El teorema de estructura de módulos finitamente generados sobre un dominio de ideales principales

Mariano Suárez-Alvarez

7 de octubre, 2015

Sea A un dominio de ideales principales que no es un cuerpo. En todo lo que sigue, llamamos simplemente módulos a los A-módulos izquierdos y escribimos $\mathrm{Max}(A)$ al conjunto de los ideales maximales de A, esto es, de los ideales primos no nulos de A.

Proposición 1. *Si M es un módulo y $\tau(M)$ es su submódulo de torsión, entonces $M/\tau(M)$ no tiene tiene torsión.*

Demostración. Supongamos que $m \in M$ es tal que su clase $\overline{m}$ en $M/\tau(M)$ es de torsión, de manera que exite un escalar no nulo $a \in A$ tal que $a \cdot \overline{m} = \overline{am} = 0$. Esto significa que $am \in \tau(M)$ y, entonces, que existe un escalar no nulo $b \in A$ tal que $bam = 0$. Como A es un dominio, $ba \neq 0$ y la última igualdad implica que m es un elemento de torsión, esto es, que $\overline{m} = 0$ en $M/\tau(M)$. □

Proposición 2. *Un submódulo de un módulo libre de rango finito es libre.*

Demostración. Sean $n \in \mathbb{N}$ y $M \subseteq A^n$ un submódulo, y mostremos que M es libre; esto es claramente suficiente para probar la proposición. Cuando $n = 1$ el submódulo M es un ideal de A y existe entonces $a \in A$ tal que $M = (a)$: como A es un dominio, el conjunto $\{a\}$ es una base de M y el resultado es cierto en este caso.

Supongamos ahora que $n > 1$, sea $p : A^n \to A$ la proyección en la última coordenada y consideremos la sucesión exacta corta

$$0 \longrightarrow M \cap \ker p \longrightarrow M \longrightarrow p(M) \longrightarrow 0$$

La imagen $p(M)$ es un submódulo de A, así que —en vista de lo que ya hicimos— se trata de un módulo libre. Como consecuencia de esto, nuestro sucesión exacta se parte y hay un isomorfismo

$$M \cong p(M) \oplus M \cap \ker p. \tag{1}$$

Por otro lado, la intersección $M \cap \ker p$ es un submódulo de $\ker p$ y este último es claramente isomorfo a A^{n-1}: inductivamente, entonces, sabemos que $M \cap \ker p$ es libre. Vemos así que los dos sumandos que aparecen a la derecha en el isomorfismo (1) son libres, así que M mismo es libre. □

Proposición 3. *Un módulo finitamente generado y sin torsión es libre.*

Demostración. Sea M un módulo finitamente generado y sin torsión, y supongamos que M no es nulo, ya que en caso contrario no hay nada que probar. Sea $B = \{m_1, \dots, m_n\}$ un subconjunto finito de M que lo genera y sea k el máximo de los cardinales de los subconjuntos linealmente independientes de B. Como $M \neq 0$, es $n \geq 1$, y como M no tiene torsión $k \geq 1$; además, a menos de renombrar los elementos de B, podemos suponer que $B' = \{m_1, \ldots, m_k\}$ es linealmente independiente. Sea M' el submódulo de M generado por B', que es libre.

Si $i \in \{k+1, \ldots, n\}$, el conjunto $\{x_1, \ldots, x_k, x_i\}$ es linealmente dependiente, así que existen escalares a_i, $a_{i,1}$, …, $a_{i,k}$ en A tales que

$$a_i m_i = \sum_{j=1}^{k} a_{i,j} m_j$$

y como $\{x_1, \ldots, x_k\}$ es linealmente independiente debe ser $a_i \neq 0$. Si ponemos $a = a_{k+1} \cdots a_n$, entonces, es $a \neq 0$ y $am_i \in M'$ para cada $i \in \{k+1, \ldots, n\}$. Como también $am_i \in M'$ si $i \in \{1, \ldots, k\}$, vemos que, de hecho, es $aM \subseteq M'$. Como M' es libre, la Proposición 2 nos dice que aM es un módulo libre. La funcion $f : m \in M \mapsto am \in aM$, que es un morfismo de módulos, es evidentemente sobreyectiva y es inyectiva porque M no tiene torsión. Se trata entonces de un isomorfismo y, como aM es libre, también lo es M. □

Proposición 4. *Un módulo finitamente generado y de torsión y tiene anulador no nulo y es artiniano.*

Demostración. Sea M un módulo finitamente generado y de torsión. Sea $B = \{m_1, \ldots, m_n\}$ un conjunto generador de M y para cada $i \in \{1, \ldots, n\}$ sea $a_i \in A$ un escalar no nulo tal que $a_i m_i = 0$. Si I es el ideal $(a_1 \cdots a_n)$, entonces $0 \subsetneq I \subseteq \operatorname{ann}(M)$, lo que prueba la primera afirmación de la proposición, y hay un morfismo $f : (A/I)^n \to M$ tal que $f(e_i) = m_i$ para cada $i \in \{1, \ldots, n\}$. Como f es sobreyectivo, para mostrar que M es artiniano es suficiente con que mostremos que A/I lo es.

Más generalmente, supongamos que $a \in A$ es un elemento no nulo cualquiera y mostremos que $A/(a)$ es un módulo artiniano. Teniendo en cuenta los teoremas de isomorfismo, es suficiente para ello mostrar que toda cadena descendente $I_1 \supseteq I_2 \supseteq \cdots$ de ideales de A con $a \in I_i$ para todo $i \in \mathbb{N}$ se estabiliza. En esa situación, existen elementos a_1, a_2, …en A tales que $I_i = (a_i)$ y $a_i \mid a_{i+1} \mid a$ para todo $i \in \mathbb{N}$. Esto implica, ya que A es un dominio de factorización única, que el número $d(i)$ de factores primos en una factorización de a_i es una función no decreciente de i y acotada superiormente, y entonces existe $i_0 \geq 1$ tal que $d(i) = d(i_0)$ para todo $i \geq i_0$. Como a_{i_0} divide a a_i cualquiera sea $i \geq i_0$, esto implica que a_i y a_{i_0} son asociados en A y, entonces, que $I_i = I_{i_0}$. Vemos así que la cadena de ideales se estabiliza, como queríamos. □

Un módulo M es *indescomponible* si es no es nulo y no posee submódulos no nulos M_1, M_2 tales que $M = M_1 \oplus M_2$.

Proposición 5. *Si M es un módulo artiniano, entonces existen $n \geq 0$ y submódulos M_1, …, M_n indescomponibles tales que $M = \bigoplus_{i=1}^{n} M_i$.*

Demostración. Digamos que un submódulo de M es *malo* si no posee una descomposición como suma directa de un número finito de submódulos indescomponibles. Es claro que un submódulo N de M que es malo no puede ser indescomponible, de manera que posee submódulos N_1, N_1' con $N = N_1 \oplus N_1'$ y que, sin pérdida de generalidad, podemos suponer que N_1 es malo.

Supongamos que M es malo. La observación que acabamos de hacer implica inductivamente que existen submódulos no nulos M_i, M_i' de M para cada $i \geq 1$ tales que $M = M_1 \oplus M_1'$ y $M_i = M_{i+1} \oplus M_{i+1}'$ si $i \geq 1$. En particular, la cadena $M_1 \supseteq M_2 \supseteq \cdots$ de submódulos de M no se estabiliza y esto es imposible, ya que M es artiniano. □

Proposición 6. *Si M es un módulo finitamente generado, de torsión e indescomponible, existe un elemento irreducible $p \in A$ y un entero $k \geq 1$ tal que $M \cong A/(p^k)$.*

Demostración. Como el ideal $\operatorname{ann}(M)$ no es nulo, existe un elemento no nulo $q \in A$ tal que $\operatorname{ann}(M) = (q)$; como M no es nulo porque es indescomponible, q no es inversible.

Supongamos que hay una factorización $q = rs$ con r y s dos elementos no inversibles y coprimos de A, y sean r', $s' \in A$ tales que $rr' + ss' = 1$. Si $m \in M$, entonces

$$m = rr'm + ss'm \in rM + rM,$$

así que $M = rM + sM$. Por otro lado, si $m \in rM \cap sM$ entonces $sm \in srM = qM = 0$ y, de manera similar, $rm = 0$ y, por lo tanto, $m = rr'm + ss'm = 0$. Concluimos de esta forma que $M = rM \oplus sM$ y, como M es indescomponible, que, por ejemplo, $rM = 0$. Esto implica que $r \in \operatorname{ann}(M) = (q)$ y, en consecuencia, que r y q son asociados en A. Esto es imposible, ya que s no es inversible.

Esta contradicción nos dice que existen un elemento irreducible $p \in A$ y un entero $k \geq 0$ tales que $q = p^k$; como q no es una unidad, tiene que ser $k \geq 1$. Como p^k y p^{k-1} no son asociados, es $p^{k-1} \notin (p^k) = \operatorname{ann}(M)$ y esto significa que existe $x \in M$ tal que $p^{k-1}x \neq 0$.

El morfismo $\phi : a \in A \mapsto ax \in Ax$ es sobreyectivo y su núcleo es $\operatorname{ann}(x) \supseteq \operatorname{ann}(M) = (p^k)$, así que si $b \in A$ es tal que $(b) = \operatorname{ann}(x)$, entonces b divide a p^k y es, por lo tanto, de la forma p^i para algún $i \in \{0, \ldots, k\}$. Como $p^{k-1}x \neq 0$, debe ser $b = p^k$. Vemos así que ϕ induce un isomorfismo $A/(p^k) \cong Ax$.

Consideremos ahora la sucesión exacta corta canónica

$$0 \longrightarrow Ax \xrightarrow{\ i\ } M \longrightarrow M/Ax \longrightarrow 0$$

en la que el morfismo i es la inclusión. Como M es un módulo noetheriano, hay un submódulo L de M maximal entre aquéllos que contienen a Ax y para los que existe un morfismo $\sigma : L \to Ax$ tal que $i \circ \sigma = \mathsf{id}_{Ax}$. Afirmamos que, de hecho, $L = M$: eso significa que el morfismo i admite una retracción $\sigma : M \to Ax$ y que entonces nuestra sucesión exacta se parte, de manera que $M \cong Ax \oplus M/Ax$. Como M es indescomponible y $Ax \neq 0$, debe ser $M/Ax = 0$ y, en consecuencia, $M = Ax \cong A/(p^k)$, que es lo que queremos probar.

Bastará entonces que mostremos que $L = M$. Supongamos que no es ése el caso, de manera que $L \subsetneq M$ y sea $\sigma : L \to Ax$ un morfismo tal que $i \circ \sigma = \mathsf{id}_{Ax}$. Si $y' \in M \setminus L$, es $p^k y' = 0 \in L$, así que existe un menor entero $l \geq 1$ tal que $p^l y' \in L$. Sea $y = p^{l-1}y'$. La elección de l implica que $y \in M \setminus L$ y $py \in L$. El conjunto $(L : y) = \{a \in A : ay \in L\}$ es un ideal propio de A que contiene a (p) y, como este último es maximal, debe ser $(L : y) = (p)$.

Sea $c \in A$ tal que $\sigma(py) = cx$. Es

$$p^{k-1}cx = p^{k-1}\sigma(py) = \sigma(p^k y) = 0,$$

así que $p^{k-1}cx = 0$. Como $\operatorname{ann}(x) = p^k$, esto implica que $c = pd$ para algún $d \in A$.

Consideremos ahora el submódulo $L' = L + Ay$ de M, que contiene propiamente a L. Existe una función $\sigma' : L + Ay \to Ax$ tal que

$$\sigma'(u + ay) = \sigma(u) + adx$$

para cada $u \in L$ y cada $a \in A$. Para verlo, hay que mostrar que si $a \in A$ es tal que $ay \in L$ entonces $\sigma(ay) = adx$; pero en ese caso es $a \in (L : y) = (p)$, así que existe $a' \in A$ tal que $a = a'p$ y

$$\sigma(ay) = \sigma(a'py) = a'\sigma(py) = a'pdx = adx,$$

como queremos. Como $Ax \subseteq L \subseteq L'$, $i \circ \sigma' = \mathsf{id}_{Ax}$ y $L \subsetneq L'$, esto contradice la elección de L. $\square$

Proposición 7. *Si M es un módulo finitamente generado, entonces existen un entero $r \geq 0$ y una función $\mu : \operatorname{Max}(A) \times \mathbb{N} \to \mathbb{N}_0$ de soporte finito tal que*

$$M \cong A^r \oplus \bigoplus_{\substack{\mathfrak{p} \in \operatorname{Max}(A) \\ k \geq 1}} (A/\mathfrak{p}^k)^{\mu(\mathfrak{p},k)}.$$

Demostración. Sabemos que $M/\tau(M)$ es libre de rango finito y hay una sucesión exacta corta

$$0 \longrightarrow \tau(M) \longrightarrow M \longrightarrow M/\tau(M) \longrightarrow 0$$

Como $M/\tau(M)$ es proyectivo, esa sucesión se parte y $M \cong \tau(M) \oplus M/\tau(M)$. Si r es el rango de $M/\tau(M)$, entonces hay un isomorfismo $M/\tau(M) \cong A^r$. Por otro lado, $\tau(M)$ es un módulo finitamente generado y de torsión, así que es artiniano y, en consecuencia, suma directa de una familia finita de submódulos finitamente generados, de torsión e indescomponibles. Se sigue entonces de la Proposición 6 que hay elementos irreducibles $p_1, \ldots, p_n$ y enteros $k_1, \ldots, k_n \geq 1$ tales que $\tau(M) = \bigoplus_{i=1}^n A/(p_i^{k_i})$. Existe, en definitiva, un isomorfismo

$$M \cong A^r \oplus \bigoplus_{i=1}^{n} A/(p_i^{k_i}) \tag{2}$$

Podemos ahora definir una función $\mu : \operatorname{Max}(A) \times \mathbb{N} \to \mathbb{N}_0$ poniendo, para cada $\mathfrak{p} \in \operatorname{Max}(A)$ y cada $k \geq 1$,

$$\mu(\mathfrak{p}, k) = \Big| \big\{ i \in \{1, \ldots, n\} : (p_i) = \mathfrak{p}, k_i = k \big\} \Big|.$$

Esta función tiene claramente soporte finito y el isomorfimo del enunciado no es más que el de (2) a menos de la asociatividad y la conmutatividad de la suma directa. □

Proposición 8. *En la situación de la proposición anterior, el entero $r \geq 0$ y la función $\mu : \operatorname{Max}(A) \times \mathbb{N} \to \mathbb{N}_0$ están unívocamente determinados por el módulo M.*

Demostración. Sean r, $r' \geq 0$ y μ, $\mu' : \operatorname{Max}(A) \times \mathbb{N} \to \mathbb{N}_0$ funcionees de soporte finito, consideremos los módulos

$$M = A^r \oplus \bigoplus_{\substack{\mathfrak{p} \in \operatorname{Max}(A) \\ k \geq 1}} (A/\mathfrak{p}^k)^{\mu(\mathfrak{p},k)}, \qquad M' = A^{r'} \oplus \bigoplus_{\substack{\mathfrak{p} \in \operatorname{Max}(A) \\ k \geq 1}} (A/\mathfrak{p}^k)^{\mu'(\mathfrak{p},k)},$$

y supongamos que hay un isomofismo $\phi : M \to M'$. Para probar la proposición bastará que mostremos que $r = r'$ y que $\mu = \mu'$.

El morfismo ϕ se restringe a un isomorfismo $\phi : \tau(M) \to \tau(M')$ e induce un isomorfismo $\bar{\phi} : M/\tau(M) \to M'/\tau(M')$. Los submódulos de torsión de M y de M' son claramente

$$\tau(M) = \bigoplus_{\substack{\mathfrak{p} \in \operatorname{Max}(A) \\ k \geq 1}} (A/\mathfrak{p}^k)^{\mu(\mathfrak{p},k)}, \qquad \tau(M') = \bigoplus_{\substack{\mathfrak{p} \in \operatorname{Max}(A) \\ k \geq 1}} (A/\mathfrak{p}^k)^{\mu'(\mathfrak{p},k)}.$$

Como entonces

$$A^r \cong M/\tau(M) \cong M'/\tau(M') \cong A^{r'}$$

y el rango de un módulo libre está bien determinado, vemos que $r = r'$.

Si $\mathfrak{q} \in \mathrm{Max}(A)$, entonces para todo primo $\mathfrak{p} \in \mathrm{Max}(A)$ distinto de $\mathfrak{q}$ y todo entero $k \geq 1$ es $(A/\mathfrak{p}^k)_\mathfrak{q} = 0$, y esto implica inmediatamente que

$$\begin{aligned}
\tau(M)_\mathfrak{q} &= \bigoplus_{k\geq 1} (A/\mathfrak{q}^k)_\mathfrak{q}^{\mu(\mathfrak{q},k)} = \bigoplus_{k\geq 1} (A_\mathfrak{q}/\mathfrak{q}^k A_\mathfrak{q})^{\mu(\mathfrak{q},k)}, \\
\tau(M')_\mathfrak{q} &= \bigoplus_{k\geq 1} (A/\mathfrak{q}^k)_\mathfrak{q}^{\mu'(\mathfrak{q},k)} = \bigoplus_{k\geq 1} (A_\mathfrak{q}/\mathfrak{q}^k A_\mathfrak{q})^{\mu'(\mathfrak{q},k)}.
\end{aligned}$$

Por otro lado, el isomorfismo $\phi : \tau(M) \to \tau(M')$ induce un isomofismo $\phi_\mathfrak{q} : \tau(M)_\mathfrak{q} \to \tau(M')_\mathfrak{q}$ de $A_\mathfrak{q}$-módulos. La igualdad de las funciones μ y μ' sigue entonces de la siguiente proposición. □

Proposición 9. *Si A es un dominio de ideales principales local de ideal maximal $\mathfrak{m}$ no nulo, $\mu : \mathbb{N} \to \mathbb{N}_0$ es una función de soporte finito y $M = \bigoplus_{k\geq 1} (A/\mathfrak{m}^k)^{\mu(k)}$, entonces para todo $k \geq 1$ vale que*

$$\mu(k) = \dim_{A/\mathfrak{m}} \frac{\mathfrak{m}^{k-1} \cdot M}{\mathfrak{m}^k \cdot M} - \dim_{A/\mathfrak{m}} \frac{\mathfrak{m}^k \cdot M}{\mathfrak{m}^{k+1} \cdot M}.$$

Demostración. Si k, $l \geq 0$, entonces

$$\mathfrak{m}^l \cdot A/\mathfrak{m}^k = \begin{cases} 0, & \text{si } l \geq k; \\ \mathfrak{m}^l/\mathfrak{m}^k, & \text{si } l < k. \end{cases}$$

Se sigue de esto que

$$\frac{\mathfrak{m}^l \cdot A/\mathfrak{m}^k}{\mathfrak{m}^{l+1} \cdot A/\mathfrak{m}^k} \cong \begin{cases} 0, & \text{si } l+1 > k; \\ \mathfrak{m}^l/\mathfrak{m}^{l+1} \cong A/\mathfrak{m}, & \text{si } l+1 \leq k \end{cases}$$

y, en consecuencia,

$$\frac{\mathfrak{m}^l \cdot M}{\mathfrak{m}^{l+1} \cdot M} \cong \bigoplus_{l+1\leq k} (A/\mathfrak{m})^{\mu(k)}.$$

Tomando dimensiones sobre el cuerpo residual $A/\mathfrak{m}$ vemos que

$$\dim_{A/\mathfrak{m}} \frac{\mathfrak{m}^l \cdot M}{\mathfrak{m}^{l+1} \cdot M} = \sum_{l+1\leq k} \mu(k)$$

y la fórmula del enunciado es consecuencia inmediata de esto. □

Proposición 10. *Si M es un módulo finitamente generado, entonces existe una cadena de ideales no nulos $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n$ tal que*

$$M = \bigoplus_{i=1}^{n} A/\mathfrak{a}_i.$$

De hecho, existe una única esa cadena de ideales con esa propiedad.

Demostración. De acuerdo a la Proposición 7, existen elementos no inversibles $x_1, \ldots, x_n \in A$ tales que

$$M \cong \bigoplus_{i=1}^{n} A/(x_i).$$

y podemos elegir, entre todas las descomposiciones de M de esta forma, una que tenga n mínimo. Más aún, entre todas las descomposiciones de M como suma directa de módulos cíclicos con esa cantidad de sumandos podemos suponer que la de arriba fue elegida de forma que el cardinal del conjunto

$$\Omega = \{(i, j) : 1 \leq i < j \leq n,\, x_j \nmid x_j, x_i \nmid x_j\}$$

es mínimo.

Supongamos que Ω no es vacío y, sin pérdida de generalidad, que $(1, 2) \in \Omega$. Si d y m son el máximo común divisor y el mínimo común múltiplo de x_1 y x_2, respectivamente, hay un isomorfismo $/(x_1) \oplus A/(x_2) \cong A/(d) \oplus A/(m)$ y entonces

$$M \cong A/(d) \oplus A/(m) \oplus \bigoplus_{i=3}^{n} A/(x_i).$$

Es fácil verificar que el cardinal del conjunto Ω correspondiente a esta descomposición es estrictamente menor al de aquélla con la que empezamos, y esto es absurdo en vista de la forma que elegimos esta última. Vemos así que, de hecho, el conjunto Ω de nuestra descomposición es vacío.

Esto significa, precisamente, que la relación de divisibilidad ordena al conjunto $\{x_1, \ldots, x_n\}$ totalmente y como consecuencia de eso, y a menos de reindexar sus elementos, que podemos suponer que $x_{i+1} \mid x_i$ para cada $i \in \{1, \ldots, n-1\}$. Si ponemos $\mathfrak{a}_i = (x_i)$, entonces, se satisfacen las condiciones del enunciado. $\square$