Capítulo

6

Estructura de los Grupos

6.1 Introducción

En nuestro viaje dentro de la teoría de grupos, hemos estudiado muchos ejemplos de grupos interesantes, como los grupos de simetría, los enteros módulo m, las permutaciones,...etc, pudiendo reconocer dentro de cada uno de ellos propiedades particulares que los diferenciaban entre sí; como una planta de helecho se diferencia de una de naranja. Hemos realizado un largo recorrido por este hermoso paraje del álgebra, deteniéndonos en cada árbol del bosque, en cada piedra del camino, en cada río que atravesamos a describir con detalle minucioso lo que ibamos descubriendo. Nos dirigimos ahora hacia una colina desde donde se puede otear todo el camino andado, desde muy arriba, y tener una visión más amplia de las cosas que están abajo en los valles.

Con toda la información que tenemos a la mano, podemos hacer un resumen general de todo lo visto en el recorrido, sintetizando en unas pocas ideas el amplio panorama de la teoría de grupos. Se trata entonces de ordenar todo el material estudiado dentro de una estructura general.

Este enfoque estructural facilita la clasificación de los grupos, permite obtener un conocimiento más profundo de ellos y genera una gran cantidad de nuevos ejemplos.

Existe mucha similitud entre el conjunto de los números enteros y el conjunto de los grupos abelianos finitos, desde el punto de vista estructural, como se verá en este capítulo. Los números primos son los elementos básicos a partir de los cuales se generan todos los demás enteros. En el caso de los grupos abelianos finitos, los grupos cíclicos juegan el mismo papel que los números primos, pues ellos son los bloques con los cuales se construyen los otros grupos.

La clasificación de todos los grupos abelianos finitos es, sin duda alguna, una de las más altas realizaciones de toda el álgebra. El primer

paso en alcanzar esta meta viene dado por el teorema Sylow, el cual permite obtener subgrupos de orden una potencia de un primo p, cuando dicha potencia es un divisor del orden del grupo dado. El teorema de Sylow es una herramienta poderosa que permite desmenuzar un grupo grande en pedazos más pequeõs, los p-grupos, de una manera rápida y eficiente, con tan sólo conocer el orden del grupo.

El proceso de clasificación culmina brillantemente con el teorema de la unicidad de los invariantes para grupos de orden una potencia de un primo p, o p-grupos. Si conocemos todos los invariantes de un p-grupo, entonces se conoce su descomposición como producto directo de grupos cíclicos.

6.2 Producto Directo de Grupos

Sean A y B dos grupos y consideremos a A y B como conjuntos. Sea G el producto cartesiano $A \times B$. Podemos definir una operación binaria en $A \times B$ mediante

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

donde $a_1 a_2$ indica el producto de a_1 con a_2 en el grupo A_1, y $b_1 b_2$ indica el producto de b_1 con b_2 en el grupo B. Probaremos que G con la operación $*$, de multiplicación por coordenadas, es un grupo.

En primer lugar la operación es cerrada, pues los respectivos productos en A y B son cerrados, con lo cual se demuestra que $(a_1 a_2, b_1 b_2)$ es un elemento de G.

Para demostrar la asociatividad, pongamos

$$\begin{aligned}
(a_1, b_1) * [(a_2, b_2) * (a_3, b_3)] &= (a_1, b_1) * (a_2 a_3, b_2 b_3) \\
&= (a_1(a_2 a_3), b_1(b_2 b_3)) \\
&= ((a_1 a_2)a_3), (b_1 b_2)b_3) \\
&= (a_1 a_2, b_1 b_2) * (a_3, b_3) \\
&= [(a_1, a_2) * (a_2, b_2)] * (a_3, b_3)
\end{aligned}$$

Sea e el elemento neutro de A y f el elemento neutro de B. Entonces el elemento (e, f) está en G. Además, si (a, b) es cualquier elemento de

G se tendrá:

$$(e, f) * (a, b) = (ea, fb) = (a, b)$$
$$(a, b) * (e, f) = (ae, bf) = (a, b)$$

Luego (e, f) es el elemento neutro para la operación $*$.

Finalmente, si $(a, b) \in G$, el elemento (a^{-1}, b^{-1}) estará en G, y se tiene entonces

$$(a, b) * (a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e, f)$$

y

$$(a^{-1}, b^{-1}) * (a, b) = (a^{-1}a, b^{-1}b) = (e, f)$$

luego el inverso de (a, b) es (a^{-1}, b^{-1}). En conclusión hemos probado que $(G, *)$ satisface todas las propiedades de la definición de grupo.

Además, si A y B son grupos abelianos, entonces $A \times B$ es un grupo abeliano.

Definición 6.2.1 *Sean A y B dos grupos. El grupo $G = A \times B$, con la operación de multiplicación por coordenadas, se llama* **producto directo externo de A y B.**

Observación: Si los grupos A y B son abelianos, entonces $G = A \times B$ se llama la suma directa de A y B y se denota por $A \oplus B$

El producto directo externo de dos grupos, se puede generalizar a cualquier número de grupos. Sean $G_1, \ldots, G_n$ grupos y sea $G = G_1 \times \cdots \times G_n$ el conjunto de $n-$uplas $(g_1, \ldots, g_n)$ con $g_i \in G_i$, $1 \leq i \leq n$.

Definimos la operación de producto en G, multiplicando componente por componente

$$(g_1, \ldots, g_n) * (h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$$

Entonces el grupo G con esta operación se llama el **producto directo externo** de $G_1, \ldots, G_n$

Observación: Si se tiene $G = A \times B$, entonces los conjuntos

$$H = \{(a, f) \mid a \in A\} \quad \text{y} \quad K = \{(e, b) \mid b \in B\}$$

son subgrupos de G y además

$$H \cap K = \{(e, f)\}.$$

Con las mismas notaciones anteriores, se tiene la siguiente

Proposición 6.2.1 *Para todo $g \in A \times B$, existen únicos elementos $g_1 \in H$ y $g_2 \in K$ tales que*

$$g = g_1 g_2.$$

Demostración: Sea $g = (a, b)$, entonces

$$\begin{aligned} g &= (a, b) \\ &= (a, f)(e, b) \\ &= g_1 g_2 \end{aligned}$$

con $g_1 \in H$, $g_2 \in K$.

Supongamos ahora que $g = g_1' g_2'$, con $g_1' \in H$ y $g_2' \in K$. Luego $g = g_1 g_2 = g_1' g_2'$, de donde $(g_1')^{-1} g_1 = g_2 (g_2')^{-1} \in H \cap K$. Por lo tanto $(g_1')^{-1} g_1 = e$, lo cual implica $g_1' = g_1$.

Similarmente se demuestra $g_2' = g_2$.

♠

Este resultado se puede generalizar de la manera siguiente:

Proposición 6.2.2 *Sean $G_1, \ldots, G_n$ grupos, y consideremos el producto directo de ellos, $G = G_1 \times \cdots \times G_n$. Para cada i, sea e_i el elemento neutro del grupo G_i y sea*

$$H_i = \{(e_1, \ldots, e_{i-1}, h, e_{i+1}, \ldots, e_n \mid h \in G_i\}$$

entonces los H_i son subgrupos de G y además

1)) $H_i \cap H_j = e$, para $i \neq j$, donde e es elemento neutro de G.

2)) Todo elemento $g \in G$ se expresa de manera única

$$g = h_1 h_2 \cdots h_n$$

donde los h_i están en H_i.

Definición 6.2.2 *Sea G un grupo y $H_1, \ldots, H_n$ subgrupos normales de G, tales que*

1) $G = H_1 \cdots H_n$

2) Para todo $g \in G$, existen elementos únicos $h_i \in H_i$, $1 \leq i \leq n$, tales que

$$g = h_1 \cdots h_n$$

Entonces G se llama el **producto directo interno** *de $H_1, \ldots, H_n$.*

Observación: Más adelante, probaremos que el producto directo externo es isomorfo al producto directo interno, y por lo tanto, al quedar probado este isomorfismo, hablaremos de producto directo, sin ser específicos.

Antes de llegar a ese resultado, necesitamos la siguiente proposición:

Proposición 6.2.3 *Sea $G = N_1 \cdots, N_s$ producto directo interno. Entonces para todo par de subíndices $i \neq j$ se tiene que*

$$N_i \cap N_j = \{e\},$$

y además se cumple

$$ab = ba$$

para cualquier $a \in N_i$, $b \in N_j$

Demostración: Sea $x \in N_i \cap N_j$, entonces de acuerdo con la definición de producto directo interno, existen elementos $g_1, \ldots, g_s$ con $g_i \in N_i$ tales que

$$x = g_1 \cdots g_s \tag{6.1}$$

Por otro lado, podemos representar a x de dos formas distintas

$$x = e_1 e_2 \cdots e_{i-1} x e_{i+1} \cdots e_n$$
$$x = e_1 e_2 \cdots e_{j-1} x e_{j+1} \cdots e_n$$

donde $e_s = e$, es el elemento neutro de G.

Usando la unicidad de la representación en (**??**) se concluye que $x = e$, de donde

$$N_i \cap N_j = \{e\}$$

Si suponemos que $a \in N_i$ y $b \in N_j$, se tiene que $aba^{-1} \in N_j$, puesto que N_j es normal.

Por estar b^{-1} en N_j, se debe tener $aba^{-1}b^{-1} \in N_j$. Pero por otro lado, usando la normalidad de N_i se sigue que $ba^{-1}b^{-1} \in N_i$, y entonces $aba^{-1}b^{-1} \in N_i$.

Combinando ambos resultados se obtiene

$$aba^{-1}b^{-1} \in N_i \cap N_j = \{e\}$$

De donde

$$ab = ba$$

♠

Teorema 6.2.1 *Sea $G = N_1 \cdots N_s$ producto directo interno y $G' = N_1 \times \cdots \times N_s$ producto directo externo, entonces*

$$G \approx G'.$$

Demostración: Consideremos la aplicación

$$\psi : G' \longrightarrow G$$
$$\psi(g_1, \ldots, g_s) = g_1 \cdots g_s$$

Entonces ψ esta bien definida, pues cada g_i pertenece a G, luego el producto de los g_i esta en G.

Sean $x, y \in G'$ y probemos que

$$\psi(x, y) = \psi(x)\psi(y)$$

Se tiene

$$x = (g_1, \ldots, g_s),\ y = (h_1, \ldots, h_s) \quad \text{con } g_i, h_i \in N_i,$$

para todo $(1 \leq i \leq s)$

Luego, usando la proposición anterior, se deduce

$$\begin{aligned} \psi(x, y) &= \psi(g_1h_1, \ldots, g_sh_s) \\ &= (g_1h_1)(g_2h_2)\cdots(g_sh_s) \\ &= (g_1 \cdots g_s)(h_1 \cdots h_s) \\ &= \psi(x)\psi(y) \end{aligned}$$

Además ψ es sobreyectiva, por la definición de producto interno.

Falta probar la inyectividad de ψ.

Sea $x = (g_1, \ldots, g_s) \in G'$ tal que $\psi(x) = e$, luego se tiene

$$g_1 \cdots g_s = e$$

Usando la unicidad de la representación de

$$g_1 \cdots g_s = e_1 \cdots e_s$$

donde $e_i = e$ para todo $1 \leq i \leq s$, se concluye $g_i = e$, para todo $1 \leq i \leq s$.

Luego

$$x = (e, \ldots, e) = e \ \text{ en } \ G'$$

Por lo tanto hemos probado $\ker \psi = \{e\}$ y se puede concluir entonces que ψ es inyectiva.

♠

Ejemplo: Sea $G = \mathbb{Z}_5 \times \mathbb{Z}_5$, donde $\mathbb{Z}_5$, es el grupo de los enteros módulo 5 bajo la adicción. Luego los elementos de G son:

$$\begin{array}{lllll} e = (0,0) & x_6 = (0,1) & x_{11} = (0,2) & x_{16} = (0,3) & x_{21} = (0,4) \\ x_2 = (1,0) & x_7 = (1,1) & x_{12} = (1,2) & x_{17} = (1,3) & x_{22} = (1,4) \\ x_3 = (2,0) & x_8 = (2,1) & x_{13} = (2,2) & x_{18} = (2,3) & x_{23} = (2,4) \\ x_4 = (3,0) & x_9 = (3,1) & x_{14} = (3,2) & x_{19} = (3,3) & x_{24} = (3,4) \\ x_5 = (4,0) & x_{10} = (4,1) & x_{15} = (4,2) & x_{20} = (4,3) & x_{25} = (4,4) \end{array}$$

Entonces G, lo identificamos con $\mathbb{Z}_5 + \mathbb{Z}_5$, haciendo la identificación

$$(a,b) \longrightarrow a(1,0) + b(0,1)$$

Nótese que todo elemento en G se escribe de manera única en esta forma. Por ejemplo

$$x_{15} = 4(1,0) + 2(0,1)$$

Obsérvese también que el orden de cualquier elemento de G es 5, luego $\mathbb{Z}_5 \times \mathbb{Z}_5$ no es isomorfo a $\mathbb{Z}_{25}$ (¿Por qué?).

Ejercicios

1) Sean $G_1, \ldots, G_n$ grupos tales que $o(G_i) = t_i$. Probar que el orden de $G = G_1 \times \cdots \times G_n$ es igual a $t_1 \cdots t_n$.

2) Sea C_4 el grupo cíclico de orden 4. Probar que $C_4 \oplus C_4$ no es un grupo cíclico. Generalice este resultado.

3) Dar una lista de todos los elementos de $C_4 \oplus C_4$. Halle todos los elementos de orden 2. Halle el diagrama de subgrupos de este grupo.

4) Demuestre que $C_4 \oplus C_2 \oplus C_2$ y $C_4 \oplus C_4$ no son isomorfos.

5) Sea $G = G_1 \times \cdots \times G_n$ y considérense las n aplicaciones

$$\pi_i : G \longrightarrow G_i$$

$$(g_1, \ldots, g_n) \longrightarrow g_i$$

π_i se llama la **i- ésima proyección canónica**.

Probar que para todo i, π_i es un homomorfismo sobreyectivo.

6) Sea $G = G_1 \times \cdots \times G_n$ y considérense las n aplicaciones

$$i_k : G_k \longrightarrow G, \;\; 1 \leq k \leq n,$$

$$g_k \longrightarrow (e_1, \ldots, e_{k-1}, g_k, e_{k+1}, \ldots, e_n)$$

la aplicación i_k se llama la **k - ésima inclusión canónica**. Probar que i_k es un homomorfismo de grupos sobreyectivo, para todo k.

7) Demuestre que si G_1, y G_2 son grupos, entonces

$$G_1 \times G_2 \approx G_2 \times G_1$$

8) Sea $G = G_1 \times G_2$, y $H = \{(a, f) \mid a \in G_1\}$, donde f es la identidad de G_2. Probar que H es normal en G y además

$$G/H \approx G_2.$$

9) Sean C_r y C_s grupos cíclicos de orden r y s, con $(r, s) = 1$. Probar que $C_r \times C_s \approx C_{rs}$.

10) Sea $G = S_3 \times S_3$. Hallar dentro de G un subgrupo de orden 9.

11) Hallar todos los posibles grupos abelianos de orden 16.

12) Sean G_1, G_1', G_2, G_2' grupos, tales que $G_1 \approx G_1'$ y $G_2 \approx G_2'$. Probar que

$$G_1 \times G_2 \approx G_1' \times G_2'.$$

6.3 La Ecuación de la Clase

En esta sección estudiaremos una nueva técnica para contar los elementos dentro de un grupo G, conocida con el nombre de relación de conjugación. Por intermedio de ésta, es posible demostrar un resultado muy interesante sobre grupos finitos debido a Cauchy. Este resultado establece que si un número primo p divide al orden de un grupo finito G, entonces G tiene un subgrupo de orden p.

Definición 6.3.1 *Sea G un grupo y $a, b \in G$. Diremos que* **b es conjugado de a**, *si existe $c \in G$, tal que*

$$b = c^{-1}ac$$

Si b es un conjugado de a, lo denotamos por

$$a \sim b$$

Se puede verificar que la relación "$\sim$" es de equivalencia en el conjunto G. Para cada $a \in G$ se tiene su clase de conjugación:

$$C(a) = \{x \in G, \mid a \sim x\}$$

Si $C(a)$ tiene C_a elementos, se tiene la siguiente fórmula de conteo en G

$$|G| = \sum C_a$$

donde C_a recorre todas las clases de equivalencia. Esta relación se conoce con el nombre de **ecuación de la clase en** G

Definición 6.3.2 *Sea G un grupo y $a \in G$. Definimos el* **Normalizador de** *a como*

$$N(a) = \{x \in G, \mid xa = ax\}.$$

Entonces es fácil probar que $N(a)$ es un subgrupo de G.

Teorema 6.3.1 *Para cada $a \in G$,*

$$C_a = \frac{\circ(G)}{\circ(N(a))}.$$

Demostración: Definimos una función

$$\begin{array}{rccc} \phi & : & C(a) & \longrightarrow & G/N(a) \\ & & T = x^{-1}ax & \longrightarrow & N(a)x \end{array}$$

Probaremos que ϕ es una biyección

1) ϕ está bien definida. Es decir, dos clases de conjugados iguales, pero con distintos representantes, tienen la misma imagen bajo el homomorfismo ϕ

Si $x^{-1}ax = y^{-1}ay$, entonces $yx^{-1}axy^{-1} = a$, lo cual implica

$$(xy^{-1})^{-1}axy^{-1} = a$$

.

Luego debemos tener $xy^{-1} \in N(a)$ y de aqui se deduce que $xN(a) = yN(a)$. Por lo tanto ϕ esta bien definida.

2) ϕ es $1:1$

Supongamos que para $T_1, T_2 \in C(a)$, donde $T_1 = x^{-1}ax$, $T_2 = y^{-1}ay$, se tiene $\phi(T_1) = \phi(T_2)$. Por lo tanto

$$N(a)x = N(a)y$$

Luego $xy^{-1} \in N(a)$, lo cual implica $xy^{-1}a = axy^{-1}$. Por lo tanto $y^{-1}ay = x^{-1}ax$, y de esto se obtiene $T_1 = T_2$.

3) ϕ es sobre (fácil).

♠

Corolario 6.3.1 *Si G es un grupo finito, se tiene*

$$\circ(G) = \sum \frac{\circ(G)}{(\circ(N(a))}$$

donde cada elemento a pertenece a una clase conjugada.

Definición 6.3.3 *Sea G un grupo, entonces* **el centro de** G *es el conjunto*

$$Z(G) = \{g \in G \mid gx = xg,\ \forall x \in G\}.$$

Es fácil verificar que $Z(G)$ es un subgrupo de G.

Observación: Usaremos el símbolo Z o $Z(G)$, indistintamente para indicar este grupo.

Observación: Si $a \in Z(G)$, entonces $N(a) = G$, luego

$$\frac{\circ(G)}{\circ(N(a))} = 1$$

Usando esta observación tenemos el corolario:

Corolario 6.3.2 *Si G es finito*

$$\circ(G) = |Z(G)| + \sum_{a \notin Z(G)} \frac{\circ(G)}{\circ(N(a))}.$$

Corolario 6.3.3 *Si $\circ(G) = p^n$, donde p es un número primo, entonces $Z(G) \neq \{e\}$.*

Demostración: Si $a \notin Z(G)$, entonces $N(a) \neq G$, luego por el teorema de Lagrange

$$\circ(N(a))| \circ (G)$$

y por lo tanto

$$\circ(N(a)) = p^\alpha \quad \text{con } 1 \leq \alpha < n$$

luego

$$p \left| \frac{\circ(G)}{\circ(N(a))} \right. ,$$

para todo $a \notin Z(G)$.

Así

$$p \left| \circ(G) - \sum_{a \notin Z(G)} \frac{\circ(G)}{\circ(N(a))} \right.$$

y por lo tanto

$$p \,|\, \circ(Z(G))$$

Esto es $\circ(Z(G)) > 1$

Corolario 6.3.4 *Si $\circ(G) = p^2$, p primo, entonces G es abeliano.*

Demostración: Por el corolario anterior, sabemos que $Z(G) \neq \{e\}$. Como $Z(G)$ es un subgrupo de G, se debe tener que

$$|Z(G)| = p^2 \quad \text{o} \quad |Z(G)| = p$$

Si $|Z(G)| = p^2$ entonces $Z(G) = G$, y estará listo. Si $|Z(G)| = p$, existe $a \in G$ tal que $a \notin Z(G)$, luego

$$Z(G) \subsetneq N(a) \subseteq G$$

Nuevamente, se debe tener

$$\circ(N(a)) = p^2$$

lo cual implica

$$N(a) = G$$

Esto es una contradicción pues $a \notin Z(G)$. Por lo tanto $Z(G) = G$ y así G es abeliano.

Teorema 6.3.2 *(Cauchy) Sea G un grupo finito y p un número primo tal que $p| \circ (G)$. Entonces G tiene un elemento de orden p.*

Demostración:

1) Supongamos que G es abeliano. Usaremos inducción sobre el orden de G. Si $\circ(G) = 1$ no hay nada que probar.

Supongamos el teorema cierto para subgrupos de orden $< n = \circ(G)$

a) Si $\circ(G) = p$, con p un número primo, entonces G es un grupo cíclico generado por un elemento $g \in G$. Luego $\circ(g) = p$ y g es el elemento buscado.

b) G no tiene subgrupos triviales distintos de $\{e\}$ y G, entonces G es cíclico de orden primo (verificarlo!).

c) Supongamos que G tiene un subgrupo H no trivial, y $\circ(H) < \circ(G)$. Si $p| \circ (H)$ estará listo.

Supongamos que $p \not| \circ (H)$. Luego

$$p \left| \frac{\circ(G)}{\circ(H)} \right.$$

y por lo tanto

$$p| \ \circ \left(\frac{G}{H}\right)$$

Como G/H es abeliano y

$$\circ \left(\frac{G}{H}\right) < \circ(G),$$

aplicamos hipótesis de inducción a G/H. Luego existe un elemento $Hg \in G/H$ de orden p. Luego

$$(Hg)^p = Hg^p = H$$

es decir, $g^p \in H$ y $g \notin H$, luego

$$(g^p)^{\circ(H)} = e$$

Sea $x = g^{\circ(H)}$. Entonces probaremos que $x \neq e$.

En efecto si

$$g^{\circ(H)} = e$$

tenemos que

$$(Hg)^{\circ(H)} = H.$$

Como $\circ(Hg) = p$, se debe tener $p| \circ (H)$, lo cual es imposible.

Así $x \neq e$ y $x^p = e$. Luego

$$\circ(x) = p$$

Con esto termina la demostración del primer caso.

2) G no Abeliano

Nuevamente usamos inducción sobre el orden de G.

Si $\circ(G) = 1$ no hay nada que probar.

Si G tiene un subgrupo H, tal que $p| \circ (H)$ está listo.

Supongamos que p no divide al orden de ningún subgrupo de G. En particular, si $a \notin Z(G)$ entonces $N(a) \neq G$ y por lo tanto $p \not| N(a)$. Luego se tiene la ecuación de la clase

$$\circ(G) = \circ(Z(G)) + \sum_{a \notin Z(G)} \frac{\circ(G)}{\circ(N(a))}$$

Puesto que $p| \circ (G)$ y $p \not| \circ (N(a))$ se tiene que $p| \frac{\circ(G)}{\circ(N(a))}$, si $a \notin Z(G)$. Luego

$$p \left| \circ (G) - \sum_{a \notin Z(G)} \frac{\circ(G)}{\circ(N(a))} \right.$$

y por lo tanto

$$p| \circ (Z(G))$$

Pero hemos supuesto que p no dividía al orden de ningún subgrupo propio de G. Como consecuencia de esto debemos tener $Z(G) = G$, con lo cual G es abeliano. Luego aplicamos el primer caso.

♠

Ejercicios

1) Probar que si G es un grupo, entonces su centro es un grupo abeliano.

2) Sea G un grupo y $a \in G$. Probar que $N(a)$ es un subgrupo de G.

3) Hallar el centro de S_3.

4) En el grupo S_3, calcular $N(\phi)$, donde ϕ es la reflexión de orden 2.

5) Sea G un grupo y $a \in G$. Probar que $a \in Z(G)$ si y sólo si $N(a) = G$.

6) Probar que si G es un grupo, la relación de conjugados, en los elementos de G es de equivalencia.

7) Escribir la ecuación de la clase para el grupo $G = S_3$.

8) Probar que si G es un grupo de orden p^α, entonces G tiene subgrupos de ordenes $1, p, p^2, \ldots, p^{\alpha-1}, p^\alpha$.

9) Sea p un número primo. Probar que existen sólo dos grupos de orden p^2, salvo isomorfismo.

10) Halle todos los conjugados de la rotación R_1 en el grupo de simetrías del cuadrado.

11) Calcule el número de clases conjugadas del grupo diédrico D_4.

12) Halle el centro de D_4.

6.4 Teoremas de Sylow

En esta sección probaremos uno de los teoremas más importantes de toda la teoría de grupos, como lo es el teorema de Sylow. Si G es un grupo cuyo orden es divisible por una potencia de un primo p, entonces el teorema de Sylow garantiza la existencia de un subgrupo de G, cuyo orden es la potencia dada de p.

Para demostrar este teorema necesitamos aplicar una técnica nueva para contar elementos dentro de un conjunto, a partir de un grupo dado, la cual se conoce con el nombre de Acción de Grupos.

Definición 6.4.1 *Sea A un conjunto y G un grupo. Diremos que G actúa sobre A, si existe una función $\phi : G \times A \longrightarrow A$ que satisface*

1. *Para todo $g \in G$, la aplicación*

$$\begin{aligned} \phi_g : A &\longrightarrow A \\ a &\longrightarrow \phi(g, a) \end{aligned}$$

es una permutación del conjunto A.

2. La aplicación

$$G \longrightarrow S(A)$$
$$g \longrightarrow \phi_g$$

es un homomorfismo de grupos.

Observación: De acuerdo con la condición 2 se tienen las siguientes fórmulas de composición.

1. $\phi_a\phi_b = \phi_{ab}$, para todo a y b en G.
2. $\phi_{g^{-1}}\phi_g = \phi_e = Id$, para todo g en G.

Ejemplo: En la demostración del Teorema de Cayley hemos visto cómo un grupo G actúa sobre el conjunto G formado por sus elementos, mediante **Traslaciones a la derecha**. Este tipo de acción viene dada por la función

$$\phi : G \times G \longrightarrow G$$
$$(g, a) \longrightarrow g.a$$

Es fácil verificar que se cumplen las condiciones 1 y 2 de la definición para esta función.

Introducimos a continuación un par de conceptos muy útiles para el conteo de los elementos de un conjunto en donde está definida una acción.

Definición 6.4.2 *Sea G un grupo, el cual actúa sobre un conjunto A. Entonces para todo a en A, se define la* **órbita de** a **bajo** G *como el conjunto*

$$A_a = \{\phi(g, a) \mid g \in G\}$$

Observación: Es fácil verificar que el conjunto de las distintas órbitas de A bajo todos los elementos de G establece una partición del conjunto A.

Definición 6.4.3 *Sea G un grupo, el cual actúa sobre un conjunto A. Entonces para todo $a \in A$ se define el* **estabilizador de a en** *G como el conjunto*

$$Est_a = \{g \in G \mid \phi(g, a) = a\}$$

Observación: Se demuestra que para todo a en A, Est_a es un subgrupo de G.

El siguiente teorema permite calcular el número de elementos dentro de cada órbita.

Teorema 6.4.1 *Sea G un grupo finito, el cual actúa sobre un conjunto A finito. Entonces, para todo $a \in A$ se tiene*

$$|A_a| = [G : Est_a] = \frac{|G|}{|Est_a|}$$

Demostración: Sea $\mathcal{C}_a$ el conjunto de las clases laterales derechas de Est_a en G. Consideremos la aplicación

$$\Psi : \mathcal{C}_a \longrightarrow A_a$$
$$g.Est_a \longrightarrow \phi_g(a)$$

donde $\phi_g(a)$ denota la aplicación de g sobre el elemento a.

En primer lugar probaremos que ϕ está bien definida, para lo cual supongamos que $g_1 Est_a = g_2 Est_a$ para algunos g_1, g_2 en G. Entonces se tiene $g_1 g_2^{-1} \in Esta_a$ si y sólo si $\phi_{g_1^{-1} g_2}(a) = a$.

Luego $\phi_{g_1^{-1}} \phi_{g_2}(a) = a$, si y sólo si $\phi_{g_2}(a) = \phi_{g_1}(a)$. Con esto hemos probado que la función está bien definida. Repitiendo los pasos en sentido inverso, se prueba la inyectividad de ψ. Luego la función es biyectiva y de esto se deduce la tesis del teorema.

♠

Damos inicio ahora a una serie de resultados de combinatoria necesarios para probar la primera parte del Teorema de Sylow.

Sea S un conjunto de n elementos. Entonces el número de formas de escoger k elementos entre los n es dado por:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{6.2}$$

Lema 6.4.1 *Sea $n = p^\alpha m$, donde p es primo y $p^r | m$ pero $p^{r+1} \not| \ m$. Entonces*

$$p^r \left| \binom{n}{p^\alpha} \quad pero \quad p^{r+1} \not| \binom{n}{p^\alpha} \right.$$

Demostración: De (**??**) obtenemos

$$\begin{aligned} \binom{p^\alpha m}{p^\alpha} &= \frac{(p^\alpha m)!}{(p^\alpha)!(p^\alpha m - p^\alpha)!} \\ &= \frac{p^\alpha m(p^\alpha m - 1)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha(p^\alpha - 1)(p^\alpha - 2)\cdots(p^\alpha - p^\alpha + 1)} \end{aligned} \tag{6.3}$$

Observando la expresión (**??**), vemos que si una potencia de p, digamos p^i divide el numerador, entonces esta potencia también divide al denominador.

En efecto, si $p^i | p^\alpha m - k$, $(k \geq 1)$, entonces $p^i | k$ y por lo tanto

$$p^i | p^\alpha - k.$$

Luego toda potencia de p en el numerador, se cancela con la correspondiente potencia de p en el denominador. Luego la única potencia de p en (**??**) es la que contiene m. De donde se obtiene el resultado.

♠

Teorema 6.4.2 *(Sylow)*
Sea G un grupo finito, p es un número primo y $p^\alpha | \circ(G)$. Entonces G tiene un subgrupo de orden p^α.

Demostración: Sea

$$\circ(G) = p^{\alpha}m,$$

tal que $p^r|m$, y $p^{r+1} \not| m$.

Sea $\mathcal{A} = \{A_1, \ldots, A_s\}$ la familia de subconjuntos de G de tamaño p^{α}. Entonces

$$s = \binom{p^{\alpha}m}{p^{\alpha}}$$

Definimos una relación sobre $\mathcal{A}$, mediante :

A_i, A_j en $\mathcal{A}$ están relacionados, sí y sólo si existe un elemento $g \in G$, tal que $A_i = gA_j$.Es fácil ver que esta relación es de equivalencia.

Afirmamos que existe una clase de equivalencia, digamos $\overline{A}_1$ tal que

$$p^{r+1} \Big| |\overline{A_1}| .$$

Caso contrario p^{r+1} divide a todas las clases de equivalencia y por lo tanto

$$p^{r+1} \mid |\mathcal{A}|$$

entonces

$$p^{r+1} \Big| \binom{p^{\alpha}m}{p^{\alpha}}$$

lo cual es imposible por el lema anterior.

Sea

$$\overline{A_1} = \{A_1, \ldots, A_n\} = \{gA_1 \mid g \in G\}$$

donde $p^{r+1} \not| n$ y sea

$$H = \{g \in G \mid gA_1 = A_1\}$$

entonces H es un subgrupo de G, y además se tiene

$$\circ(H) = \frac{\circ(G)}{n}$$

En efecto, la demostración de **??** se sigue de lo siguiente:

Si para algunos g_1, g_2 en G se tiene que $g_1A_1 = g_2A_1$, entonces $g_2^{-1}g_1A_1 = A_1$.

Luego $g_2^{-1}g_1 \in H$, y por lo tanto las clases laterales g_1H y g_2H son iguales. Por lo tanto, el número de elementos de $\overline{A}_1$, el cual denotamos por n, es igual al número de clases laterales de H en G. Luego

$$n = \frac{\circ(G)}{\circ(H)}$$

de donde

$$\circ(H) = \frac{\circ(G)}{n}$$

Como $\circ(G)/n$ es un entero se tiene que todas las potencias de p que aparecen en n, se cancelan con las respectivas potencias de $\circ(G)$. Como la mayor potencia que divide a n es p^r, se tiene que

$$p^\alpha \,|\circ(H)$$

y por lo tanto

$$\circ(H) \geq p^\alpha \tag{6.4}$$

Por otro lado, $hA_1 = A_1$, para todo $h \in H$. Si tomamos $a_1 \in A_1$ fijo se obtiene

$$ha_1 \in A_1, \quad \forall h \in H$$

Luego

$$\circ(H) \leq \circ(A_1) = p^\alpha \tag{6.5}$$

Usando (**??**) y (**??**) obtenemos

$$\circ(H) = p^\alpha$$

Luego H es el subgrupo buscado y con esto termina la demostración.

♠

Definición 6.4.4 *Sea G un grupo finito de orden $p^\alpha n$, donde p no divide a n. Entonces un subgrupo H de G de orden p^α se llama un* **p-grupo de Sylow** *de G.*

Más adelante veremos otros teoremas de Sylow, que nos darán información sobre el número de p-grupos de Sylow dentro de un grupo G. Antes de llegar a estos teoremas necesitamos una serie de definiciones y resultados sobre grupos conjugados.

Definición 6.4.5 *Sea G un grupo y H subgrupo de G. Para cualquier $a \in G$, el conjunto*

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

se llama **grupo conjugado de H inducido por** a.

La demostración de que dicho conjunto es un subgrupo de G, se deja como ejercicio.

Observación: Es claro que si H' es un conjugado de H, entonces H' y H tienen el mismo orden.

Definición 6.4.6 *Sea G un grupo. Un subgrupo H de G se dice* **invariante** *o* **autoconjugado bajo** *a si y sólo si*

$$aHa^{-1} = H.$$

Observación: Es claro que si $a \in H$, entonces H es invariante bajo a.

Si H es un subgrupo normal de G, entonces H es invariante bajo todos los elementos de G.

Definición 6.4.7 *Sea G un grupo y H, K subgrupos de G. Entonces el conjunto:*

$$N_k(H) = \{k \in K \mid kHk^{-1} = H\}$$

se denomina el **normalizador de H en K.**

Dejamos como ejercicio para el lector, el probar que $N_k(H)$ es un subgrupo de K.

Observación: Si en la definición anterior tenemos $K = G$, entonces denotamos $N_G(H)$ por $N(H)$ y lo llamamos el **Normalizador de** H

Proposición 6.4.1 *Sean H y K subgrupos de G. El número de conjugados de H, inducidos por todos los elementos de K, es igual al índice*

$$[K \ : \ N_K(H)]$$

Demostración: Sea $\mathcal{B}$ el conjunto de todos los conjungados de H, inducidos por los elementos de K y definamos la función

$$\begin{array}{rccc} f & : & K & \longrightarrow & \mathcal{B} \\ & & k & \longrightarrow & kHk^{-1} \end{array}$$

Es claro que f es sobre. Veamos en qué situación dos elementos distintos de K, digamos k_1 y k_2 pueden tener imágenes iguales.

Sea

$$k_1Hk_1^{-1} = k_2Hk_2^{-1}$$

si y sólo si

$$k_1^{-1}k_2H(k_1^{-1}k_2)^{-1} = H$$

si y sólo si

$$k_1^{-1}k_2 \in N_K(H)$$

Luego las imágenes de k_1 y k_2 son iguales si y sólo si estos elementos están en la misma clase lateral de $N_K(H)$ en K. Por lo tanto el número de elementos distintos de $\mathcal{B}$ es igual al número de clases laterales de $N_K(H)$ en K, el cual viene dado por:

$$[K \ : \ N_K(H)]$$

♠

Teorema 6.4.3 *(Sylow)*
Sea G un grupo finito y p un número primo con $p|\circ(G)$. Entonces el número de p-grupos de Sylow de G, el cual denotaremos por h, satisface:

$$h \equiv 1 \ mod \ p \quad y \quad h|\circ(G).$$

Demostración: Sea $\mathcal{D}$ el conjunto de todos los p-grupos de Sylow de G. ($\mathcal{D}$ es diferente del vacío por el primer teorema de Sylow). Sea P un elemento de $\mathcal{D}$. Entonces P actúa sobre $\mathcal{D}$ por conjugación, es decir mediante la acción

$$\begin{aligned} &\phi : P \times \mathcal{D} \longrightarrow \mathcal{D} \\ &(g, P_i) \longrightarrow gP_ig^{-1} \end{aligned}$$

Es claro que esta acción es sobreyectiva, pues si P_i es cualquier elemento de $\mathcal{D}$, se tiene

$$P_i = eP_ie^{-1}$$

donde e es el elemento neutro de P.

Entonces, el número de elementos de $\mathcal{D}$, el cual llamanmos h, se obtiene

$$h = \sum_{Q \in \mathcal{D}} |\mathcal{D}_Q|$$

donde $\mathcal{D}_Q$ es la órbita del elemento Q en $\mathcal{D}$.

Tenemos dos posibilidades para Q.

1) Si $Q = P$, entonces

$$\mathcal{D}_P = \{gPg^{-1} | g \in P\} = P$$

luego esta órbita consiste de un sólo elemento.

2) Si $Q \neq P$, entonces

$$|\mathcal{D}_Q| = \frac{|P|}{|Est_Q|} = \frac{p^\alpha}{|N_P(Q)|} = p^\beta$$

con $\beta \geq 0$.

Como $P \neq Q$, se tendrá $N_P(Q) \neq P$ (Ver los ejercicios) y por lo tanto $\beta > 0$.

En conclusión se tiene que

$$h = 1 + p^{\alpha_1} + p^{\alpha_2} + \cdots + p^{\alpha_n} \tag{6.6}$$

y por lo tanto $h \equiv 1 \ mod \ p$.

En la tercera parte del teorema de Sylow probaremos que todos los p-grupos de Sylow son conjugados entre sí. Entonces si se elige un p-grupo P los restantes p-grupos aparecen en la órbita de P cuando el grupo G actúa sobre $\mathcal{D}$ por conjugación. El tamaño de dicha órbita viene dado por

$$|\mathcal{D}_P| = \frac{|G|}{|Est_P|} = \frac{|G|}{|N(P)|} = [G : N(P)]$$

donde $N(P)$ es el normalizador de P.

♠

Teorema 6.4.4 *(Sylow)*
Sea G un grupo finito y $p| \circ (G)$. Entonces todos los $p-$grupos de Sylow son conjugados.

Demostración:
Sean P un $p-$ subgrupo de Sylow y Q otro $p-$subgrupo de Sylow que no se encuentre entre los conjugados de P.

Entonces calculemos el número total de conjugados de Q, usando la acción del grupo P sobre el conjunto de los conjugados de Q.

En primer lugar, el número de conjugados de Q, por elementos de P (la órbita de Q) viene dado por:

$$[P \ : \ N_P(Q)] = \frac{\circ(P)}{\circ(N_P(Q))} = p^{\beta} \quad \text{con } \beta \geq 0 \tag{6.7}$$

Si asumimos $\beta = 0$, se tendrá

$$\circ(P) = \circ(N_P(Q)))$$

lo cual implica

$$P = N_P(Q)$$

y por lo tanto $P = Q$, lo cual es una contradicción.

Si hay otro conjugado de Q, aparte de los senãlados en (**??**), sea Q_1 otro conjugado y repitamos el proceso. Luego el número total de conjugados de Q (contando todas las órbitas) vendrá dado por

$$h' = p^{\beta_1} + p^{\beta_2} + \cdots p^{\beta_s} \quad \text{con } \beta_i > 0.$$

donde ($\beta = \beta_1$) Por lo tanto $h' \equiv 0 \ mod\ p$, lo cual es imposible por (**??**).

Con esto se da fin a la prueba.

♠

Ejercicios

1) Sea n un entero positivo y k otro entero tal que $k \leq n$. Entonces el **factorial inferior de** n **en** k, el cual denotamos por $(n)_k$ es el número de $k-$uplas que se pueden formar a partir de un conjunto de n elementos.

Si $A = \{1, 2, \ldots, n\}$, entonces $(n)_k$ es el cardinal del conjunto

$$A^k = \{(x_1, \ldots, x_k) \mid x_i \in A \text{ y } x_i \neq x_j, \text{ si } i \neq j\}$$

Probar que $(n)_k = n(n-1)\cdots(n-k+1)$.

2) Si $n = 5$ y $k = 3$, hallar todos los elementos de A^3.

3) Sea $x = (x_1, \ldots, x_k)$ una $k-$upla en A^k. Un **desarreglo de** x es otra $k-$upla y de A^k tal que si $y = (y_1, \ldots, y_k)$, entonces

$$\{x_1, \ldots x_k\} = \{y_1, \ldots, y_k\}$$

Probar que el número de desarreglos posibles de una $k-$upla cualquiera es $k!$.

4) El número de subconjuntos de tamaño k que se puede extraer de un conjunto de n elementos, con $n \geq k$, se llama el **combinatorio de** n **sobre** k y se denota por

$$\binom{n}{k}$$

Demostrar la fórmula

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

5) Probar la fórmula

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \quad 1 \leq k \leq n$$

Ayuda: Primero cuente todos los subconjuntos de tamaño k que contienen al 1 y luego aquellos que no contienen al 1.

6) Sea G un grupo finito y $\mathcal{A}$ la familia de todos los subconjuntos de G de tamaño s, con $s < \circ(G)$. Para A_i, A_j en $\mathcal{A}$ se define la relación "$A_i \sim A_j$ si y sólo si existe un $g \in G$ tal que $gA_i = A_j$"

Probar que esta relación define una relación de equivalencia en $\mathcal{A}$.

7) Sea $\mathcal{A}$ como en el ejercicio anterior y $A_0 \in \mathcal{A}$. Diremos que dos elementos g_1 y g_2 en G están relacionados, si y sólo si

$$g_1 A_1 = g_2 A_1$$

Probar que esto define una relación de equivalencia en G.

8) Sea G un grupo, H un subgrupo de G y $a \in G$. Probar que el conjunto

$$aHa^{-1}\{aha^{-1} \mid h \in H\}$$

es un subgrupo de G, cuyo orden es igual al orden de H. Este grupo se dice **grupo conjugado de** H.

9) Sea G un grupo y H, K dos subgrupos de G. Entonces el **Normalizador de** H **en** K se define por

$$N_k(H) = \{k \in K \mid kHk^{-1} = H\}$$

Probar que $N_k(H)$ es un subgrupo de G.

10) Sea G un grupo y H, K dos subgrupos tales que H y K son conjugados y además

$$N_H(K) = H$$

Probar que $K = H$

11) Probar que un grupo finito de orden 21 tiene un solo $p-$grupo de Sylow de orden 3, o bien 1 ó 7 $p-$grupos de Sylow de orden 7.

12) Probar que cualquier subgrupo de orden p^{n-1} en un grupo de orden p^n, con $p-$primo, es normal en G.

13) Sea G un grupo, $Z(G)$ su centro y $G/Z(G)$ cíclico. Probar que G debe ser abeliano.

14) Probar que cualquier grupo de orden 15 es cíclico.

15) Hallar todas las clases de conjugados en S_4 y verificar la ecuación de la clase.

16) Probar que si G es un grupo de orden p^n con p un primo. Entonces G tiene un subgrupo de orden p^α para cualquier $0 \leq \alpha \leq n$. Use la ecuación de la clase.

17) Sea G un grupo finito de orden $3^2 \cdot 5^2$. ¿Cuántos $3-$grupos de Sylow y $5-$grupos de Sylow hay en G?.

18) Sea G un grupo de orden 30

a) Demuestre que los $3-$grupos de Sylow y los $5-$grupos de Sylow son normales.

b) Demuestre que G tiene un subgrupo normal de orden 15.

c) Clasifique todos los grupos de orden 30.

d) ¿Cuántos grupos de orden 30, no isomorfos, existen?

19) Si G es un grupo de orden 231, probar que el $11-$grupo de Sylow está en el centro de G.

20) Sea G un grupo abeliano finito. Probar que G es isomorfo al producto directo de sus grupos de Sylow.

21) Sean A y B grupos. Probar que $A \times B$ es isomorfo a $B \times A$

22) Sean A y B grupos cíclicos de orden m y n, respectivamente. Probar que $A \times B$ es cíclico si sólo si $(m, n) = 1$.

23) Si G es un grupo de orden pq, con p y q primos y $p < q$, entonces si p no divide a $q - 1$, G es un grupo cíclico.

24) Hallar en D_4 todos los conjugados de $H = \{e, h\}$, donde h es una reflexión en el eje x.

25) Sea $G = S_7$ el grupo de permutaciones de 7 elementos, y sean $H = \{\sigma \in G |\ \sigma(1) = 1\}$ y $K = \{\theta \in G |\ \theta(2) = 2\}$. Hallar a) $N_H(K)$ y b)$N_K(H)$.

26) Sea G y H como en el ejercicio anterior, y sea $\tau = (1, 2, 3)$. Hallar el grupo conjugado de H inducido por τ.

27) Sea $G = D_4$ y considérese los grupos $H =< a >$, $K =< b >$, donde $a^2 = e$, $b^2 = e$. Probar que $N_K(H) =< b^2 >$.

28) Probar que la relación de conjugación entre los subgrupos de un grupo G, define una relación de equivalencia.

29) Sea S_3 el grupo simétrico de orden tres y $H =< \phi >$. Hallar todos los conjugados de H.

30) Dar un ejemplo de un grupo de orden n, que no posea subgrupos de orden d, para algún d divisor de n.

6.5 Grupos Abelianos Finitos

Nos ocuparemos en esta sección de la clasificación de todos los grupos abelianos finitos. Usaremos los resultados obtenidos en la sección de producto directo de grupos y los teoremas de Sylow.

Teorema 6.5.1 *Sea G un grupo abeliano, de orden n, y H, K subgrupos de G de órdenes h y k con $n = hk$ y $(h.k) = 1$. Entonces G es isomorfo a el producto directo $H \times K$.*

Demostración: Sabemos que H y K son subgrupos normales de G, luego HK es un subgrupo de G de orden

$$\circ(HK) = \frac{\circ(H) \circ (K)}{\circ(H \cap K)}$$

Ahora bien, si $x \in H \cap K$ el orden del elemento x es un divisor de h y k. Pero por hipótesis se tiene que el único divisor común de h y k es 1, pues el $(h, k) = 1$. Luego $x = e$, y esto demuestra que

$$H \cap K = \{e\}$$

Entonces tenemos que

$$\circ(HK) = \circ(H) \circ (K) = hk$$

y por lo tanto $HK = G$

Usando el teorema **??** sección **??**, se concluye la demostración.

♠

Sea G un grupo finito abeliano de orden n, y supongamos que n tiene una factorización en primos distintos

$$n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$$

Entonces sabemos, por el teorema de Sylow, que G tiene subgrupos de Sylow P_i de orden p^{α_i}, usando esto y el teorema anterior se tiene:

Teorema 6.5.2 *Si G es un grupo abeliano finito de orden n, entonces G es isomorfo al producto directo $P_1 \times P_2 \times \cdots \times P_t$, donde los P_i son los grupos de Sylow de G.*

Ejemplo: Sea G un grupo abeliano de orden 600. Entonces se tiene

$$300 = 2^3 \times 3 \times 5^2.$$

Sean P_1, P_2 y P_3 subgrupos de Sylow de G de ordenes 8, 3 y 25 respectivamente. Luego se tiene el isomorfismo

$$G \approx P_1 \times P_2 \times P_3 \tag{6.8}$$

La estructura anterior todavía no nos da toda la información sobre el grupo G, pues P_1 es un grupo abeliano de orden 8 y debe ser isomorfo a uno de los grupos

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Sabemos que P_2 es un grupo de orden 3 y por lo tanto isomorfo a $\mathbb{Z}_3$.

Finalmente P_3 es isomorfo a $\mathbb{Z}_{25}$ o bien $\mathbb{Z}_5 \times \mathbb{Z}_5$. Si hacemos todos estas sustituciones para P_1, P_2 y P_3 en la expresión (**??**), nos encontramos con que G es producto directo de grupos cíclicos.

Teorema 6.5.3 *Todo grupo abeliano finito G es suma directa de grupos cíclicos C_i,*

$$G = C_1 \times \cdots \times C_s$$

donde $\circ(G) = \circ(C_1) \cdots \circ (C_s)$.

Demostración: De acuerdo con el teorema anterior, todo grupo G abeliano finito, es producto directo de sus subgrupos de Sylow. Luego el teorema quedará demostrado, si probamos que todo $p-$grupo de orden p^α con p primo, es suma directa de grupos cíclicos.

Esto precisamente lo demostramos a continuación.

♠

Teorema 6.5.4 *Sea G un grupo abeliano de orden p^α, con p primo. Entonces existen subgrupos cíclicos de G, C_i de orden p^{α_i} y tal que $1 \leq i \leq t$*

$$G \approx C_1 \times C_2 \times \cdots \times C_t \tag{6.9}$$

y además

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_t.$$

Los α_i se llaman **los invariantes de** G.

Demostración: Si G mismo es cíclico, entonces no hay nada que probar.

Si G no es cíclico, entonces los elementos de G tienen orden una potencia de p. Elegimos a_1 en G, tal que el orden de a_1 es máximo. Luego $\circ(a_1) = p^{\alpha_1}$, para algún $\alpha_1 \geq 1$.

Definimos $C_1 =< a_1 >$, con lo cual el orden del grupo cíclico C_1 es p^{α_1}.

Sea ahora $\overline{G} = G/C_1$ el cual tiene orden una potencia de p. Por el mismo razonamiento, se puede elegir un elemento $\overline{a_2}$ en $\overline{G}$ tal que el orden de $\overline{a_2}$ es maximal entre los ordenes de los elementos de $\overline{G}$.

Luego existe α_2 tal que

$$\circ(\overline{a_2}) = p^{\alpha_2}$$

Como $a_2^{p^{\alpha_1}} = e$, se tiene que

$$p^{\alpha_1} \geq \circ(a_2) \geq \circ(\overline{a_2}) = p^{\alpha_2}$$

Luego

$$\alpha_1 \geq \alpha_2$$

Ahora consideramos dos casos:

Caso I: Si $< a_1 > \cap < a_2 >= \{e\}$, entonces hacemos $C_2 =< a_2 >$ y de esta manera se tiene un producto directo $C_1 \times C_2$ dentro del grupo G, el cual podemos incrementar paso a paso, hasta obtener, después de un número finito de pasos, una descomposición de G de la forma (**??**).

Caso II: Si $< a_1 > \cap < a_2 >\neq \{e\}$, entonces elegiremos otro elemento en lugar de a_2. Tomemos p^{α_2} la menor potencia de p, tal que

$$a_2^{p^{\alpha_2}} \in < a_1 >= C_1$$

Por lo tanto existe un entero positivo i, tal que

$$a_2^{p^{\alpha_2}} = a_1^i,$$

y entonces se obtiene

$$\begin{aligned}\left(a_1^i\right)^{p^{\alpha_1}{}_1-\alpha_2{}_2} &= \left(a_2^{p^{\alpha_2}}\right)^{p^{\alpha_1-\alpha_2}} \\ &= a_2^{p^{\alpha_1}} \\ &= e\end{aligned}$$

Luego p^{α_1} divide a $i(p^{\alpha_1-\alpha_2})$, y por lo tanto

$$p^{\alpha_2}|i.$$

Luego existe j tal que

$$i = jp^{\alpha_2}$$

Tomemos entonces $b_2 = a_1^{-j}a_2$, el cual satisface

$$\begin{aligned}(b_2)^{p^{\alpha_2}} &= a_1^{-jp^{\alpha_2}}a_2^{p^{\alpha_2}} \\ &= a_1^{-i}a_2^{p^{\alpha_2}} \\ &= e\end{aligned}$$

Además, si para algún t, con $1 \leq t < p^{\alpha_2}$ se tiene

$$(b_2)^t = e,$$

entonces

$$a_1^{-jt}a_2^t = e,$$

y por lo tanto $a_2^t \in C_1$, lo cual es una contradicción, pues $t < p^{\alpha_2}$. Con esto queda demostrado que $\circ(b_2) = p^{\alpha_2}$.

Finalmente probaremos que

$$< a_1 > \cap < b_2 > = \{e\}$$

En efecto, si $x \in < a_1 > \cap < b_2 >$, se tendrá $x = b_2^t \in < a_i >$, para algún $t > 0$. Luego

$$b_2^t = (a_1^{-j} a_2)^t = a_1^{-jt} a_2^t$$

lo cual implica que $a_2^t \in < a_1 >$ y por lo tanto p^{α_2} divide a t.

Luego se tendrá

$$x = b_2^t = e$$

Vemos que el elemento b_2, cumple los requisitos buscados y volviendo al caso I, con $C_2 =< b_2 >$, se concluye la demostración.

♠

Ejemplo: Podemos clasificar todos los grupos abelianos de orden 60, usando los teoremas anteriores. Tenemos que $60 = 2^2 \cdot 3 \cdot 5$. Sean C_i grupos cíclicos de orden i, donde $i = 2, 3, 5$. Entonces si $\circ(G) = 60$ se tienen las siguientes posibilidades.

$$G \approx C_2 \times C_2 \times C_3 \times C_5 \cong C_2 \times C_{30}$$

$$G \approx C_4 \times C_3 \times C_5 \cong C_4 \times C_{15} \cong C_{60}$$

Luego existen solamente dos grupo abelianos de orden 60.

Si G es un grupo abeliano de orden p^n, entonces G es isomorfo a un producto directo

$$G \approx C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$$

donde $n_1 \geq n_2 \geq \cdots \geq n_k > 0$ y

$$\sum_{i=1}^{k} n_i = n.$$

los enteros $n_1, n_2, \ldots, n_k$ son los invariantes del grupo G.

Nuestro próximo objetivo será probar la unicidad de los invariantes de G.

Definición 6.5.1 *Sea G un grupo abeliano. Entonces para todo $s \geq 1$ se define el conjunto*

$$G(s) = \{g \in G \mid g^s = e\}.$$

Ejemplo: Sea $G = C_4 \times C_2$ Entonces $G(2)$ es el grupo formado por los elementos

$$(0,0), \quad (0,1), \quad (2,1), \quad (2,0),$$

mientras que $G(4) = G$ y $G(1) = \{e\}$. Por otro lado,

Si $s \neq 2, 4, 1 \Longrightarrow G(s) = \{e\}$.

Ejemplo: En el caso particular del grupo multiplicativo de los números complejos se tiene

$$G(n) = \{z \in \mathbb{C} \mid z^n = 1\}, \quad n \geq 1.$$

Este es el grupo de las raíces n-ésimas de la unidad.

Observación: Se demuestra que $G(s)$ es un subgrupo de G, para todo $s \geq 1$.

Proposición 6.5.1 *Sean G_1 y G_2 dos grupos isomorfos. Entonces $G_1(s) = G_2(s)$ para todo s entero.*

Demostración: Sea $f : G_1 \longrightarrow G_2$ el isomorfismo dado entre G_1 y G_2.

Sean e_1 y e_2 los elementos neutros de G_1 y G_2 respectivamente. Si $g^s = e_1$ para algún $s \geq 1$, entonces por las propiedades de isomorfismo se tiene $f(g)^s = e_2$. Luego hemos demostrado

$$f(G_1(s)) \subseteq G_2(s)$$

Por otro lado, si $h \in G_2(s)$, entonces $h_2^s = e$. Como la función f es sobre, existe un $g \in G$, tal que $h = f(g)$ y por lo tanto

$$[f(g)]^s = f(g^s) = e_2$$

Como f es inyectiva, se tiene que $g^s = e_1$. Luego hemos probado $f(G_1(s)) \subseteq G_2(s)$, con lo cual se tiene $f(G_1(s)) = G_2(s)$ y por lo tanto $G_1(s)$ y $G_2(s)$ son isomorfos.

Proposición 6.5.2 *Sea $G = C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$, donde p es un primo y cada $C_{p^{n_1}}$ es un grupo cíclico de orden p^{n_i}. Entonces*

$$G(p) = A_1 \times A_2 \times \cdots \times A_k,$$

donde $A_i = \langle x_i \rangle$ y el orden de cada x_i es igual a p.

Demostración: Para cada $1 \leq i \leq k$, sea

$$C_{p^{n_i}} = \langle g_i \rangle,$$

donde g_i es un elemento de G, de orden p^{n_i}.

Sea

$$x_i = g_i^{p^{n_i}-1}$$

para todo $1 \leq i \leq k$.

Entonces $\circ(x_i) = p$. Probaremos que el grupo

$$H = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \langle x_k \rangle.$$

es igual a $G(p)$.

Nótese que $h^p = e$ para todo $h \in H$, y por lo tanto $H \subseteq G(p)$.

Por otro lado sea $x \in G(p) - H$. Entonces debemos tener $x^p = e$. Ahora bien, como $x \in G$ se tiene que existen enteros α_i tales que

$$x = (g_1^{\alpha_1}, \ldots, g_k^{\alpha_k}).$$

Como $x \in H$, existen enteros s y t tales que

$$\alpha_i = p^{n_i-1}s + t,$$

con $0 < t < p^{n_i-1}$, para algún i, $1 \leq i \leq k$.

Luego si $x^p = e$, entonces se tiene $(g_i^{\alpha_i})^p = e$, y por lo tanto:

$$g_i^{ps+pt} = e$$

O sea

$$g_i^{pt} = e,$$

con $0 < pt < p^{n_i}$.

Esto contradice la hipótesis de que $\circ(g_i) = p^{n_i}$.

Por lo tanto

$$G(p) = H = \langle x_1 \rangle \times \cdots \times \langle x_k \rangle.$$

Finalmente, daremos el teorema de las unicidad de los invariantes para un grupo abeliano finito de orden una potencia de p.

♠

Teorema 6.5.5 *Sean G_1 y G_2 dos grupos abelianos finitos de orden p^n y supongamos que tienen descomposiciones*

$$\begin{aligned} G_1 &= C_1 \times C_2 \times \cdots \times C_k \\ G_1 &= C_1' \times C_2' \times \cdots \times C_s' \end{aligned} \tag{6.10}$$

donde C_i es grupo cíclico de orden p^{n_i} y C_i' es un grupo cíclico de orden p^{n_i}, con

$$n_1 \geq n_2 \geq \cdots \geq n_k > 0$$

$$h_1 \geq h_2 \geq \cdots \geq h_s > 0.$$

Entonces $G_1 \approx G_2$ si y sólo si tiene los mismos invariantes, esto es $k = s$ y $n_i = h_i$, para todo $1 \leq i \leq k$.

Demostración:
($\Longrightarrow$) Probaremos que si G_1 y G_2 tienen los mismos invariantes, entonces ellos son isomorfos.

Sean

$$G_1 = C_1 \times \cdots \times C_k$$

$$G_2 = D_1 \times \cdots \times D_k$$

donde C_1 y D_1 son grupos cíclicos de orden p^{n_i} y $n_1 \geq n_2 \geq \cdots n_k > 0$.

Entonces para todo $1 \leq i \leq k$, existen elementos $g_i \in G_i$ y $h_i \in D_i$, tales que

$$G_i = \langle g_i \rangle \quad \text{y} D_i = \langle h_i \rangle$$

Consideremos la aplicación

$$\begin{array}{rccc} \phi \ : & G_1 & \longrightarrow & G_2 \\ & (g_1^{\alpha_1}, \ldots, g_k^{\alpha_k}) & \longrightarrow & (h_1^{\alpha_1}, \ldots, k_k^{\alpha_k}) \end{array}$$

Entonces es fácil demostrar que ϕ es isomorfismo de G_1 en G_2.

($\longleftarrow$) Supongamos que G_1 y G_2 dados como en (**??**) son isomorfos. Entonces por la proposición **??** se tiene

$$G_1(p) = G_2(p)$$

De acuerdo con la proposición **??** se tiene que

$$|G_1(p)| = p^k \quad \text{y} \quad |G_2(p)| = p^s$$

luego $s = k$ y por lo tanto G_1 y G_2 tienen el mismo número de invariantes.

Probaremos ahora que los invariantes son iguales, comenzando por el primero. Si suponemos que $n_1 > h_1$, entonces G_1 tiene elementos de orden p^{n_1}, pues el máximo orden de los elementos de G_2 es p^{h_1}. Luego

G_1 y G_2 no pueden ser isomorfos y esto nos lleva a una contradicción. Luego $n_1 = h_1$, lo cual implica que $C_1 \approx C_1'$ en (**??**) .

Si hacemos entonces

$$H = C_2 \times C_3 \times \cdots \times C_k$$

$$K = C_2' \times C_3' \times \cdots \times C_k'$$

es fácil verificar entonces que H es isomorfo a K. Luego podemos aplicar inducción sobre el número de invariantes, se concluye entonces que

$$n_2 = h_2, \ldots, n_k = h_k$$

Con esto queda demostrado que $n_i = h_i$, $1 \leq i \leq k$.

♠

Ejercicios

1) Sea $G = C_{12}$ el grupo cíclico de orden 12. Hallar los subgrupos $G(2)$, $G(4)$ y $G(3)$.

2) Hallar todos los posibles grupos abelianos de orden 200.

3) Demuestre que el número de grupos de orden p^α, no isomorfos, con p un número primo es igual al número de particiones de α.

4) Hallar todos los posibles grupos abelianos de orden 32.

5) Probar que si un grupo finito abeliano G tiene subgrupos de ordenes p y q, con p y q primos diferentes, entonces G tiene un subgrupo de orden pq.

6) Probar que si un grupo finito abeliano tiene orden mn, entonces tiene un subgrupo de orden el mínimo común multiplo de m y n.

7) Sea G un grupo abeliano finito de orden pq con p y q números primos. Probar que todos los subgrupos de G son característicos.

8) Sea G un grupo abeliano finito de orden 5^5 con invariante: $3 > 2 > 0$. ¿Cuántos elementos de orden 5^3 hay en G?

9) Calcule el número de subgrupos de un grupo de orden p^s con invariantes $s - 1 > 1 > 0$.