Forma normal de Smith: un ejemplo

Francisco Kordon

21 de noviembre de 2017

Empezamos recordando el enunciado del Teorema de estructura de módulos finitamente generados sobre un dominio de ideales principales.

Teorema (de Estructura). *Sean A un dominio de ideales principales y M un A-módulo finitamente generado. Existen $n, r \in \mathbb{N}_0$ y $d_1, \ldots, d_r \in A \setminus \{0\}$ tales que hay un isomorfismo de A-módulos*

$$M \cong A^n \oplus \frac{A}{(d_1)} \oplus \ldots \oplus \frac{A}{(d_r)}$$

y $d_1 \mid d_2 \mid \ldots \mid d_r$. Además, esta escritura es única en el siguiente sentido: si $m, s \in \mathbb{N}_0$ y $d'_1, \ldots, d'_s \in A \setminus \{0\}$ son tales que $M \cong A^m \oplus A/(d'_1) \oplus \ldots \oplus A/(d'_s)$, entonces $m = n$, $r = s$ y $d_i = \mu_i d'_i$, con μ_i una unidad de A para todo $1 \leq i \leq r$.

Los elementos $d_1, \ldots, d_r$ son llamados los factores invariantes de M —que, vimos, están definidos salvo asociados—, y n es el rango de M.

Ejercicio. *Sea G el grupo abeliano generado por los elementos e_1, e_2 y e_3 que cumplen las relaciones*

$$\begin{aligned} 2e_1 + 2e_2 + 2e_3 &= 0; \\ 3e_1 &= 6e_3. \end{aligned}$$

Hallar el rango y los factores invariantes de G.

El Teorema, en principio, no nos da pistas de cómo encontrar rango y factores invariantes; sin embargo, si logramos descomponer a G, nuestro $\mathbb{Z}$-módulo, como en el teorema, la unicidad nos asegura que los habremos encontrado. La siguiente proposición nos da la estrategia que vamos a utilizar.

Proposición. *Sean A un dominio de ideales principales, $k \in \mathbb{N}$ y $B \in A^{k \times k}$. Existen matrices inversibles $P, Q \in A^{k \times k}$ de manera que*

$$PBQ = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & d_k \end{pmatrix},$$

con $d_1, \ldots, d_k$ elementos de A que cumplen $d_1 \mid d_2 \mid \ldots \mid d_k$. Salvo por asociados, los d's son únicos, y esta matriz es llamada la forma normal de Smith *de B.*

Veamos de qué manera la proposición puede ayudarnos a resolver el ejercicio. Nuestro G es el cociente del grupo abeliano libre en tres generadores por el subespacio H generado por las relaciones: si $H = ((2,2,2),(3,0,-6))$, es $G = \mathbb{Z}^3/H$. Poniendo ahora

$$B = \begin{pmatrix} 2 & 2 & 2 \\ 3 & 0 & -6 \\ 0 & 0 & 0 \end{pmatrix}$$

tenemos que $G = \mathbb{Z}^3/(\text{filas de } B)$. Supongamos que efectivamente encontramos matrices invertibles $P, Q \in \mathbb{Z}^{3\times 3}$ de manera que PBQ es la forma normal de Smith de B. En tal caso, multiplicamos a derecha y obtenemos

$$PB = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix} Q^{-1}.$$

Sean v_1, v_2 y v_3 las filas de la matriz Q^{-1}. Como esta matriz es invertible, $\{v_1, v_2, v_3\}$ es una base de $\mathbb{Z}^3$. Si f_1, f_2 y f_3 son las filas de PB, la invertibildad de P nos asegura que $\{f_1, f_2, f_3\}$ genera H. Como la ecuación anterior dice que $f_i = d_i v_i$, tenemos

$$G = \frac{\langle v_1, v_2, v_3 \rangle}{(d_1 v_1, d_2 v_2, d_3 v_3)} = \frac{\langle v_1 \rangle}{(d_1 v_1)} \oplus \frac{\langle v_2 \rangle}{(d_2 v_2)} \oplus \frac{\langle v_3 \rangle}{(d_3 v_3)} \cong \frac{\mathbb{Z}}{(d_1)} \oplus \frac{\mathbb{Z}}{(d_2)} \oplus \frac{\mathbb{Z}}{(d_3)}.$$

Poniendo $n \in \mathbb{N}_0$ tal que $d_{3-n+1}, \ldots, d_3 = 0$ y $d_i \neq 0$ para $1 \leq i < 3 - n$, vemos que n es el rango de G y $d_1, \ldots, d_3 - n$ son los factores invariantes de G. Concluimos, pues, que de encontrar la forma normal de Smith de B habremos resuelto el ejercicio.

Para «diagonalizar» B, sólo podemos multiplicar a izquierda o a derecha por matrices invertibles en $\mathbb{Z}$. Ahora bien, conocemos de álgebra lineal que las operaciones de filas o columnas siguientes pueden realizarse multiplicando por matrices invertibles —su determinante es una unidad—:

- permutar filas o columnas;
- multiplicar una fila o columna por una unidad; y
- sumar a una fila un múltiplo de otra (respectivamente, columnas).

Provistos de estas operaciones, diagonalizamos B:

$$\begin{pmatrix} 2 & 2 & 2 \\ 3 & 0 & -6 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow[\mapsto F_2]{F_2 - 2F_1} \begin{pmatrix} 2 & 2 & 2 \\ -1 & -4 & -10 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow[\mapsto F_1]{F_1 + 2F_2} \begin{pmatrix} 0 & -6 & -18 \\ -1 & -4 & -10 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{F_1 \leftrightarrow F_2} \begin{pmatrix} -1 & -4 & -10 \\ 0 & -6 & -18 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\xrightarrow[\mapsto C_2]{C_2 - 4C_1} \begin{pmatrix} -1 & 0 & -10 \\ 0 & -6 & -18 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow[\mapsto C_3]{C_3 - 10C_1} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -6 & -18 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow[\mapsto C_3]{C_3 - 3C_2} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Tenemos, pues, que nuestro G se descompone como

$$\mathbb{Z} \cong \frac{\mathbb{Z}}{(-1)} \oplus \frac{\mathbb{Z}}{(-6)} \oplus \frac{\mathbb{Z}}{(0)} = \mathbb{Z}_6 \oplus \mathbb{Z},$$

de manera que el único factor invariante es 6 y el rango es 1. Esto concluye la resolución del ejercicio.