Notas de Anillos y Módulos, 2025

Mariana Haim

29 de julio de 2025

Índice general

Capítulo 1

Grupos

1.1. Generalidades

Definición 1.1.1 (Grupo)**.** *Un* grupo *es una terna* $(G, *, e)$ *tal que* G *es un conjunto,* $* : G \times G \to G$ *es una función,* $e \in G$ *y se dice si 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 el *neutro* del grupo (se verá que es el único elemento del grupo que verifica la propiedad $(G2)$). La propiedad $(G1)$ se conoce como *asociatividad* del grupo y el elemento b que verifica $(G3)$ se dice *opuesto* de a (se verá que dado a existe un único elemento b que verifica la propiedad $(G3)$).

Definición 1.1.2. *Una terna* $(G, *, e)$ *como la de arriba pero que verifica sólo las propiedades* $(G1)$ *y* $(G2)$ *se dice* monoide*.*

Muchas de las propiedades que probaremos para grupos valen también en el contexto de monoides. En general se sobreentienden la operación y el neutro, por lo que es muy común que se use G en lugar de $(G, *, e)$.

Ejemplos 1.1.3 (Monoides y grupos)**.**

1. *Los naturales con la suma* $(\mathbb{N}, +, 0)$ *forman un monoide y los naturales con la multiplicación* $(\mathbb{N}, \cdot, 1)$ *también.*
2. *Los enteros con la suma* $(\mathbb{Z}, +, 0)$ *forman un grupo.*
3. *Los racionales no nulos con la multiplicación* $(\mathbb{Q}^*, \cdot, 1)$ *forman un grupo.*

4. *Las matrices cuadradas de coeficientes reales con el producto* $(M_n(\mathbb{R}), \cdot, I_n)$ *forman un monoide. Y las invertibles forman un grupo.*

5. *Las funciones de un conjunto en sí mismo con la composición* $(\mathrm{End}(A), \circ, Id_A)$ *forman un monoide. Y las biyectivas forman un grupo.*

Proposición 1.1.4.

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

2. **Unicidad del opuesto de un elemento dado:** *Si tenemos* $a * b = b * a = e$ *y* $a * c = c * a = e$ *para ciertos* $a, b, c \in G$*, entonces* $b = c$*. Esta propiedad nos permite notar* $-a$ *al (único) opuesto de* a*.*

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

4. **Sustracción:** *Si definimos* $a - b := a * (-b)$*, tenemos*

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

5. **Multiplicación por un entero:** *Para cada* $a \in G$ *y* $n \in \mathbb{Z}$ *definimos:*

$$na = \begin{cases} \overbrace{a * a * \cdots * a}^{n \text{ veces}} & si\ n > 0 \\ e & si\ n = 0 \\ (-n)(-a) & si\ n < 0 \end{cases}$$

Se cumple entonces: $1a = a, \quad -1a = -a, \quad 0a = e, \forall a \in G,$
$(n + m)a = na * ma, \quad (n \cdot m)a = n(ma), \quad \forall a \in G, \forall n, m \in \mathbb{Z}.$

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 verificar qué axiomas o propiedades de los grupos se usan en cada paso de las demostraciones).

3. Se deduce como sigue:

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

4. Queda como ejercicio.

5. Queda como ejercicio. □

Proposición 1.1.5. *Un monoide tal que todo elemento es invertible a izquierda es un grupo.*

Demostración. Queda como ejercicio. □

Definición 1.1.6 (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 $H \leq G$.

Definición 1.1.7 (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.*

Ejemplos 1.1.8 (Subgrupos)**.** *1. Si tomamos el grupo de los complejos con la suma usual $(\mathbb{C}, +, 0)$, tenemos:*

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

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

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

Proposición 1.1.9. *Sea G un grupo.*

1. *Son equivalentes, para un subconjunto $H \subseteq G$:*
   a) *H es un subgrupo de G,*
   b) *$H \neq \emptyset$ y $a - b \in H \quad \forall a, b \in H$,*
   c) *$e \in H$ y $(H, *|_{H \times H}, e)$ es un grupo.*
2. *Si H y K son subgrupos de G entonces también lo es $H \cap K$.*

Demostración. Queda como ejercicio. □

Definición 1.1.10 (Producto directo)**.** *Si H, K son grupos, el producto cartesiano $H \times K$ tiene estructura de grupo definiendo*

$$(h, k) * (h', k') := (h * h', k * k').$$

Lo notamos también $H \times K$ y lo llamamos producto directo *de H y K.*

1.2. Grupos abelianos

Definición 1.2.1 (Grupo abeliano)**.** *Un grupo* $(G, +, 0)$ *se dice* abeliano *o* conmutativo *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 llamarse* suma *del grupo.*

Observación 1.2.2. *1. Los grupos de los ejemplos 1.1.3.2 y 1.1.3.3 son abelianos. Los de los ejemplos 1.1.3.4 y 1.1.3.5 no lo son.*

2. Todo subgrupo de un grupo abeliano es un un grupo abeliano.

Proposición 1.2.3 (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

Definición 1.3.1 (Morfismo de grupos)**.** *Sean $(A, *, e_A)$ y $(B, *, e_B)$ 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 1.3.2. *Sea $f : A \to B$ morfismo de grupos.*

1. $f(e_A) = e_B$,
2. $f(-x) = -f(x) \ \forall x \in A$,
3. $f(nx) = nf(x) \ \forall n \in \mathbb{Z}, \forall x \in A$.

Demostración. Queda como ejercicio. □

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

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

Proposición 1.3.3.
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 $id_A : A \to A$ es un morfismo de grupos.*
3. *Sea $f : A \to B$ morfismo de grupos.*
   Si $K \leq A$, entonces $f(K) \leq B$. Si $H \leq B$, entonces $f^{-1}(H) \leq A$.

Demostración. Queda como ejercicio. □

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

Definición 1.3.4 (Núcleo e imagen)**.** *Sea $f : A \to B$ morfismo de grupos. El* núcleo *y la* imagen *de f son respectivamente:*

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

Proposición 1.3.5.
1. *$Ker(f) \leq A, \Im(f) \leq B$.*
2. *f es inyectiva si y sólo si $Ker(f) = 0$, f es sobreyectiva si y sólo si $\Im(f) = B$.*
3. *La función $O : A \to B$ definida por $O(x) = e_B, \forall x \in A$ es un morfismo de grupos con núcleo A e imagen el grupo 0.*

Demostración. Queda como ejercicio. □

Definición 1.3.6. *Un* monomorfismo (epimorfismo) de grupos *es un morfismo de grupos inyectivo (sobreyectivo). Un* isomorfismo de grupos *es un morfismo de grupos biyectivo. 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 de G en G se dice* endomorfismo de G *de G. Un isomorfismo de G en G se dice* automorfismo *de G.*

Proposición 1.3.7. *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. Queda como ejercicio. □

Lema 1.3.8. *Sea $(G, +, 0)$ un grupo abeliano y $H, K \leq G$. 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 $Kerf = \{0\}$: $f(h, k) = 0$ 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 1.3.9. *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 G un grupo abeliano y $H \leq G$. La relación en G definida por:*

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

es una relación de equivalencia, que llamamos relación de congruencia 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 G un grupo abeliano y notemos $\overline{a}$ a la clase de equivalencia de $a \in G$.*

1. *Si $a \equiv_H a'$ y $b \equiv_H b'$, entonces $a + b \equiv_H a' + b'$.*

2. *Si definimos*
$$+ : G/_{\equiv_H} \times G/_{\equiv_H} \to G/_{\equiv_H}$$
mediante $\overline{a}+\overline{b} = \overline{a+b}$, entonces $(G/_{\equiv_H}, +, \overline{0})$ es un grupo que llamamos grupo cociente *de G por H y notamos $\frac{G}{H}$.*

3. *La función $\pi_H : G \to \frac{G}{H}$ definida por $\pi_H(x) = \overline{x}$ es un epimorfismo de grupos que llamamos* proyección canónica *de G en el cociente $\frac{G}{H}$.*

Demostración. 1. En efecto, $(a+b)-(a'+b') = (a-a')+(b-b') \in H$ porque $a - a', b - b' \in H$ (notar que se usa fuertemente la conmutatividad en G).

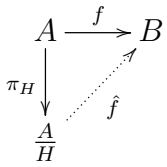
2. Por la parte anterior, tiene sentido la definición. Es fácil ver que esta nueva operación "hereda" las propiedades de G, en otras palabras: de la asociatividad de la operación de G se deduce la asociatividad de esta nueva operación; de la conmutatividad se deduce la nueva conmutatividad, el nuevo neutro es $\overline{0}$ y $-\overline{a} = \overline{-a}, \ \forall a \in G$.

3. Queda como ejercicio. □

Observación 1.4.3. *Notar que $\overline{0} = \{x \in G \mid x - 0 \in H\} = H$ y que*

$$\frac{G}{\{0\}} \cong G; \quad \frac{G}{G} = \{\overline{0}\}.$$

Teorema 1.4.4 (Propiedad Universal del Cociente)**.** *Sea $f : A \to B$ un morfismo de grupos. Si A es abeliano y $H \leq Kerf$, existe un único morfismo $\hat{f} : \frac{A}{H} \to B$ que hace conmutar el siguiente diagrama:*



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

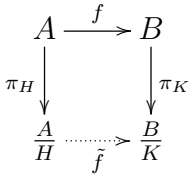
Demostración. Para que el diagrama conmute, es necesario que $\hat{f}(\overline{a}) = f(a)$, lo que prueba la unicidad. Para la existencia, veamos que tiene sentido definir $\hat{f}(\overline{a}) := f(a)$: en efecto, si $a \equiv a'$, entonces $a - a' \in H \subseteq Kerf$ y por tanto $f(a) - f(a') = f(a - a') = 0$. 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 $H \subseteq Kerf$ tiene sentido considerar el grupo $\frac{Kerf}{H}$. Además:

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

□

Corolario 1.4.5 (Teoremas de isomorfismo)**.** *Sea A un grupo abeliano.*

1. *Si $f : A \to B$ es un morfismo de grupos, entonces $\frac{A}{Kerf} \cong Imf$.*
2. *Si $H, K \leq A$ entonces $\frac{H+K}{H} \cong \frac{K}{H \cap K}$.*
3. *Si $H \leq K \leq A$ 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 $H \leq A, K \leq B$ 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:*



Demostración. 1. En el contexto del teorema anterior, se deduce que $\hat{f} : \frac{A}{Kerf} \to B$ es morfismo de grupos con $Im\hat{f} = Imf$ y $Ker\hat{f} = \frac{Kerf}{Kerf} = 0$, por lo que $\hat{f} : \frac{A}{Kerf} \to Imf$ 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 $Imf = \frac{H+K}{H}$. Por otra parte $f(k) = 0$ si y sólo si $k \in H$ de donde $Kerf = H \cap K$. 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. Queda como ejercicio. □

Teorema 1.4.6. *Sea G un grupo abeliano y $H \leq G$. Existe una correspondencia biyectiva entre los conjuntos:*

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

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 $\Omega(L) = \pi_H^{-1}(L)$. Notar 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

Definición 2.1.1 (Anillo)**.** *Un anillo es una quíntupla* $(A, +, \cdot, 0, 1)$ *tal que* A *es un conjunto,* $0, 1 \in A$*,* $+, \cdot : A \times A \to A$ *y se verifican los siguientes axiomas:*

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

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

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

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 *o* multiplicación *de un anillo, y el axioma (A3) se conoce como* propiedad distributiva *del producto a través de la suma.*

Observación 2.1.2. *La definición anterior merece dos aclaraciones:*

- *En la literatura, se puede encontrar que la definición de anillo no exige la existencia de neutro para el producto y que se llama* 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 2.1.3 (Anillos)**.**

1. *Los enteros con la suma y la multipicación usuales* $(\mathbb{Z}, +, \cdot, 0, 1)$*.*
2. *Los reales con la suma y la multiplicación usuales* $(\mathbb{R}, +, \cdot, 0, 1)$*.*

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 $\forall n \geq 2$.*

4. *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 $\forall n \geq 2$, a menos que A sea el anillo trivial.*

5. *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.*

6. *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.*

7. *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 2.1.4 (Propiedades elementales)**.** *Sea $(A, +, \cdot, 0, 1)$ un anillo. Entonces:*

1. *0 y 1 son únicos.*

2. *Para todo $a \in A$: $a \cdot 0 = 0 = 0 \cdot a$, $\quad a \cdot (-1) = -a = (-1) \cdot a$.*

3. *$0 = 1$ si y sólo si $A = \{0\}$ (decimos que A es el* anillo trivial*).*

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

5. *Para todos $n \in \mathbb{Z}, a, b \in A$: $(na) \cdot b = n(a \cdot b) = a \cdot (nb)$.*

Demostración. Queda como ejercicio. □

Definición 2.1.5. *Decimos que $a \in A$ es* invertible *si existe $b \in A$ tal que $a \cdot b = b \cdot a = 1$.*

Observación 2.1.6. *Es fácil ver que para cada $a \in A$ se tiene un único $b \in A$ como en la definición. Decimos que es el* inverso *de a y lo notamos a^{-1}.*

[1] En la sección 2.4 daremos una construcción formal de $A[x]$.

Proposición 2.1.7. *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 2.1.8 (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 2.1.9 (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 2.1.10. *$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ son inclusiones de subanillos.*

Proposición 2.1.11. *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. Queda como ejercicio. □

Definición 2.1.12 (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 isomorfismo de anillos *si es biyectivo (su inversa también es un morfismo de anillos).*

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 2.1.13. *Sea $f : A \to B$ un morfismo de anillos. Si consideramos las estruturas de grupo de A y B con cada suma respectiva, es claro que f es un morfismo de grupos, por lo que tiene sentido considerar su núcleo y su imagen como los definimos en el capítulo anterior. Además, se deduce que todo morfismo de anillos verifica $f(0) = 0, f(-a) = -f(a) \ \ \forall a \in A$. Las propiedades que involucran la estructura multiplicativa de los anillos y del morfismo se enuncian a continuación:*

1. *Si $a \in A$ 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 2.1.7).*

2. *$\mathrm{Im}(f) \subseteq B$ es un subanillo.*

3. *$\mathrm{Ker}(f) \subseteq A$ es un subgrupo aditivo.*

4. *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.*

Observación 2.1.14. *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 $f(1) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.*

2.2. 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 2.2.1 (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 2.2.2 (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 2.2.3. *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 2.2.4. *Sea A un anillo, $A \neq \{0\}$. Decimos que A es un*

- dominio de integridad, dominio íntegro, *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 2.2.5. *De la observación 2.2.3 se deduce que todo cuerpo es un dominio.*

Observación 2.2.6. *A partir de la Proposición 1.1.5 se puede probar, considerando el conjunto $A \setminus \{0\}$ que A es un anillo con división si y sólo si todos sus elementos no nulos son invertibles a izquierda (o a derecha).*

Ejemplos 2.2.7 (Anillos especiales)**.**

1. *El anillo de los enteros es un dominio. Los anillos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son cuerpos.*
2. *El subanillo de $\mathbb{R}$, $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ es un dominio.*
3. *El subanillo de $\mathbb{R}$, $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es un cuerpo.*
4. *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.*
5. *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.*

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

2.3. Construcciones con anillos y subanillos

Proposición 2.3.1. *Sea* $\{B_i\}_{i\in I}$ *una familia no vacía de subanillos de* A*. Entonces* $\bigcap_{i\in I} B_i$ *es un subanillo de* A*.*

Definición 2.3.2 (Subanillo generado)**.** *Si* $S \subset A$ *es un subconjunto de un anillo, el* subanillo generado *por* S *es* $\langle S\rangle := \bigcap\{B \mid B \text{ es subanillo de } A, B \supset S\}$*.*

Ejemplos 2.3.3 (Subanillo generado)**.**

- *Si* A *es un anillo y* $S = \{1\} \subset A$*, entonces el subanillo generado por* S *es el menor subanillo de* A *y se llama* anillo primo *de* A*.*
- *Si* $S = \{\sqrt{2}\} \subset \mathbb{R}$*, entonces* $\mathbb{Z}[\sqrt{2}]$ *es el subanillo generado por* S*.*

Observación 2.3.4. *Si* $S \subset A$ *es un subconjunto de un anillo y* B *es un subanillo de* A *que contiene a* S*, entonces* B *contiene al subanillo de* A *generado por* S*. En otras palabras el subanillo generado por* S *es el menor (con respecto a* $\subset$*) entre los subanillos de* A *que contienen a* S*.*

2.4. Series formales y polinomios

2.4.1. Series formales con coeficientes en un anillo A

Dado un anillo consideramos el conjunto de $A^{\mathbb{N}}$ 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 2.4.1.

- $(A^{\mathbb{N}}, +, \star, 0, \delta_0)$ *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 $\varphi_n(a)(k) = \begin{cases} a & si\ n = k \\ 0 & si\ no \end{cases}$ 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 $\displaystyle\sum_{n=0}^{\infty} a_n x^n$. 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 $f \star g$.

2.4.2. Polinomios con coeficientes en un anillo A

Dado $f \in A^{\mathbb{N}}$, definimos el *soporte* de f como $\text{sop}(f) = \{n \in \mathbb{N} \mid f(n) \neq 0\}$. El subconjunto $\{f \in A[[x]] \mid \sharp\text{sop}(f) < \infty\}$ 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).

2.4.3. Grado y valuación

Es claro que $\text{sop}(f) \subseteq \mathbb{N}$ tiene un elemento mínimo, y que si f es un polinomio entonces también $\text{sop}(f)$ tiene un elemento máximo.
Dado $f \in A[[x]]$ no nulo, se define la *valuación* de f como $\text{val}(f) = \text{mín}(\text{sop}(f))$. Además, el coeficiente $\text{val}(f)$-ésimo de f se dice el *coeficiente inicial* de f y se nota $\text{in}(f)$.
Si $p \in A[x]$ no nulo, se define el grado de p como $\text{gr}(p) = \text{máx}(\text{sop}(p))$. Además, el coeficiente $\text{gr}(p)$-ésimo de p se dice *coeficiente líder* de p y se nota $\ell(f)$.

Proposición 2.4.2. *Sean $f, g \in A[[x]]$ y $p, q \in A[x]$ todos no nulos. Entonces:*
Si $f + g \neq 0, \text{val}(f+g) \geq \text{mín}\{\text{val}(f), \text{val}(g)\}$, si $fg \neq 0, \text{val}(fg) \geq \text{val}(f) + \text{val}(g)$.
Si $p + q \neq 0, \text{gr}(p+q) \leq \text{máx}\{\text{gr}(p), \text{gr}(q)\}$, si $pq \neq 0, \text{gr}(pq) \leq \text{gr}(p) + \text{gr}(q)$.

Demostración. A partir de $\text{sop}(f+g) \subseteq \text{sop}(f) \cup \text{sop}(g)$ se prueban las desigualdades que involucran la suma de series.
A partir de $\text{sop}(fg) \subseteq \text{sop}(f) + \text{sop}(g)$ se prueban las que involucran al producto.
La primera inclusión sale de que $f(n) = g(n) = 0$ implica $(f+g)(n) = 0$.
La segunda inclusión sale de que $(f \star g)(n) \neq 0$ implica que existen $k, l \leq n$ tales que $k + l = n$ y $f(k)g(l) \neq 0$, de donde $f(k), g(l) \neq 0$. Es decir que si $n \in \text{sop}(fg)$, entonces $n = k + l$, con $k \in \text{sop}(f), l \in \text{sop}(g)$. □

Proposición 2.4.3. *Supongamos ahora que A es un dominio.*

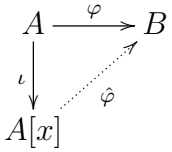
- *Si $f, g \in A[[x]]$ son no nulos, entonces $fg \neq 0$ y $\text{val}(fg) = \text{val}(f) + \text{val}(g)$.*
- *Si $p, q \in A[x]$ son no nulos, entonces $pq \neq 0$ y $\text{gr}(pq) = \text{gr}(p) + \text{gr}(q)$.*

Demostración.
- Basta observar que si A es un dominio entonces $\text{in}(f)\text{in}(g)$ es el menor coeficiente no nulo de fg y se da en el término $(\text{val}(f) + \text{val}(g))$-ésimo.

- Análogamente, basta observar que si A es un dominio entonces $\ell(p)\ell(q)$ es el mayor coeficiente no nulo de pq y se da en el término $(\mathrm{gr}(p)+\mathrm{gr}(q))$-ésimo. □

Corolario 2.4.4. *Si A es dominio, entonces $A[[x]]$ y $A[x]$ son dominios.*

Teorema 2.4.5 (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:



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 $\Im(\varphi)$ asegura la multiplicatividad de $\hat{\varphi}$. □

Observación 2.4.6. *En el caso particular en que B es conmutativo, la condición de que b conmuta con $\Im(\varphi)$ se verifica trivialmente.*

Ejemplo 2.4.7. *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 $\Im(\hat{\varphi}) = \mathbb{Z}[\sqrt{2}]$.

2.4.4. 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:

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

Los polinomios en dos variables con coeficientes en A corresponden al subanillo
$A[x,y] = \{f \in A[[x,y]] \mid \sharp\text{sop}(f) < \infty\}$. 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 $A^{\mathbb{N}^n}$.

2.5. Ideales

Definición 2.5.1. *Se considera un anillo A y un subconjunto $I \subseteq A$ tal que $(I,+,0) \leq (A,+,0)$. 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 2.5.2.
- *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 2.5.3.
- *Para cada natural n, se tiene $n\mathbb{Z} \lhd \mathbb{Z}$. Además, como se vio en el práctico, estos son los únicos subgrupos, y por lo tanto los únicos ideales, de $\mathbb{Z}$.*
- *Si $\varphi : A \to B$ es un morfismo de anillos, entonces $Ker(\varphi) \lhd A$.*
- *Para cualquier anillo A,*

$$\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in A \right\} \lhd_l M_2(A), \quad \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in A \right\} \lhd_r M_2(A).$$

- *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.*

Proposición 2.5.4. *Sea $\{J_i\}_{i \in I}$ una familia no vacía de ideales de A. Entonces $\bigcap_{i \in I} J_i$ es un ideal de A.*

Definición 2.5.5 (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 $S = \{a_1, a_2, \ldots, a_n\}$, 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 2.5.6. *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 2.5.7. *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 si y sólo si A no contiene ideales propios 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 2.5.2. 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 2.5.8. *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 $(E, \leq)$ un conjunto no vacío parcialmente ordenado (i.e. $\leq$ 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 2.5.9. *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 $\mathcal{F} \neq \emptyset$. 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 $I \subset D$.
- $D \neq A$: si $D = A$, entonces $1 \in D$, de donde $1 \in I_\lambda$ para algún $\lambda \in \Lambda$, lo cual es absurdo pues $I_\lambda \neq A$.

Aplicando el lema de Zorn a la familia $\mathcal{F}$, se tiene que existe un elemento maximal (respecto de la inclusión), llamémosle $M \in \mathcal{F}$. Por construcción, M es un ideal maximal tal que $I \subseteq M$. □

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

Corolario 2.5.10. *Si $A \neq \{0\}$ es un anillo, existen ideales biláteros (a izquierda, a derecha) maximales en A.*

Observación 2.5.11. *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 2.5.12. *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. Queda como ejercicio. □

Proposición 2.5.13. *Sea* $f : A \to B$ *morfismo de anillos. Si* $H \lhd B$*, entonces* $f^{-1}(H) \lhd A$*. Si además* f *es sobreyectiva y* $K \lhd A$*, entonces* $f(K) \lhd B$*.*

Demostración. Sea $H \lhd B$. Sabemos que $f^{-1}(H) \leq A$. 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 $f(K) \leq B$. Además, si $x \in K$ y $b \in B$, como f es sobreyectiva, 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 $ax, xa \in K$. □

2.6. Anillos 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 2.6.1. *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, $ab \equiv a'b' \pmod{I}$. □

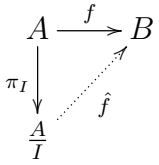
A partir de esto, es inmediato el siguiente resultado.

Teorema 2.6.2. *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 sobreyectiva.*

Teorema 2.6.3 (Propiedad Universal del Cociente)**.** *Sea $f : A \to B$ un morfismo de anillos y sea $I \lhd A$. Si $I \leq Kerf$, existe un único morfismo $\hat{f} : \frac{A}{I} \to B$ que hace conmutar el siguiente diagrama:*

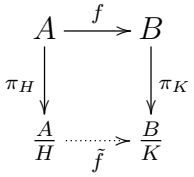


Además, se tiene $\Im \hat{f} = \Im f$ y $Ker\hat{f} = \frac{Kerf}{I}$.

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 2.6.4 (Teoremas de isomorfismo)**.** *Sea A un anillo.*

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



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

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

que preserva la inclusión.

Demostración. La prueba del resultado análogo para grupos puede adaptarse fácilmente a este contexto, usando la proposición 2.5.13. □

Es inmediato el siguiente corolario.

Corolario 2.6.6. *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 2.6.7. *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 $\Im\varepsilon_a = \mathbb{R}$ y que

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

Por otro lado $f(a) = 0 \Leftrightarrow f = (x-a)q$ para algún $q \in \mathbb{R}[x]$. En conclusión $Ker\varepsilon_a = (x-a)$. 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 sobreyectiva: dado $a + ib \in \mathbb{C}$ basta tomar $f = a + bX$. Se tiene que

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

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 $Ker\varepsilon_i = (X^2+1)$. 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.

2.7. Ideales maximales e ideales primos

Definición 2.7.1. *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 2.7.2 (Ideales primos). *1. $p\mathbb{Z} \lhd \mathbb{Z}$ es primo. Más aún, son equivalentes para un entero positivo m:*

(i) $m\mathbb{Z}$ es primo,

(ii) $m\mathbb{Z}$ es maximal,

(iii) m es un número primo.

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).

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 2.7.3. *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 2.6.6),
- B es un anillo con división si y sólo si no tiene ideales a izquierda si y sólo si no tiene ideales a derecha (proposición 2.5.7).

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 4.2.12 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. □

Se deduce el siguiente corolario.

Corolario 2.7.4. *Sea A un anillo conmutativo.*

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

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

Observación 2.7.5. *A partir de los resultados anteriores y del ejemplo 2.7.2, 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.

- *Si consideramos el morfismo $\varphi_n : \mathbb{Z}[x] \to \mathbb{Z}$ tal que $(\varphi_n)_{|\mathbb{Z}} = id_{\mathbb{Z}}$ y $\varphi_n(x) = n$, como $\Im\varphi_n = \mathbb{Z}$ es un dominio que no es un cuerpo, se deduce que $Ker\varphi_n \lhd \mathbb{Z}[x]$ es un ideal primo que no es maximal. En particular $Ker\varphi_0 = (x) = \{p \in \mathbb{Z}[x] \mid p(0) = 0\}$ 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 2.7.6. *Sea A un anillo. Llamémosle χ al único morfismo de anillos $\mathbb{Z} \to A$, es decir $\chi(n) = n \cdot 1_A = \overbrace{1_A + \cdots + 1_A}^{n \text{ veces}}$. El núcleo de χ es $Ker\chi = \{n \in \mathbb{Z} : n \cdot 1_A = 0\} = m\mathbb{Z}$ para algún $m \in \mathbb{N}$.[2] Definimos la* característica *de A como m. Notamos 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 $\frac{\mathbb{Z}}{m\mathbb{Z}} \simeq \Im\chi \subset A$. Observar que si $\varphi : R \to S$ es un morfismo de anillos y R es un anillo conmutativo, entonces $\Im\varphi$ es un subanillo conmutativo de B. En este caso tenemos que $\Im\chi \subset A$ 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 $\Im\chi$ 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.

2.8. 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 $\mathbb{Z} \times \mathbb{Z} \setminus \{0\} = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}$ y se define la relación:

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

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:

[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.

1. se puede considerar en lugar de $\mathbb{Z}$ un dominio cualquiera A y dar una estructura de cuerpo a un cociente del conjunto $A \times A \setminus \{0\}$: 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 2.8.1. *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 2.8.2 (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 $S = A \setminus P$ es multiplicativo,

4. en particular, si A es un dominio, $A \setminus \{0\}$ 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 2.8.3. *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 2.8.4. *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 *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 2.8.5. *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 $S^{-1}A$.

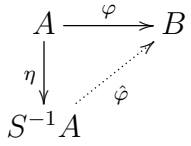
Proposición 2.8.6. *Sean A un anillo conmutativo y S un conjunto multiplicativo en A. La función*

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

es un morfismo de anillos.

Demostración. Queda como ejercicio. □

Proposición 2.8.7 (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:*



Demostración. Queda como ejercicio (haremos la demostración de un caso particular en la proposición 2.8.10). □

Observación 2.8.8.

- *Para cada elemento $x \in A$ definimos su* anulador *como el conjunto* $\mathrm{Ann}_A(x) = \{a \in A \mid ax = 0\}$. *Observar que* $\mathrm{Ann}_A(x) = \{0\}$ *si y sólo si x no es divisor de cero. En particular si A es un dominio entonces* $\mathrm{Ann}_A(x) = \{0\}$ *para todo $x \in A, x \neq 0$.*

- *El morfismo η_S es inyectivo si y sólo si* $\mathrm{Ann}_A(s) = \{0\}$ $\forall s \in S$. *En efecto,*

  $$\frac{a}{1} = 0 \iff \exists s \in S \text{ tal que } as = 0 \iff \exists s \in S \text{ tal que } a \in \mathrm{Ann}_A(s).$$

  Por lo tanto $Ker\eta_S = \bigcup_{s \in S} \mathrm{Ann}_A(s)$ *de donde se deduce la observación.*

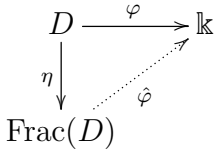
- *En particular, si A es un dominio, entonces η_S es inyectiva si y sólo si $0 \notin S$.*

- *Si $0 \notin S$, hay elemento invertible en $S^{-1}A$. Más precisamente, si $a \in A^\times$ o $a \in S$, se tiene que $\eta_S(a) \in (S^{-1}A)^\times$. En efecto, $\frac{a^{-1}}{1}$ y $\frac{1}{a}$ son los respectivos inversos de $\eta_S(a) = \frac{a}{1}$.*

Proposición-Definición 2.8.9. *Sean A un dominio y $S = A \setminus \{0\}$. 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 morfismo canónico (inyectivo) $A \to \mathrm{Frac}(A)$.*

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



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

1. $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ *(ver observación 2.8.3.4),*
2. $\mathrm{Frac}(\Bbbk) = \Bbbk$.
3. *Se define el anillo de las* funciones racionales *con coeficientes en $\Bbbk$ en indeterminadas $x_1, \ldots, x_n$ como*

$$\Bbbk(x_1, \ldots, x_n) := \mathrm{Frac}(\Bbbk[x_1, \ldots, x_n]) = \left\{ \frac{f}{g} \mid f, g \in \Bbbk[x_1, \ldots, x_n], g \neq 0 \right\},$$

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 $\Bbbk((x_1, \ldots, x_n))$ 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 2.8.12. *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 $S = A \setminus P$.*

Definición 2.8.13. *Un anillo conmutativo se dice* local *si tiene un único ideal maximal.*

Ejemplos 2.8.14.

1. *Sea $I \subset \mathbb{R}$ un intervalo abierto que contiene a 0. Consideremos, en el anillo $C(I)$ de funciones continuas de I en $\mathbb{R}$, la relación de equivalencia definida por $f \sim g$ sii existe un entorno de $\{0\}$ donde f y g coinciden. En otros términos, si consideramos el ideal J de las funciones que valen 0 en algún entorno de 0, $\sim$ es la relación de congruencia módulo J. El anillo cociente se llama* anillo de semillas *(o* de gérmenes*)* alrededor de 0 *y es un anillo local. En efecto, su único ideal maximal es $M = \{\overline{f} \mid f(0) = 0\}$.*

2. *El ejemplo anterior se generaliza remplazando I por un espacio topológico cualquiera y 0 por un punto del espacio, o remplazando I por una variedad diferenciable, 0 por un punto de la variedad, y tomando funciones diferenciables en vez de funciones continuas.*

3. *El anillo $\Bbbk[[x]]$ es local. Su único ideal maximal es (x).*

4. *Todo cuerpo es un anillo local.*

Proposición 2.8.15. *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. *$A \setminus A^\times$ 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 $A \setminus A^\times$ 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 $A \setminus A^\times \lhd A$.

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

Proposición 2.8.16. *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 2.8.17. *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 $\left\{ \frac{a}{b} \mid a \text{ es múltiplo de } p, b \text{ no es múltiplo de } p \right\}$.

Capítulo 3

Divisibilidad en dominios

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

3.1. Generalidades

Definición 3.1.1. *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 3.1.2. *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 3.1.3. *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 $a \mid c$.

Proposición 3.1.4. *Sea $\sim$ la relación en D definida por $a \sim b$ si y sólo si existe $u \in D^\times$ tal que $a = ub$. Entonces $\sim$ es una relación de equivalencia.*

Demostración. Sale de que $(D^\times, \cdot, 1)$ es un grupo. □

Definición 3.1.5. *Sean $a, b \in D$ y $\sim$ como en la proposición anterior. Decimos que a y b* son asociados *si $a \sim b$.*

Proposición 3.1.6. *Si $a, b \in D$, se tiene $a \sim b$ si y sólo si $a \mid b$ y $b \mid a$.*

Demostración. Si $a \sim b$, existe $u \in D^\times$ tal que $a = ub$ y por tanto se tiene también $b = u^{-1}a$.

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 $a = xb \sim b$. □

Observación 3.1.7. *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 3.1.8. *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. Queda como ejercicio. □

Definición 3.1.9. *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 3.1.10.
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 3.1.11.
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 $x^2 \mid x^3 x^3 = x^2 x^4$ pero $x^2 \not| x^3$.*

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 3.1.12. *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. Queda como ejercicio. □

Definición 3.1.13. *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*

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

Observación 3.1.14. 1. *En un dominio cualquiera no tiene por qué existir el máximo común divisor. En efecto, en el ejemplo 3.1.11.2, 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 $mcd(a, b)$ 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 $mcd(a, b) = d$ en lugar de $d \in mcd(a, b)$.

Proposición 3.1.15. 1. *Si $a, b \in D$ son tales que $a \mid b$, entonces $mcd(a, b) = a$. En particular $mcd(a, 0) = a$ y $mcd(a, b) = 1$ siempre que $a \in D^\times$.*

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

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 $mcd(a, b) = a$ y como $a \sim 1$, entonces $mcd(a, b) = 1$.

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

Definición 3.1.16. *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 $d = mcd(a_1, \ldots, a_n)$ si*

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

Observación 3.1.17. *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 $mcd(a_1, a_2, \ldots, a_n) = mcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$.

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

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

3.1.1. Dominios de factorización única

Definición 3.1.18. *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 3.1.19. *1. La unicidad de la factorización implica que se 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 $\sigma : \{1, 2, \ldots, n_0\} \to \{1, 2, \ldots, m\} \setminus \{j\}$ *inyectiva y extendiéndola a* $\overline{\sigma} : \{1, 2, \cdots, n_0 + 1\} \to \{1, 2, \ldots, m\}$ *mediante* $\overline{\sigma}(i) = \sigma(i), \forall i \leq n_0$, $\overline{\sigma}(n_0 + 1) = j$, *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* $n \leq m$, *y luego intercambiando los roles de los* p_i *y los* q_j *se deduce* $m \leq n$ *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* $a = q_1 q_2 \cdots q_m$, *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 3.1.20. *Sean* D *un DFU y* $a, b \in D$ *no nulos y no invertibles. Si* $a = p_1 p_2 \cdots p_n$ *y* $b = q_1 q_2 \cdots q_m$, *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 $x = r_1 r_2 \cdots r_t$, se tiene

$$p_1 p_2 \cdots p_n r_1 r_2 \cdots r_t = q_1 q_2 \cdots q_m$$

y se deduce la tesis, a partir de la Observación 3.1.19.

Recíprocamente si existe tal σ se tiene que

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

para cierto $x \in D^\times$. □

Proposición 3.1.21. *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 $i \in \{1,\dots,n\}$ tal que $p \sim p_i$ o existe $j \in \{1,\dots,m\}$ 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 $p_1p_2\dots p_n = q_1q_2\dots q_m$, con $p_i, q_j \in D$ irreducibles $\forall i \leq n, j \leq m$. Para cada $i \leq n$, como p_i es primo y divide al término de la derecha, se tiene que $p_i \mid q_j$ para cierto $j \leq m$. Como además q_j es irreducible, se deduce $p_i \sim q_j$. □

Proposición 3.1.22. *Si D es un DFU, entonces existe $mcd(a,b)$ 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 $i \leq m$, 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 $i \leq m$, $\gamma_i = \text{mín}\{\alpha_i, \beta_i\}$, entonces es fácil (y queda como ejercicio) verificar que

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

Definición 3.1.23. *Si $a, b \in D$ son no simultáneamente nulos, decimos que a y b son* primos entre sí *si existe $mcd(a,b)$ y $mcd(a,b) = 1$.*

Proposición 3.1.24 (Lema de Euclides)**.** *Sean a, b, c elementos no nulos en un dominio factorial. Si $a \mid bc$ y $mcd(a,b) = 1$, 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, $mcd(a,b) = 1$, 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 $a \mid c$. □

3.1.2. Dominios a ideales principales

Definición 3.1.25. *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 3.1.26.

- *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 $I = \{p \in \Bbbk[x] \mid p(0)$ 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[1]*. 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 $gr(g) \geq gr(f)$ se tiene $g = fq + r$, con $gr(r) < gr(f)$ 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 3.1.27. *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 $M = D$. □

Corolario 3.1.28. *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. □

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

Queremos probar que todo dominio a ideales principales es un dominio de factorización única. 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 3.1.29). 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.

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 3.1.33).

Proposición 3.1.29. *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 $I = \bigcup_{n\geq 0} I_n$. 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 $n \geq N$.
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 $x \in I \setminus M$ 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 3.1.30. *Un anillo conmutativo que verifica una de las condiciones de la Proposición 3.1.29 se dice* noetheriano.

Ejemplos 3.1.31.

- *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 3.2.23) 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 3.1.32. *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.*

Todo DIP es un DFU

Teorema 3.1.33. *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 $\mathcal{F} = \emptyset$. 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 3.1.21.
Recordamos que puede deducirse $n = m$ como se muestra en la observación 3.1.19.2. □

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 3.1.34. *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 3.1.35. *Sean D un dominio a ideales principales y $a, b \in D$ no simultáneamente nulos. Entonces:*

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

Demostración. La existencia de $mcd(a, b)$ 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 $ax + by = d$. □

3.2. Divisibilidad en anillos de polinomios

En lo queda del capítulo D será un dominio y $\Bbbk$ denotará al cuerpo de fracciones de D.

Polinomios como funciones

Recordemos que la propiedad universal de los anillos de polinomios da lugar a la existencia, para cada $a \in D$, del morfismo de anillos *evaluación en a* $\varepsilon_a : D[x] \to D$ que verifica $\varepsilon_a(d) = d$ para todo $d \in D$, y $\varepsilon_a(x) = a$.
A partir de ahora, adoptaremos, para $p \in D[x]$ y $a \in D$, 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 $p, q \in D[x]$. Además si $p = d \in D$ es un polinomio constante entonces $p(a) = d$ para todo $a \in D$.
Haciendo variar $a \in D$, se obtiene una función

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

que resulta ser un morfismo de anillos si ponemos en el conjunto de funciones D^D 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 $f(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{si no} \end{cases}$ 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:

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

De hecho vamos a probar 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.

Definición 3.2.1. *Sea $p \in D[x]$. Un elemento $a \in D$ se dice* raíz *de p si $p(a) = 0$.*

Observación 3.2.2. *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 $gr(r) \leq gr(t) - 1$.*
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 $r \in D$.

Proposición 3.2.3 (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 3.2.4 (Teorema del factor)**.** *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 3.2.5. *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 $c_1, c_2, \ldots$ 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 $c_1, \ldots, c_m$ de p, el polinomio $g_m = (x - c_1)(x - c_2) \cdots (x - c_m)$ divide a p. Pero $grg_m = m$, de donde $m \leq n$. □

Corolario 3.2.6. *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 $K[x]^\times = K^\times = K \setminus \{0\}$. Por el corolario 3.2.4 esto ocurre si y sólo si f tiene una raíz en K. □

Proposición 3.2.7. *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 $\varphi(p) \neq 0$. □

Criterios de irreducibilidad

Definición 3.2.8. *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 $cont(f) = mcd(a_n, \ldots, a_1, a_0)$. Decimos que f es* primitivo *si $cont(f) = 1$.*

Ejemplo 3.2.9.

- *Todo polinomio mónico es primitivo.*
- *$f = 2x + 3$ es primitivo en $\mathbb{Z}[x]$, pero $g = 2x + 4$ no lo es, de hecho $cont(g) = 2 \not\sim 1$.*

Observación 3.2.10.

1. *Notar que hacemos el mismo abuso de notación que para el máximo común divisor. Si bien $cont(f)$ 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 $cont(af) = acont(f)$. Además siempre existe un (único a menos de multiplicar por un invertible de D) polinomio $\overline{f} \in D[x]$ tal que $f = cont(f)\overline{f}$. Este polinomio $\overline{f}$ resulta obviamente primitivo.*
3. *Se puede definir "polinomio primitivo" en un dominio donde no necesariamente existe el mcd, como un polinomio $f \in D[x]$ tal que no existe un elemento de D no invertible que divida a todos los coeficientes de f a la vez.*

Lema 3.2.11 (Lema de Gauss)**.** *Sean D un dominio de factorización única y $f, g \in D[X]$. Entonces:*

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

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, $p \nmid cont(f)$ y $p \nmid cont(g)$, por lo que existen $i \in \{0, \ldots, n\}, j \in \{0, \ldots, m\}$ tales que a_i y b_j no son múltiplos de p. Podemos entonces considerar $\bar{\imath} := \min\{i \mid p \nmid a_i\}$ y $\bar{\jmath} = \min\{j \mid p \nmid b_j\}$. Ahora bien, sea $k = \bar{\imath} + \bar{\jmath}$; el término k-ésimo de fg es

$$a_0 b_k + a_1 b_{k-1} + \cdots + a_{\bar{\imath}} b_{\bar{\jmath}} + \cdots + a_{k-1} b_1 + a_k b_0.$$

Tenemos tres tipos de sumandos $a_i b_j$ en el término de arriba:

- sumandos en que $i < \bar{\imath}$: $p \mid a_i$ y por tanto el sumando es múltiplo de p;

- sumandos en que $j < \bar{\jmath}$: $p \mid b_j$ y por tanto el sumando es múltiplo de p:
- el sumando $a_{\bar{\imath}}b_{\bar{\jmath}}$: $p \nmid a_{\bar{\imath}}$ y $p \nmid b_{\bar{\jmath}}$, 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 $cont(fg) = 1$.

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

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

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

Lema 3.2.12. *Sean D un dominio y $\Bbbk$ su cuerpo de fracciones.*

1. *Todo polinomio $g \in \Bbbk[x]$ puede escribirse como $g = \frac{1}{a}g''$ con $a \in D\backslash\{0\}$, $g'' \in D[x]$.*

2. *Si además D es de factorización única y $f \in D[x]$ 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. 1. Dados $a_1, a_2, \ldots, a_n \in \Bbbk$, existen $a, a'_1, a'_2, \ldots, a'_n \in D$, $a \neq 0$ tales que $a_i = \frac{a'_i}{a}$ para todo $i \in \{1, \ldots, n\}$.

En efecto, si para cada $i \in \{1, \ldots, n\}$ escribimos $a_i = \frac{n_i}{d_i}$, alcanza con tomar $a = d_1 d_2 \cdots d_n$ y $a'_i = \frac{n_i a}{d_i}$. Se tiene entonces $a_i = \frac{n_i}{d_i} = \frac{n_i a}{d_i a} = \frac{a'_i}{a}$ para todo $i \in \{1, \ldots, n\}$.

Si los a_i son los coeficientes de g, entonces $g = \frac{1}{a}g''$ donde los coeficientes de g'' son los a'_i.

2. Si aplicamos la parte anterior a g y h y llamamos a y b a los respectivos elementos de D, obtenemos la igualdad en D: $abf = g''h''$. Tomando contenidos de ambos lados, se deduce que $ab \mid cont(g'')cont(h'')$ y por tanto se pueden ir cancelando en $abf = g''h''$ los irreducibles que aparecen en la descomposición de ab, obteniendo $f = g'h'$, donde g' y h' se obtienen a partir de g'' y h'' diviendo por algún elemento de D. $\square$

Teorema 3.2.13 (Criterio de irreducibilidad de Gauss)**.** [2] *Sean D un dominio de factorización única y $\Bbbk$ su cuerpo de fracciones. 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 $g \in \Bbbk^\times \cap D[x] = D \setminus \{0\}$. Pero en ese caso $cont(f) = gcont(h)$, y como $cont(f) = 1$ 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 $f = cont(f)\overline{f}$ 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 3.2.12, 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 $g' \in D\setminus\{0\}$, 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. □

Proposición 3.2.14 (Criterio de la raíz racional)**.** *Sea D un dominio de factorización única y $\Bbbk$ su cuerpo de fracciones. 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 $mcd(p, q) = 1$. 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 $a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0$ 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 $mcd(p, q) = 1$, entonces $mcd(p, q^n) = 1$. El lema de Euclides (Proposición 3.1.24) nos da que $p \mid a_0$. Análogamente $q \mid a_n$. □

Corolario 3.2.15. *Sea D un dominio de factorización única y $\Bbbk$ su cuerpo de fracciones. Si $f \in D[X]$ es un polinomio mónico y $\alpha \in \Bbbk$ es raíz de f, entonces $\alpha \in D$.*

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

Ejemplo 3.2.16. *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 el corolario 3.2.6, 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).*

Proposición 3.2.17 (Criterio de irreducibilidad de Eisenstein)**.** *Sean D un dominio de factorización única, $\Bbbk$ su cuerpo de fracciones y 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 $\Bbbk[x]$.

Demostración. Supongamos $f = gh \in D[x]$ con $g, h \in \Bbbk[x]$. Veamos que $g \in \Bbbk \setminus \{0\}$ o $h \in \Bbbk \setminus \{0\}$. 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 $p \not| b_i c_0$ 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 $gr(h) = 0$, es decir $h \in \Bbbk \setminus \{0\}$. □

Ejemplos 3.2.18. *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.

Lema 3.2.19. *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 $a \mid cont(f)cont(g)$ y por tanto $a \mid cont(f)$ o $a \mid cont(g)$. 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 $fh = ag$, con $a \in D$. Tomando contenidos y usando que f es primitivo, se deduce que $cont(h) = acont(g)$, por lo que se tiene para cierto $h' \in D[x]$, $acont(g)h'f = ag$ en $D[x]$. Como D es un dominio, se deduce $cont(g)h'f = g$ y por lo tanto $f \mid g$ en $D[x]$. □

Teorema 3.2.20. *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 $f = cont(f)\bar{f}$, con $\bar{f} \in D[x]$ no nulo y primitivo.
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 $a \in D \setminus \{0\}$. Se tiene entonces que si $\bar{f}$ no es invertible, es de la forma $\bar{f} = \frac{1}{d}h_1h_2 \dots h_n$ con $d \in D \setminus \{0\}, h_i \in D[x]$ irreducible en $\Bbbk[x]$, para todo $i \in \{1, \dots, n\}$. Para cada i podemos escribir $h_i = cont(h_i)h_i'$ con h_i' primitivo. Se tiene entonces:

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

por lo que $f = \frac{cont(h_1)\cdots cont(h_n)}{d}cont(f)h_1'h_2' \dots h_n'$.
Se deduce la existencia de la descomposición factorial en irreducibles.
Para la unicidad, por la Proposición 3.1.21, alcanza con probar que todo irreducible de $D[x]$ es primo. Sea $f \in D[x]$ irreducible.
Si $gr(f) = 0$, 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 3.2.19 que es primo en $D[x]$.
Si $gr(f) > 0$, f es irreducible como elemento en $\Bbbk[x]$ y por tanto primo. Se deduce usando la otra parte del Lema 3.2.19 que es primo en $D[x]$. □

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

Observación 3.2.22. *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. El siguiente teorema permite deducir que los anillos de polinomios en finitas variables $D[x_1, x_2 \cdots, x_n]$ sí son noetherianos siempre que D lo sea.

Teorema 3.2.23 (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 $I_n = \{a \in A \mid \text{ existe } f \in J \text{ con } gr(f) = n, a = \ell(f)\} \cup \{0\}$: 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 $i \leq \bar{n}$, 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 $gr(f)$ que f está generado por los f_{ij}. Si $gr(f) = 0$, entonces $f \in I_0$ y está generado por $\{f_{0j} \mid j \leq k_0\}$. 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 $gr(f) = n$.
Si $n \leq \bar{n}$, $l(f) = \sum_j \lambda_j a_{nj} \in I_n$, por lo que el polinomio $f - \sum \lambda_j f_{nj} \in J$ es nulo o de grado estrictamente menor que n, por lo que está generado por los f_{ij} (con $i \leq n$). Se deduce que f también lo está. Si $n > \bar{n}$, $l(f) = \sum_j \lambda_j a_{\bar{n}j}$ y el polinomio $f - \sum x^{n-\bar{n}} \lambda_j f_{\bar{n}j} \in J$ es nulo o de grado estrictamente menor que n, por lo que se deduce otra vez que f está generado por los f_{ij}. □

Capítulo 4

Módulos

Durante todo el capítulo A denotará un anillo cualquiera.

4.1. Generalidades

Definición 4.1.1. *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 4.1.2. *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 4.1.3.

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 $End(M) = \{f : M \to M \mid f$ es morfismo de grupos$\}$ es un anillo con la composición. Las igualdades (2), (3) y (4) pueden interpretarse como que la función $F : A \to End(M)$ definida por $F(a) = \varphi_a$ es un morfismo de anillos.*[1]

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

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.*

   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,* $0 \cdot m = (0 + 0) \cdot m = 0 \cdot m + 0 \cdot m$ *y* $(-1) \cdot m + 1 \cdot m = 0 \cdot m = 0$.

Veamos más ejemplos.

Ejemplos 4.1.4. 1. *Si* $A = \Bbbk$ *es un cuerpo, entonces un* $\Bbbk$*-módulo a izquierda es exactamente un* $\Bbbk$*-espacio vectorial.*

2. *Si* A *es un anillo y consideramos el grupo abeliano* $A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A\}$, *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* $\Bbbk$ *es un cuerpo y* $X \in M_n(\Bbbk)$, *se tiene que el grupo abeliano* $\Bbbk^n$ *es un* $\Bbbk[x]$*-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 $S \neq \emptyset$ 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 4.1.3.4. Además, a menudo notaremos am en lugar de $a \cdot m$, para $a \in A, m \in M$.

Definición 4.1.5. *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 4.1.6.

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 4.1.7. *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 $End_A(M)$ al conjunto de endomorfismos de M.*

Observación 4.1.8. 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 $End_A(M)$ 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 4.1.9. *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, $Ker f = f^{-1}(\{0\}) \subseteq M$ e $Im f = f(M) \subseteq N$ son submódulos.*

Demostración. Sea $H \subseteq N$. Sabemos que $f^{-1}(H) \leq M$. 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 $f(K) \leq N$. 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. □

4.2. Construcciones con módulos y submódulos

Definición 4.2.1 (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, $sop(m) = \{j \in I \mid m_j \neq 0\}$, *y es fácil ver que el subconjunto*

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

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.*

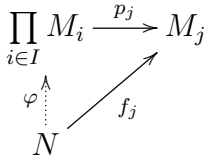
Observación 4.2.2. *1. Si en la definición de arriba el conjunto* I *es finito, la suma directa y el producto directo coinciden.*

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

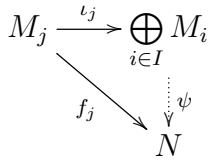
Proposición 4.2.3 (Propiedad universal de la suma directa y del producto directo)**.** [2] *Sea* $\{M_i\}_{i\in I}$ *una familia de* A*-módulos.*

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* $j \in I$*:*



[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.

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 $j \in I$:*



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.

Definición 4.2.4 (Submódulo generado)**.** *Sea M un A-módulo y $S \subseteq M$ un subconjunto. El* submódulo generado *por S es $\langle S\rangle := \bigcap\{N \mid N$ es submódulo de $M, N \supseteq S\}$.*

Observación 4.2.5. 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 $S = \emptyset$, entonces $\langle S\rangle = \{0\}$.*

3. *Si $S \neq \emptyset$, $\langle S\rangle = \left\{\sum_{i\in I} a_i m_i \mid I$ es un conjunto finito, $a_i \in A$, $m_i \in S\ \forall i \in I\right\}$.*

Definición 4.2.6. *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 4.2.7. *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 4.2.8. *1. Es claro que*

$$\sum_{i\in I} M_i = \left\{ \sum_{i\in I} m_i \mid I \text{ es un conjunto finito}, m_i \in M_i, \forall i \in I \right\}.$$

2. A partir de las inclusiones $inc_j : M_j \to M$ y usando la propiedad universal de la suma directa, se tiene un (único) morfismo $\varphi : \bigoplus_{i\in I} M_i \to \sum_{i\in I} M_i$ tal que $\varphi \circ \iota_j = inc_j$. 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 $m \in \sum_{i\in I} M_i$ 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. Como $\sum_{i\in I} M_i \subseteq M$, podemos extender el codominio de φ y considerar $\bar{\varphi} : \bigoplus_{i\in I} M_i \to M$.*

a) *Para cada $m \in M$, existe una única familia $\{m_i \in M_i \mid i \in I\}$ de soporte finito tal que $m = \sum_i m_i$.*

b) *$M \cong \bigoplus_{i\in I} M_i$ via $\bar{\varphi}$,*

c) *$M = \sum_{i\in I} M_i$ y $M_i \cap \sum_{j\neq i} M_j = \{0\}$ para todo $i \in I$.*

(La prueba la hicimos en clase y es análoga a la que se hace para espacios vectoriales).

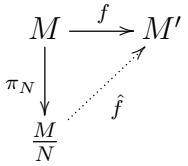
La noción de grupo cociente en grupos abelianos se extiende al contexto de A-módulos. En efecto, si $N \subseteq M$ es un submódulo, como en particular es un subgrupo, se tiene que $\frac{M}{N}$ es un grupo abeliano. El siguiente lema asegura que la acción de A induce una acción en el cociente.

Lema 4.2.9. *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. □

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



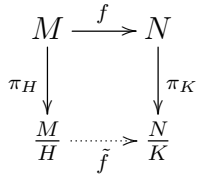
Además, se tiene $Im\hat{f} = Imf$ y $Ker\hat{f} = \frac{Kerf}{N}$.

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. □

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

Corolario 4.2.11 (Teoremas de isomorfismo)**.** *Sea M un A-módulo.*

1. *Si $f : M \to N$ es un morfismo de A-módulos, entonces $\frac{M}{Kerf} \cong Imf$.*
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:*



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. □

Teorema 4.2.12. *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 4.1.9. □

4.3. Sucesiones exactas

Definición 4.3.1.

- *Sea* $M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} M_n \xrightarrow{\varphi_n} M_{n+1}$ *una sucesión de A-módulos y morfismos de A-módulos. Decimos que es una* sucesión exacta *si $Im\varphi_i = Ker\varphi_{i+1}$ para todo $i = 1, \ldots, n-1$.*

- *Sea* $\cdots \xrightarrow{\varphi_{n-2}} M_{n-1} \xrightarrow{\varphi_{n-1}} M_n \xrightarrow{\varphi_n} M_{n+1} \xrightarrow{\varphi_{n+1}} \cdots$ *una sucesión de A-módulos y morfismos de A-módulos. Decimos que es una* sucesión exacta *si $Im\varphi_n = Ker\varphi_{n+1}$ para todo $n \in \mathbb{Z}$.*

- *Una* sucesión exacta corta *es una sucesión exacta* $0 \longrightarrow M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0$ *donde $0 \to M_1$ y $M_3 \to 0$ son los únicos morfismos posibles.*

Observación 4.3.2. $0 \longrightarrow M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \longrightarrow 0$ *es una sucesión exacta corta si y sólo si se cumplen las siguientes condiciones:*

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

Ejemplos 4.3.3.

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*

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

es una sucesión exacta corta.

3. *Definimos el* conúcleo *de un morfismo* $\varphi : M_1 \to M_2$ *como* $Coker\varphi := M_2/Im\varphi$. *Entonces*

$$0 \longrightarrow Ker\varphi \overset{\subset}{\longrightarrow} M_1 \xrightarrow{\varphi} M_2 \xrightarrow{\pi} Coker\varphi \longrightarrow 0$$

es una sucesión exacta.

4. *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 4.3.4 (Lema de los tres)**.** [3] *Consideremos el siguiente diagrama conmutativo cuyas filas son sucesiones exactas cortas:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\varphi'} & N' & \xrightarrow{\psi'} & P' & \longrightarrow & 0 \end{array}$$

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. [4]

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 $n \in Ker\psi = Im\varphi$ 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.

[3] Este lema se generaliza al *lema de los cinco*: es el ejercicio 9 del práctico 7.

[4] Esta demostración es un ejemplo arquetípico de *diagram chasing*.

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 $\beta(n)-n' \in Ker\psi' = Im\varphi'$ 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 $n' \in Im\beta$. En conclusión, β es sobreyectiva.

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

Definición 4.3.5. *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*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\varphi'} & N' & \xrightarrow{\psi'} & P' & \longrightarrow & 0 \end{array}$$

con α, β *y* γ *isomorfismos.*

Observación 4.3.6. *Toda sucesión exacta corta* $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ *es isomorfa a una como la del ejemplo 4.3.3.1: en efecto,*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle=} & & \downarrow{\scriptstyle\cong} & & \\ 0 & \longrightarrow & Im\varphi & \hookrightarrow & N & \xrightarrow{\pi} & N/Im\varphi & \longrightarrow & 0 \end{array}$$

Proposición 4.3.7. *Consideremos una sucesión exacta corta* $E:\ 0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P -$ *Son equivalentes:*

1. *Existe un morfismo* $\nu : P \to N$ *tal que* $\psi \circ \nu = id_P$, $0 \longrightarrow M \xrightarrow{\varphi} N \underset{\nu}{\overset{\psi}{\rightleftarrows}} P \longrightarrow 0$

2. *Existe un morfismo* $\eta : N \to M$ *tal que* $\eta \circ \varphi = id_M$, $0 \longrightarrow M \underset{\eta}{\overset{\varphi}{\rightleftarrows}} N \xrightarrow{\psi} P \longrightarrow 0$

3. *Existe un isomorfismo* $\beta : N \to M \oplus P$ *que hace conmutar el siguiente diagrama:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id_M} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle id_P} & & \\ 0 & \longrightarrow & M & \xrightarrow{\iota_M} & M \oplus P & \xrightarrow{\pi_P} & P & \longrightarrow & 0 \end{array}$$

Demostración. (1 $\Rightarrow$ 3) Tenemos $\nu : P \to N$ tal que $\psi \circ \nu = id_P$. 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:

$$\begin{array}{ccccc} M & \xrightarrow{\iota_M} & M \oplus P & \xleftarrow{\iota_P} & P \\ & {\scriptstyle \varphi} \searrow & \downarrow{\scriptstyle \delta} & \swarrow {\scriptstyle \nu} & \\ & & N & & \end{array}$$

En vista del lema 4.3.4, δ debe ser un isomorfismo. El isomorfismo β buscado es δ^{-1}.

(2 $\Rightarrow$ 3) Tenemos $\eta : N \to M$ tal que $\eta \circ \varphi = id_M$. 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:

$$\begin{array}{ccccc} M & \xleftarrow{\pi_M} & M \oplus P & \xrightarrow{\pi_P} & P \\ & {\scriptstyle \eta} \nwarrow & \uparrow{\scriptstyle \beta} & \nearrow {\scriptstyle \psi} & \\ & & N & & \end{array}$$

Por el lema 4.3.4, 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,

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

Definición 4.3.8. *Diremos que una sucesión exacta corta* se escinde *si satisface la proposición anterior.*

Observación 4.3.9. *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. (Si se considera, por ejemplo, la misma sucesión exacta corta con término del medio N, el isomorfismo $-id_N$ en general no hace conmutar los diagramas correspondientes).*

2. *De la demostración de $(1 \Rightarrow 3)$ se desprende que, si* $0 \longrightarrow M \xrightarrow{\varphi} N \underset{\nu}{\overset{\psi}{\rightleftarrows}} P \longrightarrow 0$

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 $Im\varphi \oplus Im\nu = N$, e $Im\nu \cong P$.

Análoga observación vale para la escisión via η.

Ejemplo 4.3.10. *Si* $0 \longrightarrow W \hookrightarrow V \xrightarrow{\pi} V/W \longrightarrow 0$ *es una sucesión exacta corta de espacios vectoriales de dimensión finita, entonces se escinde.*

4.4. Dependencia lineal y módulos libres

Definición 4.4.1. *Sea M un A-módulo. Sea $S \subseteq M$ un subconjunto. Decimos que S es* linealmente dependiente *si existen $m_1, \ldots, m_k \in S$ y $a_1, \ldots, a_k \in A$ 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 $m_1, \ldots, m_k$.*

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

Observación 4.4.2. *1. $S = \emptyset$ es linealmente independiente.*

2. *S es linealmente independiente si y sólo si para todo $m_1, \ldots, m_k \in S$ y $a_1, \ldots, a_k \in A$ tales que $\sum_{i=1}^{k} a_i m_i = 0$ se tiene que $a_i = 0$ para todo $i = 1, \ldots, n$. Es decir, si la única combinación lineal nula es la trivial.*

3. *Si $S = \{m_1, \ldots, m_k\} \subset M$ es tal que 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 $p, q \geq 2$. 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 4.4.3. *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 4.4.4. *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 4.4.5.

1. *El conjunto $\mathcal{B} = \{1, x, x^2, \dots\}$ es base de $A[x]$ como A-módulo.*

2. *Sea $n \geq 2$: 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.*

Definición 4.4.6. *Sea $B \neq \emptyset$ un conjunto arbitrario. El A-*módulo libre generado por *B es $L_A(B) = \bigoplus_{i \in S} A_i$ donde $A_i = A$ para todo $i \in S$, considerado como A-módulo con la acción regular. Explícitamente,*

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

Si $s \in S$, 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 $\chi_s \in L_A(S)$.*

Observación 4.4.7. *Sea A un anillo. Todo A-módulo es libre si y solo si A es un anillo con división.*

Demostración. Si A es un anillo con división. Se prueba que la familia de conjuntos li en A está en las hipótesis del Lema de Zorn, y que un elemento maximal en dicha familia es necesariamente generador (esto es, la prueba en espacios vectoriales, sigue valiendo en el caso no conmutativo).
Recíprocamente supongamos que $x \in A$ es no nulo y no invertible. Tenemos un ideal $I \neq 0$ izquierdo maximal de A que contiene a x. Se tiene que A/I es un A-módulo simple (es decir sin submódulos propios). Como es libre por hipótesis, una base tiene necesariamente cardinal 1. Se deduce que $A/I \cong A$ y por lo tanto A es simple como A-módulo a izquierda lo que contradice la existencia de I. □

Observación 4.4.8. *Si A es no trivial, la función $S \to L_A(S)$, $s \mapsto \chi_s$ es inyectiva, luego podemos pensar $S \subset L_A(S)$, análogamente a como hicimos en el caso $A \subset A[x]$.*

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. Además S es linealmente independiente:

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

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

Definición 4.4.9. *Sea M un A-módulo, $S \subset M$ un subconjunto. El* anulador *de S es*

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

Si $S = \{m_1, \ldots, m_k\}$ escribiremos $\mathrm{Ann}(S) = \mathrm{Ann}(m_1, \ldots, m_k)$.

Observación 4.4.10. *Sea $S = \{m\}$, para algún $m \in M$. Tenemos un morfismo $\varphi : A \to M$, $a \mapsto am$. Se tiene que $Im\varphi = Am$ y $Ker\varphi = \mathrm{Ann}(m)$. Por lo tanto $A/\mathrm{Ann}(m) \cong Am$.*

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

Observación 4.4.11. *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 $a_1m_1 + \cdots + a_km_k = 0$; 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 4.4.12. *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 un conjunto S tal que $M \cong \bigoplus_{i \in \mathcal{F}} A_i = L_A(S)$ 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 4.4.11. Ahora, como B es linealmente independiente, $\mathrm{Ann}(m) = \{0\}$ para todo $m \in \mathcal{B}$, y por lo tanto $A \cong A/\mathrm{Ann}(m) \cong Am$ en virtud de la observación 4.4.10.

(2 $\Rightarrow$ 3) Obvio.

(3 $\Rightarrow$ 1) Por definición, se tiene que $\bigoplus_{i \in \mathcal{F}} A_i = L_A(\mathcal{F})$, que ya sabemos que es libre, y por lo tanto $M \cong \bigoplus_{i \in \mathcal{F}} A_i$ es libre, en virtud de la observación 4.4.4. □

Ejemplos 4.4.13. *1. A^n es libre para todo $n \in \mathbb{N}$.*

2. Todo anillo como módulo sobre sí mismo es libre, con base $\{1\}$.

3. En particular, $\mathbb{Z}_n$ es libre como $\mathbb{Z}_n$-módulo, pero no lo es como $\mathbb{Z}$-módulo (ejemplo 4.4.52).

4. $\mathbb{Z}_3 \simeq N = \{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbb{Z}_6$ es un $\mathbb{Z}_6$-submódulo que no es libre (de hecho, $N = \langle \overline{2} \rangle$).

5. $\mathbb{Z}$ 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.

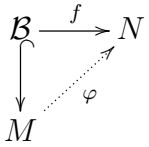
Proposición 4.4.14. *Sea M un A-módulo libre con base $\mathcal{B} \subseteq M$. Si M es finitamente generado, entonces $\#B < \infty$.*

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 B es linealmente independiente. En efecto, si existiera $e_{r+1} \in B$ distinto de los anteriores, entonces se escribiría como combinación lineal de $\{e_1, \ldots, e_r\}$, contradiciendo la independencia lineal de $\mathcal{B}$. □

La siguiente proposición, como en espacios vectoriales, muestra que para definir una transformación lineal desde un módulo libre, basta definirla en una base. Como con la suma directa y el producto directo, es fácil probar que esta propiedad universal caracteriza al par $(L_A(S), \iota)$ donde S es un conjunto y $\iota : S \to L_A(S)$ es la inclusión.

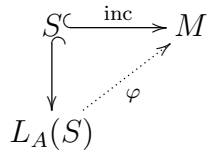
Proposición 4.4.15 (Propiedad universal del módulo libre)**.** *Sea M un A-módulo libre con base $\mathcal{B} \subseteq M$, y N un A-módulo. Si $f : B \to N$ es una función, entonces existe un único morfismo de A-módulos $\varphi : M \to N$ tal que $\varphi|_{\mathcal{B}} = f$, i.e. que hace conmutar el siguiente diagrama:*



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. □

Corolario 4.4.16. *Sea M un A-módulo. Entonces existe un A-módulo libre L y un epimorfismo $L \to M \to 0$. En otras palabras, todo A-módulo M es cociente de un libre.*

Demostración. Sea $S \subseteq M$ 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:



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 $M \simeq \frac{L_A(S)}{Ker\varphi}$. □

Corolario 4.4.17. *Si $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} F \longrightarrow 0$ es una sucesión exacta corta, donde F es un A-módulo libre, entonces se escinde.*

Demostración. Basta definir $\nu : F \to N$ morfismo tal que $\psi \circ \nu = id_F$. Sea $B \subset F$ una base. Dado $b \in \mathcal{B}$, como ψ es sobreyectiva, elegimos $n_b \in N$ tal que $\psi(n_b) = b$ (axioma de elección). Ahora definimos una función $f : \mathcal{B} \to N$, $b \mapsto n_b$ y aplicamos la propiedad universal del A-módulo libre con base $\mathcal{B}$ a F. □

Teorema 4.4.18. *Sea A un anillo con división, y sea M un A-módulo. Entonces M es libre. Además, si $\mathcal{B} \subset M$, son equivalentes:*

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

Demostración. 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. □

Teorema 4.4.19. *Sea M un A-módulo libre que admite una base 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 $x \in \mathcal{B} \setminus \mathcal{B}'$. 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 4.4.20. *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 4.4.19:*

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

Demostración. 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 $\#S \geq \#\mathcal{B}$. □

Definición 4.4.22. *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 4.4.23. *1. El corolario 4.4.21 afirma que todo anillo con división tiene NBI.*

2. $\operatorname{rg}(A^n) = n$.

Observación 4.4.24. *Dado un anillo A, para verificar si tiene NBI basta hacerlo en módulos libres que no admiten bases infinitas, en virtud de la observación 4.4.20. 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 4.4.25. *Si I es un ideal de A y M es un A-módulo a izquierda, se tiene que IM es un submódulo de M y que M/IM tiene estructura de A/I-módulo a izquierda.*

Demostración. Queda como ejecicio. □

Lema 4.4.26. *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. Por el Lema 4.4.25,

$$IM = \left\{ \sum_{i=1}^{n} a_i n_i \mid a_i \in I, n_i \in M, n \in \mathbb{Z}^+ \right\}$$

es un submódulo de M y M/IM es un A/I-módulo, con la acción $\overline{a}\cdot\overline{m} = \overline{am}$.

Veamos que $\overline{\mathcal{B}}$ es generador:[5] 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:

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

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

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

[5] 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.

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

$$\sum_{i\in I} a_i m_i = \sum_{n\in I} \left(\sum_{j=1}^{r} b_j c_{jn} \right) m_n.$$

Si $\alpha_n \in I = \sum_{j=1}^{r} b_j c_{jn}$ se deduce $\sum_{i\in I}(a_i - \alpha_i)m_i = 0$.
Como $\mathcal{B}$ 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. □

Teorema 4.4.27. *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. □

4.5. 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). Consideraremos únicamente el caso en que el anillo A es conmutativo (lo que asumiremos en lo que queda de la sección).

Definición 4.5.1. *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* $M \times N \hookrightarrow L_A(M \times N) \xrightarrow{\pi} M \otimes_A$

Observación 4.5.2. *1. Todo elemento de* $M \otimes_A N$ *es* suma *finita de tensores elementales: en efecto, si* $x \in M \otimes_A N$, *entonces:*

$$x = \pi\left(\sum_{i,j=1}^{r,s} a_{ij}(m_i, n_j)\right) = \pi\left(\sum_{i,j=1}^{r,s} a_{ij}\iota(m_i, n_j)\right) = \sum_{i,j=1}^{r,s} a_{ij}\theta(m_i, n_j)$$
$$= \sum_{i=1}^{r}\sum_{j=1}^{s} a_{ij} m_i \otimes n_j \overset{2)}{=} \sum_{i=1}^{r}\sum_{j=1}^{s} m_i \otimes (a_{ij} n_j) \overset{4)}{=} \sum_{i=1}^{r} m_i \otimes \left(\sum_{j=1}^{s} a_{ij} n_j\right)$$

Si $n_i' := \sum_{j=1}^{s} a_{ij} n_j$ *se deduce* $x = \sum_{i=1}^{r} m_i \otimes n_i'$. *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* $m \otimes n$ *(ver ejercicio 2 del práctico 9).*

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.*

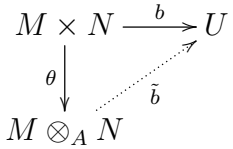
Definición 4.5.3. *Sean* A *un anillo,* M, N, U *tres* A*-módulos y* $b : M \times N \to U$ *una función. Decimos que* b *es* A-bilineal *si es lineal en cada variable; es decir, si se verifican las siguientes condiciones:*

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

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

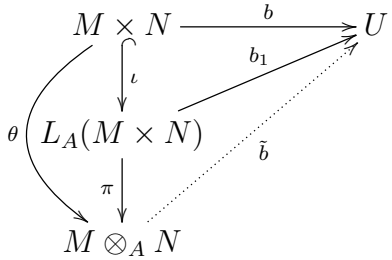
A continuación vemos la propiedad universal del producto tensorial. Informalmente, ésta dice que para definir un mapa A-lineal $M \otimes_A N \to U$, basta definir un mapa A-bilineal $M \times N \to U$. Como siempre, no es difícil probar que la propiedad universal caracteriza al objeto a menos de isomorfismo. 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 4.5.4 (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:*



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 $T \subseteq Ker b_1$ 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 $\tilde{b} \circ \pi = b_1$.



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. □

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 4.5.5. *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:*

$$\begin{array}{ccc} M \times P & \xrightarrow{\varphi \times \psi} & N \times Q \\ {\scriptstyle \theta_1}\downarrow & & \downarrow{\scriptstyle \theta_2} \\ M \otimes_A P & \xrightarrow{\varphi \otimes \psi} & N \otimes_A Q \end{array}$$

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 $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n), \forall m \in M, n \in N$. □

Observación 4.5.6. *No es difícil verificar que esta operación cumple las siguientes propiedades:*

- $id_M \otimes id_N = id_{M \otimes_A N}$,
- *Dados f, g, f', g' morfismos de A-módulos como abajo, el diagrama de la derecha conmuta:*

$$\begin{array}{cc} M & M' \\ {\scriptstyle f}\downarrow & \downarrow{\scriptstyle f'} \\ N & N' \\ {\scriptstyle g}\downarrow & \downarrow{\scriptstyle g'} \\ P & P' \end{array} \qquad \begin{array}{ccc} M \otimes_A M' & & \\ {\scriptstyle f \otimes f'}\downarrow & \searrow^{(g \circ f) \otimes (g' \circ f')} & \\ N \otimes_A N' & & \\ {\scriptstyle g \otimes g'}\downarrow & & \\ P \otimes_A P' & & \end{array}$$

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 4.5.7. *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).

   $$\begin{array}{ccc} (M \otimes_A N) \times P & \xrightarrow{F} & M \otimes_A (N \otimes_A P) \\ {\scriptstyle\theta}\downarrow & \nearrow_{\tilde{F}} & \\ (M \otimes_A N) \otimes_A P & & \end{array}$$

   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 $m \otimes 1_A$).

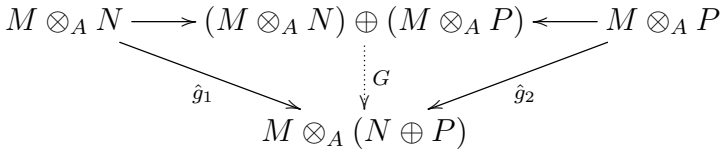
   Observar que es $\tilde{b}(m \otimes a) = am$.

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 $\tilde{f}$.



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

Observación 4.5.8. *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 4.5.9. *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 4.5.8, $M \otimes_A N \cong \bigoplus_{i,j} \left(Ab_i \otimes_A Ab'_j\right)$.

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 4.5.10. *Si M y N son libres,* $\operatorname{rg}(M \otimes_A N) = \operatorname{rg}(M)\operatorname{rg}(N)$.

Corolario 4.5.11. *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. □

Capítulo 5

Módulos f.g. sobre un dip

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.

Para acercarnos al resultado, comenzamos con una sección que lista "buenas" propiedades de los módulos finitamente generados 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.

5.1. Módulos finitamente generados

Definición 5.1.1. *Sea M un A-módulo. Definimos:*

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

Observación 5.1.2. $\mu(M) < \infty \iff M$ *es finitamente generado.*

Ejemplo 5.1.3. *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 5.1.4. *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* $\mu(M) \leq \mu(N) + \mu(M/N)$.

Demostración. 1. Consideremos el morfismo sobreyectivo $\pi : M \to M/N$. Si $M = \langle m_1, \ldots, m_k \rangle$, entonces por la observación 4.4.4, se tiene que $M/N = \langle \pi(m_1), \ldots, \pi(m_k) \rangle$.

2. Basta probar que existe un generador de M con $\mu(N) + \mu(M/N)$ elementos. Sea $\{n_1, \ldots, n_k\}$ un generador de N con $\mu(N)$ elementos, y $\{\pi(m_1), \ldots, \pi(m_r)\}$ un generador de M/N con $\mu(M/N)$ elementos. Veamos que $X = \{n_1, \ldots, n_k, m_1, \ldots, m_r\}$ 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 $m \in \langle X \rangle$. □

Observación 5.1.5. *Por la observación 4.3.6, la parte 2 de la proposición anterior es equivalente a: dada una sucesión exacta corta* $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ *, si* $\mu(M) < \infty$ *y* $\mu(P) < \infty$*, entonces* $\mu(N) < \infty$ *y* $\mu(N) \leq \mu(M) + \mu(P)$.

5.2. 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 5.2.1. *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 $G = \{g_1, \ldots, g_{n+1}\}$ 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 $\mu(M') \leq n$. Por hipótesis de inducción, ambos términos son finitamente generados, de donde se deduce que el término del medio también lo es (proposición **??**). □

El resultado anterior puede mejorarse para el caso de un DIP, como muestra la siguiente

Proposición 5.2.2. *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 $\mu(N) \leq \mu(M)$.*

Demostración. La primera parte de la afirmación es consecuencia directa de la Proposición 5.2.1, ya que todo DIP es noetheriano. Para la segunda parte de la afirmación, recorramos la prueba de la proposición 5.2.1. 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 $\mu(N) \leq 1 = \mu(M)$.

En el paso inductivo, se tiene $\mu(M'\cap N) \leq \mu(M')$ y $\mu\left(\frac{N}{M'\cap N}\right) \leq \mu\left(\frac{M}{M'}\right) = 1$, de donde $\mu(N) \leq \mu(M'\cap N) + \mu(\frac{N}{M'\cap N}) \leq \mu(M') + 1 = n+1 = \mu(M)$. □

Para el caso de submódulos de un módulo libre sobre un DIP, el resultado también es positivo, a saber:

Proposición 5.2.3. *Sean D un DIP, M un D-módulo y $N \subseteq M$ un submódulo no trivial. Si M es libre de rango finito, entonces N también lo es y $\mathrm{rg}(N) \leq \mathrm{rg}(M)$.*

Demostración. Otra vez procederemos por inducción, esta vez en $\mathrm{rg}(M)$.

Si $\mathrm{rg}(M) = 1$, 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 $a \in D$. Como D es un dominio, $\{a\}$ es linealmente independiente y por tanto $\{a\}$ 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

$$\operatorname{rg}(N) = \operatorname{rg}(M' \cap N) + \operatorname{rg}\left(\frac{N}{M' \cap N}\right) \leq \operatorname{rg}(M') + \operatorname{rg}\left(\frac{M}{M'}\right) = n+1. \qquad \square$$

5.3. Teoría de torsión

Definición 5.3.1. *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 5.3.2. $0 \in M$ *siempre es de torsión.*

La siguiente proposición muestra que la torsión de M es más interesante en el caso en que el anillo es un dominio, por lo que a partir de ahora nos situaremos en ese contexto.

Proposición 5.3.3. *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 $m \in \mathrm{Tor}(M)$ 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 $dm \in \mathrm{Tor}(M)$.

Veamos la segunda afirmación. Sea $\overline{x} \in M/\mathrm{Tor}(M)$, $\overline{x} \neq \overline{0}$ (i.e. $x \notin \mathrm{Tor}(M)$). Supongamos que $a\overline{x} = \overline{0}$. Pero entonces $\overline{ax} = \overline{0} \Rightarrow ax \in \mathrm{Tor}(M)$, es decir, existe $b \neq 0$ tal que $bax = 0$. Como $x \notin \mathrm{Tor}(M)$, entonces $ba = 0$. Como $b \neq 0$ y D es un dominio, debe ser $a = 0$. □

Observación 5.3.4. *1. Es sencillo verificar que la torsión es invariante por isomorfismos: si D es un dominio y M, N son D-módulos, entonces $M \cong N \Rightarrow \mathrm{Tor}(M) \cong \mathrm{Tor}(N)$*

2. Es un ejercicio verificar que $Tor(\bigoplus_{i\in I} M_i) \cong \bigoplus_{i\in I} Tor(M_i)$.

Ejemplos 5.3.5. *1. Si A es conmutativo, considerando A como A-módulo, se tiene $\mathrm{Tor}(A) = \{a \in A \mid a$ es divisor de cero$\}$. En particular, si D es un dominio, $\mathrm{Tor}(D) = \{0\}$.*

2. Si L es libre sobre un dominio, entonces $\mathrm{Tor}(L) = \{0\}$. En efecto, $L \cong \bigoplus_{i\in I} D$ por lo que $\mathrm{Tor}(L) \cong \bigoplus_{i\in I} \mathrm{Tor}(D) = \{0\}$ (usando la Observación 5.3.4).

3. $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo es de torsión, es decir, $\mathrm{Tor}(\mathbb{Z}_n) = \mathbb{Z}_n$. En efecto $n\overline{x} = 0$, para todo $x \in \mathbb{Z}_n$.

4. Más en general, todo grupo abeliano finito G es de torsión. En efecto, dado $g \in G$, consideremos la función $\varphi_g : \mathbb{Z} \to G$, $\varphi_g(n) = ng$. Como G es finito y $\mathbb{Z}$ es infinito, entonces debe existir $n_0 \in \mathbb{Z}$ tal que $n_0 g \in G$ tiene infinitas preimágenes. En particular, tiene otra preimagen: existe $n_1 \in \mathbb{Z}$ tal que $n_1 g = n_0 g$ con $n_1 \neq n_0$. Por lo tanto $(n_1 - n_0)g = 0$ con $n_1 - n_0 \neq 0$, luego g es de torsión, para todo $g \in G$.

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 5.3.6. *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 (si lo fuera, sería numerable).

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 5.3.7. *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 $U = \{u_1, \ldots, u_k\} \subseteq X$.

Supongamos que existe $x_i \in X \setminus U$. 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 $d_i x_i = a_1 u_1 + a_2 u_2 + \cdots + a_k u_k$.

Llamemos d al producto de los d_i obtenidos por cada $x_i \in X \setminus U$. 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 $M \simeq Im\varphi \subset \langle u_1, \ldots, u_k \rangle$ que es libre. Al ser D un DIP, todo submódulo de un D-módulo libre es libre; en particular, $Im\varphi \simeq M$ es libre. □

5.4. Teorema de estructura

El objetivo de esta sección es probar que todo módulo finitamente generado M sobre un DIP se descompone en suma directa de módulos como sigue:

$$M \cong D^r \oplus \bigoplus_{i=1}^{t} \frac{D}{d_i} : d_i \notin D^\times; d_i | d_j \text{ si } i < j \text{ y } Ann(M) = \langle d_t \rangle$$

En el resto del capítulo D será un dominio a ideales principales.
Comenzamos por descomponer los módulos finitamente generados sobre D en suma directa de una parte libre y una parte de torsión.

Teorema 5.4.1. *Si M es un D-módulo finitamente generado, $M \cong Tor(M) \bigoplus L$: L libre. Además, la descomposición es única a menos de isomorfismos.*

Demostración. Como A es un dominio, $Tor(M)$ es un submódulo y $\frac{M}{Tor(M)}$ es libre por ser sin torsión sobre un DIP. Luego la siguiente sucesión exacta escinde:

$$0 \longrightarrow \mathrm{Tor}(M) \longrightarrow M \longrightarrow \frac{M}{\mathrm{Tor}(M)} \longrightarrow 0$$

Por tanto tenemos $M \cong Tor(M) \bigoplus L : L := \frac{M}{Tor(M)}$.

Para la unicidad, supongamos $M \cong T \bigoplus \hat{L} : T$ de torsión y $\hat{L}$ libre, y sea $\varphi : M \to T \bigoplus \hat{L}$ el isomorfismo.

Como $Tor(T \bigoplus \hat{L}) = Tor(T) + Tor(\hat{L}) = T$, tenemos $\varphi|_{Tor(M)} : Tor(M) \to T$ también es un isomorfismo (ya que elementos de torsión van en elementos de torsión).
Luego, pasando al cociente por T tenemos:

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & T \oplus \hat{L} \\ \downarrow{\scriptstyle \pi_T} & & \downarrow{\scriptstyle \pi_T} \\ L = \dfrac{M}{T} & \overset{\hat{\varphi}}{\dashrightarrow} & \dfrac{T \oplus \hat{L}}{T} = \hat{L} \end{array}$$

y concluímos $T \cong Tor(M); \hat{L} \cong L$ □

Sabemos que la parte libre es isomorfa a D^r para cierto (único) r finito.

Definición 5.4.2. *Un D-módulo M no nulo se dice* **indescomponible** *si la única descomposición de M como suma directa de módulos propios es trivial, esto es, si $M = M_1 \oplus M_2$ entonces $M_1 = 0$ o $M_2 = 0$.*

Lema 5.4.3. *Los módulos de la forma $M = \frac{D}{\langle p^r \rangle}$, con p irreducible, son indescomponibles.*

Demostración. Notemos que los submódulos de M están en correspondencia con los submódulos de D que contienen a $\langle p^r \rangle$. Estos son ideales $I = \langle d \rangle$ que verifican $\langle p^r \rangle \subseteq I = \langle d \rangle$, o sea que $d \mid p^r$. Como p es irreducible (luego primo), d es una potencia de p.
Si $M = M_1 \oplus M_2$ correspondientes respectivamente a $I_1 = (p^{r_1})$ y $I_2 = (p^{r_2})$, se tiene que $(p^r) = I_1 \cap I_2$ coincide con algún I_i y por lo tanto $M_i = \frac{I_i}{(p^r)} = 0$. □

Observación 5.4.4. *Notar que el resultado anterior vale para $r = 0$ por lo que tenemos que D es indescomponible.*

Veremos cómo se descomponen los módulos de torsión en indescomponibles. Más precisamente, probaremos que todo módulo de torsión finitamente generado sobre un DIP se descompone en suma directa de "p-módulos", es decir, módulos tal que todos sus elementos son anulados por una potencia de p con p primo.
Luego, descompondremos estos p-módulos en suma directa de indescomponibles, que son de la forma $M_i \cong \frac{A}{\langle p^{r_i} \rangle}$.
Probaremos además resultados de unicidad.

Definición 5.4.5. *Sea $p \in D$ primo. Un* **p-módulo** *es un módulo tal que todo elemento es anulado por una potencia de p.*

Observación 5.4.6. *Todo p-módulo es de torsión y si M es un p-módulo finitamente generado, $Ann(M) = \langle p^r \rangle$ para cierto $r \in \mathbb{N}$*

Proposición 5.4.7. *Si M es un D-módulo de torsión finitamente generado, existen primos $p_1, \ldots, p_s$ no asociados dos a dos, tales que $M \cong \bigoplus M_{p_i}$, donde los M_{p_i} son p_i-módulos no triviales.*
Además, dicha descomposición es única, esto es: si $M \cong \bigoplus_{j=1}^{l} M_{q_j}$, donde M_{q_j} son q_j-módulos con q_j primos no asociados si $j \neq k$; entonces $l = s$ y $q_i \sim p_{\sigma(i)}$ para cierta biyección $\sigma \in S_s$. Además, $M_{q_i} \cong M_{p_{\sigma(i)}}$.

Demostración. Sea $\{m_1, \ldots, m_s\}$ un generador de M. Si $Ann(m_i) = \langle d_i \rangle \ \forall i$, tenemos que $Ann(M) = \bigcap Ann(m_i) = \bigcap \langle d_i \rangle = \langle mcm\{d_1, \ldots, d_s\} \rangle$. Pongamos $n := mcm\{d_1, \ldots, d_s\}$ y sea $n = p_1^{r_1} \ldots p_l^{r_l}$ su descomposición en irreducibles.

Vamos a ver que M es suma directa de los p_i-módulos:

$$Tor_p^{\infty}(M) := \{m \in M : p_i^t m = 0 \text{ para cierto } t \in \mathbb{N}\}, \quad i \in \{1, 2, \cdots, l\}.$$

Notar que si $m \in M_i$, $(p_i^t) \subseteq Ann(m)$ para cierto t, y por estar en un dip $Ann(m) = (p_i^{t'})$ para cierto $t' \leq t$. Más aún $t' \leq r_i$ puesto que $n \in Ann(m_i)$. Para ver que M es suma de los M_i, definimos $q_j := \prod_{i \neq j} p_i^{r_i} = \frac{n}{p_j^{r_j}}$. Para cada i, se tiene $q_i m \in M_i, \forall m \in M$ y que $mcd(q_1, \ldots, q_l) = 1$. Como D es un dip, vale la identidad de Bézout: existe $a_j \in D$ tal que $\sum a_j q_j = 1$. Para $m \in M$ se tiene entonces

$$m = 1 \cdot m = (\sum a_j q_j) \cdot m = \sum a_j q_j m \in \bigoplus M_j.$$

Para ver que la suma es directa, tomemos $m \in M_{i_0} \bigcap \bigoplus_{i \neq i_0} M_i$. Tenemos luego que $m = \sum_{i \neq i_0} \alpha_i m_i$ para ciertos $\alpha_i \in D, i \neq i_0$. Para cada $i \neq i_0$ tenemos $m_i \in M_i$, por lo que $q_{i_0} m_i = 0$. Luego, $0 = \sum_{i \neq i_0} q_{i_0} \alpha_i m_i = q_{i_0} \sum_{i \neq i_0} \alpha_i m_i$. Se deduce $q_{i_0} \in Ann(m) = (p_{i_0}^s)$ para cierto s lo que implica $s = 0$ y por lo tanto $m = 0$.

Para la unicidad, queda como ejercicio observar que si $M \cong \bigoplus_{i=1}^{n} M_{p_i}$ como arriba, entonces:

- $Ann(\bigoplus_{i=1}^{n} M_i) = (\prod_{i=1}^{n} p_i^{s_i})$, para ciertos s_i (esto determina los primos a menos de asociados),
- $Tor_{p_j}^{\infty}(\bigoplus_{i=1}^{n} M_i) = M_j$ (esto determina los sumandos directos a menos de isomorfismo).

□

Ahora nos enfocamos en la descomposición de los p-módulos en indescomponibles. Vamos antes a ponerle nombre a una parte de la torsión de M que nos será útil.

Definición 5.4.8. *Si M es un D-módulo y $d \in D$, definimos el* **submódulo de d-torsión de** *M como*

$$Tor_d(M) := \{m \in M : dm = 0\}$$

Observación 5.4.9. *Si p, es primo y $Tor_p(M) \neq 0$, entonces $(Ann(Tor_p(M)) = (p)$ que es maximal (por ser primo); se tiene que $Tor_p(M)$ es nulo o es un $\frac{D}{\langle p \rangle}$-espacio vectorial de dimensión finita, por ser submódulo de un módulo finitamente generado.*

Necesitamos una noción más y un resultado técnico antes de descomponer los p-módulos.

Definición 5.4.10. *Si M es un D-módulo, decimos que $\{m_1, \ldots, m_s\}$ es un* **conjunto linealmente disjunto** *si la suma $\sum \langle m_i \rangle$ es directa (i.e. $\sum_i a_i m_i = 0$ implica $a_i m_i = 0, \forall i$).*

Lema 5.4.11. *Sean $p \in D$ primo, M un p-módulo y $X = \{m_1, \ldots, m_s\} \subseteq M$ linealmente disjunto. Si n_i es tal que $pn_i = m_i$ para cada i, entonces $\{n_1, \ldots, n_s\}$ es linealmente disjunto.*

Demostración. Supongamos $\sum a_i n_i = 0 : a_i \in D$. Luego, tenemos:

$$\sum a_i m_i = \sum a_i p n_i = p \sum a_i n_i = 0$$

Como X es linealmente disjunto, $a_i m_i = 0 \ \forall i$, por lo que $a_i \in Ann(m_i) \ \forall i$. Como M es un p-módulo, deducimos que $p | a_i \ \forall i$, es decir, $\exists b_i \in D : a_i = p b_i$, y luego

$$0 = \sum a_i n_i = \sum p b_i n_i = \sum b_i m_i$$

Finalmente, como X es linealmente disjunto, tenemos $0 = b_i m_i = a_i n_i \forall i$. □

Proposición 5.4.12. *Si p es primo y M es un p-módulo finitamente generado, se tiene $M \cong \bigoplus \frac{D}{\langle p^{r_i} \rangle}$. Es decir, M se descompone en suma directa de indescomponibles $M_i \cong \frac{D}{\langle p^{r_i} \rangle}$.*

Demostración. Trabajaremos por inducción en $l = \text{mín}\{r : p^r \in Ann(M)\}$.

Caso base: Si $l = 1$, como estamos en un DIP y el ideal $\langle p\rangle$ es primo, entonces es maximal, luego $\frac{D}{\langle p\rangle}$ es un cuerpo,y entonces M es un $\frac{D}{\langle p\rangle}$-espacio vectorial y por tanto $M \cong \bigoplus \frac{D}{(p)}$ como $\frac{D}{(p)}$-módulo, y por lo tanto como D-módulo.

Paso inductivo: Supongamos que vale el resultado para l y que $Ann(M) = (p^{l+1})$. Consideremos el morfismo de anillos $\ell_p : M \to M, \ell_p(m) = pm$. Notar que $Im(\ell_p)$ es finitamente generado por $\ell_p(G)$ si G es un generador de M.

Como $Ann(Im(\ell_p)) = (p^l)$, por hipótesis de inducción, tenemos un isomorfismo $\varphi : \bigoplus_{i=1}^{t} \frac{D}{(p^{r_i})} \to Im(\ell_p)$. Sea $\{n_1, \ldots, n_t\} \subset Im(\ell_p)$ la imagen del generador canónico. Entonces $\{n_1, \ldots, n_t\}$ es un generador linealmente disjunto de $Im(\ell_p)$ y $n_i = pz_i$, para cierto $z_i \in M$. Por el lema 5.4.11, $\{z_1, \ldots, z_t\}$ es también linealmente disjunto. Sea $H = \langle z_1, \ldots, z_t\rangle = \bigoplus\langle z_i\rangle$. Notar que como $n_i = pz_i$ y $Ann(n_i) = (p_i^{r_i})$, entonces $Ann(z_i) = (p_i^{r_i+1})$, por lo que $\langle z_i\rangle \cong \frac{D}{(p_i^{r_i+1})}$.

Notemos ahora que $Tor_p(M)$ es un $\frac{D}{(p)}$-espacio vectorial. Como $\{z_1, z_2, \cdots, z_t\}$ es linealmente disjunto sobre D, se deduce que $X := \{p^{r_1}z_1, \ldots, p^{r_t}z_t\}$ es linealmente independiente sobre el cuerpo $\frac{D}{(p)}$. Como $X \subseteq Tor_p(M)$, podemos tomar K tal que: $Tor_p(M) = \langle X\rangle \bigoplus K$ como $\frac{D}{(p)}$ espacios vectoriales, y por lo tanto como D-módulos.
Si $K \neq 0$, como $K \subseteq Tor_p(M)$, se tiene $Ann(K) = (p)$ y por hipótesis de inducción tenemos que $K \cong \bigoplus \frac{D}{\langle p\rangle}$.

La prueba termina observando que $M = H \bigoplus K$. Veamos primero que $M = H + K$: si $m \in M$, $\ell_p(m) = pm = \sum_i a_i n_i = \sum a_i p z_i$ para ciertos a_i. Se deduce $p(m - \sum a_i z_i) = 0$, de donde $(m - \sum_i a_i z_i) \in Tor_p(M) = \langle X\rangle + K \subseteq H + K$. Como además $\sum_i a_i z_i \in H$ se deduce $m \in H + K$.
Veamos ahora que la suma es directa: si $m \in H \bigcap K$, en particular, $m \in H$, luego $m = \sum a_i z_i$. Como $K \subseteq Tor_p(M)$, se tiene $0 = pm = p\sum a_i z_i = \sum p a_i z_i \in \bigoplus_i \langle z_i\rangle$, de donde $pa_i z_i = 0\ \forall i$. Se deduce $pa_i \in Ann(z_i) = \langle p^{r_i+1}\rangle$, luego $p^{r_i} | a_i$. Se deduce $m = \sum_i d_i p^{r_i} z_i$ y por lo tanto $m \in \langle p^{r_1}z_1, \ldots, p^{r_t}z_t\rangle$. Luego tenemos que $m \in \langle X\rangle \bigcap K = \{0\}$. □

El siguiente resultado completa el anterior en el sentido de la unicidad de una tal descomposición.

Proposición 5.4.13. *Si M es un p-módulo finitamente generado tal que*

$$M \cong \bigoplus_{i=1}^{n} \frac{D}{(p^{r_i})} \cong \bigoplus_{j=1}^{l} \frac{D}{(p^{s_j})}$$

son dos descomposiciones en suma directa de indescomponibles, con $r_i \leq r_{i+1}, s_j \leq s_{j+1}\ \forall i, j$, entonces $n = l$ y las listas $r_i = s_i, \forall i \leq n$.

Demostración. Notemos que si $M = \bigoplus_{i=1}^{n} \frac{D}{(p^{r_i})}$ entonces $Ann(M) = (p^{r_n})$, por lo que $r_n = s_l$. Haremos la demostración por inducción en r_n.
Caso base: si $r_n = s_l = 1$, todos los r_i, s_j son 1 y M es un $\frac{D}{(p)}$-espacio vectorial, por lo que $n = l$.
Supongamos válido el resultado para r y supongamos $r_n = s_l = r + 1$.

Tenemos $Ann(pM) = (p^r)$. Por otra parte,

$$pM \cong \bigoplus_{i=1}^{n} p\frac{D}{(p^{r_i})} \cong \bigoplus_{j=1}^{l} p\frac{D}{(p^{s_j})},$$

(chequear que la suma se mantiene directa).

Como $p\frac{D}{(p^k)} \cong \frac{D}{(p^{k-1})}$ (chequearlo como ejercicio), queda

$$pM \cong \bigoplus_{i=i_0}^{n} \frac{D}{(p^{r_i-1})} \cong \bigoplus_{j=j_0}^{l} \frac{D}{(p^{s_j-1})}$$

Aplicando la hipótesis de inducción a pM obtenemos $n - i_0 = l - j_0$ y $r_{i_0+k} = s_{j_0+k}, \forall k$. (Notar que los sumandos directos para los cuales $r_i = 1, s_j = 1$ se anulan al ser multiplicados por p.)

Queda probar que $i_0 = j_0$. Queda como ejercicio chequear que el isomorfismo de la hipótesis lleva $\bigoplus_{i=i_0}^{n} \frac{D}{(p^{r_i-1})}$ en $\bigoplus_{j=j_0}^{l} \frac{D}{(p^{s_j-1})}$ por lo que usando una de las consecuencias de la Propiedad universal del cociente resulta:

$$\bigoplus_{i=1}^{i_0-1} \frac{D}{(p)} \cong \bigoplus_{j=1}^{j_0-1} \frac{D}{(p)}$$

Luego, como el isomorfismo es también de $\frac{D}{(p)}$-espacios vectoriales y los sumandos directos son subespacios de dimesión 1, concluimos $i_0 = j_0$. □

Los resultados anteriores se resumen en el siguiente resultado, que llamaremos **Primer Teorema de Estructura para módulos finitamente generados sobre un dip.**

Teorema 5.4.14. *Sean D un dominio a ideales principales y M un D-módulo finitamente generado.*

Existen $r \in \mathbb{N}$, $p_1, p_2, \cdots, p_k$ primos no asociados dos a dos en D y para cada $i \in \{1, 2, \cdots, k\}$, naturales $r_{i1} \leq r_{i2} \cdots \leq r_{il_i}$ tales que

$$M \cong D^r \oplus \bigoplus_{j=1}^{r_{l_1}} \frac{D}{(p_1^{r_{1j}})} \oplus \bigoplus_{j=1}^{r_{l_2}} \frac{D}{(p_2^{r_{2j}})} \oplus \cdots \oplus \bigoplus_{j=1}^{r_{l_k}} \frac{D}{(p_k^{r_{kj}})}.$$

Además, si

$$D^r \oplus \bigoplus_{j=1}^{r_{l_1}} \frac{D}{(p_1^{r_{1j}})} \oplus \bigoplus_{j=1}^{r_{l_2}} \frac{D}{(p_2^{r_{2j}})} \oplus \cdots \oplus \bigoplus_{j=1}^{r_{l_k}} \frac{D}{(p_k^{r_{kj}})} \cong D^s \oplus \bigoplus_{j=1}^{s_{t_1}} \frac{D}{(q_1^{s_{1j}})} \oplus \bigoplus_{j=1}^{s_{t_2}} \frac{D}{(q_2^{s_{2j}})} \oplus \cdots \oplus \bigoplus_{j=1}^{s_{t_n}} \frac{D}{(q_n^{r_{nj}})}.$$

con $r, s \in \mathbb{N}$, p_i primos no asociados dos a dos en D, q_i primos no asociados dos a dos en D, $r_{ij} \leq r_{ij'}, s_{ij} \leq s_{ij'}$ naturales, entonces

- $r = s$,
- $k = n$,
- *para cierta permutación $\sigma \in S_k$, $p_i \sim q_{\sigma(i)}, \forall i \leq r$,*
- $r_{l_i} = s_{t_{\sigma(i)}}, \forall i \leq r$,
- $r_{ij} = s_{\sigma(i)j}, \forall i \leq r, j \leq l_i$.

Observación 5.4.15. *Las potencias de primos que aparecen en la descomposición de M se llaman* factores invariantes de M.

La descomposición dada por el Primer Teorema de Estructura puede reformularse de manera de unir, en un mismo módulo cíclico, factores invariantes primos entre sí, de una manera ordenada que asegura la unicidad. Lo que resulta se conoce como **Segundo Teorema de Estructura para módulos finitamente generados sobre un dip**.

Teorema 5.4.16. *Sean D un dominio a ideales principales y M un D-módulo finitamente generado.*
Existen $r \in \mathbb{N}$, $d_1, d_2, \cdots, d_k \in D$ no invertibles y que verifican $d_i | d_{i+1}, \forall i \leq k$, tales que:

$$M \cong D^r \oplus \bigoplus_{i=1}^{t} \frac{D}{d_i}.$$

Además, si

$$D^r \oplus \bigoplus_{i=1}^{t} \frac{D}{d_i} \cong D^s \oplus \bigoplus_{i=1}^{k} \frac{D}{f_i},$$

con $r, s \in \mathbb{N}$, $d_i \in D$ *no invertibles tales que* $d_i | d_{i+1}, \forall i \leq t$ *y* $f_i \in D$ *no invertibles tales que* $f_i | f_{i+1}, \forall i \leq k$, *entonces*

- $r = s$,
- $t = k$,
- $d_i \sim f_i, \forall i \leq t$.

Demostración. Alcanza con usar que $\frac{D}{(d)} \oplus \frac{D}{(d')} \cong \frac{D}{dd'}$ si d y d' son coprimos y tomar d_r como el producto de todos sus factores invariantes (coprimos) de exponente máximo (uno por cada primo), luego d_{r-1} el producto de los factores invariantes (coprimos) de exponente máximo entre los que quedan (uno por cada primo de los que quedan), y así hasta agotar todos los factores invariantes.
Para la unicidad alcanza con descomponer cada $\frac{D}{(d_i)}$, $\frac{D}{(f_j)}$ según sus factores invariantes y observar que para que cada d_i divida al siguiente y cada f_j divida al siguiente, no hay otra forma que hacer lo que se indica en la parte de la existencia, puesto que $\frac{D}{(d)} \oplus \frac{D}{(d')}$ es cíclico solo si $mcd(d, d') = 1$ (en cuyo caso es isomorfo a $\frac{D}{(dd')}$ (queda como ejercicio). □

Observación 5.4.17. *Los* d_i *de la descomposición dada por el Segundo Teorema de Estructura se llaman* **divisores elementales de** M.

Corolario 5.4.18. *Como los* $\mathbb{Z}$*-módulos y los grupos abelianos están en biyección, tomando* $D = \mathbb{Z}$ *tenemos clasificados todos los grupos abelianos finitamente generados.*

Gracias a Santiago Porto por pasarnos sus valiosas notas sobre estructura de módulos finitamente generados sobre un dip, que editamos e incorporamos a esta última sección.