Universidad de la República
Facultad de Ciencias
Centro de Matemática

Dependencia lineal y bases en módulos

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

Definición 0.0.1. Sea M un A-módulo. Sea $S \subseteq M$ un subconjunto. Decimos que S es *linealmente dependiente* si existen $m_1, \dots, m_k \in S$ y $a_1, \dots, a_k \in A$ 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 $m_1, \dots, m_k$.

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

Observación 0.0.1.

1. $S = \varnothing$ es linealmente independiente.
2. S es linealmente independiente si y sólo si para todo $m_1, \dots, m_k \in S$ y $a_1, \dots, a_k \in A$ tales que $\sum_{i=1}^{k} a_i m_i = 0$ se tiene que $a_i = 0$ para todo $i = 1, \dots, n$. Es decir, si la única combinación lineal nula es la trivial.
3. Si $S = \{m_1, \dots, m_k\} \subset M$ es tal 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 $p, q \geqslant 2$. 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 0.0.2. 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 0.0.2. 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 0.0.1.

1. Si $M = V$ es un espacio vectorial sobre un cuerpo $\Bbbk$, entonces M es libre.
2. El conjunto $\mathcal{B} = \{1, x, x^2, \dots\}$ es base de $A[x]$ como A-módulo.
3. Sea $n \geqslant 2$: 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.
4. Todo anillo como módulo sobre sí mismo es libre, con base $\{1\}$.
5. En particular, $\mathbb{Z}_n$ es libre como $\mathbb{Z}_n$-módulo, pero no lo es como $\mathbb{Z}$-módulo (ejemplo 0.0.13).
6. A^n es libre para todo $n \in \mathbb{N}$.

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

8. $\mathbb{Z}$ 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.

Definición 0.0.3. Sea M un A-módulo. Definimos:

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

Observación 0.0.3. $\mu(M) < \infty \iff M$ es finitamente generado.

Ejemplo 0.0.1. 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 0.0.1. *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* $\mu(M) \leqslant \mu(N) + \mu(M/N)$.

Demostración. 1. Consideremos el morfismo sobreyectivo $\pi : M \to M/N$. Si $M = \langle m_1, \dots, m_k\rangle$, entonces por la observación 0.0.2, se tiene que $M/N = \langle\pi(m_1), \dots, \pi(m_k)\rangle$.

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

Definición 0.0.4. Sea M un A-módulo, $S \subset M$ un subconjunto. El *anulador* de S es

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

Si $S = \{m_1, \dots, m_k\}$ escribiremos $\text{Ann}(S) = \text{Ann}(m_1, \dots, m_k)$.

Observación 0.0.4. Sea $S = \{m\}$, para algún $m \in M$. Tenemos un morfismo $\varphi : A \to M$, $a \mapsto am$. Se tiene que $\text{Im}\,\varphi = Am$ y $\ker\varphi = \text{Ann}(m)$. Por lo tanto $A/\text{Ann}(m) \cong Am$.

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

Observación 0.0.5. 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 0.0.2. *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 una familia $\mathcal{F}$ tal que $M \cong \bigoplus_{i\in\mathcal{F}} A_i$ con $A_i = A$ para todo $i \in \mathcal{F}$.*

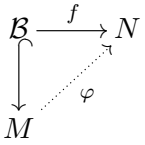
Demostración. (1 $\Rightarrow$ 2) Sea $\mathcal{B}$ base de M. Entonces $M = \langle\mathcal{B}\rangle = \bigoplus_{m\in\mathcal{B}} Am$ en virtud de la observación 0.0.5. Ahora, como $\mathcal{B}$ es linealmente independiente, $\mathrm{Ann}(m) = \{0\}$ para todo $m \in B$, y por lo tanto $A \cong A/\mathrm{Ann}(m) \cong Am$ en virtud de la observación 0.0.4.

(2 $\Rightarrow$ 3) Obvio.

(3 $\Rightarrow$ 1) La imagen en M de la base canónica de $\bigoplus_{i\in\mathcal{F}} A$ es una base de M. □

La siguiente proposición, como en espacios vectoriales, muestra que para definir una transformación lineal desde un módulo libre, basta definirla en una base.

Proposición 0.0.3 (Propiedad universal del módulo libre)**.** *Sea M un A-módulo libre con base $\mathcal{B} \subseteq M$, y N un A-módulo. Si $f : \mathcal{B} \to N$ 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. □

Proposición 0.0.4. *Sea M un A-módulo libre con base $\mathcal{B} \subseteq M$. Si M es finitamente generado, entonces $\#\mathcal{B} < \infty$.*

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

Teorema 0.0.5. *Sea M un A-módulo libre que admite una base $\mathcal{B}$ 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 $x \in \mathcal{B} \backslash \mathcal{B}'$. 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 0.0.6. 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 0.0.5:

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

Demostración. Observar primero que si A es un anillo con división, todo A-módulo es libre. Además, son equivalentes:

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

En efecto, 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.
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 $\#S \geqslant \#\mathcal{B}$. □

Definición 0.0.5. 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 0.0.2.
1. El corolario 0.0.6 afirma que todo anillo con división tiene NBI.
2. $\operatorname{rg}(A^n) = n$.

Observación 0.0.7. Dado un anillo A, para verificar si tiene NBI basta hacerlo en módulos libres que no admiten bases infinitas, en virtud de la observación 0.0.6. 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 0.0.7. *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. El ejercicio 10 del práctico 6 nos da que $IM = \left\{ \sum_{i=1}^{n} a_i n_i \mid a_i \in I, n_i \in M, n \in \mathbb{Z}^+ \right\}$ es un submódulo de M, y que M/IM es un A/I-módulo, con la acción $\overline{a} \cdot \overline{m} = \overline{am}$.

Veamos que $\overline{\mathcal{B}}$ es generador:[1] 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:

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

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

$$\sum_{i\in I} a_i m_i = \sum_{n\in I} \overbrace{\left(\sum_{j=1}^{r} b_j c_{jn}\right)}^{\alpha_n \in I} m_n \Rightarrow \sum_{i\in I} (a_i - \alpha_i) m_i = 0$$

Como 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 0.0.8. *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. □

[1] 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.