11 El subgrupo de torsión. Teorema de invariancia

La descomposición de un grupo abeliano de tipo finito en suma directa de subgrupos cíclicos y/o monógenos no es única. De hecho,

$$\mathbf{Z}^2 =< (1,0) > \oplus < (0,1) >=< (1,2) > \oplus < (3,5) >$$

En general, si (v_i) y (w_i) son bases de $\mathcal{S}$,

$$\mathcal{S} =< v_1 > \oplus \cdots \oplus < v_n >=< w_1 > \oplus \cdots \oplus < w_n >$$

Notemos que un cambio de base viene dado por una matriz P regular, por lo que es viable la exposición de múltiples descomposiciones de un grupo abeliano libre en suma directa de cíclicos y/o monógenos. Sin embargo, el número de sumandos y los órdenes de los generadores en cada descomposición permanecerán invariantes.

Antes de abordar este resultado de invariancia descompondremos cada grupo abeliano de tipo finito en su parte finita y su parte libre. Comencemos por la parte finita,

Definición 11.1 *Un elemento x de un grupo abeliano se dice de torsión si $o(x)$ es finito.*

Proposición 11.2 *El conjunto de elementos de torsión*[1] *de un grupo abeliano G es un subgrupo que se dice subgrupo de torsión de G. Se escribe G_T.*

Demostración: $o(x) = n, o(y) = m \Longrightarrow mn(x+y) = 0_G$. Puesto que un elemento y su opuesto tienen el mismo orden, hemos terminado.

Observación 11.3 Por el teorema de Lagrange, si G es finito $G = G_T$. En general, se tiene

Proposición 11.4 *Todo grupo abeliano de tipo finito es suma directa de su subgrupo de torsión y un subgrupo libre.*

Demostración: Sea $G =< b_1 > \oplus \cdots \oplus < b_r >$ con $< b_i >\cong \mathbf{Z}/d_i\mathbf{Z}$, $d_i \mid d_{i+1}$. Sean $d_s \neq 0 = d_{s+1}$. Entonces,

$$< b_{s+1} > \oplus \cdots \oplus < b_r >\cong \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$$

que es libre.

Veamos que $< b_1 > \oplus \cdots \oplus < b_s >$ es el subgrupo de torsión. Es claro, que los $b_i, i < s$ son elementos de torsión y se tiene la inclusión " $\subseteq$ ". Recíprocamente, sea x un elemento de torsión; su orden será $z \neq 0$ y

$$x = \sum_{i=1}^{r} z_i b_i \in G_T \Longrightarrow \sum_{i=1}^{r} z z_i b_i = 0_G \Longrightarrow z z_i b_i = 0_G \forall i \Longrightarrow d_i \mid z z_i \, \forall i$$

[1] incluido el cero

$$\Longrightarrow 0 \mid zz_i \,\forall i > s \Longrightarrow zz_i = 0 \,\forall i > s \Longrightarrow z_i = 0 \,\forall i > s$$

Así,

$$x = \sum_{i=1}^{s} z_i b_i \in < b_1 > \oplus \cdots \oplus < b_s >$$

Observación 11.5 Notemos que el subgrupo de torsión es finito. Dado un primo p sabemos que cada grupo abeliano finito posee un único p-Sylow P. Por tanto, la teoría de Sylow nos indica que

$$G_T = P_1 \oplus \cdots \oplus P_r$$

donde $p_1, \cdots, p_r$ son los diferentes primos divisores de $|G_T|$.

Siguiendo las ideas con las que comienza esta observación podemos demostrar el siguiente

Teorema 11.6 (Segundo teorema de estructura) *Todo grupo abeliano de tipo finito es suma directa de un número finito de subgrupos monógenos y/o cíclicos, éstos de orden potencia de primo.*

Demostración: Sea $G =< b_1 > \oplus \cdots \oplus < b_r >$ con $< b_i > \cong \mathbf{Z}/d_i\mathbf{Z}$, $d_i \mid d_{i+1}$. Sean $d_s \neq 0 = d_{s+1}$. Para $i \leq s$, $< b_i >$ es un grupo abeliano que será suma directa de sus p-subgrupos de Sylow; ahora bien, los subgrupos de un cíclico son cíclicos luego

$$< b_i >=< b_{i1} > \oplus \cdots \oplus < b_{in_i} >$$

Por tanto,

$G =$

$$(< b_{11} > \oplus \cdots \oplus < b_{1n_1} >) \oplus \cdots \oplus (< b_{s1} > \oplus \cdots \oplus < b_{sn_s} >) \oplus < b_{s+1} > \oplus \cdots \oplus < b_r >$$

Observación 11.7 Notemos las hipótesis; de hecho $\mathbf{Q}$, al ser libre de torsión, no puede tener subgrupos cíclicos, y al no ser libre no puede ser suma directa de monógenos (copias de $\mathbf{Z}$).

Ejemplo Sea

$$G = \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_2\mathbf{Z} \oplus \mathbf{Z}/d_3\mathbf{Z} \qquad d_1 = 17364375 \quad d_2 = 4725 \quad d_3 = 9$$

Ahora

$$d_1 = 17364375 = 3^4 5^4 7^3 \quad d_2 = 4725 = 3^3 5^2 7 \quad d_3 = 9 = 3^2$$

Luego

$$\mathbf{Z}/d_1\mathbf{Z} \cong \mathbf{Z}/3^4\mathbf{Z} \oplus \mathbf{Z}/5^4\mathbf{Z} \oplus \mathbf{Z}/7^3\mathbf{Z} \quad \mathbf{Z}/d_2\mathbf{Z} \cong \mathbf{Z}/3^3\mathbf{Z} \oplus \mathbf{Z}/5^2\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z} \quad \mathbf{Z}/d_3\mathbf{Z} \cong \mathbf{Z}/3^2\mathbf{Z}$$

y

$$G \cong \mathbf{Z}/3^4\mathbf{Z} \oplus \mathbf{Z}/5^4\mathbf{Z} \oplus \mathbf{Z}/7^3\mathbf{Z} \oplus \mathbf{Z}/3^3\mathbf{Z} \oplus \mathbf{Z}/5^2\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z}/3^2\mathbf{Z}$$

Observación 11.8 Teniendo en cuenta que

$$(m,n)=1 \Longrightarrow \mathbf{Z}/m\mathbf{Z}\oplus\mathbf{Z}/n\mathbf{Z}=\mathbf{Z}/(mn)\mathbf{Z}$$

la descomposición del segundo teorema de estructura permite recuperar la del primero. Por ejemplo, sea

$$G=\mathbf{Z}/3\mathbf{Z}\oplus\mathbf{Z}/3^2\mathbf{Z}\oplus\mathbf{Z}/7^3\mathbf{Z}\oplus\mathbf{Z}/7^3\mathbf{Z}\oplus\mathbf{Z}/5^2\mathbf{Z}\oplus\mathbf{Z}/7\mathbf{Z}\oplus\mathbf{Z}/3^2\mathbf{Z}$$

Entonces, la sucesión de potencias de primos es

$$\begin{array}{l}3,3^2,3^2\\7,7^3,7^3\\5^2\end{array}$$

Siguiendo un proceso análogo al del cálculo del mcm, tomamos

$$3^2 7^3 5^2=77175 \quad 3^2 7^3=3087 \quad 3.7=21 \Longrightarrow G\cong\mathbf{Z}/21\mathbf{Z}\oplus\mathbf{Z}/3087\mathbf{Z}\oplus\mathbf{Z}/77175\mathbf{Z}$$

Observación 11.9 Este sencillo hecho nos permite observar que la unicidad de la descomposición en el primer teorema de estructura está intrínsecamente relacionada con la del segundo.

La idea de la unicidad es muy simple. Hemos visto que un grupo abeliano es

$$G=G_T\oplus F$$

donde G_T es el subgrupo (finito) de los elementos de orden finito y F es un subgrupo libre, que será o 0_G o infinito. De esta parte infinita poco o mucho[2] se puede decir; la dimensión es un invariante y, por tanto, F es una suma directa finita de m copias de $\mathbf{Z}$, siendo m fijo.

Vayamos con la parte finita G_T. Se trata de la suma directa de subgrupos cíclicos de órdenes d_i. Descomponiendo su orden en factores primos

$$p_1^{m_1},\ldots,p_r^{m_r}$$

las posibilidades para descomponer G_T en suma directa de subgrupos cíclicos de órdenes potencia de primo partirán de la contemplación de la siguiente tabla

$p_1^{m_1}$	$p_1^{m_1-1}p_1$	$p_1^{m_1-2}p_1^2$	$p_1^{m_1-2}p_1p_1$	$\cdots$	$p_1\cdots p_1$
$p_2^{m_2}$	$p_2^{m_2-1}p_2$	$p_2^{m_2-2}p_2^2$	$p_2^{m_2-2}p_2p_2$	$\cdots$	$p_2\cdots p_2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$p_r^{m_r}$	$p_r^{m_r-1}p_r$	$p_r^{m_1-2}p_r^2$	$p_r^{m_1-2}p_rp_r$	$\cdots$	$p_r\cdots p_r$

Construir una tabla, a partir de la anterior, reemplazando cada casilla $p_i^{n_{i_1}}\cdots p_i^{n_{i_s}}$ por el grupo $C_{p_i^{n_{i_1}}}\oplus\cdots\oplus C_{p_i^{n_{i_s}}}$; seleccionando un grupo de cada fila y columna,

[2] depende de la visión personal

escríbase la suma directa de grupos cíclicos correspondientes. Tendremos todas las posibilidades para el segundo teorema de estructura.

Ejemplo Sea G un grupo abeliano de orden $2^4 3^5 7^3$. Entonces,

$\mathbf{2^4}$	$2^3.2$	$2^2.2^2$	$2^2.2.2$	2.2.2.2		
3^5	$3^4.3$	$3^3.3^2$	$\mathbf{3^3.3.3}$	$3^2.3^2.3$	$3^2.3.3.3$	3.3.3.3.3
7^3	$\mathbf{7^2.7}$	7.7.7				

que da lugar a 105 grupos abelianos de orden $2^4 3^5 7^3$. Seleccionando, por ejemplo, las casillas resaltadas 1,4 y 2

$$C_{2^4} \oplus C_{3^3} \oplus C_3 \oplus C_3 \oplus C_{7^2} \oplus C_7$$

Para obtener la descomposición del primer teorema de estructura, en este ejemplo, se actúa de la siguiente manera: Reagrupamos todos los primos elevados a su máximo exponente: $2^4, 3^3, 7^2$, lo que da lugar al grupo C_{21168}; iterando en la sucesión de primos restante obtenemos $3, 7$, es decir, el grupo C_{21}. Finalmente, queda C_3. Es decir,

$$C_{2^4} \oplus C_{3^3} \oplus C_3 \oplus C_3 \oplus C_{7^2} \oplus C_7 = C_{21168} \oplus C_{21} \oplus C_3$$

Antes de seguir conviene que el lector aplique esta técnica a los grupos abelianos de orden bajo, (≤ 20 por ejemplo).

Comencemos a sistematizar estas ideas comenzando por los casos más concretos, que serán necesarios en el caso general.

El caso más simple estructuralmente, el de un p-grupo abeliano utiliza el hecho de que $\mathbf{Z}/p\mathbf{Z}$ es un cuerpo y podremos construir un espacio vectorial de dimensión finita al que aplicar los conocidos resultados del álgebra lineal.

Proposición 11.10 *Sea G un p-grupo abeliano tal que,*

$$G = < b_1 > \oplus \cdots \oplus < b_r > = < c_1 > \oplus \cdots \oplus < c_s >$$

con

$$< b_i > \cong \mathbf{Z}/d_i\mathbf{Z} \quad 1 \neq d_1 \mid \ldots \mid d_i \mid \ldots \mid d_r$$
$$< c_j > \cong \mathbf{Z}/e_j\mathbf{Z} \quad 1 \neq e_1 \mid \ldots \mid e_j \mid \ldots \mid e_s$$

Entonces,

$$r = s \quad \text{y} \quad d_i = e_i, i = 1 \ldots, r$$

Demostración:

$$p^\alpha = |G| = d_1 \cdots d_r = e_1 \cdots e_s \Longrightarrow d_i = p^{\alpha_i}, e_j = p^{\beta_j} \Longrightarrow \sum \alpha_i = \sum \beta_j$$

Ahora las relaciones de divisibilidad dan

$$\alpha_1 \leq \ldots \leq \alpha_r \quad \beta_1 \leq \ldots \leq \beta_s$$

Probaremos que $r = s$ y que $\alpha_i = \beta_i, \forall i$.

Al efecto, consideremos los subgrupos de G

$$p^k G = \{p^k x \mid x \in G\} \quad k \in \mathbf{N}$$

Es claro que $p^{k+1}G \subseteq p^k G$ y la operación $(z+p\mathbf{Z}, \overline{x}) \longrightarrow \overline{zx}$ convierte a $p^k G/p^{k+1}G$ en un $\mathbf{Z}/p\mathbf{Z}$-espacio vectorial; lo único complicado es comprobar que se trata efectivamente de una operación; al efecto,

$$(z + p\mathbf{Z}, \overline{x}) = (u + p\mathbf{Z}, \overline{y}) \Longrightarrow p \mid u - z, y - x = p^{k+1}v \Longrightarrow yu = xz + p^{k+1}w$$

Ahora, sea $\alpha_{m-1} \leq k < \alpha_m$. Entonces,

$$p^k G/p^{k+1}G = \mathbf{Z}/p\mathbf{Z} < \overline{p^k b_1}, \ldots, \overline{p^k b_r} >= \mathbf{Z}/p\mathbf{Z} < \overline{p^k b_m}, \ldots, \overline{p^k b_r} >$$

Puesto que

$$\begin{aligned} \sum_{i=m}^{r} \overline{z_i}\overline{p^k b_i} = 0 \quad &\Longrightarrow \quad \sum_{i=m}^{r} z_i p^k b_i \in p^{k+1}G \Longrightarrow \sum_{i=m}^{r} z_i p^k b_i = p^{k+1} \sum_{i=m}^{r} u_i b_i \Longrightarrow \\ &\Longrightarrow \quad z_i p^k b_i = p^{k+1} u_i b_i \Longrightarrow p^{\alpha_i} \mid z_i p^k - p^{k+1} u_i \Longrightarrow \\ &\Longrightarrow \quad p \mid p^{\alpha_i - k} \mid z_i - p u_i \Longrightarrow p \mid z_i \Longrightarrow \overline{z_i} = 0, i = m, \ldots, r \end{aligned}$$

estamos ante una base y

$$\alpha_{m-1} \leq k < \alpha_m \Longrightarrow \dim_{\mathbf{Z}/p\mathbf{Z}}(p^k G/p^{k+1}G) = r - m + 1$$

Análogamente,

$$\beta_{n-1} \leq k < \beta_n \Longrightarrow \dim_{\mathbf{Z}/p\mathbf{Z}}(p^k G/p^{k+1}G) = s - n + 1$$

Es decir,

$$\#\{i \mid k < \alpha_i\} = \dim_{\mathbf{Z}/p\mathbf{Z}}(p^k G/p^{k+1}G) = \#\{j \mid k < \beta_j\}$$

Tomando $k = 0$, se tiene $r = s$. Por ejemplo, con $p = 5$, concrete el lector la imposibilidad de

$$C_{5^2} \oplus C_{5^2} = C_{5^4}$$

Si existiera un índice j con $\beta_j < \alpha_j$, tomando $k = \beta_j$ se obtendría una contradicción. Por ejemplo, con $p = 5$ y $k = 2$, concrete el lector la imposibilidad de

$$C_{5^3} \oplus C_{5^3} = C_{5^2} \oplus C_{5^4}$$

Avancemos un paso más y consideremos el caso finito $G = G_T$.

La técnica de la demostración es simple. Veremos que

$$G \cong C_2 \oplus C_2 \oplus C_6 \cong C_2 \oplus C_{12} \Longrightarrow \exp(G) = 6, 12$$

lo que es imposible; por tanto, concluiremos que el último factor invariante debe coincidir.

$$G \cong C_2 \oplus C_6 \oplus C_{12} \cong C_{12} \oplus C_{12} \Longrightarrow \mathrm{Syl}_2(G) \cong C_2 \oplus C_2 \oplus C_4 \cong C_4 \oplus C_4$$

que contradice el resultado anterior, para un 2-grupo; por tanto, concluiremos que el número de sumandos debe coincidir.

$$G \cong C_6 \oplus C_6 \oplus C_{36} \cong C_2 \cong C_{18} \oplus C_{36} \Longrightarrow \mathrm{Syl}_3(G) \cong C_3 \oplus C_3 \oplus C_9 \cong C_9 \oplus C_9$$

que contradice también el resultado anterior, para un 3-grupo; por tanto, concluiremos que cada factor invariante debe coincidir.

Proposición 11.11 *Sea G un grupo abeliano finito tal que,*

$$G =< b_1 > \oplus \cdots \oplus < b_r >=< c_1 > \oplus \cdots \oplus < c_s >$$

con

$$< b_i > \cong \mathbf{Z}/d_i\mathbf{Z} \quad 1 \neq d_1 \mid \ldots \mid d_i \mid \ldots \mid d_r$$
$$< c_j > \cong \mathbf{Z}/e_j\mathbf{Z} \quad 1 \neq e_1 \mid \ldots \mid e_j \mid \ldots \mid e_s$$

Entonces,

$$r = s \quad \text{y} \quad d_i = e_i, i = 1 \ldots, r$$

Demostración: En primer lugar, $d_r = \mathrm{mcm}(o(x) \mid x \in G) = e_s$.

Sean pues $p_1, \ldots, p_n$ los primos divisores de d_r y pongamos

$$d_i = p_1^{\alpha_{i1}} \cdots p_n^{\alpha_{in}} \qquad e_j = p_1^{\beta_{j1}} \cdots p_n^{\beta_{jn}}$$

Cada sumando cíclico es suma directa de sus subgrupos de Sylow

$$< b_i >=< b_{i1} > \oplus \cdots \oplus < b_{in} > \quad < c_j >=< c_{j1} > \oplus \cdots \oplus < c_{jn} >$$

Si $r > s$, sea p_k un divisor primo de d_1. Entonces,

$$< b_{1k} > \oplus \cdots \oplus < b_{rk} > \quad \text{y} \quad < \mathrm{c_{1k}} > \oplus \cdots \oplus < \mathrm{c_{sk}} >$$

son p_k- Sylows de G. Puesto que G es abeliano, sólo hay un p_k-Sylow, y

$$< b_{1k} > \oplus \cdots \oplus < b_{rk} >=< c_{1k} > \oplus \cdots \oplus < c_{sk} >$$

La descomposición de la izquierda tiene r sumandos y la de la derecha, a lo sumo, s, lo que contradice el resultado anterior; por tanto $r \leq s$ y por simetría $r = s$.

Una vez más, el teorema anterior aplicado a cada p_k-Sylow, $k = 1, \ldots, n$, da

$$< b_{1k} > \oplus \cdots \oplus < b_{rk} > = < c_{1k} > \oplus \cdots \oplus < c_{rk} >$$

$$\Downarrow$$

$$p_k^{\alpha_{ik}} = p_k^{\beta_{ik}}, i = 1, \ldots, r, k = 1, \ldots, n \Longrightarrow e_i = d_i,\ i = 1, \ldots, r$$

Ya podemos pasar a enunciar y probar la unicidad de la descomposición del primer teorema de estructura.

Teorema 11.12 *Sea un grupo abeliano tal que*

$$G = < b_1 > \oplus \cdots \oplus < b_m > = < c_1 > \oplus \cdots \oplus < c_n >$$

con

$$< b_i > \cong \mathbf{Z}/d_i\mathbf{Z} \quad 1 \neq d_1 \mid \ldots \mid d_i \mid \ldots \mid d_m$$
$$< c_j > \cong \mathbf{Z}/e_j\mathbf{Z} \quad 1 \neq e_1 \mid \ldots \mid e_j \mid \ldots \mid e_n$$

Entonces,

$$m = n \quad \text{y} \quad d_i = e_i,\ i = 1 \ldots, m$$

Demostración: Sean $d_r \neq 0 = d_{r+1}, e_s \neq 0 = e_{s+1}$ entonces,

$$< b_{r+1} > \oplus \cdots \oplus < b_m > \cong G/G_T \cong < c_{s+1} > \oplus \cdots \oplus < c_n >$$

son grupos abelianos libres isomorfos de dimensiones $m - r$ y $n - s$. Por tanto, $m - r = n - s$.

Ahora,

$$< b_1 > \oplus \cdots \oplus < b_r > = G_T = < c_1 > \oplus \cdots \oplus < c_s >$$

Y basta aplicar el resultado anterior para obtener $r = s$, $d_i = e_i$. Finalmente, $m = n$.

Ejemplo Describir todos los grupos abelianos de orden 2250. Descomponiendo en factores primos $2250 = 2.3^2.5^3$, construimos las tablas

2		
3^2	3.3	
5^3	$5^2.5$	5.5.5

C_2		
C_9	$C_3 \oplus C_3$	
C_{125}	$C_{25} \oplus C_5$	$C_5 \oplus C_5 \oplus C_5$

Seleccionando un grupo cíclico de cada fila y columna, y reagrupando primos se obtienen los 6 grupos

$$C_2 \oplus C_9 \oplus C_{125} = C_{2250}$$
$$C_2 \oplus C_3 \oplus C_3 \oplus C_{125} = C_{750} \oplus C_3$$
$$C_2 \oplus C_9 \oplus C_{25} \oplus C_5 = C_{450} \oplus C_5$$
$$C_2 \oplus C_3 \oplus C_3 \oplus C_{25} \oplus C_5 = C_{150} \oplus C_{15}$$
$$C_2 \oplus C_9 \oplus C_5 \oplus C_5 \oplus C_5 = C_{90} \oplus C_5 \oplus C_5$$
$$C_2 \oplus C_3 \oplus C_3 \oplus C_5 \oplus C_5 \oplus C_5 = C_{30} \oplus C_{15} \oplus C_5$$

EJERCICIO

1. Describir todos los grupos abelianos de orden 360.
2. Sea $G =< b >$ un grupo cíclico de orden $d = \prod_{i=1}^{r} p_i^{m_i}$. Encontrar $(b_1, \ldots, b_r)$ tales que
$$G = \bigoplus_{i=1}^{r} < b_i > \quad o(b_i) = p_i^{m_i}$$