Algebra II (Doble grado Informática-Matemáticas)

Mayo- 2020

Tema 7: Clasificación de grupos abelianos finitos.

Nos ocupamos en estas notas de demostrar el *Teorema de Estructura de grupos abelianos finitos* que nos permitirá clasificarlos completamente. Esto es, dado un número natural n podremos listar todos los grupos abelianos de orden n, salvo isomorfismo.

Comenzaremos recordando dos hechos fundamentales:

1. Si C_n denota el grupo cíclico de orden n entonces
$$C_n \times C_m \cong C_{nm} \Longleftrightarrow m.c.d.(n,m) = 1. \tag{0.1}$$
2. Si G es un grupo finito con $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ y G posee un único p_i-subgrupo de Sylow $\mathcal{P}_i$, para cada $i = 1, \dots, k$, entonces
$$G \cong \mathcal{P}_1 \times \cdots \times \mathcal{P}_k.$$

Comenzaremos viendo cómo es la estructura de los p-grupos abelianos finitos.

Definición 0.1. *Un p-grupo abeliano E diremos que es un p-grupo abeliano elemental si $x^p = 1$ para todo $x \in E$.*

Ejemplo 0.2. Para cada $n \geq 1$, $C_p \times \overset{n}{\dots} \times C_p$ es un p-grupo abeliano elemental. De hecho, haciendo uso de la proposición siguiente, los p-grupos abelianos elementales y finitos son todos de esta forma.

El resultado fundamental es la siguiente proposición:

Teorema 0.3. *Sea A un p-grupo abeliano finito con $|A| = p^n$, $n \geq 1$. Entonces existen enteros $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ tal que $\beta_1 + \beta_2 + \cdots + \beta_t = n$ y*
$$A \cong C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \cdots \times C_{p^{\beta_t}}.$$
Además está expresión es única salvo el orden. Esto es si
$$A \cong C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_s}},$$
con $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_s \geq 1$ y $\alpha_1 + \alpha_2 + \cdots + \alpha_s = n$, entonces
$$s = t \text{ y } \alpha_i = \beta_i$$
para todo $i = 1, \dots, t$.

Para su demostración, veamos primero el siguiente lema:

Lema 0.4. *Sea E un p-grupo abeliano finito y elemental. Para cada $x \in E$ existe un subgrupo $M \leq E$ tal que $E = M \times \langle x \rangle$.*

Demostración. Para $x = 1$ basta tomar $M = E$. Supongamos pues $x \neq 1$ (y entonces $ord(x) = p$ pues E es un p-grupo abeliano elemental) y sea $\sum := \{H \leq E / x \notin H\}$. Puesto que el subgrupo trivial pertenece a $\sum$, entonces $\sum \neq \emptyset$ y elegimos $M \in \sum$ de orden mayor.

Puesto que $[E : M]$ divide a $|E|$ entonces $[E : M] = p^i$ con $i > 0$ pues $x \notin M$. Veamos que $i = 1$

Supongamos $i > 1$ y consideremos el grupo cociente E/M que tendrá $|E/M| = p^i > p$. E/M es también un p-grupo abeliano elemental y podemos elegir $yM \in E/M$ con $yM \notin \langle xM \rangle$ y con $ord(yM) = p$. Además $xM \notin \langle yM \rangle$, pues si así fuera sería $\langle xM \rangle = \langle yM \rangle$ pues ambos elementos tienen orden p.

Consideramos la proyección $q : E \to E/M$. Puesto que $xM \notin \langle yM \rangle$ entonces $x \notin q^*(\langle yM \rangle)$ y entonces $q^*(\langle yM \rangle)$ es un elemento de $\sum$ que contiene propiamente a M pues $y \notin M$, en contradicción con la elección de M.

Así $[E : M] = p$, con lo que si $|E| = p^k \Rightarrow |M| = p^{k-1}$. Además $M \cap \langle x \rangle = 1$, pues si $\exists x^j \in M, j \neq 0$ entonces $\langle x^j \rangle = \langle x \rangle \leq M$ y en particular $x \in M$ en contra de que $M \in \sum$. Aplicando ahora el tercer teorema de isomorfía a M y $\langle x \rangle$ (notemos que la normalidad la tenemos asegurada pues el grupo E es abeliano) tendremos

$$M\langle x \rangle / \langle x \rangle \cong M / M \cap \langle x \rangle = M$$

y entonces $|M\langle x \rangle| = |M| \cdot |\langle x \rangle| = p^k$. Consecuentemente $M\langle x \rangle = E$ y $E \cong M \times \langle x \rangle$, como queríamos demostrar. □

Demostración del Teorema 0.3.

Demostración. Nos ocupamos en primer lugar de la existencia de tal descomposición.

Procedemos por inducción en el orden de A. Si $|A| = p \Rightarrow A \cong C_p$ y se tiene el resultado con $t = 1$ y $\beta_1 = 1$. Supongamos $|A| = p^n > p$ y el resultado cierto para todo p-grupo abeliano finito de orden $< |A|$.

Consideramos el homomorfismo

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

y sean

$$K = Ker(\varphi) = \{x \in A / x^p = 1\}\ \text{y}\ H = Img(\varphi) = \{x^p / x \in A\}.$$

Se tiene

- Por definición, tanto K como A/H son p-grupos abelianos elementales.
- $A/K \cong H$ y entonces $[A : K] = |H|$,
- $|A/H| = \frac{|A|}{|H|} = \frac{|A|}{[A:K]} = |K|$ y entonces $[A : H] = |K|$.

Como en A existen elementos de orden p (por el Teorema de Cauchy), entonces K es no trivial y entonces $|A/H| = |K| \neq 1$. Consecuentemente H es un subgrupo propio de A y por hipótesis de inducción, si $|H| = p^m$, $m < n$, existen enteros $\gamma_1 \geq \gamma_2 \geq \cdots \geq \gamma_r \geq 1$, con $\gamma_1 + \cdots + \gamma_r = m$ y

$$H \cong \langle h_1 \rangle \times \cdots \times \langle h_r \rangle \cong C_{p^{\gamma_1}} \times \cdots \times C_{p^{\gamma_r}},$$

siendo cada $\langle h_i \rangle \leq H$ y $\langle h_i \rangle \cong C_{p^{\gamma_i}}$.

Como $H = Img(\varphi)$, para cada $i = 1, \ldots, r$ elegimos $g_i \in A$ tal que $\varphi(g_i) = g_i^p = h_i$. Notemos que puesto que $ord(h_i) = p^{\gamma_i}$ entonces

$$ord(g_i) = p^{\gamma_i + 1}$$

para todo $i = 1, \ldots, r$.

Consideremos el grupo

$$A_0 := \langle g_1, \ldots, g_r \rangle.$$

Por definición H es un subgrupo de A_0 y se verifica

(a) $A_0 \cong \langle g_1 \rangle \times \cdots \times \langle g_r \rangle$,

(b) $A_0/H \cong \langle g_1 H \rangle \times \cdots \times \langle g_r H \rangle$, y es un p-grupo abeliano elemental con orden p^r.

(c) $H \cap K \cong \left\langle h_1^{p^{\gamma_1 - 1}} \right\rangle \times \cdots \times \left\langle h_r^{p^{\gamma_r - 1}} \right\rangle$, y es un p-grupo abeliano elemental de orden p^r.

Supuesto demostrado (a), (b) y (c), razonamos como sigue:

Caso 1: K es un subgrupo de H, entonces $K = K \cap H$ y será $|K| \overset{(c)}{=} p^r$. Como $[A : H] = |K| = p^r$ y $[A_0 : H] \overset{(b)}{=} p^r$, entonces $[A_0 : H] = [A : H]$ y entonces $A_0 = A$ con lo que

$$A \cong \langle g_1 \rangle \times \cdots \times \langle g_r \rangle \cong C_{p^{\gamma_1 + 1}} \times \cdots \times C_{p^{\gamma_r + 1}}$$

y obtendríamos la descomposición buscada para A siendo $\beta_1 = \gamma_1 + 1 \geq \beta_2 = \gamma_2 + 1 \geq \cdots \geq \beta_r = \gamma_r + 1$. Notemos que $\beta_1 + \beta_2 + \cdots + \beta_r = \gamma_1 + \cdots + \gamma_r + r = m + r$ y $|A| = |A_0| \overset{(a)}{=} p^{m+r}$.

Caso 2: K no es un subgrupo de H. Elegimos entonces $x \in K - H$. Entonces $xH \in A/H$ es un elemento no trivial y, puesto que A/H es un p-grupo

abeliano elemental, será $ord(xH) = p$. Además, por el lema anterior, existe un subgrupo $M/H \leq A/H$ tal que $A/H \cong M/H \times \langle xH \rangle$.

Tenemos entonces $x \notin M$ pues $xH \notin M/H$, y $ord(x) = p$ pues $x \in K$, con lo que $M \cap \langle x \rangle = 1$. Como

$$|A/H| = |M/H| \cdot |\langle xH \rangle| = |M/H|p \Rightarrow |A| = |M|p = |M\langle x \rangle| \Rightarrow A = M\langle x \rangle,$$

concluimos que $A \cong M \times \langle x \rangle$ y entonces basta aplicar la hipótesis de inducción a M.

Veamos pues la demostración de (a), (b) y (c):
Demostración de (a): Hemos de ver que

1. $\langle g_1 \rangle \dots \langle g_r \rangle = A_0$ y
2. $\langle g_1 \rangle \dots \langle g_{i-1} \rangle \cap \langle g_i \rangle = 1$ para todo $i \geq 2$.

La primera igualdad es clara pues $\langle g_1 \rangle \dots \langle g_r \rangle = \langle g_1, \dots, g_r \rangle = A_0$. La segunda la vemos por inducción en i. Para $i = 2$ sea

$$x \in \langle g_1 \rangle \cap \langle g_2 \rangle \Rightarrow \left\{ \begin{array}{l} x \in \langle g_1 \rangle \Rightarrow x = g_1^t \Rightarrow x^p = h_1^t \in \langle h_1 \rangle \\ x \in \langle g_2 \rangle \Rightarrow x^p \in \langle h_2 \rangle \end{array} \right\} \Rightarrow x^p \in \langle h_1 \rangle \cap \langle h_2 \rangle = 1.$$

Consecuentemente $x^p = 1 \Rightarrow ord(x) = p$. Como $x = g_1^t$, entonces

$$p = ord(x) = \frac{ord(g_1)}{mcd(t, ord(g_1))} = \frac{p^{\gamma_1+1}}{mcd(t, p^{\gamma_1+1})} \Rightarrow mcd(t, p^{\gamma_1+1}) = p^{\gamma_1} \Rightarrow t = p^{\gamma_1} k$$

con lo que

$$x = (g_1)^{p^{\gamma_1} k} = (h_1)^{p^{\gamma_1 - 1} k} \in \langle h_1 \rangle.$$

De la misma forma concluimos que $x \in \langle h_2 \rangle$ y como $\langle h_1 \rangle \cap \langle h_2 \rangle = 1$, será $x = 1$.

Supuesto cierto para i, veámoslo para $i + 1$. Notemos que, puesto que $\langle g_1 \rangle \dots \langle g_{j-1} \rangle \cap \langle g_j \rangle = 1$ para todo $j \leq i$, entonces $\langle g_1, \dots, g_i \rangle = \langle g_1 \rangle \times \dots \times \langle g_i \rangle$.

Sea $x \in (\langle g_1 \rangle \dots \langle g_i \rangle) \cap \langle g_{i+1} \rangle$, entonces

$$\left\{ \begin{array}{l} x = g_1^{t_1} \dots g_i^{t_i} \Rightarrow x^p = h_1^{t_1} \dots h_i^{t_i} \\ x = g_{i+1}^{t_{i+1}} \Rightarrow x^p = h_{i+1}^{t_{i+1}} \end{array} \right\} \Rightarrow x^p \in (\langle h_1 \rangle \dots \langle h_i \rangle) \cap \langle h_{i+1} \rangle$$

con lo que $x^p = 1$ y $ord(x) = p$. Razonando como anteriormente, concluimos que $x \in \langle h_{i+1} \rangle$.

Como $\langle g_1, \dots, g_i \rangle = \langle g_1 \rangle \times \dots \times \langle g_i \rangle$, entonces el elemento $(g_1^{t_1}, \dots, g_i^{t_i}) \in \langle g_1 \rangle \times \dots \times \langle g_i \rangle$ tiene orden p y tenemos

$$\begin{aligned} p &= ord(g_1^{t_1}, \dots, g_i^{t_i}) = mcm(ord(g_1^{t_1}), \dots, ord(g_i^{t_i})) \\ &= mcm(\tfrac{p^{\gamma_1+1}}{mcd(t_1, p^{\gamma_1+1})}, \dots, \tfrac{p^{\gamma_i+1}}{mcd(t_1, p^{\gamma_i+1})}). \end{aligned}$$

Entonces o todos valen p o algunos valen p y otros valen 1. Pero si $\frac{p^{\gamma_j+1}}{mcd(t_1,p^{\gamma_j+1})} = p \Rightarrow t_j = p^{\gamma_j} r$, mientras que si $\frac{p^{\gamma_j+1}}{mcd(t_1,p^{\gamma_j+1})} = 1 \Rightarrow t_j = p^{\gamma_j+1}$. En el primer caso $g_j^{t_j} = (h_j)^{p^{\gamma_j-1}r}$ y en el segundo caso $g_j^{t_j} = 1$. Consecuentemente

$$\left.\begin{array}{l} x = g_1^{t_1} \dots g_i^{t_i} \in \langle h_1 \dots h_i \rangle \\ x \in \langle h_{i+1} \rangle \end{array}\right\} \Rightarrow x \in (\langle h_1 \rangle \dots \langle h_i \rangle) \cap \langle h_{i+1} \rangle = 1$$

esto es, $x = 1$, lo que concluye la demostración de (a).
Demostración de (b): En primer lugar, puesto que $(g_i H)^p = g_i^p H = h_i H = H$ entonces $ord(g_i H) = p$ con lo que

$$|\langle g_1 H \rangle \times \dots \times \langle g_r H \rangle| = p^r.$$

y es además un p-grupo abeliano elemental pues es isomorfo a $C_p \times \overset{r}{\dots} \times C_p$. Sea

$$f : A_0/H \to \langle g_1 H \rangle \times \dots \times \langle g_r H \rangle$$

dado por

$$f(g_1^{t_1} \dots g_r^{t_r} H) = (g_1^{t_1} H, \dots, g_r^{t_r} H),$$

f está bien definido pues si $g_1^{t_1} \dots g_r^{t_r} \in H$ entonces $g_1^{t_1} \dots g_r^{t_r} = h_1^{s_1} \dots h_r^{s_r} = g_1^{pt_1} \dots g_r^{pt_r}$, lo que implica, utilizando el apartado (a) ya probado, que $t_i = ps_i$ para todo $i = 1, \dots, r$ y entonces $g_i^{t_i} = h_i^{s_i} \in H$. Es decir $g_i^{t_i} H = H$ para todo $i = 1, \dots, r$.

Es fácil ver que f es un epimorfismo de grupos. Como

$$|A_0/H| = \frac{|A_0|}{|H|} \overset{(a)}{=} \frac{|\langle g_1 \rangle \times \dots \langle g_r \rangle|}{|\langle h_1 \rangle \times \dots \langle h_r \rangle|} = \frac{p^{\gamma_1+1} \dots p^{\gamma_r+1}}{p^{\gamma_1} \dots p^{\gamma_r}} = p^r$$

y $|\langle g_1 H \rangle \times \dots \langle g_r H \rangle| = p^r$ entonces $Ker(f) = 1$ y f es un isomorfismo, lo que demuestra (b).
Demostración de (c): Puesto que $ord(h_i) = p^{\gamma_i}$ entonces $ord(h_i^{p^{\gamma_i-1}}) = p$ para todo $i = 1, \dots, r$. Pero entonces $h_i^{p^{\gamma_i-1}} \in K$ y consecuentemente $\langle h_i^{p^{\gamma_i-1}} \rangle \leq H \cap K$, para todo $i = 1, \dots, r$. Tendremos entonces que

$$\langle h_1^{p^{\gamma_1-1}} \rangle \dots \langle h_r^{p^{\gamma_r-1}} \rangle = \langle h_1^{p^{\gamma_1-1}}, \dots, h_r^{p^{\gamma_r-1}} \rangle \leq H \cap K.$$

Veamos la otra inclusión: sea

$$x \in H \cap K \Rightarrow \left\{\begin{array}{l} x \in H = \langle h_1 \rangle \times \dots \times \langle h_r \rangle \Rightarrow x = (h_1^{t_1}, \dots, h_r^{t_r}) \\ x \in K \Rightarrow ord(x) = p \end{array}\right.$$

entonces $ord(h_i^{t_i} = 1 \text{ ó } p$. Como $ord(h_i) = p^{\gamma_i}$ ha de ser $mcd(p^{\gamma_i}, t_i) = \left\{\begin{array}{l} p^{\gamma_i-1} \\ p^{\gamma_i} \end{array}\right.$. En ambos casos $p^{\gamma_i-1} | t_i$ y por tanto $x \in \langle h_1^{p^{\gamma_1-1}}, \dots, h_r^{p^{\gamma_r-1}} \rangle$, lo que demuestra la otra inclusión.

Obviamente $\langle h_1^{p^{\gamma_1-1}}\rangle \dots \langle h_i^{p^{\gamma_i-1}}\rangle \cap \langle h_{i+1}^{p^{\gamma_{i+1}-1}}\rangle = 1$ pues dicha intersección está contenida en $\langle h_1\rangle \dots \langle h_i\rangle \cap \langle h_{i+1}\rangle$ que sabemos que es trivial. Consecuentemente

$$H \cap K \cong \left\langle h_1^{p^{\gamma_1-1}} \right\rangle \times \cdots \times \left\langle h_r^{p^{\gamma_r-1}} \right\rangle \cong C_p \times \overset{r}{\dots} \times C_p$$

y así $H \cap K$ es un p-grupo abeliano elemental de orden p^r.
Demostración de la unicidad: Supongamos $|A| = p^n$ y sean

$$A \cong C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \cdots \times C_{p^{\beta_t}}, \text{ con } \beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1 \text{ y } \beta_1+\beta_2+\cdots+\beta_t = n$$

y

$$A \cong C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \cdots \times C_{p^{\alpha_s}}, \text{ con } \alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_s \geq 1 \text{ y } \alpha_1+\alpha_2+\cdots+\alpha_s = n$$

dos expresiones distintas de A como producto directo de grupos cíclicos. Hemos de ver que $t = s$ y $\alpha_i = \beta_i$ para todo i. Hacemos inducción en n. Si $n = 1$ entonces $A \cong C_p$ con lo que necesariamente $t = 1 = s$ y $\beta_1 = 1 = \alpha_1$ y se tiene el resultado. Supongamos $n > 1$ y consideremos el subgrupo $H = Img(\varphi) = \{x^p / x \in G\}$.

Si H fueran el grupo trivial entonces todos los elementos de A tendrían orden p con lo que necesariamente $\beta_1 = \beta_2 = \cdots = \beta_t = 1$ y $\alpha_1 = \alpha_2 = \cdots = \alpha_s = 1$. Pero entonces

$$|A| = p^t = p^s \Rightarrow s = t$$

y lo tendríamos probado.

Supongamos $H \neq 1$. Por el primer isomorfismo ponemos $A = \langle a_1\rangle \times \cdots \times \langle a_t\rangle$ con $ord(a_i) = p^{\beta_i}$, $i = 1, \dots, t$; por el segundo tendremos $A = \langle b_1\rangle \times \cdots \times \langle b_s\rangle$ con $ord(b_j) = p^{\alpha_j}$, $j = 1, \dots, s$. Pero entonces, es fácil ver que

$$H = \langle a_1^p\rangle \times \cdots \times \langle a_t^p\rangle$$

con $ord(a_i^p) = p^{\beta_i - 1}$, $i = 1, \dots, t$ y también

$$H = \langle b_1^p\rangle \times \cdots \times \langle b_s^p\rangle$$

con $ord(b_j^p) = p^{\alpha_j - 1}$, $j = 1, \dots, s$. Aplicando la hipótesis de inducción $t = s$ y $\beta_i - 1 = \alpha_i - 1$ para todo $i = 1, \dots, t$, lo que acaba la demostración de la unicidad y de la proposición.

□

Como corolario tenemos:

Teorema 0.5. Teorema de estructura de grupos abelianos finitos. Descomposición cíclica primaria.

Sea A un grupo abeliano finito con $|A| = p_1^{r_1} \dots p_k^{r_k}$. Entonces

$$A \cong \prod_{i=1}^{k} \left(\prod_{j=1}^{t_i} C_{p_i^{n_{ij}}} \right)$$

donde para cada $i = 1, \dots k$

$$n_{i1} \geq n_{i2} \geq \cdots \geq n_{it_i} \geq 1 \quad y \quad n_{i1} + n_{i2} + \cdots + n_{it_i} = r_i.$$

Además esta descomposición es única salvo el orden. Esta descomposición se llama la descomposición cíclica primaria (DCP) de A. Los

$$\{p_i^{n_{ij}} / 1 \leq i \leq k, 1 \leq j \leq t_i\}$$

se llaman los divisores elementales del grupo A.

Demostración. Es consecuencia directa del teorema anterior pues, al ser A abeliano finito A es el producto directo interno de sus subgrupos de Sylow. Esto es

$$A = \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_k$$

con $|\mathcal{P}_i| = p_i^{r_i}$, $i = 1, \dots, k$.

Ahora no hay mas que aplicar la proposición anterior a cada $\mathcal{P}_i$. □

Observación 0.6. Después del teorema anterior, un grupo abeliano finito está totalmente determinado por sus divisores elementales. Esto es dos grupos abelianos finitos son isomorfos si y sólamente si tienen los mismos divisores elementales.

Consecuentemente, podemos entonces clasificar todos los grupos abelianos finitos del mismo orden. Veamos un ejemplo:

Ejemplo 0.7. Vamos a determinar todos los grupos abelianos de orden 360, salvo isomorfismo.

Puesto que $360 = 2^3 3^2 5$, entonces las posibles listas de divisores elementales son:

1. $\{2^3, 3^2, 5\}$ que corresponde a los grupos isomorfos a $C_8 \times C_9 \times C_5$,
2. $\{2^2, 2, 3^2, 5\}$ que corresponde a los grupos isomorfos a $C_4 \times C_2 \times C_9 \times C_5$,
3. $\{2, 2, 2, 3^2, 5\}$ que corresponde a los grupos isomorfos a $C_2 \times C_2 \times C_2 \times C_9 \times C_5$,
4. $\{2^3, 3, 3, 5\}$ que corresponde a los grupos isomorfos a $C_8 \times C_3 \times C_3 \times C_5$,

5. $\{2^2, 2, 3, 3, 5\}$ que corresponde a los grupos isomorfos a $C_4 \times C_2 \times C_3 \times C_3 \times C_5$,

6. $\{2, 2, 2, 3, 3, 5\}$ que corresponde a los grupos isomorfos a $C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$,

Teniendo en cuenta el hecho (0.1), la descomposición cíclica primaria de un grupo abeliano nos da lugar a la que es conocida simplemente por *descomposición cíclica* de grupos abelianos finitos y que enunciamos en el teorema siguiente:

Teorema 0.8. TEOREMA DE DESCOMPOSICIÓN CÍCLICA DE UN GRUPO ABELIANO FINITO

Sea A un grupo abeliano finito. Entonces

$$A \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$$

donde $d_1, d_2, \ldots, d_t$ son números enteros positivos tales que

$$d_1 d_2 \ldots d_t = |A| \;\; y \;\; d_i | d_j \;\; \textit{para cada} \;\; j \leq i.$$

Además esta descomposición es única. Esto es si

$$A \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_s}$$

con $m_1 m_2 \ldots m_s = |A|$ y $m_i | m_j$ para cada $j \leq i.$, entonces

$$s = t \;\; y \;\; d_i = m_i, i = 1, \ldots, t.$$

La lista $\{d_1, d_2, \ldots, d_t\}$ se llaman los factores invariantes del grupo A y la descomposición anterior se llama la descomposición cíclica (DC) del grupo A.

Demostración. Supongamos que $|A| = p_1^{r_1} \ldots p_k^{r_k}$ y consideremos la descomposición cíclica primaria de A

$$A \cong \prod_{i=1}^{k} \left(\prod_{j=1}^{t_i} C_{p_i^{n_{ij}}} \right)$$

con $n_{i1} \geq n_{i2} \geq \cdots \geq n_{it_i} \geq 1$ y $n_{i1} + n_{i2} + \cdots + n_{it_i} = r_i$. Sea $t = máx\{t_1, t_2, \ldots, t_r\}$ y pongamos $n_{i\ell} = 0$ si $t_i < \ell \leq t$, formamos la matriz

$$\begin{pmatrix} p_1^{n_{11}} & p_2^{n_{21}} & \ldots & p_k^{n_{k1}} \\ p_1^{n_{12}} & p_2^{n_{22}} & \ldots & p_k^{n_{k2}} \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ p_1^{n_{1t}} & p_2^{n_{2t}} & \ldots & p_k^{n_{kt}} \end{pmatrix}$$

Sean

$$\begin{aligned} d_1 &= p_1^{n_{11}} p_2^{n_{21}} \dots p_k^{n_{k1}} \\ d_2 &= p_1^{n_{12}} p_2^{n_{22}} \dots p_k^{n_{k2}} \\ &\vdots \\ d_t &= p_1^{n_{1t}} p_2^{n_{2t}} \dots p_k^{n_{kt}} \end{aligned}$$

es decir, cada d_i es el producto de los elementos de la fila i-ésima. Puesto que $n_{ij} \geq n_{ij+1}$ para todo $1 \leq i \leq k$ y $1 \leq j \leq t$, entonces $d_i | d_j$ para todo $j \leq i$ y como

$$\begin{aligned} C_{d_1} &\cong C_{p_1^{n_{11}}} \times C_{p_2^{n_{21}}} \times \dots \times C_{p_k^{n_{k1}}}, \\ C_{d_2} &\cong C_{p_1^{n_{12}}} \times C_{p_2^{n_{22}}} \times \dots \times C_{p_k^{n_{k2}}}, \\ &\vdots \\ C_{d_t} &\cong C_{p_1^{n_{1t}}} \times C_{p_2^{n_{2t}}} \times \dots \times C_{p_k^{n_{kt}}}, \end{aligned}$$

concluimos que

$$A \cong C_{d_1} \times C_{d_2} \times \dots \times C_{d_t}.$$

La unicidad de la descomposición cíclica se sigue de la unicidad de la descomposición cíclica primaria. □

Ejemplo 0.9. Veamos cúal es la descomposición cíclica de los grupos de orden 360.

En el ejemplo anterior hemos calculado las posibles listas de divisores elementales: Entonces si

1. los divisores elementales del grupo A son $\{2^3, 3^2, 5\}$ (y entonces su DCP es $A \cong C_8 \times C_9 \times C_5$) entonces hay únicamente un factor invariante $d_1 = 2^3 35 = 360$ y la descomposición cíclica será $A \cong C_{365}$.

2. Si los divisores elementales son $\{2^2, 2, 3^2, 5\}$ (y entonces su DCP es $C_4 \times C_2 \times C_9 \times C_5$), entonces, procediendo como en la demostración del teorema, los colocamos en forma matricial, completando con 1:

$$\begin{pmatrix} 2^2 & 3^2 & 5 \\ 2 & 1 & 1 \end{pmatrix} \Rightarrow d_1 = 2^2 3^2 5 = 180, d_2 = 2$$

   y la DC será $A \cong C_{180} \times C_2$.

3. Si los divisores elementales son $\{2, 2, 2, 3^2, 5\}$ (y entonces su DCP es $A \cong C_2 \times C_2 \times C_2 \times C_9 \times C_5$), entonces la matriz sería

$$\begin{pmatrix} 2 & 3^2 & 5 \\ 2 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix} \Rightarrow d_1 = 2\,3^2\,5 = 90, d_2 = 2, d_3 = 2$$

   y la DC será $A \cong C_{90} \times C_2 \times C_2$.

4. Para el caso de que la lista de divisores elementales sean $\{2^3, 3, 3, 5\}$ (y la DCP de A sea $A \cong C_8 \times C_3 \times C_3 \times C_5$), entonces

$$\begin{pmatrix} 2^3 & 3 & 5 \\ 1 & 3 & 1 \end{pmatrix} \Rightarrow d_1 = 2^3 3\,5 = 120, d_2 = 3$$

y la DC será $A \cong C_{120} \times C_3$.

5. Si los divisores elementales son $\{2^2, 2, 3, 3, 5\}$ (y la DCP es $A \cong C_4 \times C_2 \times C_3 \times C_3 \times C_5$) entonces

$$\begin{pmatrix} 2^2 & 3 & 5 \\ 2 & 3 & 5 \end{pmatrix} \Rightarrow d_1 = 60, d_2 = 6$$

y la DC será $A \cong C_{60} \times C_6$.

6. Finalmente si los divisores elementales son $\{2, 2, 2, 3, 3, 5\}$ (y la DCP es $A \cong C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$) entonces

$$\begin{pmatrix} 2 & 3 & 5 \\ 2 & 3 & 1 \\ 2 & 1 & 1 \end{pmatrix} \Rightarrow d_1 = 30, d_2 = 6, d_3 = 2$$

y entonces la DC será $A \cong C_{30} \times C_6 \times C_2$.

Observación 0.10. A la hora de listar los grupos, salvo isomorfismo, de un orden dado, podemos también dar las posibles listas de factores invariantes, Para ello hay que tener en cuenta que si A es un grupo finito con $|A| = n$ y

$$A \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$$

es su descomposición cíclica, entonces

- Como $d_1 d_2 \ldots d_t = n$ entonces $d_i | n$ para todo $i = 1, \ldots t$.
- Si p es un número primo con $p|n$ entonces $\exists i \geq 1$ tal que $p|d_i$, pero entonces (puesto que $d_i|d_j$ para $j \leq i$) $p|d_j$ para todo $j \leq i$. En particular
- Cada divisor primo de n divide a d_1

En particular tenemos:

Corolario 0.11. *Si $n = p_1 p_2 \ldots p_k$, entonces salvo isomorfismo el único grupo abeliano de orden n es el grupo cíclico C_n.*

Demostración. Si $|A| = n$, únicamente puede tener un factor invariante $d_1 = p_1 p_2 \ldots p_k$ con lo que

$$A \cong C_n \cong C_{p_1} \times C_{p_2} \times \cdots \times C_{p_k}$$

. □