Universidad de la República
Facultad de Ciencias
Centro de Matemática

Módulos-Generalidades

Notas adaptadas por Mariana Haim para el curso "Anillos y Módulos" 2021.

Durante todo el capítulo A denotará un anillo cualquiera.

Definición 0.0.1. 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 0.0.1. El anillo A es un A-módulo a izquierda si se considera con la *acción regular*, es decir, la acción dada por el producto de A.

Observación 0.0.1.

1. De (1) se deduce que para cada $a \in A$, la función $\varphi_a : M \to M$ definida por $\varphi_a(m) = a \cdot m$ es un morfismo de grupos.

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

3. Análogamente se define *A-módulo a derecha* mediante una acción a derecha $M \times A \to M$.

4. Si $A = (A, +, \cdot, 0, 1)$ es un anillo y se considera la operación $\cdot^{op} : A \times A \to A$ definida por $a \cdot^{op} b = b \cdot a$, entonces $A^{op} = (A, +, \cdot^{op}, 0, 1)$ es otro anillo que llamamos *anillo opuesto*. Se tiene $(A^{op})^{op} = A$ y $A^{op} = A$ si y sólo si A es conmutativo. Si $(M, +, 0)$ es un grupo abeliano y $\cdot : A \times M \to M$ y $\star : M \times A^{op} \to M$ son dos acciones vinculadas por $a \cdot m = m \star a$, es fácil ver que las siguientes afirmaciones son equivalentes:

   - $(M, +, 0, \cdot)$ es un A-módulo a izquierda,
   - $(M, +, 0, \star)$ es un A^{op}-módulo a derecha.

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

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

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

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

Veamos más ejemplos.

Ejemplos 0.0.1. 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 $S \neq \varnothing$ es un conjunto, el grupo de funciones M^S tiene estructura de A-módulo a izquierda definiendo $(a \cdot \varphi)(s) = a \cdot \varphi(s)$.

6. Si A es un anillo, entonces $A[[x]]$ es un $A[x]$-módulo donde la acción es la restricción de la acción regular de $A[[x]]$, con la identificación $A[x] \subset A[[x]]$.

7. (Para los que cursaron Cálculo 3). Sea X una variedad diferenciable. Notemos $C^\infty(X)$ al anillo de las funciones diferenciables $X \to \mathbb{R}$ con las operaciones punto a punto. El conjunto de las n-formas diferenciales en X, notado $\Omega^n(X)$, es un $C^\infty(X)$-módulo: si $f \in C^\infty(X)$ y $\omega \in \Omega^n(X)$, se define $f \cdot \omega$ como $(f \cdot \omega)(p) = f(p)\omega(p)$ para todo $p \in X$.

A partir de ahora, salvo mención explícita, M será un A-módulo a izquierda. Es claro que los enunciados para A-módulos a izquierda tendrán su versión para A-módulos a derecha, a partir de la observación 0.0.1.4. Además, a menudo notaremos am en lugar de $a \cdot m$, para $a \in A, m \in M$.

Definición 0.0.2. Sea M un A-módulo. Un subconjunto $N \subseteq M$ se dice *submódulo* de M si :

(1) $0 \in N$,

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

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

Observación 0.0.2. 1. Es un ejercicio sencillo verificar que son equivalentes, para un A-módulo M y un subconjunto $N \subseteq M$:

- N es un submódulo de M,
- N es un subgrupo de M que es A-*estable* (es decir, que cumple (3)),
- N con las operaciones de M restringidas a N es un A-módulo.

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

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

Definición 0.0.3. Sean M y N A-módulos. Una función $f : M \to N$ es un *morfismo de A-módulos*, o simplemente *A-lineal* si verifica:

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

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

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

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

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

Observación 0.0.3.

1. Un morfismo de A-módulos en particular es morfismo de grupos (abelianos).
2. Si $A = \Bbbk$ es un cuerpo, entonces un morfismo de $\Bbbk$-módulos es exactamente una transformación $\Bbbk$-lineal.
3. Se verifica fácilmente que la composición de morfismos de A-módulos es un morfismo de A-módulos, y que la identidad también lo es. En particular $\operatorname{End}_A(M)$ 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 0.0.1. *Sea $f : M \to N$ morfismo de módulos. Si $H \subseteq N$ es un submódulo, entonces $f^{-1}(H) \subseteq M$ también lo es. Si $K \subseteq M$ es un submódulo, entonces $f(K) \subseteq N$ también lo es. En particular,* $\operatorname{Ker} f = f^{-1}(\{0\}) \subseteq M$ *e* $\operatorname{Im} f = f(M) \subseteq N$ *son submódulos.*

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

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

Definición 0.0.4 (Producto directo y suma directa)**.** Sean I un conjunto no vacío y $\{M_i\}_{i \in I}$ una familia de A-módulos. El *producto directo* de $\{M_i\}_{i \in I}$ es el producto cartesiano $\prod\limits_{i \in I} M_i$ 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 $a \in A, (m_i)_{i \in I}, (n_i)_{i \in I} \in \prod\limits_{i \in I} M_i$. Es fácil verificar que $\prod\limits_{i \in I} M_i$ con estas operaciones es un A-módulo.

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

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

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

Observación 0.0.4. 1. Si en la definición de arriba el conjunto I es finito, la suma directa y el producto directo coinciden.

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

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

Proposición 0.0.2 (Propiedad universal de la suma directa y del producto directo)**.** [2] *Sea $\{M_i\}_{i \in I}$ una familia de A-módulos.*

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

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

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

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

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

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

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

Definición 0.0.5 (Submódulo generado)**.** Sea M un A-módulo y $S \subseteq M$ un subconjunto. El *submódulo generado* por S es $\langle S \rangle := \bigcap \{N \mid N \text{ es submódulo de } M, N \supseteq S\}$.

Observación 0.0.5. 1. Si $S \subseteq M$ es un subconjunto y $N \subseteq M$ es un submódulo que contiene a S, entonces N contiene a $\langle S \rangle$. En otras palabras el submódulo generado por S es el menor (con respecto a $\subseteq$) entre los submódulos de M que contienen a S.

2. Si $S = \varnothing$, entonces $\langle S \rangle = \{0\}$.

[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.

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

Definición 0.0.6. 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 0.0.7. 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 0.0.6.

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 $\mathrm{inc}_j : M_j \to M$ 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 $\varphi \circ \iota_j = \mathrm{inc}_j$. Además φ resulta sobreyectivo. Notar que explícitamente $\varphi\left((m_i)_{i\in I}\right) = \sum_{i\in I} m_i$.
3. Si φ es inyectivo, la suma es isomorfa a la suma directa y se dice que *la suma es directa.* En este caso, cada $m \in \sum_{i\in I} M_i$ se puede escribir de manera única como una suma finita de $m_i \in M_i$. De hecho, son equivalentes las siguientes afirmaciones para una familia $\{M_i\}_{i\in I}$ de submódulos de M.

    a) $\bigoplus_{i\in I} M_i \cong \sum_{i\in I} M_i$ via φ,

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

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

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

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

Lema 0.0.3. *Sean M un A-módulo, $N \subseteq M$ un submódulo, $a \in A, m, m' \in M$. Si $m \equiv m' \pmod N$ entonces $am \equiv am' \pmod N$.*

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

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

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

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

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

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

Corolario 0.0.5 (Teoremas de isomorfismo)**.** *Sea M un A-módulo.*

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

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

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

Teorema 0.0.6. *Sean M un módulo y $N \subseteq M$ un submódulo. Existe una correspondencia biyectiva entre los conjuntos:*

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

que preserva la inclusión.

Demostración. La prueba del resultado análogo para grupos puede adaptarse fácilmente a este contexto, usando la proposición 0.0.1. □