Módulos sobre un dominio de ideales principales

Índice

Notación

En general, recurrimos a la siguiente notación.

- R: anillo no necesariamente conmutativo.
- K: anillo conmutativo, ocasionalmente, cuerpo.
- F: cuerpo.
- D: dominio, dominio de ideales principales.
- A, B, C, T: módulos sobre un anillo.
- V: espacio vectorial.
- M, P o A o B: matrices.
- f, g: polinomios.
- t, f: transformaciones lineales, morfismos de módulos, endomorfismos.

Otras convenciones Escribiremos "DIP" en lugar de "dominio de ideales principales", "DFU" en lugar de "dominio de factorización única" y "f.g." en lugar de "finitamente generado".

1 Módulos noetherianos

Sea R un anillo con unidad. Sea A un R-módulo (a derecha). Se dice que A *cumple con la condición de cadenas ascendentes (de submódulos)*, o que A *es noetheriano*, si toda sucesión

$$S_0 \subset S_1 \subset \cdots \subset A$$

de submódulos es eventualmente constante, es decir, existe $m \geq 0$ tal que $S_{m+k} = S_m$ para todo $k \geq 0$ ($S_{n+1} = S_n$ para todo $n \geq m$).

Teorema 1.1. *Un R-módulo a derecha cumple con la condición de cadenas ascendentes, si y sólo si todo submódulo es f.g. En particular, en tal caso, el R-módulo es f.g.*

Se dice que el anillo R *es noetheriano a derecha*, si R_R es noetheriano en tanto R-módulo a derecha. Si R es conmutativo, se dice, simplemente, que R es noetheriano. Todo dominio de ideales principales es noetheriano.

Observación 1.2. Todo módulo noetheriano posee submódulos propios maximales. En particular, todo anillo noetheriano posee ideales (unilaterales) propios maximales. Más aun, sean R y Q anillos y sea M un Q, R-bimódulo, noetheiano respecto de R. Consideremos la familia de sub-R-módulos de M invariantes por la acción de Q a izquierda. Dentro de esta familia tomamos una cadena, $\mathcal{C}$. Si $N = \bigcup \mathcal{C}$, entonces N es un sub-Q, R-bimódulo de M. Podría no ser propio, *a priori*. Pero N es f.g., por ser sub-R-módulo, es decir que existe un conjunto finito $\{x_1, \ldots, x_n\}$ de generadores de N (en tanto R-módulo). Ahora, como $x_1 \in N$, existe $S_1 \in \mathcal{C}$ tal que $x_1 \in S_1$. Para $k > 1$, existe $S_k \in \mathcal{C}$ tal que $x_k \in S_k$. Si x_k no perteneciera a S_{k-1}, entonces, como $\mathcal{C}$ es un conjunto totalmente ordenado, $S_{k-1} \subset S_k$. En todo caso, para $k > 1$, existe S_k tal que S_{k-1} esté contenido en S_k y x_k pertenezca a S_k. Inductivamente, $S_n \supset \{x_1, \ldots, x_n\}$ y, dado que N está generado por este conjunto, S_n es un R-módulo y $N \supset S_n$,

$$N = \bigcup \mathcal{C} = S_n \in \mathcal{C}$$

es un elemento de la cadena y, en particular, de la familia de sub-Q, R-bimódulos propios de M. Como corolario, todo anillo noetheriano posee ideales *biláteros* propios maximales, también.

Lema 1.3. *Sea $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ una suceseción exacta corta de R-módulos a derecha. Entonces B es noetheriano, si y sólo si A y C lo son.*

Teorema 1.4. *Si R es un anillo noetheriano a derecha, un R-módulo a derecha es noetheriano, si (y sólo si) es f.g. (Recíprocamente, si R tiene esta propiedad, entonces es noetheriano).*

Demostración. Considerar $0 \longrightarrow R^{n-1} \longrightarrow R^n \longrightarrow R \longrightarrow 0$ e inducción en n. $\square$

2 Dominios de ideales principales

En esta sección hacemos un breve repaso de algunas propiedades de un DIP.

Fijamos D un DIP. En particular, D es conmutativo, con lo cual no haremos énfasis en distinguir entre módulos a derecha y módulos a izquierda.

Ejemplos 2.1. El anillo de enteros racionales $\mathbb{Z}$, el anillo de enteros de Gauss $\mathbb{Z}[i]$ y el anillo de polinomios con coeficientes en un cuerpo son DIPs.

Ejemplo 2.2. El anillo $\mathbb{Z}[X]$ de polinomios con coeficientes enteros no es un DIP: el ideal $\langle 2, X\rangle$, por ejemplo, no es principal. En general, si D es un DIP y $p \in D$ es un irreducible/primo, entonces $\langle p, X\rangle \leq D[X]$ es un ideal que no es principal. Si $f|p$, como D es dominio, por grado, $f \in D$ debe ser constante. Si, además, $f|X$, entonces $(g_0 + g_1 X + g_2 X^2 + \cdots) f = X$ implica que $g_1 f = 1$ y $f \in D^\times$. Notamos que lo único que necesitamos es que existan elementos no invertibles en D para poder hallar un ideal que no sea principal.

Ejemplo 2.3. El anillo $K = (\mathbb{Z}/9)[X]$ de polinomios con coeficientes en los enteros módulo 9 no es un DIP. El ideal $\langle 3, X\rangle$ no es principal: si $f \in K$ dividiera a 3 y a X, entonces

$$h f = 3 \pmod 9 \quad \text{y} \quad k f = X \pmod 9$$

Para ciertos $h, k \in K$. Reduciendo módulo 3,

$$h f = 0 \pmod 3 \quad \text{y} \quad k f = X \neq 0 \pmod 3 \; .$$

En particular, Como $D = (\mathbb{Z}/3)[X]$ es dominio, o bien $h = 0$ en D, o bien $f = 0$ en D. Esto último no puede ocurrir, porque $X \neq 0$, con lo cual, los coeficientes de h son todos divisibles por 3. Pero, ahora, $3 \neq 0$ en $\mathbb{Z}/9$ implica que el término independiente de f debe ser una unidad. Finalmente, como $\mathbb{Z}/3$ es un cuerpo, X es irreducible en el DIP D y, por lo tanto, o bien $f \in D^\times$, o bien f es asociado a X en D. Esto último tampoco puede ocurrir, dado que el término independiente de f es distinto de cero. En definitiva, f debe ser de la forma

$$f = f_0 + f_1 X + f_2 X^2 + \cdots ,$$

con $f_0 \in (\mathbb{Z}/9)^\times$ y f_i divisible por 3, si $i > 0$. Esto quiere decir que f es una unidad en el anillo de polinomios K, pues el término independiente es una unidad y el resto de los coeficientes son nilpotentes.[1]

Ejemplo 2.4. Dado $n \geq 2$, no es cierto que el anillo cociente $\mathbb{Z}/n$ sea un DIP. Salvo en los casos en que $n = p$ es primo, $\mathbb{Z}/n$ no es dominio. Aun así, todos los ideales son principales: por los teoremas de isomorfismo, hay una correspondencia

$$\big\{ I \subset \mathbb{Z}/n \,:\, \text{ideal} \big\} \leftrightarrow \big\{ \langle n\rangle \subset J \subset \mathbb{Z} \,:\, \text{ideal} \big\} ,$$

[1] Ver [1, p. 11], ejercicio 2 del capítulo 1.

dada por $J \mapsto \overline{J} = \{x \,(\mathsf{mod}\, n) \,:\, x \in J\}$. Si $I = \overline{J}$ es un ideal en el cociente, y $J = \langle x \rangle$, entonces $I = \langle x \,(\mathsf{mod}\, n) \rangle$ es principal. En general, si bien un cociente de un DIP puede no ser un dominio, todos sus ideales son principales.

Ejemplo 2.5. Sean E, F dos cuerpos y sea $K = E \times F$ el anillo producto. Los ideales de K son exactamente

$$\begin{tikzcd} & E \times 0 \arrow[dr, hook] & \\ 0 \arrow[ur, hook] \arrow[dr, hook] & & E \times F \\ & 0 \times F \arrow[ur, hook] & \end{tikzcd}$$

Todos ellos son principales: $0 = \langle 0 \rangle$, $E \times 0 = \langle (1,0) \rangle$, $0 \times F = \langle (0,1) \rangle$ y $K = \langle (1,1) \rangle$.

3 Módulos cíclicos

Sea R un anillo.

Definición 3.1. Un R-módulo C se dice *cíclico* si está generado por un único elemento, es decir, existe $c_0 \in C$ tal que

$$C = \langle c_0 \rangle_R \;.$$

Decimos que c_0 es un *generador* de C o que C *está generado por* c_0.

Observación 3.2. Dado un R-módulo cíclico C y un generador $c_0 \in C$, queda determinado un epimorfismo $R \to C$ por $1 \in R \mapsto c_0 \in C$. El módulo C es isomorfo a un cociente de R por un submódulo (un ideal) $I \leq R$:

$$C \simeq R/I \;.$$

El ideal I no es otra cosa que el *anulador de* C, o bien de c_0, en R:

$$I = \mathsf{Ann}_R(C) = \mathsf{Ann}(C) = \mathsf{Ann}(c_0) \;.$$

Ahora tomamos un DIP, D. En este caso, todo ideal tiene la forma $I = \langle \mu \rangle$, para cierto $\mu \in D$; el generador del ideal, μ, está determinado salvo unidades en D.

Definición 3.3. Sea $C = \langle c_0 \rangle$ un D-módulo cíclico. El *orden de* C es cualquier elemento $\mu \in D$ tal que $C \simeq D/\langle \mu \rangle$. A veces, también llamaremos *orden de* C al ideal $\langle \mu \rangle$. Dado un D-módulo A y $x \in A$ el *orden de* x es el orden del submódulo cíclico, $\langle x \rangle \subset A$, generado por x.

Observación 3.4. Si C es un D-módulo cíclico, entonces $\mathsf{Ann}(C) = \langle \mu \rangle$. Si $\mu = 0$, $C \simeq D$ es libre.

Ejemplo 3.5. Tomamos $D = \mathbb{Z}$ y $\mu = m \in \mathbb{Z}$. Si $C = \mathbb{Z}/\langle m \rangle$, entonces C posee m elementos y m, el menor entero positivo tal que $m \cdot 1 = 0$, es el orden de C. Los $\mathbb{Z}$-módulos son exactamente los grupos abelianos. Los cocientes $\mathbb{Z}/\langle m \rangle$ son precisamente los grupos cíclicos; el grupo cíclico de m elementos se corresponde con el cociente de $\mathbb{Z}$ por el ideal $m\mathbb{Z}$. A un grupo finito se le asocian dos números que dan una idea de su tamaño y su "dinámica": su cardinal, es decir, la cantidad de elementos, y su *orden*, el menor entero positivo m tal que $x^m = 1$ para todo x del grupo. Para los grupos cíclicos estas dos nociones coinciden: si $C = \langle x \rangle$, su orden es el menor entero positivo m tal que $x^m = 1$, y x^k son todos distintos para $k \in [\![1, m]\!]$.

Si $n \mid m$, entonces la inclusión de ideales $\langle m \rangle \subset \langle n \rangle$ induce un morfismo sobreyectivo

$$\mathsf{red}_n \ : \ \mathbb{Z}/m \ \to \ \mathbb{Z}/n \ ,$$

dado por reducir módulo n –es decir, $j \pmod{m} \ \mapsto \ j \pmod{n}$– y cuyo núcleo es el submódulo $\langle n \pmod{m} \rangle \subset \mathbb{Z}/m$. Por otro lado, si $m = n \cdot k$, tenemos un morfismo bien definido

$$\mathsf{mult}_k \ : \ \mathbb{Z}/n \ \to \ \mathbb{Z}/m \ ,$$

dado por multiplicar por k: la imagen de $i \pmod{n}$ es $k \cdot i \pmod{m}$. Esta aplicación está bien definida: si $i \in i' + l \cdot n$ en $\mathbb{Z}$, entonces

$$k \cdot i \ = \ k \cdot i' + (k \cdot l) \cdot n \ = \ k \cdot i' + l \cdot m \ .$$

En particular, la clase módulo m de $k \cdot i$ está bien definida, cualquiera sea el representante i de la clase módulo n. Esta aplicación es un morfismo de $\mathbb{Z}$-módulos: multiplicar es lineal. Finalmente, este morfismo es inyectivo:

$$k \cdot i \ \equiv \ 0 \pmod{m} \ \Leftrightarrow \ k \cdot i \ = \ l \cdot m \ = \ k \cdot (l \cdot n) \ \Leftrightarrow \ i \ = \ l \cdot n \ \Leftrightarrow \ i \ \equiv \ 0 \pmod{n} \ .$$

La imagen de este morfismo es el submódulo generado por k en $\mathbb{Z}/m$, es decir, $\langle k \pmod{m} \rangle$. Notemos que, si $x \in \langle k \pmod{m} \rangle$, entonces $n \cdot x \equiv 0 \pmod{m}$. Recíprocamente, si $n \cdot x \equiv 0 \pmod{m}$, entonces

$$n \cdot x \ = \ l \cdot m \ = \ n \cdot (k \cdot l)$$

y, en particular, $x = k \cdot l$. En definitiva,

$$\mathsf{img}(\mathsf{mult}_k) \ = \ \langle k \pmod{m} \rangle \ = \ \mathsf{ker}(\mathsf{mult}_n) \ ,$$

donde $\mathsf{mult}_n : \mathbb{Z}/m \to \mathbb{Z}/m$ es el morfismo dado por multiplicar por n las clases módulo m. Así, podemos armar la siguiente sucesión exacta:

$$0 \longrightarrow \mathbb{Z}/n \xrightarrow{\mathsf{mult}_k} \mathbb{Z}/m \xrightarrow{\mathsf{mult}_n} \mathbb{Z}/m \longrightarrow \mathbb{Z}/n \longrightarrow 0$$

Estas observaciones son válidas, en general, para cualquier módulo cíclico sobre un DIP. Más precisamente, si D es un DIP, $C = \langle c_0 \rangle$ es un módulo cíclico de orden μ y $\mu = \kappa \cdot \nu$ en D, entonces lo morfismos análogos a los del Ejemplo 3.5 producen la siguiente sucesión exacta:

$$
\begin{tikzcd}
0 \arrow[r] & D/\langle \nu \rangle \arrow[r, "\mathsf{mult}_\kappa"] \arrow[d, dashed] & D/\langle \mu \rangle \arrow[r, "\mathsf{mult}_\nu"] \arrow[d, "\sim"] & D/\langle \mu \rangle \arrow[r] \arrow[d, "\sim"] & D/\langle \nu \rangle \arrow[r] \arrow[d, dashed] & 0 \\
0 \arrow[r] & \langle \kappa \cdot c_0 \rangle \arrow[r] & C = \langle c_0 \rangle \arrow[r, "\mathsf{mult}_\nu"'] & C \arrow[r] & C/\langle \nu \cdot c_0 \rangle \arrow[r] & 0
\end{tikzcd}
$$

La exactitud en la composición $\mathsf{mult}_\nu \circ \mathsf{mult}_\kappa$ es el resultado del siguiente lema.

Lema 3.6 (fundamental)**.** *Sea C un D-módulo cíclico de orden μ y supongamos que $\mu = \nu \cdot \kappa$ es una factorización en D. Si $x \in C$ es tal que $\nu \cdot x = 0$, entonces existe $x' \in C$ tal que $\kappa \cdot x' = x$.*

Demostración. Sea $C = \langle c_0 \rangle$ y sea $\lambda \in D$ tal que $x = \lambda \cdot c_0$. Si $\nu \cdot x = 0$, entonces $\nu \cdot \lambda \in \langle \mu \rangle$. Esto significa que existe $\lambda' \in D$ tal que $\nu \cdot \lambda = \nu \cdot (\kappa \cdot \lambda')$. Como D es dominio, cancelando, $\lambda = \kappa \cdot \lambda'$. Así, $x = \kappa \cdot x'$ con $x' = \lambda' \cdot c_0$. $\square$

Proposición 3.7. *Sea A un D-módulo noetheriano. Sea $C \subset A$ un submódulo cíclico de orden μ. Si $\mu \in \mathsf{Ann} A$ ($\mu \cdot A = 0$), entonces C es un sumando directo de A.*

Demostración. Como A es noetheriano, existe un conjunto finito $\{a_1, \ldots, a_k\}$ tal que

$$A = C + \langle a_1, \ldots, a_k \rangle \ .$$

Si $k = 0$, $A = C$ y no hay nada que probar. Para $k \geq 1$, definimos $a = a_k$ y $A_0 = C + \langle a_1, \ldots, a_{k-1} \rangle$. Supongamos, inductivamente, que la proposición es cierta cuando A/C está generado por, a lo sumo, $k - 1$ elementos. La condición $\mu \cdot A = 0$ implica $\mu \cdot A_0 = 0$ y, por hipótesis inductiva, C es sumando directo de A_0:

$$A_0 = C \oplus B_0 \ . \tag{1}$$

Es decir, existe un complemento $B_0 \subset A_0$ de C en A_0:

$$A_0 = C + B_0 \quad \text{y} \quad C \cap B_0 = 0 \ .$$

Dado que $A = A_0 + \langle a \rangle$, el cociente A/A_0 es cíclico generado por la clase $a + A_0$. Si $\kappa \in D$ es el orden de este cociente, $\mu \cdot (A/A_0) = 0$ implica que $\mu \in \mathsf{Ann}(A/A_0) = \langle \kappa \rangle$ y existe $\nu \in D$ tal que $\mu = \nu \cdot \kappa$.[2]

Ahora bien, como κ anula a A/A_0, debe estar $\kappa \cdot a \in A_0$. Por (1), existen $x \in C$ y $b_0 \in B_0$ tales que $\kappa \cdot a = x + b_0$. Multiplicando por ν, se deduce que $\nu \cdot x + \nu \cdot b_0 = 0$ y,

[2] Notemos que $\Leftrightarrow A = A_0 \Leftrightarrow \kappa \in D^\times$ y podemos aplicar la hipótesis inductiva. Es decir, $A_0 \neq A$ equivale a que exista una factorización no trivial de μ en D.

por lo tanto, $\nu \cdot x = 0$ (y $\nu \cdot b_0 = 0$). Por el Lema 3.6, existe $x' \in C$ tal que $x = \kappa \cdot x'$, de lo que se deduce una igualdad

$$\kappa \cdot (a - x') \,=\, b_0 \; . \tag{2}$$

Si $a' = a - x'$, entonces $A = A_0 + \langle a \rangle = A_0 + \langle a' \rangle$. En particular, A/A_0 está generado por la clase $a' + A_0$. Definimos $B = B_0 + \langle a' \rangle$ y observamos que $A = C + B$. Pero también se cumple $C \cap B = 0$.[3] Se ve, entonces, que B es un complemento para C en A y el paso inductivo queda demostrado. □

Ejemplo 3.8. Si $D = F$ es un cuerpo y $A = V$ un F-e.v. de dimensión finita, entonces todo subespacio de dimensión 1 está complementado. Un poco más en general, si $t \in \mathsf{End}_F(V)$, V es un módulo sobre el álgebra de polinomios $F[X]$ con acción dada por $X \cdot v = t(v)$. Este módulo es f.g. (es de dimensión finita sobre F) y, por lo tanto, es noetheriano. Si $C \subset V$ es el subespacio $C = \big\langle v, t\,v, t^2\,v, \ldots \big\rangle$, entonces existe un subespacio t-invariante $W \subset V$ tal que

$$V \,=\, C \oplus W \; .$$

Ejemplo 3.9. Sea C un grupo cíclico (abstracto). Sea x un generador del grupo y sea $C' \leq C$ un subgrupo. Para todo $z \in C'$, existe $k \in \mathbb{Z}$ tal que $z = x^k$. Queremos probar que C' es cíclico. Si $C' = 1$, no hay nada que probar. Supongamos que este no es el caso y sea $n \geq 1$ el menor entero *positivo* k tal que $x^k \in C'$. Afirmamos que $C' = \langle y \rangle$, con $y = x^n$. Sea $z \in C'$ y sea $\tilde{n}$ tal que $z = x^{\tilde{n}}$. Escribimos $\tilde{n} = q\,n + r$, con $q, r \in \mathbb{Z}$ y $0 \leq r < n$, y

$$x^r \,=\, x^{\tilde{n} - q\,n} \,=\, z\,y^{-q} \,\in\, C' \; .$$

Por definición de n, debe ser $r = 0$ y $z = y^q \in \langle y \rangle$.

Ejemplo 3.10. Sea G un grupo abstracto, no necesariamente abeliano, de orden m.[4] Entonces G es un grupo cíclico, si y sólo si, por cada divisor $d \mid m$, G posee a lo sumo un subgrupo cíclico de orden d. Demostremos esta afirmación.

Supongamos, primero, que G es cíclico de orden m, que está generado por un elemento x_0, y sea d un divisor del orden –en particular, esto implica que el cardinal de G es finito e igual a m. El elemento $x = x_0^{m/d}$ verifica:

$$x^n = 1 \;\Leftrightarrow\; d \mid n \; .$$

[3]Esto es así, pues, en primer lugar, si $c \in C$, $b_0' \in B_0$ y $\alpha \in D$ verifican $c = \alpha \cdot a' + b_0' \in C \cap B$, entonces $\alpha \cdot a' = c - b_0' \in A_0$ y $\alpha \in \langle \kappa \rangle$ y, en segundo lugar, $\alpha \cdot a'$ es múltiplo de b_0 (por (2)), también, con lo que $c \in C \cap B_0 = 0$.

[4]Estamos llamando *orden de G* al menor entero positivo m tal que, para todo $x \in G$, $x^m = 1$. Es decir, *a priori*, G podría ser infinito. Para referirnos espcíficamente a la cantidad de elementos de G usaremos la palabra "cardinal" y escribiremos $|G|$. Si supiésemos que $|G| < \infty$, entonces, como $x^{|G|} = 1$ para todo $x \in G$, debe ser $m \leq |G|$.

En particular, $C_d :\equiv \langle x \rangle \leq G$ es un subgrupo cíclico de orden d. Tomemos, ahora, dos subgrupos cíclicos $\langle y \rangle, \langle z \rangle \leq G$ ambos de orden un divisor de d. Existen $k, l \in \mathbb{Z}$ tales que $y = x_0^k$ e $z = x_0^l$. Entonces

$$x_0^{d\,(k-l)} \;=\; (yz^{-1})^d \;=\; y^d\,(z^d)^{-1} \;=\; 1\;,$$

de lo que se deduce que $k \equiv l\,(\mathsf{mod}\, m/d)$. En consecuencia, todo subgrupo cíclico de orden un divisor de d es de la forma $\left\langle x_0^{t\,(m/d)} \right\rangle$ para algún entero t. Así, todo subgrupo cíclico de orden un divisor de d, está contenido en C_d y, por cardinalidad, C_d es el único subgrupo de G de orden exactamente d.

Supongamos, ahora, que, para cada divisor $d \mid m$, G posee a lo sumo un subgrupo cíclico de orden d. Veamos, en primer lugar, que esto implica que G es finito. Si $G = 1$, no hay nada que probar. En otro caso, sea $x \in G$, $x \neq 1$. El subgrupo $C = \langle x \rangle$ es cíclico y $x^m = 1$ implica que C es finito. Si d es el orden de C, el menor entero positivo tal que $x^d = 1$, entonces $d \mid m$. Ahora, o bien $G = C$ es cíclico, o bien existe $x' \in G \smallsetminus C$. En este segundo caso, $C' = \langle x' \rangle$ es un subgrupo cíclico, finito y de orden un divisor de m que, por unicidad, debe ser distinto de d. Para cada divisor $d \mid m$ elegimos $C_d \leq G$ cíclico de orden d o $C_d = 1$, si no existe tal subgrupo. Afirmamos que

$$G \;=\; \bigcup_{d \mid m} C_d\;.$$

Si $x \in G$, por lo que dijimos antes, o bien $x = 1$, o bien $\langle x \rangle$ es uno de los subgrupos C_d. En todo caso, x pertenece a la unión de la derecha. Ahora bien, la unión se realiza sobre una cantidad finita de divisores d y cada uno de los subgrupos C_d es finito. Por lo tanto, G es finito. Más precisamente, como:

- $C_d = 1$ o $C_d = \langle x \rangle$ (lo segundo sólo si existe x de orden d),
- $e \mid d \Rightarrow C_e \leq C_d$ (por unicidad) y
- la cantidad de elementos de orden d es, a lo sumo, $\varphi(d)$ (también por unicidad),

tenemos la siguiente cota:

$$|G| \;\leq\; \sum_{d \mid m} \varphi(d) \;=\; m\;.$$

Dado que, además, $m \leq |G|$, debe valer la igualdad. En particular, debe existir $x \in G$ de orden exactamente m.

El siguiente resultado generaliza esta observación a módulos cíclicos sobre un DIP.

Proposición 3.11. *Sea C un D-módulo cíclico de orden μ. Entonces:*

1. *todo submódulo $C' \subset C$ es cíclico de orden μ' un divisor de μ;*

2. *dado un ideal principal $\langle\lambda\rangle \supset \langle\mu\rangle$ en D, existe un único submódulo $C' \subset C$ de orden λ.*

Demostración. Sea $C' \subset C$ un submódulo. Como C es cíclico existe un epimorfismo $\theta : D \to C$, lo que, como D es noetheriano, implica que C es noetheriano. Como C' es un submódulo de C, es noetheriano, también. En particular, C' es f.g. Sea $c_0 \in C$ un generador –concretamente, el generador $c_0 = \theta(1)$– y sean $c_1, \ldots, c_k \in C'$ tales que $C' = \langle c_1, \ldots, c_k\rangle$. Como $c_i \in C$, existen $a_i \in D$ tales que $c_i = a_i\, c_0$. Los coeficientes a_i generan un ideal en D. Sea $\nu \in D$ un generador de este ideal:

$$\langle\nu\rangle = \langle a_1, \ldots, a_k\rangle \subset D\ .$$

Elegimos $b_i \in D$ de manera que $a_i = b_i\,\nu$ y definimos $c_0' = \theta(\nu)$. Entonces

$$c_i = \theta(a_i) = \theta(b_i\,\nu) = b_i\, c_0'\ .$$

De esto se deduce que $C' = \langle c_1, \ldots, c_k\rangle \subset \langle c_0'\rangle \subset C$. Recíprocamente, $\nu = \sum_i b_i'\, a_i$ para ciertos $b_i' \in D$. Entonces

$$c_0' = \theta(\nu) = \theta\Big(\sum_i b_i'\, a_i\Big) = \sum_i b_i'\, c_i\ ,$$

que es una expresión en C'. En definitiva, $C' = \langle c_0'\rangle = \langle\theta(\nu)\rangle$ y, como $\mu\cdot C' = 0$, μ debe ser un múltiplo del orden del sub-D-módulo (D-submódulo) cíclico C'. Esto demuestra 1.

Sean, ahora, $C', C'' \subset C$ submódulos (necesariamente cíclicos) de orden $\langle\lambda\rangle$, ambos. Por 1, la suma $C' + C''$ también es cíclica y, si μ' es su orden, la cadena de inclusiones $C', C'' \subset C' + C'' \subset C$ implica que $\langle\lambda\rangle \supset \langle\mu'\rangle \supset \langle\mu\rangle$.[5] Dado que $\lambda\cdot\big(C' + C''\big) = 0$, debe cumplirse $\lambda \in \langle\mu'\rangle$ y

$$\langle\lambda\rangle = \big\langle\mu'\big\rangle\ .$$

Pero, entonces, C' (por ejemplo) es un submódulo cíclico de orden λ del módulo noetheriano $C' + C''$, que verifica $\lambda\cdot\big(C' + C''\big) = 0$. Por la Proposición 3.7,

$$C' + C'' = C' \oplus B\ ,$$

para cierto $B \subset C' + C''$. Sea c_0 un generador de $C' + C''$ y sea c_0' un generador de C'. Sea $\theta : D \to C' + C''$ el epimorfismo dado por $\theta(1) = c_0$ y sea $\theta' : D \to C'$ el epimorfismo $\theta'(1) = c_0'$. Tomamos $\kappa \in D$ tal que $c_0' = \kappa\, c_0$ y $\gamma \in D$ y $b \in B$ tales que $c_0 = \gamma\, c_0' + b$. Entonces

$$c_0' = \kappa\, c_0 = (\kappa\gamma)\, c_0' + \kappa\, b\ .$$

[5] A partir de este punto, ya no se hace referencia a C.

Como $C' \cap B = 0$, vale que $\kappa\, b = 0$ y $1 - \kappa\gamma \in \langle\lambda\rangle$, es decir, $\theta'(1) = \theta'(\kappa\gamma)$. Pero, como el núcleo de θ' coincide con el núcleo de θ,

$$\theta(1) \;=\; \theta(\kappa\gamma) \;,$$

también. Ahora, como D es conmutativo, multiplicar por γ es un morfismo de D-módulos. En particular,

$$c_0 \;=\; \theta(1) \;=\; \gamma\,\theta(\kappa) \;=\; \gamma\, c_0' \;,$$

que pertenece a C'. Así, $C' = C' + C''$. Análogamente, $C'' = C' + C''$ y $C' = C''$. $\square$

La siguiente proposición caracteriza los cocientes de los módulos cíclicos.

Proposición 3.12. *Sea C un D-módulo cíclico de orden μ.* (i) *Todo cociente de C es cíclico de orden $\langle\nu\rangle + \langle\mu\rangle$, para algún elemento $\nu \in D$;* (ii) *dado $\nu \in D$, existe un cociente de C de orden $\langle\nu\rangle + \langle\mu\rangle$.*

Demostración. Sea $\langle\nu\rangle$ un ideal (principal) arbitrario de D. Sea $\theta : D \to C$ *un* epi y sea $C' = \theta\big(\langle\nu\rangle\big)$ el submódulo imagen del ideal $\langle\nu\rangle$. Entonces el siguiente diagrama es conmutativo y sus filas y columnas son exactas:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \nu \cap \mu \arrow[r] \arrow[d] & \mu \arrow[r] \arrow[d] & \begin{array}{c} \mu/\nu \cap \mu \\ \simeq (\nu+\mu)/\nu \end{array} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \nu \arrow[r] \arrow[d] & D \arrow[r] \arrow[d, "\theta"'] & D/\nu \arrow[r] \arrow[d, "\bar{\theta}"] & 0 \\
0 \arrow[r] & C' \arrow[r] \arrow[d] & C \arrow[r, "\pi"'] \arrow[d] & C/C' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

En definitiva,

$$C/C' \;\simeq\; (D/\nu)/((\nu+\mu)/\nu) \;\simeq\; D/(\nu+\mu) \;.$$

Por otro lado, si $C' \subset C$ es un submódulo, $C' = \theta\big(\langle\nu\rangle\big)$ para algún ideal $\langle\nu\rangle \subset D$, con lo cual, todo cociente es de esta forma. $\square$

4 Módulos de torsión y el Teorema de estructura

4.1 Definiciones y enunciado del teorema

Definición 4.1. Sea R un anillo y sea A un R-módulo (a izquierda). Un elemento $x \in A$ se dice *de torsión*, si existe $\kappa \in R \smallsetminus \{0\}$ tal que $\kappa \cdot x = 0$, es decir, si el ideal $\mathsf{Ann}_R(x) \subset R$ no es cero. Se dice que A es un *módulo de torsión*, si todos sus elementos son de torsión.

Observación 4.2. Si $x \in A$ es de torsión y $x \neq 0$, necesariamente, $\mathsf{Ann}(x) \subsetneq R$ es un ideal propio. Sea A un R-módulo f.g. y sea $\{a_1, \ldots, a_k\}$ un conjunto generador. Entonces

$$\mathsf{Ann}(A) = \mathsf{Ann}(a_1) \cap \cdots \cap \mathsf{Ann}(a_k) .$$

En particular, A es de torsión, si y sólo si los a_i son de torsión.

Observación 4.3. Sea A un R-módulo. Si A no es de torsión, entonces $\mathsf{Ann}(A) = 0$, pero la recíproca no es cierta. Por ejemplo, si

$$A = \bigoplus_p \mathbb{Z}/p$$

entonces A es de torsión, pero $\mathsf{Ann}(A) = \bigcap_p \langle p \rangle = 0$. Supongamos que $A = \langle a_1, \ldots, a_k \rangle$. Como los ideales anuladores son ideales biláteros,

$$\mathsf{Ann}(A) \supset \mathsf{Ann}(a_1) \cdots \mathsf{Ann}(a_k) .$$

Podría suceder que el producto de la derecha sea cero. Pero, si R fuese "dominio", es decir, si no tuviese elementos de torsión (divisores de cero), entonces un producto de ideales distintos de cero no puedría ser cero. En definitiva, si R es un anillo sin elementos de torsión y A es un R-módulo f.g., A es de torsión, si y sólo si $\mathsf{Ann}(A) \neq 0$.

Observación 4.4. Si D es un DIP y A es un D-módulo de torsión, existen $\mu_i \in D \smallsetminus \{0\}$ tales que $\mathsf{Ann}(a_i) = \langle \mu_i \rangle$. Como D es un dominio, el producto $\mu_1 \cdots \mu_k \in D$ es no nulo y pertenece al ideal anulador de A. En particular,

$$\mathsf{Ann}(A) = \langle \mu_1 \rangle \cap \cdots \cap \langle \mu_k \rangle \supset \langle \mu_1 \cdots \mu_k \rangle \neq 0 .$$

Por lo tanto, existe $\nu \in D$, no nulo, tal que $\mathsf{Ann}(A) = \langle \nu \rangle$.

Definición 4.5. Dado un D-módulo de torsión A, se denomina *anulador minimal de A* a cualquier generador del ideal $\mathsf{Ann}(A)$.

Definición 4.6. Sea K un anillo conmutativo. Dos ideales $I, J \leq K$ son *coprimos*, si $I + J = 1$. En ese caso, I y J verifican $I \cap J = I \cdot J$.[6]

Proposición 4.7. *Sea A un D-módulo, sean $x, y \in A$ elementos de torsión y sean $\mu, \nu \in D$ sus órdenes respectivos. Si μ y ν son coprimos, entonces $x + y$ tiene orden $\mu \cdot \nu$.*

[6] $x \in I \cap J \Rightarrow x = x \cdot 1 = x \cdot (y + z) \Rightarrow x \in J \cdot I + I \cdot J$.

Demostración. Asumiendo que $\langle\mu\rangle + \langle\nu\rangle = 1$, existen $\gamma, \delta \in D$ tales que $\gamma\,\mu + \delta\,\nu = 1$ en D. En particular,

$$x \,=\, \delta\,\nu\,x \,=\, \delta\,\nu\,(x+y) \quad \text{e} \quad y \,=\, \gamma\,\mu\,y \,=\gamma\,\mu\,(x+y)\ .$$

Si λ denota el orden de $x+y$, entonces $\mu\,\nu \in \langle\lambda\rangle$. Pero

$$\lambda\,x \,=\, \lambda\,(\delta\,\nu)\,(x+y) \,=\, (\delta\,\nu)\,\lambda\,(x+y) \,=\, 0\ .$$

Similarmente, $\lambda\,y = 0$. En definitiva, $\lambda \in \langle\mu\rangle \cap \langle\nu\rangle = \langle\mu\,\nu\rangle$. □

Teorema 4.8 (de estructura)**.** *Sea A un módulo de torsión f.g. sobre un dominio de ideales principales D. Existen escalares $\mu_1, \ldots, \mu_k \in D$ tales que*

$$\langle\mu_1\rangle \,\subset\, \cdots \,\subset\, \langle\mu_k\rangle$$

y un isomorfismo

$$A \,\simeq\, C_1 \oplus \cdots \oplus C_k\ , \tag{3}$$

donde C_i es un D-módulo cíclico de orden $\langle\mu_i\rangle$.

4.2 Demostración del Teorema de estructura

La idea de la demostración es usar la Proposición 4.7 para reconstruir el módulo A a partir de submódulos cíclicos. Para poder aplicar este resultado, necesitamos garantizar que exista un submódulo cíclico $C \subset A$ con $\mathsf{Ann}(C) = \mathsf{Ann}(A)$. Si aceptamos esto, deberíamos poder encontrar una descomposición de la forma:

$$A \,=\, C \,\oplus\, A'\ .$$

Recordando que A es noetheriano, sabemos que A' es noetheriano; además, como A es un módulo de torsión, A' es de torsión, también. En resumen, A' satisface las mismas hipótesis que A, con lo cual, deberíamos poder hallar un submódulo cíclico $C' \subset A'$ y una descomposción $A' = C' \oplus A''$. Así,

$$A \,=\, C \,\oplus\, C' \,\oplus\, A''\ .$$

Lema 4.9. *Si A es un D-módulo de torsión, f.g., con anulador minimal ν, entonces existe un elemento en A de orden exactamente ν.*

Demostración de 4.9. Como D es un DIP, D es un DFU. Si ν es un anulador minimal de A, $\nu \,=\, u_0\,p_1^{e_1}\cdots p_r^{e_r}$, para ciertos primos no asociados $p_1, \ldots, p_r \in D$, exponentes positivos $e_i \geq 1$ y una unidad $u_0 \in D^{\times}$. Para cada i, como $e_i \geq 1$, existen factorizaciones $\nu = p_i\,\nu_i = p_i^{e_i}\,\kappa_i$ en D. En particular, la inclusión $\langle\nu\rangle \subsetneq \langle\nu_i\rangle$ es estricta. Por definición, existe $x_i \in A$ tal que $\nu_i\,x_i \neq 0$. Si $y_i = \kappa_i\,x_i$, entonces

$$p_i^{e_i}\,y_i \,=\, (p_i^{e_i}\,\kappa_i)\,x_i \,=\, \nu\,x_i \,=\, 0 \quad \text{pero} \quad p_i^{e_i-1}\,y_i \,=\, \nu_i\,x_i \,\neq\, 0\ .$$

Si denotamos el orden de y_i por μ_i, entonces $\langle p_i^{e_i} \rangle \subset \langle \mu_i \rangle$. Por ser D un DFU, $\mu_i = p_i^{d_i}$, con $d_i \in [\![1, e_i]\!]$, o un asociado. Pero, la segunda de las igualdades anteriores implica que la inclusión $\langle \mu_i \rangle \subsetneq \left\langle p_i^{e_i-1} \right\rangle$ es estricta, con lo que $\mu_i = p_i^{e_i}$. En definitiva, para cada factor coprimo $p_i^{e_i}$ de ν, es posible hallar un elemento de orden exactamente $p_i^{e_i}$. Ahora, como los p_i son primos no asociados, la suma $y_1 + \cdots + y_r$ tiene orden $\langle p_1^{e_1} \cdots p_r^{e_r} \rangle = \langle \nu \rangle$. □

Demostración de 4.8. Sea A un D-módulo f.g. de torsión. Como D es un DIP, A es noetheriano. Por el Lema 4.9, existe $c_1 \in A$ de orden $\langle \nu \rangle = \mathsf{Ann}(A)$. Si $C_1 = \langle c_1 \rangle \subset A$, por la Proposición 3.7, $A = C_1 \oplus A_1$, para cierto submódulo complementario $A_1 \subset A$. Por ser un submódulo de A, A_1 es noetheriano y $\mathsf{Ann}(A_1) \supset \mathsf{Ann}(A)$. Si ν_1 es un generador del anulador de A_1, o bien A_1 es cíclico de orden ν_1, o bien se descompone como una suma directa $A_1 = C_2 \oplus A_2$, donde C_2 es cíclico de orden ν_1 y A_2 es no nulo, de torsión y f.g. En general, si $k \geq 1$, y existen submódulos cíclicos $C_1, \ldots, C_k$ de A y $A_k \subset A$ no nulo tales que

$$
\begin{gathered}
A = C_1 \oplus \cdots \oplus C_k \oplus A_k \quad \text{y} \\
\mathsf{Ann}(C_1) \subset \cdots \subset \mathsf{Ann}(C_k) \subset \mathsf{Ann}(A_k) \ ,
\end{gathered}
$$

entonces A_k es cíclico o existe una descomposición $A_k = C_{k+1} \oplus A_{k+1}$ con C_{k+1} cíclico y $\mathsf{Ann}(C_{k+1}) = \mathsf{Ann}(A_k)$. Si A no admitiese una descomposición como en (3), podríamos definir una sucesión creciente no acotada

$$
C_1 \subset C_1 \oplus C_2 \subset \cdots \subset A \ .
$$

Pero esto contradiría la noetherianeidad de A. □

4.3 Unicidad de la descomposición (3)

Teorema 4.10 (de unicidad)**.** *Sea A un D-módulo de torsión f.g. y sean $A = C_1 \oplus \cdots \oplus C_k$ y $A = C'_1 \oplus \cdots \oplus C'_l$ dos descomposiciones de A como suma directa de submódulos cíclicos tales que, si μ_i denota el orden de C_i y μ'_i el orden de C'_i, entonces $\langle \mu_i \rangle \subset \langle \mu_{i+1} \rangle$ y $\langle \mu'_i \rangle \subset \langle \mu'_{i+1} \rangle$. Entonces $l = k$ y $\langle \mu_i \rangle = \langle \mu'_i \rangle$ para cada i.*[7]

Observación 4.11. Sea K un anillo conmutativo. Dado un K-módulo A y un elemento $\kappa \in K$, la aplicación $\mathsf{mult}_\kappa : A \to A$ dada por $\mathsf{mult}_\kappa(x) = \kappa\, x$ induce un endomorfismo en A. Introducimos la siguiente notación:

$$
\kappa \cdot A :\equiv \mathsf{img}(\mathsf{mult}_\kappa) \quad , \quad A[\kappa] :\equiv \mathsf{ker}(\mathsf{mult}_\kappa) \ .
$$

Si $f : A \to B$ un morfismo de K-módulos, se cumple que

$$
f\big(\kappa \cdot A\big) \subset \kappa \cdot B \quad \text{y} \quad f\big(A[\kappa]\big) \subset B[\kappa] \ ,
$$

[7] Si $\mathsf{Ann}(C_i) \subset \mathsf{Ann}(C_{i+1})$ para todo i y $\mathsf{Ann}(C'_j) \subset \mathsf{Ann}(C'_{j+1})$ para todo j, entones $k = l$ y $\mathsf{Ann}(C_i) = \mathsf{Ann}(C'_i)$ para cada i.

con lo que, por restricción y correstricción, quedan definidos morfismos

$$f : \kappa \cdot A \to \kappa \cdot B \quad \text{y} \quad f : A[\kappa] \to B[\kappa] \ .$$

Las aplicaciones $A \mapsto \kappa \cdot A$ y $A \mapsto A[\kappa]$ determinan endofuntores en la categoría de K-módulos. Estos funtores son *aditivos*: dados $f, g : A \to B$, entonces, por ejemplo, $f + g : A[\kappa] \to B[\kappa]$ coincide con la suma de $f, g : A[\kappa] \to B[\kappa]$. En particular, estos funtores respetan sumas directas, es decir,

$$\kappa \cdot (A \oplus B) = (\kappa \cdot A) \oplus (\kappa \cdot B) \quad \text{y} \quad (A \oplus B)[\kappa] = A[\kappa] \oplus B[\kappa] \ .$$

Lema 4.12. *Sea C un D-módulo ciclico de orden $\langle \mu \rangle$.*

1. *Si $\kappa \in D$ es coprimo con μ, entonces $\kappa \cdot C = C$ y $C[\kappa] = 0$.*
2. *Si, en cambio, $\langle \mu \rangle \subset \langle \kappa \rangle$ y $\mu = \nu\, \kappa$, entonces los submódulos (cíclicos) $\kappa \cdot C$ y $C[\kappa]$ son de orden ν y κ, respectivamente.*

Demostración de 4.12. Si $\langle \mu \rangle + \langle \kappa \rangle = 1$, existen $\gamma, \delta \in D$ tales que $\gamma\, \mu + \delta\, \kappa = 1$. Si $x \in C$, entonces $x = \kappa\, (\delta\, x) \in \kappa \cdot C$. Pero también $x = \delta\, (\kappa\, x)$, con lo que $x \in C[\kappa]$ fuerza que $x = 0$.

Si $\langle \mu \rangle \subset \langle \kappa \rangle$ y $\mu = \nu\, \kappa$, entonces $\nu \cdot \big(\kappa \cdot C\big) = 0$ y $\kappa \cdot C \subset C[\nu]$. Pero, por el Lema 3.6, si $x \in C[\nu]$, existe $x' \in C$ tal que $x = \kappa\, x'$ y, por lo tanto, $x \in \kappa \cdot C$. En definitiva,

$$\kappa \cdot C = C[\nu] \ .$$

Si $\lambda \in D$ anula el submódulo $\kappa \cdot C$, entonces $\lambda\, \kappa$ anula C y $\lambda\, \kappa \in \langle \mu \rangle$. Por ser D un dominio, cancelando, se deduce que $\lambda \in \langle \nu \rangle$ y que $\kappa \cdot C = C[\nu]$ es un submódulo (cíclico) de orden ν. Por simetría (conmutatividad), $\nu \cdot C = C[\kappa]$ es de orden κ. □

Observación 4.13. Sea K un anillo conmutativo y sea R una K-álgebra. Sea M un R-módulo a izquierda y supongamos que existe un ideal bilátero $I \triangleleft R$ tal que $I \cdot M = 0$.[8] El cociente R/I tiene estructura de K-álgebra y M admite una estructura de R/I-módulo a izquierda dada por $\bar{r} \cdot x :\equiv r \cdot x$, para todo $\bar{r} \in R/I$ y todo $x \in M$. Estas estructuras son compatible en el sentido de que el diagrama de morfismos de álgebras siguiente es conmutativo:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & \mathsf{End}_K(M) \\ R/I \arrow[ur, dashed] & \end{tikzcd}$$

[8] El ideal $\mathsf{Ann}_R(M)$ es bilátero. Estamos suponiendo que no es nulo y consideramos cualquier subideal bilátero contenido en el anulador. Por otra parte, si I es bilátero, podemos definir, para un R-módulo a izquierda arbitrario, los submódulos $I \cdot M$ y $M[I]$, de manera análoga.

Notemos que, si R es conmutativa, podemos reemplazar $\mathsf{End}_K(M)$ por $\mathsf{End}_R(M)$ en el diagrama anterior. Recíprocamente, dado un R/I-módulo a izquierda, podemos darle una estructura natural de R-módulo por $r \cdot x :\equiv \bar{r} \cdot x$. Con esta definición, I actúa trivialmente. En el caso conmutativo, si tenemos un morfismo de K-módulos $f : A \to B$, y sea cumple que $\kappa{\cdot}A = 0$ y que $\kappa{\cdot}B = 0$, entonces f induce un morfismo de $\bar{f} : A \to B$ de las estructuras de $K/\langle\kappa\rangle$-módulos correspondientes. En particular, si $f : A \to B$ es un morfismo arbitrario, la restricción $f : A[\kappa] \to B[\kappa]$ induce un morfismo $\bar{f} : A[\kappa] \to B[\kappa]$ de $K/\langle\kappa\rangle$-módulos.

Demostración de 4.10. Primero, hacemos una observación general. Si $A = C_1 \oplus \cdots \oplus C_k$ es una descomposición en sumandos cíclicos cuyos órdenes verifican $0 \neq \langle\mu_1\rangle \subset \cdots \subset \langle\mu_k\rangle$ y $p \in D$ es un primo tal que $\langle\mu_k\rangle \subset \langle p\rangle$, tomando el núcleo por la multiplicación por p, se deduce que

$$A[p] = C_1[p] \oplus \cdots \oplus C_k[p] \ . \tag{4}$$

Pero, por el Lema 4.12,

$$C_i[p] \simeq D/\langle p\rangle \ .$$

Como $\langle p\rangle$ es primo, el cociente $F = D/\langle p\rangle$ es un cuerpo y (4) se puede interpretar, por la Observación 4.13, como una descomposición en tanto espacio vectorial sobre F.

Supongamos, ahora, que contamos con una segunda descomposición $A = C'_1 \oplus \cdots \oplus C'_l$ y veamos que $k \leq l$. Elegimos $h \in [\![1, l]\!]$ como el máximo tal que $\langle\mu'_h\rangle \subset \langle p\rangle$, o, si no existe, $h = 0$. Si $h = l$, comparando (4) con $A[p] = C'_1[p] \oplus \cdots \oplus C'_l[p]$ como espacios vectoriales, concluimos que $k = l$.[9] Si $h < l$, entonces $\left\langle\mu'_{h+1}\right\rangle \not\subset \langle p\rangle$, con lo que μ'_{h+1} y p son coprimos. Por el Lema 4.12, si $h = 0$, entonces $A[p] = 0$ y, por lo tanto, $k = h = 0$ y $A = 0$. Finalmente, si $0 < h < l$, entonces $A[p] = C'_1[p] \oplus \cdots \oplus C'_h[p]$, siendo el resto de los sumandos $C'_{h+j}[p] = 0$. Como antes, $h = k$, por ser iguales a la dimensión del mismo F-e.v. Conlcuimos que $k = h \leq l$ en todos los casos. Por simetría, $l \leq k$ y las longitudes de las descomposiciones debían ser iguales.

Sabiendo que $k = l$, sea $t \in [\![0, k]\!]$ tal que $\langle\mu_i\rangle = \langle\mu'_i\rangle$ para todo $i \leq t$, o bien $t = 0$. Si $t = k$, no hay nada más que demostrar. Si $t < k$, $\langle\mu_{t+1}\rangle \neq \left\langle\mu'_{t+1}\right\rangle$. Sin pérdida de generalidad, se puede asumir que $\mu_{t+1} \notin \left\langle\mu'_{t+1}\right\rangle$. Sea $\kappa := \mu_{t+1}$. Si $t = 0$, multiplicando por κ las dos descomposiciones de A, se deduce que $\kappa \cdot C_i = \mu_1 \cdot C_i = 0$ para todo i. Pero $\kappa \cdot C'_1 \neq 0$, porque $\kappa = \mu_1 \notin \langle\mu'_1\rangle$, lo que se contradice con

$$\left(\kappa \cdot C'_1\right) \oplus * = \kappa \cdot A = 0 \ .$$

Si $0 < t < k$, un argumento similar muestra que

$$\left(\kappa \cdot C'_1\right) \oplus \cdots \oplus \left(\kappa \cdot C'_t\right) \oplus \left(\kappa \cdot C'_{t+1}\right) \oplus * = \kappa \cdot A = \left(\kappa \cdot C_1\right) \oplus \cdots \oplus \left(\kappa \cdot C_t\right) \ .$$

Pero, entonces, el D-módulo $\kappa \cdot A$ admitiría dos descomposiciones como suma directa de submódulos cíclicos de órdenes encajados de longitudes distintas (una de longitud t y otra de longitud, al menos, $t + 1$), lo cual es absurdo, teniendo en cuenta lo demostado en el párrafo anterior. □

[9] Invarianza de la dimensión para espacios vectoriales.

Ejemplo 4.14. Si $D = \mathbb{Z}$ es el aniillo de enteros racionales, entonces todo grupo abeliano *finito* $A \neq 0$ admite una descomposición de la forma

$$A \simeq \mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_k \ , \tag{5}$$

donde los enteros $m_1, \ldots, m_k$ son positivos, mayores que 1 y $m_{i+1}|m_i$. El entero m_1 es el entero (positivo) m más chico (en términos del orden usual de $\mathbb{Z}$) tal que $m \cdot A = 0$. La cantidad de elementos de A es el producto $m_1 \cdots m_k$.[10] Entonces, para hallar una descripción de todos los grupos abelianos finitos de orden prescripto n, basta con hallar todas las listas $m_1, \ldots, m_k \in \mathbb{Z}_{\geq 2}$ tales que $m_1 \cdots m_k = n$ y $m_{i+1}|m_i$.

Definición 4.15. Dado un D-módulo de torsión A, los órdenes de los submódulos que aparecen en una descomposición como en el Teorema 4.8 se denominan *factores invariantes* de A.

4.4 La noción de longitud

Definición 4.16. Sea D es un DIP.[11] En particular, D es DFU. Dado $\mu \in D$ no nulo ni unidad, existen primos $p_1, \ldots, p_r$, permitiendo asociados, tales que $\mu = p_1 \cdots p_r$. La *longitud* de μ es la cantidad de factores irreducibles $r \geq 1$ que aparecen en ésta, como en cualquier factorización como producto de irreducibles. Denotamos la longitud de μ por $\mathsf{l}(\mu)$. Si $u \in D^\times$, definimos $\mathsf{l}(u) :\equiv 0$. Definimos, además, $\mathsf{l}(0) :\equiv \infty$ y $n \leq \infty$ para todo $n \in \mathbb{Z}$.

Definición 4.17. Si A es un D-módulo de torsión, la *longitud* de $x \in A$ se define como $\mathsf{l}(x) :\equiv \mathsf{l}(\mu)$, donde $\mu \in D$ verifica $\langle \mu \rangle = \mathsf{Ann}(x)$. La *longitud* de A se define como $\mathsf{l}(A) = \mathsf{l}(\nu)$, donde $\langle \nu \rangle = \mathsf{Ann}(A)$.

En particular, si $x \in A$, $\mathsf{l}(\langle x \rangle) = \mathsf{l}(x)$. Si $\langle x \rangle \simeq D/\langle \mu \rangle$, entonces, cuanto mayor sea $\mathsf{l}(\mu)$, más chico será el ideal $\langle \mu \rangle$ y más grande será el módulo $\langle x \rangle$. En general, si $B \subset A$ es un submódulo, entonces $\mathsf{l}(B) \leq \mathsf{l}(A)$.

Observación 4.18. Si A no es f.g., podría suceder que $\mathsf{Ann}(A) = 0$ y, por lo tanto $\mathsf{l}(A) = \infty$. Si A es f.g., esto no puede suceder.[12]

Veamos cómo quedan expresados algunos de los resultados anteriores en términos de la longitud. Fijamos un DIP D. Los siguientes resultados son los análogos de la Proposición 3.7 y el Lema 4.9, respectivamente.

Proposición 4.19. *Sea A un D-módulo noetheriano. Si $C \subset A$ es un submódulo cíclico y $\mathsf{l}(C) = \mathsf{l}(A)$, entonces C es un sumando directo de A.*

Lema 4.20. *Si A es un D-módulo de torsión y f.g., existe $x \in A$ tal que $\mathsf{l}(x) = \mathsf{l}(A)$.*

[10] El orden, pero no el anulador minimal (el anulador minimal es m_1)

[11] Esta definición es válida en un DFU, pero, en aquel caso, no resulta ser la definición adecuada, habiendo ideales primos no principales.

[12] C.f. la Observación 4.2

A continuación, damos una segunda demostración del Teorema 4.8, intentando formalizar el argumento de la demostración anterior utilizando el concepto de longitud.[13]

Lema 4.21. *Sea $A = \langle x_1, \ldots, x_k \rangle$ un D-módulo f.g. Dada una lista $\gamma_1, \ldots, \gamma_k \in D$ de elementos coprimos. Existe un conjunto $\{y_1, \ldots, y_k\}$ de generadores de A, tal que $y_1 = \gamma_1 x_1 + \cdots + \gamma_k x_k$.*

Veamos la versión para grupos abelianos, es decir, $D = \mathbb{Z}$.[14]

Lema 4.22. *Sea $A = \langle x_1, \ldots, x_k \rangle$ un grupo abeliano f.g. Dada una lista $c_1, \ldots, c_k \in \mathbb{N} \cup \{0\}$ tal que $(c_1, \ldots, c_k) = 1$, existe un conjunto $\{y_1, \ldots, y_k\}$ de generadores de A tal que $y_1 = c_1 x_1 + \cdots + c_k x_k$.*

Demostración de 4.22. Sea $s = c_1 + \cdots + c_k$ y sea $y = c_1 x_1 + \cdots + c_k x_k$. La demostración es por inducción en s. Si $s = 1$, entonces $k = 1$ y $c_1 = 1$, con lo cual $y = x_1$. Supongamos que $s > 1$ –o, lo que es lo mismo, que $k > 1$. Como $(c_1, \ldots, c_k) = 1$, al menos dos de los c_i deben ser distintos de 0. Permutando los coeficientes, podemos asumir que $c_1 \geq c_2 > 0$. En ese caso, definimos

$$y' = (c_1 - c_2)\, x_1 + c_2\, (x_1 + x_2) + c_3\, x_3 + \cdots + c_k\, x_k \; .$$

Ahora, el conjunto $\{x_1, x_2 + x_1, x_3, \ldots, x_k\}$ genera A y $c_1 - c_2, c_2, c_3, \ldots, c_k$ es una lista de enteros no negativos y coprimos. Pero, además, $(c_1 - c_2) + c_2 + \cdots + c_k < s$. Por hipótesis inductiva, existe un conjunto de generadores $\{y_1, \ldots, y_k\}$ con $y_1 = y'$. Dado que $y' = y$, este conjunto de generadores satisface la conclusión del enunciado para s, demostrando el paso inductivo. □

Esta demostración se basa en el orden en el monoide $\mathbb{N} \cup \{0\}$ y su relación con la suma. Así como está, no está claro cómo se puede generalizar, incluso al otro caso importante: polinomios con coeficientes en un cuerpo. a demostración para un DIP arbitrario es un poco distinta.

Demostración de 4.21. Sea $y = \gamma_1 x_1 + \cdots + \gamma_k x_k$. La demostración es por inducción en la cantidad k de generadores. El caso $k = 1$ es trivial. Si $k = 2$, $(\gamma_1, \gamma_2) = 1$ implica que existen $\kappa_1, \kappa_2 \in D$ tales que $\gamma_1 \kappa_1 + \gamma_2 \kappa_2 = 1$. Esto quiere decir que la matriz

$$\begin{bmatrix} \gamma_1 & -\kappa_2 \\ \gamma_2 & \kappa_1 \end{bmatrix}$$

tiene determinante 1 y es invertible. Explícitamente, su inversa está dada por

$$\begin{bmatrix} \kappa_1 & \kappa_2 \\ -\gamma_2 & \gamma_1 \end{bmatrix} .$$

[13] C.f. [2, p. 188, § 3.8, exs. 4–6].
[14] C.f. [4, p. 26]

Si definimos $y_1 = \gamma_1 x_1 + \gamma_2 x_2$ e $y_2 = -\kappa_2 x_1 + \kappa_1 x_2$, entonces

$$x_1 = \kappa_1 y_1 - \gamma_2 y_2 \quad \text{y} \quad x_2 = \kappa_2 y_1 + \gamma_1 y_2 .$$

Es decir, $\{y_1, y_2\}$ es un conjunto de generadores e y_1 es como queríamos. Supongamos que $k > 2$ y que el resultado es cierto para una $k-1$ generadores. Llamamos A' al submódulo generado por $x_2, \ldots, x_k$ y $\delta = (\gamma_2, \ldots, \gamma_k)$ y definimos $\gamma_i' \in D$ tal que $\gamma_i = \delta \gamma_i'$, para $i \geq 2$. Por hipótesis inductiva, sabemos que existe un conjunto de generadores $\{z_2, \ldots, z_k\}$ del submódulo A' tal que $z_2 = \gamma_2' x_2 + \cdots + \gamma_k' x_k$. Sea, ahora, $B = \langle x_1, z_2 \rangle$. Como $(\gamma_1, \delta) = 1$, podemos aplicar el resultado con $k = 2$ y deducimos que existe un conjunto $\{y_1, y_2\}$ de generadores de B tal que $y_1 = \gamma_1 x_1 + \delta z_2$. Definiendo $y_i = z_i$, para $i \geq 3$, el conjunto $\{y_1, \ldots, y_k\}$ genera $B + A' = A$ e $y_1 = y$, como queríamos. □

Lema 4.23. *Sea A un D-módulo f.g. Sea $k \geq 1$ la mínima cantidad de generadores necesarios para generar A y sea $\{x_1, \ldots, x_k\}$ un conjunto de generadores con la propiedad de que el valor $\mathsf{l}(x_1)$ es mínimo, entre todos los posibles conjuntos de generadores con k elementos. Entonces $A = \langle x_1 \rangle \oplus A'$, donde $A' = \langle x_2, \ldots, x_k \rangle$. Además, se cumple que $\mathsf{Ann}(x) \supset \mathsf{Ann}(y)$, para todo $y \in A'$.*

Demostración. Por definición, $\mathsf{Ann}(x_1) \supset \mathsf{Ann}(\langle x_1 \rangle + A')$. Supongamos que $\langle x_1 \rangle \cap A' \neq 0$. Entonces existe una expresión

$$\gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_k x_k = 0 , \tag{6}$$

con $\gamma_1 x_1 \neq 0$ (y $\gamma_2 x_2 + \cdots + \gamma_k x_k \neq 0$). Si $\mathsf{Ann}(x_1) = \langle \mu \rangle$, entonces $\kappa := \gamma_1/(\gamma_1, \mu)$ es coprimo con μ. Por el Lema 4.12,

$$\langle x_1 \rangle = \langle \kappa x_1 \rangle \quad \text{y} \quad \mathsf{l}(\kappa x_1) = \mathsf{l}(x_1) .$$

En particular, el conjunto $\{\tilde{x}_1, \ldots, \tilde{x}_k\}$ donde $\tilde{x}_1 = \kappa x_1$ y $\tilde{x}_i = x_i$, para $i \geq 2$, genera A, posee k elementos y $\mathsf{l}(\tilde{x}_1)$ es, también, mínima. Entonces, sin pérdida de generalidad, podemos suponer que el coeficiente γ_1 en (6) es divisor (¡estricto!) de μ, generador de $\mathsf{Ann}(x_1)$.

Siguiendo con la demostración, sea $\delta = (\gamma_1, \ldots, \gamma_k)$ y sean $\gamma_i' \in D$ tales que $\gamma_i = \delta \gamma_i'$. Por el Lema 4.21, existe un conjunto $\{y_1, \ldots, y_k\}$ de generadores de A con $y_1 = \gamma_1' x_1 + \cdots + \gamma_k' x_k$. Pero entonces

$$\delta y_1 = 0 .$$

Esto quiere decir que $\delta \in \mathsf{Ann}(y_1)$ y, por lo tanto,

$$\mathsf{l}(y_1) \leq \mathsf{l}(\delta) \leq \mathsf{l}(\gamma_1) < \mathsf{l}(x_1) .$$

Esto contradice la minimalidad del conjunto de generadores.

Finalmente, veamos que $\mathsf{Ann}(x) \supset \mathsf{Ann}(y)$, para todo $y \in A'$. Es suficiente demostrar esta inclusión con $y = x_2$. Sean $\mu_1, \mu_2 \in D$ tales que $\mathsf{Ann}(x_i) = \langle \mu_i \rangle$ $(i = 1, 2)$ y sea

$\delta = (\mu_1, \mu_2)$. Si μ_1 y μ_2 no son asociados, entonces $\mathsf{l}(\delta) < \mathsf{l}(\mu_1)$. Elegimos $\mu_i' \in D$ tales que $\mu_i = \delta\, \mu_i'$ y aplicamos el Lema 4.21 a $B = \langle x_1, x_2 \rangle$ con la lista $\{\mu_1', \mu_2'\}$. Deducimos que existen y_1, y_2 generadores de B con $y_1 = \mu_1'\, x_1 + \mu_2'\, x_2$. Pero esto implica que, tomando $y_i = x_i$ para $i \geq 3$, el conjunto $\{y_1, \ldots, y_k\}$ genera $B + A' = A$ y cumple

$$\mathsf{l}(y_1) \;\leq\; \mathsf{l}(\delta) \;<\; \mathsf{l}(x_1) \;,$$

pues $\delta\, y_1 = \mu_1\, x_1 + \mu_2\, x_2 = 0$. Esto contradice, nuevamente, la minimalidad del conjunto $\{x_1, \ldots, x_k\}$. $\square$

Demostración alternativa de 4.8. Si A es un D-módulo f.g. Si A es cíclico, no hay nada que probar. Supongamos que la cantidad mínima de generadores para A es $k > 1$ y que el resultado es válido para módulos que admiten un conjunto de generadores con una cantidad menor de elementos. Elijamos (existe) un conjunto de generadores $\{x_1, \ldots, x_k\}$ que cumpla las hipótesis del Lema 4.23. Entonces $A = \langle x_1 \rangle \oplus A'$ y $\mathsf{Ann}(\tilde{C}_1) \supset \mathsf{Ann}(A')$, donde $\tilde{C}_1 = \langle x_1 \rangle$ y $A' = \langle x_2, \ldots, x_k \rangle$. Por hipótesis inductiva, como A' admite un conjunto de generadores más chico, sabemos que se descompone como una suma directa de submódulos cíclicos $\tilde{C}_2, \ldots, \tilde{C}_t$ tales que $\mathsf{Ann}(\tilde{C}_2) \supset \cdots \supset \mathsf{Ann}(\tilde{C}_t)$. La lista de submódulos se obtiene dando vuelta el orden de los $\tilde{C}_i$: $C_1 = \tilde{C}_t$, $C_2 = \tilde{C}_{t-1}$, $\ldots$, $C_t = \tilde{C}_1$. $\square$

En esta segunda demostración, en lugar de empezar por un elemento cuyo orden es el anulador minimal del módulo (un elemento longitud $\mathsf{l}(x) = \mathsf{l}(A)$, lo más grande posible), empezamos por un elemento de longitud lo más chica posible, siempre que el mismo pertenezca a una “base”, un conjunto minimal de generadores.

5 Módulos primarios y el Teorema de descomposición

Ejemplo 5.1. Supongamos que $m = a\, b$ con $(a, b) = 1$ (coprimos), entonces existen $r, s \in \mathbb{Z}$ tales que $r\, a + s\, b = 1$. Miramos la siguiente sucesión exacta:

$$\begin{tikzcd}
 & & & \mathbb{Z}/b \arrow[dl, "\mathsf{mult}_a"'] & & \\
0 \arrow[r] & \mathbb{Z}/a \arrow[r, "\mathsf{mult}_b"] & \mathbb{Z}/m \arrow[rr, "\mathsf{red}_b"'] & & \mathbb{Z}/b \arrow[ul, "\mathsf{mult}_r"', "\sim"] \arrow[r] & 0
\end{tikzcd}$$

Dado que r es una unidad módulo b, mult_r es un isomorfismo en $\mathbb{Z}/b$. Además,

$$\mathsf{red}_b \circ (\mathsf{mult}_a \circ \mathsf{mult}_r) \;=\; \mathsf{id}_{\mathbb{Z}/b} \;,$$

pues $r\, a \equiv 1 \,(\mathsf{mod}\, b)$. Análogamente, tenemos

$$\mathsf{red}_a \circ (\mathsf{mult}_b \circ \mathsf{mult}_s) \;=\; \mathsf{id}_{\mathbb{Z}/a} \;.$$

Pero también valen las igualdades

$$\mathsf{red}_a \circ (\mathsf{mult}_a \circ \mathsf{mult}_r) \;=\; 0 \quad \text{y} \quad \mathsf{red}_b \circ (\mathsf{mult}_b \circ \mathsf{mult}_s) \;=\; 0$$

Definamos $\mathsf{inc}_a = \mathsf{mult}_b \circ \mathsf{mult}_s$ e $\mathsf{inc}_b = \mathsf{mult}_a \circ \mathsf{mult}_s$. Entonces, dado $x \in \mathbb{Z}$ un entero arbitario,

$$\mathsf{inc}_b \circ \mathsf{red}_b(x) \;=\; \mathsf{mult}_a(\mathsf{mult}_r(x\,(\mathsf{mod}\,b))) \;=\; (r\,a)\,x\,(\mathsf{mod}\,m)\ .$$

De manera similar, $\mathsf{inc}_a \circ \mathsf{red}_a(x) \;=\; (s\,b)\,x\,(\mathsf{mod}\,m)$. Sumando ambas expresiones, deducimos que

$$\mathsf{inc}_b \circ \mathsf{red}_b \;+\; \mathsf{inc}_a \circ \mathsf{red}_a \;=\; \mathsf{id}_{\mathbb{Z}/m}\ .$$

En conclusión, vale la descomposición

$$\mathbb{Z}/m \;\simeq\; \mathbb{Z}/a \,\oplus\, \mathbb{Z}/b\ .$$

Sea D un DIP. El siguiente lema podría pensarse como un refinamiento del Lema fundamental 3.6 y generaliza la situación descripta en el Ejemplo 5.1.

Lema 5.2. *Sea A un D-módulo y sea $\nu \in D$ tal que $\mathsf{Ann}(A) = \langle \nu \rangle$. Si $\nu = \lambda\,\kappa$, con κ y λ coprimos. Entonces*

$$A \;=\; A[\kappa] \,\oplus\, A[\lambda] \;=\; \lambda \cdot A \,\oplus\, \kappa \cdot A\ .$$

Demostración. Como κ y λ son coprimos, $\langle\kappa\rangle + \langle\lambda\rangle = 1$ y $A = \big(\kappa \cdot A\big) + \big(\lambda \cdot A\big)$. En particular, $A[\kappa] \cap A[\lambda] = 0$. Pero $\kappa \cdot A \subset A[\lambda]$ y $\lambda \cdot A \subset A[\kappa]$, con lo cual, $A = A[\kappa] + A[\lambda]$ y, también, $\big(\kappa \cdot A\big) \cap \big(\lambda \cdot A\big) = 0$. $\square$

Dicho de otra manera, la descomposición del anulador minimal de un D-módulo en factores coprimos se traduce en una descomposición análoga del D-módulo.

Definición 5.3. Dado un elemento primo $p \in D$, se denomina *D-módulo p-primario* a todo D-módulo cuyos elementos tengan orden una potencia de p. Un *D-módulo primario* es un módulo que es p-primario para algún primo p.

Observación 5.4. Todo D-módulo p-primario es de torsión. Si A es p-primario y $x \in A$, entonces $\mathsf{Ann}(x) = \langle p^e \rangle$ para cierto $e \geq 1$, pero el exponente puede no estar acotado en A.

Teorema 5.5 (de descomposición primaria)**.** *Sea A un D-módulo de torsión f.g. y sea $\mathsf{Ann}(A) = \langle \nu \rangle$ el anulador minimal de A. Si $\nu = p_1^{e_1} \cdots p_r^{e_r}$ es una descomposición de ν como producto de primos no asociados a potencias,*[15] *entonces*

$$A \;=\; \mathrm{T}_{p_1}A \,\oplus\, \cdots \,\oplus\, \mathrm{T}_{p_r}A\ , \tag{7}$$

donde

$$\mathrm{T}_p A \;=\; \bigcup_{k \geq 1} \Big\{ x \in A \,:\, \mathsf{Ann}(x) = \Big\langle p^k \Big\rangle \Big\} \;=\; \bigcup_{k \geq 1} \Big\{ x \in A \,:\, p^k\,x = 0 \Big\}$$

es el submódulo p-primario maximal en A.

[15] Una expresión de la forma $\nu = p_1^{e_1} \cdots p_r^{e_r}$ es una descomposición o factorización de $\nu \in D$ como producto de primos no asociados a potencias, si los elementos de la lista $p_1, \ldots, p_r$ son primos en D, coprimos de a pares y $e_1, \ldots, e_r \geq 1$.

Demostración. Si $r = 1$, $A = \mathrm{T}_{p_1}A$ y no hay nada más que probar. En otro caso, $\nu = \lambda\,\kappa$, con $\lambda = p_1^{e_1} \cdots p_{r-1}^{e_{r-1}}$ y $\kappa = p_r^{e_r}$. Por el Lema 5.2, $A = A[\kappa] \oplus A[\lambda]$. Pero $A[\kappa] \subset \mathrm{T}_{p_r}A$. Esta inclusión es una igualdad, porque ν es el anulador minimal ($\mathrm{T}_{p_r}A \subset A[\kappa]$). Análogamente, $\mathsf{Ann}(A[\lambda]) = \left\langle p_1^{e_1} \cdots p_{r-1}^{e_{r-1}} \right\rangle$ y vale que $\mathrm{T}_{p_i}\bigl(A[\lambda]\bigr) = \mathrm{T}_{p_i}A$, para todo $i \leq r-1$. Inductivamente, $A[\lambda] = \mathrm{T}_{p_1}A \oplus \cdots \oplus \mathrm{T}_{p_{r-1}}A$. $\square$

Aplicando el Teorema 4.8 a un módulo p-primario f.g., cada sumando cíclico en la descomposición es de orden una potencia de p. Entonces, por ejemplo,

$$\mathrm{T}_pA = C_1 \oplus \cdots \oplus C_k\ , \tag{8}$$

donde $\mathsf{Ann}(C_i) = \left\langle p^{d_i} \right\rangle$ y $d_1 \geq \cdots \geq d_k$.

Corolario 5.6. *Sea A un D-módulo de torsión f.g. Entonces A se descompone como suma directa de submódulos cíclicos, cada uno de orden una potencia de un primo en D. La lista de los órdenes de estos submódulos es única, salvo permutaciones o reemplazo de un primo por un primo asociado.*

Referencias

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Reading, Mass.-Menlo Park, Calif.-London-Don Mills, Ont.: Addison-Wesley Publishing Company (1969). 1969.

[2] N. Jacobson. *Basic algebra I. 2nd ed.* New York: W. H. Freeman and Company. XVIII, 499 p. £ 19.95 (1985). 1985.

[3] S. MacLane and G. Birkhoff. *Algebra.* 3rd. ed. New York etc.: Chelsea Publishing Company, 1999.

[4] J. S. Milne. *Group Theory (v4.00)*. Available at www.jmilne.org/math/. 2021.