

# Notas de Álgebra Moderna IV. Módulos.

Cristo Daniel Alvarado

3 de noviembre de 2024

# Índice general

<b>1. Módulos, Homomorfismos y Secuencias exactas</b>	<b>2</b>
1.1. Módulos y homomorfismos . . . . .	2
1.2. Secuencias Exactas . . . . .	9
1.3. Ejercicios . . . . .	12
<b>2. Módulos Libres y Espacios Vectoriales</b>	<b>17</b>
2.1. Conceptos Fundamentales . . . . .	17
2.2. Referencias . . . . .	18

# Capítulo 1

## Módulos, Homomorfismos y Secuencias exactas

### 1.1. Módulos y homomorfismos

Los módulos son una generalización de los grupos abelianos y los enteros (los cuales son módulos sobre  $\mathbb{Z}$ ).

#### Definición 1.1.1

Sea  $R$  un anillo no trivial. Decimos que  $R$  es un **anillo de división**, si  $R$  es unitario y para cada  $a \in A$  existe  $a^{-1} \in A$ .

Si  $R$  es conmutativo, entonces  $R$  es un **campo**.

#### Definición 1.1.2

Sea  $R$  un anillo, un  **$R$ -módulo (izquierdo)** es un grupo abeliano  $A$  junto con una función  $\cdot : R \times A \rightarrow A$  (denotada simplemente por  $(r, a) \mapsto ra$ ) tal que para todo  $r, s \in R$  y para todo  $a \in A$ :

$$(1) \quad r(a + b) = ra + rb.$$

$$(2) \quad (r + s)a = ra + sa.$$

$$(3) \quad r(sa) = (rs)a.$$

si  $R$  además tiene elemento identidad  $1_R$  y se cumple que

$$(4) \quad 1_R a = a, \text{ para todo } a \in A.$$

entonces decimos que  $A$  es un  **$R$ -módulo unitario (izquierdo)**. En caso de que  $R$  sea un anillo de división, el módulo unitario  $A$  será llamado **espacio vectorial (izquierdo)**.

De forma análoga podemos definir los  $R$ -módulos derechos, cambiando el orden en el que se hacen las operaciones. Sin embargo, a lo largo del texto solo trabajaremos con módulos izquierdos y todos los resultados que se prueben para esto, también se cumplirán para los derechos.

#### Ejercicio 1.1.1

Sea  $A$  un  $R$ -módulo izquierdo. Si  $R$  es conmutativo, podemos hacer de  $A$  un  $R$ -módulo derecho

definiendo:

$$ar = ra, \quad \forall a \in A \text{ y } \forall r \in R$$

### Demostración:

Considere la función de  $\cdot : A \times R \rightarrow A$  dada por:

$$(a, r) \mapsto ar = ra, \quad \forall (a, r) \in A \times R$$

Afirmamos que esta función hace de  $A$  un  $R$ -módulo derecho. En efecto, debemos verificar tres condiciones, sean  $r, s \in R$  y  $a, b \in A$ :

(1) Se tiene que:

$$\begin{aligned}(a + b)r &= r(a + b) \\ &= ra + rb \\ &= ar + br\end{aligned}$$

(2) Se tiene que:

$$\begin{aligned}a(r + s) &= (r + s)a \\ &= ra + sa \\ &= ar + as\end{aligned}$$

(3) Se tiene que:

$$\begin{aligned}(as)r &= r(as) \\ &= r(sa) \\ &= (rs)a, \text{ como } R \text{ es conmutativo:} \\ &= (sr)a \\ &= a(sr)\end{aligned}$$

por los tres incisos anteriores se sigue que  $A$  es un  $R$ -módulo derecho. ■

#### Observación 1.1.1

A menos que se especifique lo contrario, todo  $R$ -módulo  $A$  sobre un anillo conmutativo  $R$  será izquierdo y derecho haciendo:

$$ra = ar, \quad \forall a \in A \text{ y } \forall r \in R$$

#### Observación 1.1.2

Denotaremos al elemento identidad de un  $R$ -módulo  $A$  por  $0_A$ , y al elemento neutro de  $R$  por  $0_R$ .

---

#### Proposición 1.1.1

Sea  $A$  un  $R$ -módulo, entonces:

$$r0_A = 0_A \quad \text{y} \quad 0_R a = 0_A$$

para todo  $r \in R$  y para todo  $a \in A$ .

---

### Demostración:

Sea  $r \in R$ , se tiene que:

$$r0_A = r(0_A + 0_A) = r0_A + r0_A \Rightarrow r0_A = 0_A$$

y, para todo  $a \in A$ :

$$0_R a = (0_R + 0_R)a = 0_R a + 0_R a \Rightarrow 0_R a = 0_A$$

■

Por lo que, en lo que sigue del texto se denotará por  $0$  a  $0_A, 0_R, 0 \in \mathbb{Z}$  y al módulo trivial  $\{0\}$ .

#### Ejemplo 1.1.1

Todo grupo abeliano  $G$  es un  $\mathbb{Z}$  módulo unitario izquierdo (en particular, puede ser derecho por ser abeliano), bajo la operación  $(n, a) \mapsto na$ , siendo  $na$  la suma de  $a$  consigo mismo  $n$ -veces.

#### Ejemplo 1.1.2

Si  $S$  es un anillo y  $R$  es un subanillo, entonces  $S$  es un  $R$ -módulo (pero no al revés, ya que puede que la operación se salga de  $S$ ) con  $ra$  siendo  $r \in R$  y  $a \in S$ . En particular, los anillos:

$$R[x_1, \dots, x_n] \quad \text{y} \quad R[[x]]$$

son  $R$ -módulos, los cuáles son unitarios si  $R$  posee identidad.

#### Ejemplo 1.1.3

Sean  $R, S$  anillos y  $\varphi : R \rightarrow S$  un homomorfismo de anillos. Entonces todo  $S$ -módulo puede hacerse un  $R$ -módulo definiendo  $rx$  (con  $x \in A$ ) por  $\varphi(r)x$ , esto es:

$$rx = \varphi(r)x$$

donde la operación de la derecha se toma en el  $S$ -módulo,  $A$ . En este caso se dice que la estructura de  $R$ -módulo de  $A$  está dada por el **pullback a lo largo de  $\varphi$** .

#### Definición 1.1.3

Sean  $A$  y  $B$  módulos sobre un anillo  $R$ . Una función  $f : A \rightarrow B$  es un **homomorfismo de  $R$ -módulos**, si para todo  $a, b \in A$  y para todo  $r \in R$  se tiene que:

$$f(a + b) = f(a) + f(b) \quad \text{y} \quad f(ra) = rf(a)$$

si  $R$  es un anillo de división, entonces  $f$  es llamada **transformación lineal**.

En el contexto actual, los homomorfismos de  $R$ -módulos serán simplemente llamados homomorfismos. Se adopta la misma terminología de monomorfismo, epimorfismo e isomorfismo. Se define también de forma análoga el **núcleo** o **kernel** de  $f$  por:

$$\ker(f) = \left\{ a \in A \mid f(a) = 0 \right\}$$

con lo que se tienen los siguientes resultados (que provienen directamente de lo probado en anillos):

#### Teorema 1.1.1

Sean  $A$  y  $B$  dos  $R$ -módulos y  $f : A \rightarrow B$  un homomorfismo.

(a)  $f$  es monomorfismo si y sólo si  $\ker(f) = \{0\}$ .

(b)  $f$  es isomorfismo si y sólo si existe un homomorfismo de  $R$ -módulos  $g : B \rightarrow A$  tal que  $g \circ f = \mathbb{1}_A$  y  $f \circ g = \mathbb{1}_B$ .

#### Ejemplo 1.1.4

Todo homomorfismo entre grupos abelianos es un homomorfismo de  $\mathbb{Z}$ -módulos.

#### Ejemplo 1.1.5

Si  $R$  es un anillo, la función de  $R[x]$  en  $R[x]$  dada por:  $f(x) \mapsto xf(x)$  es un homomorfismo de  $R$ -módulos, pero no es un homomorfismo de anillos (no separa productos).

#### Observación 1.1.3

Para un anillo  $R$  dado, la clase de todos los  $R$ -módulos forma una categoría concreta, denotada por  $\mathcal{M}_R$  para los módulos derechos y  ${}_R\mathcal{M}$  para los izquierdos.

#### Definición 1.1.4

Sea  $R$  un anillo,  $A$  un  $R$ -módulo y  $B \subseteq A$  un subconjunto no vacío. Se dice que  $B$  es un **submódulo de  $A$**  si  $B$  es un subgrupo aditivo de  $A$  y, para todo  $r \in R$  se tiene que:

$$rb \in B, \quad \forall b \in B$$

un submódulo de un espacio vectorial es llamado **subespacio vectorial**.

#### Observación 1.1.4

Todo submódulo es en sí mismo un módulo. Todo submódulo de un módulo unitario es también unitario.

#### Ejemplo 1.1.6

Si  $\{B_i \mid i \in I\}$  es una familia de submódulos de un módulo  $A$ , entonces  $\bigcap_{i \in I} B_i$  es un submódulo de  $A$ .

#### Definición 1.1.5

Sea  $A$  un  $R$ -módulo y  $X \subseteq A$ , entonces la intersección de todos los submódulos que contienen a  $X$  es llamado el **submódulo generado por  $X$** .

Si  $X$  es finito y  $X$  genera al módulo  $B$ , se dice que  $B$  es **finitamente generado**. Si  $X$  tiene un solo elemento, se dice que  $B$  es un **módulo cíclico**.

Si  $\{B_i\}_{i \in I}$  es una familia de submódulos de  $A$ , entonces el submódulo generado por  $\bigcup_{i \in I} B_i$  es llamado la **suma de los módulos  $B_i$** . Si el conjunto  $I$  es finito, esto se denota por:

$$B_1 + \cdots + B_n$$

#### Teorema 1.1.2

Sea  $R$  un anillo,  $A$  un  $R$ -módulo,  $X \subseteq A$ ,  $\{B_i\}_{i \in I}$  una familia de submódulos de  $A$  y  $a \in A$ . Tomemos  $Ra = \{ra \mid r \in R\}$ .

(a)  $Ra$  es un submódulo de  $A$  y la función de  $R$  en  $Ra$  dada por  $r \mapsto ra$  es un epimorfismo de  $R$ -módulos.

(b) El submódulo cíclico  $C$  generado por  $a$  es

$$\left\{ ra + na \mid r \in R, n \in \mathbb{Z} \right\}$$

si  $R$  tiene identidad y  $C$  es unitario, entonces  $C = Ra$ .

(c) El submódulo  $D$  generado por  $X$  es:

$$\left\{ \sum_{i=1}^s r_i a_i + \sum_{j=1}^t n_j b_j \mid s, t \in \mathbb{N}^*; a_i, b_j \in X; r_i \in R; n_j \in \mathbb{Z} \right\}$$

si  $R$  tiene identidad y  $A$  es unitario, entonces:

$$D = RX = \left\{ \sum_{i=1}^s r_i a_i \mid i \in \mathbb{N}^*; r_i \in R; a_i \in X \right\}$$

(d) La suma de la familia  $\{B_i \mid i \in I\}$  consiste de todas las sumas finitas  $b_1 + \cdots + b_{i_n}$  con  $b_{i_k} \in B_{i_k}$  para todo  $k = 1, \dots, n$ .

### **Demostración:**

De (a): Veamos que  $Ra$  es un  $R$ -módulo. Claramente  $s(ra)$  está bien definida (sigue en  $Ra$  ya que  $A$  es un  $R$ -módulo). Veamos que:

- Sean  $ra, sa \in Ra$ , entonces:

$$t(ra + sa) = t(ra) + t(sa)$$

- Sean  $r, s \in R$  y  $ta \in Ra$ , entonces:

$$\begin{aligned} (r + s)(ta) &= ((r + s)t)a \\ &= (rt + st)a \\ &= (rt)a + (st)a \\ &= r(ta) + s(ta) \end{aligned}$$

- Sean  $r, s \in R$  y  $ta \in Ra$ , entonces:

$$\begin{aligned} r(s(ta)) &= r((st)a) \\ &= (r(st))a \\ &= ((rs)t)a \\ &= (rs)(ta) \end{aligned}$$

por tanto,  $Ra$  es un  $R$ -módulo. Claramente la función  $r \mapsto ra$  es un epimorfismo de módulos.

De (b): Sea  $C$  el submódulo cíclico generado por  $a$ , esto es, es la intersección de todos los submódulos que contienen a  $a$ . ■

### **Teorema 1.1.3**

Sea  $B$  un submódulo de un módulo  $A$  sobre un anillo  $R$ . Entonces, el grupo cociente  $A/B$  es un  $R$ -módulo con la acción de  $R$  en  $A/B$  dada por:

$$r(a + B) = ra + B, \quad \forall r \in R \text{ y } \forall a \in A$$

la función  $\pi : A \rightarrow A/B$  dada por  $a \mapsto a + B$  es un epimorfismo de  $R$ -módulos con kernel  $B$ .

---

**Demostración:**

Como  $B$  es submódulo de  $A$ , en particular es subgrupo del grupo abeliano  $A$ , por lo que el grupo cociente  $A/B$  está bien definido. Consideremos ahora la operación

$$(r, a + B) \mapsto r(a + B) = ra + B$$

de  $R \times A/B$  en  $A/B$ . Afirmamos que esta función está bien definida. En efecto, si  $a, a' \in A$  son tales que  $a - a' \in B$ , entonces al ser  $B$  submódulo de  $A$ , se sigue que  $r(a - a') = ra - ra' \in B$ , lo cual implica que:

$$ra + B = ra' + B$$

así, la acción está bien definida. Veamos ahora que  $A/B$  es un  $R$ -módulo. En efecto, hay que verificar tres condiciones:

(a) Sean  $r \in R$  y  $a, c \in A$ . Entonces:

$$\begin{aligned} r[(a + B) + (c + B)] &= r[a + c + B] \\ &= r(a + c) + B \\ &= ra + rc + B \\ &= (ra + B) + (rc + B) \\ &= r(a + B) + r(c + B) \end{aligned}$$

(b) Sean  $r, s \in R$  y  $a \in A$ . Entonces:

$$\begin{aligned} (r + s)(a + B) &= (r + s)a + B \\ &= ra + sa + B \\ &= (ra + B) + (sa + B) \\ &= r(a + B) + s(a + B) \end{aligned}$$

(c) Sean  $s, t \in R$  y  $a \in A$ . Entonces:

$$\begin{aligned} r(s(a + B)) &= r(sa + B) \\ &= r(sa) + B \\ &= (rs)a + B \\ &= (rs)(a + B) \end{aligned}$$

por los incisos anteriores se sigue que  $A/B$  es un  $R$ -módulo. Ya se sabe que  $\pi : A \rightarrow A/B$  es un epimorfismo de grupos, para ver que lo es de  $R$ -módulos, veamos que:

$$\begin{aligned} \pi(r(a + B)) &= \pi(ra + B) \\ &= ra \\ &= r\pi(a + B) \end{aligned}$$

para todo  $a \in A$  y para todo  $r \in R$ . Por ende,  $\pi$  es un epimorfismo de  $R$ -módulos. ■

También se cumplen los teoremas de isomorfismos, que solo se van a enlistar (después se van a probar, solo falta con ver que es homomorfismo de  $R$ -módulos dependiendo del caso).



---

**Teorema 1.1.4 (Primer Teorema de Isomorfismo)**

Sea  $R$  un anillo,  $f : A \rightarrow B$  un homomorfismo de  $R$ -módulos y  $C$  un submódulo de  $\ker f$ . Entonces, existe un único homomorfismo de  $R$ -módulos  $\bar{f} : A/C \rightarrow B$  tal que

$$\bar{f}(a + C) = f(a), \quad \forall a \in A$$

además,  $\text{Im } \bar{f} = \text{Im } f$  y  $\ker \bar{f} = \ker f / C$ . Además,  $\bar{f}$  es un isomorfismo de  $R$ -módulos si y sólo si  $f$  es un epimorfismo de  $R$ -módulos tal que  $C = \ker f$ . En particular,

$$A / \ker f \cong \text{Im } f$$

---

**Corolario 1.1.1**

Sea  $R$  un anillo,  $A'$  un submódulo del  $R$ -módulo  $A$  y  $B'$  submódulo del  $R$ -módulo  $B$  y  $f : A \rightarrow B$  un homomorfismo de  $R$ -módulos tal que  $f(A') \subseteq B'$ . Entonces,  $f$  induce un homomorfismo de  $R$ -módulos  $\bar{f} : A/A' \rightarrow B/B'$  dado por:

$$a + A' \mapsto f(a) + B'$$

$\bar{f}$  es un isomorfismo de  $R$ -módulos si y sólo si  $\text{Im } f + B' = B$  y  $f^{-1}(B') \subseteq A'$ . En particular, si  $f$  es un epimorfismo tal que  $f(A') = B'$  y  $\ker f \subseteq A'$  entonces  $\bar{f}$  es un isomorfismo de  $R$ -módulos.

---

**Teorema 1.1.5 (Segundo y Tercer Teorema de isomorfismos)**

Sean  $B$  y  $C$  submódulos de un  $R$ -módulo  $A$ .

- (a) Existe un isomorfismo de  $R$ -módulos,  $B/(B \cap C) \cong (B + C)/C$ .
  - (b) Si  $C \subseteq B$ , entonces  $B/C$  es un submódulo de  $A/C$ , y existe un isomorfismo de  $R$ -módulos,  $(A/C)/(B/C) \cong A/B$ .
- 

**Teorema 1.1.6**

Si  $R$  es un anillo y  $B$  es un submódulo de un  $R$ -módulo  $A$ , entonces existe una correspondencia uno a uno en el conjunto de todos los submódulos de  $A$  que contienen a  $B$  y el conjunto de todos los submódulos de  $A/B$ , dada por  $C \mapsto C/B$ . Por tanto, todo submódulo de  $A/B$  es de la forma  $C/B$  donde  $C$  es un submódulo de  $A$  que contiene a  $B$ .

---

Ahora daremos la existencia de los productos y coproductos en la categoría  ${}_R\mathcal{M}$ .

---

**Teorema 1.1.7**

Sea  $R$  un anillo y  $\{A_i\}_{i \in I}$  una familia no vacía de  $R$ -módulos,  $\prod_{i \in I} A_i$  el producto directo de los grupos abelianos  $A_i$ , y  $\sum_{i \in I} A_i$  la suma directa de los grupos abelianos.

- (a)  $\prod_{i \in I} A_i$  es un  $R$ -módulo con la acción de  $R$  dada por:  $(rf)(i) = rf(i)$ , para todo  $f \in \prod_{i \in I} A_i$  y para todo  $i \in I$ . En otras palabras, si  $\{a_i\}_{i \in I} \in \prod_{i \in I} A_i$ , entonces  $r\{a_i\}_{i \in I} = \{ra_i\}_{i \in I}$ .
- (b)  $\sum_{i \in I} A_i$  es un submódulo de  $\prod_{i \in I} A_i$ .
- (c) Para cada  $k \in I$ , la proyección canónica  $\pi_k : \prod_{i \in I} A_i \rightarrow A_k$  es un epimorfismo de  $R$ -módulos.
- (d) Para cada  $k \in I$ , la inyección canónica  $\iota_k : A_k \rightarrow \prod_{i \in I} A_i$  es un monomorfismo de  $R$ -módulos.

### Demostración:

De (a): Ya se sabe que  $\prod_{i \in I} A_i$  es un grupo abeliano, veamos que con la acción

$$(r, \{a_i\}_{i \in I}) \mapsto r \{a_i\}_{i \in I} = \{ra_i\}_{i \in I}$$

es un  $R$ -módulo. En efecto, verifiquemos las tres condiciones:

(1) Sean  $\{a_i\}_{i \in I}, \{b_i\}_{i \in I} \in \prod_{i \in I} A_i$  y  $r \in R$ , se tiene que:

$$\begin{aligned} r(\{a_i\}_{i \in I} + \{b_i\}_{i \in I}) &= r \{a_i + b_i\}_{i \in I} \\ &= \{r(a_i + b_i)\}_{i \in I} \\ &= \{ra_i + rb_i\}_{i \in I} \\ &= \{ra_i\}_{i \in I} + \{rb_i\}_{i \in I} \\ &= r \{a_i\}_{i \in I} + r \{b_i\}_{i \in I} \end{aligned}$$

(2) Sean  $r, s \in R$  y  $\{a_i\}_{i \in I} \in \prod_{i \in I} A_i$ , se tiene que:

$$\begin{aligned} (r + s) \{a_i\}_{i \in I} &= \{(r + s)a_i\}_{i \in I} \\ &= \{ra_i + sa_i\}_{i \in I} \\ &= \{ra_i\}_{i \in I} + \{sa_i\}_{i \in I} \\ &= r \{a_i\}_{i \in I} + s \{a_i\}_{i \in I} \end{aligned}$$

(3) Sean  $r, s \in R$  y  $\{a_i\}_{i \in I} \in \prod_{i \in I} A_i$ , se tiene que:

$$\begin{aligned} r(s \{a_i\}_{i \in I}) &= r \{sa_i\}_{i \in I} \\ &= \{r(sa_i)\}_{i \in I} \\ &= \{(rs)a_i\}_{i \in I} \\ &= (rs) \{a_i\}_{i \in I} \end{aligned}$$

por los incisos anteriores, se sigue que  $\prod_{i \in I} A_i$  es un  $R$ -módulo.

De (b): Se sigue del hecho de que para todo  $r \in R$ ,  $r0_{A_i} = 0_{A_i}$ , para todo  $i \in I$ .

De (c) y (d): Son inmediatos por la definición de la acción de  $R$  sobre  $\prod_{i \in I} A_i$ . ■

#### Definición 1.1.6

En el contexto del teorema anterior,  $\prod_{i \in I} A_i$  es llamado el **producto directo (externo)** de la familia de  $R$ -módulos,  $\{A_i\}_{i \in I}$  y  $\sum_{i \in I} A_i$  es llamado la **suma directa (externa)** de la familia de  $R$ -módulos,  $\{A_i\}_{i \in I}$ .

En el caso en que  $I$  sea finito, digamos  $I = \{1, \dots, n\}$ , el producto directo y la suma directa coincidirán y se denotarán simplemente por:

$$A_1 \oplus A_2 \oplus \dots \oplus A_n$$

Las funciones  $\pi_k$  (respectivamente,  $\iota_k$ ) son llamadas **proyecciones canónicas** (respectivamente, **inyecciones**).

## 1.2. Secuencias Exactas

**Definición 1.2.1**

Un par de homomorfismos de módulos

$$A \xrightarrow{f} B \xrightarrow{g} C$$

se dice **exacta en**  $B$ , si  $\text{Im} f = \ker g$ .

Una secuencia finita de homomorfismos de módulos

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} A_n$$

se dice **exacta**, si

$$\text{Im} f_i = \ker f_{i+1}, \quad \forall i = 0, 1, \dots, n-1$$

Una secuencia infinita de homomorfismos de módulos

$$\dots \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \dots$$

es **exacta**, si  $\text{Im} f_i = \ker f_{i+1}$ , para todo  $i \in \mathbb{Z}$ .

Siempre que sea conveniente, nos referiremos a la secuencia exacta de homomorfismos módulos como la secuencia de módulos.

**Ejemplo 1.2.1**

Sea  $A$  un  $R$ -módulo. Existen únicos homomorfismos de módulos  $0 \rightarrow A$  y  $A \rightarrow 0$ . Por lo que, podemos considerar a la secuencia:

$$0 \rightarrow A \rightarrow 0$$

pero esta no es exacta, ya que la imagen del primer homomorfismo es 0 y el kernel del segundo es  $A$ .

**Ejemplo 1.2.2**

Si  $A$  y  $B$  son módulos sobre un anillo  $R$ , entonces las secuencias:

$$0 \rightarrow A \xrightarrow{\iota_1} A \oplus B \xrightarrow{\pi_2} B \rightarrow 0 \text{ y } 0 \rightarrow B \xrightarrow{\iota_2} A \oplus B \xrightarrow{\pi_1} A \rightarrow 0$$

son exactas, donde  $\pi$ 's y  $\iota$ 's son las proyecciones e inyecciones canónicas, respectivamente.

**Ejemplo 1.2.3**

Si  $C$  es submódulo de un módulo  $D$ , entonces la secuencia

$$0 \rightarrow C \xrightarrow{i} D \xrightarrow{\pi} D/C \rightarrow 0$$

es exacta, siendo  $i : C \rightarrow D$  el mapeo inclusión, y  $\pi : D \rightarrow D/C$  el epimorfismo canónico.

**Definición 1.2.2**

Si  $f : A \rightarrow B$  es un homomorfismo de módulos, entonces  $A/\ker f$  (respectivamente,  $B/\text{Im} f$ ) es llamada la **coimagen** de  $f$  (respectivamente, **cokernel** de  $f$ ) y es denotado por  $\text{Coim} f$  (respectivamente,  $\text{Coker} f$ ).

### Ejemplo 1.2.4

Sea  $f : A \rightarrow B$  es un homomorfismo de módulos. Entonces, cada una de las siguientes secuencias es exacta:

- (a)  $0 \rightarrow \ker f \rightarrow A \rightarrow \text{Coim} f \rightarrow 0$ .
- (b)  $0 \rightarrow \text{Im} f \rightarrow B \rightarrow \text{Coker} f \rightarrow 0$ .
- (c)  $0 \rightarrow \ker f \rightarrow A \xrightarrow{f} B \rightarrow \text{Coker} f \rightarrow 0$ .

### Observación 1.2.1

Se tiene que  $0 \rightarrow A \xrightarrow{f} B$  es una secuencia exacta si y sólo si  $f$  es monomorfismo. Similarmente,  $B \xrightarrow{g} C \rightarrow 0$  es exacta si y sólo si  $g$  es epimorfismo de módulos.

Si  $A \xrightarrow{f} B \xrightarrow{g} C$  es exacta, entonces:  $g \circ f = 0$ , pues  $\text{Im} f = \ker g$ .

Finalmente, si  $A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  es exacta, entonces:  $\text{Coker} f = B/\text{Im} f = B/\ker g = \text{Coim} g \cong C$ .

### Definición 1.2.3

Una secuencia exacta de la forma:

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

es llamada una **secuencia exacta corta**. Observe que en particular,  $f$  es monomorfismo y  $g$  es epimorfismo.

Con la observación y definición anterior, una secuencia exacta es sólo una forma de presentar un submódulo ( $A \cong \text{Im} f$ ) y su módulo cociente ( $B/\text{Im} f = B/\ker g \cong C$ ).

### Lema 1.2.1 (El Lema de los cinco cortos)

Sea  $R$  un anillo, y

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

Figura 1. Diagrama del Lema de los cinco cortos.

un diagrama conmutativo de  $R$ -módulos y homomorfismos de  $R$ -módulos tal que cada fila es una secuencia exacta. Entonces:

- (a)  $\alpha, \gamma$  monomorfismos implica que  $\beta$  es monomorfismo.
- (b)  $\alpha, \gamma$  epimorfismos implica que  $\beta$  es epimorfismo.
- (c)  $\alpha, \gamma$  isomorfismos implica que  $\beta$  es isomorfismo.

### Demostración:

De (a):

■

## 1.3. Ejercicios

### Observación 1.3.1

$R$  es un anillo.

#### Ejercicio 1.3.1

Si  $A$  es un grupo abeliano y  $n > 0$  es natural tal que  $na = 0$  para todo  $a \in A$ , entonces  $A$  es un  $\mathbb{Z}/\mathbb{Z}n$ -módulo unitario con la acción dada por:

$$[k]a = ka, \quad \forall k \in \mathbb{Z}$$

#### Demostración:

Primero, veremos que la acción está bien definida. En efecto, sean  $k, l \in \mathbb{Z}$  tales que  $[k] = [l]$ , entonces  $k - l \in \mathbb{Z}n$ , es decir que existe  $q \in \mathbb{Z}$  tal que:

$$k - l = qn$$

Por tanto:

$$\begin{aligned} [k]a &= ka \\ &= (qn + l)a \\ &= (qn)a + la \\ &= 0 + la \\ &= la \\ &= [l]a \end{aligned}$$

por lo cual, la acción está bien definida. Veamos ahora que en efecto,  $A$  es un  $\mathbb{Z}/\mathbb{Z}n$ -módulo:

(a)

■

#### Ejercicio 1.3.2

Sea  $f : A \rightarrow B$  un homomorfismo de  $R$ -módulos.

(a)  $f$  es monomorfismo si y sólo si para todo par de homomorfismos de  $R$ -módulos,  $g, h : D \rightarrow A$  tales que  $f \circ g = f \circ h$ , tenemos que  $g = h$ .

(b)

#### Demostración:

■

#### Ejercicio 1.3.3

Sea  $I$  un ideal izquierdo de un anillo  $R$  y sea  $A$  un  $R$ -módulo.

(a) Si  $S$  es un subconjunto no vacío de  $A$ , entonces

$$IS = \left\{ \sum_{i=1}^n r_i a_i \mid n \in \mathbb{N}^*; r_i \in I; a_i \in S \right\}$$

es un submódulo de  $A$ . Note que si  $S = \{a\}$ , entonces  $IS = Ia = \{ra \mid r \in I\}$ .

(b) Si  $I$  es un ideal por ambos lados, entonces  $A/IA$  es un  $R/I$  módulo con la acción de  $R/I$  dada por:

$$(r + I)(a + I) = ra + IA$$

**Demostración:**

**Ejercicio 1.3.4**

Si  $R$  tiene identidad, entonces todo  $R$ -módulo unitario cíclico es isomorfo a un  $R$ -módulo de la forma  $R/J$ , donde  $J$  es un ideal izquierdo de  $R$ .

**Demostración:**

Sea  $C$  el  $R$ -módulo unitario cíclico generado por  $a$ , esto es:

$$C = \{ra \mid r \in R\}$$

definimos el conjunto  $J$  dado por:

$$J = \{r \in R \mid ra = 0\}$$

Afirmamos que  $J$  es ideal izquierdo de  $R$ . En efecto, veamos que:

(1) Sean  $s, t \in J$ , se tiene que:

$$\begin{aligned}(s - t)a &= sa - ta \\ &= 0\end{aligned}$$

por ende,  $s - t \in J$ .

(2) Sea  $s \in J$  y  $r \in R$ , se tiene que:

$$\begin{aligned}(rs)a &= r(sa) \\ &= r \cdot 0 \\ &= 0\end{aligned}$$

por ende,  $rs \in J$ .

por los dos incisos anteriores se sigue que  $J$  es un ideal izquierdo de  $R$ . Por ejemplos anteriores se tiene que  $R/J$  es un  $R$ -módulo. Considere la función  $f : C \rightarrow R/J$  dado por:

$$f(ra) = r + J, \quad \forall ra \in C$$

afirmamos que  $f$  es un homomorfismo de  $R$ -módulos. En efecto:

■  **$f$  es homomorfismo de  $R$ -módulos.** Sean  $r_1a_1, r_2a_2 \in C$ . Se tiene:

$$\begin{aligned}f(r_1a_1 + r_2a_2) &= r_1 + r_2 + J \\ &= (r_1 + J) + (r_2 + J) \\ &= f(r_1a_1) + f(r_2a_2)\end{aligned}$$

y, si  $ra \in C$ , entonces para  $t \in R$  se tiene que:

$$\begin{aligned}f(t(ra)) &= f((tr)a) \\ &= tr + J \\ &= t(r + J) \\ &= tf(ra)\end{aligned}$$

- $f$  es **monomorfismo**: Sea  $ra \in C$ . Veamos que:

$$\begin{aligned} f(ra) = J &\iff r + J = J \\ &\iff r \in J \\ &\iff ra = 0 \end{aligned}$$

por lo que,  $\ker f = \{0\}$ .

- Para cada  $r + J \in R/J$  existe  $ar \in C$  tal que  $f(ar) = r + J$ .

por los tres incisos anteriores, se tiene que  $f$  es isomorfismo de  $R$ -módulos. ■

### Definición 1.3.1

Si  $R$  tiene identidad, entonces un  $R$ -módulo unitario  $A$  no cero es **simple** si sus únicos submódulos son  $0$  y  $A$ .

### Ejercicio 1.3.5

Pruebe lo siguiente:

- (1) Todo  $R$ -módulo simple es cíclico.
- (2) Si  $A$  es simple, entonces todo  $R$ -módulo endomorfismo es la función cero o es un isomorfismo.

### Demostración:

De (1): Sea  $A$  un  $R$ -módulo simple. Si  $A$  no es el módulo  $0$ , entonces existe  $c \in A$  no cero. Considere el  $R$ -módulo generado por  $c$ , digamos:

$$C = \{rc + nc \mid r \in R; n \in \mathbb{Z}\}$$

como  $A$  es simple, debe suceder que  $C = A$  ya que  $c \neq 0$  y  $c \in C$ . Por tanto,  $A$  es cíclico.

De (2): Sea  $f : A \rightarrow A$  un  $R$ -módulo endomorfismo. Por un teorema anterior se tiene que  $\ker f$  es un submódulo de  $A$ , el cual debe ser  $0$ , lo cual implicaría que  $f$  es isomorfismo, o es  $A$ , lo cual implicaría que  $f$  es la función cero. ■

### Ejercicio 1.3.6

Pruebe que un  $R$ -módulo finitamente generado no necesariamente es un grupo abeliano finitamente generado.

### Demostración:

Considere el grupo  $(\mathbb{Q}, +)$ , se tiene que este grupo no es finitamente generado. En efecto, si lo fuese sería de la forma:

$$\mathbb{Q} = \langle a_1, \dots, a_n \rangle$$

con  $a_1, \dots, a_n \in \mathbb{Q} \setminus \{0\}$ . Podemos asumir sin pérdida de generalidad que  $a_i \geq 0$  para todo  $i = 1, \dots, n$ . También, estos elementos son de la forma:

$$a_i = \frac{p_i}{q_i}, \quad \forall i = 1, \dots, n$$

donde  $p_i, q_i \in \mathbb{N}$  son primos relativos. Sea

$$q = q_1 \cdots q_n$$

Considere ahora el conjunto:

$$A = \left\{ qa \mid a \in \langle a_1, \dots, a_n \rangle; a > 0 \right\}$$

al ser todos los elementos de  $\langle a_1, \dots, a_n \rangle$  sumas finitas de  $a_i$ , entonces se tiene que los elementos de  $A$  son números naturales. Así que  $A$  es un subconjunto de los naturales no vacío, en particular tiene primer elemento, digamos  $p$ . Se tiene que  $\frac{p}{q}$  es el mínimo elemento positivo de  $\langle a_1, \dots, a_n \rangle$ . Ahora, sabemos que:

$$\frac{p}{q+1} \in \mathbb{Q}$$

pero,  $\frac{p}{q+1} \notin \langle a_1, \dots, a_n \rangle$ , pues este elemento es menor que el mínimo elemento positivo de este conjunto. Por ende,  $\mathbb{Q}$  no es finitamente generado como grupo abeliano.

Pero,  $\mathbb{Q}$  es un  $\mathbb{Q}$ -módulo, el cual es finitamente generado por 1 (se verifica rápidamente). ■

### Ejercicio 1.3.7

**Demostración:** ■

### Ejercicio 1.3.8

Sea  $f : A \rightarrow A$  un homomorfismo de  $R$ -módulos tal que  $f \circ f = f$ , entonces:

$$A = \ker f \oplus \operatorname{Im} f$$

**Demostración:**

Veamos primero que  $A = \ker f + \operatorname{Im} f$ . Sea  $a \in A$ , si  $a \notin \operatorname{Im} f$ , entonces veamos que:

$$f(a) = f(f(a)) \Rightarrow f(a - f(a)) = 0$$

por lo que,  $a - f(a) \in \ker f$ , luego  $a \in \ker f + \operatorname{Im} f$  (pues,  $f(a) \in \operatorname{Im} f$ ).

Veamos ahora que es suma directa interna. En efecto, sea  $a \in \ker f \cap \operatorname{Im} f$ , entonces existe  $b \in A$  tal que:

$$f(b) = a$$

como  $a \in \ker f$  se sigue que  $f(a) = 0$ . Observemos que:

$$f(b) = f(f(b)) = f(a) = 0$$

por lo que,  $b \in \ker f$ , así que  $a = f(b) = 0$ , esto es que  $a = 0$ . Por tanto, se tiene que la suma es directa, esto es:

$$A = \ker f \oplus \operatorname{Im} f$$

### Ejercicio 1.3.9 (Nombre)

**Demostración:** ■

### Ejercicio 1.3.10

Haga lo siguiente:

- (a) Si  $A$  es un módulo sobre un anillo conmutativo  $R$  y  $a \in A$ , entonces  $\mathcal{O}_a = \left\{ r \in R \mid ra = 0 \right\}$



es un ideal de  $R$ . Si  $\mathcal{O}_a \neq 0$ , se dice que  $a$  es un **elemento de torsión** de  $A$ .

- (b) Si  $R$  es un dominio entero, entonces el conjunto  $T(A)$  de todos los elementos de torsión de  $A$  es un submódulo de  $A$  ( $T(A)$  es llamado el **submódulo de torsión**).
- (c) Muestre que el inciso anterior puede ser falso para un anillo conmutativo  $R$  que no sea dominio entero.

en lo que sigue,  $R$  es un dominio entero.

- (d) Si  $f : A \rightarrow B$  es un homomorfismo de  $R$ -módulos, entonces  $f(T(A)) \subseteq T(B)$ ; por ende, la restricción  $f_T$  de  $f$  a  $T(A)$  es un homomorfismo de  $R$ -módulos.
- (e) Si  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C$  es una secuencia exacta de  $R$ -módulos, entonces también lo es  $0 \rightarrow T(A) \xrightarrow{f_T} T(B) \xrightarrow{g_T} T(C)$ .

## Capítulo 2

# Módulos Libres y Espacios Vectoriales

### 2.1. Conceptos Fundamentales

No queda de otra más que asumir este resultado de categorías:

---

**Teorema 2.1.1 (Hungerford, Theorem I.7.8)**

Si  $\mathcal{C}$  es una categoría concreta,  $F$  y  $F'$  son objetos en  $\mathcal{C}$  tales que  $F$  es libre en el conjunto  $X$  y  $F'$  lo es en  $X'$  siendo estos conjuntos tales que  $|X| = |X'|$ , entonces  $F$  es equivalente a  $F'$ .

---

En particular, la categoría de  $R$ -módulos unitarios es una categoría concreta, donde la equivalencia entre dos objetos de la categoría es un isomorfismo entre ambos  $R$ -módulos.

---

**Teorema 2.1.2**

Sea  $R$  un anillo conmutativo con identidad. Las siguientes condiciones son equivalentes en un  $R$ -módulo unitario  $F$ :

- I.  $F$  tiene base no vacía.
- II.  $F$  es la suma interna directa de una familia cíclica de  $R$ -módulos, cada uno de los cuales es isomorfo a  $R$  como un  $R$ -módulo.
- III.  $F$  es un  $R$ -módulo isomorfo a la suma directa de copias del  $R$ -módulo izquierdo  $R$ .
- IV. Existe un conjunto no vacío  $X$  y una función  $i : X \rightarrow F$  con la siguiente propiedad: dado un  $R$ -módulo,  $A$  y una función  $f : X \rightarrow A$  existe un único homomorfismo de  $R$ -módulos  $\bar{f} : F \rightarrow A$  tal que

$$\bar{f} \circ i = f$$

En otras palabras,  $F$  es un objeto libre en la categoría de  $R$ -módulos unitarios.

---

**Demostración:**

(i)  $\Rightarrow$  (iv): Sea  $X$  una base no vacía de  $F$  y sea  $i : X \rightarrow F$  el mapeo inclusión. Sea  $A$  un  $R$ -módulo y  $f : X \rightarrow A$  una función.

Si  $u \in F$ , entonces existen  $n \in \mathbb{N} \cup \{0\}$ ,  $r_i \in R$  y  $x_i \in X$ , para todo  $i \in \{1, \dots, n\}$  tales que

$$u = \sum_{i=1}^n r_i x_i$$

Definimos la función  $\bar{f} : F \rightarrow A$  dada por:

$$\bar{f}(u) = \sum_{i=1}^n r_i f(x_i)$$

Esta función está bien definida, pues  $F$  tiene como base a  $X$  (por ende, todo elemento se representa de forma única como combinación lineal finita de elementos de  $X$ ). Además,

$$\begin{aligned}\bar{f} \circ i(x_i) &= \bar{f}(x_i) \\ &= 1_R \cdot f(x_i) \\ &= f(x_i), \quad \forall x_i \in X\end{aligned}$$

por ende,  $\bar{f} \circ i = f$ .

Veamos que es homomorfismo de  $R$ -módulos (no sé como se verifica eso, chécalo porfa Roque).

Ahora, si  $g : F \rightarrow A$  es otro homomorfismo de  $R$ -módulos tal que

$$g \circ i = f$$

se tiene que

$$\bar{f} \circ i = g \circ i \Rightarrow \bar{f}|_X = g|_X$$

Como  $X$  genera  $F$  y todo homomorfismo de  $R$ -módulos que vaya de  $F$  en algún  $R$ -módulo,  $B$  queda únicamente determinado por  $X$ , basta ver que  $\bar{f} = g$  en  $X$ , lo cual sucede por la igualdad anterior. Por tanto,  $\bar{f}$  es único.

(iv)  $\Rightarrow$  (iii): Asumiendo (iv), sean  $X \subseteq F$  no vacío y una función  $i : X \rightarrow F$  que cumplan esta propiedad. Considere el  $R$ -módulo

$$A = \sum_{x \in X} R$$

(es decir, es la suma directa de  $|X|$ -veces el  $R$ -módulo izquierdo  $R$ ). Sea

$$Y = \left\{ \theta_x \mid x \in X \right\}$$

donde

$$\theta_x(y) = \begin{cases} 1_R & \text{si } y = x \\ 0_R & \text{si } y \neq x \end{cases}, \quad \forall y \in Y$$

Como  $X$  es no vacío, entonces  $Y$  es no vacío. Por la parte (iii)  $\Rightarrow$  (i), se sabe que  $Y$  es una base del  $R$ -módulo unitario  $A$ . En particular, como (iii)  $\Rightarrow$  (iv), se tiene que  $A$  es un  $R$ -módulo libre en la categoría de  $R$ -módulos unitarios.

En particular,  $F$  y  $A$  son  $R$ -módulos libres en la categoría de  $R$ -módulos unitarios y son tales que  $|X| = |Y|$  (por la forma en que se construyó  $Y$ ), luego por el Teorema anterior son equivalentes en esta categoría, es decir que existe un isomorfismo  $f : F \rightarrow A$ . Así que

$$F \cong \sum_{x \in X} R$$

lo que prueba el resultado. ■

## 2.2. Referencias

- *Algebra* de Thomas Hungerford, ed. Springer.