

Notas de Álgebra Moderna IV. Módulos.

Cristo Daniel Alvarado

31 de octubre de 2024

Índice general

1. Módulos, Homomorfismos y Secuencias exactas	2
1.1. Módulos y homomorfismos	2
1.2. Ejercicios	8
1.3. Referencias	9
2. Módulos Libres y Espacios Vectoriales	10
2.1. Conceptos Fundamentales	10

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 φ** .

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:

■

1.2. Ejercicios

Observación 1.2.1

R es un anillo.

Ejercicio 1.2.1

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:

Veamos que en efecto, A es un $\mathbb{Z}/\mathbb{Z}n$ -módulo: ■

1.3. Referencias

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

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. ■