10 Teoremas de estructura de grupos abelianos de tipo finito

Quedan cuestiones por reponder. Es cierto, aunque arduo de probar en el caso infinito, que todo subgrupo de un grupo abeliano libre es libre de rango no superior al del grupo. En las próximas lineas nos dedicamos pues al estudio de grupos abelianos finitamente generados, libres o no. En esencia, probaremos que todo grupo abeliano de tipo finito es la suma directa de unas cuantas copias de grupos monógenos y cíclicos. Para ello lo primero a resolver es la primera cuestión.

En efecto, sea $G =< x_1, \ldots, x_n >$. Entonces, G es isomorfo a $\mathbf{Z}^n/S$. Si conocemos un sistema generador finito $< f_1, \ldots, f_m >$ de S, lo que se reducirá a calcular el núcleo de un epimorfismo, podemos escribirlo como combinación lineal de la base canónica de $\mathbf{Z}^n$; ello da lugar a una matriz[1] A con coeficientes enteros:

$$(f_1, \ldots, f_m) = (e_1, \ldots, e_n)A$$

El algoritmo de la división euclídea permitirá encontrar[2] matrices P y Q regulares tales que

$$PAQ = \text{diag}\,[d_1, d_2, \ldots, d_r, 0, \ldots, 0]$$

donde los enteros positivos d_i están unívocamente determinados por S y cumplen

$$0 \neq d_1 \mid d_2 \mid \cdots \mid d_r$$

Ahora

$$(f_1, \ldots, f_m)Q = (e_1, \ldots, e_n)AQ = (e_1, \ldots, e_n)P^{-1}\text{diag}\,[d_1, d_2, \ldots, d_r, 0, \ldots, 0]$$

Luego, poniendo

$$(g_1, \ldots, g_m) = (f_1, \ldots, f_m)Q \quad (v_1, \ldots, v_n) = (e_1, \ldots, e_n)P^{-1}$$

tenemos respectivos sistema generador de S y base de $\mathbf{Z}^n$ tales que

$$(g_1, \ldots, g_m) = (v_1, \ldots, v_n)\text{diag}\,[d_1, d_2, \ldots, d_r, 0, \ldots, 0]$$

Es decir, $(d_1v_1, \ldots, d_rv_r)$ es el nuevo sistema generador de S. Puesto que los v_i son libres y los d_i no nulos, hemos obtenido una base de S. Así, será fácil ver que

$$G \cong \mathbf{Z}^n/S \cong \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_r\mathbf{Z} \oplus \mathbf{Z}^{n-r}$$

con $d_r \mid \cdots \mid d_2 \mid d_1$.

Veamos un ejemplo.

[1] la matriz cuyas columnas contiene las coordenadas de los generadores de S

[2] operaciones elementales en matrices enteras

Ejemplo Sea G el subgrupo de $M_2(\mathbf{Z}/6\mathbf{Z})$ generado por

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad N = \begin{pmatrix} 3 & 3 \\ 0 & 0 \end{pmatrix} \quad R = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}$$

Entonces, el núcleo del epimorfismo de $\mathbf{Z}^3$ en G está dado por

$$\{a, b, c) \in \mathbf{Z}^3 \mid a\,M + b\,N + c\,R = (0)$$

Haciendo operaciones,

$$\begin{pmatrix} 3b & a + 3b + 2c \\ a + 3c & 0 \end{pmatrix} = (0_{\mathbf{Z}/6\mathbf{Z}})$$

lo que conducirá a

$$(a, b, c) \in \mathbf{Z} < (18, 0, -6), (-18, 2, 6), (-12, 0, 6) >$$

Por tanto, un sistema generador del núcleo (f_1, f_2, f_3) está formado por esas tres ternas y

$$A = \begin{pmatrix} 18 & -18 & -12 \\ 0 & 2 & 0 \\ -6 & 6 & 6 \end{pmatrix}$$

Ahora

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -3 & 3 \\ 1 & -6 & 2 \end{pmatrix} \quad Q = \begin{pmatrix} 3 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \Longrightarrow PAQ = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Por tanto, poniendo $(v_i) = (e_i)P^{-1}$ y $(g_i) = (f_i)Q$ se tiene $(2v_1, 6v_2, 6v_3)$ como sistema generador del núcleo.

Finalmente, G es isomorfo a

$$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$$

Comencemos las justificaciones.

El primer resultado nos garantiza que el núcleo siempre es de tipo finito.

Por convenio, el grupo $\{0\}$ es libre de base vacía y por tanto de rango 0.

Teorema 10.1 *Todo subgrupo S de un grupo abeliano F libre de rango n es libre de rango $m \leq n$.*

Demostración: Razonaremos por inducción sobre n, siendo obvio el caso $n = 0$. Sea (e_i) una base de F y sea $G =< e_2, \ldots, e_n >$. Si $S \leq G$ el resultado es cierto por inducción. En caso contrario, existe $s \in S$ fuera de G; ahora,

$$s = z_1e_1 + \ldots + z_ne_n \notin G \Longrightarrow z_1 \neq 0$$

Por tanto, $\{z \in \mathbf{Z} \mid ze_1 + y \in S, y \in G\}$ es un subgrupo no nulo $d\mathbf{Z}$ de $\mathbf{Z}$; sea $f_1 = de_1 + y$ el elemento de S que debe existir.

Por otro lado, $S \cap G$ es un subgrupo de G y su rango $m-1$ será no superior a $n-1$. Por tanto, $m \leq n$; veremos que si $(f_2, \ldots, f_m)$ es base de $S \cap G$, $(f_1, f_2, \ldots, f_m)$ es base de S. Al efecto,

$\underline{(f_1, f_2, \ldots, f_m) \text{ es s.g. de } S}$

Dado $s \in S$, $s = z_1e_1 + (z_2e_2 + \cdots + z_ne_n)$ por lo que $z_1 = kd$ y

$$s - kf_1 = kde_1 + (z_2e_2 + \cdots + z_ne_n) - kf_1 = -ky + (z_2e_2 + \cdots + z_ne_n) \in S \cap G$$

Por tanto, s es c.l. de $(f_1, f_2, \ldots, f_m)$.

$\underline{(f_1, f_2, \ldots, f_m) \text{ es libre}}$

Sea $z_1f_1 + \cdots + z_nf_n = 0$. Es suficiente ver que $z_1 = 0$. Sustituyendo

$$z_1(de_1 + y) + (z_2f_2 + \cdots + z_nf_n) = 0 \Longrightarrow z_1de_1 + (z_1y + z_2f_2 + \cdots + z_nf_n) = 0$$

escribiendo el segundo sumando como c.l. de $(e_2, \ldots, e_n)$ y teniendo en cuenta que las $(e_1, e_2, \ldots, e_n)$ son libres $z_1d = 0$, por lo que $z_1 = 0$.

Observación 10.2 Antes de seguir, recordemos que es posible trabajar con matrices sobre cualquier conjunto. En particular podemos trabajar con matrices enteras, de polinomios,...; ahora bien, no debemos extender los conceptos de rango, regularidad,... a la ligera. En consecuencia, establezcamos poco apoco las premisas.

Definición 10.3 *Una matriz A sobre un dominio de integridad $\mathcal{D}$ se dice regular si existe otra matriz B sobre $\mathcal{D}$ tal que $AB = I_n$.*

Notemos que $AB = I_n$ es una igualdad en el cuerpo de fracciones K de $\mathcal{D}$, luego $BA = I_n$. Notemos asimismo que si P es regular lo es sobre K, y sus líneas deben ser libres en K^n. Por tanto, lo son en $\mathcal{D}^n$.

Por otro lado,

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

es una matriz de números enteros que no es regular en $M_2(\mathbf{Z})$. En efecto, su inversa sobre $\mathbf{Q}$ es única y tiene denominadores. Sin embargo, sus líneas son libres.

A fin de que las operaciones elementales constituyan cambios de base las matrices elementales deben ser regulares lo que afecta directamente a las de tipo 3. Por tanto,

Definición 10.4 *Se dice matriz elemental tipo 3 a $I_3 + (s-1)E_{ii}$, donde s es una unidad de $\mathcal{D}$.*

Ejemplos

Proposición 10.5 *Una matriz P es regular sobre $\mathcal{D}$ si y sólo si su determinante es una unidad en $\mathcal{D}$.*

Demostración: $PQ = I_n$ es una igualdad en el cuerpo de fracciones K; por tanto, $\det(P)\det(Q) = 1$ y $\det(P)$ es una unidad de $\mathcal{D}$.

Recíprocamente, si $\det(P)$ es una unidad de $\mathcal{D}$, en K la inversa de P no tiene fracciones, luego es inversa en $\mathcal{D}$.

Observación 10.6 Habrá observado el lector que en el ejemplo anterior se utiliza con cierto *descaro*

$$\begin{pmatrix} 3b & a+3b+2c \\ a+3c & 0 \end{pmatrix} = (0_{\mathbf{Z}/6\mathbf{Z}}) \iff$$

$$\iff (a,b,c) \in \mathbf{Z} < (18,0,-6), (-18,2,6), (-12,0,6) >$$

¿Cómo se ha llegado a esa conclusión? Notemos que la igualdad matricial conduce a un sistema homogéneo de 3 ecuaciones con 6 incógnitas sobre $\mathbf{Z}$.

Si $A \in M_{m\times n}(\mathbf{Z})$, el conjunto de soluciones enteras del sistema $AX = (0)$ es un subgrupo de $\mathbf{Z}^n$, que recibe el nombre de núcleo de A; se denota mediante $\mathcal{N}(A)$.

El cálculo del núcleo será paralelo al clásico de álgebra lineal sobre un cuerpo, ¡con cuidado!. El concepto de matriz escalonada, idéntico para este contexto, es clave.

Los dominios de integridad más conocidos en este contexto son $\mathbf{Z}$, por supuesto un cuerpo K, y $K[x]$. Poseen una propiedad esencial, la división euclídea; reciben el nombre de dominios euclídeos.

Definición 10.7 *Se dice dominio euclídeo a un dominio de integridad $\mathcal{D}$ con una función δ definida en los elementos no nulos de $\mathcal{D}$ y valores en $\mathbf{N}$ que cumple*

- $\delta(ab) \geq \max(\delta(a), \delta(b))$
- *Dados a, $b \neq 0$ existen q, r tales que $a = bq + r$ y $r = 0$ ó $\delta(r) < \delta(b)$.*

La función δ recibe el nombre de *norma euclídea*, o simplemente *norma*.

Ejemplos y contraejemplos

1. $\mathbf{Z}$ con la funnción valor absoluto.
2. Un cuerpo K con la función constante 1.
3. $K[x]$ con la función que asocia a cada polinomio no nulo su grado.
4. $\mathbf{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbf{Z}\}$ con la función $\|a + b\sqrt{-1}\| = \sqrt{a^2 + b^2}$.
5. $\mathbf{Z}[x]$ no puede ser un dominio euclídeo pues $x = 2x\,q(x) + r(x) \Longrightarrow 2 \mid 1$.

Proposición 10.8 *Sea $\mathcal{D}$ un dominio euclídeo. Entonces*

i) $\delta(1) \leq \delta(a)\, \forall a \in \mathcal{D}$.

ii) *Un elemento u es una unidad en $\mathcal{D}$ si y sólo si $\delta(1) = \delta(u)$*

iii) *Las unidades son divisores de cualquier elemento.*

Demostración:

El item i) es consecuencia directa de la definición pues $\delta(a) = \delta(a.1) \geq \delta(1)$.

Para el ii), $uv = 1 \Longrightarrow \delta(u) \leq \delta(uv) = \delta(1) \leq \delta(u) \Longrightarrow \delta(1) = \delta(u)$.

Recíprocamente, sea $\delta(u) = \delta(1)$ y dividamos 1 entre u; entonces $1 = uq + r$ y puesto que $\delta(r)$ no puede ser inferior a $\delta(1) = \delta(u)$, $r = 0$. Por tanto, $1 = uq$.

Finalmente, si u es unidad, $a = uq + r \Longrightarrow r = 0$ ya que $\delta(r)$ no puede ser inferior a $\delta(1) = \delta(u)$.

Podemos dar ya los resultados que nos interesan en los futuros cálculos.

Teorema 10.9 (Hermite) *Si A es una matriz sobre un dominio euclídeo, es posible describir matrices elementales $P_1, \ldots, P_s$ tales que*

$$P_s, \ldots, P_1 A = H$$

es escalonada por filas.

Demostración: La afirmación de Hermite es algo superior, pero en este contexto no es necesario afinar más.

La demostración es constructiva, utilizando la división euclídea. Recordemos que las matrices elementales a izquierda corresponden a operaciones elementales en las filas.

Paso 1: Mediante permutación de filas, colocar en el lugar (1,1) el término no nulo de la primera columna de menor norma. Si no existen término no nulos, pasar a la columna siguiente. Si se han acabado las columnas, FIN.

Paso 2: Si $a_{11} \mid a_{j1}\, \forall j$ hacer ceros en la primera columna. En caso contrario, sea a_{11} no divisor de a_{j1} y q el cociente de la división euclídea entre éste y aquél. Sumando a la fila j la primera multiplicada por $-q$, obtenemos en el lugar (j,1) el resto r no nulo, cuya norma es inferior a la de a_{11}. Permutando las filas 1 y j, r, ocupa el primer término de la matriz.

Paso 3: Iterar el paso 2 hasta obtener como primera columna $(a, 0, \ldots, 0)^t$. Esto es posible pues al ir descendiendo la norma, en el peor de los casos, llegamos a una unidad como lugar $(1, 1)$.

Paso 4: Si hay más de una columna, iterar desde el paso 1 en la submatriz que resulta de suprimir la primera fila y columna.

Paso 5: FIN.

Corolario 10.10 *Si A es una matriz sobre un dominio euclídeo, es posible describir matrices elementales $Q_1, \ldots, Q_t$ tales que*

$$AQ_1 \cdots Q_t = H$$

es escalonada por columnas.

Demostración: Como en el caso clásico, basta trasponer.

La unión de los dos resultados anteriores da para cada matriz A sobre un dominio euclídeo $\mathcal{D}$, matrices P y Q regulares, sobre $\mathcal{D}$, tales que

$$PAQ = \text{diag}\,[d_1, \ldots, d_r, 0, \ldots, 0]$$

Como aplicación se tiene:

Corolario 10.11 *Sea $\mathcal{S} =< a_1, \ldots, a_m >$ un subgrupo de $\mathbf{Z}^n$.*

i) *Sea A la matriz $n \times m$ cuyas columnas están formadas por las n-tuplas a_i. Sea Q regular tal que $AQ = G$ es escalonada por columnas. Entonces, las columnas $(G^1, \ldots, G^r)$ no nulas de G forman una base de $\mathcal{S}$*

ii) *Sea A la matriz $m \times n$ cuyas filas están formadas por las n-tuplas a_i. Sea P regular tal que $PA = F$ es escalonada por filas. Entonces, las filas $(F_1, \ldots, F_r)$ no nulas de G forman una base de $\mathcal{S}$*

Demostración:

i) Sistema generador

$$S \in \mathcal{S} \Longrightarrow S = AT = (AQ)(Q^{-1}T) = G(Q^{-1}T) \in < G^1, \ldots, G^r, (0), \ldots, (0) >$$
$$=< G^1, \ldots, G^r >$$

Libre

$$AQ = G \Longrightarrow PG = \text{diag}\,[d_1, \ldots, d_r, 0, \ldots, 0] \Longrightarrow G = [d_1 C^1, \ldots, d_r C^r, 0, \ldots, 0]$$

donde C^j es la columna j-sima de P^{-1}.

Luego,

$$\sum_{i=1}^{r} z_i G^i = (0) \Longrightarrow \sum_{i=1}^{r} z_i d_i C^i = (0) \overset{P\text{regular}}{\Longrightarrow} z_i d_i = 0, i = 1 \ldots, r \overset{d_i \neq 0}{\Longrightarrow} z_i = 0$$

ii) Basta trasponer. Este segundo enunciado recupera exactamente el método de encontrar una base en un subespacio de K^n a partir de un sistema generador.

Ejemplo Calcular una base del subgrupo de $\mathbf{Z}^2$ generado por $(2, 4), (3, 6)$.

Sea

$$A = \begin{pmatrix} 2 & 4 \\ 3 & 6 \end{pmatrix}$$

$$P = \begin{pmatrix} -1 & 1 \\ -3 & 2 \end{pmatrix} \Longrightarrow PA = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = F$$

Luego se trata de $F_1 = (1, 2)$

De esta manera el par $(1, 2)$ es una base del subgrupo.

Asimismo, estamo en condiciones de calcular el núcleo de una matriz.

Corolario 10.12 *Sea A una matriz de n columnas sobre un dominio euclídeo $\mathcal{D}$; sea Q regular tal que $AQ = G$ es escalonada por columnas y r el número de columnas no nulas de G. Entonces, $\mathcal{N}(A)$ es el conjunto de combinaciones lineales de las $n - r$ últimas columnas de Q, con coeficientes en $\mathcal{D}$.*

Demostración: Sea $G = (g_{ij})$. Notemos que existe P regular tal que

$$PG = \operatorname{diag}[g_{11}, \ldots, g_{rr}, 0, \ldots, 0]$$

Si S pertenece al núcleo,

$$\begin{aligned} S \quad &= \quad I_n S = Q(Q^{-1}S) = \sum_{j=1}^{n} t_j Q^j \Longrightarrow \\ &\Longrightarrow \quad (0) = AS = \sum_{j=1}^{n} t_j AQ^j \Longrightarrow (0) = \sum_{j=1}^{r} t_j AQ^j \Longrightarrow (0) = \sum_{j=1}^{r} t_j PAQ^j \\ &\Longrightarrow \quad t_j g_{jj} = 0, j \leq r \Longrightarrow t_j = 0, j \leq r \Longrightarrow S = \sum_{j=r+1}^{n} t_j Q^j \end{aligned}$$

Observación 10.13 Los resultados anteriores describen un procedimiento para calcular el núcleo de una matriz A sobre un dominio euclídeo $\mathcal{D}$:

1. Mediante operaciones elementales, en $\mathcal{D}$, escalonar por columnas A hasta obtener Q regular tal que $AQ = G$.

2. Sea r el número de términos no nulos de G. Escribir las columnas $Q^{r+1}, \ldots, Q^n$.

Observación 10.14 El procedimiento expuesto parece breve; sin embargo, los resultados pueden ser mejorados si lo alargamos un poquito. De hecho, es claro que encontrar el núcleo de A equivale a encontrar el de PA para cualquier P regular; ahora bien, si PA es escalonada por filas, el cálculo de su núcleo será más sencillo. Observemos el siguiente

Ejemplo Intentemos resolver nuestro problema inicial de la página 49

$$\begin{pmatrix} 3b & a+3b+2c \\ a+3c & 0 \end{pmatrix} = (0_{\mathbf{Z}/6\mathbf{Z}})$$

$$\Updownarrow$$

$$\begin{pmatrix} 3b & a+3b+2c \\ a+3c & 0 \end{pmatrix} = \begin{pmatrix} 6z_1 & 6z_2 \\ 6z_3 & 6z_4 \end{pmatrix}$$

$$\Updownarrow$$

$$\begin{pmatrix} 0 & 3 & 0 & -6 & & & \\ 1 & 3 & 2 & 0 & -6 & & \\ 1 & 0 & 3 & 0 & 0 & -6 & \\ 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = (0)$$

Sea A la matriz de coeficientes. Entonces, un escalonado por columnas de A conduce, mediante 8 operaciones elementales, a

$$A \begin{pmatrix} 0 & 1 & -2 & 0 & 18 & -12 & -18 \\ 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & -6 & 6 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -6 & 0 & 0 & 0 \end{pmatrix}$$

y las 3 últimas columnas de

$$\begin{pmatrix} 0 & 1 & -2 & 0 & 18 & -12 & -18 \\ 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & -6 & 6 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

dan el núcleo.

Sin embargo,

$$P_{12}A = \begin{pmatrix} 1 & 3 & 2 & 0 & -6 & & \\ 0 & 3 & 0 & -6 & & & \\ 1 & 0 & 3 & 0 & 0 & -6 & \\ 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{pmatrix} = B$$

$$P_{31}(-1)B = \begin{pmatrix} 1 & 3 & 2 & 0 & -6 & & \\ 0 & 3 & 0 & -6 & & & \\ 0 & -3 & 1 & 0 & 6 & -6 & \\ 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{pmatrix} = C$$

$$P_{32}(1)C = \begin{pmatrix} 1 & 3 & 2 & 0 & -6 & & \\ 0 & 3 & 0 & -6 & & & \\ 0 & 0 & 1 & -6 & 6 & -6 & \\ 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{pmatrix} = F$$

$$FP_{12}(-3)P_{13}(-2)P_{15}(6) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & -6 & 0 & 0 & 0 \\ 0 & 0 & 1 & -6 & 6 & -6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{pmatrix} = F_1$$

$$F_1P_{24}(2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -6 & 6 & -6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{pmatrix} = F_2$$

$$F_2P_{34}(6)P_{35}(-6)P_{36}(6) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -6 \end{pmatrix} = F_3$$

$$F_3P_{47} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -6 & 0 & 0 & 0 \end{pmatrix}$$

Ahora

$$Q = P_{12}(-3)P_{13}(-2)P_{15}(6)P_{24}(2)P_{34}(6)P_{35}(-6)P_{36}(6)P_{47} =$$

$$= \begin{pmatrix} 1 & -3 & -2 & 0 & 6 & -12 & -18 \\ 0 & 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & -6 & 6 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Por tanto, el núcleo de A está generado por las 3 últimas columnas de Q:

$$\begin{pmatrix} 6 & -12 & -18 \\ 0 & 0 & 2 \\ -6 & 6 & 6 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Lo hemos obtenido en 7 pasos y los resultados son más sencillos.

Finalmente,

$$\begin{pmatrix} 3b & a+3b+2c \\ a+3c & 0 \end{pmatrix} = (0_{\mathbf{Z}/6\mathbf{Z}})$$

$$\Updownarrow$$

$$(a,b,c) \in \mathbf{Z} < (6,0,-6), (-12,0,6), (-18,2,6) >$$

y hemos encontrado un sistema generador del núcleo de $\mathbf{Z}^3$ en G (véase el ejemplo de la p. 49). ¡Por cierto! el sistema generador que hemos calculado, paso a paso incluyendo operaciones elementales en las filas, es más sencillo que el entonces descrito, que había sido calculado mediante ordenador; de hecho, éste coincide con nuestro primer cálculo que obviava las operaciones elementales en las filas.

Siguiendo con el citado ejemplo, también se incluyen con cierto *descaro* matrices P y Q regulares tales que PAQ es diag $[2,6,6]$. En efecto,

Teorema 10.15 (Smith) *Si M es una matriz sobre un dominio euclídeo es posible describir matrices elementales $P_1, \ldots, P_s$, $Q_1, \ldots, Q_t$ tales que*

$$P_s \cdots P_1 M Q_1 \cdots Q_t = \text{diag}\,[d_1, \ldots, d_r, 0, \ldots, 0]$$

donde $d_1 \mid d_2 \mid \cdots \mid d_r$.

Demostración: La demostración es constructiva, utilizando la división euclídea de manera análoga a la demostración del teorema de Hermite. Esta será más complicada, en tanto en cuanto se pide algo más.

Paso 0: Colocar a la derecha y debajo de la matriz M las matrices identidad adecuadas.

Paso 1: Mediante permutación de filas y columnas, colocar en el lugar (1,1) el término no nulo de la matriz de menor norma. Si no existen términos no nulos, FIN.

Paso 2: Si $m_{11} \mid m_{1j}$, $\forall j$ hacer ceros en la primera fila. En caso contrario, sea m_{11} no divisor de m_{1j} y q el cociente de la división euclídea entre éste y aquél. Sumando a la columna j la primera multiplicada por $-q$, obtenemos en el lugar (1,j) el resto r no nulo, cuya norma es inferior al de m_{11}. Permutando las columnas 1 y j, r, ocupa el primer término de la matriz.

Paso 3: Iterar el paso 2 hasta obtener como primera fila $(m, 0, \ldots, 0)$. Esto es posible pues al ir descendiendo la norma, en el peor de los casos, llegamos a una unidad como lugar $(1, 1)$.

Paso 4: Si el nuevo $m_{11} \mid m_{k1}$, $\forall k$ hacer[3] ceros en la primera columna. En caso contrario, sea m_{11} no divisor de m_{k1} y q el cociente de la división entera entre éste y aquél. Sumando a la fila k la primera multiplicada por $-q$, obtenemos en el lugar (k,1) el resto r no nulo, cuya norma es inferior a la de a_{11}. Permutando las filas 1 y k, r, ocupa el primer término de la matriz.

Paso 4: Iterar desde el paso 2 hasta obtener la matriz

$$\begin{pmatrix} m & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & * & \cdots & * \\ 0 & * & \cdots & * \end{pmatrix}$$

Esto es posible pues al ir descendiendo la norma, en el peor de los casos, llegamos a una unidad como lugar $(1, 1)$.

Paso 5: Si no hay más filas o columnas, FIN.

Paso 6: Si m es divisor de todos los términos de la matriz, iterar desde el paso 1 en la submatriz que resulta de suprimir la primera fila y columna. Nótese que justo antes de llegar nuevamente al paso 5 obtendremos

$$\begin{pmatrix} m & 0 & \cdots & 0 \\ 0 & p & \cdots & 0 \\ \vdots & 0 & \cdots & * \\ 0 & 0 & \cdots & * \end{pmatrix}$$

Puesto que p es combinación lineal con coeficientes en el dominio de los elementos de la submatriz, y m dividía a todos ellos debe ser m un divisor de p.

Paso 7: Sea m_{jk} un término no múltiplo de m. Sumar a la fila 1 la j e iterar todo el procedimiento desde el paso 2.

Paso 8: FIN.

[3] basta colocarlos, pues los demás elementos no cambian en el proceso

Ejemplo Tomemos la matriz que hemos obtenido como sistema generador en el ejemplo anterior

$$M = \begin{pmatrix} 6 & -12 & -18 \\ 0 & 0 & 2 \\ -6 & 6 & 6 \end{pmatrix}$$

$$P_{12}MP_{13} = \begin{pmatrix} 2 & 0 & 0 \\ -18 & -12 & 6 \\ 6 & 6 & -6 \end{pmatrix} = N \quad P_{21}(9)N = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & 6 \\ 6 & 6 & -6 \end{pmatrix} = L$$

$$P_{31}(-3)L = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -12 & 6 \\ 0 & 6 & -6 \end{pmatrix} = J \quad P_{23}J = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & -6 \\ 0 & -12 & 6 \end{pmatrix} = K$$

Finalmente,

$$P_{32}(2)KQ_3(-1) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

$$P = P_{32}(2)P_{23}P_{31}(-3)P_{21}(9)P_{12} \qquad Q = P_{13}Q_3(-1)$$

El ejemplo nos ha salido muy fácil. Observe el lector el siguiente aparentemente inofensivo

Ejemplo Encontrar matrices P y Q enteras y regulares tales que

$$P\text{diag}\,[6,9]Q$$

sea diagonal.

$$P_{12}(1)\text{diag}\,[6,9] = \begin{pmatrix} 6 & 9 \\ 0 & 9 \end{pmatrix} = J \quad NP_{12}(-1) = \begin{pmatrix} 6 & 3 \\ 0 & 9 \end{pmatrix} = K$$

$$KP_{12} = \begin{pmatrix} 3 & 6 \\ 9 & 0 \end{pmatrix} = L \quad LP_{12}(-2) = \begin{pmatrix} 3 & 0 \\ 9 & -18 \end{pmatrix} = M$$

$$P_{21}(-3)M = \begin{pmatrix} 3 & 0 \\ 0 & -18 \end{pmatrix} \quad Q_2(-1)M = \begin{pmatrix} 3 & 0 \\ 0 & 18 \end{pmatrix}$$

Observación 10.16 Puede probarse que los términos de la diagonal, con esas condiciones de divisibilidad, están, salvo unidades, unívocamente determinados por M; reciben el nombre de **factores invariantes** de M. La matriz diagonal obtenida se dice forma canónica de Smith.

Todos los términos diagonales que sean unidades pueden ser transformados en 1, mediante multiplicación de las filas correspondientes por sus inversos. Asimismo, en el caso de matrices polinómicas todos los elementos diagonales no nulos pueden obtenerse mónicos, previa multiplicación por constantes no nulas.

Pasamos a justificar ahora que el grupo G del ejemplo de la página 49 es isomorfo a $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}/ \oplus \mathbf{Z}/6\mathbf{Z}$.

Teorema 10.17 (Primer teorema de estructura) *Todo grupo abeliano de tipo finito G posee un sistema generador $(b_1, \ldots, b_s)$ tal que*

$$G =< b_1 > \oplus \cdots \oplus < b_s > \quad < b_i > \cong \mathbf{Z}/d_i\mathbf{Z} \quad d_i \mid d_{i+1}$$

Demostración: Sea $(a_1, \ldots, a_n)$ un sistema generador de G y $\varphi\colon \mathbf{Z}^n \longrightarrow G$ dado por $e_i \longrightarrow a_i$. Sea A la matriz $n \times m$ coordenada de un sistema generador del núcleo; por el teorema de Smith existen matrices P y Q regulares enteras tales que

$$PAQ = \operatorname{diag}[d_1, \ldots, d_r, \overbrace{0, \ldots, 0}^{m-r}] \quad d_1 \mid \cdots \mid d_i \mid d_{i+1} \mid \cdots$$

Tómese

$$(b_1, \ldots, b_n) = (a_1, \ldots, a_n)P^{-1}$$

Es claro que la familia obtenida es un sistema generador de G. Ahora,

$$\begin{aligned}(b_1, \ldots, b_n)\operatorname{diag}[d_1, \ldots, d_r, 0, \ldots, 0] &= (b_1, \ldots, b_n)PAQ = \\ &= (a_1, \ldots, a_n)P^{-1}PAQ = (a_1, \ldots, a_n)AQ = \\ &= (0)Q = (0)\end{aligned}$$

Por tanto, $d_i b_i = 0, i = 1, \ldots, r$.

$\underline{G =< b_1 > \oplus \cdots \oplus < b_n >}$

Sea $c_i \in < b_i > \cap (\sum_{j \neq i} < b_j >)$; entonces, $z_i b_i = \sum_{j \neq i}(-z_j)b_j$, por lo que $P^{-1}(z_1, \ldots, z_n)^t \in \ker\varphi$ y $P^{-1}(z_j) = A(s_j) = AQQ^{-1}(s_j)$. Poniendo $(t_j) = Q^{-1}(s_j)$, se tiene

$$(z_j) = PAQ(t_j) = \operatorname{diag}[d_1, \ldots, d_r, 0, \ldots, 0](t_j) \Longrightarrow \begin{cases} z_i = d_i t_i \quad i = 1, \ldots, r \\ z_{r+1} = \cdots = z_n = 0 \end{cases}$$

Por tanto,

$$c_i = z_i b_i = \begin{cases} d_i t_i b_i = 0_G \quad i = 1 \ldots, r \\ 0 b_i = 0_G \quad i = r+1, \ldots, n \end{cases}$$

En conclusión

$$G =< b_1 > \oplus \cdots \oplus < b_n >$$

Por otro lado, si $d_j = 1$, $b_j = 0_G$; suprimiendo tales b_j y renumerando

$$G =< b_1 > \oplus \cdots \oplus < b_s >$$

$\underline{o(b_i) = d_i}$

Es suficiente ver que $z_i b_i = 0 \Longrightarrow d_i \mid z_i$, pero ello es caso particular del razonamiento anterior.

Observación 10.18 Ya tenemos la parte constructiva. La pregunta que se puede plantear ahora es ¿puede un grupo abeliano de tipo finito ser isomorfo a la vez a

$$\mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_r\mathbf{Z} \oplus \mathbf{Z}^m$$

y

$$\mathbf{Z}/c_1\mathbf{Z} \oplus \mathbf{Z}/c_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/c_s\mathbf{Z} \oplus \mathbf{Z}^p$$

con $c_i > 0$ y $c_1 \mid c_2 \mid \cdots \mid c_s$. Por rangos, $m + r = s + p$. Veremos que $r = s$ y que $c_i = d_i$.

Antes de afrontar este asunto de tipo *cualitativo*, veamos otra aplicación *cuantitativa* del teorema de Smith aplicado a la clásica matriz característica $xI - A$.

10.1 La forma canónica racional de un endomorfismo

Sea V un espacio vectorial de dimensión n sobre K, y h un endomorfismo de V.

Para cada polinomio $f(x) = \sum a_i x^i$ con coeficientes en K, denotemos, como es usual, $f(h)$ el endomorfismo $\sum a_i h^i$ dado por $f(h)(v) = \sum a_i h^i(v)$.

Sea A la matriz coordenada de h en cierta base (v_i). Entonces,

$$(hv_1, \ldots, hv_n) = (v_1, \ldots, v_n)A \Longrightarrow (xv_1, \ldots, xv_n) = (v_1, \ldots, v_n)A$$

$$\Updownarrow$$

$$(v_1, \ldots, v_n)xI_n = (v_1, \ldots, v_n)A \Longrightarrow (v_1, \ldots, v_n)(xI_n - A) = (0_V, \ldots, 0_V)$$

Sean P y Q matrices regulares, obtenidas por ejemplo mediante el teorema de Smith, tales que $P(xI-A)Q = \operatorname{diag}[f_1, \ldots, f_n]$. Mediante matrices elementales de tipo 1 podemos conseguir $f_{i+1} \mid f_i$. Sea $(w_1, \ldots, w_n) = (v_1, \ldots, v_n)P^{-1}$. Entonces,

$$\begin{aligned}
(w_1, \ldots, w_n)\operatorname{diag}[f_1, \ldots, f_n] &= (w_1, \ldots, w_n)P(xI - A)Q = \\
&= (v_1, \ldots, v_n)P^{-1}P(xI - A)Q = \\
&= (v_1, \ldots, v_n)(xI - A)Q = (0_V, \ldots, 0_V)Q = \\
&= (0_V, \ldots, 0_V)
\end{aligned}$$

Notemos que

$$f_1 \cdots f_n = \det(P)\det(xI - A)\det Q = x^n + \cdots$$

Luego todos los f_i son no nulos. Sean $f_{s+1} = 1 = \cdots = f_n$. Entonces, $(w_{s+1}, \ldots, w_n) = (0_V, \ldots, 0_V)$. Sea $m_i = \mathrm{gr} f_i$; nótese que

$$m_1 + \cdots + m_s = \mathrm{gr} f_1 \cdots f_s = \mathrm{gr}\det(P(xI - A)Q) = n$$

Se tiene

Teorema 10.19 (Frobenius) *Con la notación anterior,*

i) *La familia* $B = (w_1, hw_1, \ldots, h^{m_1-1}w_1, \ldots, w_s, hw_s, \ldots, h^{m_s-1}w_s)$ *es una base de* V.

ii) *El polinomio mínimo de* w_i *es* f_i.

iii) *Los subespacios* $S_i = K < w_i, hw_i, \ldots, h^{m_i-1}w_i >$ *son* h*-invariantes.*

iv) *La matriz coordenada de* h *en dicha base es*

$$\mathrm{diag}\,[C(f_1), \ldots, C(f_s)]$$

la forma canónica racional de h *(y de* A*)*

v) *Los polinomios* $(f_1 \ldots, f_r)$ *son los factores invariantes de* A

Demostración:

i) Contando vectores se tiene un total de $m_1 + \cdots + m_s = n$. Es suficiente ver que son un sistema generador de V. Al efecto, cada vector de la base inicial v_i cumple

$$v_i = (w_1, \ldots, w_s, 0_V, \ldots, 0_V)P^i$$

por lo que existen polinomios[4] $g_1, \ldots, g_s$ tales que $v_i = g_1 w_1 + \cdots + g_s w_s$.

Dividiendo g_i entre f_i,

$$g_i w_i = (q_i f_i + r_i)w_i = r_i w_i = \sum_{j=0}^{m_i-1} \mu_j h^j w_i$$

Por tanto, la base de V es c.l. de B.

ii) Puesto que $f_i w_i = 0_V$ es suficiente ver que si p es de grado inferior a f_i, $pw_i \neq 0$, y esto es consecuencia de que la familia $(w_i, hw_i, \ldots, h^{m_i-1}w_i)$ es parte de una base, luego libre.

iii) En efecto, sea $f_i = x^{m_i} + \sum_{j=0}^{m_i-1} \lambda_j x^j$. Entonces,

$$f_i w_i = 0_V \Longrightarrow h^{m_i}(w_i) = \sum_{j=0}^{m_i-1} (-\lambda_j) h^j w_i \in S_i$$

iv) Veremos que la m.c. del endomorfismo restricción a S_i es $C(f_i)$. Ahora bien, es obvio que las $m_i - 1$ primeras columnas son las de $C(f_i)$; para la última, basta observar el argumento anterior.

[4] los s primeros de la columna i-sima de P

v) Es consecuencia de iv).

Ejemplo Sea h el endomorfismo de un espacio vectorial V, que en cierta base (v_i) tiene por matriz coordenada $A = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$. Entonces, tomando

$$P = \begin{pmatrix} x-1 & 2 \\ -1/2 & 0 \end{pmatrix} \quad Q = \begin{pmatrix} 1 & 0 \\ -1/2 + 1/2\,x & 1 \end{pmatrix}$$

$$PAQ = \begin{pmatrix} x^2 - 2x - 5 & 0 \\ 0 & 1 \end{pmatrix}$$

Por tanto, la forma racional de h es

$$F = \begin{pmatrix} 0 & 5 \\ 1 & 2 \end{pmatrix}$$

Ahora

$$P^{-1} = \begin{pmatrix} 0 & -2 \\ 1/2 & x-1 \end{pmatrix} \Longrightarrow (w_1, w_2) = (v_1, v_2)P^{-1} = (1/2\,v_2, 0_V)$$

y la base asociada a la forma racional es $(1/2\,v_2, h(1/2\,v_2))$. Puede terminar los cálculos el lector.

EJERCICIOS

1. Probar que si F es libre con n generadores su rango es $m \leq n$.
2. Sea G un grupo abeliano libre. Probar que son equivalentes:
   (a) P es regular sobre $\mathbf{Z}$
   (b) Para cada base (v_i) de G, $(w_i) = (v_i)P$ es base de G.
   (c) Existe una base (v_i) de G tal que $(w_i) = (v_i)P$ es base de G.
3. Encontrar una base en el subgrupo de $\mathbf{Z}^3$ generado por
$$(1, 0, -1), (2, -3, 1), (0, 3, 1), (3, 1, 5)$$
4. Encontrar una base en el subgrupo de $\mathbf{Z}^3$
$$\{(x_i) \mid x_1 + 2x_2 + 3x_3 = 0, x_1 + 4x_2 + 9x_3 = 0\}$$
5. Dada la matriz
$$M = \begin{pmatrix} 2x-1 & x & x+1 \\ x & x & x^2 \\ x^2+3 & x^2 & 2x^2-3 \end{pmatrix}$$
encontra P y Q regulares tales que PMQ es la forma noermal de Smith de M.
6. Probar que la relación en $M_{m\times n}(\mathcal{D})$
$$M \sim N \iff PMQ = N, P \in GL(m, \mathcal{D}), Q \in GL(n, \mathcal{D})$$
es de equivalencia.
7. Probar que toda matriz regular sobre un dominio euclídeo es producto de matrices elementales tipo 1 y 2.
8. Probar que la forma canónica de Smith de una matriz sobre un cuerpo es $[I_r, 0]$ donde r es su rango.
9. Probar que una matriz de determinante 1 sobre un cuerpo K es producto de matrices elementales tipo 2.
10. Dado el subgrupo S de $\mathbf{Z}^3$ generado por
$$(2, 1, -3), (1, -1, 2)$$
describir el grupo cociente $\mathbf{Z}^3/S$ como suma directa de grupos cíclicos y/o monógenos, ordenados completamente sus órdenes por divisibilidad.