Grupos finitos

Notas de clase de
Eugenio Miranda Palacios
para el curso 2010/2011
Adaptadas por Manuel Bullejos
para el curso 2020/2021

Índice

6. Clasificación de grupos abelianos

Si G es un grupo abeliano todos sus subgrupos son normales y por tanto para cada primo p que divida a su orden existe un único p-subgrupo de Sylow y por el teorema 5.28 tenemos:

Teorema 6.1. *Si G es un grupo de orden n y la factorización de n como producto de primos distintos es $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ entonces G es el producto directo de sus p_i-subgrupos de Sylow.*

$$G = P_{p_1} P_{p_2} \cdots P_{p_r}, \text{ directo.}$$

Además esta descomposición de G como producto directo de p-grupos es única salvo orden y es llamada Descomposición Cíclica Primaria de G.

Como consecuencia tenemos que para clasificar los grupos abelianos finitos basta con que clasifiquemos los p-grupos abelianos. Abordamos esto en el teorema de estructura de p-grupos abelianos. Para demostrar este teorema necesitamos una definición y algunos resultados previos.

Definición 6.2. Diremos que un p-grupo es elemental si todos sus elementos cumplen la ecuación $x^p = 1$.

Notar que una suma directa de grupos cíclicos es un p-grupo elemental si, y sólo, si todos los grupos son isomorfos a C_p.

Lema 6.3. *Si P es un p-grupo abeliano elemental, entonces para todo $x \in P$ existe un subgrupo $M \leq P$ tal que $P =< x > M$ como producto directo.*

Demostración. Si $x = 1$, tomamos $H = P$.

Supongamos $x \neq 1$, por ser $x^p = 1$, tenemos que $|x| = p$. Consideremos el conjunto

$$\Sigma = \{K \leq P;\, x \notin K\},$$

claramente $1 \in \Sigma$ y por tanto $\Sigma \neq \emptyset$. Sea $H \in \Sigma$ un elemento maximal, veamos que $P =< x > H$ cómo producto directo.

La intersección $< x > \bigcap H$ es un subgrupo de $< x >$, que tiene orden p y por tanto es el total o es trivial, pero cómo $x \notin H$ tenemos que $< x > \bigcap H = 1$.

Para probar que $< x > H = P$ veamos que los dos grupos tienen el mismo orden. Por ser $< x > \bigcap H = 1$ tenemos que $| < x > H| = |x|\,|H| = p|H|$. Para ver que $| < x > H| = |P|$ basta entonces con probar que $[P : H] = p$. Para ello veamos que el grupo cociente P/H está generado por xH, que claramente es un elemento de orden p, de nuevo por ser $< x > \bigcap H = 1$. Entonces $P/H =< xH >$ y tendríamos $[P : H] = |P/H| = |xH| = p$.

Sea $y \in P$ un elemento que no esté en H, entonces H es un subgrupo propio de $< y > H$. Por el carácter máximal de H, tenemos que $x \in < y > H$. Por lo que debe de existir $i < p$ talque $x \in y^i H$, tomando u el inverso de i módulo p, tenemos $x^u \in y^{iu} H = yH$ y por tanto $yH = x^u H \in < xH >$ y tenemos $P/H = xH >$.

Concluimos entonces que $P =< x > H$ cómo producto directo.

□

Como corolario inmediato tenemos:

Corolario 6.4. *Todo p-grupo abeliano elemental es suma directa de grupos cíclicos de orden p.*

Definición 6.5. Dado un entero positivo n una partición de n es una sucesión no decreciente de enteros positivos $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_r$ tal que $\alpha_1 + \alpha_2 + \ldots \alpha_r = n$.

Por ejemplo las particiones de 5 serían

$$\begin{array}{lllll} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & \\ 1 & 1 & 3 & & \\ 1 & 2 & 2 & & \\ 1 & 4 & & & \\ 2 & 3 & & & \\ 5 & & & & \end{array}$$

así que el número de particiones de 5 sería 7.

Teorema 6.6 (De clasificación o estructura de p grupos finitos)**.** *Si P es un p-grupo abeliano finito de orden p^e existe una única partición $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_r$ de e tal que*

$$P \cong C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \ldots \oplus C_{p^{\alpha_r}}.$$

De manera que el número de p-grupos abelianos de orden p^e, salvo isomorfismo, coincide con el número de particiones de e.

Demostración.

Probemos primero la existencia.

Por inducción sobre e.

Si $e = 1$, $P \cong C_p$ y la partición es 1.

Suponemos el teorema cierto para exponentes menores que e y lo demostramos para e.

Consideremos el endomorfismo de grupos

$$\varphi : P \to P\,;\, \varphi(x) := x^p$$

y llámenos

$$K = \ker(\varphi) \quad \text{y} \quad H = \mathrm{Im}(\varphi)$$

Claramente K y P/H son p-grupos elementales. Además, por el teorema de Cauchy, existe $x \in P$ de orden p y por tanto $K \neq 1$, además

$$H = \mathrm{Im}(\varphi) \cong P/\ker(\varphi) = P/K$$

y por tanto

$$\frac{P}{H} \cong \frac{P}{\frac{P}{K}} \cong K,$$

por lo que P/H no es trivial y, por tanto, H es un subgrupo propio de P que tendrá orden p^m para algún $m < e$.

Aplicando hipótesis de inducción, existirá una partición de m, $\gamma_1 \geq \gamma_2 \geq \ldots \geq \gamma_s$ tal que

$$H \cong C_{p^{\gamma_1}} \oplus C_{p^{\gamma_2}} \oplus \ldots \oplus C_{p^{\gamma_s}}.$$

Hagamos interna la suma directa anterior, para ello elegimos $h_i \in H, i = 1, \ldots, s$, tales que $C_{p^{\gamma_i}} \cong < h_i >$ y $H =< h_1 > \ldots < h_s >$ como producto interno.

Cómo $h_i \in H = \mathrm{Im}(\varphi)$ existen $x_i \in P$ tales que $h_i = x_i^p$, $i = 1, \ldots, s$.

Notemos que el orden de h_i es p^{γ_i} y por tanto el orden de x_i es p^{γ_i+1}.

Tomemos $P_0 =< x_1, \ldots, x_s >$. Vamos a demostrar los siguientes resultados:

i.- $P_0 =< x_1 >< x_2 > \ldots < x_s >$ es un producto directo. Como consecuencia

$$|P_0| = |x_1||x_2| \ldots |x_s| = p^{\gamma_1+1} \ldots p^{\gamma_s+1} = p^{m+s}$$

ii.- $H \leq P_0$ y el cociente $P_0/H =< x_1H >< x_2H > \ldots < x_sH >$ es un producto directo que además es un p-grupo elemental de orden p^s.

iii.- $K \bigcap H =< h_1^{p^{\gamma_1-1}} > \ldots < h_s^{p^{\gamma_s-1}} >$ es un producto directo y por tanto es un p-grupo elemental de orden p^s.

Demostración.

[**Demostración de i.-**] Claramente $P_0 =< x_1, \ldots, x_s >=< x_1 >< x_2 > \ldots < x_s >$, por lo que, para ver que el producto es directo basta con que demostremos que

$$< x_i > \bigcap < x_1 >< x_2 > \ldots < x_{i-1} >= 1, i = 2, \ldots, n.$$

Lo hacemos por inducción sobre i, para $i = 2$ veamos que $< x_2 > \bigcap < x_1 >= 1$. Si $x \in < x_2 > \bigcap < x_1 >$ es no trivial, podemos poner $x = x_1^a = x_2^b$, entonces $x^p = h_1^a = h_2^b \in < h_2 > \bigcap < h_1 >= 1$ por tanto $x^p = 1$ y el orden de x sería p pero

$$|x| = \frac{|x_1|}{mcd(|x_1|, a)} = \frac{p^{\gamma_1+1}}{mcd(\gamma_1 + 1, a)} = p$$
$$|x| = \frac{|x_1|}{mcd(|x_2|, b)} = \frac{p^{\gamma_2+1}}{mcd(\gamma_2 + 1, b)} = p$$

Así $mcd(\gamma_1 + 1, a) = p^{\gamma_1}$ y $mcd(\gamma_2 + 1, b) = p^{\gamma_2}$ y podemos escribir

$$x = x_1^{p^{\gamma_1} a'} = h_1^{p^{(\gamma_1-1)} a'}$$
$$x = x_2^{p^{\gamma_2} b'} = h_2^{p^{(\gamma_2-1)} b'}$$

por lo que $x \in < h_2 > \bigcup < h_1 >= 1$.

Supongamos $< x_j > \bigcap < x_1 >< x_2 > \ldots < x_{j-1} >= 1$ para $j \leq i$ y veamos que también es cierto para $i+1$. Tenemos entonces que $< x_1, \ldots, x_i >=< x_1 > \cdots < x_i >$ es un producto directo, entonces si $x \in < x_1 > \cdots < x_i > \bigcap < x_{i+1} >$ tenemos que

$$x = x_1^{a_1} \ldots x_i^{a_i} = x_{i+1}^{a_{I+1}},$$

elevamos a p y tenemos

$$x^p = h_1^{a_1} \ldots h_i^{a_i} = h_{i+1}^{a_{i+1}} \in < h_1 > \cdots < h_i > \bigcap < h_{i+1} >$$

y ha de ser (por ser este producto directo) $h_1^{a_1} = \ldots = h_i^{a_i} = h_{i+1}^{a_{i+1}} = 1$. Razonando igual que antes, los a_j han de ser múltiplos de $p_j^{\gamma_j}$ y entonces podemos concluir que $x \in < h_1 > \cdots < h_i > \bigcap < h_{i+1} >= 1$.

□

Demostración de ii.-. Puesto que $P_0 \cong < x_1 > \oplus < x_2 > \oplus \ldots \oplus < x_s >$ y $H =< x_1^p > \oplus < x_2^p > \oplus \ldots \oplus < x_s^p >$, tenemos que

$$\begin{aligned} P_0/H &\cong (< x_1 > \oplus \ldots \oplus < x_s >)/(< x_1^p > \oplus \ldots \oplus < x_s^p >) \\ &\cong < x_1 > / < x_1^p > \oplus \ldots \oplus < x_s > / < x_s^p > \\ &\cong C_p \oplus C_p \oplus \ldots \oplus C_p \end{aligned}$$

y $[P_0, H] = |P_0/H| = p^s$ y es un p-grupo elemental.

□

Demostración de iii.-. De forma análoga a lo que hemos visto, el producto $< h_1^{p^{\gamma_1 - 1}} > \ldots < h_s^{p^{\gamma_s - 1}} >$ es un producto directo. Además, puesto que $|h_i| = p^{\gamma_i}$ tenemos que $|h_i^{\gamma_i - 1}| = p$ y por tanto $h_i^{\gamma_i - 1} \in K \bigcap H$ de manera que $< h_1^{p^{\gamma_1 - 1}} > \ldots < h_s^{p^{\gamma_s - 1}} > \subseteq K \bigcap H$.

Recíprocamente, si $x \in K \bigcap H$, tenemos $|x| = p$ y $x = h_1^{a_1} \ldots h_s^{a_s}$, entonces

$$x^p = h_1^{a_1 p} \ldots h_s^{a_s p} = 1 \Rightarrow h_1^{a_1 p} = \cdots = h_s^{a_s p} = 1$$

por ser el producto directo, por lo que $p^{\gamma_i} | a_i p$ y por tanto $p^{\gamma_i} - 1 | a_i$ lo que implica que $x \in < h_1^{p^{\gamma_1 - 1}} > \ldots < h_s^{p^{\gamma_s - 1}} >$.

Además está claro que $< h_1^{p^{\gamma_1 - 1}} > \ldots < h_s^{p^{\gamma_s - 1}} >$ es un p grupo elemental isomorfo a C_p^s y por tanto de orden p^s. □

Para terminar con la demostración de la existencia, distinguimos dos casos:

Caso 1.- $K \leq H$.

Caso 2.- $K \not\leq H$.

Caso 1.-

Si $K \leq H$, entonces $K = K \bigcap H =< h_1^{p^{\gamma_1 - 1}} > \ldots < h_s^{p^{\gamma_s - 1}} >$ tiene orden p^s y

$$[P : H] = |K| = p^s = \frac{p^{m+s}}{p^m} = [P_0 : H]$$

de donde P y P_0 tienen el mismo orden y así

$$P = P_0 =< x_1 >< x_2 > \ldots < x_s > \cong C_{p^{\gamma_1+1}} \oplus C_{p^{\gamma_2+1}} \oplus \ldots \oplus C_{p^{\gamma_s+1}}.$$

y la partición que buscamos sería $\gamma_1 + 1 \geq \gamma_2 + 1 \geq \ldots \geq \gamma_s + 1$

Caso 2.-

Si $K \not\leq H$ tomemos $x \in K$ tal que $x \notin H$, entonces $xH \in P/H$ es un elemento no trivial de un p-grupo elemental, por el lema, existe un subgrupo $\overline{M} \leq P/H$ tal que $P/H =< xH > \overline{M}$, como producto directo. Escribimos $\overline{M} = M/H$ y tenemos que

$$|P/H| = |xK|\frac{|M|}{|H|} = p\frac{|M|}{|H|}$$

de donde $|P| = p|M|$ y además $< x > \bigcap M = 1$, de donde $P =< x > M$ como producto directo. Entonces $|M| = p^{e-1}$ y aplicando inducción existe una partición $\beta_1 \geq \ldots \geq \beta_t$ de $e-1$ tal que

$$M \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \ldots \oplus C_{p^{\beta_t}},$$

y tenemos

$$P =< x > M \cong C_p \oplus C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \ldots \oplus C_{p^{\beta_t}},$$

y la partición de e que buscamos sería $\beta_1 \geq \ldots \geq \beta_t \geq 1$.

Probemos ahora la unicidad.

Supongamos dos descomposiciones de P como suma directa

$$P \cong C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \ldots \oplus C_{p^{\alpha_r}} \quad \text{y} \quad P \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \ldots \oplus C_{p^{\beta_s}}$$

asociadas a particiones $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_s$ y $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t$ de e, queremos probar que las dos particiones son iguales. Haremos la demostración por inducción sobre e.

Si $e = 1$ la única partición de 1 es 1 y por tanto tenemos garantizada la unicidad.

Supongamos que el resultado es cierto para grupos con orden p^m y $m < e$. Consideremos, igual que antes, el morfismo $\varphi : P \to P$ y $H = \mathrm{Im}(\varphi) = \{x^p; x \in P\}$ y $K = \ker(\varphi)$. Si H es trivial, entonces P sería un p-grupo elemental (todos sus elementos no triviales tienen orden p) y por tanto la única descomposición como suma directa de grupos cíclicos de P sería $P \cong C_p \oplus C_p \oplus \ldots \oplus C_p$ y la única partición de e sería $1 \leq 1 \leq \ldots \leq 1$.

Si hacemos interna la descomposición $P \cong C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \ldots \oplus C_{p^{\alpha_r}}$ encontraremos elementos $x_i \in P$ de orden p^{α_i}, con $P =< x_1 >< x_2 > \ldots < x_r >$ como producto directo interno.

Análogamente para la descomposición $P \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \ldots \oplus C_{p^{\beta_s}}$ encontraremos elementos $y_i \in P$ de orden p^{β_i}, con $P =< y_1 >< y_2 > \ldots < y_s >$ como producto directo interno.

Estas dos descomposiciones me dan descomposiciones de H y K como producto directo que serían:

$$\begin{aligned} K &=< x_1^{p^{\gamma_1-1}} >< x_2^{p^{\gamma_2-1}} > \ldots < x_r^{p^{\gamma_r-1}} > \cong C_p^s \\ K &=< y_1^{p^{\beta_1-1}} >< y_2^{p^{\beta_2-1}} > \ldots < y_s^{p^{\beta_s-1}} > \cong C_p^r \\ H &=< x_1^p >< x_2^p > \ldots < x_r^p >=< y_1^p >< y_2^p > \ldots < y_s^p > \end{aligned}$$

De la unicidad para p-grupos elementales aplicada a K obtenemos que $r = s$. La hipótesis de inducción aplicada a H nos asegura que el número de x_i tales que $x_i^p \neq 1$ coincide con el número de y_i tales que $y_i^p \neq 1$ y que para estos $\gamma_i = \beta_i$. Deducimos entonces que el número de x_i tales que $x_i^p = 1$ tiene que coincidir con el número de y_i tales que $y_i^p = 1$ y así que $\gamma_i = \beta_i$ para todo $i = 1, \ldots, r$. □

Uniendo los teoremas 6.1 y 6.6 tenemos

Teorema 6.7 (Teorema de estructura de grupos abelianos finitos. Descomposición Cíclica Primaria)**.**

Sea G un grupo abeliano de orden n y sea $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ su descomposición en primos distintos. Entonces existen particiones únicas $\alpha_1^i \geq \alpha_2^i \geq \ldots \geq \alpha_{s^i}^i$ de $e_i, i = 1, 2, \ldots, r$ tales que

$$G \cong C_{p_1^{\alpha_1^1}} \oplus \cdots \oplus C_{p_1^{\alpha_{s_1}^1}} \oplus C_{p_2^{\alpha_1^2}} \oplus \cdots \oplus C_{p_2^{\alpha_{s^2}^2}} \oplus \ldots \oplus C_{p_r^{\alpha_1^r}} \oplus \cdots \oplus C_{p_r^{\alpha_{s_r}^r}}$$

A esta descomposición del grupo G se le llama descomposición cíclica primaria de G y es única salvo orden. A las potencias de primos $p_i^{\alpha_j^i}$ se les llama divisores elementales.

Utilizando ahora que si n y m son primos relativos entonces $C_n \oplus C_m \cong C_{nm}$, podemos agrupar los distintos primos en la descomposición cíclica primaria de un grupo abeliano para obtener el siguiente

Teorema 6.8 (Teorema de Decomposición Cíclica)**.**

Dado un grupo abeliano G de orden n, existen enteros únicos $d_1 \leq d_2 \leq \cdots \leq d_t$ tales que d_i divide a d_{i+1} y

$$G \cong C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_t},$$

A esta descomposición se le llama descomposición cíclica de G. A los enteros d_i se les llama factores invariantes. Notar que n es el producto de los factores invariantes.

Veamos como podemos utilizar los teoremas de descomposición cíclica primaria y de descomposición cíclica para clasificar los grupos abelianos finitos.

Ejercicio 6.1. Clasificar todos los grupos de orden 360.

Paso 1.- Descomponemos 360 como producto de primos: $360 = 2^3 3^2 5$.

Paso 2.- Calculamos las particiones de los exponentes:

particiones de 3	particiones de 2	particiones de 1
1 1 1 1 2 3	1 1 2	1

Paso 3.- Calculamos los divisores elementales y las decomposiciones cíclicas primarias

divisores elementales	descomposición cíclica primaria
$2, 2, 2, 3, 3, 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$
$2, 2, 2, 3^2, 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$
$2, 2^2, 3, 3, 5$	$C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5$
$2, 2^2, 3^2, 5$	$C_2 \oplus C_2 \oplus C_4 \oplus C_9 \oplus C_5$
$2^3, 3, 3, 5$	$C_8 \oplus C_3 \oplus C_3 \oplus C_5$
$2^3, 3^2, 5$	$C_8 \oplus C_9 \oplus C_5$

Paso4.- Agrupamos los divisores elemetales para calcular los factores invariantes en cada caso.

$$
\begin{array}{l}
d_1 = 2 \\
d_2 = 2 \cdot 3 = 6 \\
d_3 = 2 \cdot 3 \cdot 5 = 30 \\
\hline
d_1 = 2 \\
d_2 = 2 \\
d_3 = 2 \cdot 3^2 \cdot 5 = 90 \\
\hline
d_1 = 2 \cdot 3 = 6 \\
d_2 = 2^2 \cdot 3 \cdot 5 = 60 \\
\hline
d_1 = 2 \\
d_2 = 2^2 \cdot 3^2 \cdot 5 = 180 \\
\hline
d_1 = 3 \\
d_2 = 3 \cdot 2^3 \cdot 5 = 120 \\
\hline
d_1 = 2^3 \cdot 3^2 \cdot 5 = 360 \\
\hline
\end{array}
$$

y lo ponemos en una tabla

factores invariantes	descomposición cíclica
$2, 6, 30$	$C_2 \oplus C_6 \oplus C_{30}$
$2, 2, 90$	$C_2 \oplus C_2 \oplus C_{90}$
$6, 60$	$C_6 \oplus C_{60}$
$2, 180$	$C_2 \oplus C_{180}$
$3, 120$	$C_3 \oplus C_{120}$
360	C_{360}

Concluimos que hay 6 grupos abelianos no isomorfos de orden 360.

El siguiente problema que vamos a tratar será obtener las descomposiciones cíclica y cíclica primaria de un grupo abeliano.

En el caso en que el grupo esté dado por una presentación, el problema de palabras para el caso abeliano está totalmente resuelto, veamos como se procede.

Vamos a pasar a notación aditiva en lugar de multiplicativa, en este caso, las relaciones o relatores serán expresiones lineales en los generadores igualadas a cero.

Por ejemplo, si en notación multiplicativa, tenemos una presentación de un grupo dada por:

$$G = \langle x, y, z;\ x^3 = y^4, x^2 z = z^{-1} y, xy = yx, xz = zx, yz = zy \rangle,$$

en notación aditiva esta presentación sería

$$G = \langle x, y, z;\ 3x = 4y, 2x + z = -z + y, x + y = y + x, x + z = z + x, y + z = z + y \rangle.$$

Pero siempre que estemos en notación aditiva asumiremos las conmutatividades de los generadores y suprimiremos estas relaciones en la presentación, de manera que el ejemplo anterior quedaría:

$$G = \langle x, y, z;\ 3x = 4y, 2x + z = -z + y, \rangle.$$

Además procuraremos siempre poner las relaciones de forma "*combinación lineal igualada a cero*", de manera que procuraremos dar la presentación anterior como

$$G = \langle x, y, z;\ 3x - 4y = 0, 2x + 2z - y = 0 \rangle.$$

Así una presentación de un grupo abeliano siempre estará dada en notación aditiva y tendrá la forma:

$$G = \langle x_1, x_2, \ldots, x_n; \begin{array}{c} a_{11}x_1 + a_{12}x_2 + \cdots a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots a_{2n}x_n = 0 \\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots a_{mn}x_n = 0 \end{array} \rangle. \tag{6.1}$$

A la matriz

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}. \tag{6.2}$$

la llamaremos matriz de relaciones o relatores del grupo y determina totalmente la presentación.

Recordemos ahora que dar una presentación de un grupo (abeliano) como 6.1 es realmente dar un morfismo sobreyectivo $f : F \to G$, con F un grupo (abeliano) libre con base $\{e_1, e_2, \ldots, e_n\}$, $f(e_i) = x_i$, $i = 1, \ldots, n$ y $\{a_{11}e_1 + a_{12}e_2 + \cdots a_{1n}e_n,\ a_{21}e_1 + a_{22}e_2 + \cdots a_{2n}e_n,\ \cdots,\ a_{m1}e_1 + a_{m2}e_2 + \cdots a_{mn}e_n\}$ un sistema de generadores del núcleo $\ker f$.

Observamos ahora que podemos hacer los siguientes cambios en una base de un grupo libre y seguimos teniendo una base:

Cambio 1.- Sustituir un elemento de la base por su opuesto.

Cambio 2.- Reordenar los elementos de la base.

Cambio 3.- Sustituir un elemento e_i en la base por $e_i + ke_j$ con $j \neq i$.

Estos cambios en la base del grupo libre F dan lugar a las siguientes transformaciones elementales en las columnas de la matriz de relaciones:

Tipo 1.- Cambiar una columna por su opuesto.

Tipo 2.- Reordenar las columnas de la matriz.

Tipo 3.- Sustituir la columna i en la matriz por la columna i más un múltiplo de la columna con $j \neq i$.

Análogamente, cambios del tipo 1,2 o 3 en el sistema de generadores del núcleo dan lugar trasformaciones elementales del tipo 1,2 o 3 respectivamente en las filas de la matriz de relaciones. De manera que tenemos:

Teorema 6.9. *Si M es la matriz de relaciones de una presentación de un grupo abeliano G y M' es una matriz obtenida mediante trasformaciones elementales del tipo 1,2 o 3 en las filas y/o columnas de M. Entonces M' también es una matriz de relaciones de una presentación de G.*

Damos ahora el siguiente teorema sin demostración.

Teorema 6.10. *Dada una matriz $M \in \mathcal{M}_{m,n}(\mathbb{Z})$ podemos realizar transformaciones elementales en M hasta llegar a una matriz diagonal de la forma*

$$M' = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & d_r & \cdots \\ 0 & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

tal que d_i divide a d_{i+1} para $i = 1, \ldots r-1$. Además si M' es la matriz de relaciones de un grupo G, entoces

$$G \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus Z^{n-r}.$$

Además a

$$n - r = \textit{ número de geeradores } - \textit{ rango de la matriz de relaciones}$$

se llamará "rango de la parte libre de" *G. Y a $\mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ se llamará* "parte de torsión" *de G.*

Definición 6.11. Dada una matriz $M \in \mathcal{M}_{m,n}(\mathbb{Z})$ a la matriz M' diagonal en las condiciones del teorema 6.10 se le llama "*forma normal de Smith*"de M y a los elementos d_i no nulos en la diagonal de M' se les llama "*factores invariantes*"de M.

Observación 6.1. El primer factor invariante d_1 de una matriz M es el máximo común divisor de los términos de la matriz.

Veamos en un ejemplo como obtener la forma normal de Smith de una matriz.

Ejemplo 6.1. Vamos a obtener la forma normal de la matriz

$$M = \begin{pmatrix} 14 & 4 & 4 & 14 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix}$$

Observamos que el mcd de los términos de la matriz es 2 intentamos obtener mediante trasformaciones elementales ± 2, lo conseguimos por ejemplo sumando a la primera columna la segunda

$$M = \begin{pmatrix} 14 & 4 & 4 & 14 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix} \xrightarrow{c_1+c_2} \begin{pmatrix} 18 & 4 & 4 & 14 \\ -2 & 4 & 4 & 10 \\ -20 & -4 & -4 & -20 \end{pmatrix}$$

Ponemos -2 en el lugar $1,1$, para ello intercambiamos las filas uno y dos

$$\begin{pmatrix} 18 & 4 & 4 & 14 \\ -2 & 4 & 4 & 10 \\ -20 & -4 & -4 & -20 \end{pmatrix} \xrightarrow{f_1 \leftrightarrows f_2} \begin{pmatrix} -2 & 4 & 4 & 10 \\ 18 & 4 & 4 & 14 \\ -20 & -4 & -4 & -20 \end{pmatrix}$$

Es posible que necesitemos varios pasos para obtener el mcd de los términos en el lugar $1,1$.

Elegimos hacer ceros en la primera fila o columna, en este caso elegimos columna. Para ello a la segunda fila le sumamos 9 veces la primera y a la tercera le restamos 10 veces la primera

$$\begin{pmatrix} -2 & 4 & 4 & 10 \\ 18 & 4 & 4 & 14 \\ -20 & -4 & -4 & -20 \end{pmatrix} \xrightarrow[f_2+9f_1]{f_3-10f_1} \begin{pmatrix} -2 & 4 & 4 & 10 \\ 0 & 40 & 4 & 54 \\ 0 & -44 & -44 & -120 \end{pmatrix}$$

Hacemos ceros en la primera fila.

$$\begin{pmatrix} -2 & 4 & 4 & 10 \\ 0 & 40 & 4 & 54 \\ 0 & -44 & -44 & -120 \end{pmatrix} \to \begin{pmatrix} -2 & 0 & 0 & 0 \\ 0 & 40 & 4 & 54 \\ 0 & -44 & -44 & -120 \end{pmatrix}$$

Ponemos positivo el valor en el lugar $1,1$,

$$\begin{pmatrix} -2 & 0 & 0 & 0 \\ 0 & 40 & 4 & 54 \\ 0 & -44 & -44 & -120 \end{pmatrix} \xrightarrow{f_1 \to -f_1} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 40 & 4 & 54 \\ 0 & -44 & -44 & -120 \end{pmatrix}$$

Nos aseguramos que el valor en el lugar $1,1$ divide a todos los términos de la matriz.

Procedemos de igual forma pero olvidando la primera fila y la primera columna. Tendremos que conseguir el mcd de los restantes términos. Dividimos 54 por 4 y tenemos de cociente 13 y resto 2, así que a la cuarta columna le restamos 13 veces la tercera

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 40 & 4 & 54 \\ 0 & -44 & -44 & -120 \end{pmatrix} \xrightarrow{c_4-13c_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 40 & 4 & 2 \\ 0 & -44 & -44 & 452 \end{pmatrix}$$

Ponemos en el lugar $2,2$ al 2, para ello intercamiamos columnas 2 con 4

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 40 & 4 & 2 \\ 0 & -44 & -44 & 452 \end{pmatrix} \xrightarrow{c_2 \leftrightarrows c_4} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 40 \\ 0 & 452 & -44 & -44 \end{pmatrix}$$

Elegimos filas y hacemos ceros

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 40 \\ 0 & 452 & -44 & -44 \end{pmatrix} \xrightarrow{c_3-226c_2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 40 \\ 0 & 0 & -948 & -9084 \end{pmatrix}$$

Hacemos ceros en la fila 2

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 4 & 40 \\ 0 & 0 & -948 & -9084 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -948 & -9084 \end{pmatrix}$$

Nos aseguramos que el valor en el lugar $2,2$ divide a todos los términos de la matriz salvo a d_1.

Repetimos el proceso olvidando las dos primeras filas y columnas.

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -948 & -9084 \end{pmatrix} \xrightarrow{c_4-9c_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -948 & -552 \end{pmatrix} \xrightarrow{c_3-c4}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -396 & -552 \end{pmatrix} \xrightarrow{c_4-c_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -396 & -156 \end{pmatrix} \xrightarrow{c_3-2c_4}$$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -84 & -156 \end{pmatrix} \xrightarrow{c_4+c_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -84 & -72 \end{pmatrix} \xrightarrow{c_3-c_4} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -12 & -72 \end{pmatrix}$$

$$\xrightarrow{c_4-6c_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -12 & 0 \end{pmatrix} \xrightarrow{c_3 \leftrightarrows -c_3} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix}$$

Y como consecuencia

Corolario 6.12. *Un grupo abeliano es finito si, y sólo si, el rango de su parte libre es cero, o equivalengtemte, el rango de la matriz de relatores en cualquier presentación suya coincide con el número de generadores de la presentación.*

Ejercicio 6.2. Una presentación del grupo abeliano A está dada por:

$$A = \langle x, y, z, t; \begin{array}{l} 14x + 4y + 4z + 14t = 0 \\ -6x + 4y + 4z + 10t = 0 \\ -16x - 4y - 4z - 20t = 0 \end{array} \rangle$$

Calcula el rango (de la parte libre) y todos los grupos abelianos no isomorfos de orden igual al de la torsión de A. ¿Tiene A algún elemento de orden infinito? ¿Y de orden 12?

Solución.-

La matriz de relaciones de la presentación es

$$\begin{pmatrix} 14 & 4 & 4 & 14 \\ -6 & 4 & 4 & 10 \\ -16 & -4 & -4 & -20 \end{pmatrix}$$

En el Ejemplo 6.1 hemos calculado su forma normal de Smith que es

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix}$$

Por tanto los factores invariantes son $d_1 = 2, d_2 = 2$ y $d_3 = 12$, loa divisores elementales de la torsión serían $2, 2, 2^2$ y 3. El rango de la parte libre sería n$^{\text{a}}$ generadores $-$ rango de la matriz de relaciones $= 4 - 3 = 1$ y por tanto el grupo sería

$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}.$$

La torsión tiene orden $2 \cdot 2 \cdot 12 = 48 = 2^4 \cdot 3$ y grupos de orden 48 habría

divisores elementales	descomposición cíclica primaria
$2, 2, 2, 2, 3$	$C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3$
$2, 2, 2^2, 3$	$C_2 \oplus C_2 \oplus C_4 \oplus C_3$
$2, 2^3, 3$	$C_2 \oplus C_8 \oplus C_3$
$2^2, 2^2, 3$	$C_4 \oplus C_4 \oplus C_3$
$2^4, 3$	$C_{16} \oplus C_3$

factores invariantes	descomposición cíclica
$2, 2, 2, 6$	$C_2 \oplus C_2 \oplus C_2 \oplus C_6$
$2, 2, 12$	$C_2 \oplus C_2 \oplus C_{12}$
$2, 24$	$C_2 \oplus C_{24}$
$2^2, 12$	$C_4 \oplus C_{12}$
48	C_{48}

Mirando la descomposición cíclica de $A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}$ vemos que tiene elementos de orden 12, por ejemplo el correspondiente a $(0, 0, 1, 0)$ y de orden infinito, por ejemplo el correspondiente a $(0, 0, 0, 1)$.