morfismo de grupos.*
2. *Si G es un grupo, entonces $Aut(G) = \{f : G \to G \mid f$ es isomorfismo$\}$ es un grupo con la composición.*

Demostración. A cargo del lector. □

Lema 1.3.5. *Sea $(G, +, 0)$ un grupo abeliano y $H, K \leqslant G$. Sea además $f : H \times K \to H + K$ definida por $f(h, k) = h + k$. Entonces:*

- *f es un epimorfismo de grupos,*
- *f es un isomorfismo si y sólo si $H \cap K = \{0\}$.*

Demostración. Es fácil ver que f es epimorfismo de grupos.

Supongamos ahora que $H \cap K = \{0\}$. Veamos que $\operatorname{Ker} f = \{0\}$: $f(h,k) = 0$ implica $h = -k \in H \cap K$ y por tanto $h = k = 0$.

Recíprocamente, si f es inyectiva, tomemos $x \in H \cap K$. Como $f(x,-x) = x - x = 0$ se tiene $(x,-x) = (0,0)$ y por tanto $x = 0$. □

Observación 1.3.1. La segunda afirmación puede expresarse como sigue: si H y K son subgrupos de un grupo abeliano G cuya suma es directa, entonces se tiene

$$H \times K \cong H \oplus K.$$

Por esta razón estos grupos suelen llamarse en el caso abeliano *suma directa externa* de H y K y *suma directa interna* de H y K respectivamente, o solamente *suma directa* de H y K si no interesa la distinción.

1.4. Grupo cociente

Proposición-Definición 1.4.1 (Congruencia)**.** Sean A un grupo y $H \leqslant A$. La relación en A definida por:

$$a \equiv_H b \Leftrightarrow a - b \in H \quad (a, b \in A)$$

es una relación de equivalencia, que llamamos relación de *conAruencia módulo H*.

Demostración. Es reflexiva porque $0 \in H$, es simétrica porque H es cerrado por opuestos y es transitiva porque H es cerrado por la suma. □

Proposición-Definición 1.4.2. Sea A un grupo abeliano y $H \leqslant A$. Notemos $\overline{a}$ a la clase de equivalencia de $a \in A$.

1. Si $a \equiv_H a'$ y $b \equiv_H b'$, entonces $a + b \equiv_H a' + b'$.
2. Si definimos
   $$+ : A/_{\equiv_H} \times A/_{\equiv_H} \to A/_{\equiv_H}$$
   mediante $\overline{a} + \overline{b} = \overline{a+b}$, entonces $(A/_{\equiv_H}, +, \overline{0})$ es un grupo que llamamos *grupo cociente* de A por H y notamos $\frac{A}{H}$.
3. La función $\pi_H : A \to \frac{A}{H}$ definida por $\pi_H(x) = \overline{x}, \forall x \in A$ es un epimorfismo de grupos que llamamos *proyección canónica* de A en el cociente $\frac{A}{H}$.

Demostración.

1. En efecto, $(a+b)-(a'+b') = (a-a')+(b-b') \in H$ porque $a-a', b-b' \in H$ (observar que se usa fuertemente la conmutatividad en A).
2. Por la parte anterior, tiene sentido la definición. Es fácil ver que esta nueva operación "hereda" las propiedades de A, en otras palabras: de la asociatividad de la operación de A se deduce la asociatividad de esta nueva operación; de la conmutatividad se deduce la nueva conmutatividad, el nuevo neutro es $\overline{0}$ y $-\overline{a} = \overline{-a}, \ \forall a \in A$.
3. A carAo del lector. □

Observación 1.4.1. Observar que $\overline{0} = \{x \in A \mid x - 0 \in H\} = H$ y que

$$\frac{A}{\{0\}} \cong A; \quad \frac{A}{A} = \{0\}.$$

Teorema 1.4.1 (Propiedad Universal del Cociente)**.** *Sea $f : A \to B$ un morfismo de grupos. Si A es abeliano y $H \leqslant \operatorname{Ker} f$, existe un único morfismo $\hat{f} : \frac{A}{H} \to B$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_H"'] & B \\ \frac{A}{H} \arrow[ur, dotted, "\hat{f}"'] & \end{tikzcd}$$

Además, se tiene $\operatorname{Im} \hat{f} = \operatorname{Im} f$ *y* $\operatorname{Ker} \hat{f} = \frac{\operatorname{Ker} f}{H}$.

Demostración. Para que el diagrama conmute, es necesario que $\hat{f}(\overline{a}) = f(a)$, lo que prueba la unicidad.

Para la existencia, veamos que tiene sentido definir $\hat{f}(\overline{a}) := f(a)$: en efecto, si $a \equiv a'$, entonces $a - a' \in H \subseteq \operatorname{Ker} f$ y por tanto $f(a) - f(a') = f(a - a') = 0$. Queda a cargo del lector verificar que la función $\hat{f}$ así definida es un morfismo de grupos.

Es claro que las imágenes de f y $\hat{f}$ coinciden. Por otro lado como $H \subseteq \operatorname{Ker} f$ tiene sentido considerar el grupo $\frac{\operatorname{Ker} f}{H}$. Además:

$$\overline{a} \in \frac{\operatorname{Ker} f}{H} \iff a \in \operatorname{Ker} f \iff f(a) = 0 \iff \hat{f}(\overline{a}) = 0 \iff \overline{a} \in \operatorname{Ker} \hat{f} \qquad \square$$

Corolario 1.4.2 (Teoremas de isomorfismo)**.** *Sea A un grupo abeliano.*

1. *Si $f : A \to B$ es un morfismo de grupos, entonces $\frac{A}{\operatorname{Ker} f} \cong \operatorname{Im} f$.*

2. *Si $H, K \leqslant A$ entonces $\frac{H+K}{H} \cong \frac{K}{H \cap K}$.*

3. *Si $H \leqslant K \leqslant A$ entonces $\frac{A/H}{K/H} \cong \frac{A}{K}$.*

4. *Si $f : A \to B$ es un morfismo de grupos, con B también abeliano, y $H \leqslant A, K \leqslant B$ con $f(H) \subseteq K$, entonces existe un único morfismo $\tilde{f} : \frac{A}{H} \to \frac{B}{K}$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_H"'] & B \arrow[d, "\pi_K"] \\ \frac{A}{H} \arrow[r, dotted, "\tilde{f}"'] & \frac{B}{K} \end{tikzcd}$$

Demostración. 1. En el contexto del teorema anterior, se deduce que $\hat{f} : \frac{A}{\operatorname{Ker} f} \to B$ es morfismo de grupos con $\operatorname{Im} \hat{f} = \operatorname{Im} f$ y $\operatorname{Ker} \hat{f} = \frac{\operatorname{Ker} f}{\operatorname{Ker} f} = 0$, por lo que $\hat{f} : \frac{A}{\operatorname{Ker} f} \to \operatorname{Im} f$ es un isomorfismo.

2. Sea $f : K \to \frac{H+K}{H}$ definida por $f(k) = \overline{k}$. Es claro que f es un morfismo de grupos. Además si $\overline{h + k} \in \frac{H+K}{H}$ entonces $\overline{h + k} = \overline{k} = f(k)$ por lo que $\operatorname{Im} f = \frac{H+K}{H}$. Por otra parte $f(k) = 0$ si y sólo si $k \in H$ de donde $\operatorname{Ker} f = H \cap K$. Usando la parte anterior, se deduce la tesis.

3. Consideremos $\pi_H : A \to \frac{A}{H}$ la proyección canónica. Es claro que $\pi_H(K) = \frac{K}{H}$ por lo que aplicando la parte 4 se tiene que π_H induce un morfismo $\tilde{\pi_H} : A/K \to \frac{A/H}{K/H}$ que verifica $\tilde{\pi_H}([a]_K) = \overline{[a]_H}$, donde $[a]_H$ denota la clase de equivalencia de $a \in A$ según la congruencia módulo H y $\overline{x}$ denota la clase de equivalencia de $x \in A/H$ módulo K/H. Queda a cargo del lector verificar que $\tilde{\pi_H}$ es efectivamente un isomorfismo.

4. A cargo del lector. □

Teorema 1.4.3. *Sea G un grupo abeliano y $H \leqslant G$. Existe una correspondencia biyectiva entre los conjuntos:*

$$\mathcal{F}_1 = \left\{ L \leqslant \frac{G}{H} \right\} \quad y \quad \mathcal{F}_2 = \{K \leqslant G \mid K \supseteq H\}$$

que preserva la inclusión.

Demostración. Sean $\Lambda : \mathcal{F}_2 \to \mathcal{F}_1$ definida como $\Lambda(K) = \frac{K}{H}$ y $\Omega : \mathcal{F}_1 \to \mathcal{F}_2$ definida como $\Omega(L) = \pi_H^{-1}(L)$.

Observar primero que $\Lambda(K) = \frac{K}{H} = \pi_H(K)$ es un subgrupo de $\frac{G}{H}$ y que $\Omega(L) \supseteq \pi_H^{-1}(\{0\}) = H$.

Queda para el lector verificar que estas funciones son inversas entre sí.

Por otra parte, es claro que si $L \subseteq L'$ entonces $\Lambda(L) = \pi_H(L) \subseteq \pi_H(L') = \Lambda(L')$. □

Capítulo 2

Anillos

2.1. Generalidades

2.1.1. Definiciones generales

Definición 2.1.1 (Anillo)**.** Un anillo es una quíntupla $(A, +, \cdot, 0, 1)$ donde

(A1) $(A, +, 0)$ es un grupo abeliano,

(A2) $(A, \cdot, 1)$ es un monoide,

(A3) Propiedad distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c, \ \ (a + b) \cdot c = a \cdot c + b \cdot c, \ \ \forall a, b, c \in A.$

Si además se cumple $a \cdot b = b \cdot a \ \forall a, b \in A$ se dice que el anillo es *conmutativo*. Cuando las operaciones y los neutros se sobreentienden, decimos "el anillo A" en lugar de "el anillo $(A, +, \cdot, 0, 1)$". Las operaciones $+$ y $\cdot$ se llaman usualmente la *suma* y el *producto* de un anillo.

Observación 2.1.1. La definición anterior merece dos aclaraciones:

- Algunas definiciones de *anillo* que aparecen en la literatura no exigen la existencia de neutro para $\cdot$ y llaman *anillo con unidad* a una quíntupla como la de la definición 2.1.1.
- A menudo notaremos ab en lugar de $a \cdot b$, para $a, b \in A$.

Ejemplos 2.1.1 (Anillos)**.**

1. Los enteros con la suma y el producto usual $(\mathbb{Z}, +, \cdot, 0, 1)$.
2. Los reales con la suma y el producto usual $(\mathbb{R}, +, \cdot, 0, 1)$.
3. El anillo de las matrices cuadradas de tamaño $n \in \mathbb{N}$ con coeficientes en $\mathbb{R}$, con la suma y el producto usual de matrices $(M_n(\mathbb{R}), +, \cdot, 0, I_n)$. Es un anillo no conmutativo $\forall n \geqslant 2$.
4. El anillo trivial $A = \{0\}$ con $0 = 1$.
5. De manera similar al ejemplo anterior, si A es un anillo y n un natural, puede definirse una suma y un producto en el conjunto de las matrices cuadradas de tamaño n con coeficientes en A y se obtiene un anillo que se nota $M_n(A)$. Es no conmutativo $\forall n \geqslant 2$ si A no es el anillo trivial.
6. El anillo de los polinomios en una variable con coeficientes en $\mathbb{R}$, con la suma y el producto usual de polinomios $(\mathbb{R}[x], +, \cdot, 0, 1)$. Es un anillo conmutativo.

7. El ejemplo anterior puede generalizarse a polinomios con coeficientes en un anillo A. Este anillo se nota $A[x]$.[1] Es claro que $A[x]$ es conmutativo si y sólo si A lo es.

8. Si A es un anillo y S es un conjunto no vacío, el conjunto de las funciones de S en A se nota A^S o también $\mathrm{Fun}(S, A)$, y es un anillo con las operaciones heredadas de A, es decir $(f+g)(s) = f(s) +_A g(s), (f \cdot g)(s) = f(s) \cdot_A g(s), \forall s \in S$. Si A es un conmutativo, también lo es A^S.

Proposición 2.1.1 (Propiedades elementales)**.** *Sea* $(A, +, \cdot, 0, 1)$ *un anillo. Entonces:*

1. 0 *y* 1 *son únicos.*

2. *Para todos* $a, b \in A$*:* $(-a) \cdot b = -(ab) = a \cdot (-b), \quad (-a) \cdot (-b) = a \cdot b.$

3. *Para* $a \in A, n \in \mathbb{Z}$*, notamos* $na = \begin{cases} a + a \cdots + a \ \ (nveces) & si\ n \geqslant 0 \\ (-a) + (-a) + \cdots + (-a) \ \ (nveces & si\ n < 0 \end{cases}$.
   Se tiene, para $n \in \mathbb{Z}, a, b \in A$ *las siguientes igualdades:*
$$(na) \cdot b = n(a \cdot b) = a \cdot (nb).$$

Demostración. A cargo del lector. □

Definición 2.1.2. Decimos que $a \in A$ es *invertible*, si existe $b \in A$ tal que $a \cdot b = b \cdot a = 1$.

Observación 2.1.2. Es fácil ver que para cada $a \in A$ existe un único $b \in A$ como en la definición. Decimos que es el *inverso* de a y lo notamos a^{-1}.

Proposición 2.1.2. *Sea* $(A, +, \cdot, 0, 1)$ *un anillo no trivial. Si definimos* $A^\times = U(A) := \{a \in A \mid a \text{ es invertible}\}$*, la terna* $(U(A), \cdot, 1)$ *es un grupo.*

Demostración. Primero veamos que si $a, b \in A$ son invertibles, entonces ab también lo es, y su inverso es $b^{-1}a^{-1}$. En efecto $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$. El producto es entonces una operación en $U(A)$, que además es asociativa.
Por otra parte 1 es invertible ($1 \cdot 1 = 1$ luego $1^{-1} = 1$), por lo que $U(A)$ tiene neutro.
Finalmente, todo elemento de $U(A)$ es invertible por definición. □

Ejemplos 2.1.2 (Invertibles)**.**

- $U(M_n(\mathbb{R})) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$.
- $U(\mathbb{R}[x]) = \{p \in \mathbb{R}[x] \mid p \text{ constante } p \neq 0\}$.

Definición 2.1.3 (Subanillo)**.** Sea $(A, +, \cdot, 0, 1)$ un anillo. Un subconjunto $B \subseteq A$ se dice *subanillo* si B es un subgrupo de $(A, +, 0)$ y B es un submonoide de $(A, \cdot, 1)$.

Ejemplo 2.1.1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ son dos a dos subanillos.

Proposición 2.1.3. *Sea* $(A, +, \cdot, 0, 1)$ *un anillo,* $B \subset A$ *un subconjunto. Son equivalentes:*

1. B *es un subanillo de* A*,*

2. $1 \in B$ *y* $a, b \in B \Rightarrow a - b \in B$ *y* $ab \in B$*,*

3. $(B, +_{|B \times B}, \cdot_{|B \times B}, 0, 1)$ *es un anillo.*

Demostración. A cargo del lector. □

[1] En la sección 2.1.3 daremos una construcción formal de $A[x]$.

Definición 2.1.4 (Morfismo de anillos)**.** Sean A, B anillos y $f : A \to B$ una función. Decimos que f es un *morfismo de anillos* si:

- $f(a + b) = f(a) + f(b) \quad \forall a, b \in A$,
- $f(ab) = f(a)f(b) \quad \forall a, b \in A$,
- $f(1_A) = 1_B$.

Un morfismo de anillos f se dice *monomorfismo, epimorfismo* o *isomorfismo de anillos* si es respectivamente inyectivo, sobreyectivo o biyectivo.

Dos anillos A y B se dicen *isomorfos* (o *isomorfos via* f) si existe un isomorfismo de anillos $f : A \to B$.

Un *endomorfismo* de A es un morfismo de anillos $A \to A$. Notaremos $\mathrm{End}(A)$ al conjunto de endomorfismos de A.

Un endomorfismo que es un isomorfismo se dice un *automorfismo*. Notaremos por $\mathrm{Aut}(A)$ al conjunto de automorfismos de A.

Observación 2.1.3.

1. Es claro que si $f : A \to B$ un morfismo de anillos en particular $f : (A, +_A, 0_A) \to (B, +_B, 0_B)$ es morfismo de grupos y $f : (A, \cdot_A, 1_A) \to (B, \cdot_B, 1_B)$ es morfismo de monoides. Entonces $f(0) = 0, f(-a) = -f(a) \quad \forall a \in A$, por i $a \in A$ es invertible, entonces $f(a) \in B$ es invertible y $f(a)^{-1} = f(a^{-1})$. En otras palabras, $f_{|U(A)} : U(A) \to U(B)$ es un morfismo de grupos (con la estructura de grupo en los invertibles definida en la proposición 2.1.2).

2. Considerando a f como morfismo de grupos bajo las estructuras aditivas de A y B, se tiene que se pueden definir $Ker(f)$ e $Im(f)$ y además:
   - $\mathrm{Im}(f) \subseteq B$ es un subanillo.
   - $\mathrm{Ker}(f) \subseteq A$ es un subgrupo aditivo.

3. La composición de morfimos de anillos es un morfismo de anillos, la identidad es un morfismo de anillos, la inversa de un morfismo de anillos biyectivo es un morfismo de anillos. En otras palabras $\mathrm{Aut}(A)$ es un grupo con la composición.

4. Es necesario pedir que un homomorfismo de anillos $f : A \to B$ cumpla $f(1) = 1$. Si bien todo morfismo de grupos cumple automáticamente que $f(0) = 0$, esto no es cierto para los monoides, por lo tanto debemos pedirlo si queremos que f respete la unidad. Por ejemplo, sea $f : \mathbb{R} \to M_2(\mathbb{R})$ definida por $f(a) = \left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Entonces f respeta la suma y el producto, pero $f(1) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

2.1.2. Anillos especiales y ejemplos

Es claro que la igualdad $ab = 0$ en un anillo no implica $a = 0$ o $b = 0$ (basta mirar un anillo de matrices por ejemplo). Esta propiedad es interesante y muy útil en esta teoría, por lo que tiene relevancia la siguiente definición.

Definición 2.1.5 (Divisor de cero)**.** Sea A un anillo. Un elemento $a \in A, a \neq 0$ se dice *divisor de cero* si existe $b \in A, b \neq 0$, tal que $ab = 0$ o $ba = 0$.

Ejemplos 2.1.3 (Divisores de cero)**.**

- La matriz $A = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ es un divisor de cero en $M_2(\mathbb{R})$ (se verifica por ejemplo $A \cdot A = 0$ y $A \neq 0$).

- Sea A un anillo no trivial. En el anillo A^S, toda función no nula que admite una raíz es divisor de cero. En efecto, si $f : S \to A$ es no nula y tal que para cierto $s \in S$ se tiene $f(s) = 0$, entonces, tomando $g : S \to A$ tal que $g(t) = 0 \forall t \neq s$ y $g(s) \neq 0$, se tiene $(fg)(x) = 0, \forall x \in S$ y $g \neq 0$.

Observación 2.1.4. Los invertibles no son divisores de cero. En efecto, tomemos $a, b \in A$ tal que $ab = 0$. Si a es invertible, entonces $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Análogamente se prueba que si $ba = 0$ entonces $b = 0$.

Algunos anillos tienen buenas propiedades que tienen que ver con sus invertibles y sus divisores de cero. Los presentamos en la siguiente definición.

Definición 2.1.6. Sea A un anillo, $A \neq \{0\}$. Decimos que A es un

- *dominio de integridad* o simplemente *dominio* si es conmutativo y no tiene divisores de cero,
- *anillo con división* si todo elemento no nulo es invertible,
- *cuerpo* si es un anillo con división conmutativo.

Observación 2.1.5. De la observación 2.1.4 se deduce que todo cuerpo es un dominio.

Ejemplos 2.1.4 (Anillos especiales)**.** 1. Todo cuerpo es un dominio.

2. Cualquier subanillo de un dominio es un dominio. En particular los subanillos de $\mathbb{R}$ son dominios, como por ejemplo $\mathbb{Z}, \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

3. El subanillo (conmutativo) $C[0,1] \subseteq \mathbb{R}^{[0,1]}$ de las funciones continuas en $[0,1]$ a valores reales no es un dominio.

4. Consideremos en $\mathbb{R}^4$ una base que notaremos $\{1, i, j, k\}$. Consideremos el conjunto $\mathbb{H} = \{a1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\} = \mathbb{R}^4$ con la suma definida mediante:

$$(a1 + bi + cj + dk) + (a'1 + b'i + c'j + d'k) = (a + a')1 + (b + b')i + (c + c')j + (d + d')k$$

para todo $a, a', b, b', c, c', d, d' \in \mathbb{R}$, y el producto definido a partir de

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik$$

y extendiendo por linealidad. Se puede ver que esto define una estructura de anillo en $\mathbb{H}$. Este anillo recibe el nombre de *anillo de los cuaterniones* y es un ejemplo de anillo con división que no es un cuerpo. En efecto, todo elemento no nulo $a1 + bi + cj + dk$ tiene por inverso a $\frac{1}{a^2+b^2+c^2+d^2}(a1 - bi - cj - dk)$. Por otra parte, $\mathbb{H}$ no es conmutativo.

5. Para $n \geqslant 2$ y $A \neq \{0\}$, el anillo de matrices $M_n(A)$ no es un dominio.

Definición 2.1.7 (Subanillo generado)**.** Si $S \subset A$ es un subconjunto de un anillo, el *subanillo generado* por S es $\langle S \rangle := \bigcap \{B \mid B \text{ es subanillo de } A, B \supset S\}$.

2.1.3. Series formales y polinomios

2.1.4. Series formales con coeficientes en un anillo A

Dado un anillo consideramos el conjunto $A^{\mathbb{N}}$ de sucesiones con términos en A. Definimos en $A^{\mathbb{N}}$ las operaciones

$$(f+g)(n) = f(n) + g(n), \quad (f \star g)(n) = \sum_{k+l=n} f(k)g(l),$$

y las funciones $0, \delta_n : \mathbb{N} \to A$ dadas por $0(k) = 0, \forall k \in \mathbb{N}$ y $\delta_n(k) = \begin{cases} 1 & \text{si } n = k \\ 0 & \text{si no} \end{cases}$.

En este contexto, la siguiente observación es fácil de verificar.

Observación 2.1.6.

- $(A^{\mathbb{N}}, +, \star, 0, \delta_0)$ es un anillo. El producto se llama *producto de convolución*, *producto de Cauchy* o sencillamente *convolución*, y es conmutativo si y sólo si A es un anillo conmutativo.
- Si definimos $x = \delta_1$ (que llamaremos la *indeterminada*), entonces $x^n = \delta_n, \forall n \in \mathbb{N}$.
- Para cada $n \in \mathbb{N}$, la aplicación $\varphi_n : A \to A^{\mathbb{N}}$ definida por $\varphi_n(a)(k) = \begin{cases} a & \text{si } n = k \\ 0 & \text{si no} \end{cases}$ es un monomorfismo de grupos que verifica $\varphi_n(ab) = \varphi_0(a)\varphi_n(b), \forall a, b \in A$ y $\varphi_n(1) = x^n$. En particular φ_0 es un monomorfismo de anillos.

A partir de la observación anterior, podemos escribir los elementos de $A^{\mathbb{N}}$ como:

$$(a_n)_n = \sum_{n=0}^{\infty} \varphi_n(a_n) = \sum_{n=0}^{\infty} \varphi_n(a_n \cdot 1) = \sum_{n=0}^{\infty} \varphi_0(a_n) \star x^n = \sum_{n=0}^{\infty} a_n x^n,$$

donde en la última igualdad, estamos haciendo un doble abuso de notación: identificamos el anillo A con su copia en $A^{\mathbb{N}}$ y eliminamos la $\star$ del producto de convolución.

Por esta razón es que este anillo recibe el nombre de *anillo de las series formales (en una variable) con coeficientes en A*. Decimos que a_n es el *coeficiente n-ésimo* de la serie $\sum_{n=0}^{\infty} a_n x^n$. El anillo se nota $A[[x]]$ y bajo la nueva notación, las operaciones se explicitan como sigue:

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) + \left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$
$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} \left(\sum_{k+\ell=n} a_k b_\ell\right) x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n.$$

A partir de ahora notaremos fg para $f \star g$.

2.1.5. Polinomios con coeficientes en un anillo A

Dado $f \in A^{\mathbb{N}}$, definimos el *soporte* de f como $\mathrm{sop}(f) = \{n \in \mathbb{N} \mid f(n) \neq 0\}$. El subconjunto $\{f \in A[[x]] \mid \sharp\mathrm{sop}(f) < \infty\}$ es un subanillo de A que llamamos *anillo de polinomios con coeficientes en* A y notamos $A[x]$. Más específicamente, cada elemento de $A[x]$ se dice *polinomio con coeficientes en* A.

Es fácil ver que $A[x]$ es un anillo conmutativo si y sólo si lo es A. Más aún, $A[x]$ es el subanillo de $A[[x]]$ generado por $A \cup \{x\}$.

Observar que se tiene la cadena de inclusiones de anillos: $A \subset A[x] \subset A[[x]]$ (donde un elemento $a \in A$ se piensa en $A[x]$ como el polinomio con soporte $\{0\}$ y único coeficiente a).

Teorema 2.1.4 (Propiedad universal del anillo de polinomios)**.** *Sea $\varphi : A \to B$ un morfismo de anillos. Para cada elemento $b \in B$ que conmuta con $Im(\varphi)$ existe un único morfismo de anillos $\hat{\varphi} : A[x] \to B$ y $\varphi(x) = b$ que extiende a φ.*

En otras palabras, para cada $b \in B$ tal que $\varphi(a)b = b\varphi(a), \forall a \in A$, existe un único morfismo de anillos que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\iota"'] & B \\ A[x] \arrow[ur, dotted, "\hat{\varphi}"'] & \end{tikzcd}$$

donde $\iota : A \to A[x]$ denota la inclusión.

Demostración. Es fácil probar que una función $\hat{\varphi} : A[x] \to B$ es un morfismo de grupos y que verifica $\hat{\varphi}(a) = \varphi(a)\ \forall a \in A$ si y sólo si $\hat{\varphi}\left(\sum_{k=0}^{n} a_i x^i\right) = \sum_{k=0}^{n} \varphi(a_i) b^i$. La condición de que b conmuta con $\operatorname{Im}(\varphi)$ asegura la multiplicatividad de $\hat{\varphi}$. $\square$

Observación 2.1.7. En el caso particular en que B es conmutativo, la condición de que b conmuta con $\operatorname{Im}(\varphi)$ se verifica trivialmente.

Ejemplo 2.1.2. Tomando en la proposición anterior $A = \mathbb{Z}, B = \mathbb{R}, \varphi : \mathbb{Z} \to \mathbb{R}$ la inclusión y $b = \sqrt{2}$, tenemos

$$\hat{\varphi}\left(\sum_{k=0}^{n} a_i x^i\right) = \sum_{k=0}^{n} a_i (\sqrt{2})^i.$$

Se tiene $\operatorname{Im}(\hat{\varphi}) = \mathbb{Z}[\sqrt{2}]$.

2.1.6. Generalización a varias indeterminadas

Si queremos definir el anillo de las series formales en dos variables con coeficientes en A, tomamos el conjunto $\{f : \mathbb{N} \times \mathbb{N} \to A\}$, con las operaciones:

$$(f+g)(n,m) = f(n,m) + g(n,m), \qquad (fg)(n,m) = \sum_{\substack{k+l=n \\ q+r=m}} f(k,q)\, g(l,r)$$

Se trabaja análogamente que en el caso de una variable y se nota al anillo obtenido $A[[x,y]]$. Con identificaciones análogas, se obtiene que:

$$A[[x,y]] = \left\{ \sum_{i+j \geqslant 0} a_{ij} x^i y^j \mid a_{ij} \in A \right\}$$

Los polinomios en dos variables con coeficientes en A corresponden al subanillo $A[x,y] = \{f \in A[[x,y]] \mid \sharp\mathrm{sop}(f) < \infty\}$. Con identificaciones análogas, se obtiene que:

$$A[x,y] = \left\{ \sum_{i+j=0}^{n} a_{ij} x^i y^j \mid a_{ij} \in A, n \in \mathbb{N} \right\}$$

Se tiene además que $A[[x,y]] \cong A[[x]][[y]] \cong A[[y]][[x]]$ y que $A[x,y] \cong A[x][y] \cong A[y][x]$. En efecto, las aplicaciones:

$$\begin{array}{ll} \varphi : A[[x,y]] \to A[[x]][[y]] & \psi : A[[x,y]] \to A[[y]][[x]] \\ \varphi(f)(n) \in A[[x]], (\varphi(f)(n))(m) = f(m,n) & \psi(f)(n) \in A[y], (\psi(f)(n))(m) = f(n,m) \end{array}$$

definen isomorfismos de anillos cuyas restricciones a $A[x,y]$ tienen respectivamente por imagen a $A[x][y]$ y $A[y][x]$ (subanillos de $A[[x]][[y]]$ y $A[[y]][[x]]$ respectivamente). Observar por ejemplo que se tiene

$$\begin{aligned} f &= 5 + xy^2 - xy^3 + 3x^2 - 2x^2y^3 \ \in \mathbb{Z}[x,y] \\ &= 5 + (y^2 - y^3)x + (3 - 2y^3)x^2 \ \in \mathbb{Z}[y][x] \\ &= 5 + 3x^2 + xy^2 + (-x - 2x^2)y^3 \in \mathbb{Z}[x][y] \end{aligned}$$

Sin mayor dificultad todo lo anterior puede hacerse para un número n cualquiera de variables considerando el conjunto $A^{\mathbb{N}^n}$.

2.1.7. Ideales

Definición 2.1.8. Se considera un anillo A y un subconjunto $I \subseteq A$ tal que $(I,+,0) \leqslant (A,+,0)$. Decimos que:

- I es un *ideal a izquierda* de A si $ax \in I, \forall a \in A, x \in I$. En este caso notamos $I \lhd_l A$,
- I es un *ideal a derecha* de A si $xa \in I, \forall a \in A, x \in I$. En este caso notamos $I \lhd_r A$,
- I es un *ideal bilátero* (o simplemente un *ideal*) de A si I es a la vez ideal izquierdo y derecho de A. En este caso notamos $I \lhd A$.

Observación 2.1.8.

- Se tiene que $\{0\} \lhd A$ y $A \lhd A$: son los llamados *ideales triviales* de A. Los demás ideales se dicen *ideales propios* de A.
- Si $I \lhd A$ y $1 \in I$, entonces $I = A$. En particular, I no es un subanillo a menos que $I = A$.
- Un anillo con división no tiene ideales biláteros propios. En efecto, si $I \neq 0$ es un ideal de un anillo con división A, tomemos $x \in I, x \neq 0$. Existe $y \in A$ tal que $yx = 1 \in I$, por lo que $I = A$.
- Todas las afirmaciones anteriores valen tomando $\lhd_l$ y $\lhd_r$ en lugar de $\lhd$.

Ejemplos 2.1.5.

- **Ideales de $\mathbb{Z}$**
  Son los conjuntos nZ de los múltiplos de n, con $n \in \mathbb{N}$ cualquiera.
  En efecto, se puede ver fácilmente que para cada $n \in \mathbb{N}$, nZ es un ideal de $\mathbb{Z}$.
  Por otra parte, si I es un subgrupo de $\mathbb{Z}$, consideremos el menor natural no nulo n que pertenece a I. Sea $x \in I$ cualquiera. Vamos a probar que x es múltiplo de n. Usando la división entera se tiene $x = qn + r$, con $0 \leqslant r < n$. Como $r = x - qn \in I$ (observar que de $n \in I$ se deduce $qn \in I$ y como además $x \in I$, se tiene $x - qn \in I$), y $r < n$, se deduce $r = 0$ y por lo tanto x es múltiplo de n.
- **Ideales y morfismos**
  Si $\varphi : A \to B$ es un morfismo de anillos, entonces $\mathrm{Ker}(\varphi) \lhd A$.

Proposición 2.1.5. *Sea $f : A \to B$ morfismo de anillos. Si $H \lhd B$, entonces $f^{-1}(H) \lhd A$. Si además f es un epimorfismo y $K \lhd A$, entonces $f(K) \lhd B$.*

Demostración. Sea $H \lhd B$. Sabemos que $f^{-1}(H) \leqslant A$. Además, si $x \in f^{-1}(H)$ y $a \in A$ se tiene $f(ax) = f(a)f(x) \in H$ y $f(xa) = f(x)f(a) \in H$ porque $f(x) \in H$. Se deduce que $ax, xa \in f^{-1}(H)$.

Por otra parte, si $K \lhd A$, sabemos que $f(K) \leqslant B$. Además, si $x \in K$ y $b \in B$, como f es un epimorfismo, se tiene que $b = f(a)$ para algún $a \in A$, de donde $bf(x) = f(a)f(x) = f(ax) \in f(K)$ y $f(x)b = f(x)f(a) = f(xa) \in f(K)$ porque $ax, xa \in K$. □

Observar que la inclusión de $\mathbb{Z}$ en $\mathbb{R}$ es un morfismo de anillos que muestra que la condición de ser epimorfismo en la proposición anterior es necesaria.

- **Ideales en matrices**
  Para cualquier anillo A,
  $$\left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in A\right\} \lhd_l M_2(A), \qquad \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in A\right\} \lhd_r M_2(A).$$

  En $M_2(\mathbb{Z})$, las matrices con todas sus entradas pares forman un ideal bilátero.

  En $M_2(\mathbb{R})$, los únicos ideales biláteros son los triviales. En particular, cualquier morfismo de anillos $\varphi : M_2(\mathbb{R}) \to A$ es inyectivo o nulo.

Proposición 2.1.6. *Sea $\{J_i\}_{i\in I}$ una familia no vacía de ideales de A. Entonces $\bigcap\limits_{i\in I} J_i$ es un ideal de A.*

Definición 2.1.9 (Ideal generado)**.** Si $S \subset A$ es un subconjunto de un anillo, el *ideal bilátero generado por S* es:
$$[S] := \bigcap\{I \mid I \lhd A, I \supset S\}$$
Si $S = \{a_1, a_2, \dots, a_n\}$, notamos $[S] = (a_1, a_2, \cdots, a_n)$. Los ideales generados por un conjunto finito se dicen *finitamente generados.*

Un ideal (x) generado por un conjunto unitario se dice *ideal principal.*

Remplazando $\lhd$ por $\lhd_l$, $\lhd_r$ se define el *ideal a izquierda* o *ideal a derecha* generado por S, que se nota $[S]_l$ y $[S]_r$ respectivamente.

Observación 2.1.9. El ideal bilátero (a izquierda, a derecha) generado por S es el menor (con respecto a $\subset$) entre los ideales biláteros (a izquierda, a derecha) de A que contienen a S. Además se tiene:
$$[S] = \left\{\sum_{i\in F} a_i s_i b_i \mid F \text{ finito}, a_i, b_i \in A, s_i \in S\ \forall i \in F\right\}$$
$$[S]_l = \left\{\sum_{i\in F} a_i s_i \mid F \text{ finito}, a_i \in A, s_i \in S\ \forall i \in F\right\}$$
$$[S]_r = \left\{\sum_{i\in F} s_i b_i \mid F \text{ finito}, b_i \in A, s_i \in S\ \forall i \in F\right\}$$
Es claro que en el caso conmutativo los tres conjuntos coinciden.

La siguiente proposición recoge observaciones ya hechas y las completa.

Proposición 2.1.7. *1. Sea $I \lhd A$. Entonces $I = A$ si y sólo si $1 \in I$, si y sólo si existe $x \in U(A)$ tal que $x \in I$.*

2. Sea A un anillo. Entonces A es un anillo con división si y sólo si A no contiene ideales propios izquierdos ni derechos.

3. Sea A un anillo conmutativo. Entonces A es un cuerpo si y sólo si A no tiene ideales biláteros propios.

Demostración. 1. Es claro.

2. Para el directo, ver la observación 2.1.8. Para el recíproco, tomemos $x \in A$, $x \neq 0$ y consideremos el ideal izquierdo I generado por x. Como A no tiene ideales propios y además $I \neq 0$, se tiene $I = A$ por lo que $1 \in I$, de donde se deduce que existe $y \in A$ tal que $1 = yx$, por lo que x es invertible a izquierda. Análogamente se prueba que x es invertible a derecha, por lo que x es invertible en A.

3. Es la parte anterior aplicada al caso conmutativo. □

Definición 2.1.10. Sea A un anillo. Un ideal M bilátero (a izquierda, a derecha) se dice *maximal* si $M \neq A$ y para cualquier otro ideal J bilátero (a izquierda, a derecha) que contiene a M se tiene $J = M$ o $J = A$.

Recordemos el

Lema de Zorn. *Sea $(E, \leqslant)$ un conjunto no vacío parcialmente ordenado (i.e. $\leqslant$ es una relación binaria reflexiva, antisimétrica y transitiva) tal que toda cadena T en E (i.e. $T \subset E$ es totalmente ordenado) tiene cota superior en E. Entonces E admite un elemento maximal.*

Teorema 2.1.8. *Sea I un ideal bilátero (a izquierda, a derecha) de A, $I \neq A$. Existe un ideal bilátero (a izquierda, a derecha) maximal M tal que $I \subseteq M$.*

Demostración. Haremos la prueba para ideales biláteros, pero es fácilmente adaptable a los casos de ideales a izquierda y a derecha.

Consideremos la familia $\mathcal{F} = \{J \lhd A \mid I \subseteq J \subsetneq A\}$. Como $I \in \mathcal{F}$, se tiene que $\mathcal{F} \neq \varnothing$. Ordenemos $\mathcal{F}$ por inclusión; sea $T = \{I_\lambda \mid \lambda \in \Lambda\} \subseteq \mathcal{F}$ una cadena. Está acotada superiormente por $D := \bigcup_{\lambda \in \Lambda} I_\lambda$. Veamos que $D \in \mathcal{F}$:

- $D \lhd A$: sean $a \in D, b \in D$. Entonces $a \in I_\alpha$, $b \in I_\beta$ para ciertos $\alpha, \beta \in \Lambda$. Como T es una cadena, podemos suponer $I_\alpha \subset I_\beta$, de donde $a, b \in I_\beta$. Esto implica que $a - b \in I_\beta \subset D$. Además $0 \in I_\beta \subset D$, y si $a \in A$, $x \in D$ entonces $x \in I_\gamma$ para algún $\gamma \in \Lambda$, de donde $xa, ax \in I_\gamma \subset D$.
- Como $I \subset I_\lambda$ para todo $\lambda \in \Lambda$, entonces $I \subset D$.
- $D \subsetneqq A$: si $D = A$, entonces $1 \in D$, de donde $1 \in I_\lambda$ para algún $\lambda \in \Lambda$, lo cual es absurdo pues $I_\lambda \subsetneqq A$.

Aplicando el lema de Zorn a la familia $\mathcal{F}$, se tiene que existe un elemento maximal en $\mathcal{F}$ (ordenado por la inclusión), llamémosle $M \in \mathcal{F}$. Se deduce que M es un ideal maximal en A, y por construcción $I \subseteq M$. □

Aplicando el teorema anterior al ideal $I = \{0\}$, se obtiene el siguiente corolario.

Corolario 2.1.9. *Si $A \neq \{0\}$ es un anillo, existen ideales biláteros (a izquierda, a derecha) maximales en A.*

Observación 2.1.10. Se puede demostrar que el teorema anterior (a veces llamado *teorema de Krull*), que usa el axioma de elección bajo la forma del lema de Zorn, es equivalente al axioma de elección. Observar además que usamos fuertemente que nuestro anillo tiene unidad: este teorema es falso para anillos sin unidad.

Proposición-Definición 2.1.1. Sean I, J ideales biláteros (a izquierda, a derecha) de A. Entonces los siguientes son ideales biláteros (a izquierda, a derecha) de A:

- $I + J = \{x + y \mid x \in I, y \in J\}$: es el *ideal suma* de I y J,
- $IJ = [\{xy \mid x \in I, y \in J\}] = \left\{ \sum_{k=1}^{n} x_k y_k \mid n \in \mathbb{N}, x_k \in I, y_k \in J, \forall k \in \{1, 2, \cdots, n\} \right\}$: es el *ideal producto* de I y J,

Demostración. A cargo del lector. □

2.1.8. Anillo cociente

Sean A un anillo e $I \lhd A$. Como I es un subgrupo de $(A, +, 0)$, tiene sentido considerar la relación de congruencia módulo I. El siguiente resultado asegura que esta relación es compatible con la estructura multiplicativa de A.

Lema 2.1.10. *Sean A un anillo e $I \lhd A$. Si $a \equiv a' \pmod{I}$ y $b \equiv b' \pmod{I}$, entonces $ab \equiv a'b' \pmod{I}$.*

Demostración. Pongamos $a' = a + i, b' = b + j$ con $i, j \in I$. Se tiene entonces

$$a'b' = (a + i)(b + j) = ab + ib + aj + ij.$$

Como $I \lhd A$, $a'b' - ab = ib + aj + ij \in I$, es decir, $ab \equiv a'b' \pmod{I}$. □

A partir de esto, es inmediato el siguiente resultado.

Teorema 2.1.11. *Si A es un anillo e $I \lhd A$, entonces el conjunto $A/_{\equiv}$ con las operaciones*

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b} \qquad \forall a, b \in A$$

y los neutros $\overline{0}$ y $\overline{1}$ forman un anillo que llamamos anillo cociente de A sobre I *y que notamos $\frac{A}{I}$. Además la proyección canónica $\pi_I : A \to \frac{A}{I}$ es un epimorfismo de anillos.*

Teorema 2.1.12 (Propiedad Universal del Cociente)**.** *Sea $f : A \to B$ un morfismo de anillos y sea $I \lhd A$. Si $I \leqslant \operatorname{Ker} f$, existe un único morfismo $\hat{f} : \frac{A}{I} \to B$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_I"'] & B \\ \frac{A}{I} \arrow[ur, dotted, "\hat{f}"'] & \end{tikzcd}$$

Además, se tiene $\operatorname{Im} \hat{f} = \operatorname{Im} f$ *y* $\operatorname{Ker} \hat{f} = \frac{\operatorname{Ker} f}{I}$.

Demostración. Sabemos que existe un único morfismo de grupos que hace conmutar el diagrama y verifica las condiciones en el núcleo y la imagen. Es inmediato verificar que dicho morfismo preserva el producto y la unidad del anillo. □

Corolario 2.1.13 (Teoremas de isomorfismo)**.** *Sea A un anillo.*

1. *Si $f : A \to B$ es un morfismo de anillos, entonces $\frac{A}{\operatorname{Ker} f} \cong \operatorname{Im} f$,*

2. *Si $f : A \to B$ es un morfismo de anillos, y $H \lhd A, K \lhd B$ con $f(H) \subseteq K$, entonces existe un único morfismo de anillos $\tilde{f} : \frac{A}{H} \to \frac{B}{K}$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_H"'] & B \arrow[d, "\pi_K"] \\ \frac{A}{H} \arrow[r, dotted, "\tilde{f}"'] & \frac{B}{K} \end{tikzcd}$$

Demostración. 1. Se deduce del teorema anterior, de manera análoga que para grupos.

2. Sabemos que existe un único morfismo de grupos. Basta verificar que preserva el producto y la unidad. □

Teorema 2.1.14. *Sean A un anillo e $I \lhd A$. Existe una correspondencia biyectiva entre los conjuntos:*

$$\mathcal{F}_1 = \left\{ L \lhd \frac{A}{I} \right\} \qquad y \qquad \mathcal{F}_2 = \{K \lhd A \mid K \supseteq I\}$$

que preserva la inclusión.

Demostración. La prueba del resultado análogo para grupos puede adaptarse fácilmente a este contexto, usando la proposición 2.1.5. □

Es inmediato el siguiente corolario.

Corolario 2.1.15. *Sea M un ideal bilátero de un anillo A. Son equivalentes:*

- *M es maximal,*
- *El anillo $\frac{A}{M}$ es no nulo y no tiene ideales biláteros propios (es un anillo* simple*).*

Este último resultado relaciona propiedades del ideal con propiedades del cociente. Vamos a dar otros resultados en este sentido, en el caso de anillos conmutativos, en la siguiente sección.

Ejemplo 2.1.3. Sea $A = \mathbb{R}[x], a \in \mathbb{C}$. El *morfismo de evaluación en a* es $\varepsilon_a : \mathbb{R}[x] \to \mathbb{C}$, $\varepsilon_a(f) = f(a)$.

Supongamos $a \in \mathbb{R}$. Entonces se tiene que $\operatorname{Im} \varepsilon_a = \mathbb{R}$ y que

$$\operatorname{Ker} \varepsilon_a = \{f \in \mathbb{R}[x] : f(a) = 0\} \ni X - a.$$

Por otro lado $f(a) = 0 \Leftrightarrow f = (x-a)q$ para algún $q \in \mathbb{R}[x]$. En conclusión $\operatorname{Ker} \varepsilon_a = (x-a)$. Por el primer teorema de isomorfismo concluimos que $\frac{\mathbb{R}[x]}{(x-a)} \cong \mathbb{R}$ que es un cuerpo.

Tomemos ahora $a = i$, la unidad imaginaria. Entonces ε_i es un epimorfismo: dado $a + ib \in \mathbb{C}$ basta tomar $f = a + bX$. Se tiene que

$$\operatorname{Ker} \varepsilon_i = \{f \in \mathbb{R}[x] : f(i) = 0\} \ni X^2 + 1.$$

y que Im $\varepsilon_i = \mathbb{C}$. Por otro lado $f(i) = 0 \Rightarrow f(-i) = 0 \Rightarrow f$ es divisible por $(x + i)(x - i) = x^2 + 1$. En conclusión $\operatorname{Ker} \varepsilon_i = (X^2 + 1)$. Por el primer teorema de isomorfismo concluimos que $\mathbb{C} \cong \frac{\mathbb{R}[x]}{(X^2+1)}$. Esta es una construcción algebraica de los números complejos.

2.1.9. Ideales maximales e ideales primos

Definición 2.1.11. Sea A un anillo conmutativo. Un ideal P de A se dice *primo* si $P \neq A$ y

$$\forall a, b \in A : ab \in P \Rightarrow a \in P \text{ o } b \in P.$$

Ejemplos 2.1.6 (Ideales primos). 1. $p\mathbb{Z} \lhd \mathbb{Z}$ es primo.

2. si $D \neq \{0\}$ es un dominio, el ideal $\{0\}$ es primo,

3. si D es un dominio, entonces $(x, y) = \{p \in D[x, y] \mid p(0) = 0\} \lhd D[x, y]$ es un ideal primo.

Proposición 2.1.16. *Sean A un anillo conmutativo e $I \lhd A$. Entonces:*

1. I es maximal si y sólo si $\frac{A}{I}$ es cuerpo,

2. I es primo si y sólo si $\frac{A}{I}$ es dominio.

Demostración. 1. Esta parte puede deducirse fácilmente combinando los dos resultados que siguen en el caso de anillos conmutativos:

- I es maximal si y sólo si $\frac{A}{I}$ no tiene ideales biláteros (corolario 2.1.15),
- B es un anillo con división si y sólo si no tiene ideales a izquierda ni a derecha (proposición 2.1.7).

Sin embargo, presentamos una prueba autocontenida para ejercitar la manipulación con ideales maximales y con anillos cociente:
($\Rightarrow$) Sea $\overline{a} \in \frac{A}{I}$ tal que $\overline{a} \neq 0$. Veamos que es invertible.

Como $a \notin I$, se tiene que $I \subsetneq I + (a) = \{x + ay : x \in I, y \in A\}$. Como I es maximal, esto implica que $I + (a) = A$. En particular $A \ni 1 = x + ay$ para ciertos $x \in I, y \in A$. Por lo tanto $ay - 1 \in I$, es decir, $\overline{ay} = \overline{1} = \overline{ya}$.

($\Leftarrow$) Si $\frac{A}{I}$ es un cuerpo, entonces sus únicos ideales son $\{0\}$ y $\frac{A}{I}$. El teorema de correspondencia 3.1.6 nos indica que estos están en biyección con los ideales de A que contienen a I, entre los cuales necesariamente están I y A, por lo tanto no puede haber más. Esto nos dice exactamente que I es maximal.

2. ($\Rightarrow$) Sean $\overline{a}, \overline{b} \in \frac{A}{I}$ tales que $\overline{a}\overline{b} = \overline{ab} = \overline{0}$. Entonces $ab \in I$. Como I es primo esto implica que $a \in I$ o $b \in I$, es decir, $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$, probando que $\frac{A}{I}$ es un dominio.

($\Leftarrow$) Sea $ab \in I$. Entonces $\overline{0} = \overline{ab} = \overline{a}\overline{b}$. Como $\frac{A}{I}$ es dominio, esto implica que $\overline{a} = \overline{0}$ o $\overline{b} = \overline{0}$, es decir $a \in I$ o $b \in I$, de donde I es un ideal primo. $\square$

Se deduce el siguiente corolario.

Corolario 2.1.17. *Sea A un anillo conmutativo.*

1. *Todo ideal maximal en A es primo.*

2. *Si $\varphi : A \to B$ un morfismo de anillos, entonces* $\operatorname{Ker}\varphi$ *es maximal si y sólo si* $\operatorname{Im}\varphi$ *es un cuerpo, y* $\operatorname{Ker}\varphi$ *es primo si y sólo si* $\operatorname{Im}\varphi$ *es un dominio.*

Observación 2.1.11. A partir de los resultados anteriores y del ejemplo 2.1.6, se tiene:

- Sea $m \in \mathbb{Z}$. Son equivalentes:

  (i) $\mathbb{Z}_m$ es un cuerpo,

  (ii) $\mathbb{Z}_m$ es un dominio,

  (iii) m es un número primo.

  En efecto, tenemos (iii) implica (i) y (iii) implica (ii). Para los recíprocos, supongamos que m no es primo. Se tiene entonces $m = ab, a, b \notin \{1, -1\}$. Entonces $(m) \subsetneq (a)$ por lo que no vale (ii) y además $a, b \notin m\mathbb{Z}$ mientras que $ab \in n\mathbb{Z}$, por lo que no vale (i).

- Si consideramos el morfismo $\varphi_n : \mathbb{Z}[x] \to \mathbb{Z}$ tal que $(\varphi_n)_{|\mathbb{Z}} = \operatorname{id}_{\mathbb{Z}}$ y $\varphi_n(x) = n$, como $\operatorname{Im}\varphi_n = \mathbb{Z}$ es un dominio que no es un cuerpo, se deduce que $\operatorname{Ker}\varphi_n \lhd \mathbb{Z}[x]$ es un ideal primo que no es maximal. En particular $\operatorname{Ker}\varphi_0 = (x) = \{p \in \mathbb{Z}[x] \mid p(0) = 0\}$ es un ideal primo no maximal. En efecto, $(x) \subsetneq \{p \in \mathbb{Z}[x] \mid p(0) \in 2\mathbb{Z}\}$.

- Sea $\Bbbk$ un cuerpo. Para cada $\alpha \in \Bbbk$, el ideal $I_\alpha = (x - \alpha)$ es maximal en $\Bbbk[x]$. (Veremos más adelante que hay ideales maximales que no son de la forma I_α).

- Sea $\Bbbk$ un cuerpo. El único ideal maximal de $\Bbbk[[x]]$ es (x). En efecto, supongamos que M es maximal. Observemos primero que si $f \in \Bbbk[[x]]$ es tal que $f(0) \neq 0$, entonces f es invertible. Es claro entonces que $\forall f \in M$ se tiene $f(0) = 0$, entonces todo $f \in M$ es de la forma $f = gx$ y por tanto $M \subseteq (x) \subsetneq \Bbbk[[x]]$ es decir $M = (x)$.

Observación 2.1.12. Sea A un anillo. Llamémosle χ al único morfismo de anillos $\mathbb{Z} \to A$, es decir $\chi(n) = n \cdot 1_A = \overbrace{1_A + \cdots + 1_A}^{n veces}$. El núcleo de χ es $\operatorname{Ker}\chi = \{n \in \mathbb{Z} : n \cdot 1_A = 0\} = m\mathbb{Z}$ para algún $m \in \mathbb{N}$.[2] Definimos la *característica* de A como m. Notamos $\operatorname{car} A = m$. A modo de ejemplo, el único anillo de característica 1 es el anillo trivial $\{0\}$.

El primer teorema de isomorfismo afirma que $\frac{\mathbb{Z}}{m\mathbb{Z}} \simeq \operatorname{Im}\chi \subset A$. Observar que si $\varphi : R \to S$ es un morfismo de anillos y R es un anillo conmutativo, entonces $\operatorname{Im}\varphi$ es un subanillo conmutativo de B. En este caso tenemos que $\operatorname{Im}\chi \subset A$ es un subanillo conmutativo.

Si además A no tiene divisores de cero ni a izquierda ni a derecha (por ejemplo, si A es un dominio o un anillo con división), entonces $\operatorname{Im}\chi$ tampoco tendrá. En este caso $\frac{\mathbb{Z}}{m\mathbb{Z}}$ es un dominio, de donde $m\mathbb{Z}$ es un ideal primo. En conclusión, $m = 0$ o $m = p$ es un número primo.

En particular, un cuerpo tiene característica cero o característica prima.

2.1.10. Anillos de fracciones y localización

Los números racionales pueden construirse de manera algebraica a partir de los enteros de la siguiente manera: se considera el conjunto $\mathbb{Z} \times \mathbb{Z}\backslash\{0\} = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$ y se define la relación:

$$(a, b) \sim (c, d) \text{ si y sólo si } ad = bc.$$

[2]De manera equivalente se define la característica del anillo como el menor n positivo tal que $n \cdot 1_A = 0$ si existe, o como 0 si no existe.

A partir de la conmutatividad y la ausencia de divisores de cero en $\mathbb{Z}$, se prueba que esta relación es de equivalencia y se nota $\frac{a}{b}$ a la clase del elemento (a, b) y $\mathbb{Q}$ al conjunto cociente. La idea es que $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$ permite definir un racional como un par de enteros, con el segundo no nulo.

La aplicación que asocia a cada entero n el par $(n, 1) \in \mathbb{Q}$ es una función inyectiva. Se quiere dar a $\mathbb{Q}$ una estructura de anillo que sea coherente con la estructura de anillo de $\mathbb{Z}$ (esto es, una estructura tal que la inyección antes mencionada sea un morfismo de anillos). Para esto se define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \bullet \frac{c}{d} = \frac{ac}{bd}$$

y se prueba que $(\mathbb{Q}, +, \frac{0}{1}, \bullet, \frac{1}{1})$ es un cuerpo.

Esta construcción puede generalizarse en dos etapas:

1. se puede considerar en lugar de $\mathbb{Z}$ un dominio cualquiera A y dar una estructura de cuerpo a un cociente del conjunto $A \times A \backslash \{0\}$: este cuerpo se llama *cuerpo de fracciones* de A,

2. en la construcción del cuerpo de fracciones se toman todos los elementos no nulos de A y se transforman en invertibles: una construcción más general permite transformar en invertibles los elementos de un *subconjunto multiplicativo* S de un anillo conmutativo A, mediante un proceso cuyo resultado no es necesariamente un cuerpo sino un anillo conmutativo llamado *anillo de fracciones de A respecto de S*.

La construcción del cuerpo de fracciones a partir de un dominio A es análoga a la de $\mathbb{Q}$ a partir de $\mathbb{Z}$. Vamos a concentrarnos en la segunda etapa y luego ver al cuerpo de fracciones como un caso particular de anillo de fracciones.

Definición 2.1.12. Sea A un anillo conmutativo. Un conjunto $S \subseteq A$ se dice *multiplicativo* o *multiplicativamente cerrado* si $1 \in S$ y $st \in S \;\; \forall s, t \in S$.

Ejemplos 2.1.7 (Conjuntos multiplicativos)**.**

1. $\{1\}$, A son conjuntos multiplicativos en A,

2. para cada $a \in A$, el conjunto $\{a^n \mid n \in \mathbb{N}\}$ es multiplicativo en A,

3. si P es un ideal primo de A, el conjunto $S = A \backslash P$ es multiplicativo,

4. en particular, si A es un dominio, $A \backslash \{0\}$ es multiplicativo.

Definimos en $A \times S$ la siguiente relación:

$$(a, s) \sim_S (b, r) \text{ si y sólo si existe } t \in S \text{ tal que } t(ar - bs) = 0.$$

Notamos $\frac{a}{s}$ a la clase de equivalencia del par (a, s).

Observación 2.1.13.

1. Sean A un anillo conmutativo y S un conjunto multiplicativo en A. La relación $\sim_S$ definida en $A \times S$ es de equivalencia. En efecto, es reflexiva porque $(a, s) \sim_S (a, s)$ se verifica tomando $t = 1 \in S$ y usando la conmutatividad de A. La relación es simétrica porque A es conmutativo. Para la transitividad, supongamos $(a, s) \sim_S (b, r)$ y $(b, r) \sim_S (c, v)$. Existen $t, t' \in S$ tales que $t(ar - bs) = 0$ y $t'(bv - cr) = 0$. Se tiene que $tt'rav = tt'bsv = tt'crs$ de donde $tt'r(av - cs) = 0$. Como $t, t', r \in S$ se tiene que $tt'r \in S$, de donde $(a, s) \sim_S (c, v)$.

2. Se tiene que $\frac{a}{s} = \frac{at}{st} \;\; \forall a \in A, s, t \in S$.

3. Si A es un dominio y $0 \notin S$, la relación puede expresarse como $(a,s) \sim_S (b,t)$ si y sólo si $at = bs$.

Proposición-Definición 2.1.2. Sean A un anillo conmutativo y S un conjunto multiplicativo en A. El conjunto cociente $\frac{A\times S}{\sim_S}$ admite una estructura de anillo conmutativo que llamamos *anillo de fracciones* (o *de localización*) de A respecto de S y notamos $S^{-1}A$, cuyas operaciones se definen como sigue:

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}, \qquad \frac{a}{s} \bullet \frac{b}{t} = \frac{ab}{st}, \qquad \forall a,b \in A, s,t \in S.$$

Demostración. Verifiquemos primero que las operaciones están bien definidas. Para $+$, es claro por la conmutatividad de la suma y el producto en A que alcanza con probar que si $\frac{a}{s} = \frac{a'}{s'}$ entonces $\frac{at+bs}{st} = \frac{a't+bs'}{s't}$ para todo $b \in A, t \in S$. Ahora bien, si existe $x \in S$ tal que $xas' = xa's$, entonces

$$x(at+bs)(s't) = xas't^2 + xbs'st = xa'st^2 + xbs'st = xst(a't+bs')$$

y se deduce la igualdad.

Análogamente, para $\bullet$ alcanza con observar que si $\frac{a}{s} = \frac{a'}{s'}$ entonces $\frac{a'b}{s't} = \frac{ab}{st}$ para todo $b \in A, t \in S$. La implicancia es inmediata puesto que $xas' = xa's$ implica $xas'bt = xa'sbt$.

Veamos ahora que $+$ define una estructura de grupo abeliano. La conmutatividad es clara. La asociatividad se deduce de:

$$\frac{(at+bs)r+cst}{str} = \frac{atr+(br+ct)s}{str} \quad \forall a,b,c \in A, s,t,r \in S.$$

Se tiene además $\frac{a}{s} + \frac{0}{1} = \frac{a\cdot 1 + s\cdot 0}{s\cdot 1} = \frac{a}{s}$ y $\frac{-a}{s} + \frac{a}{s} = \frac{0}{s^2} = \frac{0}{1}$, $\forall a \in A, s \in S$.

La operación $\bullet$ es claramente asociativa y conmutativa y $\frac{1}{1}$ es su neutro.

Finalmente, para verificar que el producto es distributivo respecto de la suma, es decir que se cumple

$$\frac{a}{s} \bullet \left(\frac{b}{t} + \frac{c}{r}\right) = \frac{ab}{st} + \frac{ac}{sr} \quad \forall a,b,c \in A, s,t,r \in S.$$

observemos que el término de la izquierda de la igualdad es $\frac{a}{s} \bullet \frac{br+ct}{tr} = \frac{a(br+ct)}{str}$ y el de la derecha es $\frac{absr+acst}{s^2tr} = \frac{abr+act}{str}$. ☐

Observación 2.1.14. Si $0 \in S$, entonces $\frac{a}{s} = \frac{0}{1}$ $\forall a \in A, s \in S$, y por tanto $S^{-1}A = \{0\}$.

Veamos ahora como se relacionan el anillo original A con el anillo de fracciones $S^{-1}A$.

Proposición 2.1.18. *Sean A un anillo conmutativo y S un conjunto multiplicativo en A. La función*

$$\begin{aligned} \eta_S : A &\to S^{-1}A \\ a &\mapsto \frac{a}{1} \end{aligned}$$

es un morfismo de anillos.

Demostración. A cargo del lector. ☐

Proposición 2.1.19 (Propiedad universal del anillo de fracciones)**.** *Sean A un anillo conmutativo y $S \subset A$ un conjunto multiplicativo. Si $\varphi : A \to B$ es un morfismo de anillos, donde*

B es un anillo conmutativo tal que $\varphi(S) \subset B^{\times}$, entonces existe un único morfismo de anillos $\hat{\varphi} : S^{-1}A \to B$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\eta"'] & B \\ S^{-1}A \arrow[ur, dotted, "\hat{\varphi}"'] & \end{tikzcd}$$

Demostración. A cargo del lector (haremos la demostración de un caso particular en la proposición 2.1.21). ☐

Observación 2.1.15. Supongamos que $0 \notin S$.

- El morfismo η_S es inyectivo si y sólo si S no tiene divisores de cero. En efecto, sea $a \in A$ tal que $\eta_S(a) = 0$. Entonces $\frac{a}{1} = \frac{0}{1}$ lo que implica que existe $s \in S$ tal que $as = 0$. Como $s \neq 0$ y S no tiene divisores de cero, se deduce $a = 0$. Recíprocamente, si $s \in S$ es un divisor de cero, existe $a \in A$ tal que $as = 0$ y $a \neq 0$. Se deduce $\eta_S(a) = 0$ y por lo tanto que η_S no es inyectiva.
- En particular, si A es un dominio, entonces η_S es inyectiva si y sólo si $0 \notin S$.

Proposición 2.1.20. *η_S es un isomorfismo si y sólo si todos los elementos de S son invertibles en A.*

Demostración. Es claro que si todos sus elementos son invertibles, S no tiene divisores de cero y por lo tanto se tiene que η_S es inyectiva. Además, $\forall a \in A, s \in S : \frac{a}{s} = \frac{s^{-1}a}{1} = \eta_S(s^{-1}a)$, por lo que se tiene también la sobreyectividad. Recíprocamente, si η_S es sobreyectiva, $\forall s \in S$, existe $a \in A$ tal que $\frac{1}{s} = \frac{a}{1}$, por lo que existe $t \in S$ tal que $t = ast$. Se deduce $\frac{1}{1} = \frac{as}{1}$ de donde $1 = as$ y por lo tanto s es invertible. ☐

Proposición-Definición 2.1.3. Sean A un dominio y $S = A \backslash \{0\}$. El anillo de fracciones $S^{-1}A$ es un cuerpo que llamamos *cuerpo de fracciones de A* y notamos $\mathrm{Frac}(A)$. Notaremos η al monomorfismo canónico $A \to \mathrm{Frac}(A)$.

Demostración. Si $\frac{a}{s} \neq 0$, entonces no existe $t \in S$ tal que $ta = 0$. En particular $a = 1 \cdot a \neq 0$, por lo que $a \in S$ y $\frac{s}{a}$ es el inverso de $\frac{a}{s}$. ☐

Proposición 2.1.21 (Propiedad universal del cuerpo de fracciones)**.** *Sea D un dominio. Para cada cuerpo $\Bbbk$ y cada monomorfismo de anillos $\varphi : D \to \Bbbk$ existe un único morfismo de anillos $\hat{\varphi} : \mathrm{Frac}(D) \to \Bbbk$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} D \arrow[r, "\varphi"] \arrow[d, "\eta"'] & \Bbbk \\ \mathrm{Frac}(D) \arrow[ur, dotted, "\hat{\varphi}"'] & \end{tikzcd}$$

Demostración. Para la existencia, alcanza con definir

$$\hat{\varphi}\left(\frac{a}{b}\right) := \varphi(a)\varphi(b)^{-1}, \forall a, b \in A, b \neq 0 \quad (*)$$

(notar que si $b \neq 0$ entonces $\varphi(b) \neq 0$ y por tanto es invertible en $\Bbbk$) y probar que es un morfismo de anillos que hace conmutar el diagrama.

Para la unicidad basta ver que la condición de conmutatividad del diagrama es $\hat{\varphi}(\frac{a}{1}) = \varphi(a)\ \forall a \in A$ y la condición de que $\hat{\varphi}$ es morfismo de anillos implica $\hat{\varphi}(\frac{1}{b}) = \varphi(b)^{-1}$ $\forall b \in A, b \neq 0$. Combinando ambas igualdades y usando que $\hat{\varphi}$ preserva el producto, se deduce que $\hat{\varphi}$ tiene que estar definida por la fórmula $(*)$. ☐

Ejemplos 2.1.8 (Cuerpos de fracciones)**.** Sea $\Bbbk$ un cuerpo.

1. $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ (ver observación 2.1.13.4),
2. $\mathrm{Frac}(\Bbbk) = \Bbbk$.
3. Se define el anillo de las *funciones racionales* con coeficientes en $\Bbbk$ en indeterminadas $x_1, \dots, x_n$ como
$$\Bbbk(x_1,\dots,x_n) := \mathrm{Frac}(\Bbbk[x_1,\dots,x_n]) = \left\{ \frac{f}{g} \mid f, g \in \Bbbk[x_1,\dots,x_n], g \neq 0 \right\},$$
4. Se define el anillo de las *series de Laurent formales* como
$$\Bbbk((x)) := \mathrm{Frac}\left(\Bbbk[[x]]\right) = \left\{ \frac{f}{g} \mid f, g \in \Bbbk[[x]], g \neq 0 \right\} = \left\{ \frac{h}{x^n} \mid h \in \Bbbk[[x]], n \in \mathbb{N} \right\}.$$
La última igualdad se prueba usando que todo $g \in \Bbbk[x]$ no nulo es de la forma $g = x^n g_1$ para cierto natural n y cierto $g_1 \in \Bbbk[[x]]$ invertible. Análogamente se define $\Bbbk((x_1,\dots,x_n))$ como el cuerpo de fracciones del anillo de series en las variables $x_1, x_2, \cdots, x_n$.

En el caso particular en que el conjunto multiplicativo S es el complemento de un ideal primo P, el proceso se llama de *localización respecto del ideal P*. La construcción del cuerpo de fracciones de un dominio es un caso particular de localización respecto de un ideal (considerando $P = \{0\}$).

Definición 2.1.13. Si A es un anillo conmutativo y P es un ideal primo en A, llamamos *localización de A respecto de P* y notamos $A_{(P)}$ al anillo de fracciones $S^{-1}A$, donde $S = A \backslash P$.

Definición 2.1.14. Un anillo conmutativo se dice *local* si tiene un único ideal maximal.

Ejemplos 2.1.9. Todo cuerpo es un anillo local.
Vamos a ver que la construcción del anillo de fracciones permite obtener anillos locales a partir de ideales primos.
El anillo de series formales en x con coeficientes en un cuerpo es local (su único ideal maximal es (x). Ver ejercicio del repartido 4 al respecto).

Proposición 2.1.22. *Sea A un anillo conmutativo no trivial. Son equivalentes:*

1. *A es local,*
2. *la suma de dos elementos no invertibles es no invertible,*
3. *$A \backslash A^\times$ es un ideal de A.*

Demostración. ($1 \Rightarrow 2$) Supongamos que A es local y que M es su ideal maximal. Si $x, y \notin A^\times$ entonces existe un ideal maximal que contiene a x y otro que contiene a y. Como hay un único ideal maximal, se tiene $x, y \in M$ y por tanto $x + y \in M$. Como $M \neq A$, se deduce que $x + y$ es no invertible.

($2 \Rightarrow 3$) Sabemos que $A \backslash A^\times$ es no vacío (porque A es no trivial) y cerrado por la suma. Por otra parte si x es no invertible, también lo es $-x$. Además, si x es no invertible, es claro que ax es no invertible para cualquier $a \in A$. Se deduce que $A \backslash A^\times \lhd A$.

($3 \Rightarrow 1$) Es claro que cualquier ideal propio de A está formado por elementos no invertibles, es decir que está contenido en $A \backslash A^\times$. Como consecuencia, si $A \backslash A^\times$ es un ideal, entonces es el único ideal maximal. □

Proposición 2.1.23. *Dado A un anillo conmutativo y P un ideal primo de A, el anillo $A_{(P)}$ es local y su único ideal maximal es $S^{-1}P := \{\frac{p}{s} \mid p \in P, s \notin P\}$.*

Demostración. Es claro que $S^{-1}P$ es un ideal de $A_{(P)}$. Además, su complemento consiste de los elementos de la forma $\frac{t}{s}$ con $t, s \in S$, y por tanto consiste de elementos invertibles. Se deduce por la proposición anterior que $S^{-1}P$ es el único ideal maximal de $A_{(P)}$. □

Ejemplo 2.1.4. Tomemos $p\mathbb{Z} \lhd \mathbb{Z}$, siendo $p \in \mathbb{Z}$ primo. La localización de $\mathbb{Z}$ respecto de $p\mathbb{Z}$ es el subanillo

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \mid b \text{ no es múltiplo de } p\right\} \subseteq \mathbb{Q}.$$

Su único ideal maximal es $\left\{\frac{a}{b} \mid a \text{ es múltiplo de } p, b \text{ no es múltiplo de } p\right\}$.

2.2. Divisibilidad en dominios

En este capítulo D siempre será un dominio, es decir un anillo conmutativo $D \neq \{0\}$ sin divisores de cero.

2.2.1. Generalidades

Definición 2.2.1. Sean $a, b \in D$. Decimos que *a divide a b*, que *a es divisor de b* o que *b es múltiplo de a* si existe $c \in D$ tal que $b = ac$. En este caso notamos $a \mid b$.

Ejemplos 2.2.1. Para todo $a \in D$, se tiene:

$$1 \mid a, \qquad a \mid a, \qquad a \mid 0, \qquad 0 \mid a \quad \text{si y sólo si } a = 0, \qquad a \mid 1 \quad \text{si y sólo si } a \in D^\times.$$

Observación 2.2.1.

- Las siguientes propiedades se verifican fácilmente:

  Si $a \mid b$ y $a \mid b'$ entonces $a \mid (b + b')$, $a \mid (b - b')$ y $a^2 \mid bb'$.

  Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

- La relación "divide a.$^{\text{es}}$ entonces lo que se conoce como un preorden en D^* (es reflexiva y transitiva, pero en general no antisimétrica: $1 \mid -1 \mid 1$). Como todo preorden induce una relación de equilalencia definida por $a \sim b$ si y sólo si $a \mid b$ y $b \mid a$.

Proposición 2.2.1. *Sea $\sim$ la relación en D definida en la observación anterior. Se tiene $a \sim b$ si y sólo si existe $u \in D^\times$ tal que $a = ub$.*

Demostración. Si existe $u \in D^\times$ tal que $a = ub$, se tiene también $b = u^{-1}a$ y por lo tanto $a \sim b$. Recíprocamente, supongamos que $a = xb$ y que $b = ya$. Entonces $a = xya$ y por tanto $a(1 - xy) = 0$. Como D es un dominio, tenemos dos posibilidades: $a = 0$ o $xy = 1$. Si $a = 0$, entonces $b = ya = 0$ y se deduce $a \sim b$. Si $xy = 1$, entonces $x \in D^\times$ y por tanto $a = xb \sim b$. □

Definición 2.2.2. Sean $a, b \in D$. Decimos que *a y b son asociados* si $a \sim b$.

Observación 2.2.2. La prueba de la proposición anterior permite afirmar además que si $b \in D$ es no nulo, entonces

$$xb \sim b \Rightarrow x \in D^\times.$$

La siguiente proposición traduce estas nociones de divisibilidad en términos de ideales principales.

Proposición 2.2.2. *Sean $a, b \in D$. Entonces:*

1. *$a \mid b$ si y sólo si $(b) \subseteq (a)$,*

2. $a \sim b$ *si y sólo si* $(a) = (b)$*,*

3. $a \mid b$ *y* $a \not\sim b$ *si y sólo si* $(b) \subsetneq (a)$*,*

4. $a \in D^\times$ *si y sólo si* $(a) = D$*.*

Demostración. A cargo del lector. □

Definición 2.2.3. Sea $a \in D$ no nulo y no invertible. Decimos que a es:

- *irreducible* si $\forall b, c \in D : a = bc$ implica $b \in D^\times$ o $c \in D^\times$,
- *primo* si $\forall b, c \in D : a \mid bc$ implica $a \mid b$ o $a \mid c$.

Observación 2.2.3. 1. Sea $a \in D$ no nulo y no invertible. Entonces a es irreducible si y sólo si $\forall b \in D : b \mid a$ implica $b \in D^\times$ o $b \sim a$.

2. Todo primo es irreducible.

3. Supongamos $p \sim q$. Si p es irreducible, también lo es q. Si p es primo también lo es q.

Ejemplos 2.2.2. 1. En $\mathbb{Z}$ y $\Bbbk[x]$ ($\Bbbk$ cuerpo) los primos y los irreducibles coinciden.

2. Sea $\Bbbk$ un cuerpo. Pongamos $D = \{a + x^2 p(x) \mid a \in \Bbbk, p(x) \in \Bbbk[x]\} \subseteq \Bbbk[x]$. El elemento $x^2 \in D$ es irreducible pero no es primo. En efecto $x^2 \mid x^3x^3 = x^2x^4$ pero $x^2 \nmid x^3$.

3. El polinomio $x^2 - 2$ es irreducible y primo como elemento de $\mathbb{Z}[x]$ pero no lo es como elemento de $\mathbb{R}[x]$.

4. El polinomio $2x - 2$ es irreducible y primo como elemento de $\mathbb{R}[x]$ pero no lo es como elemento de $\mathbb{Z}[x]$.

Proposición 2.2.3. *Sea* $a \in D$ *no nulo y no invertible. Entonces:*

1. a *es primo si y sólo si* (a) *es un ideal primo en* D*,*

2. a *es irreducible si y sólo si* (a) *es maximal (respecto de la inclusión) en la familia de ideales principales propios de* D*.*

Demostración. A cargo del lector. □

Definición 2.2.4. Si $a, b \in D$ no son simultáneamente nulos, decimos que $d \in D$ es un *máximo común divisor* de a y b si verifica

$$d \mid a, \quad d \mid b, \quad \text{y} \quad \forall c \in D \;\; c \mid a,\; c \mid b \Rightarrow c \mid d.$$

Observación 2.2.4. 1. En un dominio cualquiera no tiene por qué existir el máximo común divisor. En efecto, en el ejemplo 2.2.2.2, los elementos x^5 y x^6 tienen como conjunto de divisores comunes a $\{a \mid a \in \mathbb{R}\} \cup \{ax^2 \mid a \in \mathbb{R}\} \cup \{ax^3 \mid a \in \mathbb{R}\}$. Sin embargo ninguno de los elementos de este conjunto es múltiplo de todos los demás.

2. Si d y d' son máximos comunes divisores de a y b, entonces $d \sim d'$. Notamos $\operatorname{mcd}(a, b)$ a la clase de equivalencia definida por a y b.

Abuso de notación: En caso de existir máximos comunes divisores de a y b, notaremos $\operatorname{mcd}(a, b) = d$ en lugar de $d \in \operatorname{mcd}(a, b)$.

Proposición 2.2.4. 1. *Si* $a, b \in D$ *son tales que* $a \mid b$*, entonces* $\operatorname{mcd}(a, b) = a$*. En particular* $\operatorname{mcd}(a, 0) = a$ *y* $\operatorname{mcd}(a, b) = 1$ *siempre que* $a \in D^\times$*.*

2. *Si* $p \in D$ *es irreducible, entonces* $\operatorname{mcd}(a, p) = 1$ *o* $\operatorname{mcd}(a, p) = p$*.*

Demostración. 1. La afirmación y el primer caso particular son claros. Si a es invertible, entonces $b = aa^{-1}b$ y por tanto $a \mid b$. Se deduce que $\operatorname{mcd}(a, b) = a$ y como $a \sim 1$, entonces $\operatorname{mcd}(a, b) = 1$.

2. Como p es irreducible, sus divisores son 1, p o sus asociados, en particular $\operatorname{mcd}(a, p)$ es uno de estos. □

Definición 2.2.5. Sean $a_1, a_2, \ldots, a_n \in D$ no simultáneamente nulos. Decimos que $d \in D$ es un *máximo común divisor* de $a_1, a_2, \ldots, a_n$ y notamos $d = \operatorname{mcd}(a_1, \ldots, a_n)$ si

$$d \mid a_i \quad \forall i \in \{1, 2, \ldots, n\} \quad \text{y} \quad \forall c \in D \;\; c \mid a_i \; \forall i \Rightarrow c \mid d.$$

Observación 2.2.5. 1. Aquí también vale la unicidad a menos de asociados y haremos un abuso de notación análogo.

2. Sin pérdida de generalidad, se puede asumir que todos los a_i son no nulos puesto que si $a_i = 0$, es fácil ver que se tiene $\operatorname{mcd}(a_1, a_2, \ldots, a_n) = \operatorname{mcd}(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$.

3. Supongamos que $a_i \neq 0$ para todo $i \leqslant n$. Entonces si $d_1 := \operatorname{mcd}(a_1, a_2, \ldots, a_{n-1})$, se tiene $\operatorname{mcd}(a_1, a_2, \ldots, a_n) = \operatorname{mcd}(d_1, a_n)$.

4. De la observación anterior se deduce que si existe $\operatorname{mcd}(a, b)$ para cualesquiera $a, b \in D$, entonces existe $\operatorname{mcd}(a_1, a_2, \ldots, a_n)$ cualesquiera sean $a_1, a_2, \ldots, a_n \in D$, $n \geqslant 3$.

2.2.2. Dominios de factorización única

Definición 2.2.6. Un dominio D se dice *dominio factorial* o *dominio de factorización única* (abreviado *DFU*) si verifica:

- (Existencia de la descomposición factorial) Para cada $a \in D$ no nulo y no invertible, existen $p_1, p_2, \ldots, p_n$ irreducibles tales que $a = p_1 p_2 \cdots p_n$.
- (Unicidad de la descomposición factorial) Si $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, con p_i, q_j irreducibles para cada $i \in \{1, 2, \ldots, n\}, j \in \{1, 2, \ldots, m\}$, entonces $n = m$ y existe una función $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ tal que $p_i \sim q_{\sigma(i)}$.

Observación 2.2.6. 1. La unicidad de la factorización implica que puede asumirse σ inyectiva. En efecto, si $n = 1$ es claro. Supongamos que σ es inyectiva para n_0 y probémoslo para $n_0 + 1$. Tomemos

$$p_1 p_2 \cdots p_{n_0} p_{n_0+1} = q_1 q_2 \cdots q_m.$$

Existe $j \in \{1, 2, \ldots, m\}$ tal que $q_j \sim p_{n_0+1}$, por lo que se tiene $x p_{n_0+1} = q_j$ para cierto x invertible. Cancelando p_{n_0+1} en la igualdad de arriba, se deduce:

$$p_1 p_2 \cdots p_{n_0} = x^{-1} q_1 q_2 \cdots q_{j-1} q_{j+1} \cdots q_m.$$

Tomando $\sigma : \{1, 2, \ldots, n_0\} \to \{1, 2, \ldots, m\} \backslash \{j\}$ inyectiva y extendiéndola a $\overline{\sigma} : \{1, 2, \cdots, n_0 + 1\} \to \{1, 2, \ldots, m\}$ mediante $\overline{\sigma}(i) = \sigma(i), \forall i \leqslant n_0$, $\overline{\sigma}(n_0 + 1) = j$, obtenemos $\overline{\sigma}$ inyectiva.

2. En la prueba de la observación anterior no se usó la condición $n = m$ exigida para la unicidad de la descomposición factorial. De hecho, esta condición puede eliminarse de la definición. En efecto, por la observación anterior se deduce $n \leqslant m$, y luego intercambiando los roles de los p_i y los q_j se deduce $m \leqslant n$ y se obtiene $m = n$ (y por lo tanto σ es, de hecho, biyectiva).

3. La existencia de la factorización implica que todo elemento no nulo $a \in D$ es de la forma $a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, con $u \in D^\times$, $n \in \mathbb{Z}^+$, p_i irreducibles no asociados dos a dos y $\alpha_i \in \mathbb{N}$ para todo $i \in \{1, \ldots, n\}$.

   En efecto, si a es invertible, se toma n cualquiera y $\alpha_i = 0$ para todo $i \in \{1, \ldots, n\}$. Si a no es invertible, se tiene $a = q_1q_2\cdots q_m$, con q_i irreducible para todo $j \in \{1, \ldots, m\}$. Agrupando los q_i que sean asociados y usando que el producto de invertibles es invertible, se tiene el resultado.

La siguiente proposición muestra que $a \mid b$ si y sólo si "la factorización de a está contenida en la de b".

Proposición 2.2.5. *Sean D un DFU y $a, b \in D$ no nulos y no invertibles. Si $a = p_1p_2\cdots p_n$ y $b = q_1q_2\cdots q_m$, entonces son equivalentes:*

(i) $a \mid b$

(ii) *existe una función inyectiva $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ tal que $p_i \sim q_{\sigma(i)}$.*

Demostración. Si $a \mid b$, entonces existe $x \in D$ tal que $ax = b$. Poniendo $x = r_1r_2\cdots r_t$, se tiene

$$p_1p_2\cdots p_nr_1r_2\cdots r_t = q_1q_2\cdots q_m$$

y se deduce la tesis, a partir de la Observación 2.2.6.

Recíprocamente si existe tal σ se tiene que

$$b = \prod_{j=1}^{m} q_j = x\prod_{i=1}^{n} p_i \prod_{j\notin \operatorname{Im}(\sigma)} q_j = xa \prod_{j\notin \operatorname{Im}(\sigma)} q_j$$

para cierto $x \in D^\times$. □

Proposición 2.2.6. *Sea D un dominio en el que todo elemento no nulo y no invertible se descompone en producto de irreducibles. Entonces son equivalentes:*

- *D es un DFU,*
- *todo irreducible en D es primo.*

Demostración. Supongamos primero que D es un DFU y que p es irreducible y que $p \mid ab$. Pongamos $a = p_1p_2\cdots p_n$ y $b = q_1q_2\cdots q_m$. Se tiene $ab = pc$ para cierto $c = r_1r_2\cdots r_t \in D$. De la igualdad

$$pr_1r_2\cdots r_t = p_1p_2\cdots p_nq_1q_2\cdots q_m,$$

y la unicidad de la descomposición en irreducibles, se deduce que existe $i \in \{1, \ldots, n\}$ tal que $p \sim p_i$ o existe $j \in \{1, \ldots, m\}$ tal que $p \sim q_j$. En el primer caso $p \mid a$ y en el segundo $p \mid b$.

Recíprocamente, supongamos que todo irreducible en D es primo y que $p_1p_2\ldots p_n = q_1q_2\ldots q_m$, con $p_i, q_j \in D$ irreducibles $\forall i \leqslant n, j \leqslant m$. Para cada $i \leqslant n$, como p_i es primo y divide al término de la derecha, se tiene que $p_i \mid q_j$ para cierto $j \leqslant m$. Como además q_j es irreducible, se deduce $p_i \sim q_j$. □

2.2.3. Dominios a ideales principales

Definición 2.2.7. Un dominio D se dice *dominio a ideales principales* (DIP) si todo ideal de D es principal, es decir, si todo ideal de D está generado por un elemento.

Ejemplos 2.2.3.

- El anillo de enteros $\mathbb{Z}$ es un DIP puesto que sus ideales son de la forma $n\mathbb{Z}$, es decir principales.
- El anillo de polinomios $\Bbbk[x]$ es un DIP si y sólo si $\Bbbk$ es un cuerpo.

  Observemos primero que si $\Bbbk$ no es un cuerpo, existe $a \in \Bbbk$ no invertible y no nulo. Es fácil ver que el ideal $I = \{p \in \Bbbk[x] \mid p(0) \text{ es múltiplo de } a\}$ no es principal. En efecto, $a \in I$ y $x \in I$, pero el único divisor común entre ellos es 1, por lo que si I fuera principal sería $I = (1) = \Bbbk[x]$.

  Recíprocamente, si $\Bbbk$ es un cuerpo, la división euclídea de polinomios nos permite probar de manera análoga que en el caso de $\mathbb{Z}$ que todos los ideales de $\Bbbk[x]$ son principales[3]. En efecto, dado un ideal I, consideremos un polinomio $f \in I$ de grado mínimo entre los grados de los polinomios en I. Sea $g \in I$ cualquiera. Como $\mathrm{gr}(g) \geqslant \mathrm{gr}(f)$ se tiene $g = fq + r$, con $\mathrm{gr}(r) < \mathrm{gr}(f)$ o $r = 0$. Pero $r = g - fq \in I$, por lo que no puede tener grado menor que el grado de f. Se deduce $r = 0$ y por tanto $I = (f)$.

Proposición 2.2.7. *Sean D un DIP, $I \lhd D$. Son equivalentes:*

1. *I es maximal,*
2. *I es primo.*

Demostración. Ya sabemos que (1) implica (2) en un anillo conmutativo. Para (2) implica (1), supongamos que I es primo y que $I \subsetneq M \subseteq D$. Sean $p, q \in D$ tales que $I = (p)$ y $M = (q)$. Se tiene $p = xq$ para cierto $x \in D$ no invertible. Por ser I primo y como $q \notin I$, se deduce $x \in I$, de donde $x = py$ y por tanto $x \sim p$. Pero entonces q es invertible y por tanto $M = D$. $\square$

Corolario 2.2.8. *En un dominio a ideales principales, todo irreducible es primo (y recíprocamente).*

Demostración. Si $p \in D$ es irreducible, entonces $I = (p)$ es maximal respecto de la inclusión en la familia de ideales principales propios; como D es un DIP, se deduce que I es maximal y por tanto primo. En consecuencia, p es primo. $\square$

Queremos probar que todo dominio a ideales principales es un dominio de factorización única. El lector podrá observar que, existiendo la descomposición en producto de irreducibles, el corolario anterior asegura la unicidad de la descomposición a menos de asociados (esto quedará claro de todas formas en la prueba del Teorema 2.2.9). Queremos entonces estudiar qué particularidad de los dominios a ideales principales es la que asegura la existencia de la descomposición. Esta es el hecho de que todo ideal sea finitamente generado. Los anillos que verifican esto tienen su importancia propia en teoría de anillos, es por esto que les dedicamos el próximo apartado.

[3] Estos dos son casos particulares de una observación más general, y es que cualquier *dominio euclídeo* es a ideales principales: ver práctico 5.

Anillos noetherianos

En esta sección, estudiamos una condición de finitud de anillos, que se muestra ligada a la existencia de la descomposición factorial en dominios (ver Teorema 2.2.11).

Proposición 2.2.9. *Consideremos un anillo conmutativo A. Las siguientes proposiciones son equivalentes:*

1. *Todo ideal de A es finitamente generado.*
2. *Toda sucesión creciente de ideales en A estabiliza. Esto es, si $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ es una cadena de ideales de A, entonces existe $n \in \mathbb{Z}^+$ tal que $I_n = I_{n+1} = \cdots$.*
3. *Toda familia no vacía de ideales de A contiene un elemento maximal respecto de la inclusión.*

Demostración. Supongamos primero que todo ideal de A es finitamente generado y tomemos una sucesión creciente de ideales:

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots \subset A.$$

Sea $I = \bigcup_{n\geqslant 0} I_n$. Como los I_k están encajados, I es un ideal de A (como en la demostración de la existencia de ideales maximales). Existen entonces $x_1, x_2, \ldots, x_k \in A$ tales que el conjunto $\{x_1, x_2, \ldots, x_k\}$ genera al ideal I. Para cada $i \in \{1, \ldots, k\}$ se tiene que $x_i \in I$, luego existe $n_i \in \mathbb{Z}^+$ tal que $x_i \in I_{n_i}$. Por lo tanto si $N = \text{máx}\{n_1, \ldots, n_k\}$ entonces $I \subseteq I_N$. Se deduce que $I_n = I$ para todo $n \geqslant N$.

Para probar (2) implica (3), consideremos una familia $\mathcal{F}$ no vacía de ideales y un elemento $I_1 \in \mathcal{F}$. Si I_1 no es maximal, está propiamente contenido en otro ideal $I_2 \in \mathcal{F}$. Si I_2 no es maximal, está propiamente contenido en otro ideal $I_3 \in \mathcal{F}$. Se construye así una cadena estrictamente creciente de ideales en $\mathcal{F}$: $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \cdots$, lo que contradice (2). Se deduce que para algún n, I_n es maximal en $\mathcal{F}$.

Finalmente, supongamos que vale (3) y que I es un ideal de A. Consideremos la familia $\{J \subseteq I \mid J \lhd A, J \text{ finitamente generado}\}$. Es no vacía porque contiene al ideal $\{0\}$ y tiene por tanto un elemento maximal M. Si $M \neq I$, entonces existe $x \in I \backslash M$ y el ideal generado por $M \cup \{x\}$ es finitamente generado y está incluido en I. Esto contradice la maximalidad de M como elemento de la familia. Se deduce entonces que $M = I$ y por tanto que I es finitamente generado. □

Definición 2.2.8. Un anillo conmutativo que verifica una de las condiciones de la Proposición 2.2.9 se dice *noetheriano*.

Ejemplos 2.2.4.

- Todo DIP es noetheriano.
- El anillo de polinomios en infinitas variables $\Bbbk[x_1, x_2, \ldots, x_n, \ldots]$ no es noetheriano.
- Más adelante (Teorema 2.2.10) probaremos el *teorema de la base de Hilbert* que afirma que si A es un anillo noetheriano, entonces $A[x_1, \ldots, x_n]$ es noetheriano.

Observación 2.2.7. La noción de noetherianidad tiene su versión lateral (considerando ideales a izquierda o a derecha), pero estamos interesados en el caso de anillos conmutativos, y por eso así la definimos.

El siguiente teorema permite deducir que los anillos de polinomios en finitas variables $A[x_1, x_2 \cdots, x_n]$ sí son noetherianos siempre que A lo sea.

Teorema 2.2.10 (Teorema de la base de Hilbert)**.** *Sea A un anillo conmutativo. Si A es noetheriano, entonces $A[x]$ también lo es.*

Demostración. Tomemos un ideal $J \lhd A[x]$. Vamos a probar que J es finitamente generado. Para esto, consideramos $I_n = \{a \in A \mid \text{ existe } f \in J \text{ con } \operatorname{gr}(f) = n, a = \ell(f)\} \cup \{0\}$: en otras palabras, el conjunto de los coeficientes líderes de los polinomios de grado n de J. Es fácil ver que I_n es un ideal de A y que $I_n \subseteq I_{n+1}, \forall n \in \mathbb{N}$. Como A es noetheriano, la sucesión estabiliza en algún $I_{\bar{n}}$.

Para cada $i \leqslant \bar{n}$, el ideal I_i es finitamente generado, pongamos que está generado por ciertos $\{a_{i1}, a_{i2}, \ldots, a_{ik_i}\}$. Sean $f_{ij} \in J$ de grado i tales que $\ell(f_{ij}) = a_{ij}$.

Tomemos $f \in J$ no nulo. Probaremos por inducción en $\operatorname{gr}(f)$ que f está generado por los f_{ij}. Si $\operatorname{gr}(f) = 0$, entonces $f \in I_0$ y está generado por $\{f_{0j} \mid j \leqslant k_0\}$. Supongamos que todos los polinomios en J de grado menor que n están generados por los f_{ij} y probemos que los de grado n también lo están.

Sea $f \in J$, con $\operatorname{gr}(f) = n$. Se tiene $\ell(f) \in I_n \subseteq I_{\bar{n}}$, por lo que $\ell(f) = \sum_{j \leqslant k_{\bar{n}}} \lambda_{\bar{n}j} a_{\bar{n}j}$. Si $n \leqslant \bar{n}$, el polinomio $f - \sum \lambda_{\bar{n}j} f_{\bar{n}j} \in J$ es nulo o de grado estrictamente menor que n, por lo que está generado por los f_{ij}. Se deduce que f también lo está. Si $n > \bar{n}$, el polinomio $f - \sum x^{n-\bar{n}} \lambda_{\bar{n}j} f_{\bar{n}j} \in J$ es nulo o de grado estrictamente menor que n, por lo que se deduce otra vez que f está generado por los f_{ij}. $\square$

Todo DIP es un DFU

Teorema 2.2.11. *Si D es un dominio tal que:*

1. *D es noetheriano,*
2. *todo irreducible en D es primo,*

entonces D es un dominio de factorización única.

Demostración. Vamos a ver que la primera condición implica la existencia de la descomposición, y que la segunda implica la unicidad.

Para la existencia, consideremos la familia

$$\mathcal{F} = \{(a) \mid a \notin D^\times, a \neq 0, a \text{ no se descompone en producto de irreducibles}\}.$$

Queremos ver que $\mathcal{F} = \varnothing$. Si fuera no vacía, como D es noetheriano, existe $a_M \in D$ tal que (a_M) es un elemento maximal en $\mathcal{F}$. En particular se tiene que a_M es no nulo y no invertible y que a_M no es irreducible (por no ser producto de irreducibles). Por tanto a_M se descompone en producto de dos elementos no nulos y no invertibles de D: $a_M = xy$. Además, como a_M no es producto de irreducibles, o bien x o bien y no es producto de irreducibles. Supongamos sin pérdida de generalidad que x no es producto de irreducibles. Se tiene entonces

$$(x) \in \mathcal{F} \text{ y } (a_M) \subsetneq (x),$$

lo que contradice la maximalidad de (a_M) como elemento de $\mathcal{F}$.

Para la unicidad de la descomposición, alcanza con aplicar la Proposición 2.2.6.

Recordamos que puede deducirse $n = m$ como se muestra en la observación 2.2.6.2. $\square$

Como todo dominio a ideales principales es noetheriano y verifica la condición de que los irreducibles son (los) primos, se deduce el siguiente corolario.

Corolario 2.2.12. *Todo dominio a ideales principales es un dominio de factorización única.*

El recíproco no es cierto, i.e. hay dominios de factorización única que no son dominios a ideales principales. Un ejemplo es el anillo de polinomios $\mathbb{Z}[x]$ y generalizaciones de éste. Entenderemos bien este hecho en la próxima sección, dedicada a divisibilidad en anillos de polinomios. Pero antes, una última observación general.

Proposición 2.2.13. *Si D es un DFU, entonces existe* $\operatorname{mcd}(a,b)$ *para cualesquiera $a,b \in D$ no simultáneamente nulos.*

Demostración. Pongamos

$$a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m}, \qquad b = vp_1^{\beta_1}p_2^{\beta_2}\cdots p_m^{\beta_m},$$

con $u, v \in D^\times$, y para cada $i \leqslant m$, p_i irreducible tal que $p_i \not\sim p_j$ si $i \neq j$, y $\alpha_i, \beta_i \in \mathbb{N}$. Si tomamos para cada $i \leqslant m$, $\gamma_i = \text{mín}\{\alpha_i, \beta_i\}$, entonces es fácil (y queda a cargo del lector) verificar que

$$\operatorname{mcd}(a,b) = p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_m^{\gamma_m}.$$ □

Definición 2.2.9. Si $a, b \in D$ son no simultáneamente nulos, decimos que a y b son *primos entre sí* si existe $\operatorname{mcd}(a,b)$ y $\operatorname{mcd}(a,b) = 1$.

Proposición 2.2.14 (Lema de Euclides)**.** *Sean a, b, c elementos no nulos en un dominio factorial. Si $a \mid bc$ y* $\operatorname{mcd}(a,b) = 1$*, entonces $a \mid c$.*

Demostración. Supongamos $a = p_1p_2\cdots p_m$ una descomposición en irreducibles de a. Para cada $i \in \{1, \dots, m\}$, se tiene que $p_i \mid bc$ y como p_i es primo, se tiene que p_i divide a b o divide a c. Ahora bien, $\operatorname{mcd}(a,b) = 1$, por lo que si $p_i \mid b$, como también $p_i \mid a$ se tendría $p_i \mid 1$ y por tanto sería p_i invertible. Entonces $p_i \mid c$ para todo $i \in \{1, \dots, m\}$, de donde $a \mid c$. □

Proposición 2.2.15. *Sean D un dominio a ideales principales y $a, b \in D$ no simultáneamente nulos. Entonces:*

1. *existe* $\operatorname{mcd}(a,b)$*,*

2. *si* $\operatorname{mcd}(a,b) = d$ *entonces $(a,b) = (d)$. En particular existen $x, y \in D$ tales que $ax + by = d$* (identidad de Bézout).

Demostración. La existencia de $\operatorname{mcd}(a,b)$ se debe a que D es en particular un dominio de factorización única. Además, si consideramos el ideal

$$I = (a,b) = \{ax + by \mid x, y \in D\},$$

como D es un dominio a ideales principales, existe $c \in D$ tal que $I = (c)$.

Como $(a) \subseteq I$, se tiene que $c \mid a$. Análogamente se tiene que $c \mid b$ y por lo tanto $c \mid d$.

Por otra parte $d \mid ax + by$ para todo $x, y \in D$, en particular $d \mid c$. Se deduce $I = (d)$, por lo que existen $x, y \in D$ tales que $ax + by = d$. □

2.2.4. Divisibilidad en anillos de polinomios

Polinomios como funciones

Recordemos que la propiedad universal de los anillos de polinomios da lugar a la existencia, para cada $a \in A$, del morfismo de anillos *evaluación en a* $\varepsilon_a : A[x] \to A$ que verifica $\varepsilon_a(d) = d$ para todo $d \in D$, y $\varepsilon_a(x) = a$.

Para $p \in A[x]$ y $a \in D$, usamos la notación $p(a) := \varepsilon_a(p)$. Observar que el hecho de que ε_a sea morfismo de anillos se interpreta con la nueva notación mediante $(p+q)(a) = p(a) + q(a), (pq)(a) = p(a)q(a)$ para todo $p, q \in A[x]$. Además si $p = c \in A$ es un polinomio constante entonces $p(a) = c$ para todo $a \in A$.

Haciendo variar $a \in A$, se obtiene una función

$$\varphi : A[x] \to A^A, \text{ definida por } \varphi(p)(a) = p(a),$$

que resulta ser un morfismo de anillos si ponemos en el conjunto de funciones A^A la estructura dada por la suma y el producto punto a punto.

Ahora bien, es claro que φ en general no es sobreyectiva (no toda función de D en D es un polinomio: la función $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = \begin{cases} 1 & \text{si } x \geqslant 0 \\ 0 & \text{si no} \end{cases}$ no es un polinomio, pues $\lim_{x\to+\infty} f(x) = 1$ y eso implicaría que fuera el polinomio constante 1).

En cuanto a la inyectividad, el siguiente ejemplo muestra que φ en general no es inyectiva:

$$p(x) = x^3 - x \in \mathbb{Z}_3[x] \text{ es no nulo; sin embargo, } p(a) = 0 \quad \forall a \in \mathbb{Z}_3, \text{ es decir } \varphi(p) = 0.$$

De hecho vamos a probar en la próxima sección, para el caso de polinomios sobre dominios, que φ es inyectiva si y sólo si D es infinito. Por lo tanto podemos identificar D con su imagen $\varphi(D)$ de *funciones polinómicas* sólo en el caso que D sea un dominio infinito.

Raíces

Se tiene la función $deg : A[x]^* \to \mathbb{N}$ que asocia a cada polinomio no nulo el máximo exponente en x de los monomios que lo conforman que nota $deg(p)$ y se llama **grado de p**. Al coeficiente asociado a $x^deg(p)$ se le llama **coeficiente líder de** p. Notar que $deg(p) = 0$ si y solo si p es constante.

Si $A = D$ es un dominio y $p, qsonnonulos$, se verifica $deg(pq) = deg(p) + deg(q), \forall p, q \in D[x]$ y esto permite deducir que $D[x]$ también es un dominio.

Además, si $A = \Bbbk$ es un cuerpo, se tiene que para todos $p, d \in \Bbbk[x], d \neq 0$, existen $q, r \in \Bbbk[x]$ tales que $p = dq + r$ y $r = 0$ o $deg(r) < deg(d)$. (esto asegura que $\Bbbk[x]$ es un dominio euclídeo como se vio en un ejercicio de práctico, y por tanto un dominio a ideales principales).

Observación 2.2.8. Si $t \in D[x]$ es un polinomio con coeficiente líder invertible, entonces para cualquier $p \in D[x]$, existen $q, r \in D[x]$ tales que $p = qt + r$ y $r = 0$ o $\operatorname{gr}(r) < \operatorname{gr}(t)$.

En efecto, se puede ver que la división euclídea en $\Bbbk[x]$ da lugar a $q \in D[x]$ y por tanto $r = p - qt \in D[x]$. Decimos que r *es el resto de dividir* p *por* q.

En particular, como el coeficiente líder de $x - a$ es 1 y por tanto invertible, para cualquier polinomio $p \in D[x]$ existen $q, r \in D[x]$ tales que $p = (x-a)q + r$ y $r \in D$.

Definición 2.2.10. Sea $p \in D[x]$. Un elemento $a \in D$ se dice *raíz* de p si $p(a) = 0$.

Proposición 2.2.16 (Teorema del resto)**.** *El resto de dividir un polinomio $p \in D[x]$ por $x - a$ es $p(a)$.*

Demostración. Basta aplicar el morfismo de anillos ε_a a la igualdad $p(x) = q(x)(x - a) + r$. □

Corolario 2.2.17. *Un polinomio $p \in D[x]$ se escribe como $(x - a)q$ para algún $q \in D[x]$ si y sólo si $p(a) = 0$.*

De este corolario sacamos dos corolarios:

Corolario 2.2.18. *Todo polinomio no nulo $p \in D[x]$ tiene una cantidad finita de raíces.*

Demostración. Sea $p \in D[x]$ un polinomio de grado n. Sean $c_1, c_2, \dots$ las raíces diferentes de p en D. Entonces $p(x) = q_1(x)(x - c_1)$, de donde $0 = p(c_2) = q_1(c_2)(c_2 - c_1)$. Como $c_1 \neq c_2$ y D es un dominio, entonces $q_1(c_2) = 0$. Por lo tanto $x - c_2$ divide a q_2, y $p(x) = q_3(x)(x - c_2)(x - c_1)$. Por inducción llegamos a que dadas m raíces diferentes $c_1, \dots, c_m$ de p, el polinomio $g_m = (x - c_1)(x - c_2) \cdots (x - c_m)$ divide a p. Pero gr $g_m = m$, de donde $m \leqslant n$. □

Proposición 2.2.19. *El morfismo $\varphi : D[x] \to D^D$ definido por $\varphi(p)(a) = p(a)$ es inyectivo si y sólo si D es infinito.*

Demostración. Si D es finito, entonces D^D también lo es, pero $D[x]$ es infinito, por lo que φ no es inyectivo.

Si D es infinito y $p \in D[x]$ es no nulo, entonces p tiene una cantidad finita de raíces y por lo tanto algún elemento de D no es raíz de p, de lo que se deduce $\varphi(p) \neq 0$. □

Contenido

Definición 2.2.11. Sea D un dominio de factorización única y $f = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ no nulo. Se define el *contenido* de f como $\operatorname{cont}(f) = \operatorname{mcd}(a_n, \dots, a_1, a_0)$. Decimos que f es *primitivo* si $\operatorname{cont}(f) = 1$.

Ejemplo 2.2.1.

- Todo polinomio mónico es primitivo.
- $f = 2x + 3$ es primitivo en $\mathbb{Z}[x]$, pero $g = 2x + 4$ no lo es, de hecho $\operatorname{cont}(g) = 2 \nsim 1$.

Observación 2.2.9.

1. Notar que hacemos el mismo abuso de notación que para el máximo común divisor. Si bien $\operatorname{cont}(f)$ es una $\sim$-clase de equivalencia en D, usamos la notación para referirnos a cualquiera de sus representantes.
2. Si $f \in D[x]$ y $a \in D, a \neq 0$, entonces $\operatorname{cont}(af) = a \operatorname{cont}(f)$. Además siempre existe un (único a menos de multiplicar por un invertible de D) polinomio $\overline{f} \in D[x]$ tal que $f = \operatorname{cont}(f)\overline{f}$. Este polinomio $\overline{f}$ resulta obviamente primitivo.

Lema 2.2.20 (Lema de Gauss)**.** *Sean $f, g \in D[X]$, donde D es un dominio de factorización única.*

1. *Si f y g son primitivos, su producto fg también lo es.*
2. *Más en general, se tiene* $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$.

Demostración.

1. Supongamos primero que f y g son primitivos y que $p \in D$ es primo. Pongamos $f = a_n x^n + \cdots + a_1 x + a_0$ y $g = b_m x^m + \cdots + b_1 x + b_0$. Por ser f y g primitivos, $p \nmid \operatorname{cont}(f)$ y $p \nmid \operatorname{cont}(g)$, por lo que existen $i \in \{0, \dots, n\}, j \in \{0, \dots, m\}$ tales que

a_i y b_j no son múltiplos de p. Podemos entonces considerar $\bar{i}_0 := \text{mín}\{i \mid p \nmid a_i\}$ y $j_0 = \text{mín}\{j \mid p \nmid b_j\}$. Ahora bien, sea $k = i_0 + j_0$; el término k-ésimo de fg es

$$a_0b_k + a_1b_{k-1} + \cdots + a_{i_0}b_{j_0} + \cdots + a_{k-1}b_1 + a_kb_0.$$

Tenemos tres tipos de sumandos a_ib_j en el término de arriba:

- sumandos en que $i < i_0$: $p \mid a_i$ y por tanto el sumando es múltiplo de p;
- sumandos en que $j < j_0$: $p \mid b_j$ y por tanto el sumando es múltiplo de p:
- el sumando $a_{i_0}b_{j_0}$: $p \nmid a_{i_0}$ y $p \nmid b_{j_0}$, por lo que el sumando no es múltiplo de p.

Para cada primo p, existe entonces un coeficiente que no es múltiplo de p (el k-ésimo, según la construcción de arriba). Se deduce $\text{cont}\,(fg) = 1$.

2. Supongamos ahora que f y g son polinomios cualesquiera y pongamos $f = \text{cont}\,(f)\bar{f}$ y $g = \text{cont}\,(g)\bar{g}$, con $\bar{f}, \bar{g}$ primitivos. Se tiene $fg = \text{cont}\,(f)\,\text{cont}\,(g)\bar{f}\bar{g}$, y como $\bar{f}\bar{g}$ es primitivo (por la parte anterior) se deduce que

$$\text{cont}\,(fg) = \text{cont}\,(f)\,\text{cont}\,(g)\,\text{cont}\,(\bar{f}\bar{g}) = \text{cont}\,(f)\,\text{cont}\,(g). \qquad \square$$

Criterios de irreducibilidad

Proposición 2.2.21. *Sea K un cuerpo y $p \in K[x]$ un polinomio de grado dos o tres. Entonces p es reducible si y sólo si tiene una raíz en K.*

Demostración. Un polinomio de grado dos o tres con coeficientes en un cuerpo es reducible si y sólo si tiene un factor lineal, pues $K[x]^\times = K^\times = K\backslash\{0\}$. Por el corolario 2.2.17 esto ocurre si y sólo si f tiene una raíz en K. $\square$

En lo queda de esta sección, D será un dominio y $\Bbbk$ denotará al cuerpo de fracciones de D.

Proposición 2.2.22 (Criterio de la raíz racional)**.** *Sea $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in D[X]$ con $a_n \neq 0$, y sea $\frac{p}{q} \in \Bbbk$ una raíz de f, con $\operatorname{mcd}(p,q) = 1$. Entonces $p \mid a_0$ y $q \mid a_n$ en D.*

Demostración. Tenemos que $a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1\frac{p}{q} + a_0 = 0$, por lo tanto $a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$ y entonces:

$$a_0 q^n = -p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1})$$

Esto prueba que $p \mid a_0 q^n$. Como $\operatorname{mcd}(p,q) = 1$, entonces $\operatorname{mcd}(p,q^n) = 1$. El lema de Euclides (Proposición 2.2.14) nos da que $p \mid a_0$. Análogamente $q \mid a_n$. □

Corolario 2.2.23. *Si $f \in D[X]$ es un polinomio mónico y $\alpha \in \Bbbk$ es raíz de f, entonces $\alpha \in D$.*

El siguiente es un lema técnico que será de utilidad en los resultados que le siguen:

Lema 2.2.24. *Si $f \in D[x]$ es tal que $f = gh$ para ciertos $g, h \in \Bbbk[x]$, entonces existen $g', h' \in D[x]$ y $\lambda, \mu \in \Bbbk$ no nulos, tales que $f = g'h'$, $g = \lambda g'$ y $h = \mu h'$.*

Demostración. Tomando $a, b \in D^*$ como los respectivos productos de los denominadores de los coeficientes de g y h, surge que existen $\tilde{g}, \tilde{h} \in D[x]$ tales que $g = \frac{1}{a}\tilde{g}, h = \frac{1}{b}\tilde{h}$ (observar que para esto alcanza con que D sea un dominio).
Obtenemos la igualdad en D: $abf = \tilde{g}\tilde{h} = cont(\tilde{g})cont(\tilde{h})g''h''$, con $g'', h'' \in D[x]$ primitivos. Tomando contenidos de ambos lados, se deduce que $abcont(f) = \operatorname{cont}(\tilde{g})\operatorname{cont}(\tilde{h}) = cont(ag)cont(bh) = abcont(g)cont(h)$ y por tanto, se deduce de la primera igualdad de este párrafo $abf = abcont(f)g''h''$ y, cancelando ab, se tiene $f = cont(f)g''h''$. La prueba termina considerando por ejemplo $g' = cont(f)g'' = \frac{acont(f)}{cont(\tilde{g})}g, h' = h'' = \frac{b}{cont(\tilde{h})}$. □

Teorema 2.2.25 (Criterio de irreducibilidad de Gauss)**.** [4] *Sea $f \in D[x]$ no constante. Entonces f es irreducible en $D[x]$ si y sólo si es irreducible en $\Bbbk[x]$ y es primitivo en $D[x]$.*

Demostración. Supongamos primero que f es irreducible como polinomio en $\Bbbk[x]$ y es primitivo como polinomio en $D[x]$. Si $f = gh$ es una descomposición de f en producto de polinomios $g, h \in D[x]$, también lo es en $\Bbbk[x]$ y por tanto g o h es invertible en $\Bbbk[x]$. Supongamos sin perder generalidad que g lo es. Esto implica que $g \in \Bbbk^\times \cap D[x] = D \backslash \{0\}$. Pero en ese caso $\operatorname{cont}(f) = g \operatorname{cont}(h)$, y como $\operatorname{cont}(f) = 1$ se tiene que $g \in D$ es invertible. Se deduce que f es irreducible en $D[x]$.

Recíprocamente, supongamos que f es irreducible y no constante como polinomio en $D[x]$. Por la descomposición $f = \operatorname{cont}(f)\overline{f}$ con $\overline{f}$ primitivo, debe ser f primitivo.

Supongamos que $f = gh$ es una descomposición de f en producto de polinomios $g, h \in \Bbbk[x]$. Usando el Lema 2.2.24, se deduce $f = g'h'$ para ciertos $g', h' \in D[x]$ primitivos (porque f es primitivo) tales que $g = \lambda g', h = \mu h'$ para ciertos $\lambda, \mu \in \Bbbk$ no nulos.

Como f es irreducible en $D[x]$ se deduce que g' o h' son invertibles. Supongamos sin perder generalidad que g' es invertible en $D[x]$. Entonces $g' \in D\backslash\{0\}$, por lo que $g' \in D$ y por tanto $g \in \Bbbk$. Esto implica que en la descomposición original $f = gh$, el polinomio $g \in \Bbbk[x]$ es invertible. □

Ejemplo 2.2.2. Sea $f = x^3 + x^2 + 10x + 1 \in \mathbb{Z}[x]$. Por el criterio de la raíz racional, sus únicas posibles raíces racionales son ± 1. Se verifica fácilmente que $f(\pm 1) \neq 0$, luego f no tiene raíces racionales. En particular, por la Proposición 2.2.21, al ser f de grado tres, es irreducible en $\mathbb{Q}$ (y como es primitivo, es irreducible también en $\mathbb{Z}$, por el criterio de irreducibilidad de Gauss).

[4] En muchos textos se llama también a este resultado *lema de Gauss*.

Proposición 2.2.26 (Criterio de irreducibilidad de Eisenstein). *Sea* $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in D[X]$ *con* $a_n \neq 0$. *Supongamos que existe* $p \in D$ *irreducible tal que:*

- $p \mid a_1, \ldots, p \mid a_{n-1}$,
- $p \nmid a_n$,
- $p \mid a_0, p^2 \nmid a_0$.

Entonces f *es irreducible en* $\Bbbk[x]$.[5]

Demostración. Supongamos $f = gh \in D[x]$ con $g, h \in \Bbbk[x]$. Veamos que $g \in \Bbbk \backslash \{0\}$ o $h \in \Bbbk \backslash \{0\}$. Escribamos $g = b_r x^r + \cdots + b_1 x + b_0$, $h = c_s x^s + \cdots + c_1 x + c_0$, con $b_r c_s \neq 0$. Ahora bien, por hipótesis $a_0 = b_0 c_0$ es múltiplo de p y no es múltiplo de p^2. Podemos suponer entonces sin pérdida de generalidad que $p \mid b_0$ y $p \nmid c_0$.

Por otra parte, como $p \nmid a_n = b_r c_s$, tenemos que b_r no es múltiplo de p. En particular, existe $i \in \{0, \ldots, r\}$ tal que $p \mid b_k$ para todo $k < i$ y $p \nmid b_i$. Se tiene entonces $p \nmid b_i c_0$ y por tanto $p \nmid a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_1 c_{i-1} + b_0 c_i$. Se deduce que $i = n$ y por tanto $\mathrm{gr}\,(h) = 0$, es decir $h \in \Bbbk \backslash \{0\}$. □

Ejemplos 2.2.5.

1. $f = x^4 + 2x^3 + 2x^2 + 2x + 2 \in \mathbb{Z}[x]$ es irreducible.
2. $f = x^n + p \in \mathbb{Z}[x]$, es irreducible para cualquier primo $p \in \mathbb{Z}$. Este ejemplo muestra que hay polinomios irreducibles en $\mathbb{Z}$ de grado arbitrario.

Preservación de la Factorización única

Lema 2.2.27. *Sean* D *un dominio y* $\Bbbk$ *su cuerpo de fracciones.*

1. *Si* $a \in D$ *es primo, entonces es primo en* $D[x]$.
2. *Sea* $f \in D[x]$ *es primitivo; si* f *es primo en* $\Bbbk[x]$ *entonces es primo en* $D[x]$.

Demostración.

1. Si $a \mid fg$, entonces $a \mid \mathrm{cont}\,(f)\,\mathrm{cont}\,(g)$ y por tanto $a \mid \mathrm{cont}\,(f)$ o $a \mid \mathrm{cont}\,(g)$. Se deduce que $a \mid f$ o $a \mid g$.
2. Si $f \mid gh$ en $D[x]$, entonces también $f \mid gh$ en $\Bbbk[x]$. Supongamos para fijar ideas que $f \mid g$ en $\Bbbk[x]$. Existe entonces $\varphi \in \Bbbk[x]$ tal que $f\varphi = g$. Multiplicando por el denominador común de los términos de φ se obtiene una igualdad en $D[x]$ de la forma $f\varphi' = ag$, con $a \in D$. Tomando contenidos y usando que f es primitivo, se deduce que $cont(\varphi') = acont(g)$, por lo que se tiene para cierto $h \in D[x]$, $acont(g)hf = ag$ en $D[x]$. Como D es un dominio, se deduce $cont(g)hf = g$ y por lo tanto $f \mid g$ en $D[x]$. □

Teorema 2.2.28. *Si* D *es un dominio de factorización única, entonces* $D[x]$ *también lo es.*

Demostración. Sabemos que $D[x]$ es también un dominio. Además, para $f \in D[x]$ no nulo y no invertible se tiene $f = \mathrm{cont}\,(f)\bar{f}$, con $\bar{f} \in D[x]$ no nulo y primitivo.

Sea $\Bbbk = Frac(D)$. Como $\Bbbk[x]$ es un dominio de factorización única (pues es un DIP), $\bar{f} \neq 0$ es invertible o se descompone en $\Bbbk[x]$ como producto de irreducibles. Cada irreducible en $\Bbbk[x]$ es de la forma $\frac{1}{a}h(x)$ con $h(x) \in D[x]$ irreducible en $\Bbbk[x]$ y $a \in D\backslash\{0\}$. Se tiene entonces que si $\bar{f}$ no es invertible, es de la forma $\bar{f} = \frac{1}{d}h_1 h_2 \ldots h_n$ con $d \in D\backslash\{0\}, h_i \in D[x]$ irreducible en $\Bbbk[x]$, para todo $i \in \{1, \ldots, n\}$. Para cada i podemos escribir $h_i = \mathrm{cont}\,(h_i)h_i'$ con h_i' primitivo. Se tiene entonces:

[5] En el práctico 5 aparece como ejercicio opcional una generalización del criterio de Eisenstein a dominios cualesquiera.

- h_i' es primitivo y por tanto irreducible en $D[x]$, para todo $i \in \{1, \ldots, n\}$,
- $\frac{\text{cont}(h_1)\cdots\text{cont}(h_n)}{d} \in D$ es invertible en D,
- $cont(f)$ se descompone en irreducibles en D y por tanto en $D[x]$,
- $\bar{f} = \frac{\text{cont}(h_1)\cdots\text{cont}(h_n)}{d} h_1' h_2' \ldots h_n'$,

por lo que $f = \frac{\text{cont}(h_1)\cdots\text{cont}(h_n)}{d} cont(f) h_1' h_2' \ldots h_n'$.

Se deduce la existencia de la descomposición factorial en irreducibles.

Para la unicidad, por la Proposición 2.2.6, alcanza con probar que todo irreducible de $D[x]$ es primo. Sea $f \in D[x]$ irreducible.

Si $\text{gr}(f) = 0$, entonces es claro que f es irreducible como elemento en D y por tanto primo en D, de lo que se deduce usando el Lema 2.2.27 que es primo en $D[x]$.

Si $\text{gr}(f) > 0$, f es irreducible como elemento en $\Bbbk[x]$ y por tanto primo. Se deduce usando la otra parte del Lema 2.2.27 que es primo en $D[x]$. $\square$

Este último teorema nos permite deducir que $\mathbb{Z}[x]$ y $\Bbbk[x, y] \cong \Bbbk[x][y]$ son dominios de factorización única (que no son dominios a ideales principales). Más en general, se tiene el siguiente corolario.

Corolario 2.2.29. *Si D es un dominio de factorización única $D[x_1, x_2, \ldots, x_n]$ también lo es.*

Observación 2.2.10. El anillo de polinomios en infinitas variables $A = \Bbbk[x_1, x_2, \ldots, x_n, \ldots]$ es un dominio de factorización única. En efecto, si tomamos un polinomio $f \in A$, existe $n \in \mathbb{N}$ tal que $f \in A_n = \Bbbk[x_1, \ldots, x_n]$ y por tanto f se descompone en producto de irreducibles de A_n. Es un ejercicio probar que los irreducibles de A_n son irreducibles en A. Usando argumentos similares, se prueba que los primos de A son irreducibles, de lo que se deduce la unicidad de la descomposición.

Este es un ejemplo de dominio de factorización única que no es noetheriano.

Capítulo 3

Módulos

3.1. Generalidades

Durante todo el capítulo A denotará un anillo cualquiera.

Definición 3.1.1. Un A-módulo a izquierda M es una terna $(M, +, 0, \cdot)$ donde

- $(M, +, 0)$ es un grupo abeliano,
- $\cdot : A \times M \to M$ es una función (que llamaremos *acción* del anillo sobre el módulo) que verifica, para todo $a, b \in A$, $m, n \in M$:

  (1) $a \cdot (m + n) = a \cdot m + a \cdot n$,

  (2) $(a + b) \cdot m = a \cdot m + b \cdot n$,

  (3) $(ab) \cdot m = a \cdot (b \cdot m)$,

  (4) $1_A \cdot m = m$.

Ejemplo 3.1.1. El anillo A es un A-módulo a izquierda si se considera con la *acción regular*, es decir, la acción dada por el producto de A.

Observación 3.1.1.

1. De (1) se deduce que para cada $a \in A$, la función $\varphi_a : M \to M$ definida por $\varphi_a(m) = a \cdot m$ es un morfismo de grupos.
2. El conjunto $\mathrm{End}(M) = \{f : M \to M \mid f \text{ es morfismo de grupos}\}$ es un anillo con la composición. Las igualdades (2), (3) y (4) pueden interpretarse como que la función $F : A \to \mathrm{End}(M)$ definida por $F(a) = \varphi_a$ es un morfismo de anillos.[1]
3. Análogamente se define *A-módulo a derecha* mediante una acción a derecha $M \times A \to M$.
4. Si $A = (A, +, \cdot, 0, 1)$ es un anillo y se considera la operación $\cdot^{op} : A \times A \to A$ definida por $a \cdot^{op} b = b \cdot a$, entonces $A^{op} = (A, +, \cdot^{op}, 0, 1)$ es otro anillo que llamamos *anillo opuesto*. Se tiene $(A^{op})^{op} = A$ y $A^{op} = A$ si y sólo si A es conmutativo. Si $(M, +, 0)$ es un grupo abeliano y $\cdot : A \times M \to M$ y $\star : M \times A^{op} \to M$ son dos acciones vinculadas por $a \cdot m = m \star a$, es fácil ver que las siguientes afirmaciones son equivalentes:
   - $(M, +, 0, \cdot)$ es un A-módulo a izquierda,
   - $(M, +, 0, \star)$ es un A^{op}-módulo a derecha.

[1] Es un ejercicio del práctico probar que un A-módulo "es lo mismo" que un morfismo de anillos $A \to \mathrm{End}(M)$ donde M es un grupo abeliano.

En particular si A es conmutativo, todo A-módulo a izquierda es A-módulo a derecha y recíprocamente (y en este caso hablaremos sencillamente de *A-módulos*). Además esto nos muestra que no perdemos generalidad al demostrar los teoremas para módulos *a izquierda*.

5. Si M es un A-módulo a izquierda y $m \in M$, entonces $0 \cdot m = 0$ y $(-1) \cdot m = -m$. En efecto,

$$0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m \quad \text{y} \quad (-1) \cdot m + 1 \cdot m = 0 \cdot m = 0.$$

Veamos más ejemplos.

Ejemplos 3.1.1.
1. Si $A = \mathbb{k}$ es un cuerpo, entonces un $\mathbb{k}$-módulo a izquierda es exactamente un $\mathbb{k}$-espacio vectorial.
2. Si A es un anillo y consideramos el grupo abeliano $A^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A\}$, se tiene que A^n es un $M_n(A)$-módulo a izquierda y también a derecha considerando el producto usual (a izquierda y a derecha respectivamente) de una matriz por un vector.
3. Si $\mathbb{k}$ es un cuerpo y $X \in M_n(\mathbb{k})$, se tiene que el grupo abeliano $\mathbb{k}^n$ es un $\mathbb{k}[x]$-módulo a izquierda mediante $p \cdot v = p(X)v$, donde si $p = \sum_{i=0}^{r} a_i x^i$, se define $p(X) = \sum_{i=0}^{r} a_i X^i$ (con $X^0 := Id_n$).
4. Todo grupo abeliano es un $\mathbb{Z}$-módulo. En efecto, si G es un grupo abeliano, la operación usual $\mathbb{Z} \times G \to G$, definida por $(n, g) \mapsto ng$ dota a G de una estructura de $\mathbb{Z}$-módulo. Además, por definición todo $\mathbb{Z}$-módulo es un grupo abeliano. Esto muestra que un $\mathbb{Z}$-módulo "es lo mismo" que un grupo abeliano.
5. Si M es un A-módulo a izquierda y $S \neq \varnothing$ es un conjunto, el grupo de funciones M^S tiene estructura de A-módulo a izquierda definiendo $(a \cdot \varphi)(s) = a \cdot \varphi(s)$.
6. Si A es un anillo, entonces $A[[x]]$ es un $A[x]$-módulo donde la acción es la restricción de la acción regular de $A[[x]]$, con la identificación $A[x] \subset A[[x]]$.
7. (Para los que cursaron Cálculo 3). Sea X una variedad diferenciable. Notemos $C^\infty(X)$ al anillo de las funciones diferenciables $X \to \mathbb{R}$ con las operaciones punto a punto. El conjunto de las n-formas diferenciales en X, notado $\Omega^n(X)$, es un $C^\infty(X)$-módulo: si $f \in C^\infty(X)$ y $\omega \in \Omega^n(X)$, se define $f \cdot \omega$ como $(f \cdot \omega)(p) = f(p)\omega(p)$ para todo $p \in X$.

A partir de ahora, salvo mención explícita, M será un A-módulo a izquierda. Es claro que los enunciados para A-módulos a izquierda tendrán su versión para A-módulos a derecha, a partir de la observación 3.1.1.4. Además, a menudo notaremos am en lugar de $a \cdot m$, para $a \in A, m \in M$.

Definición 3.1.2. Sea M un A-módulo. Un subconjunto $N \subseteq M$ se dice *submódulo* de M si :

(1) $0 \in N$,

(2) $x + y \in N$ para todo $x, y \in N$,

(3) $an \in N$ para todo $a \in A, n \in N$.

Observación 3.1.2.
1. Es un ejercicio sencillo verificar que son equivalentes, para un A-módulo M y un subconjunto $N \subseteq M$:
   - N es un submódulo de M,
   - N es un subgrupo de M que es *A-estable* (es decir, que cumple (3)),

- N con las operaciones de M restringidas a N es un A-módulo.

2. En el caso particular en que se considera A como A-módulo a izquierda con la acción regular, un subconjunto $N \subseteq A$ es un submódulo si y sólo si es un ideal a izquierda. Si además A es conmutativo, entonces los submódulos son los ideales biláteros.

3. $\{0\}$ y M son submódulos de M y se dicen *triviales*.

Definición 3.1.3. Sean M y N A-módulos. Una función $f : M \to N$ es un *morfismo de A-módulos*, o simplemente *A-lineal* si verifica:

(1) $f(m + n) = f(m) + f(n)$ para todo $m, n \in M$,

(2) $f(a \cdot m) = a \cdot f(m)$ para todo $a \in A, m \in M$.

Si f es inyectivo o sobreyectivo, se dice que es respectivamente un *monomorfismo* o un *epimorfismo* de A-módulos.

Si $f : M \to N$ es un morfismo de A-módulos inyectivo y sobreyectivo, se dice que es un *isomorfismo* de A-módulos y que M y N son A-módulos *isomorfos* o *isomorfos via f*.

Si $f : M \to M$ se dice que es un *endomorfismo*. Notamos $\mathrm{End}_A(M)$ al conjunto de endomorfismos de M.

Observación 3.1.3. 1. Un morfismo de A-módulos en particular es morfismo de grupos (abelianos).

2. Si $A = \Bbbk$ es un cuerpo, entonces un morfismo de $\Bbbk$-módulos es exactamente una transformación $\Bbbk$-lineal.

3. Se verifica fácilmente que la composición de morfismos de A-módulos es un morfismo de A-módulos, y que la identidad también lo es. En particular $\mathrm{End}_A(M)$ es un anillo con la suma punto a punto y la composición.

4. Si f es un isomorfismo y $g : N \to M$ es su inversa, entonces g también es un morfismo de A-módulos.

Proposición 3.1.1. *Sea $f : M \to N$ morfismo de módulos. Si $H \subseteq N$ es un submódulo, entonces $f^{-1}(H) \subseteq M$ también lo es. Si $K \subseteq M$ es un submódulo, entonces $f(K) \subseteq N$ también lo es. En particular,* $\mathrm{Ker}\, f = f^{-1}(\{0\}) \subseteq M$ *e* $\mathrm{Im}\, f = f(M) \subseteq N$ *son submódulos.*

Demostración. Sea $H \subseteq N$. Sabemos que $f^{-1}(H) \leqslant M$. Además, si $x \in f^{-1}(H)$ y $a \in A$ se tiene $f(ax) = af(x) \in H$ porque $f(x) \in H$ que es un submódulo. Se deduce que $ax \in f^{-1}(H)$.

Por otra parte, si $K \subseteq M$, sabemos que $f(K) \leqslant N$. Además, si $x \in K$ y $a \in A$, $af(x) = f(ax) \in f(K)$ porque $ax \in K$ por ser éste un submódulo. □

Definición 3.1.4 (Producto directo y suma directa)**.** Sean I un conjunto no vacío y $\{M_i\}_{i \in I}$ una familia de A-módulos. El *producto directo* de $\{M_i\}_{i \in I}$ es el producto cartesiano $\prod_{i \in I} M_i$ con las operaciones

$$(m_i)_{i \in I} + (n_i)_{i \in I} = (m_i + n_i)_{i \in I}, \qquad a(m_i)_{i \in I} = (am_i)_{i \in I},$$

para todo $a \in A, (m_i)_{i \in I}, (n_i)_{i \in I} \in \prod_{i \in I} M_i$. Es fácil verificar que $\prod_{i \in I} M_i$ con estas operaciones es un A-módulo.

Para cada $m \in \prod_{i\in I} M_i$, se define el *soporte* de m, $\operatorname{sop}(m) = \{j \in I \mid m_j \neq 0\}$, y es fácil ver que el subconjunto

$$\left\{ m \in \prod_{i\in I} M_i \mid \operatorname{sop}(m) \text{ es finito} \right\}$$

es un submódulo de $\prod_{i\in I} M_i$. Lo denotamos $\bigoplus_{i\in I} M_i$ y lo llamamos *suma directa* (o *suma directa externa*, como hacíamos en grupos) de la familia.

Observación 3.1.4. 1. Si en la definición de arriba el conjunto I es finito, la suma directa y el producto directo coinciden.

2. Las proyecciones naturales $p_j : \prod_{i\in I} M_i \to M_j$ definidas por $p_j\left((m_i)_{i\in I}\right) = m_j$ son epimorfismos de módulos y las inyecciones naturales $\iota_j : M_j \to \bigoplus_{i\in I} M_i$ definidas mediante $\left(\iota_j(m)\right)_i = \begin{cases} m & \text{si } i = j \\ 0 & \text{si no} \end{cases}$ son monomorfismos de módulos.

Los pares $\left(\prod_{i\in I} M_i, (p_i)_{i\in I}\right)$ y $\left(\bigoplus_{i\in I} M_i, (\iota_i)_{i\in I}\right)$ verifican propiedades universales que presentamos a continuación.

Proposición 3.1.2 (Propiedad universal de la suma directa y del producto directo)**.** [2] *Sea $\{M_i\}_{i\in I}$ una familia de A-módulos.*

1. *Dados un A-módulo N y una familia de morfismos de A-módulos $\{f_i : N \to M_i\}_{i\in I}$, existe un único morfismo de A-módulos $\varphi : N \to \prod_{i\in I} M_i$ que hace conmutar la siguiente familia de diagramas, para todo $j \in I$:*

$$\begin{tikzcd} \prod_{i\in I} M_i \arrow[r, "p_j"] & M_j \\ N \arrow[u, dotted, "\varphi"] \arrow[ur, "f_j"'] & \end{tikzcd}$$

2. *Dados un A-módulo N y una familia de morfismos de A-módulos $\{f_i : M_i \to N\}_{i\in I}$, existe un único morfismo de A-módulos $\psi : \bigoplus_{i\in I} M_i \to N$ que hace conmutar la siguiente familia de diagramas, para todo $j \in I$:*

$$\begin{tikzcd} M_j \arrow[r, "\iota_j"] \arrow[dr, "f_j"'] & \bigoplus_{i\in I} M_i \arrow[d, dotted, "\psi"] \\ & N \end{tikzcd}$$

Demostración. Para el producto directo, es fácil ver que la única posible función está dada por $f(n)_i = f_i(n)$ para todo $n \in N$ y que esto define un morfismo de módulos.

Para la suma directa, es fácil ver que la única posible función está dada por $f\left((m_i)_{i\in I}\right) = \sum_{i\in I} f_i(m_i)$ y que esto define un morfismo de módulos. □

Es fácil probar que la intersección de una familia no vacía de submódulos es un submódulo, lo que posibilita la siguiente definición.

[2] Es un ejercicio del práctico 6 probar que las propiedades universales *caracterizan* al producto directo y a la suma directa, en el sentido que cualquier otro par que la satisfaga va a ser naturalmente isomorfo a estos.

Definición 3.1.5 (Submódulo generado)**.** Sea M un A-módulo y $S \subseteq M$ un subconjunto. El *submódulo generado* por S es $\langle S\rangle := \bigcap\{N \mid N \text{ es submódulo de } M, N \supseteq S\}$.

Observación 3.1.5.
1. Si $S \subseteq M$ es un subconjunto y $N \subseteq M$ es un submódulo que contiene a S, entonces N contiene a $\langle S\rangle$. En otras palabras el submódulo generado por S es el menor (con respecto a $\subseteq$) entre los submódulos de M que contienen a S.
2. Si $S = \varnothing$, entonces $\langle S\rangle = \{0\}$.
3. Si $S \neq \varnothing$, $\langle S\rangle = \left\{\sum\limits_{i\in I} a_i m_i \mid I \text{ es un conjunto finito, } a_i \in A,\ m_i \in S\ \ \forall i \in I\right\}$.

Definición 3.1.6. Sea M un A-módulo y $S \subseteq M$ un subconjunto. Si $M = \langle S\rangle$, decimos que S es un *generador* de M, o que S *genera* a M. Si existe $S \subseteq M$ generador finito, decimos que M está *finitamente generado.*

En el caso particular en que existe $m \in M$ tal que $\{m\}$ genera M, se dice que M es un A-módulo *cíclico* y se nota $M = Am$.

Definición 3.1.7. Sea M un A-módulo y $\{M_i\}_{i\in I}$ una familia de submódulos de M. Se define la *suma* de los submódulos M_i como

$$\sum_{i\in I} M_i = \left\langle \bigcup_{i\in I} M_i \right\rangle$$

Observación 3.1.6.
1. Es claro que $\sum\limits_{i\in I} M_i = \left\{\sum\limits_{i\in I} m_i \mid I \text{ es un conjunto finito}, m_i \in M_i, \forall i \in I\right\}$.
2. A partir de las inclusiones $\mathrm{inc}_j : M_j \to M$ y usando la propiedad universal de la suma directa, se tiene un (único) morfismo $\varphi : \bigoplus\limits_{i\in I} M_i \to \sum\limits_{i\in I} M_i$ tal que $\varphi \circ \iota_j = \mathrm{inc}_j$. Además φ resulta sobreyectivo. Notar que explícitamente $\varphi\left((m_i)_{i\in I}\right) = \sum_{i\in I} m_i$.
3. Si φ es inyectivo, la suma es isomorfa a la suma directa y se dice que *la suma es directa*. En este caso, cada $m \in \sum\limits_{i\in I} M_i$ se puede escribir de manera única como una suma finita de $m_i \in M_i$. De hecho, son equivalentes las siguientes afirmaciones para una familia $\{M_i\}_{i\in I}$ de submódulos de M.
   a) $\bigoplus\limits_{i\in I} M_i \cong \sum\limits_{i\in I} M_i$ via φ,
   b) Para cada $m \in \sum\limits_{i\in I} M_i$, existe una única familia $\{m_i \in M_i \mid i \in I\}$ de soporte finito tal que $m = \sum\limits_{i} m_i$,
   c) $M_i \cap \sum\limits_{j\neq i} M_j = \{0\}$ para todo $i \in I$.

   (La prueba es análoga a la que se hace para espacios vectoriales).

La noción de grupo cociente en grupos abelianos se extiende al contexto de A-módulos. En efecto, si $N \subseteq M$ es un submódulo, como en particular es un subgrupo, se tiene que $\frac{M}{N}$ es un grupo abeliano. El siguiente lema asegura que la acción de A induce una acción en el cociente.

Lema 3.1.3. *Sean M un A-módulo, $N \subseteq M$ un submódulo, $a \in A, m, m' \in M$. Si $m \equiv m' \pmod{N}$ entonces $am \equiv am' \pmod{N}$.*

Demostración. En efecto, si $m - m' \in N$, entonces $am - am' = a(m - m') \in N$ por ser N un submódulo. $\square$

A partir del lema, es claro que está bien definir la operación $\cdot : A \times \frac{M}{N} \to \frac{M}{N}$, $a \cdot \overline{m} = \overline{am}$. Se obtiene una estructura de A-módulo en el cociente $\frac{M}{N}$ y un epimorfismo de A-módulos $\pi_N : M \to \frac{M}{N}$, que verifican la siguiente propiedad universal:

Teorema 3.1.4 (Propiedad universal del cociente)**.** *Sea $f : M \to M'$ un morfismo de A-módulos y sea $N \subseteq M$ un submódulo. Si $N \subseteq \operatorname{Ker} f$, entonces existe un único morfismo $\hat{f} : \frac{M}{N} \to M'$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi_N"'] & M' \\ \frac{M}{N} \arrow[ur, dotted, "\hat{f}"'] & \end{tikzcd}$$

Además, se tiene $\operatorname{Im} \hat{f} = \operatorname{Im} f$ *y* $\operatorname{Ker} \hat{f} = \frac{\operatorname{Ker} f}{N}$.

Demostración. Sabemos que existe un único morfismo de grupos que hace conmutar el diagrama y verifica las condiciones en el núcleo y la imagen. Es inmediato verificar que dicho morfismo preserva la acción. $\square$

Al igual que en grupos abelianos, se deducen los siguientes resultados conocidos como *teoremas de isomorfismo.*

Corolario 3.1.5 (Teoremas de isomorfismo)**.** *Sea M un A-módulo.*

1. *Si $f : M \to N$ es un morfismo de A-módulos, entonces $\frac{M}{\operatorname{Ker} f} \cong \operatorname{Im} f$.*
2. *Si $H, K \subseteq M$ son submódulos, entonces $\frac{H+K}{H} \cong \frac{K}{H \cap K}$.*
3. *Si $H \subseteq K \subseteq M$ son dos a dos submódulos, entonces $\frac{M/H}{K/H} \cong \frac{M}{K}$.*
4. *Si $f : M \to N$ es un morfismo de A-módulos, y $H \subseteq M, K \subseteq N$ son submódulos con $f(H) \subseteq K$, entonces existe un único morfismo de A-módulos $\tilde{f} : \frac{M}{H} \to \frac{N}{K}$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi_H"'] & N \arrow[d, "\pi_K"] \\ \frac{M}{H} \arrow[r, dotted, "\tilde{f}"'] & \frac{N}{K} \end{tikzcd}$$

Demostración. Para 1, 2 y 3, ya sabemos que hay un isomorfismo de grupos. Basta verificar que preserva la acción. Para 4, ya sabemos que hay un tal morfismo de A-módulos. De nuevo, basta verificar que preserva la acción. $\square$

Teorema 3.1.6. *Sean M un módulo y $N \subseteq M$ un submódulo. Existe una correspondencia biyectiva entre los conjuntos:*

$$\mathcal{F}_1 = \left\{ L \subseteq \frac{M}{N} \text{ submódulo} \right\} \quad y \quad \mathcal{F}_2 = \{ K \subseteq M \text{ submódulo} \mid K \supseteq N \}$$

que preserva la inclusión.

Demostración. La prueba del resultado análogo para grupos puede adaptarse fácilmente a este contexto, usando la proposición 3.1.1. $\square$

3.2. Dependencia lineal en módulos

Definición 3.2.1. Sea M un A-módulo. Sea $S \subseteq M$ un subconjunto. Decimos que S es *linealmente dependiente* si existen $m_1, \dots, m_k \in S$ y $a_1, \dots, a_k \in A$ con algún $a_i \neq 0$ tales que $\sum_{i=1}^{k} a_i m_i = 0$. Una tal suma se denomina *combinación lineal* de $m_1, \dots, m_k$.

Decimos que S es *linealmente independiente* si no es linealmente dependiente.

Observación 3.2.1.

1. $S = \varnothing$ es linealmente independiente.
2. S es linealmente independiente si y sólo si para todo $m_1, \dots, m_k \in S$ y $a_1, \dots, a_k \in A$ tales que $\sum_{i=1}^{k} a_i m_i = 0$ se tiene que $a_i = 0$ para todo $i = 1, \dots, n$. Es decir, si la única combinación lineal nula es la trivial.
3. Si $S = \{m_1, \dots, m_k\} \subset M$ es tal un m_i es combinación lineal de los otros, entonces S es linealmente dependiente. El recíproco, válido si M es un espacio vectorial (o más en general, si A es un anillo con división), no es cierto en general.

   En efecto, tomemos $A = \mathbb{Z}, M = \mathbb{Z}$ con la acción regular, y $p, q \in \mathbb{Z}$ coprimos, con $p, q \geqslant 2$. Entonces $qp + (-p)q = 0$ es una combinación lineal no trivial de p y q, luego $\{p, q\}$ es linealmente dependiente. Sin embargo $p \notin q\mathbb{Z}$ y $q \notin p\mathbb{Z}$.

Definición 3.2.2. Sea M un A-módulo, y $\mathcal{B} \subseteq M$ un subconjunto. Decimos que $\mathcal{B}$ es una *base* de M si es linealmente independiente y generador de M. Si M admite una base, diremos que es un módulo *libre*.

Observación 3.2.2. Sea $\varphi : M \to N$ un mapa A-lineal. Es fácil probar (y es la misma prueba de álgebra lineal) que si φ es sobreyectiva entonces lleva generadores en generadores y que si φ es inyectiva entonces lleva conjuntos linealmente independientes en conjuntos linealmente independientes.

En particular, un isomorfismo lleva bases en bases, y por lo tanto "ser libre" es invariante bajo isomorfismos.

Ejemplos 3.2.1.

1. Si $M = V$ es un espacio vectorial sobre un cuerpo $\Bbbk$, entonces M es libre.
2. El conjunto $\mathcal{B} = \{1, x, x^2, \dots\}$ es base de $A[x]$ como A-módulo.
3. Sea $n \geqslant 2$: consideremos $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo. Sea $S = \{\overline{a}\} \subset \mathbb{Z}_n$. Tenemos que $n\overline{a} = \overline{na} = \overline{0}$ con $n \neq 0$, luego $\{S\}$ no es linealmente independiente. En particular, $\mathbb{Z}_n$ no admite ninguna base.
4. Todo anillo como módulo sobre sí mismo es libre, con base $\{1\}$.
5. En particular, $\mathbb{Z}_n$ es libre como $\mathbb{Z}_n$-módulo, pero no lo es como $\mathbb{Z}$-módulo (ejemplo 3.2.13).
6. A^n es libre para todo $n \in \mathbb{N}$.
7. $\mathbb{Z}_3 \simeq N = \{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbb{Z}_6$ es un $\mathbb{Z}_6$-submódulo que no es libre (de hecho, $N = \langle \overline{2} \rangle$).
8. $\mathbb{Z}$ como $\mathbb{Z}$-módulo: $\{1\}$ es base, y $\{2\}$ (que tiene el mismo cardinal) es linealmente independiente pero no es base, y tampoco se puede completar a una base. También: $\{2, 3\}$ es un generador que no está contenido en una base ni contiene a una.

Definición 3.2.3. Sea M un A-módulo. Definimos:

$$\mu(M) := \inf\{\#S : S \subset M, M = \langle S \rangle\}$$

Observación 3.2.3. $\mu(M) < \infty \iff M$ es finitamente generado.

Ejemplo 3.2.1. Sea $\Bbbk$ un cuerpo, y $A = M = \Bbbk[x_1, \dots, x_n, \dots]$ el anillo de polinomios en infinitas variables con coeficientes en $\Bbbk$, considerado como módulo sobre sí mismo con la acción regular. Tenemos $M = \{1\}$, luego $\mu(M) = 1$. Sin embargo, el ideal $I = (x_1, \dots, x_n, \dots)$ es un submódulo de M tal que $\mu(I) = \infty$.

Este ejemplo muestra que un submódulo de un módulo finitamente generado puede no ser finitamente generado.

La siguiente proposición muestra un resultado afirmativo en el mismo sentido.

Proposición 3.2.1. *Sea M un A-módulo y $N \subseteq M$ un submódulo. Se tiene:*

1. $\mu(M) < \infty \Rightarrow \mu(M/N) < \infty$
2. $\mu(N) < \infty$ *y* $\mu(M/N) < \infty \Rightarrow \mu(M) < \infty$. *Además* $\mu(M) \leqslant \mu(N) + \mu(M/N)$.

Demostración.

1. Consideremos el morfismo sobreyectivo $\pi : M \to M/N$. Si $M = \langle m_1, \dots, m_k \rangle$, entonces por la observación 3.2.2, se tiene que $M/N = \langle \pi(m_1), \dots, \pi(m_k) \rangle$.
2. Basta probar que existe un generador de M con $\mu(N)+\mu(M/N)$ elementos. Sea $\{n_1, \dots, n_k\}$ un generador de N con $\mu(N)$ elementos, y $\{\pi(m_1), \dots, \pi(m_r)\}$ un generador de M/N con $\mu(M/N)$ elementos. Veamos que $X = \{n_1, \dots, n_k, m_1, \dots, m_r\}$ es un generador de M. Sea $m \in M$.
$$\pi(m) = \sum_{j=1}^{r} b_j \pi(m_j) = \pi\left(\sum_{j=1}^{r} b_j m_j\right) \Rightarrow \pi\left(m - \sum_{j=1}^{r} b_j m_j\right) = 0$$
para ciertos $b_j \in A$, de donde $m - \sum_{j=1}^{r} b_j m_j \in \ker \pi = N$. Por lo tanto
$$m - \sum_{j=1}^{r} b_j m_j = \sum_{i=1}^{k} a_i n_i \Rightarrow m = \sum_{j=1}^{r} b_j m_j + \sum_{i=1}^{k} a_i n_i$$
para ciertos $a_i \in A$, y por lo tanto $m \in \langle X \rangle$. □

Definición 3.2.4. Sea M un A-módulo, $S \subset M$ un subconjunto. El *anulador* de S es

$$\operatorname{Ann}(S) := \{a \in A : as = 0 \quad \forall s \in S\}$$

Si $S = \{m_1, \dots, m_k\}$ escribiremos $\operatorname{Ann}(S) = \operatorname{Ann}(m_1, \dots, m_k)$.

Observación 3.2.4. Sea $S = \{m\}$, para algún $m \in M$. Tenemos un morfismo $\varphi : A \to M$, $a \mapsto am$. Se tiene que $\operatorname{Im} \varphi = Am$ y $\ker \varphi = \operatorname{Ann}(m)$. Por lo tanto $A/\operatorname{Ann}(m) \cong Am$.

Observar además que $\{m\}$ es linealmente independiente si y sólo si $\operatorname{Ann}(m) = \{0\}$.

Observación 3.2.5. Sea $S = \{m_i\}_{i \in I} \subset M$ un subconjunto linealmente independiente. Entonces $\langle S \rangle = \bigoplus_{i \in I} Am_i$. En efecto, por definición, $\langle S \rangle = \sum_{i \in I} Am_i$. Además la suma es directa, pues si $x_1 + \cdots + x_k = 0$ con $x_i \in Am_i$, entonces $x_i = a_i m_i$ para ciertos a_i. Resulta $a_1 m_1 + \cdots + a_k m_k = 0$; de la independencia lineal de S se deduce que $a_i = 0$ para todo i, y por lo tanto $x_i = 0$ para todo i.

Teorema 3.2.2. *Sea M un A-módulo. Son equivalentes:*

1. *M es libre,*

2. *Existe $\mathcal{B} \subset M$ tal que $M = \bigoplus_{m \in \mathcal{B}} Am$ (suma directa interna) con $Am \cong A$ para todo $m \in \mathcal{B}$,*

3. *Existe una familia $\mathcal{F}$ tal que $M \cong \bigoplus_{i \in \mathcal{F}} A_i$ con $A_i = A$ para todo $i \in \mathcal{F}$.*

Demostración. ($1 \Rightarrow 2$) Sea $\mathcal{B}$ base de M. Entonces $M = \langle \mathcal{B} \rangle = \bigoplus_{m \in \mathcal{B}} Am$ en virtud de la observación 3.2.5. Ahora, como $\mathcal{B}$ es linealmente independiente, $\mathrm{Ann}(m) = \{0\}$ para todo $m \in B$, y por lo tanto $A \cong A/\mathrm{Ann}(m) \cong Am$ en virtud de la observación 3.2.4.

($2 \Rightarrow 3$) Obvio.

($3 \Rightarrow 1$) La imagen en M de la base canónica de $\bigoplus_{i \in \mathcal{F}} A$ es una base de M. □

La siguiente proposición, como en espacios vectoriales, muestra que para definir una transformación lineal desde un módulo libre, basta definirla en una base.

Proposición 3.2.3 (Propiedad universal del módulo libre)**.** *Sea M un A-módulo libre con base $\mathcal{B} \subseteq M$, y N un A-módulo. Si $f : \mathcal{B} \to N$ es una función, entonces existe un único morfismo de A-módulos $\varphi : M \to N$ tal que $\varphi|_{\mathcal{B}} = f$, i.e. que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} \mathcal{B} \arrow[r, "f"] \arrow[d, hook] & N \\ M \arrow[ur, dotted, "\varphi"'] & \end{tikzcd}$$

Demostración. Sabemos que $M = \bigoplus_{m \in \mathcal{B}} Am$. La función f induce morfismos de A-módulos $Am \to N$, $am \mapsto af(m)$. Por la propiedad universal de la suma directa, existe una única φ como la que buscamos. □

Proposición 3.2.4. *Sea M un A-módulo libre con base $\mathcal{B} \subseteq M$. Si M es finitamente generado, entonces $\#\mathcal{B} < \infty$.*

Demostración. Como M es finitamente generado, existen $m_1, \ldots, m_k \in M$ tales que $M = \langle m_1, \ldots, m_k \rangle$. Cada m_i es combinación lineal de un número finito de elementos de $\mathcal{B}$, entonces existen $e_1, \ldots, e_r \in \mathcal{B}$ tales que $m_i \in \langle e_1, \ldots, e_r \rangle$ para todo $i = 1, \ldots, k$.

Por lo tanto $M = \langle m_1, \ldots, m_k \rangle \subset \langle e_1, \ldots, e_r \rangle$, luego $\mathcal{B} = \{e_1, \ldots, e_r\}$, pues $\mathcal{B}$ es linealmente independiente. En efecto, si existiera $e_{r+1} \in \mathcal{B}$ distinto de los anteriores, entonces se escribiría como combinación lineal de $\{e_1, \ldots, e_r\}$, contradiciendo la independencia lineal de $\mathcal{B}$. □

Teorema 3.2.5. *Sea M un A-módulo libre que admite una base $\mathcal{B}$ infinita. Entonces toda base de M es infinita.*

Demostración. Supongamos que $\mathcal{C}$ es una base finita de M. Alcanzan finitos elementos de $\mathcal{B}$ para generar cada uno de los elementos de $\mathcal{C}$, y por lo tanto alcanza con un subconjunto finito $\mathcal{B}' \subseteq \mathcal{B}$ para generar $\mathcal{C}$. Se deduce que $\mathcal{B}' \subseteq \mathcal{B}$ es un generador finito de M. Como $\mathcal{B}$ es infinito, existe $x \in \mathcal{B} \backslash \mathcal{B}'$. Pero x está generado por $\mathcal{B}'$, de donde el conjunto $\mathcal{B}' \cup \{x\}$ es linealmente dependiente y está incluido en $\mathcal{B}$, lo que contradice que $\mathcal{B}$ sea base. □

Observación 3.2.6. El lector familiarizado con la teoría de conjuntos y cardinales podrá observar que la prueba de arriba puede extenderse para deducir el siguiente resultado, más fuerte que el teorema 3.2.5:

Sea M un A-módulo libre que admite una base $\mathcal{B}$ de cardinal infinito. Entonces toda base de M tiene cardinal $\#\mathcal{B}$.

Corolario 3.2.6. *Sea A un anillo con división y M un A-módulo. Entonces todas las bases de M tienen el mismo cardinal.*

Demostración. Observar primero que si A es un anillo con división, todo A-módulo es libre. Además, son equivalentes:

1. $\mathcal{B}$ es un conjunto linealmente independiente maximal,
2. $\mathcal{B}$ es un conjunto generador minimal,
3. $\mathcal{B}$ es base.

En efecto, analizando la demostración de este teorema hecha para espacios vectoriales en el curso de álgebra lineal se observa que la hipótesis de conmutatividad es superflua.
Sea $\mathcal{B}$ base de M. Si $\#\mathcal{B} = \infty$, el resultado se sigue del teorema. Si $\#\mathcal{B} < \infty$, la demostración es la misma del curso de álgebra lineal: si $S \subseteq M$ es generador, se prueba que $\#S \geqslant \#\mathcal{B}$. ☐

Definición 3.2.5. Un anillo A tiene *número de base invariante*, abreviado NBI, si para todo A-módulo libre M, dos bases de M tienen el mismo cardinal.

Si A tiene NBI y M es un A-módulo libre, el *rango* de M es $\operatorname{rg} M := \#\mathcal{B}$ para alguna base $\mathcal{B}$ de M.

Ejemplos 3.2.2.

1. El corolario 3.2.6 afirma que todo anillo con división tiene NBI.
2. $\operatorname{rg}(A^n) = n$.

Observación 3.2.7. Dado un anillo A, para verificar si tiene NBI basta hacerlo en módulos libres que no admiten bases infinitas, en virtud de la observación 3.2.6. Por lo tanto, A tiene NBI si y sólo si cada vez que $A^n \cong A^m$ se tiene $n = m$.

Nos dirigimos a probar que todo anillo conmutativo tiene NBI. Para ello, probamos primero un

Lema 3.2.7. *Sean A un anillo conmutativo e I un ideal de A. Si M es un A-módulo libre de base $\mathcal{B} = \{m_i\}_{i\in I}$, entonces M/IM es un A/I-módulo libre de base $\overline{\mathcal{B}} = \{\overline{m_i}\}_{i\in I}$.*

Demostración. El ejercicio 10 del práctico 6 nos da que $IM = \left\{ \sum_{i=1}^{n} a_i n_i \mid a_i \in I, n_i \in M, n \in \mathbb{Z}^+ \right\}$ es un submódulo de M, y que M/IM es un A/I-módulo, con la acción $\overline{a} \cdot \overline{m} = \overline{am}$.

Veamos que $\overline{\mathcal{B}}$ es generador:[3] dado $\overline{m} \in M/IM$, como $m \in M$ se tiene $m = \sum_{i\in I} a_i m_i$ para ciertos $a_i \in A$ nulos salvo una cantidad finita. Entonces:

$$\overline{m} = \overline{\sum_{i\in I} a_i m_i} = \sum_{i\in I} \overline{a_i}\, \overline{m_i}$$

[3] No podemos decir que sea generador al ser $\pi(\mathcal{B})$ y ser $\mathcal{B}$ una base, pues $\pi : M \to M/IM$ sólo es un morfismo de grupos abelianos: M es un A-módulo mientras que M/IM es un A/I-módulo.

Veamos ahora que $\overline{\mathcal{B}}$ es linealmente independiente: sea $\sum\limits_{i \in I} \overline{a_i}\ \overline{m_i} = \overline{0}$ en M/IM, donde $\overline{a_i} \in A/I$ son nulos salvo una cantidad finita. Entonces:

$$\overline{\sum_{i\in I} a_i m_i} = \overline{0} \Rightarrow \sum_{i\in I} a_i m_i \in IM \Rightarrow \sum_{i\in I} a_i m_i = \sum_{j=1}^{r} b_j x_j = \sum_{j=1}^{r} b_j \sum_{n\in I} c_{jn} m_n$$

para ciertos $b_j \in I, x_j \in M$; y $c_{jn} \in A$ nulos salvo una cantidad finita. Por lo tanto,

$$\sum_{i\in I} a_i m_i = \sum_{n\in I} \overbrace{\left(\sum_{j=1}^{r} b_j c_{jn}\right)}^{\alpha_n \in I} m_n \Rightarrow \sum_{i\in I} (a_i - \alpha_i) m_i = 0$$

Como B es linealmente independiente, entonces $a_i = \alpha_i \in I$ para todo i, luego $\overline{a_i} = \overline{0}$ en A/I, para todo i. $\square$

Teorema 3.2.8. *Todo anillo conmutativo tiene NBI.*

Demostración. Consideremos I ideal maximal en un anillo conmutativo A. Al ser A conmutativo, resulta A/I un cuerpo, luego M/IM es un A/I-espacio vectorial, de donde todas sus bases tienen el mismo cardinal. Basta probar entonces que toda A-base de M tiene el mismo cardinal que una A/I-base de M/IM, que es lo que probamos en el lema previo. $\square$

3.3. Sucesiones exactas cortas

Durante todo el capítulo A denotará un anillo cualquiera.

Definición 3.3.1. Sean M_1, M_2, M_3 A-módulos, φ_1, φ_2 morfismos de A-módulos. Decimos que $0 \longrightarrow M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0$ es una sucesión exacta corta (de A-módulos) si y sólo si se cumplen las siguientes condiciones:

- φ_1 es un monomorfismo,
- φ_2 es un epimorfismo,
- $\mathrm{Im}\ \varphi_1 = \mathrm{Ker}\,\varphi_2$.

Ejemplos 3.3.1. 1. Dados M un A-módulo y $N \subset M$ un submódulo,

$$0 \longrightarrow N \hookrightarrow M \xrightarrow{\pi} M/N \longrightarrow 0$$

es una sucesión exacta corta.

2. Más en general, si $\varphi : M_1 \to M_2$ es un morfismo de A-módulos, entonces

$$0 \longrightarrow \mathrm{Ker}\,\varphi \hookrightarrow M_1 \xrightarrow{\varphi} \mathrm{Im}\ \varphi \longrightarrow 0$$

es una sucesión exacta corta.

3. Sean M_1, M_2 dos A-módulos y $\iota : M_1 \to M_1 \oplus M_2$, $p : M_1 \oplus M_2 \to M_2$ la inyección y la proyección canónica respectivamente. Entonces

$$0 \longrightarrow M_1 \xrightarrow{\iota} M_1 \oplus M_2 \xrightarrow{p} M_2 \longrightarrow 0$$

es una sucesión exacta corta.

Lema 3.3.1 (Lema de los tres). [4] *Consideremos el siguiente diagrama conmutativo cuyas filas son sucesiones exactas cortas:*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & N \arrow[r, "\psi"] \arrow[d, "\beta"'] & P \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & M' \arrow[r, "\varphi'"] & N' \arrow[r, "\psi'"] & P' \arrow[r] & 0
\end{tikzcd}$$

1. Si α y γ son inyectivas, entonces β es inyectiva.

2. Si α y γ son sobreyectivas, entonces β es sobreyectiva.

3. Si α y γ son isomorfismos, entonces β es un isomorfismo.

Demostración. [5]

1. Sea $n \in N$ tal que $\beta(n) = 0$.
$$0 = \psi'(\beta(n)) = \gamma(\psi(n))$$
por conmutatividad del cuadrado derecho. Luego $\psi(n) = 0$ pues γ es inyectiva. Entonces $n \in \operatorname{Ker}\psi = \operatorname{Im}\varphi$ por exactitud de la fila de arriba. Por lo tanto existe $m \in M$ tal que $\varphi(m) = n$.
$$0 = \beta(n) = \beta(\varphi(m)) = \varphi'(\alpha(m))$$
por conmutatividad del cuadrado izquierdo. Luego $\alpha(m) = 0$ pues φ' es inyectiva. Entonces $m = 0$ pues α es inyectiva, de donde $\varphi(m) = n = 0$. En conclusión, β es inyectiva.

2. Sea $n' \in N'$. Se tiene que $\psi'(n') \in P'$, luego como γ es sobreyectiva, existe $p \in P$ tal que $\gamma(p) = \psi'(n')$. Como ψ es sobreyectiva, existe $n \in N$ tal que $\psi(n) = p$. Considero $\beta(n) - n'$:
$$\psi'(\beta(n) - n') = \psi'(\beta(n)) - \psi'(n') = \gamma(\psi(n)) - \psi'(n') = \gamma(p) - \psi'(n') = 0$$
por conmutatividad del cuadrado derecho. Entonces $\beta(n) - n' \in \operatorname{Ker}\psi' = \operatorname{Im}\varphi'$ por exactitud de la fila de abajo. Por lo tanto existe $m' \in M'$ tal que $\varphi'(m') = \beta(n) - n'$. Como α es sobre, existe $m \in M$ tal que $\alpha(m) = m'$.
$$\beta(\varphi(m)) = \varphi'(\alpha(m)) = \varphi'(m') = \beta(n) - n'$$
por conmutatividad del cuadrado izquierdo, luego $n' = \beta(n - \varphi(m))$, y $n' \in \operatorname{Im}\beta$. En conclusión, β es sobreyectiva.

3. Es consecuencia directa de las dos partes anteriores. ☐

Definición 3.3.2.
- Dos sucesiones exactas cortas $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ y $0 \longrightarrow M' \xrightarrow{\varphi'} N' \xrightarrow{\psi'} P' \longrightarrow 0$ son *isomorfas* si existe un diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varphi"] \arrow[d, "\alpha"'] & N \arrow[r, "\psi"] \arrow[d, "\beta"'] & P \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & M' \arrow[r, "\varphi'"] & N' \arrow[r, "\psi'"] & P' \arrow[r] & 0
\end{tikzcd}$$

con α, β y γ isomorfismos.

[4] Este lema se generaliza al que se conoce como *lema de los cinco*.
[5] Esta demostración es un ejemplo arquetípico de *diagram chasing*.

- Dos sucesiones exactas cortas $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ y $0 \longrightarrow M \xrightarrow{\varphi'} N' \xrightarrow{\psi'} P \longrightarrow 0$ son *equivalentes* si existe un isomorfismo $\beta : N \to N'$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}_M"'] & N \arrow[r, "\psi"] \arrow[d, "\beta"'] & P \arrow[r] \arrow[d, "\mathrm{id}_P"'] & 0 \\
0 \arrow[r] & M \arrow[r, "\varphi'"] & N' \arrow[r, "\psi'"] & P \arrow[r] & 0
\end{tikzcd}$$

Observación 3.3.1. Toda sucesión exacta corta $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ es isomorfa a una como la del ejemplo 3.3.1.1: en efecto,

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varphi"] \arrow[d, "\cong"'] & N \arrow[r, "\psi"] \arrow[d, "="'] & P \arrow[r] \arrow[d, "\cong"'] & 0 \\
0 \arrow[r] & \mathrm{Im}\ \varphi \arrow[r, hook] & N \arrow[r, "\pi"] & N/\mathrm{Im}\ \varphi \arrow[r] & 0
\end{tikzcd}$$

Proposición 3.3.2. *Consideremos una sucesión exacta corta* $E :\ 0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$. *Son equivalentes:*

1. *Existe un morfismo* $\nu : P \to N$ *tal que* $\psi \circ \nu = \mathrm{id}_P$, $\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\varphi"] & N \arrow[r, "\psi"] & P \arrow[r] \arrow[l, dotted, bend left, "\nu"] & 0 \end{tikzcd}$

2. *Existe un morfismo* $\eta : N \to M$ *tal que* $\eta \circ \varphi = \mathrm{id}_M$, $\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\varphi"] & N \arrow[r, "\psi"] \arrow[l, dotted, bend left, "\eta"] & P \arrow[r] & 0 \end{tikzcd}$

3. *La sucesión* E *es equivalente a la sucesión exacta corta* $0 \longrightarrow M \xrightarrow{\iota_M} M \oplus P \xrightarrow{\pi_P} P \longrightarrow 0$. *Es decir, existe un isomorfismo* $\beta : N \to M \oplus P$ *que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}_M"'] & N \arrow[r, "\psi"] \arrow[d, "\beta"'] & P \arrow[r] \arrow[d, "\mathrm{id}_P"'] & 0 \\
0 \arrow[r] & M \arrow[r, "\iota_M"] & M \oplus P \arrow[r, "\pi_P"] & P \arrow[r] & 0
\end{tikzcd}$$

Demostración. ($1 \Rightarrow 3$) Tenemos $\nu : P \to N$ tal que $\psi \circ \nu = \mathrm{id}_P$. La propiedad universal de la suma directa nos dice que existe un único $\delta : M \oplus P \to N$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd}
M \arrow[r, "\iota_M"] \arrow[dr, "\varphi"'] & M \oplus P \arrow[d, dotted, "\delta"'] & P \arrow[l, "\iota_P"'] \arrow[dl, "\nu"] \\
& N &
\end{tikzcd}$$

En vista del lema 3.3.1, δ debe ser un isomorfismo. El isomorfismo β buscado es δ^{-1}.

($2 \Rightarrow 3$) Tenemos $\eta : N \to M$ tal que $\eta \circ \varphi = \mathrm{id}_M$. Como la suma directa y el producto directo coinciden para un conjunto de índices finito, podemos usar la propiedad universal del producto directo. Por lo tanto, existe una única $\beta : N \to M \oplus P$ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} M & M \oplus P \arrow[l, "\pi_M"'] \arrow[r, "\pi_P"] & P \\ & N \arrow[ul, "\eta"] \arrow[u, dotted, "\beta"] \arrow[ur, "\psi"'] & \end{tikzcd}$$

Por el lema 3.3.1, β es el isomorfismo buscado.

$(3 \Rightarrow 1)$ Sea $\nu = \beta^{-1} \circ \iota_P$. Entonces, por conmutatividad del cuadrado derecho:

$$\psi \circ \nu = \pi_P \circ \beta \circ \beta^{-1} \circ \iota_P = \pi_P \circ \iota_P = id_P$$

$(3 \Rightarrow 2)$ Sea $\nu = \pi_M \circ \beta$. Entonces, por conmutatividad del diagrama izquierdo,

$$\eta \circ \varphi = \pi_M \circ \beta \circ \varphi = \pi_M \circ \iota_M = id_M$$ □

Observación 3.3.2.

1. La condición 3 no sólo expresa que $N \cong M \oplus P$, sino que el isomorfismo hace conmutar dos cuadrados, lo cual es más fuerte (ver ejercicio 7 del práctico 7).

2. De la demostración de $(1 \Rightarrow 3)$ se desprende que, si $\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\varphi"] & N \arrow[r, "\psi"] & P \arrow[l, dotted, bend left, "\nu"] \arrow[r] & 0 \end{tikzcd}$ es una sucesión exacta corta que "se escinde via ν", entonces tenemos que el morfismo $\delta : M \oplus P \to N$ definido por $\delta(m, p) = \varphi(m) + \nu(p)$ es un isomorfismo. Además $\operatorname{Im} \varphi \oplus \operatorname{Im} \nu = N$, e $\operatorname{Im} \nu \cong P$.

   Análoga observación vale para la escisión via η.

Definición 3.3.3. Diremos que una sucesión exacta corta *se escinde* si satisface la proposición anterior.

Ejemplo 3.3.1. Toda sucesión exacta corta $E : \begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\varphi"] & N \arrow[r, "\psi"] & L \arrow[r] & 0 \end{tikzcd}$, con L libre se escinde. En efecto, alcanza con definir ν en una base de L y, usando la propiedad universal para módulos libres, extenderla a L.
En particular, toda sucesión exacta corta de espacios vectoriales se escinde.

3.4. Producto tensorial

3.4.1. Algo más sobre módulos libres

Definición 3.4.1. El *A-módulo libre generado por un conjunto S* es $L_A(S) = \bigoplus_{i \in S} A_i$ donde $A_i = A$ para todo $i \in S$, considerado como A-módulo con la acción regular. Explícitamente,

$$L_A(S) = \{f : S \to A : f \text{ función, } \operatorname{sop}(f) \text{ finito}\}$$

Observación 3.4.1.

1. Si A no es el anillo trivial y $s \in S$, la *función indicatriz de s* es $\chi_s(t) : S \to A$, definida como $\chi_s(t) = \begin{cases} 1 & \text{si } t = s \\ 0 & \text{si } t \neq s \end{cases}$. Observar que $\chi_s \in L_A(S)$ y que la función $S \to L_A(S)$, $s \mapsto \chi_s$ es inyectiva, luego podemos pensar $S \subset L_A(S)$.

2. Dado $f \in L_A(S)$, se tiene que $f = \sum_{i \in S} f(i)\chi_i = \sum_{i \in S} f(i)i$ donde en la última igualdad ya hicimos la identificación recién descrita.

   Esto muestra que S (formalmente, la copia de S en $L_A(S)$) es generador de $L_A(S)$ como A-módulo.

3. Además S es linealmente independiente:

$$\sum_{i=1}^{n} a_i \chi_i = 0 \iff \sum_{i=1}^{n} a_i \chi_i(j) = 0 \quad \forall j \in S \iff a_i = 0 \quad \forall i = 1, \dots, n$$

Por lo tanto $L_A(S)$ es un A-módulo libre con base S, justificando su denominación.

Corolario 3.4.1. *Todo A-módulo M es cociente de uno libre.*

Demostración. Sean M un A-módulo y $S \subseteq M$ un generador de M (por ejemplo $S = M$). Entonces por la propiedad universal del A-módulo libre con base S, existe una única φ que hace conmutar el siguiente diagrama:

$$\begin{tikzcd} S \arrow[r, hook, "\text{inc}"] \arrow[d, hook] & M \\ L_A(S) \arrow[ur, dotted, "\varphi"'] & \end{tikzcd}$$

Es decir, $\varphi(s) = s$ para todo $s \in S$. Se tiene que φ es sobreyectiva, pues dado $m \in M$,

$$m = \sum_{i=1}^{k} a_i s_i = \sum_{i=1}^{k} a_i \varphi(s_i) = \varphi\left(\sum_{i=1}^{k} a_i s_i\right)$$

Por lo tanto $M \simeq \frac{L_A(S)}{\ker \varphi}$. □

3.4.2. Producto tensorial

El producto tensorial es una construcción que permite llevar el álgebra multilineal al contexto lineal. Más en concreto, el producto tensorial de A-módulos permite pensar funciones A-bilineales (y más en general A-multilineales) como funciones A-lineales (es decir, como morfismos de A-módulos).

Asumiremos para el resto del capítulo que A es conmutativo.

Definición 3.4.2. Sean A un anillo conmutativo, M y N dos A-módulos. El *producto tensorial* entre M y N se define como el A-módulo

$$M \otimes_A N := \frac{L_A(M \times N)}{T}$$

donde T es el submódulo de $L_A(M \times N)$ generado por los elementos

1) $(am, n) - a(m, n)$,

2) $(m, an) - a(m, n)$,

3) $(m, n) + (m, n') - (m, n + n')$,

4) $(m, n) + (m', n) - (m + m', n)$,

donde $m, m' \in M, n, n' \in N, a \in A$.

Notamos $m \otimes n$ a la clase de (m, n) y llamamos a estos elementos *tensores elementales*. Además, definimos $\theta : M \times N \to M \otimes_A N$ como $\theta(m, n) := m \otimes n$ para todo $m \in M$, $n \in N$. Es decir, θ es la composición $M \times N \hookrightarrow L_A(M \times N) \xrightarrow{\pi} M \otimes_A N$.

Observación 3.4.2. 1. Todo elemento de $M \otimes_A N$ es *suma* finita de tensores elementales: en efecto, si $x \in M \otimes_A N$, entonces:

$$x = \pi\left(\sum_{i,j=1}^{r,s} a_{ij}(m_i, n_j)\right) = \pi\left(\sum_{i,j=1}^{r,s} a_{ij}\iota(m_i, n_j)\right) = \sum_{i,j=1}^{r,s} a_{ij}\theta(m_i, n_j)$$

$$\overset{1)}{=} \sum_{j=1}^{s}\sum_{i=1}^{r} a_{ij} m_i \otimes n_j \overset{4)}{=} \sum_{j=1}^{s} \overbrace{\left(\sum_{i=1}^{r} a_{ij} m_i\right)}^{:=m'_i \in M} \otimes n_j = \sum_{j=1}^{s} m'_j \otimes n_j$$

En particular, si $\varphi, \psi : M \otimes_A N \to U$ son morfismos de A-módulos, entonces se cumple que $\varphi = \psi$ si y sólo si $\varphi(m \otimes n) = \psi(m \otimes n)$ para todo $m \in M, n \in N$.

2. No es cierto que todo elemento de $M \otimes_A N$ sea de la forma $m \otimes n$.

3. Los tensores elementales no son linealmente independientes. En efecto, se tiene por ejemplo $m \otimes n + m \otimes n' = m \otimes (n + n')$.

4. $0_M \otimes n = 0_{M \otimes_A N} = m \otimes 0_N$ para todo $m \in M, n \in N$.

5. El submódulo T puede ser muy grande; más aún, puede ser todo $L_A(M \times N)$ como muestra el siguiente ejemplo:
$$\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 = \{0\}$$
En efecto, $\bar{1} \otimes \hat{1} = \bar{1} \otimes (4 \cdot \hat{1}) = 4 \cdot (\bar{1} \otimes \hat{1}) = (4 \cdot \bar{1}) \otimes \hat{1} = \bar{0} \otimes \hat{1} = 0$, y por lo tanto $\bar{m} \otimes \hat{n} = (m \cdot \bar{1}) \otimes (n \cdot \hat{1}) = mn \cdot (\bar{1} \otimes \hat{1}) = 0$ para todo $\bar{m} \in \mathbb{Z}_2, \hat{n} \in \mathbb{Z}_3$.

6. La noción de producto tensorial puede generalizarse a anillos no conmutativos, pero se hace en el contexto en que M es un A-módulo a derecha y N es un A-módulo a izquierda. En este caso el producto tensorial resulta apenas un grupo abeliano, a menos que M o N tengan más estructura.

Definición 3.4.3. Sean A un anillo, M, N, U tres A-módulos y $b : M \times N \to U$ una función. Decimos que b es *A-bilineal* si es lineal en cada variable; es decir, si se verifican las siguientes condiciones:

- $b(am + m', n) = ab(m, n) + b(m', n)$,
- $b(m, an + n') = ab(m, n) + b(m, n')$,

para todo $m, m' \in M, n, n' \in N, a \in A$.

A continuación vemos la propiedad universal del producto tensorial. Informalmente, ésta dice que para definir un mapa A-lineal $M \otimes_A N \to U$, basta definir un mapa A-bilineal $M \times N \to U$. Como siempre, no es difícil probar que la propiedad universal caracteriza al objeto a menos de isomorfismo. Por lo tanto, es práctico cuando se trata con el producto tensorial usar siempre su propiedad universal, no apelando por lo general a su definición, que si bien es natural, puede ser un poco enrevesada para manipular.

Teorema 3.4.2 (Propiedad universal del producto tensorial)**.** *Sean A un anillo conmutativo y M, N, U tres A-módulos. Para cada función A-bilineal $b : M \times N \to U$ existe un único morfismo de A-módulos $\tilde{b} : M \otimes_A N \to U$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd} M \times N \arrow[r, "b"] \arrow[d, "\theta"'] & U \\ M \otimes_A N \arrow[ur, dotted, "\tilde{b}"'] & \end{tikzcd}$$

Demostración. Llamemos $\iota : M \times N \to L_A(M \times N)$ a la inclusión. Por la propiedad universal de los módulos libres, existe $b_1 : L_A(M \times N) \to U$ tal que $b_1(m, n) = b(m, n)$ para todo $m \in M, n \in N$, es decir $b_1 \circ \iota = b$.

Ahora bien, es fácil ver que las condiciones de bilinealidad de b implican que $T \subseteq \operatorname{Ker} b_1$ y por tanto, por la propiedad universal del cociente, b_1 induce un morfismo de A-módulos $\tilde{b} : M \otimes_A N \to U$ tal que $\tilde{b} \circ \pi = b_1$.

$$\begin{tikzcd}
M \times N \arrow[r, "b"] \arrow[d, hook, "\iota"] \arrow[dd, bend right=60, "\theta"'] & U \\
L_A(M \times N) \arrow[ur, "b_1"] \arrow[d, "\pi"'] & \\
M \otimes_A N \arrow[uur, dotted, "\tilde{b}"'] &
\end{tikzcd}$$

Observando que, por construcción, $\tilde{b} \circ \theta = \tilde{b} \circ \pi \circ \iota = b_1 \circ \iota = b$, se tiene que $\tilde{b}$ es el morfismo buscado.

Para ver la unicidad: si existe $h : M \otimes_A N \to U$ tal que $h \circ \theta = b$, entonces como cualquier elemento de $M \otimes_A N$ es suma de tensores elementales,

$$h\left(\sum_{i=1}^{r} m_i \otimes n_i\right) = \sum_{i=1}^{r} h(m_i \otimes n_i) = \sum_{i=1}^{r} b(m_i, n_i)$$

de donde h está unívocamente determinada por b. $\square$

La siguiente proposición es una aplicación de la propiedad universal que permite generar algo que podríamos llamar (y formalmente así se llama) *productos tensoriales de morfismos de A-módulos.*

Proposición 3.4.3. *Sean $\varphi : M \to N, \psi : P \to Q$ morfismos de A-módulos. Existe un único morfismo $\varphi \otimes \psi : M \otimes_A P \to N \otimes_A Q$ que hace conmutar el siguiente diagrama:*

$$\begin{tikzcd}
M \times P \arrow[r, "\varphi \times \psi"] \arrow[d, "\theta_1"'] & N \times Q \arrow[d, "\theta_2"] \\
M \otimes_A P \arrow[r, dotted, "\varphi \otimes \psi"] & N \otimes_A Q
\end{tikzcd}$$

donde $\varphi \times \psi : M \times P \to N \times Q$ se define como $\varphi \times \psi(m, p) = (\varphi(m), \psi(p))$ para todo $m \in M, p \in P$.

Demostración. Queda a cargo del lector probar que $\theta_2 \circ (\varphi \times \psi) : M \times P \to N \otimes_A Q$ es A-bilineal. El resultado se deduce entonces de la propiedad universal del producto tensorial. La función resultante queda definida por $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n), \forall m \in M, n \in N$. $\square$

Observación 3.4.3. No es difícil verificar que esta operación cumple las siguientes propiedades:

- $\mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes_A N}$,
- Dados f, g, f', g' morfismos de A-módulos como abajo, el diagrama de la derecha conmuta:

$$\begin{tikzcd}
M \arrow[d, "f"'] & M' \arrow[d, "f'"'] & M \otimes_A M' \arrow[d, "f \otimes f'"'] \arrow[dd, bend left=60, "(g \circ f) \otimes (g' \circ f')"] \\
N \arrow[d, "g"'] & N' \arrow[d, "g'"'] & N \otimes_A N' \arrow[d, "g \otimes g'"'] \\
P & P' & P \otimes_A P'
\end{tikzcd}$$

La siguiente proposición lista propiedades "buenas" del producto tensorial; afirma que es esencialmente (a menos de isomorfismos) asociativo, conmutativo, que tiene neutro y que es distributivo respecto de la suma directa.

Proposición 3.4.4. *Sean A un anillo conmutativo y M, N, P A-módulos. Entonces*

1. $(M \otimes_A N) \otimes_A P \cong M \otimes_A (N \otimes_A P)$,
2. $M \otimes_A N \cong N \otimes_A M$,
3. $M \otimes_A A \cong A \otimes_A M \cong M$,
4. $M \otimes_A (N \oplus P) \cong (M \otimes_A N) \oplus (M \otimes_A P)$.

Demostración. La estrategia para probar estos isomorfismos es siempre la misma: construir con la propiedad universal un morfismo, y análogamente se construye un morfismo en el otro sentido que resulta ser su inversa.

1. Para cada $p \in P$, la función $F_p : M \times N \to M \otimes_A (N \otimes_A P)$ definida por $F_p(m, n) = m \otimes (n \otimes p)$ es A-bilineal y por lo tanto induce un morfismo de A-módulos, $\hat{F}_p : M \otimes_A N \to M \otimes_A (N \otimes_A P)$ de A-módulos.

   Por otra parte, la función $F : (M \otimes_A N) \times P \to M \otimes_A (N \otimes_A P)$ definida como $F(m \otimes n, p) = \hat{F}_p(m \otimes n)$ es A-bilineal y por lo tanto induce un morfismo de A-módulos $\tilde{F} : (M \otimes_A N) \otimes_A P \to M \otimes_A (N \otimes_A P)$ que resulta ser un isomorfismo (su inversa se define análogamente).

$$\begin{tikzcd} (M \otimes_A N) \times P \arrow[r, "F"] \arrow[d, "\theta"'] & M \otimes_A (N \otimes_A P) \\ (M \otimes_A N) \otimes_A P \arrow[ur, dotted, "\tilde{F}"'] & \end{tikzcd}$$

   Observar que es $\tilde{F}((m \otimes n) \otimes p) = m \otimes (n \otimes p)$.

2. La función $\tau : M \times N \to N \otimes_A M$ definida por $\tau(m, n) = n \otimes m$ es A-bilineal y por tanto induce un morfismo $\tilde{\tau} : M \otimes_A N \to N \otimes_A M$ de A-módulos que resulta ser un isomorfismo (su inversa se define análogamente).

   Observar que es $\tilde{\tau}(m \otimes n) = n \otimes m$.

3. La función $b : M \times A \to M$, definida por $b(m, a) = am$ es A-bilineal y por tanto induce un morfismo $\tilde{b} : M \otimes_A A \to M$ de A-módulos que resulta ser un isomorfismo (con inversa que lleva $m \in M$ en $m \otimes 1_A$).

   Observar que es $\tilde{b}(m \otimes a) = am$.

4. La función $f : M \times (N \oplus P) \to (M \otimes_A N) \oplus (M \otimes_A P)$, $f(m, n + p) = (m, n) + (m, p)$ es A-bilineal y por tanto induce un morfismo $\tilde{f} : M \otimes_A (N \oplus P) \to (M \otimes_A N) \oplus (M \otimes_A P)$ de A-módulos.

   Observar que es $\tilde{f}(m \otimes (n, p)) = (m \otimes n, m \otimes p)$.

   Por otro lado, las funciones $g_1 : M \times N \to M \otimes_A (N \oplus P)$ y $g_2 : M \times P \to M \otimes_A (N \oplus P)$ definidas por $g_1(m, n) = m \otimes n$, $g_2(m, p) = m \otimes p$ son A-bilineales y por tanto inducen morfismos $\hat{g}_1 : M \otimes_A N \to M \otimes_A (N \oplus P)$ y $\hat{g}_2 : M \otimes_A P \to M \otimes_A (N \oplus P)$ de A-módulos.

A partir de éstos se construye, con la propiedad universal de la suma directa, un morfismo de A-módulos $G : (M \otimes_A N) \oplus (M \otimes_A P) \to M \otimes_A (N \oplus P)$ que resulta ser el inverso de $\tilde{f}$.

$$\begin{tikzcd}
M \otimes_A N \arrow[r] \arrow[dr, "\hat{g}_1"'] & (M \otimes_A N) \oplus (M \otimes_A P) \arrow[d, dotted, "G"] & M \otimes_A P \arrow[l] \arrow[dl, "\hat{g}_2"] \\
& M \otimes_A (N \oplus P) &
\end{tikzcd}$$

Observar que es $G(m \otimes n, m' \otimes p) = m \otimes (n, 0) + m' \otimes (0, p)$. □

Observación 3.4.4. En realidad hemos probado que el producto tensorial es distributivo respecto de sumas directas *finitas*. Análogamente se prueba que existen isomorfismos $(\bigoplus M_i) \otimes_A P \xrightarrow{\cong} \bigoplus (M_i \otimes_A P)$ y $M \otimes_A (\bigoplus P_i) \xrightarrow{\cong} \bigoplus (M \otimes_A P_i)$.

Si bien los tensores elementales no son linealmente independientes, se puede probar que a partir de bases de M y N se construye una base (formada por tensores elementales) de $M \otimes_A N$.

Proposición 3.4.5. *Sean M y N dos A-módulos libres con bases respectivas $B = \{b_i\}_{i \in I}$, $B' = \{b'_j\}_{j \in J}$. Entonces:*

- *$M \otimes_A N$ es libre,*
- *$X = \{b_i \otimes b'_j \mid i \in I, j \in J\}$ es base de $M \otimes_A N$.*

Demostración. Probaremos directamente la segunda afirmación (de la cual se deduce la primera). Veamos primero que X genera $M \otimes_A N$.

Todo elemento $u \in M \otimes_A N$ es de la forma $u = \sum_{k=1}^{K} m_k \otimes n_k$. Ahora bien, para cada k se tiene $m_k = \sum_i \lambda_{ki} b_i, n_k = \sum_j \mu_{kj} b'_j$, donde ambas sumas involucran una cantidad finita de elementos (los coeficientes no nulos son sólo una cantidad finita). Por lo tanto:

$$u = \sum_{k,i,j} \lambda_{ki} \mu_{kj} b_i \otimes b'_j.$$

de donde X es generador de $M \otimes_A N$.

Veamos que X es linealmente independiente. Tenemos $M = \bigoplus_i Ab_i$, $N = \bigoplus_j Ab'_j$. Entonces por la observación 3.4.4, $M \otimes_A N \cong \bigoplus_{i,j} \left(Ab_i \otimes_A Ab'_j \right)$.

Además $Ab_i \otimes_A Ab'_j \cong A \otimes_A A \cong A$, mediante $b_i \otimes b'_j \mapsto 1 \otimes 1 \mapsto 1 \cdot 1 = 1$.

Se tiene entonces que $M \otimes_A N \simeq \bigoplus_{i,j} A$ y X se corresponde con la base canónica de $\bigoplus_{i,j} A$ mediante el isomorfismo. Por lo tanto como un isomorfismo lleva bases en bases, debe ser X una base de $M \otimes_A N$. □

El siguiente corolario es inmediato.

Corolario 3.4.6. *Si M y N son libres,* $\mathrm{rg}(M \otimes_A N) = \mathrm{rg}(M) \,\mathrm{rg}(N)$.

Corolario 3.4.7. *Si V y W son $\Bbbk$-espacios vectoriales y $v \in V, w \in W$ son no nulos, entonces $v \otimes w \neq 0$.*

Demostración. Como los conjuntos $\{v\}$ y $\{w\}$ son linealmente independientes en V y W respectivamente, se extienden a bases. El elemento $v \otimes w$ forma parte entonces de una base de $V \otimes_{\Bbbk} W$ y en particular es no nulo. □

3.5. Teorema de estructura

Notas adaptadas por Mariana Haim para el curso "Anillos y Módulos" 2021.

Este capítulo está dedicado al llamado *Teorema de Estructura* de módulos finitamente generados sobre un DIP, que describe cómo son todos los módulos finitamente generados indescomponibles sobre un DIP y asegura que los demás se construyen a partir de estos tomando sumas directas finitas.

Para acercarnos al resultado, comenzamos con una sección que lista "buenas" propiedades de los módulos sobre un DIP y seguimos con una sección que presenta los módulos de torsión y su también "buen comportamiento" sobre un DIP, fundamentales para entender el Teorema de Estructura. La última sección es una aplicación del Teorema de Estructura que permite obtener la forma de Jordan de una matriz, y una construcción general de ésta para el caso de un cuerpo cualquiera.

3.5.1. Propiedades hereditarias de los módulos sobre un DIP

Recordamos que un anillo es *noetheriano a izquierda* si sus ideales a izquierda son finitamente generados.

Proposición 3.5.1. *Sean A un anillo noetheriano a izquierda, M un A-módulo y $N \subseteq M$ un submódulo. Si M es finitamente generado, entonces N también lo es.*

Demostración. Haremos inducción en $\mu(M)$.

Si $\mu(M) = 1$, entonces $M = Am \cong \frac{A}{\mathrm{Ann}(m)}$ para algún $m \in M$ y por tanto N es isomorfo a un submódulo de $\frac{A}{\mathrm{Ann}(m)}$. Por el teorema de correspondencia, existe J ideal izquierdo de A tal que $N \cong \frac{J}{\mathrm{Ann}(m)}$. Como J es finitamente generado, N también lo es.

Supongamos que vale el resultado para valores menores o iguales a n y que $\mu(M) = n + 1$. Tomemos $G = \{g_1, \dots, g_{n+1}\}$ generador de M y definamos $M' = Ag_1 + \cdots + Ag_n$. En la sucesión exacta:

$$0 \to M' \cap N \hookrightarrow N \to \frac{N}{M' \cap N} \to 0$$

el término de la derecha es $\frac{N}{M' \cap N} \cong \frac{M'+N}{M'} \subseteq \frac{M}{M'} = A\overline{g_{n+1}}$ por el segundo teorema de isomorfismo, y el término de la izquierda es un submódulo de M' que verifica $\mu(M') \leqslant n$. Por hipótesis de inducción, ambos términos son finitamente generados, de donde se deduce que el término del medio también lo es (proposición 4.4.3). $\square$

El resultado anterior puede mejorarse para el caso de un DIP, como muestra la siguiente

Proposición 3.5.2. *Sean D un DIP, M un D-módulo y $N \subseteq M$ un submódulo. Si M es finitamente generado, entonces N también lo es y $\mu(N) \leqslant \mu(M)$.*

Demostración. La primera parte de la afirmación es consecuencia directa de la Proposición 3.5.1, ya que todo DIP es noetheriano. Para la segunda parte de la afirmación, recorramos la prueba de la proposición 3.5.1. En el caso base, se tiene que J es generado por un elemento por ser D DIP y por lo tanto N también, de donde $\mu(N) \leqslant 1 = \mu(M)$. En el paso inductivo, se tiene $\mu(M' \cap N) \leqslant \mu(M')$ y $\mu\left(\frac{N}{M' \cap N}\right) \leqslant \mu\left(\frac{M}{M'}\right) = 1$, de donde $\mu(N) \leqslant \mu(M' \cap N) + \mu(\frac{N}{M' \cap N}) \leqslant \mu(M') + 1 \leqslant n + 1 = \mu(M)$. $\square$

Para el caso de submódulos de un módulo libre sobre un DIP, se puede afinar el resultado, a saber:

Proposición 3.5.3. *Sean D un DIP, M un D-módulo y $N \subseteq M$ un submódulo. Si M es libre de rango finito, entonces N también lo es y* $\operatorname{rg}(N) \leqslant \operatorname{rg}(M)$.

Demostración. Otra vez procederemos por inducción, esta vez en $\operatorname{rg}(M)$.

Si $\operatorname{rg}(M) = 1$, entonces $M \cong D$ y por tanto $N \cong J$ siendo J un ideal de D, por lo tanto principal. Se tiene entonces $N \cong (a)$ para cierto $a \in D$. Si $a = 0$, ya está. Si no, como D es un dominio, $\{a\}$ es linealmente independiente y por lo tanto la imagen de $\{a\}$ por el isomorfismo $N \cong (a)$ es base de N, que resulta libre de rango 1.

Supongamos que vale el resultado para módulos de rango menor o igual a n y probémoslo para M de rango $n+1$. Si $B = \{b_1, \ldots, b_{n+1}\}$ es base de M, sea $M' = Ab_1 + \cdots + Ab_n$. Nuevamente, en la sucesión exacta:

$$0 \to M' \cap N \hookrightarrow N \to \frac{N}{M' \cap N} \to 0$$

el término de la derecha es $\frac{N}{M' \cap N} \subseteq \frac{M}{M'} = A\overline{b_{n+1}}$ que es libre de rango 1. En efecto, $\{\overline{b_{n+1}}\}$ es base de $\frac{M}{M'}$: si $a\overline{b_{n+1}} = 0$, entonces $ab_{n+1} \in M'$ y por tanto es combinación lineal del conjunto $\{b_1, \ldots, b_n\}$; como B es linealmente independiente, se obtiene $a = 0$.

Por hipótesis de inducción, se tiene que el término de la derecha es libre y por tanto la sucesión se escinde (corolario 4.4.6), y $N \cong (M' \cap N) \oplus \frac{N}{M' \cap N}$.

Por otra parte, $M' \cap N$ es un submódulo de M' que es libre de rango n. Por hipótesis de inducción, se deduce que N es libre y

$$\operatorname{rg}(N) = \operatorname{rg}(M' \cap N) + \operatorname{rg}\left(\frac{N}{M' \cap N}\right) \leqslant \operatorname{rg}(M') + \operatorname{rg}\left(\frac{M}{M'}\right) = n+1. \qquad \square$$

Observación 3.5.1. El resultado anterior es válido aunque M no sea finitamente generado. Es decir, sobre un DIP, submódulo de un libre es libre. El lector interesado puede encontrar la prueba del resultado general en el apéndice.

3.5.2. Teoría de torsión

Definición 3.5.1. Sean A un anillo no trivial y M un A-módulo. Un elemento $m \in M$ se dice *de torsión* si existe $a \in A$ no nulo tal que $am = 0$. Además, se define la *torsión de M* como el subconjunto

$$\operatorname{Tor}(M) = \{m \in M \mid m \text{ es de torsión}\}$$

El módulo M se dice *de torsión* si $\operatorname{Tor}(M) = M$ y se dice *sin torsión* o *libre de torsión* si $\operatorname{Tor}(M) = \{0\}$.

Observación 3.5.2.

- $0 \in M$ siempre es de torsión.
- Si A es conmutativo, considerando A como A-módulo, se tiene $\operatorname{Tor}(A) = \{a \in A \mid a \text{ es divisor de cero}\}$. En particular, si D es un dominio, $\operatorname{Tor}(D) = \{0\}$.

La siguiente proposición muestra que la torsión de M tiene buenas propiedades en el caso en que el anillo es un dominio, por lo que a partir de ahora nos situaremos en ese contexto.

Proposición 3.5.4. *Sea D un dominio y M un D-módulo. Entonces $\operatorname{Tor}(M) \subseteq M$ es un submódulo, y $M/\operatorname{Tor}(M)$ es sin torsión.*

Demostración. Sean $m, n \in \operatorname{Tor}(M)$. Existen entonces $a, b \in D$ no nulos tales que $am = bn = 0$ y por lo tanto $ab(m+n) = 0$, puesto que D es conmutativo. Como D no tiene divisores de cero, se tiene $ab \neq 0$ y por lo tanto $m + n \in \operatorname{Tor}(M)$.

Por otra parte, si $m \in \operatorname{Tor}(M)$ y $d \in D$, entonces existe $a \in D$ no nulo tal que $am = 0$ y por lo tanto $a(dm) = d(am) = 0$, por lo que $dm \in \operatorname{Tor}(M)$.

Veamos la segunda afirmación. Sea $\overline{x} \in M/\operatorname{Tor}(M)$, $\overline{x} \neq \overline{0}$ (i.e. $x \notin \operatorname{Tor}(M)$). Supongamos que $a\overline{x} = \overline{0}$. Pero entonces $\overline{ax} = \overline{0} \Rightarrow ax \in \operatorname{Tor}(M)$, es decir, existe $b \neq 0$ tal que $bax = 0$. Como $x \notin \operatorname{Tor}(M)$, entonces $ba = 0$. Como $b \neq 0$ y D es un dominio, debe ser $a = 0$. $\square$

Observación 3.5.3.

1. Es sencillo verificar que si $f : M \to N$ es un isomorfismo, se tiene $f(\operatorname{Tor}(M)) = \operatorname{Tor}(N)$, por lo que si D es un dominio y M, N son D-módulos, entonces $M \cong N \Rightarrow \operatorname{Tor}(M) \cong \operatorname{Tor}(N)$.

2. Es un ejercicio verificar que $\operatorname{Tor}(\bigoplus_{i\in I} M_i) \cong \bigoplus_{i\in I} \operatorname{Tor}(M_i)$.

Ejemplos 3.5.1.

1. Si L es libre sobre un dominio, entonces $\operatorname{Tor}(L) = \{0\}$. En efecto, $L \cong \bigoplus_{i\in I} D$ por lo que $\operatorname{Tor}(L) \cong \bigoplus_{i\in I} \operatorname{Tor}(D) = \{0\}$.

2. $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo es de torsión, es decir, $\operatorname{Tor}(\mathbb{Z}_n) = \mathbb{Z}_n$. En efecto $n\overline{x} = 0$, para todo $x \in \mathbb{Z}_n$.

3. Más en general, todo grupo abeliano finito G es de torsión. En efecto, dado $g \in G$ no nulo, consideremos el morfismo de $\mathbb{Z}$-módulos $\varphi_g : \mathbb{Z} \to G$, $\varphi_g(n) = ng$. Si g no es de torsión, entonces $\operatorname{Ker}\varphi = 0$ y por lo tanto G contiene una copia de $\mathbb{Z}$, por lo que es infinito.

En el ejemplo anterior observamos que todo módulo libre sobre un dominio es sin torsión. El recíproco no es cierto, como muestran los siguientes

Ejemplos 3.5.2.

1. $\mathbb{Q}$ es un $\mathbb{Z}$-módulo sin torsión que no es libre.

2. (x, y) es un $\Bbbk[x, y]$-módulo sin torsión que no es libre.

3. $\mathbb{Z}^{\mathbb{N}}$ (el producto directo de infinitas copias de $\mathbb{Z}$) es un $\mathbb{Z}$-módulo sin torsión que no es libre.

Sin embargo, el resultado es positivo para el caso en que D es un DIP y M es finitamente generado, como enuncia la siguiente

Proposición 3.5.5. *Si D es un DIP y M es un D-módulo finitamente generado y sin torsión, entonces M es libre.*

Demostración. Sea $X = \{x_1, \ldots, x_n\}$ un generador de M. Como M es sin torsión, cada uno de los conjuntos $\{x_i\}$ es linealmente independiente, por lo que existe un subconjunto de X linealmente independiente maximal $U = \{u_1, \ldots, u_k\} \subseteq X$. [6]

Supongamos que existe $x_i \in X\backslash U$. Entonces, por maximalidad de U, el conjunto $U \cup \{x_i\}$ es linealmente dependiente, y por lo tanto (como U es linealmente independiente), existe $d_i \in D$ no nulo tal que $d_i x_i = a_1u_1 + a_2u_2 + \cdots + a_ku_k$.

Llamemos d al producto de los d_i obtenidos por cada $x_i \in X\backslash U$. Como D es un dominio, debe ser $d \neq 0$. Además, para cada $i \in \{1, \ldots, n\}$, se tiene $dx_i \in \langle u_1, \ldots, u_k\rangle$.

Sea $\varphi : M \to M$, $\varphi(m) = dm$. Es un morfismo de D-módulos. Es inyectivo porque M es sin torsión. Por lo tanto, el primer teorema de isomorfismo nos da $M \simeq \operatorname{Im}\varphi \subset \langle u_1, \ldots, u_k\rangle$ que es libre. Al ser D un DIP, todo submódulo de un D-módulo libre es libre; en particular, $\operatorname{Im}\varphi \simeq M$ es libre. $\square$

[6] Se puede probar, de hecho, que en un módulo finitamente generado sobre un dominio, todo conjunto linealmente independiente tiene $\leqslant$ elementos que un generador.

3.5.3. Teorema de estructura

Proposición 3.5.6. *Sean D un DIP y M un D-módulo finitamente generado. Entonces existen D-módulos L y T, con L libre y T de torsión, tales que $M \cong T \bigoplus L$. Además, L y T son únicos a menos de isomorfismo.*

Demostración. Alcanza con observar que en la sucesión exacta

$$0 \hookrightarrow \mathrm{Tor}(M) \to M \to \frac{M}{\mathrm{Tor}(M)} \to 0$$

el término de la derecha es sin torsión, y por tanto libre (proposición 3.5.5). Se tiene entonces que la sucesión se escinde, y por consecuencia

$$M \cong \mathrm{Tor}(M) \oplus \frac{M}{\mathrm{Tor}(M)}.$$

Tomando $T = \mathrm{Tor}(M)$ y $L = \frac{M}{\mathrm{Tor}(M)}$ se tiene la descomposición buscada.

Supongamos ahora que $T \oplus L \cong T' \oplus L'$ via un isomorfismo φ. Entonces, por la Observación 3.5.3, se tiene $\varphi\left(\mathrm{Tor}(T \oplus L)\right) = \mathrm{Tor}(T' \oplus L')$, i.e. $\varphi(T) = T'$. Tenemos entonces $T \cong T'$ y la prueba termina observando que

$$L \cong \frac{T \oplus L}{T} \cong \frac{\varphi(T \oplus L)}{\varphi(T)} = \frac{T' \oplus L'}{T'} \cong L'.$$ □

Tenemos entonces descompuesto a un módulo finitamente generado M sobre un DIP de manera única como suma directa de un libre con su torsión $\mathrm{Tor}(M)$. Como ya sabemos, la parte libre es de la forma $\bigoplus_I D$. Ahora investigaremos qué forma tiene la parte de torsión.

Definición 3.5.2. Un módulo $M \neq 0$ se dice **indescomponible** si $M = X \oplus Y$ implica $X = 0$ o $Y = 0$.

Proposición 3.5.7. *Si D es un dip, los D-módulos D y $\frac{D}{(p^\alpha)}$, con p primo y α positivo son indescomponibles y cíclicos.*

Demostración. Sale usando que la intersección de dos ideales de D distintos y no triviales es no trivial, sale la afirmación para D, que está generado por 1.
Para la segunda hay que considerar ideales de D que contienen a (p^α) y sale la afirmación para $\frac{D}{(p^\alpha)}$, que está generado por $\bar{1}$. □

Teorema 3.5.8 (de estructura de módulos finitamente generados de torsión)**.** *Sean D un DIP y M un D-módulo finitamente generado. Existen $p_1, \ldots, p_k \in D$ irreducibles, $n_1, \ldots, n_t \in \mathbb{Z}^+$ y $\alpha_{ij} \in \mathbb{Z}^+, i \in \{1, 2, \ldots, t\}, j \in \{1, 2, \ldots, n_i\}$ tales que*

$$\mathrm{Tor}(M) \cong \frac{D}{(p_1^{\alpha_{11}})} \oplus \cdots \oplus \frac{D}{(p_1^{\alpha_{1n_1}})} \oplus \cdots \oplus \frac{D}{(p_t^{\alpha_{t1}})} \oplus \cdots \oplus \frac{D}{(p_t^{\alpha_{tn_t}})}.$$

Además, los p_i son únicos a menos de asociados y los n_i, α_{ij} son únicos.

Observación 3.5.4.

- Los $p_i^{\alpha_{ij}}$ se dicen *factores invariantes de M*.
- Se trata de una descomposición de $Tor(M)$ en submódulos cíclicos indescomponibles.
- Juntando la segunda afirmación con la proposición 3.5.6, se tiene que todo módulo finitamente generado se descompone en suma directa de submódulos cíclicos indescomponibles (la parte libre aporta sumandos del tipo D, y la parte de torsión sumandos del tipo $\frac{D}{(p^\alpha)}$ con $p \in D$ irreducible y $\alpha \in \mathbb{Z}^+$).

- El conjunto $\{r, t, p_1^{\alpha_{11}}, \ldots, p_t^{\alpha_{tn_t}}\}$ es un *conjunto completo de invariantes*; es decir, si dos D-módulos son isomorfos, entonces tienen los mismos invariantes. Además este conjunto de invariantes es *completo*: es decir, que si dos D-módulos tienen los mismos invariantes entonces son isomorfos.

Demostración. No vamos a demostrar este Teorema en el contexto general; para simplificar, haremos la prueba (en la próxima sección) para el caso $D = \mathbb{Z}$ (esto es, para grupos abelianos). □

3.5.4. Prueba del Teorema de Estructura de Grupos abelianos finitamente generados

Proposición 3.5.9.

- *Todo grupo abeliano finito se descompone en suma de indescomponibles.*
- *Un grupo abeliano es finitamente generado y de torsıón si y solo si es finito.*

Demostración.

- En efecto, si el grupo es indescomponible, ya está, si no es suma directa de subgrupos de cardinal estrictamente menor. Si ambos son indescomponibles ya está, si no el proceso sigue y para porque el cardinal del grupo original es finito y va bajando estrictamente en cada descomposición no tirival.
- Supongamos que G es finito. Si tiene un elemento sin torsión $x \in G$, el morfismo de grupos $\mathbb{Z} \to G$ que multiplica por x es inyectivo, contradiciendo la finitud de G.
  Recíprocamente si X es un generador finito de G, para todo $x \in X$ existe $n \in \mathbb{Z}$ no nulo tal que $n_x x = 0$. Se deduce que todo elemento de G es combinación de los elementos de X con coeficiente en x un entero entre 0 y $n_x - 1$, por lo que hay finitos elementos en G.

□

Proposición 3.5.10.

- *Un grupo abeliano es finitamente generado y de torsión si y sólo si es finito.*
- *Si G es un grupo abeliano finito, existe $n \in \mathbb{N}$ tal que $nx = 0, \forall x \in G$.* [7]

Demostración.

- Si G es finito entonces es finitamente generado por el propio G. Además, si tiene un elemento $x \neq 0$ que no es de torsión, se deduce que el morfismo $\mathbb{Z} \to G$ que multiplica por x es inyectivo y por tanto G es infinito.
  Recíprocamente, sea X un generador finito de G. Cada elemento $x \in X$ tiene un testigo $n_x \in \mathbb{N}$ de la torsión. Se puede probar a partir de aquíque todo elemento de G es de la forma $\sum_{x \in X} r_x x$, con $0 \leqslant r_x < n_x$, por lo que G tiene a lo sumo $\prod_{x \in X} n_x$ elementos.
- Alcanza con tomar un testigo de la torsión para cada $x \in G$ y multiplicarlos todos entre sí , obteniendo un posible n.

□

Definición 3.5.3. Sea p un natural primo. Un grupo abeliano G es un **p-grupo** si para todo $x \in G$, existe α tal que $p^\alpha x = 0$

[7] Se puede probar, a partir del conocido Teorema de Lagrange para grupos - pero no lo haremos acá- que $\#G$ sirve como un posible n.

Observación 3.5.5. Dado un grupo abeliano G y un primo p, se define

$$Tor_p(G) = \{g \in G \mid \exists \alpha \geqslant 1 : p_i^\alpha g = 0\}.$$

Es fácil probar que $Tor_p(G)$ es un subgrupo de $Tor(G)$ y que si $G \cong G'$ via φ, entonces $Tor_p(G) \cong Tor_p(G')$ via la correspondiente restricción de φ

Teorema 3.5.11. *Todo grupo abeliano finito se descompone en suma directa de p-grupos.*

Demostración. Sea n como en la Proposición 3.5.10. Para todo $g \in G$, se tiene $ng = 0$. Supongamos $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ con $mcd(p_i, p_j) = 1, \forall i \neq j$ y consideremos para cada $i \in \{1, 2, \cdots, t\}$, el subgrupo

$$G_i = Tor_{p_i}(G) \leqslant G.$$

Veamos primero que $G = \bigoplus_{i=1}^t G_i$.
Notar que si $q_i = \frac{n}{p_i^{e_i}}$, se tiene $q_i x \in G_i \forall x \in G$ y $mcd(q_1, q_2, \ldots q_t) = 1$, por lo que existen $a_i \in \mathbb{Z}$ tales que $\sum_{i=1}^k a_i q_i = 1$. Se deduce, para todo $x \in G$:

$$x = 1 \cdot x = a_1 q_1 x + \cdots a_t q_t x \in \sum_{i=1}^k G_i.$$

Además, si $x \in G_i \cap \sum_{j \neq i} G_j$, entonces $p_i^\alpha x = 0$ y $x = \sum_{j \neq i} x_j, x_j \in G_j$. Para cada $j \neq i$ sea α_j tal que $p_j^{\alpha_j} x_j = 0$ y $t = \prod_{j \neq i} p_j^{\alpha_j}$. Se deduce $tx = 0$. Pero mcd $(p_i^{\alpha_i}, t) = 1$ de donde $x = 1 \cdot x = 0$.

□

Lema 3.5.12. *Sea G un p-grupo abeliano y $Y = \{y_1, y_2, \cdots, y_t\} \subseteq G$ tal que $< Y >= \bigoplus_{i=1}^t < y_i >$.*

1. *Si $pz_i = y_i, \forall i \in \{1, 2, \cdots, t\}$, entonces $< y_1, y_2, \cdots, y_t >= \bigoplus_{i=1}^t < y_i >$.*
2. *Si $k_i \in \mathbb{Z}, \forall i \in \{1, 2, \cdots, t\}$, entonces $< k_1 y_1, k_2 y_2, \cdots, k_t y_t >= \bigoplus_{i=1}^t < k_i y_i >$.*

Demostración. 1. Supongamos que $\sum_{i=1}^t a_i z_i = 0$. Entonces $\sum_{i=1}^t a_i y_i = \sum_{i=1}^t a_i p z_i = p \sum_{i=1}^t a_i z_i = 0$. Usando la hipótesis, se deduce que $a_i y_i = 0, \forall i \in \{1, 2, \cdots, t\}$. Como G es un p-grupo, se deduce que $a_i = p a_i', \forall i$. Se tiene entonces $\sum_{i=1}^t a_i' y_i = \sum_{i=1}^t a_i' p z_i = 0 = \sum_{i=1}^t a_i z_i = 0$ y por tanto $a_i z_i = a_i' p z_i = a_i' y_i = 0, \forall i \in \{1, 2, \cdots, t\}$.

2. Supongamos que $\sum_{i=1}^t a_i k_i z_i = 0$ se deduce de la parte anterior que $a_i k_i z_i = 0, \forall i \in \{1, 2, \cdots, t\}$.

□

Teorema 3.5.13. *Todo p-grupo finito es isomorfo a la suma directa finita de grupos de la forma $\mathbb{Z}_{p^{e_i}}$, con $e_i \in \mathbb{N}, e \geqslant 1$.*

Demostración. Haremos la prueba por inducción en

$$m = min\{\alpha \mid p^\alpha x = 0, \forall x \in G\}$$

Si $m = 1$, entonces $px = 0, \forall x \in G$, de lo que se deduce que G es un $\mathbb{Z}_p$-espacio vectorial, y como tal, es suma directa de copias de $\mathbb{Z}_p$ (en particular lo es como grupo abeliano).
Supongamos que el resultado vale hasta m. Lo probaremos para $m + 1$. Consideremos $H = pG \leqslant G$. Como $p^m x = 0, \forall x \in H$, se tiene por inducción que $H = \oplus_{i=1}^t \mathbb{Z}_{p_i^e}$.
Tomemos $\{pz_1, pz_2, \cdots, pz_t\}$ generador de H tal que pz_i genera $\mathbb{Z}_{p_i^e}$. Por otra parte sea $A_p =$

$\{x \in G \mid px = 0\}$. Para cada z_i en L, si $k_i = min\{n \mid ny_i = 0\}$, entonces $k_i z_i \in A_p$. En efecto $p(k_i z_i) = k_i(pz_i) = ky_i = 0$.
Ahora bien, A_p es un $\mathbb{Z}_p$- espacio vectorial y por lo tanto es suma directa de copias de $\mathbb{Z}_p$. Por el Lema 3.5.12, el conjunto $X = \{k_1 z_1, \cdots k_t z_t\}$ es linealmente independiente (en A_p como $\mathbb{Z}_p$-espacio vectorial), y por tanto se extiende a una base $X \sqcup Y$ de A_p.
Consideremos los subgrupos K Y L generados respectivamente por Y y $\{z_1, z_2, \cdots, z_t\}$. Por un lado, $K \subseteq A_p$, está en las hipotésis de inducción y por lo tanto es suma de (p-) grupos cíclicos. Por otro lado, L es suma directa de los subgrupos generados por los z_i, que son cíclicos (de orden pk_i).
Vamos a probar que $G = K \oplus L$ y con eso tenemos la tesis.
Veamos primero que $K \cap L = 0$: sea $y = \sum_{i=1}^t a_i z_i \in < Y > \subseteq A_p$. Se tiene entonces $py = 0$ y por tanto $a_i y_i = pa_i z_i = 0, \forall i = \{1, 2, \cdots, t\}$, de donde $a_i = a_i' k_i$ y se deduce $0 = y - y = \sum_{i=1}^t a_i' k_i z_i - y$ y por construcción de Y resulta $y = 0$.
Veamos ahora que $G = K + L$. Para cada $x \in G$, se tiene $px \in H$, por lo que $px = \sum -i = 1^t a_i y_i = \sum_{i=1}^t pa_i z_i$, de donde $p(x - \sum_{i=1}^t a_i z_i) = 0$. Se deduce que $x - \sum_{i=1}^t a_i z_i \in A_p$ y por lo tanto en $K + L$. Finalmente $x \in K + L$ puesto que $\sum_{i=1}^t a_i z_i \in L$.

□

Observación 3.5.6. Notar que los grupos finitos indescomponibles son de la forma $\mathbb{Z}_{p^\alpha}$.

Ejemplo 3.5.1. Hallemos todas las clases de isomorfismo de un grupo abeliano G de cardinal 180. Como $180 = 2^2 \cdot 3^2 \cdot 5$. Por lo tanto G es isomorfo a uno y sólo uno de los siguientes:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_5$,
- $\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_5$.

Corolario 3.5.14 (Clasificación de grupos abelianos finitamente generados)**.** *Sea G un grupo abeliano finitamente generado.*
Existe un único $r \in \mathbb{N}$, y únicos (a menos del orden) $p_1, \ldots, p_k \in \mathbb{N}$ primos (no necesariamente diferentes) y $n_1, \cdots, n_k \in \mathbb{N}$ no nulos y $\alpha_{ij} \geqslant 1, \forall i \in \{1, 2, \cdots, k\}, j \in \{1, 2, \cdots n_i\}$, tales que

$$G \cong (\mathbb{Z}_{p_1^{\alpha_{11}}} \oplus \mathbb{Z}_{p_1^{\alpha_{12}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{\alpha_{1n_1}}}) \oplus \cdots \oplus (\mathbb{Z}_{p_k^{\alpha_{k1}}} \oplus \mathbb{Z}_{p_k^{\alpha_{k2}}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{\alpha_{kn_k}}}) \oplus \mathbb{Z}^r$$

Demostración.
Existencia
Como $\mathbb{Z}$ es un DIP, sabemos que todo grupo abeliano G finitamente generado se descompone en suma directa de un subgrupo libre y uno de torsión. La parte libre es de la forma $\mathbb{Z}^r$.
La parte de torsión es finita (porque es finitamente generada) por lo que el resto de la prueba se deduce de los Teoremas 3.5.11 y 3.5.13.
Unicidad Por un lado si $T \oplus L \cong T' \oplus L'$ con T, T' de torsión y L, L' libres, se tiene por la Proposición 3.5.6 que $T \cong T', L \cong L'$. Se deduce que r es único, puesto que D tiene número de base invariante.
Ahora bien, en vista de la Observación 3.5.5, queda probar que si p es primo y

$$\mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_n}} \cong \mathbb{Z}_{p^{\beta_1}} \oplus \mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_k}} \qquad (*)$$

para ciertos $n, k > 0$, $\alpha_i \geqslant \alpha_j \geqslant 1$, $\beta_i \geqslant \beta_j \geqslant 1$ cuando $i > j$, entonces $n = k, \alpha_i = \beta_i, \forall i$.
Lo probaremos por inducción en el cardinal de T. Si es p (es el caso $\mathbb{T} = \mathbb{Z}_p$), la unicidad es clara. Supongamos ahora que la afirmación vale para $\#T < h$ y que

$$\mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_n}} \cong \mathbb{Z}_{p^{\beta_1}} \oplus \mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_k}}$$

con $\alpha_i \geqslant \alpha_j$, $\beta_i \geqslant \beta_j$ cuando $i > j$. Se deduce que

$$p\mathbb{Z}_{p^{\alpha_1}} \oplus p\mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus p\mathbb{Z}_{p^{\alpha_h}} \cong p\mathbb{Z}_{p^{\beta_1}} \oplus p\mathbb{Z}_{p^{\beta_2}} \oplus \cdots \oplus p\mathbb{Z}_{p^{\beta_k}} \qquad (**)$$

Ahora bien, observemos que

$$p\mathbb{Z}_{p^\gamma} \cong \begin{cases} 0 & \text{si } \gamma = 1 \\ \mathbb{Z}_{p^{\gamma-1}} & \text{si no} \end{cases}$$

(el segundo caso se prueba observando que el morfismo de $\mathbb{Z}_{p^{\gamma-1}} \to \mathbb{Z}_{p^\gamma}$ que multiplica por p está bien definido, es inyectivo y tiene imagen $p\mathbb{Z}_{p^\gamma}$). Si $\alpha_i = 1, \forall i$ entonces queda el grupo trivial a la izquierda, y por lo tanto el grupo trivial a la derecha, lo que implica que $\beta_j = 1 \forall j$ y además, por cardinalidad, que $n = k$.
Si no, se tiene que, en $(**)$, el grupo de torsión involucrado tiene estrictamente al menos p y estrictamente menos de h elementos y

$$\mathbb{Z}_{p^{\alpha_1 - 1}} \oplus \mathbb{Z}_{p^{\alpha_2 - 1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_l - 1}} \cong \mathbb{Z}_{p^{\beta_1 - 1}} \oplus \mathbb{Z}_{p^{\beta_2 - 1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\beta_r - 1}}.$$

donde todos los sumandos son no nulos. Se deduce, aplicando la hipótesis de inducción, que $r = l$, $\alpha_i - 1 = \beta_i - 1, \forall i \leqslant l$.
Además $p\mathbb{Z}_{p^{\alpha_u}} = p\mathbb{Z}_{p^{\beta_u}} = 0, \forall u > l$, de donde $\alpha_u = \beta_u = 1, \forall u > l$. $\square$

3.5.5. Aplicación: forma de Jordan

En lo que sigue $\Bbbk$ es un cuerpo cualquiera, V un $\Bbbk$-espacio vectorial y $T : V \to V$ una transformación lineal.
Usaremos el Teorema de Estructura para, en el caso en que $\Bbbk = \mathbb{C}$ y V de dimensión finita, obtener una descomposición de V en subespacios T-cíclicos (i.e. generados por un elemento v y sus transformados a través de T y sus iteradas), que da lugar a una base B de V para la cual la matriz asociada ${}_B[T]_B$ es en algún sentido "simple". Dicha matriz es esencialmente única y se llama forma de Jordan de T.

Antes de enunciar el primer resultado, conviene recordar algunas definiciones. Decimos que un subespacio W de V es *T-invariante* si $T(W) \subseteq W$, y que es *T-cíclico* si para cierto $w \in W$, se tiene que el conjunto $\{w, T(w), T^2(w), \dots, T^n(w), \dots\}$ es un generador de W. En este último caso, notamos $W = Z(T, w)$.

Recordemos además que un A-módulo M se dice *cíclico* si $M = Am = \{am \mid a \in A\}$ para cierto $m \in M$.

La siguiente proposición permite poner nuestra situación en contexto de módulos sobre $\Bbbk[x]$.

Proposición 3.5.15. *Sean $\Bbbk$ un cuerpo, V un $\Bbbk$-espacio vectorial y $T : V \to V$ una transformación lineal. Entonces:*

1. *Definiendo $p\dot{v} = p(T)(v)$ para todo $v \in V, p \in \Bbbk[x]$, se obtiene que V es un $\Bbbk[x]$-módulo.*
2. *Si $W \subseteq V$ es un subespacio vectorial, entonces se tiene que:*

a) *W es T-invariante si y sólo si W es un $\Bbbk[x]$-submódulo de V,*

b) *W es T-cíclico si y sólo si W es un $\Bbbk[x]$-módulo cíclico.*

Demostración. 1. La estructura aditiva de V como $\Bbbk[x]$-módulo es la de V como $\Bbbk$-módulo. Por otra parte es claro que la operación $\cdot : \Bbbk[x] \times V \to V$ es distributiva con respecto a la suma en $\Bbbk[x]$ y con respecto a la suma en V. Observemos además que $1\dot{v} = \mathrm{Id}(v) = v$ para todo $v \in V$. Falta entonces verificar que

$$\dot{p(q\dot{v})} = (pq)\dot{v} \quad \forall p, q \in \Bbbk[x], v \in V$$

Para esto, es claro que alcanza con verificarlo para p y q monomios de $\Bbbk[x]$. En efecto, basta con observar que si $p = \sum_{i=0}^{k} a_i x^i$, entonces

$$p \cdot v = \sum_{i=0}^{k} a_i \left(x^i \cdot v\right) \tag{3.1}$$

Tomemos entonces $p = ax^i, q = bx^j$. Tenemos que $q\dot{v} = (bT^j)(v) = bT^j(v)$. Entonces

$$\dot{p(q\dot{v})} = \dot{p(bT^j(v))} = (aT^i)\left(bT^j(v)\right) = aT^i\left(bT^j(v)\right) = abT^i\left(T^j(v)\right) = abT^{i+j}(v)$$

Como $pq = abx^{i+j}$, se deduce la tesis.

2. Tomemos ahora $W \subseteq V$ subespacio.

   a) W es T-invariante si y sólo si $T(w) \in W$ para todo $w \in W$, si y sólo si $x \cdot w \in W$ para todo $w \in W$. Es claro por (3.1) que esto último equivale a $p \cdot w \in W$ para todo $w \in W, p \in \Bbbk[x]$, es decir, a que W sea un $\Bbbk[x]$-submódulo de V.

   b) $W = Z(T, w)$ si y sólo si W es generado como $\Bbbk$-espacio vectorial por $\{T^i(w) \mid i \in \mathbb{N}\}$, si y sólo si W es generado como $\Bbbk[x]$-módulo por w (puesto que $T^n(w) = x^n \cdot w$). □

Observación 3.5.7. 1. Considerando $\Bbbk \subseteq \Bbbk[x]$, la acción de $\Bbbk[x]$ en V definida arriba extiende a la acción original de $\Bbbk$ en V. En efecto, $\lambda \cdot v = (\lambda\,\mathrm{Id})(v) = \lambda v$ para todo $\lambda \in \Bbbk, v \in V$.

2. A partir de la Observación 3.5.7.1, se deduce que un generador de V como $\Bbbk$-espacio vectorial también es generador de V como $\Bbbk[x]$-módulo.

3. Es claro que si V es de dimensión finita $Z(T, w)$ también lo es, y por lo tanto existe $k \in \mathbb{N}$ tal que el conjunto $\{w, T(w), T^2(w), \dots, T^{k-1}(w)\}$ es generador de $Z(T, w)$. Más adelante, veremos que se puede optimizar dicho k para obtener una base.

4. Si $f \in \Bbbk[x]$, se tiene que $\frac{\Bbbk[x]}{(f)}$ es un espacio vectorial de dimensión $\mathrm{gr}(f)$. En efecto, es fácil verificar que el conjunto $\{\bar{1}, \bar{x}, \dots, \bar{x}^{\mathrm{gr}(f)-1}\}$ es una base.

Polinomios característico y minimal Consideremos la inclusión $\iota : \Bbbk \to \mathrm{End}(V)$, definida por $\iota(\lambda) = \lambda\,\mathrm{Id}$. Es claro que es un morfismo de anillos y por tanto se extiende de manera única a un morfismo de anillos $\varepsilon_T : \Bbbk[x] \to \mathrm{End}(V)$ tal que $\varepsilon_T(x) = T$. Explícitamente, se tiene $\varepsilon_T(p) = p(T)$.

Si V tiene dimensión finita, podemos considerar el polinomio $\chi_T = \det(T - x\,\mathrm{Id})$. Dicho polinomio se llama *polinomio característico de T*, es de grado $\dim(V)$ y por tanto no nulo. El Teorema de Cayley-Hamilton asegura que $\chi_T(T) = 0$.

Se deduce que $\ker(\varepsilon_T)$ es un ideal de $\Bbbk[x]$ no nulo, y por tanto generado por un polinomio no nulo $m_T \in \Bbbk[x]$ que se elige mónico y se llama *polinomio minimal de* T. (Notar que al elegir m_T mónico, forzamos que sea único).

Es claro entonces que $m_T(T) = 0$, que $m_T \mid \chi_T$ y que m_T es el polinomio mónico de menor grado entre los que anulan a T.

La siguiente proposición permite poner a V, en el caso en que tenga dimensión finita, en el contexto del Teorema de Estructura.

Proposición 3.5.16. *Sean* $\Bbbk$*,* V *y* T *como antes. Supongamos además que* V *es de dimensión finita. Entonces* V *es un* $\Bbbk[x]$*-módulo finitamente generado y de torsión.*

Demostración. Por la Observación 3.5.7.2 es claro que V es finitamente generado, puesto que es de dimensión finita.

Además si V es de dimensión finita, podemos considerar el polinomio característico de T. Como $\chi_T(T) = 0$, tenemos $\chi_T \cdot v = 0$ para todo $v \in V$. Se deduce que todo $v \in V$ es de torsión. □

Estamos entonces en condiciones de aplicar el Teorema de Estructura al $\Bbbk[x]$-módulo V, y eso es lo que nos permitirá demostrar el siguiente resultado.

Teorema 3.5.17. *Sea* V *un espacio vectorial de dimensión* $n < \infty$ *y* $T \in \operatorname{End}(V)$*. Sea además* $m_T = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$ *la descomposición en irreducibles mónicos no asociados dos a dos del polinomio minimal. Entonces existen* $k_1, \ldots, k_r \in \mathbb{Z}^+$ *y subespacios* $V_{ij}, i \in \{1, \ldots, r\}, j \in \{1, \ldots, k_i\}$ *de* V*, tales que*

1. $V = \displaystyle\bigoplus_{i=1}^{r} \bigoplus_{j=1}^{k_i} V_{ij}$*,*
2. *para todo par* (i, j)*, el subespacio* V_{ij} *es* T*-cíclico,*
3. *para todo par* (i, j)*, existe* $n_{ij} \in \mathbb{Z}^+$ *tal que* $V_{ij} \cong \frac{\Bbbk[x]}{(q_i^{n_{ij}})}$*,*
4. *para todo* i*, se tiene* $n_i = \max\{n_{ij} \mid j \in \{1, \ldots, k_i\}\}$*,*
5. $n = \sum_{ij} \operatorname{gr}(q_i) n_{ij}$*.*

Más aún, los V_{ij} *son únicos a menos de isomorfismos y de reordenaciones.*

Demostración. Como V es de torsión y finitamente generado sobre el dominio de ideales principales $\Bbbk[x]$, el Teorema de Estructura nos da una descomposición de V en submódulos cíclicos indescomponibles:

$$V \cong \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{s_i} \frac{\Bbbk[x]}{(p_i^{n_{ij}})},$$

para ciertos $p_i \in \Bbbk[x]$ irreducibles no asociados dos a dos y ciertos $n_{ij} \in \mathbb{Z}^+$ no nulos. Es claro que los p_i pueden elegirse mónicos, y eso hacemos.

Llamemos $\varphi : \displaystyle\bigoplus_{i=1}^{t} \bigoplus_{j=1}^{s_i} \frac{\Bbbk[x]}{(p_i^{n_{ij}})} \to V$ al isomorfismo involucrado y definamos entonces, para cada $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s_i\}$,

$$V_{ij} := \varphi\left(\frac{\Bbbk[x]}{(p_i^{n_{ij}})}\right).$$

Es claro que $V = \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{s_i} V_{ij}$, que $\operatorname{Ann}(V_{ij}) = (p_i^{n_{ij}})$. Además, para cada $i \in \{1, \ldots, t\}$, podemos reordenar los $j \in \{1, \ldots, s_i\}$ para que $n_{i1} \geqslant \cdots \geqslant n_{is_i}$.

Veamos ahora que:

- $r = t$,
- podemos reordernar los $i \in \{1, \ldots, r = t\}$ para que $p_i = q_i$ y $s_i = k_i$, para todo $i \in \{1, \ldots, r = t\}$,
- $n_i = n_{i1}$, para todo $i \in \{1, \ldots, r = t\}$.

Como $\mathbb{k}[x]$ es un dominio factorial, m_T se descompone de manera única (a menos de reordenaciones) en producto de irreducibles mónicos, por lo que alcanza con ver que

$$m_T = p_1^{n_{11}} p_2^{n_{21}} \cdots p_t^{n_{t1}} \tag{3.2}$$

para deducir las tres afirmaciones de arriba. Llamemos p al polinomio del lado derecho de (3.2). Como $p_i^{n_{ij}}$ anula a cada V_{ij}, se tiene que $p_i^{n_{i1}}$ anula a cada V_{ij}, y por tanto p anula a V. Se deduce que p es múltiplo de m_T.

Recíprocamente, observar que el polinomio minimal de $T_{|V_{ij}}$ es $p_i^{n_{ij}}$; como m_T anula a V_{ij} se tiene que m_T es múltiplo de cada $p_i^{n_{ij}}$. Como p es el el mínimo común múltiplo de los $p_i^{n_{ij}}$, se obtiene que m_T es múltiplo de p.

Al ser m_T y p asociados y mónicos, se deduce que son iguales.

Finalmente, notar que por la observación 3.5.7.4, tenemos $\dim(V_{ij}) = \operatorname{gr}(p_i) n_{ij} = \operatorname{gr}(q_i) n_{ij}$ de donde deducimos que la dimensión de V es $n = \sum_{ij} \operatorname{gr}(q_i) n_{ij}$.

La unicidad se deduce de la unicidad en el Teorema de Estructura. $\square$

Lema 3.5.18. *Para cualquier $\lambda \in \mathbb{k}$, se tiene $Z(T, v) = Z(T + \lambda id_V, v)$.*

Demostración. Es claro que alcanza con probar una inclusión (la otra se deduce tomando $-\lambda$ en lugar de λ). Para cada $w \in Z(T, v)$, existe $p \in \mathbb{k}[x]$ tal que $w = p(T)(v)$. Sea $q(x) := p(x - \lambda)$. Si $S = T + \lambda id_V$, se tiene $q(S) = p(S - \lambda id_V) = p(T)$, por lo que $w = q(S)(v) \in Z(S, v)$. $\square$

Corolario 3.5.19 (Forma canónica de Jordan)**.** *Sean $\mathbb{k}$ un cuerpo y $A \in M_n(\mathbb{k})$ tal que el polinomio minimal es producto de polinomios de grado 1 con coeficientes en $\mathbb{k}$. Entonces A es semejante a una matriz de la forma*

$$J = \begin{pmatrix} \begin{matrix} J_{11} & 0 & \cdots & 0 \\ 0 & J_{12} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{1k_1} \end{matrix} & 0 & & 0 \\ 0 & \begin{matrix} J_{21} & 0 & \cdots & 0 \\ 0 & J_{22} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{2k_2} \end{matrix} & & 0 \\ & & \ddots & \\ 0 & 0 & & \begin{matrix} J_{t1} & 0 & \cdots & 0 \\ 0 & J_{t2} & & 0 \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & J_{tk_t} \end{matrix} \end{pmatrix},$$

donde para cada $i \in \{1, \ldots, t\}, j \in \{1, \ldots, k_i\}$*, se tiene que*

$$J_{ij} = \begin{pmatrix} \lambda_i & 0 & \cdots & \cdots & 0 \\ 1 & \lambda_i & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda_i & 0 \\ 0 & \cdots & 0 & 1 & \lambda_i \end{pmatrix},$$

para cierto $\lambda_i \in \Bbbk$.

Más aún, la matriz J *es única a menos de reordenaciones de los bloques* J_{ij}.

Demostración. Consideremos los V_{ij} de la descomposición del Teorema 3.5.17 y para cada par (i, j), sea $T_{ij} = T_{|V_{ij}}$. Sabemos, por el dicho Teorema, que el polinomio minimal de T_{ij} es de la forma $q_i^{n_{ij}}$, para cierto $q_i \in \Bbbk[x]$ mónico e irreducible. Pero por hipótesis, dicho irreducible debe ser de grado 1 y por tanto de la forma $x - \lambda_i$, para cierto $\lambda_i \in \Bbbk$.

Consideremos entonces $S_{ij} : V_{ij} \to V_{ij}$ definida por $S_{ij} = T_{ij} - \lambda_i \operatorname{Id}_{V_{ij}}$. Por el Lema 3.5.13, se tiene que V_{ij} es S_{ij}-cíclico, y por lo tanto admite una base $C_{ij} = \{v_{ij}, S_{ij}(v_{ij}), S_{ij}^2(v_{ij}), \ldots, S_{ij}^{n_{ij}-1}(v_{ij})\}$. Como además $S_{ij}^{n_{ij}} = 0$, tenemos que la matriz asociada a S_{ij} en dicha base es

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Como $T_{ij} = S_{ij} + \lambda_i \operatorname{Id}_{V_{ij}}$, la matriz asociada a T_{ij} en la base C_{ij} es

$$\begin{pmatrix} \lambda_i & 0 & \cdots & \cdots & 0 \\ 1 & \lambda_i & \ddots & & \vdots \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda_i & 0 \\ 0 & \cdots & 0 & 1 & \lambda_i \end{pmatrix}$$

Tomando la base $C = \bigcup_{i,j} C_{ij}$ (ordenando los pares (i, j) según el orden lexicográfico), se obtiene que la matriz asociada a T en la base C es la buscada.

La unicidad se deduce de la unicidad en el Teorema 3.5.17. □

Definición 3.5.4. La matriz R del Corolario 3.5.19 se dice *forma canónica de Jordan* de la matriz A en el cuerpo $\Bbbk$.

Observaciones 3.5.1.

1. La forma de Jordan sobre un cuerpo $\Bbbk$ no siempre está definida.
2. Si A es diagonalizable semejante a D, la forma canónica de Jordan de A está definida y es D (puesto que el polinomio minimal es el producto de los polinomios $x - d_i$, variando d_i en todas las entradas distintas de la diagonal de D).
3. Si A es nilpotente, la forma canónica de Jordan de A está definida (puesto que su polinomio minimal es de la forma X^n y por tanto se descompone en producto de polinomios irreducibles de grado 1).

Ejemplos 3.5.3. 1. Sean $\Bbbk$ un cuerpo y $T : \Bbbk^5 \to \Bbbk^5$ definida por $T(a,b,c,d,e) = (2b, -2a, a+5c, a+b+c-2d, 5e)$. Hallemos, si corresponde, la forma de Jordan de T en los casos $\Bbbk = \mathbb{R}$ y $\Bbbk = \mathbb{C}$.
El polinomio característico de T es $\chi_T = (x^2+4)(5-x)^2(-2-x)$. Calculemos el polinomio minimal m_T. Tenemos dos posibilidades

$$m_T = \chi_T \text{ o } m_T = (x^2+4)(5-x)(-2-x).$$

Ahora bien se tiene $(A^2 + 4Id)(5Id - A)(-2Id - A) = 0$, por lo que $m_T = (x^2+4)(5-x)(-2-x)$. En el caso $\Bbbk = \mathbb{C}$, como A es diagonalizable, su forma de Jordan es

$$J_{\mathbb{C}} = \begin{pmatrix} 2i & 0 & 0 & 0 & 0 \\ 0 & -2i & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}.$$

.

2. Supongamos ahora que $T : \Bbbk^5 \to \Bbbk^5$ es tal que $\chi_T = (x-2)^3(x+5)^2 = m_T$. Tanto en el caso $\Bbbk = \mathbb{C}$ como en el caso $\Bbbk = \mathbb{R}$ se tiene que la matriz de Jordan es

$$J = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & -5 & 0 \\ 0 & 0 & 0 & 1 & -5 \end{pmatrix}.$$

Supongamos que $B = \{v_1, v_2, v_3, v_4, v_5\}$ es una base para R. Esto es $T(v_1) = v_2, T(v_2) = v_3, T(v_3) = 8v_1 - 12v_2 + 6v_3, T(v_4) = v_5, T(v_5) = -25v_4 - 10v_5$. Hallemos una base para J.
Es fácil ver que $w_3 = 4v_1 - 4v_2 + v_3$ y $w_5 = 5v_4 + v_5$ son vectores propios asociados respectivamente a 2 y -5 (para hallarlos se impuso la condición de vector propio a combinaciones lineales de v_1, v_2 y v_3 y a de v_4 y v_5 respectivamente). Para completar la base, buscamos w_1 y w_2 combinaciones lineales de v_1, v_2 y v_3 tales que $T(w_1) = 2w_1 + w_2$ y $T(w_2) = 2w_2 + w_3$ y además $w_4 = \lambda v_4 + \mu v_5$ tal que $T(w_4) = -5w_4 + w_5$.
Hallemos primero w_4. La condición para su transformado implica $\lambda v_5 + \mu(-25v_4 - 10v_5) = -5\lambda v_4 - 5\lambda v_5 + 5v_4 + v_5$, lo que implica

$$-25\mu = -5\lambda + 5, \quad \lambda - 10\mu = -5\lambda + 1,$$

esto es $\lambda - 5\mu = 1, \quad 6\lambda - 10\mu = 1$ y por lo tanto $\lambda = \frac{1}{4}, \mu = \frac{-3}{20}$. Se obtuvo $w_4 = \frac{1}{4}v_4 - \frac{3}{20}v_5$.
Análogamente, se tiene $w_2 = 2v_1 - 3v_2 + v_3$ y $w_1 = 3v_1 - 3v_2 + v_3$.
Así, si la base original B es la base canónica de $\mathbb{C}^5$, la base de Jordan es

$$\{(3,-3,1,0,0), (2,-3,1,0,0), (4,-4,1,0,0), (0,0,0,5,1), (0,0,0,\frac{1}{4},\frac{3}{20})\}.$$