Estructuras algebraicas
Tema 3
Módulos

Resumen
Tema de módulos del peazo profe Javier Majaderias.

Sergio Mayo, Manuel de Prada, Jorge Vázquez
Universidade de Santiago de Compostela
lalala@gmail.com

Índice

1. Módulos

Sea A un anillo conmutativo.
Definición 1.1. Un A-módulo es un grupo abeliano M con una operación:

$$A \times M \longrightarrow M$$

$$(a, m) \longmapsto a \cdot m = am$$

que verifica:

i) $(a + b)m = am + bm$

ii) $a(m + n) = am + an$

iii) $(ab)m = a(bm)$

iv) $1m = m$

Observación. A es un A-módulo

$$A \times A \longrightarrow A$$

$$(a, b) \longmapsto a \cdot b$$

Propiedades.

1. $0m = 0$ ya que $0m = (0 + 0)m = 0m + 0m$
2. $a0 = 0$
3. $(-a)m = -(am) = a(-m)$

Observación. $am = 0 \not\Rightarrow \begin{cases} a = 0 \\ \text{ó} \\ m = 0 \end{cases}$

Observación. Como A conmutativo, $ma := am$

$$m(ab) = (ab)m = a(bm) = mb(a) = m(ba)$$

Proposición 1.1. *Sea M grupo abeliano. Entonces M es un $\mathbb{Z}$-módulo.*
Nota clase: la estructura de un $\mathbb{Z}$ módulo y de grupo abeliano es la misma

Demostración. Sea $n \in \mathbb{Z}, x \in M$

$$n \cdot x = \begin{cases} x + ... + x & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ (-x) + ... + (-x) = -(-n)x & \text{si } n < 0 \end{cases}$$

$nx = (1 + ... + 1)x = 1x + .., 1x = x + ... + x$ □

Nota. Descomposición en primos:
$x^2 - y^2 = n$
$(x + y)(x - y) = n = p_1 p_2 p_3$
$(x + iy)(x - iy) = n$ (no tiene sentido hablar de primos en los números complejos(?))

EJEMPLO 1.1: Utilización anillos: cálculo raíces polinomios.
$f(x, y) = y^2 - x^3 - x^2$
$A = \frac{K[x,y]}{f(x,y)}$ aporta información sobre las raíces.

Comentario clase. ¿Cual es la motivación de estudiar los módulos?
Aparecen en representaciones de grupos: Sabiendo los módulos de un anillo, se puede saber como es un anillo.
Otra razón (se ve en el máster): Si un anillo es regular, es útil en el estudio de puntos no singulares. Cada punto de la curva esta determinado por un anillo. Si algunos anillos son regulares, otros también lo son. Es un vago ejemplo de que los módulos tienen utilidad.

Definición 1.2. Sea M un A-módulo, N subconjunto de M.
Se dice que N es un A-submódulo de M si N es un A-módulo con la operación de A en M.

Observación.

1. $\forall y \in N, a \in A \quad \Rightarrow ay \in N$
2. $\forall x, y \in N \quad \Rightarrow x - y \in N$
3. $\{0\}, M$ son submódulos de M
4. Si I es un ideal de A, M un A-módulo, entonces
$$IM := \{\sum_{i=1}^{n} a_i \cdot x_i \quad : n \in N, a_i \in I, x_i \in M\}$$
es un submódulo de M. ($a \cdot \sum a_i x_i = \sum (a \cdot a_i) \cdot x_i$, nótese que $aa_i \in I$)
5. Si I es un subconjunto de A, entonces I es A-submódulo de $A \Leftrightarrow I$ es ideal de A (A como A-módulo).

Definición 1.3. Si M_1 y M_2 son submódulos de un A-módulo M se define la suma de M_1 y M_2:
$$M_1 + M_2 = \{x_1 + x_2 \in M : x_1 \in M_1, x_2 \in M_2\}$$
Es el menor submódulo de M que contiene a M_1 y M_2.
Nótese:

1. $x_1 + x_2 - (x'_1 + x'_2) = (x_1 - x'_1) + (x_2 - x'_2) \in M_1 + M_2$
2. $a(x_1 + x_2) = a(x_1) + a(x_2) \in M_1 + M_2$

Definición 1.4. Sea $\{M_i\}_{i \in I}$ familia de submódulos de M. Definimos en general
$$\sum_{i \in I} M_i = \{\sum_{i \in I} x_i \in M : x_i \in M_i \text{para cada i, } a_i \in A, \text{casi todos los } x_i = 0\}$$
$$= \{\text{sumas finitas de elementos de } \bigcap M_i\} = x_1 + ... + x_r$$
Es el menor submódulo de M que contiene $\bigcup_{i \in I} M_i$

Proposición 1.2. *La intersección de una familia de submódulos de M es un submódulo de M.*

Proposición 1.3. *Sea M un A-módulo, X contenido en M, se llama A-submódulo de M generado por X al menor A-submódulo de M que contiene a X. Se denota $< X >$ o $< X >_A$.*
Se dice que X es un conjunto de generadores de $< X >$
$$< X >= \{\sum_{i=1}^{n} a_i x_i / n \in \mathbb{N}, a_i \in A, x_i \in X\}$$

Ejemplo 1.2: Observamos que:

1. Por ejemplo, tenemos que si $X = x$, tenemos que:

$$< x >=< x >= Ax = \{ax/a \in A\}$$

2. $< X >= \sum_{x \in X} A_x$
3. $\sum_i M_i =< \bigcup_i M_i >$

Definición 1.5. Sean M, N A-módulo. Una aplicación $f : M \to N$ es un homomorfismo de A-módulo si:

1. $f(x + y) = f(x) + f(y)$
2. $f(ax) = af(x)$

Proposición 1.4. *La composición de homomorfismos de A-módulos es un homomorfismo de A-módulos.*

Demostración. Prueba sencilla. □

Ejemplo 1.3: Tenemos que:

1. $id_M : M \to M$ es un homomorfismo de módulos.
2. $f : M \to N$ $f(x) = 0$ $\forall x \in M$ es un homomorfismo de A-módulo.

Es necesario destacar que de forma inmediata que se cumple que: $f(0) = 0$, $f(-x) = -f(x)$.

Proposición 1.5. *Si $f : M \to N$ es un homomorfismo de A-módulo.*
$M' \subset M$ un submódulo $\Rightarrow f(M')$ es un submódulo de N. $N' \subset N$ un submódulo $\Rightarrow f^{-1}(N')$ es un submódulo de M.

Se cumple además que $ker(f) = f^{-1}(0)$ es un submódulo de M y también $Im(f) = f(M)$ submódulo de N. Tenemos de forma inmediata f inyectiva si y sólo si $kerf = 0$.

Proposición 1.6. *Sea M y N un A-submódulo de M. Teniendo M/N:*

1. $(x + N) + (y + N) = x + y + N$
2. $a(x + N) = ax + N$
3. *Si* $x + N = x\prime + N$ *tenemos que* $ax + N = ax\prime + N$

 Demostración.

$$x - x\prime \in N \Rightarrow a(x + x\prime) \in N \in ax + ax\prime \in N$$

□

Además, tenemos que $\pi : M \to M/N$ homomorfismo de anillos A-módulo. Tenemos además que $ker(f) = N$, ($M = N$, entonces $M/N = 0$).

Proposición 1.7. *Sea N un submódulo de M. Existe una biyección que conserva las inclusiones de tal forma:*

$$\{A\textit{-submódulos de } M \textit{ que contienen a } N\} \rightleftarrows \{A\textit{-submódulo de } M/N\}].$$

Definición 1.6. Si $f : M \to N$ es un homorfismo de A-módulos se llama conúcleo de f al A-módulo:

$$coker(f) = M/Im(f).$$

Definición 1.7. Sea A un anillo. Un A-módulo M es cíclico si está generado por un elemento, es decir:

$$\exists x \in M \ / \ M =< x >= Ax$$

Observación. Sea $f : A \to B$ un homomorfismo de anillos. Entonces B es un A-módulo definiendo la operación externa como:

$$a \in A, b \in B \quad a \cdot b := f(a)b$$

En particular si I es un ideal de A, A/I es un A-módulo ($p : A \to A/I$).

Proposición 1.8. *Si M es un A-módulo son equivalentes:*

i) M es cíclico.

ii) Existe un homomorfismo sobreyectivo de A-módulos $\phi : A \to M$

iii) Existe un ideal I de A y un isomorfismo de A-módulos $A/I \simeq M$

Demostración.
$i) \Rightarrow ii)$:

$$M \text{ cíclico} \Rightarrow M =< x >$$

$$\phi : a \in A \to \phi(a) := ax \in M \text{ es un homomorfismo de } A\text{-módulos sobreyectivo:}$$

$$\phi(a+b) = (a+b)x = ax + bx = \phi(a) + \phi(b)$$

$$\phi(\lambda a) = (\lambda a)x = \lambda(ax) = \lambda\phi(a) \quad \forall \lambda \in A$$

$$Im(\phi) = \{ax \ / \ a \in A\} =< x >= M$$

$ii) \Rightarrow iii)$:

Por hipótesis existe $\phi : A \to M$ homomorfismo sobreyectivo de A-módulos.

$$A/Ker(\phi) \simeq M \text{ y } Ker(\phi) \text{ es un ideal de } A$$

$iii) \Rightarrow i)$:

$$A/I \text{ es un } A\text{-módulo cíclico.}$$

$$A/I =< \bar{1} > \Rightarrow M \text{ es cíclico}$$

□

Definición 1.8. Sean A anillo y M A-módulo. Se llama aniquilador de M al ideal de A definido por:

$$(0 : M) := \{a \in A \ / \ ax = 0 \ \forall x \in M\}$$

Definición 1.9. Tomando $M =< x >$ definimos:

$$(0 : x) := (0 :< X >) = \{a \in A \ / \ ax = 0\}$$

Proposición 1.9. *Sea A un anillo y M un A-módulo. Se verifica que en efecto $(0 : M)$ es un ideal.*

Demostración.

$$\text{Trivialmente } 0 \in (0:M) \Rightarrow (0:M) \neq \emptyset$$

$$a, b \in (0:M) \Rightarrow ax = 0 = bx \ \forall x \in M \Rightarrow (a-b)x = ax - bx = 0 - 0 = 0 \ \forall x \in M \Rightarrow a - b \in (0:M)$$

$$\lambda \in A, a \in (0:M) \Rightarrow ax = 0 \ \forall x \in M \Rightarrow (\lambda a)x = 0 \ \forall x \in M \Rightarrow \lambda a \in (0:M)$$

□

Observación. Sea $x \in M$, definimos:

$$A \xrightarrow{\phi} M \text{ homomorfismo de } A\text{-módulos}$$

$$\phi(a) := ax$$

$$Ker(\phi) = (0:x)$$

$$A/(0:x) \xrightarrow{\cdot x} M \text{ homomorfismo inyectivo}$$

Observación. Tomando $A = \mathbb{Z}$:

$$\mathbb{Z}\text{-módulo} = \text{ grupo abeliano}$$

$$\mathbb{Z}\text{-módulo cíclico} = \text{ grupo cíclico}$$

Definición 1.10. Sea $\{M_i\}_{i \in I}$ una familia de A-módulos. Definimos el producto directo de los M_i como el A-módulo:

$$\prod_{i \in I} M_i := \{f : I \to \bigcup_{i \in I} M_i \ / \ f \text{ aplicación}, f(i) \in M_i \ \forall i \in I\} = \{(x_i)_{i \in I} \ / \ x_i \in M_i \ \forall i \in I\}$$

$$(x_i)_{i \in I} + (y_i)_{i \in I} := (x_i + y_i)_{i \in I}$$

$$a(x_i)_{i \in I} := (ax_i)_{i \in I}$$

Observación. En el caso finito, los elementos del producto los representamos con n-tuplas:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$$

Observación. La proyección habitual $\pi_j : \prod_{i \in I} M_i \longrightarrow M_j$ es un homomorfismo de A-módulos para todo j.

Definición 1.11. Sea $\{M_i\}_{i \in I}$ una familia de A-módulos. Definimos la suma directa de los M_i como el A-submódulo de $\prod_{i \in I} M_i$:

$$\bigoplus_{i \in I} M_i = \{(x_i)_{i \in I} \in \prod_{i \in I} M_i \ / \ x_i = 0 \text{ para casi todo } i \in I\}$$

Observación. La aplicación

$$M_j : M_j \longrightarrow \bigoplus_{i \in I} M_i$$

$$M_j(m) := (x_i)_{i \in I} \ / \ x_j = m, \ x_i = 0 \ \forall i \neq j$$

es un homomorfismo de A-módulos inyectivo para cualquier j.

Observación. Si I es finito:

$$\prod_{i \in I} M_i = \bigoplus_{i \in I} M_i$$

Proposición 1.10. *Sea M un A-módulo y $\{M_i\}_{i\in I}$ una familia de A-submódulos de M. La aplicación:*

$$\bigoplus_{i\in I} M_i \longrightarrow \sum_{i\in I} M_i$$

$$(x_i)_{i\in I} \rightsquigarrow \sum_{i\in I} x_i$$

es un homomorfismo de A-módulos.

Proposición 1.11. *Sea $\{M_i\}_{i\in I}$ familia de submódulos de M. Consideremos:*

$$\phi : \oplus_{i\in I} M_i \longrightarrow \oplus_{i\in I} M_i$$

$$\phi((x_i)_{i\in I}) = \sum_{i\in I} x_i$$

Equivalen:

i) *ϕ isomorfismo*

ii) $\sum_{i\in I} x_i = 0, x_i \in M_i\ \forall i, x_i = 0$ *para casi todo* $i \Rightarrow x_i = 0\ \forall i \in I$

iii) $M_j \cap (\sum_{i\neq j} M_i) \forall j \in I$

Demostración.
i) $\Rightarrow$ *ii)*:

$$0 = \sum_{i\in I} x_i = \phi((x_i)_{i\in I}) \Rightarrow \text{(ya que } \phi \text{ inyectiva) } (x_i) \in I = 0 \Rightarrow x_i = 0\ \forall i \in I$$

ii) $\Rightarrow$ *iii)*:

$$x \in M_j \cap (\sum_{i\neq j} M_i) \Rightarrow x = \sum_{i\in I, i\neq j, x_i \in M_i} x_i \Rightarrow$$

$$\sum_{i\in I, i\neq j} x_i - x = 0 \text{ (ya que } x \in M_j) \Rightarrow x = 0$$

iii) $\Rightarrow$ *i)*:

Sea $(x_i)_{i\in I} \in \oplus_{i\in I} M_i$ tal que $\phi((X_i)_{i\in I}) = \sum_{i\in I} x_i = 0$.
Tenemos que demostrar que $x_i = 0\ \forall i \in I$.
Sea $j \in I, x_j = -\sum_{i\in I, i\neq j} x_i \in \sum_{i\in I} M_j \Rightarrow x_j \in M_j \cap (\sum_{i\neq j} M_i) = 0 \Rightarrow x_j = 0$ □

Definición 1.12. A dominio. Sea M un A-módulo. Un elemento $x \in M$ es de torsión si $(0 : x) \neq 0$. (si existe $a \in A, a \neq 0$ tal que $ax = 0$). El conjunto de elementos de tensión de M se denota $T(M)$ y es un A-submódulo de M.

Observación.

$$x, y \in T(M) \Rightarrow \exists a, b \in A, a \neq 0 \neq b \text{ con } ax = 0, by = 0$$

$$ab(x - y) = abx - aby = 0 - 0 = 0$$

$$0 \neq ab \in A \Rightarrow x - y \in T(M)$$

Observación.

$$a \in A, x \in T(M) \Rightarrow \exists a \neq b \in A : bx = 0 \Rightarrow b(ax) = 0 \Rightarrow ax \in T(M)$$

Definición 1.13. Si $T(M) = M$ se dice que M es un A-módulo de torsión. Si $T(M) = 0$ se dice que M es un A-modulo libre de torsión.

Proposición 1.12.

$$T(M) \hookrightarrow M \twoheadrightarrow M/T(M)$$

$M/T(M)$ es libre de torsión.

Demostración.

$$\left.\begin{array}{r}\left.\begin{array}{r}\overline{x} = x + T(M) \in M/T(M)\\ 0 \neq a \in A \quad a \cdot \overline{x} = \overline{a}\end{array}\right\} \overline{ax} = \overline{0} \Rightarrow ax \in T(M)\\ 0 \neq bb(ax) = 0, (ba)x = 0, ba \neq 0\end{array}\right\} x \in T(M) \Rightarrow \overline{x} \neq \overline{0}$$ □

Ejercicio 1.1: $f : M \longrightarrow N$ homomorfismo de A-módulo. Probar que $f(T(M)) \subset T(N)$

Definición 1.14. Sea M un A-módulo.
Una familia $\{x_i\}_{i \in I}$ de elementos de M es linealmente independiente si:

$$0 = \sum_{i \in I} a_i x^i, a_i \in A \ \forall i, a_i = 0 \text{ para casi todo } i \Rightarrow a_i = 0 \ \forall i \in I$$

Observación. $\{x_i\}_{i \in I}$ linealmente independiente $\Leftrightarrow$ toda subfamilia finita de $\{x_i\}_{i \in I}$ es linealmente independiente.
Observación. $\{x_i\}_{i \in I}$ linealmente independiente. $Ax_i =< x_i >$

$$\oplus_{i \in I} Ax_i \longrightarrow \phi \sum_{i \in I} Ax_i$$

$$(a_i x_i)_{i \in I} \longmapsto \sum_{i \in I} a_i x_i$$

es sobreyectiva e inyectiva ya que $\sum_{i \in I} a_i x_i = 0 \Rightarrow a_i = 0 \ \forall i \in I \Rightarrow (a_i x_i)_{i \in I} = (0)_{i \in I}$.

Ejemplo 1.4:

- $\{0\}$ no es un conjunto linealmente independiente $a0 = 0, a \neq 0$.
- $\{0\} \cup S$ no es linealmente independiente. $a0 + \sum_{s \in S} 0 \cdot s = 0$.

Definición 1.15. $\{x_i\}_{i \in I}$ linealmente independiente.

$$\psi : A \longrightarrow Ax_i =< x_i >$$

$$a \longmapsto \psi(a) = ax_i$$

homomorfismo de A-módulo sobreyectivo. Además,

$$\text{Ker}(\psi) = (=: x_i) = \{a \in A : ax_i = 0\}$$

$$A = A/(0 : x_i) \simeq Ax_i$$

Observación. $\{x\}$ linealmente independiente $\Leftrightarrow (0 : x) = 0$
Definición 1.16. Una base de un A-módulo M es un conjunto de generadores linealmente independiente.

$$M =< \{x_i\}_{i \in I} >= \sum_{i \in I} Ax_i, \{x_i\}_{i \in I} \text{ linealmente independientes.}$$

Definición 1.17. Un A-módulo F es libre si tiene una base $\{x_i\}_{i\in I}$ que cumple:

- $x \in F \Rightarrow$ x se puede expresar como $x = \sum_{i\in I} a_i x_i$.
- Esta expresión es única, es decir, $\sum a_i x_i = \sum b_i x_i \Rightarrow \sum (a_i - b_i)x_i = 0 \Rightarrow (a_i - b_i) = 0\ \forall i$

Observación. A cuerpo $\Rightarrow$ todo A-módulo es libre.
Si A no es un cuerpo $\Rightarrow$ existen módulos no libres.
Observación. Sea I un ideal propio no nulo de A.
$M = A/I$ no es A-módulo libre. Si $\overline{x} \in A/I, 0 \neq a \in I, 0 \neq I \subset (0\overline{\lambda}), a\overline{x} = \overline{0}$

Ejemplo 1.5:

- A es A-módulo libre base $\{1\}$
- $\{0\}$ es A-módulo libre base $\emptyset$

JORGE 15-11

SERGIO 19-11

Proposición 1.13. *Sea $A = \mathbb{Z}$ y M A-módulo con generadores x_1, x_2 y la relación $x_1 + x_2 = 0$. Veamos que $Z \simeq M$.*

Demostración.
Vamos a definir un ϕ de forma que $\mathbb{Z} \xrightarrow{\phi} M$ sea isomorfismo. Definimos $\phi(a) = ax_1\ \forall a \in \mathbb{Z}$.

$$\left.\begin{array}{r} x_1 = \phi(1) \Rightarrow x_1 \in Im(\phi) \\ x_2 = -x_1 = -\phi(1) = \phi(-1) \Rightarrow x_2 \in Im(\phi) \end{array}\right\} \Rightarrow \phi \text{ es sobreyectiva.}$$

Veamos que $Ker(\phi) = \{0\} \Leftrightarrow \phi$ inyectiva. □

END SERGIO 19-11