Proposición 3.2.7. Sea $(G, *)$ un grupo. Las siguientes propiedades son equivalentes:

i) $(G, *)$ es abeliano.
ii) $(a * b)^{-1} = a^{-1} * b^{-1}$ para todo $a, b \in G$.

Demostración. Si $(G, *)$ es abeliano, utilizando la proposición 3.2.6 deducimos $(a * b)^{-1} = b^{-1} * a^{-1} = a^{-1} * b^{-1}$ para todo $a, b \in G$, lo cual demuestra que i) implica ii). Supongamos ahora que ii) es cierta y sean $x, y \in G$. Tenemos

$$x * y = (x^{-1})^{-1} * (y^{-1})^{-1} \quad \text{(proposición 3.2.5)}$$

$$= (x^{-1} * y^{-1})^{-1} \quad \text{(hipótesis)}$$

$$= (y^{-1})^{-1} * (x^{-1})^{-1} \quad \text{(proposición 3.2.6)}$$

$$= y * x \quad \text{(proposición 3.2.5)}$$

Esto demuestra que $(G, *)$ es abeliano. ■

Si $(G, *)$ es un grupo y G posee un número finito de elementos se define el **orden de G**, que se simboliza mediante $|G|$, como el número de elementos de G y se dice que $(G, *)$ es un grupo finito. En caso contrario diremos que $(G, *)$ es un grupo infinito.

Los grupos finitos pueden definirse totalmente mediante tablas, de manera que el resultado de operar dos elementos a y b del grupo se coloca en la intersección de la fila de a con la columna de b, como muestra la siguiente figura:

$*$		b	
a		$a * b$	

La ley de cancelación por la derecha se interpreta en la tabla de la operación como que los elementos no se repiten en ninguna de las columnas y la ley de cancelación por la izquierda como que los elementos no se repiten en ninguna de las filas de la tabla de la operación.

Teniendo esto en cuenta y que el neutro siempre debe aparecer en la tabla de un grupo, se deduce que todos los grupos de dos elementos poseen una tabla de operación similar a la siguiente:

$*$	e	a
e	e	a
a	a	e

Puede observarse que este grupo es conmutativo; la propiedad de conmutatividad se observa en la tabla de la operación viendo si la tabla es simétrica con respecto a la diagonal principal.

Si G posee tres elementos, G = {e, a, b}, inmediatamente podemos escribir

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

El resultado de operar a con a puede ser b o e; el resultado de operar a con b debe de ser e (si fuera b, se tendría a = e); por tanto a * a = b; se puede ahora completar la tabla de este grupo:

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Obsérvese que este grupo también es abeliano.

Un ejemplo de un grupo con cuatro elementos es el grupo S = {1, i, −1, −i}, $i^2 = -1$, con la operación de multiplicación, dado en la sección 3.1, en donde se ha escrito su tabla de operación. En el ejercicio 5 al final de esta sección se pide comprobar que "esencialmente" sólo existe otro grupo de cuatro elementos y que también es abeliano.

EJERCICIOS 3.2

1. Justificar cuáles de las siguientes operaciones son asociativas y cuáles son conmutativas

   a) En $\mathbf{R}$, a * b = |a|b.
   b) En $\mathbf{Z}$, a * b = a + b + b^2
   c) En $\mathbf{Z}$, a * b = a + b + ab

2. Tomar G = $\mathbf{R}$ − {0} = $\mathbf{R}^*$ y la operación * definida por a * b = 3ab. Encontrar un elemento identidad en (G, *). Encontrar el inverso de cualquier elemento x de G. ¿Es (G, *) un grupo?

3. Tomar G = $\mathbf{R}$ − {−1} y la operación a * b = a + b + ab. ¿Es (G, *) un grupo? Encontrar x ∈ G tal que 2 * x * 3 = 35.

4. En un grupo $(G, *)$ definimos $a^2 = a * a$, $a^3 = a * a * a$, ..., $a^n = a * \ldots * a$ (n veces).

   i) Para todo $n \in \mathbb{Z}^+$, demostrar que $(a^n)^{-1} = (a^{-1})^n$.

   ii) Si G es abeliano, demostrar que $(a * b)^n = a^n * b^n$. (Utilizar el método de demostración por inducción.)

5. Encontrar las tablas de todos los grupos de cuatro elementos (seguir un procedimiento análogo al utilizado con los grupos de 2 y de 3 elementos).

6. Completar la siguiente tabla de manera que sea la tabla de un grupo. (Será necesario utilizar la propiedad asociativa.) ¿Es este grupo abeliano?

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

7. Demostrar que $(G, *)$ es abeliano si y sólo si $(ab)^2 = a^2b^2$ para todo $a, b \in G$.

8. Si G es un grupo tal que $x^2 = e$ para todo $x \in G$, demostrar que G es abeliano.

9. Probar que $x^n = e$ si y sólo si $(y^{-1}xy)^n = e$. (Sugerencia: probar primero que $(y^{-1}xy)^n = y^{-1}x^ny$ utilizando el método de inducción.)

10. Probar que los siguientes conjuntos forman grupos respecto a la multiplicación ordinaria

    a) $\{(1 + 2m)/(1 + 2n): m, n = 0, \pm1, \pm2, \ldots\}$

    b) $\{\cos q + i \operatorname{sen} q: q \in \mathbb{Q}\}$.

11. Si $b^{-1}ab = a^k$, demostrar que $b^{-r}a^sb^r = a^{sk^r}$.

3.3. GRUPOS DE CONGRUENCIAS

Dado un número entero positivo m, mostraremos que siempre existe al menos un grupo con m elementos. Para ello haremos uso del concepto de congruencia introducido en el capítulo 2. Recordemos que dados dos números enteros a y b, a se dice **congruente con** b **módulo** m, y se simboliza mediante $a \equiv b(m)$ si su diferencia, $a - b$, es un múltiplo de m,

es decir, $a - b = km$ para algún $k \in \mathbb{Z}$. Se sabe que la relación de congruencia definida en el conjunto $\mathbb{Z}$ de los números enteros es una relación de **equivalencia**. Podemos, por tanto, considerar el **conjunto cociente** de $\mathbb{Z}$ mediante esta relación de equivalencia, el cual se simboliza mediante $\mathbb{Z}_m$ y se denomina el **conjunto de las clases de congruencias módulo m.**

Los elementos del conjunto $\mathbb{Z}_m$ son, pues, clases de equivalencia que se denotarán mediante [a], donde $[a] = \{b \in \mathbb{Z} : b \equiv a\ (m)\}$. Dada una clase de equivalencia $[a] \in \mathbb{Z}_m$ siempre podremos elegir un "representante" b de [a], de manera que $[a] = [b]$ y $0 \leq b < m$; basta dividir a entre m y tomar b como el resto de esta división (véase el algoritmo de la división desarrollado en la proposición 2.1.1). Entonces, podemos escribir

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

donde $\{0, 1, 2, \ldots, m-1\}$ es un sistema completo de restos módulo m.

En el teorema 2.4.4 se demostró que las operaciones

$$[a] + [b] = [a + b] \qquad \text{y} \qquad [a] \cdot [b] = [ab]$$

están bien definidas en $\mathbb{Z}_m$ y son operaciones cerradas en este conjunto. Con la operación de suma de clases residuales módulo m, $(\mathbb{Z}_m, +)$ es un grupo abeliano, como se demostró en el teorema 2.4.4. Queda así demostrado que para todo entero positivo m siempre existe un grupo con m elementos.

Con la operación de multiplicación de clases residuales módulo m, $(\mathbb{Z}_m, \cdot)$ no es un grupo; basta observar que el elemento [0] no posee inverso. Podríamos preguntarnos si eliminando el [0], es decir considerando $\mathbb{Z}_m^* = \mathbb{Z}_m - \{[0]\}$, $\mathbb{Z}_m^*$ es un grupo con respecto a la multiplicación de clases residuales módulo m. La respuesta es, en general, negativa puesto que ni [2], ni [3], ni [4] poseen inverso en $(\mathbb{Z}_6^*, \cdot)$. En general, si $m = s \cdot r$ con $s, r \in \mathbb{Z}$, $s, r > 1$, se tiene que $[s] \cdot [r] = = [m] = [0]$ en $\mathbb{Z}_m$; esto sugiere que $(\mathbb{Z}_m^*, \cdot)$ será un grupo solamente cuando m sea primo.

Proposición 3.3.1. Para todo número entero positivo primo p, $(\mathbb{Z}_p^*, \cdot)$ es un grupo abeliano con $p - 1$ elementos.

Demostración. Ya se ha demostrado en el teorema 2.4.4 que la operación $\cdot$ está bien definida en $\mathbb{Z}_p$, y en particular en $\mathbb{Z}_p^*$. Para demostrar que es cerrada es suficiente demostrar que dados $[a], [b] \in \mathbb{Z}_p^*$, el caso $[a] \cdot [b] = [0]$ es imposible. En efecto, si suponemos que $[a] \cdot [b] = = [0]$, deducimos que $ab = kp$ para algún $k \in \mathbb{Z}$; entonces p divide a $a \cdot b$, y como p es primo, el lema 2.3.2 nos permite deducir que $p \mid a$ o $p \mid b$; se tendría entonces que $[a] = [0]$ o $[b] = [0]$ en contra de la hipótesis de que $[a], [b] \in \mathbb{Z}_p^*$. La clase residual [1] es el elemento neutro. El resto de las afirmaciones de la proposición son fáciles de comprobar, excepto quizá la existencia del elemento inverso de cualquier elemento del conjunto. Para probar esto sea $[a] \in \mathbb{Z}_p^*$ y observar que el máximo común divisor de a y p es 1; por la propiedad lineal del máximo común divisor (véase corolario 2.2.3), existen $m, n \in \mathbb{Z}$ tales que $1 = ma + np$; de aquí se deduce que

$$[1] = [m][a] + [n][p] = [m][a]$$

y por tanto m es el inverso de a en $(\mathbb{Z}_p^*, \cdot)$, puesto que $(\mathbb{Z}_p^*, \cdot)$ tiene la propiedad conmutativa. ■

El recíproco de la proposición anterior también es cierto. Concretamente, si $(\mathbf{Z}_m^*, \cdot)$ es un grupo, entonces m debe de ser primo. Esto puede demostrarse mediante el método de reducción al absurdo, siguiendo las ideas expuestas antes de la proposición 3.3.1. En efecto, si m fuera compuesto, existirían dos números enteros positivos distintos de 1 tales que rs = m; entonces $[r] \cdot [s] = [m] = [0]$ en $\mathbf{Z}_m$ y la operación de multiplicación de clases no sería cerrada en $(\mathbf{Z}_m^*,)$.

3.4. EL GRUPO DE LAS BIYECCIONES DE UN CONJUNTO. GRUPOS DE PERMUTACIONES

Dado un conjunto A, llamamos B(A) al conjunto de todas las biyecciones del conjunto A en sí mismo. Si f y g son dos aplicaciones biyectivas del conjunto A en sí mismo, puede comprobarse que $g \circ f$ es también una aplicación biyectiva de A en sí mismo, donde $\circ$ denota la composición de aplicaciones. En efecto, si x, y $\in$ A y se tiene $g \circ f(x) = g \circ f(y)$, esto es equivalente a escribir g(f(x)) = g(f(y)); como g es inyectiva, f(x) = f(y); como f es inyectiva, x = y, y esto demuestra que $g \circ f$ es inyectiva. Para demostrar que $g \circ f$ es suprayectiva, basta tomar z $\in$ A y observar que existe y $\in$ A tal que g(y) = z; como f es suprayectiva existe x $\in$ A tal que f(x) = = y. Sustituyendo en la igualdad anterior obtenemos g(f(x)) = z, que es el resultado deseado.

Esto prueba que la operación de composición de aplicaciones es cerrada en el conjunto B(A). La siguiente proposición demuestra que el conjunto B(A) con la operación de composición es un grupo.

Proposición 3.4.1. Dado un conjunto A, $(B(A), \circ)$ es un grupo.

Demostración. Ya se ha demostrado anteriormente que la composición de aplicaciones es cerrada en B(A) y se demuestra fácilmente que es asociativa. La aplicación identidad de A en A, que denotamos por I_A, es el elemento neutro. Finalmente, si f $\in$ B(A), su inversa, f^{-1} es también un elemento de B(A); en efecto, si $f^{-1}(x) = f^{-1}(y)$, tenemos que $f(f^{-1}(x)) = f(f^{-1}(y))$ de donde se deduce que x = y, y por tanto f^{-1} es inyectiva; además si y $\in$ A, el elemento x = f(y) satisface $f^{-1}(x) = f^{-1}(f(y)) = y$, con lo que f^{-1} es también suprayectiva. Como la definición de f^{-1} implica

$$f^{-1} \circ f(x) = f \circ f^{-1}(x)$$

para todo x $\in$ A, queda demostrada la proposición. ■

Cuando el conjunto A es el conjunto de los n primeros números naturales, los elementos de B(A) se denominan **permutaciones de n elementos**; el conjunto de las permutaciones de n elementos se simboliza mediante S_n y el grupo $(S_n, \circ)$ se llama **el grupo simétrico de n ele-**

mentos. Un elemento de S_n queda determinado si se conocen las imágenes de los n primeros números naturales; así, si $\alpha \in S_n$, α puede escribirse de la forma

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}$$

y la operación de composición de permutaciones se escribirá $\circ$, o simplemente se omitirá este símbolo; escribiremos pues $\beta \circ \alpha$ o $\beta\alpha$ para indicar $\beta \circ \alpha$, cuando $\alpha, \beta \in S_n$.

★★ EJEMPLO A. Sean α y β dos permutaciones de S_3 dadas por

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Entonces

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

mientras que

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Se urge al lector a que observe que $\beta\alpha$ es una composición de aplicaciones y como tal se comienza operando con α y a continuación β; también es conveniente que el lector se anime a hacer más ejemplos de su propia cosecha, para familiarizarse con esta operación.

El ejemplo que acabamos de realizar muestra que $(S_3, \circ)$ es un grupo **no abeliano**; puede demostrarse que $(S_2, \circ)$ es un grupo abeliano, mientras que $(S_n, \circ)$ es un grupo **no** abeliano si $n \geq 3$. Observar también que el número de elementos de S_n es n!.

Escribiremos la tabla del grupo $(S_3, \circ)$. La permutación que deja fijos todos los elementos del conjunto $\{1, 2, 3\}$ se simboliza mediante I:

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Se tienen además los elementos

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \alpha' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

que intercambian todos los elementos, y

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \beta' = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \beta'' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

que dejan fijo un elemento e intercambian los dos restantes entre sí. Entre estos elementos se tienen las siguientes relaciones:

$$\alpha^2 = \alpha\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \alpha'$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \beta'$$

$$\alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta''$$

Se tiene además que $\alpha^3 = I$, $\beta^2 = I$ y $\beta\alpha = \alpha^2\beta$. Estas relaciones determinan completamente la tabla del grupo de permutaciones de 3 elementos, que es la siguiente:

$\circ$	I	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
I	I	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	I	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	I	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	I	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	I	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	I

En la sección 4.8 del próximo capítulo se estudiarán más detenidamente los grupos de permutaciones de n elementos.

3.5. GRUPOS DE MATRICES

Sea $M_2(\mathbb{R})$ el conjunto de todas las matrices de orden 2 cuyos elementos son números reales, en el cual se define la operación

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

para todo par de matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ de $M_2(\mathbf{R})$. Puede probarse fácilmente que **$(M_2(\mathbf{R}), +)$ es un grupo abeliano**. Si a la matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{R})$ le asociamos la aplicación lineal $T_A : \mathbf{R}^2 \to \mathbf{R}^2$ dada por

$$T_A\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

se tiene que el conjunto $M_2(\mathbf{R})$ está en correspondencia biyectiva con el conjunto de las aplicaciones lineales de $\mathbf{R}^2$ en $\mathbf{R}^2$; además

$$T_{A+B}\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = (A + B)\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix} + B\begin{pmatrix} x \\ y \end{pmatrix} = (T_A + T_B)\left(\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

Debido a esta igualdad se obtiene que el **conjunto de las aplicaciones lineales de $\mathbf{R}^2$ en $\mathbf{R}^2$ con la operación + es un grupo abeliano**.

Con respecto a la multiplicación de matrices el conjunto $M_2(\mathbf{R})$ no es un grupo; el inverso de una matriz $A \in M_2(\mathbf{R})$ sólo está definido si su determinante es distinto de cero, es decir $\det A \neq 0$. Esto nos lleva a considerar el subconjunto de $M_2(\mathbf{R})$ formado por las matrices A tales que $\det A \neq 0$, al cual denominamos $GL_2(\mathbf{R})$.

Proposición 3.5.1. El conjunto $GL_2(\mathbf{R})$, de todas las matrices de orden 2 con coeficientes reales cuyo determinante es distinto de cero, es un grupo con respecto a la multiplicación de matrices.

Demostración. La operación de multiplicación de matrices es cerrada en $GL_2(\mathbf{R})$ ya que el producto de dos matrices con determinante no nulo es otra matriz cuyo determinate es no nulo. La demostración de la propiedad asociativa es un ejercicio de cálculo. El elemento identidad es la matriz

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Finalmente, dada una matriz $A \in GL_2(\mathbf{R})$, su inversa es otra matriz A^{-1}, cuyo determinante es el inverso del determinante de la matriz A, y por tanto no nulo. ■

★★ EJEMPLO A. El conjunto $GL_2(\mathbf{R})$ con respecto a la multiplicación de matrices es un grupo **no abeliano.** Basta observar que

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix},$$

mientras que

$$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}$$

La demostración de que la multiplicación de matrices tiene la propiedad asociativa puede simplificarse si se asocia a cada matriz $A \in GL_2(\mathbf{R})$ la aplicación T_A como se definió anteriormente. Puesto que

$$T_{AB}\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = AB\begin{pmatrix} x \\ y \end{pmatrix} = T_A\left(B\begin{pmatrix} x \\ y \end{pmatrix}\right) = (T_A \, T_B)\left(\begin{pmatrix} x \\ y \end{pmatrix}\right),$$

para todo par de matrices $A, B \in GL_2(\mathbf{R})$, la asociatividad de la composición de funciones prueba la asociatividad de la multiplicación de matrices.

★★ EJEMPLO B. Se muestran a continuación otros ejemplos de grupos de matrices. La demostración de que cada uno de ellos cumple las cuatro propiedades requeridas para ser grupo se deja como ejercicio para el final de este capítulo. Son el grupo **especial lineal**

$$SL_2(\mathbf{R}) = \{A \in GL_2(\mathbf{R}) : \det A = 1\},$$

el grupo de las matrices **ortogonales de orden 2**

$$O_2(\mathbf{R}) = \{A \in GL_2(\mathbf{R}) : AA^t = I\},$$

donde A^t denota la matriz traspuesta de A, y el grupo **ortogonal especial de las matrices de orden** 2,

$$SO_2(\mathbf{R}) = O_2(\mathbf{R}) \cap SL_2(\mathbf{R}),$$

todos ellos con la operación de multiplicación de matrices.

Todos los resultados de los ejemplos A y B se extienden sin dificultad a matrices de orden n con coeficientes reales, obteniéndose los grupos $(GL_n(\mathbf{R}), \cdot)$, $(SL_n(\mathbf{R}), \cdot)$, $(O_n(\mathbf{R}), \cdot)$ y $(SO_n(\mathbf{R}), \cdot)$, que reciben los mismos nombres que los correspondientes para $n = 2$.

3.6. GRUPOS LIGADOS A CONFIGURACIONES GEOMÉTRICAS PLANAS

Llamamos **movimiento** en un plano a toda transformación del plano en sí mismo que conserva las distancias. Las traslaciones, las rotaciones, las simetrías con respecto a una recta y las simetrías deslizantes (entendemos por estas últimas la composición de una simetría con una traslación paralela al eje de simetría) son ejemplos de movimientos en el plano. Estos son todos los movimientos en el plano (una demostración de este resultado puede verse en el capí-

tulo 10 del libro "Algebra y Geometría", E. Hernández, Addison-Wesley Iberoamericana y Universidad Autónoma de Madrid, 1994).

Dado un conjunto A del plano, llamamos S(A) al conjunto de todos los movimientos del plano que dejan A invariante, es decir, el conjunto de los movimientos M del plano que satisfacen M(A) = A. La letra S, que aparece en el símbolo S(A), se debe a que este conjunto se llama el **conjunto de las simetrías de A.** Las simetrías de la figura A se reflejan en el tamaño de este grupo: cuanto más elementos tiene el grupo, mayor simetría tiene la figura.

Proposición 3.6.1. El conjunto de las simetrías de un conjunto A del plano es un grupo con la composición de movimientos.

Demostración. La composición de simetrías de A es una operación cerrada en S(A), ya que si R y S son elementos de S(A) se tiene que $R \circ S(A) = R(S(A)) = R(A) = A$, y por tanto $R \circ S$ es también un elemento de S(A). La propiedad asociativa la cumple este grupo ya que se cumple para la composición de funciones. El movimiento Identidad es el neutro y si R es un elemento de S(A), R^{-1} también lo es ya que $R^{-1}(A) = R^{-1}(R(A)) = R^{-1} \circ R(A) = A$. ■

★★ EJEMPLO A. Consideremos el conjunto de las simetrías de un triángulo equilátero. Hay 3 rotaciones alrededor de su centro, incluyendo la identidad, que transforman el triángulo en sí mismo: éstas son rotaciones alrededor del origen de ángulos 0, $2\pi/3$ y $4\pi/3$, a las cuales simbolizaremos mediante I, A y A^2, respectivamente (véase la ilustración 2).

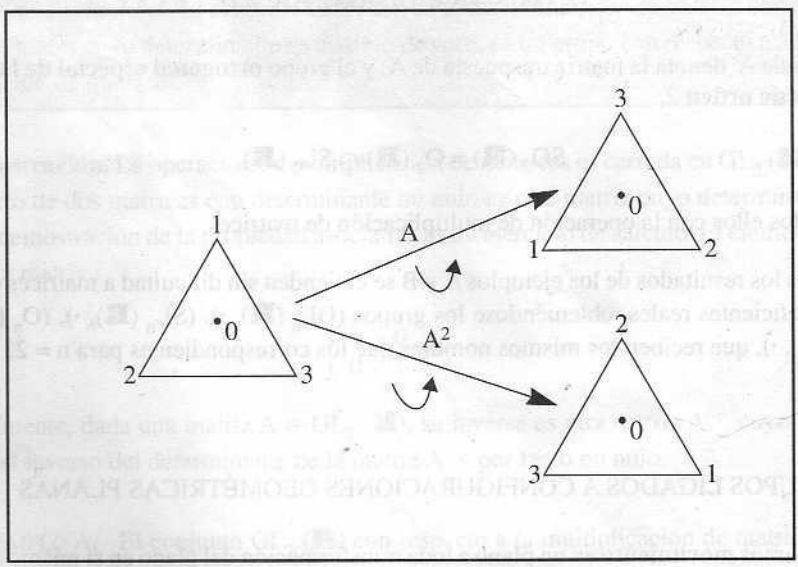


Ilustración 2. Rotaciones que dejan invariante un triángulo equilátero

Obsérvese que $A^3 = I$. Otros nuevos elementos que dejan invariante un triángulo equilátero son las simetrías con respecto a rectas que pasan por el centro y por cada

uno de los vértices del triángulo, como se muestra en la ilustración 3, y que se simbolizan mediante B_i, i = 1, 2, 3.

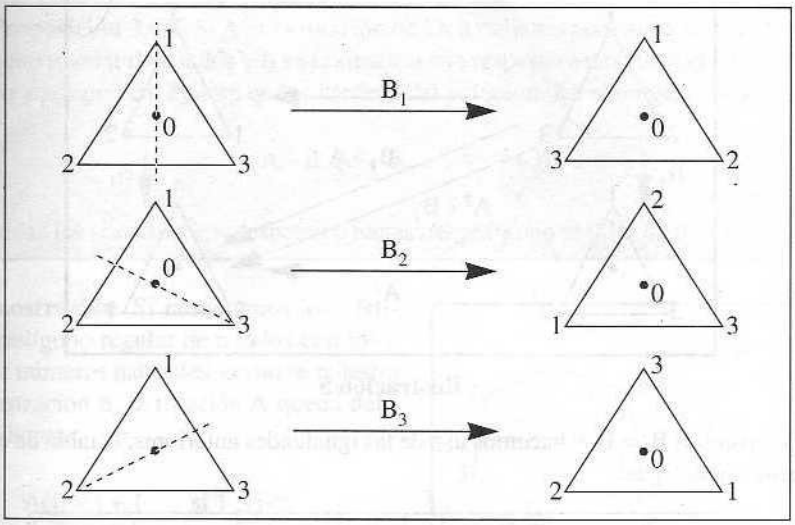


Ilustración 3. Simetrías de un triángulo equilátero

Se tiene que $B_i^2 = I$, i = 1, 2, 3. Estos son todos los movimientos que llevan el triángulo equilátero a coincidir consigo mismo. Observar que

$$A \circ B_1 = B_2 \qquad \text{y} \qquad A^2 \circ B_1 = B_3 ,$$

como se muestra en la ilustración 4.

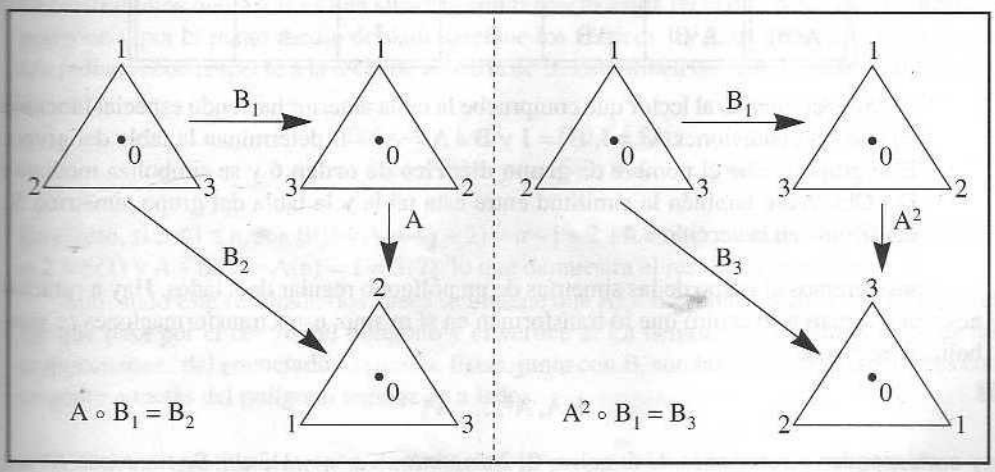


Ilustración 4. Composición de simetrías de un triángulo equilátero

Se tiene, además, que $B_1 \circ A = A^2 \circ B_1$ como se observa en la ilustración 5.

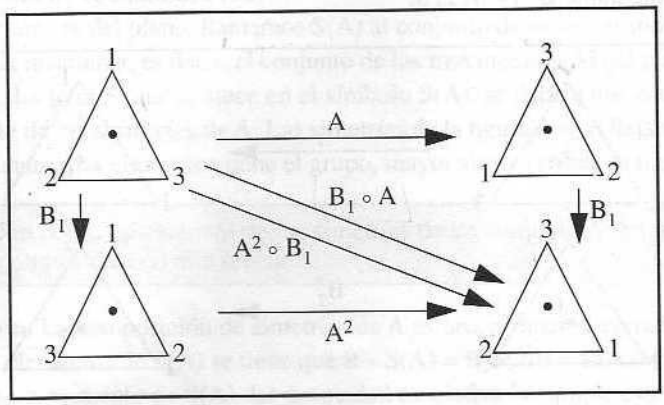


Ilustración 5

Si escribimos $B_1 = B$, y hacemos uso de las igualdades anteriores, la tabla de este grupo queda como sigue:

$\circ$	I	A	A^2	B	AB	A^2B
I	I	A	A^2	B	AB	A^2B
A	A	A^2	I	AB	A^2B	B
A^2	A^2	I	A	A^2B	B	AB
B	B	A^2B	AB	I	A^2	A
AB	AB	B	A^2B	A	I	A^2
A^2B	A^2B	AB	B	A^2	A	I

Se recomienda al lector que compruebe la tabla anterior haciendo especial hincapié en que las condiciones $A^3 = I$, $B^2 = I$ y $B \circ A = A^2 \circ B$ determinan la tabla del grupo. Este grupo recibe el nombre de **grupo diédrico de orden 6** y se simboliza mediante D_6. Obsérvese también la similitud entre esta tabla y la tabla del grupo simétrico S_3 construida en la sección 3.4.

Consideremos el grupo de las simetrías de un polígono regular de n lados. Hay n rotaciones con respecto a su centro que lo transforman en sí mismo; estas transformaciones se simbolizan mediante

$$I, A, A^2, \ldots, A^{n-1}$$

y corresponden a rotaciones de ángulos $0, 2\pi/n, 4\pi/n, \ldots, (n-1)2\pi/n$. Se tiene que $A^n = I$ puesto que A^n corresponde a una rotación de ángulo 2π. Otro movimiento nuevo, B, es una

simetría con respecto a una recta que pase por el centro del polígono y por uno de sus vértices. El resto de los movimientos se obtienen en la proposición siguiente.

Proposición 3.6.2. Si A es la rotación de $2\pi/n$ radianes con respecto al centro de un polígono regular de n lados y B es la simetría con respecto a una recta que pasa por este centro y por uno cualquiera de los vértices del polígono, las composiciones

$$A \circ B, A^2 \circ B, \ldots, A^{n-1} \circ B$$

son todas las simetrías con respecto a rectas del polígono regular de n lados.

Demostración. Si numeramos los vértices del polígono regular de n lados con los n primeros números naturales, como se muestra en la ilustración 6, la rotación A queda definida mediante:

$$A(j) = j + 1 \qquad \text{si } 1 \leq j < n$$
$$A(n) = 1.$$

La simetría B queda definida mediante:

$$B(j) = n - j + 2 \qquad \text{si } 1 < j \leq n$$
$$B(1) = 1.$$

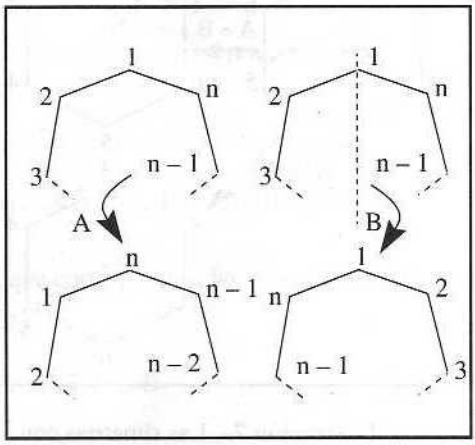


Ilustración 6

Demostraremos que $A \circ B$ es una simetría con respecto a una recta que pasa por el centro del polígono y por el punto medio del lado que une los vértices 1 y 2, es decir, una recta girada π/n radianes con respecto a la recta de simetría de B. Esta simetría S queda definida mediante:

$$S(j) = n - j + 3 \qquad \text{si } 3 \leq j \leq n$$
$$S(1) = 2 \quad \text{y} \quad S(2) = 1.$$

En efecto, si $3 \leq j \leq n$, $A \circ B(j) = A(n - j + 2) = n - j + 2 + 1 = S(j)$; además, $A \circ B(1) = A(1) = 2 = S(1)$ y $A \circ B(2) = A(n) = 1 = S(2)$, lo que demuestra el resultado deseado.

Aplicando este resultado dos veces se obtiene que $A^2 \circ B$ es una simetría con respecto al eje que pasa por el centro del polígono y el vértice 2. La demostración para el resto de las composiciones del enunciado es similar. Estas, junto con B, son las n simetrías diferentes con respecto a rectas del polígono regular de n lados. ■

Observar que las simetrías descritas en la proposición anterior corresponden a simetrías respecto a rectas que pasan por el centro y por cada uno de los vértices o por el

centro y por los puntos medios de lados opuestos. El caso n = 6 se muestra en la ilustración 7.

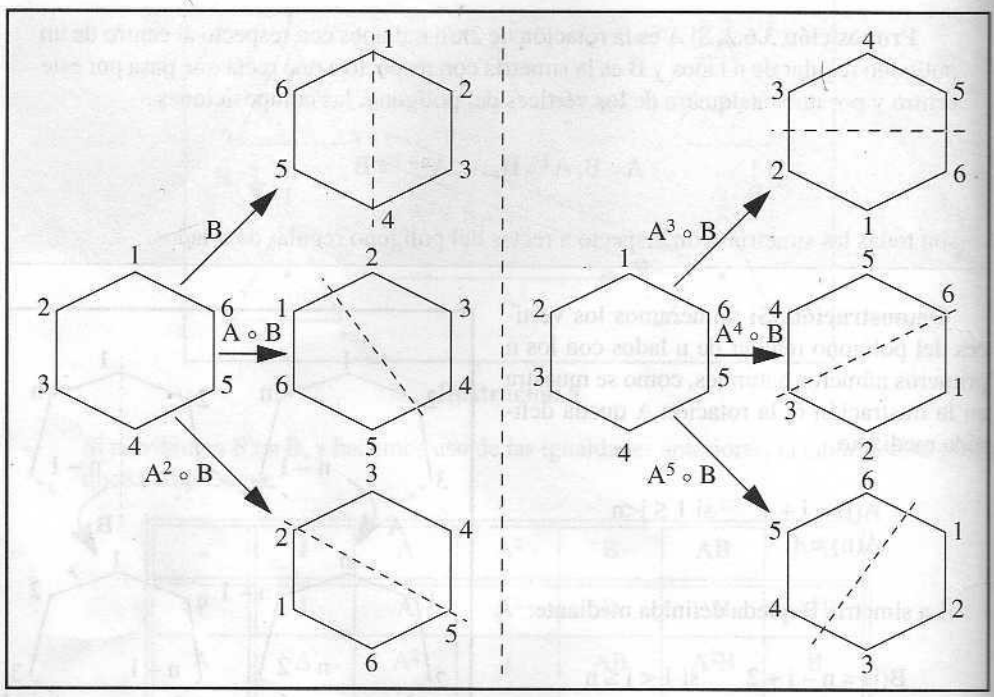


Ilustración 7. Las simetrías con respecto a rectas de un hexágono regular

El grupo de las simetrías de un polígono regular de n lados recibe el nombre de **grupo diédrico de orden 2n**, y se simboliza mediante D_{2n}. Contiene los elementos

$$\{ I, A, A^2, \ldots, A^{n-1}, B, A \circ B, A^2 \circ B, \ldots, A^{n-1} \circ B \}.$$

La siguiente proposición nos ayudará a confeccionar la tabla de los grupos diédricos.

Proposición 3.6.3. Si A es una rotación de $2\pi/n$ radianes alrededor del centro de un polígono regular de n lados y B es una simetría con respecto a una recta que pasa por el centro y por uno de los vértices del polígono se tiene que

$$B \circ A = A^{-1} \circ B$$

Demostración. En la demostración de esta proposición usamos las mismas definiciones de A y B que en la demostración de la proposición 3.6.2. Observar que A^{-1} queda definida mediante:

$$A^{-1}(j) = j - 1 \quad \text{si } 2 \leq j \leq n$$
$$A^{-1}(1) = n.$$

Si $2 \le j < n$, $B \circ A(j) = B(j+1) = n - (j+1) + 2 = n - j + 1$ y $A^{-1} \circ B(j) = A^{-1}(n - j + 2) = n - j + 2 - 1 = n - j + 1$. Se dejan para el lector los casos $j = 1$ y $j = n$ que son fáciles de comprobar con las definiciones. ■

Para completar la tabla del grupo diédrico de orden $2n$ es suficiente observar que $A^{-1} = A^{n-1}$, ya que $A^n = I$, por lo que usando la proposición anterior se obtiene

$$B \circ A = A^{n-1} \circ B .$$

El resto de las posibles operaciones entre los elementos de este grupo pueden deducirse de esta relación y de las igualdades $A^n = I$ y $B^2 = I$; así, por ejemplo,

$$B \circ A^2 = (B \circ A) \circ A = (A^{n-1} \circ B) \circ A = A^{2n} \circ A^{-2} \circ B = A^{-2} \circ B = A^{n-2} \circ B$$

y si $j = 3, 4, \ldots, n-1$,

$$B \circ A^j = A^{n-1} \circ B \circ A^{j-1} = A^{2(n-1)} \circ B \circ A^{j-2} = \ldots = A^{j(n-1)} \circ B = A^{-j} \circ B = A^{n-j} \circ B$$

★★ EJEMPLO B. El grupo diédrico de orden 8, que corresponde a las simetrías de un cuadrado, tiene los siguientes elementos

$$I, A, A^2, A^3, B, A \circ B, A^2 \circ B, A^3 \circ B,$$

de los que el lector debe encontrar su significado geométrico. Su tabla de composición es la siguiente:

$\circ$	I	A	A^2	A^3	B	AB	A^2B	A^3B
I	I	A	A^2	A^3	B	AB	A^2B	A^3B
A	A	A^2	A^3	I	AB	A^2B	A^3B	B
A^2	A^2	A^3	I	A	A^2B	A^3B	B	AB
A^3	A^3	I	A	A^2	A^3B	B	AB	A^2B
B	B	A^3B	A^2B	AB	I	A^3	A^2	A
AB	AB	B	A^3B	A^2B	A	I	A^3	A
A^2B	A^2B	AB	B	A^3B	A^2	A	I	A
A^3B	A^3B	A^2B	AB	B	A^3	A^2	A	I

EJERCICIOS PARA LAS SECCIONES 3.3, 3.4, 3.5 Y 3.6

1. Escribir las tablas de los grupos $(\mathbf{Z}_6, +)$ y $(\mathbf{Z}_7^*, \cdot)$.
2. Calcular $[0] + [1] + [2] + \ldots + [n-1]$ en $(\mathbf{Z}_n, +)$, comenzando con los casos $n = 2, 3, 4$ y 5.
3. Dadas

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix},$$

ambas permutaciones de S_6, calcular α^2, α^{21}, β^3 y $\alpha^3\beta^6$.

4. Demostrar que los conjuntos $SL_2(\mathbf{R})$, $O_2(\mathbf{R})$ y $SO_2(\mathbf{R})$ definidos en la sección 3.5 tienen estructura de grupo con respecto a la multiplicación de matrices.
5. Demostrar que existe una correspondencia biunívoca entre los elementos de $SO_2(\mathbf{R})$ y los elementos del conjunto

$$R = \left\{ \begin{pmatrix} \cos\alpha & \operatorname{sen}\alpha \\ -\operatorname{sen}\alpha & \cos\alpha \end{pmatrix} : 0 \le \alpha < 2\pi \right\}$$

(es decir, este conjunto está en correspondencia biunívoca con el conjunto de las rotaciones del plano en sentido positivo con respecto al origen).

6. Escribir la tabla del grupo diédrico de 10 elementos.
7. En el grupo diédrico de $2n$ elementos, encontrar el inverso de cada uno de sus elementos.
8. Demostrar que si $(G, *)$ es un conjunto finito y G tiene una operación binaria cerrada y asociativa $*$ tal que $x * a = x * b \Rightarrow a = b$ y $a * x = b * x \Rightarrow a = b$, entonces $(G, *)$ es un grupo.
9. Probar que el conjunto de todas las matrices

$$A_v = (1 - v^2)^{-1/2} \begin{pmatrix} 1 & -v \\ -v & 1 \end{pmatrix}$$

donde $v \in (-1, 1)$, forman un grupo con respecto a la multiplicación de matrices (Este grupo recibe el nombre de grupo de Lorentz y desempeña un papel importante en la teoría de la relatividad). (Sugerencia: demostrar que $A_{v_1} A_{v_2} = A_{v_3}$ donde $v_3 = (v_1 + v_2)/(1 + v_1 v_2)$.

10. Sea el conjunto Γ formado por las siguientes funciones:

$$\varphi_1(z) = z, \quad \varphi_2(z) = 1/(1-z), \quad \varphi_3 = (z-1)/z,$$

$$\varphi_4(z) = 1/z, \quad \varphi_5(z) = 1 - z, \quad \varphi_6 = z/(z-1)$$

donde cada función depende de la variable compleja z. Escribir la tabla de composición de estas funciones y demostrar que $(\Gamma, \circ)$ es un grupo.

11. Obtener el grupo de simetrías del plano que transforman una lámina rectangular en sí misma.

12. Demostrar que las matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} w & 0 \\ 0 & w^2 \end{pmatrix}, \begin{pmatrix} w^2 & 0 \\ 0 & w \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & w^2 \\ w & 0 \end{pmatrix}, \begin{pmatrix} 0 & w \\ w^2 & 0 \end{pmatrix},$$

en las que $w^3 = 1$ y $w \neq 1$ forman un grupo con respecto a la multiplicación de matrices.

CAPÍTULO 4

GRUPOS: PROPIEDADES BÁSICAS

4.1. Subgrupos de un grupo y grupos cíclicos
4.2. Teorema de Lagrange
4.3. Subgrupos normales. Grupo cociente
4.4. Homomorfismos de grupos
4.5. Teoremas de isomorfía
4.6. Clasificación de los grupos cíclicos
4.7. Producto directo de grupos
4.8. Grupos de permutaciones
4.9. Comentarios históricos

4.1. SUBGRUPOS DE UN GRUPO Y GRUPOS CÍCLICOS

Dado un grupo $(G, *)$ y un subconjunto H de G, diremos que H es un **subgrupo de $(G, *)$, y escribiremos $(H, *) \leq (G, *)$, si H es un grupo con respecto a la operación $*$ definida en G.** Puesto que la operación $*$ es asociativa en G, esta operación también será asociativa en cualquier subconjunto H de G; se tiene entonces que $(H, *)$ es un subgrupo de $(G, *)$ si se cumplen las tres condiciones siguientes:

1) $*$ es cerrada en H,
2) el elemento neutro de G pertenece a H,
3) si $x \in H$, su inverso, x^{-1}, también pertenece a H.

Cuando la operación del grupo G sea conocida se utilizará la notación $H \leq G$ para indicar que H es un subgrupo de G.

★★ EJEMPLO A. $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$ y este, a su vez, es un subgrupo de $(\mathbb{R}, +)$.

★★ EJEMPLO B. $(\mathbb{Q}^*, \cdot)$ es un subgrupo de $(\mathbb{R}^*, \cdot)$, donde $\mathbb{Q}^*$ y $\mathbb{R}^*$ son los conjuntos de números racionales y reales, respectivamente, de los que se ha eliminado el cero.

★★ EJEMPLO C. Si $n\mathbb{Z}$ es el conjunto de los múltiplos enteros del número natural n, es decir $n\mathbb{Z} = \{nx: x \in \mathbb{Z}\}$, se tiene que $(n\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Z}, +)$.

★★ EJEMPLO D. Sea A un conjunto y $a \in A$; se define $B_a = \{f \in B(A): f(a) = a\}$. Con respecto a la composición de funciones se tiene que $B_a \leq B(A)$, el grupo de las biyecciones de A.

★★ EJEMPLO E. $(SL_2(\mathbb{R}), \circ)$ es un subgrupo de $(GL_2(\mathbb{R}), \circ)$ y $(SO_2(\mathbb{R}), \circ)$ es un subgrupo de $(SL_2(\mathbb{R}), \circ)$. El lector puede ver la definición de estos conjuntos de matrices en la sección 3.5.

Todo grupo $(G, *)$ posee al menos dos subgrupos; éstos son el subgrupo formado por el elemento neutro de G y el subgrupo formado por todos los elementos de G. Estos subgrupos de $(G, *)$ reciben el nombre de **subgrupos impropios** de $(G, *)$. Al resto de los subgrupos de un grupo se les denomina **subgrupos propios** de $(G, *)$. Un gráfico en el cual se representen todos los subgrupos de un grupo de manera que si, para dos subgrupos H_1, H_2 de $(G, *)$, H_1 está incluido en H_2 y no hay ningún subgrupo entre H_1 y H_2, dibujemos

H_2
$\uparrow$
H_1 ,

se llama **retículo de los subgrupos** de $(G, *)$.

★★ EJEMPLO F. Tratemos de encontrar el retículo de los subgrupos de $(\mathbb{Z}_4, +)$. Como $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$, si H es un subgrupo de $(\mathbb{Z}_4, +)$ que contiene a [1], $[1] + [1] = [2] \in H$ y $[1] + [1] + [1] = [3] \in H$, con lo cual $H = \mathbb{Z}_4$; análogamente, si $[3] \in H$, $[3] + [3] = [2] \in H$, $[3] + [3] + [3] = [1] \in H$ y $[3] + [3] + [3] + [3] = [0] \in H$, y por tanto $H = \mathbb{Z}_4$. El conjunto $\{[0], [2]\}$ es un subgrupo de $(\mathbb{Z}_4, +)$ como puede comprobarse fácilmente. El retículo de los subgrupos de $(\mathbb{Z}_4, +)$ se muestra en la ilustración 1.

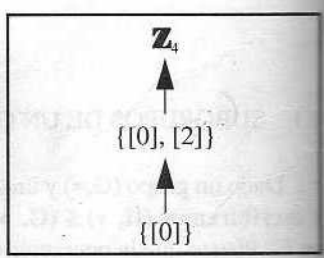


Ilustración 1. Retículo de los sugrupos de $\mathbb{Z}_4$

★★ EJEMPLO G. Tratemos de encontrar el retículo de los subgrupos del grupo de las simetrías de un rectángulo. Las simetrías de un rectángulo son, aparte de la identidad, a, b y c, donde a es un giro de 180° alrededor de su centro y b y c son simetrías respecto de

ejes que pasan por los puntos medios de los lados opuestos. Estas simetrías se muestran en la ilustración 2.

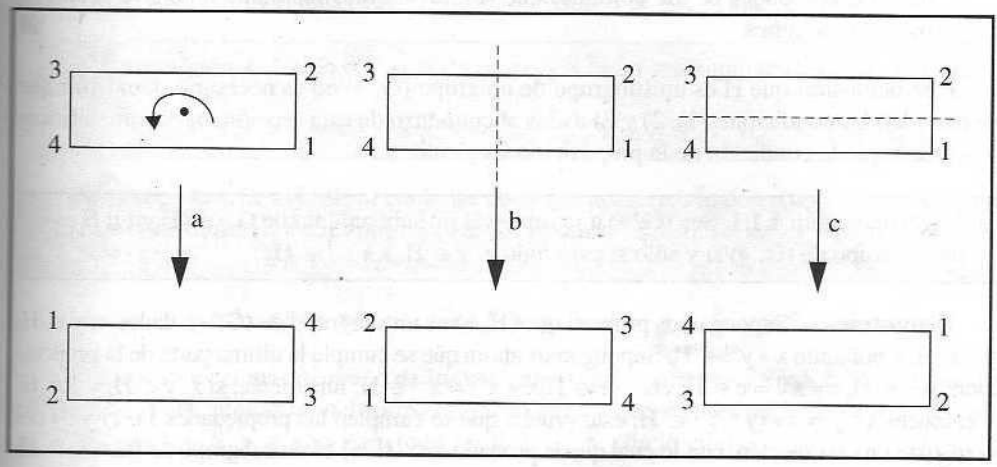


Ilustración 2. Simetrías de un rectángulo

La tabla de este grupo, que se simboliza con la letra V, es:

∘	I	a	b	c
I	I	a	b	c
a	a	I	c	b
b	b	c	I	a
c	c	b	a	I

En este grupo se dan las relaciones $a^2 = b^2 = c^2 = I$. Si V posee un subgrupo H que contiene tres elementos se ha de tener H = V: en efecto, si suponemos que H = {I, a, b}, como c = a ∘ b se tiene que c ∈ H y análogamente se harían el resto de los casos. El retículo de los subgrupos del grupo V es el que se muestra en la ilustración 3. Sólo existen dos grupos de cuatro elementos (véase problema 5 de la sección 3.2). Uno de ellos tiene una tabla "semejante" a la de $(\mathbf{Z}_4, +)$ y el otro tiene una tabla "semejante" a la de (V, ∘), y ambos son abelianos.

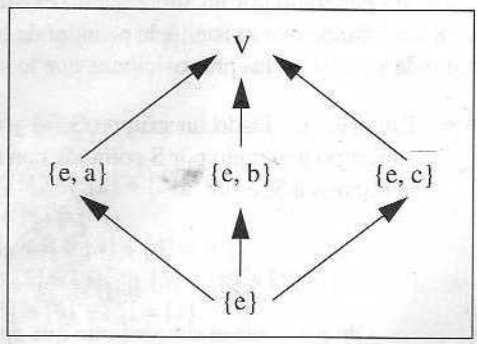


Ilustración 3. Retículo del grupo de Klein

El grupo V se llama **grupo de Klein** en honor al matemático Felix Klein (1849-1925), nacido en Düsseldorf (Alemania), y que contribuyó decisivamente al estudio de las propiedades de un conjunto que son invariantes mediante un cierto grupo de transformaciones. ■

Para demostrar que H es un subgrupo de un grupo $(G, *)$ no es necesario demostrar que se cumplen las condiciones 1), 2) y 3) dadas al comienzo de esta sección; basta con verificar que se cumple la condición de la proposición siguiente:

Proposición 4.1.1. Sea $(G, *)$ un grupo y H un subconjunto de G, con $H \neq \emptyset$; H es un subgrupo de $(G, *)$ si y sólo si para todo $x, y \in H$, $x * y^{-1} \in H$.

Demostración. Supongamos primero que $(H, *)$ es un subgrupo de $(G, *)$; dados $x, y \in H$, $y^{-1} \in H$, y por tanto $x * y^{-1} \in H$. Supongamos ahora que se cumple la última parte de la proposición; si $x \in H$, $x * x^{-1} = e \in H$; como $e \in H$, $e * x^{-1} = x^{-1} \in H$; finalmente, si $x, y \in H$, $y^{-1} \in H$ y entonces $x * y = x * (y^{-1})^{-1} \in H$; esto prueba que se cumplen las propiedades 1), 2) y 3) del comienzo de esta sección, con lo cual queda probado que $(H, *)$ es un subgrupo de $(G, *)$. ■

★★ EJEMPLO H. Si $\{A_j\}_{j=1,\ldots,\infty}$ es una colección de subgrupos de un grupo $(G, *)$, su intersección

$$A = \bigcap_{j=1}^{\infty} A_j$$

es también un subgrupo de $(G, *)$. Para demostrar este resultado consideremos dos elementos x e y de A; por tanto ambos elementos pertenecen a A_j para todo $j = 1, \ldots, \infty$; puesto que estos subconjuntos son subgrupos de $(G, *)$, $x * y^{-1} \in A_j$ para todo $j = 1, \ldots, \infty$, debido a la proposición 4.1.1; por tanto $x * y^{-1} \in A$. Esto prueba que A es un grupo.

A continuación presentamos una forma de obtener subgrupos de un grupo comenzando con cualquier subconjunto de éste. Dado un subconjunto S de un grupo $(G, *)$, se llama **subgrupo generado por S,** y se simboliza mediante $<S>$, **al más pequeño de los subgrupos de $(G, *)$ que contienen a S.** Esta definición presenta dos dificultades: no sabemos si el subgrupo generado por un subconjunto existe siempre, ni si hay una forma sencilla de obtenerlo en caso de que exista. A la primera de ellas responde afirmativamente el ejemplo I y la segunda se trata en las proposiciones que le siguen.

★★ EJEMPLO I. Dado un grupo $(G, *)$ y un subconjunto S de G demostraremos que el subgrupo generado por S coincide con la intersección de todos los subgrupos de G que contienen a S, es decir:

$$<S> = \bigcap_{\substack{H \leq G \\ H \supset S}} H$$

Observar que el subconjunto que aparece a la derecha en la igualdad anterior, al que llamaremos A, es un subgrupo de $(G, *)$ debido al ejemplo H. Tenemos que probar que

$\langle S\rangle = A$. Claramente $\langle S\rangle \subseteq A$ ya que $(A, *)$ es un subgrupo que contiene a S; si $(H, *)$ es un subgrupo que contiene a S, de la definición de A se deduce que $H \supseteq A$; por tanto, $A \subseteq \langle S\rangle$, y A es el más pequeño de los subgrupos de $(G, *)$ que contienen a S.

Proposición 4. 1.2. Si $(G, *)$ es un grupo y S es un subconjunto de G, se tiene que

$$\langle S\rangle = \{x_1^{\alpha_1} * x_2^{\alpha_2} * \ldots * x_n^{\alpha_n} : \quad x_1, x_2, \ldots, x_n \in S, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{Z}\}$$

Demostración. Sea H_S el subconjunto de G que aparece a la derecha de la igualdad que se quiere demostrar; H_S es un subgrupo de $(G, *)$ puesto que si $a = x_1^{\alpha_1} * x_2^{\alpha_2} * \ldots * x_n^{\alpha_n}$ y $b = y_1^{\beta_1} * y_2^{\beta_2} \ldots * y_m^{\beta_m}$ tenemos que

$$a * b^{-1} = x_1^{\alpha_1} * x_2^{\alpha_2} * \ldots * x_n^{\alpha_n} * y_m^{-\beta_m} * \ldots * y_2^{-\beta_2} * y_1^{-\beta_1} \in H_S.$$

Como $\langle S\rangle$ es el más pequeño de los subgrupos que contienen a S y $S \subset H_S$ se tiene que $\langle S\rangle \subset H_S$. Falta probar la inclusión contraria: puesto que $\langle S\rangle$ es un subgrupo de $(G, *)$ y $S \subset \langle S\rangle$, si $x_i \in S$, $x_i \in \langle S\rangle$ para todo i = 1, 2, ..., n, con lo cual

$$x_1^{\alpha_1} * x_2^{\alpha_2} * \ldots * x_n^{\alpha_n} \in \langle S\rangle \text{ y por tanto } H_S \subset \langle S\rangle. \quad \blacksquare$$

★★ EJEMPLO J. El subgrupo generado por [3] en $(\mathbf{Z}_9, +)$ es $\langle[3]\rangle = \{[0], [3], [6]\}$ ya que el opuesto de [3] en $(\mathbf{Z}_9, +)$ es [6] y cualquier otro múltiplo de 3 es congruente con 0, 3 o 6 módulo 9.

El subgrupo generado por los elementos A y B de D_6 (véase el ejemplo A de la sección 3.6) es D_6 ya que en su tabla se observa que todas sus combinaciones generan el grupo.

Si el conjunto S está formado por una cantidad finita de elementos $x_1, x_2, \ldots, x_n \in G$, escribiremos $\langle x_1, x_2, \ldots, x_n\rangle$ en lugar de $\langle\{x_1, x_2, \ldots, x_n\}\rangle$. De manera similar, $\langle x\rangle$ representa el subgrupo generado por el elemento x del grupo $(G, *)$

Definición 4.1.3. Un grupo $(G, *)$ se dice **cíclico** si existe al menos un elemento $x \in G$ tal que el subgrupo generado por x es G, es decir $\langle x\rangle = G$; en este caso x se denomina un **generador** de G.

★★ EJEMPLO K. $(\mathbf{Z}, +)$ y $(\mathbf{Z}_n, +)$ son ejemplos de grupos cíclicos con generadores 1 y [1], respectivamente.

★★ EJEMPLO L. Tratemos de encontrar todos los generadores de $(\mathbf{Z}_6, +)$; como

$$[2] + [2] = [4], \quad [2] + [2] + [2] = [0]$$
$$[3] + [3] = [0]$$
$$[4] + [4] = [2], \quad [4] + [4] + [4] = [0],$$

y $\quad [5] + [5] = [4], \quad [5] + [5] + [5] = [3], \quad [5] + [5] + [5] + [5] = [2],$
$$[5] + [5] + [5] + [5] + [5] = [1],$$

solamente [1] y [5] son generadores de $(\mathbf{Z}_6, +)$.

★★ EJEMPLO M. Tratemos de encontrar todos los generadores de $(\mathbf{Z}_5^*, \cdot)$; como

$$[2]\cdot[2]=[4],\quad [2]\cdot[2]\cdot[2]=[3],\quad [2]\cdot[2]\cdot[2]\cdot[2]=[1],$$
$$[3]\cdot[3]=[4],\quad [3]\cdot[3]\cdot[3]=[2],\quad [3]\cdot[3]\cdot[3]\cdot[3]=[1].$$
$$\text{y } [4]\cdot[4]=[1],\quad [4]\cdot[4]\cdot[4]=[4],$$

se deduce que [2] y [3] son los únicos generadores de $(\mathbf{Z}_5^*, \cdot)$.

Definición 4.1.4. Dado un grupo $(G, *)$ y un elemento $x \in G$, definimos el **orden de x** como el número de elementos que posee el subgrupo generado por x, si éste es finito. En caso contrario, diremos que el orden de x es infinito.

Recordemos que en la sección 2 del capítulo 3 hemos definido el orden de un grupo finito $(G, *)$ como el número de elementos de G y tal número se ha simbolizado mediante $|G|$. Aquí acabamos de definir el orden de un elemento $x \in G$ como $|\langle x\rangle|$.

Proposición 4.1.5. Sea $(G, *)$ un grupo finito y x un elemento de G; existe un entero positivo n tal que $x^n = e$ y el subgrupo generado por x es

$$\langle x\rangle = \{x, x^2, \ldots, x^{n-1}, x^n = e\}$$

Demostración. Puesto que $(G, *)$ es un grupo finito, el conjunto $\{x, x^2, \ldots, x^k, \ldots\}$ debe tener repeticiones; existen pues enteros positivos i, j tal que $x^i = x^j$. De aquí se deduce que

$$e = x^i * x^{-i} = x^j * x^{-i} = x^{j-i}.$$

Como siempre podemos suponer $j > i$, basta tomar $n = j - i$.

De la proposición 4.1.2 deducimos que

$$\langle x\rangle = \{x, x^2, \ldots, x^k, \ldots, x^{-1}, x^{-2}, \ldots, x^{-k}, \ldots\}.$$

Si $k > n$, tomamos $c, r \in \mathbf{N}$ tal que $k = cn + r$ con $0 < r \leq n$; entonces $x^k = x^{cn} * x^r = x^r$. Esto nos dice que los elementos x^k, con $k > n$, pueden ser eliminados de $\langle x\rangle$ puesto que aparecen repetidos. De manera similar se puede razonar para probar que los elementos de la forma x^{-i} aparecen repetidos: basta tomar $c, r \in \mathbf{Z}$ tal que $-i = cn + r$ con $0 < r \leq n$. ■

Si $(G, *)$ es un grupo finito, $x \in G$, y se toma n como el menor entero positivo que satisface $x^n = e$, entonces los elementos $x, x^2, \ldots, x^{n-1}, x^n = e$ son todos distintos; en efecto si $x^i = x^j$ con $1 \leq i \leq j \leq n$, se tiene que

$$x^{j-i} = x^j * x^{-i} = x^i * x^{-i} = e\ ;$$

como $j - i < n$ y n es el menor entero positivo tal que $x^n = e$, deducimos que $j = i$.

Esta observación, junto con la proposición 4.1.5, demuestra la siguiente proposición:

Proposición 4.1.6. Si (G, $*$) es un grupo finito y x un elemento de G, el orden de x coincide con el menor entero positivo k tal que $x^k = e$. Además

$$\langle x \rangle = \{x, x^2, \ldots, x^{k-1}, x^k = e\},$$

y todos los elementos de este conjunto son distintos.

★★ EJEMPLO N. Indicando por **orden(x),** el orden de un elemento x en un grupo dado, se deduce del ejemplo L que, considerados como elementos de $(\mathbb{Z}_6, +)$,

$$\text{orden}([0]) = 1, \text{orden}([1]) = 6, \text{orden}([2]) = 3, \text{orden}([3]) = 2,$$
$$\text{orden}([4]) = 3, \text{orden}([5]) = 6.$$

Del ejemplo M se deduce que, considerados como elementos de $(\mathbb{Z}_5^*, \cdot)$,

$$\text{orden}([1]) = 1, \text{orden}([2]) = 4, \text{orden}([3]) = 4, \text{orden}([4]) = 2.$$

Proposición 4.1.7. Sea (G, $*$) un grupo y $x \in G$ un elemento de orden finito k; si m es un entero positivo tal que $x^m = e$, se tiene que k divide a m.

Demostración. Si $x^m = e$, escribimos $m = ck + r$ con $0 \leq r < k$, y por tanto, $e = x^m = x^{ck} * x^r = (x^k)^c * x^r = (e)^c * x^r = x^r$. Como $0 \leq r < k$ y k es el menor entero que satisface $x^k = e$, de la igualdad anterior se deduce que $r = 0$ y por tanto $m = ck$, lo que prueba que k divide a m. ■

EJERCICIOS 4.1

1. Encontrar todos los subgrupos de $(\mathbb{Z}_6, +)$ y colocarlos en un retículo. Hacer lo mismo con $(\mathbb{Z}_8, +)$.

2. Escribir el retículo de los subgrupos de S_3 y D_8 (véanse las definiciones de estos grupos en las secciónes 3.4 y 3.6 del capítulo 3).

3. Demostrar que el conjunto de los números complejos de módulo 1 es un subgrupo del grupo multiplicativo de los números complejos $(\mathbb{C}^*, \cdot)$.

4. ¿Es cierto que si H y K son subgrupos de un grupo (G, $*$), $H \cup K$ es también un subgrupo del mismo grupo?

5. Dados H y K subgrupos de un grupo (G, $*$), demostrar que $H \cup K$ es un subgrupo de (G, $*$) si y sólo si $H \subseteq K$ o $K \subseteq H$.

6. Demostrar que el conjunto $T = \{x \in D_{2n} : x^2 = I\}$ no es un subgrupo de D_{2n}.

7. Sea $S = \{x \in \mathbb{R} : x = a + b\sqrt{2}, a, b \in \mathbb{Q}, a \neq 0 \text{ o } b \neq 0\}$. Estudiar si S es un subgrupo de $(\mathbb{R}^*, \cdot)$.

8. Demostrar que $(\mathbb{Z}_7^*, \cdot)$ es un grupo cíclico y encontrar todos sus generadores.

9. Encontrar un grupo $(G, *)$ y un subconjunto H de G tal que H sea cerrado con respecto a la operación de G, pero que H no sea un subgrupo de $(G, *)$.

10. Demostrar que si H es un subconjunto finito de un grupo $(G, *)$ tal que $*$ es cerrada en H, $(H, *)$ es un subgrupo de $(G, *)$. ¿Contradice esto el resultado del problema 9?

11. Demostrar que todo grupo cíclico es abeliano.

12. ¿Es cíclico el grupo de Klein? (Véase el ejemplo G de la sección 4.1.)

13. Estudiar si $(\mathbb{Q}^*, \cdot)$ es un grupo cíclico.

14. Sea p un número primo. Definimos el conjunto $G_p = \{m/p^n : m, n \in \mathbb{Z}\}$. Demostrar que $(G_p, +)$ es un grupo abeliano. ¿Es $(G_p, +)$ un grupo cíclico?

15. Si $(G, *)$ es un grupo, probar que el orden de cualquier elemento $x \in G$ coincide con el orden de x^{-1}.

16. Demostrar que si $(G, *)$ es un grupo cíclico con sólo un generador, G tiene como máximo 1 o 2 elementos. ¿Es cierto este resultado si $(G, *)$ posee dos generadores?

17. Sea $(G, *)$ un grupo abeliano y n un entero positivo; demostrar que $H = \{x^n : x \in G\}$ es un subgrupo de $(G, *)$.

18. Sea $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 6 & 5 \end{pmatrix} \in S_6$. Encontrar todos los elementos del subgrupo generado por α en S_6.

19. ¿Es D_6 un grupo cíclico? Encontrar el orden de cada uno de los elementos de D_6.

4.2. TEOREMA DE LAGRANGE

De ahora en adelante no se indicará más que cuando sea necesario la operación con respecto a la cual un conjunto G es un grupo, y si x e y son dos elementos de este conjunto, la operación de x con y se escribirá mediante xy.

En el ejemplo N de la sección 4.1 se demostró que los órdenes de los elementos de $(\mathbb{Z}_6, +)$ son 1, 2, 3 ó 6, mientras que los órdenes de los elementos de $(\mathbb{Z}_5^*, \cdot)$ son 1, 2 ó 4. En el ejercicio 19 de la misma sección se pidió encontrar los órdenes de los elementos de D_6, que son 1, 2 ó 3. En todos estos casos es posible observar que el orden de los elementos de un grupo es un divisor del orden del grupo: divisores de 6 en el caso de $(\mathbb{Z}_6, +)$ y D_6, y divisores de 4 en el caso de $(\mathbb{Z}_5^*, \cdot)$. Para abundar en esta observación puede comprobarse a partir de la tabla del

grupo D_8 obtenida en el ejemplo B de la sección 3.6 del capítulo 3, que los órdenes de los elementos de D_8 son 1, 2 ó 4.

Esto sugiere que la observación anterior puede ser cierta para cualquier grupo finito.

Proposición 4.2.1. Sea G un grupo finito y x un elemento de G; el orden de x es un divisor del número de elementos de G.

Demostración. Sea k el orden de x y n el número de elementos de G. Por la proposición 4.1.6 se sabe que

$$\langle x \rangle = \{x, x^2, \ldots, x^{k-1}, x^k = e\},$$

y las distintas potencias de x que aparecen en $\langle x \rangle$ no se repiten. Dado $g_1 \in G$ definimos $f_{g_1} : \langle x \rangle \to G$ mediante

$$f_{g_1}(x^j) = x^j g_1, \quad j = 1, 2, \ldots, k.$$

La aplicación f_{g_1} es inyectiva puesto que si $f_{g_1}(x^j) = f_{g_1}(x^i)$ se tiene que $x^j g_1 = x^i g_1$ y de la propiedad cancelativa por la derecha deducimos $x^j = x^i$. El conjunto imagen de $\langle x \rangle$ mediante f_{g_1}, simbolizado mediante $f_{g_1}(\langle x \rangle)$, tiene, pues, el mismo número de elementos que $\langle x \rangle$.

Si ahora consideramos $g_2 \in G$ de manera que $g_2 \notin f_{g_1}(\langle x \rangle)$ se tiene que $f_{g_1}(\langle x \rangle) \cap f_{g_2}(\langle x \rangle) = \emptyset$; en efecto, si y es un elemento común a ambos conjuntos, existirán j y s enteros positivos, $j \leq k$, $s \leq k$ tales que $x^j g_2 = y = x^s g_1$, de donde se deduce que $g_2 = x^{s-j} g_1 \in f_{g_1}(\langle x \rangle)$, en contra de lo supuesto.

Si ahora tomamos $g_3 \in G$ de manera que $g_3 \notin f_{g_1}(\langle x \rangle)$ y $g_3 \notin f_{g_2}(\langle x \rangle)$, un razonamiento similar al anterior prueba que $f_{g_3}(\langle x \rangle)$ es disjunto con $f_{g_1}(\langle x \rangle)$ y $f_{g_2}(\langle x \rangle)$.

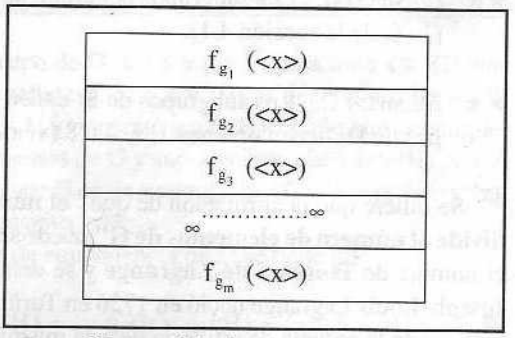


Ilustración 4. Participación G

Como el grupo G es finito, el proceso anterior agota todos los elementos de G después de un número finito m de pasos. Se obtiene así una partición del conjunto G en m subconjuntos de manera que todos ellos poseen el mismo número de elementos. Entonces

$$|\langle x \rangle| m = |G| = n,$$

lo cual prueba el resultado deseado. ■

★★ EJEMPLO A. Esta proposición tiene como consecuencia inmediata una demostración muy sencilla del **Pequeño Teorema de Fermat.** Recordar que el Pequeño Teorema de

Fermat establece que si p es primo y a es un número natural tal que p no divide a a, entonces $a^{p-1} \equiv 1$ (p) (véase teorema 2.4.7 del capítulo 2).

Para demostrar este resultado, considerar el grupo $(\mathbb{Z}^*_p, \cdot)$, que es un grupo con p – 1 elementos (proposición 3.3.1 del capítulo 3) y la clase de equivalencia [a] de a. Como p no es divisor de a, $[a] \in \mathbb{Z}^*_p$. Si k es el orden de [a], debido a la proposición 4.2.1 existe $s \in \mathbb{N}$ tal que $k \cdot s = p - 1$; entonces

$$[a^{p-1}] = [a]^{p-1} = ([a]^k)^s = ([1])^s = [1],$$

lo cual es equivalente a escribir $a^{p-1} \equiv 1$ (p), que era lo que queríamos demostrar.

La demostración de la proposición 4.2.1 está íntimamente ligada con el concepto de partición de un conjunto; este concepto está a su vez íntimamente ligado con el concepto de relación de equivalencia definida en un conjunto (véase la sección 1.2 del capítulo 1). Esto sugiere que la demostración de la proposición anterior podría haberse hecho definiendo una cierta relación de equivalencia en G. Por otro lado, la demostración anterior no parece ligada esencialmente a la forma del subgrupo <x>, sino que podría hacerse para cualquier subgrupo H de G. Los siguientes ejemplos muestran que el resultado de la proposición 4.2.1 puede ser también cierto para todos los subgrupos de G.

★★ EJEMPLO B. Los subgrupos del grupo de Klein tienen órdenes 1, 2 ó 4 (véase el ejemplo G de la sección 4.1).

★★ EJEMPLO C. Los subgrupos de S_3 tienen órdenes 1, 2, 3 ó 6, mientras que los subgrupos de D_8 tienen órdenes 1, 2, 4 u 8 (véase el ejercicio 2 de la sección 4.1).

Se infiere que la afirmación de que **"el número de elementos de un subgrupo H de G divide al número de elementos de G"** puede ser cierta siempre. Este resultado se conoce con el nombre de **Teorema de Lagrange** y se demostrará más adelante en esta misma sección. Joseph–Louis Lagrange nació en 1736 en Turín (Italia) y ya en sus años mozos enseñó matemáticas en la escuela de artillería de esta misma ciudad; en 1764 fue premiado por la Academia de Ciencias de París por sus trabajos sobre la luna; enseñó en Berlín y en París, ciudad esta última en la que murió en 1813. Es de resaltar que J.-L. Lagrange murió mucho antes de que apareciera la definición abstracta de grupo, y que el resultado que hoy se conoce como "teorema de Lagrange" no fue probado por él como tal, sino en un caso particular.

Definición 4.2.2. Si G es un grupo, H es un subgrupo de G y $x \in G$, definimos $xH = \{xh : h \in H\}$.

★★ EJEMPLO D. Si en $(\mathbb{Z}, +)$ consideramos el subconjunto $5\mathbb{Z}$, tenemos entonces que $2 + 5\mathbb{Z} = \{2 + 5z : z \in \mathbb{Z}\} = 7 + 5\mathbb{Z}$.

★★ EJEMPLO E. En S_3 considerar el subconjunto $H = \{I, \alpha, \alpha^2\}$ (véase la sección 3.4 del capítulo 3). En este caso

$$\alpha H = \{\alpha, \alpha^2, I\} = H$$
$$\beta H = \{\beta, \beta\alpha, \beta\alpha^2\} = \{\beta, \alpha^2\beta, \alpha\beta\}.$$

Proposición 4.2.3. Si G es un grupo finito, H es un subconjunto de G y x es un elemento de G, el número de elementos de xH coincide con el número de elementos de H.

Demostración. La aplicación $f: H \to xH$ dada por $f(h) = xh$ es una biyección; en efecto, si $f(h_1) = f(h_2)$ para $h_1, h_2 \in H$, $xh_1 = xh_2$ y debido a la propiedad cancelativa por la izquierda se tiene que $h_1 = h_2$; además, si $xh \in xH$, basta observar que $f(h) = xh$, para tener que f es suprayectiva. ■

Definición 4.2.4. Sea G un grupo y H un subgrupo de G; diremos que dos elementos $x, y \in G$ están relacionados mediante H, y escribiremos $x \equiv y$ (H), si $x^{-1}y \in H$.

Proposición 4.2.5. Sea G un grupo y H un subgrupo de G; la relación definida en 4.2.4 es una relación de equivalencia y la clase de equivalencia de un elemento x de G en esta relación coincide con xH.

Demostración. Puesto que H es un subgrupo de G, $x^{-1}x = e \in H$ para todo $x \in G$; por tanto $x \equiv x$(H) y queda probada la propiedad reflexiva. Si $x \equiv y$ (H) se tiene que $x^{-1}y \in H$; como H es un subgrupo de G, $y^{-1}x = (x^{-1}y)^{-1} \in H$ y por tanto $y \equiv x$ (H), con lo que se cumple la propiedad simétrica. Sean ahora x, y, z elementos de G y supongamos que $x \equiv y$ (H), $y \equiv z$ (H); se tiene que $x^{-1}y \in H$ e $y^{-1}z \in H$, y puesto que H es un subgrupo de G, $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, con lo que queda probada la propiedad transitiva.

Sea ahora $x \in G$; si [x] representa la clase de equivalencia de x, se tiene que

$$[x] = \{y \in G: x \equiv y\ (H)\} = \{y \in G: x^{-1}y \in H\} = \{y \in G: y \in xH\} = \{xh: h \in H\} = xH \blacksquare$$

La clase de equivalencia del elemento x según la relación definida en 4.2.4 será simbolizada mediante [x] en los siguientes ejemplos.

★★ EJEMPLO F. En $(\mathbb{Z}, +)$ la relación de equivalencia que define el subgrupo $5\mathbb{Z}$ es: $n \equiv m$ $(5\mathbb{Z})$ si y sólo si $-m + n \in 5\mathbb{Z}$. Esta es la definición que dimos de números congruentes módulo 5. Sus clases de equivalencia son $[0] = 0 + 5\mathbb{Z} = 5\mathbb{Z}$, $[1] = 1 + 5\mathbb{Z}$, $[2] = 2 + 5\mathbb{Z}$, $[3] = 3 + 5\mathbb{Z}$ y $[4] = 4 + 5\mathbb{Z}$, que se corresponden con 0, 1, 2, 3 y 4.

★★ EJEMPLO G. Dado $H = \{I, \alpha, \alpha^2\}$, $\alpha^2 \equiv \alpha$(H) en S_3 ya que $\alpha^{-1}\alpha^2 = \alpha \in H$. Sin embargo β no está relacionado con α ya que $\alpha^{-1}\beta = \alpha^2\beta \notin H$. Con esta relación las clases de equivalencia de α y β son $[\alpha] = H$ y $[\beta] = \{I, \alpha\beta, \alpha^2\beta\}$.

Estamos ya en condiciones de demostrar el teorema de Lagrange:

Teorema de Lagrange. Si G es un grupo finito y H un subgrupo de G, el número de elementos de H divide al número de elementos de G.

Demostración. Por ser la relación dada en la definición 4.2.4 una relación de equivalencia en G, se tiene que las clases de equivalencia de esta relación establecen una partición de G; puesto que debido a la proposición 4.2.5 estas clases de equivalencia coinciden con xH, tenemos

$$G = (x_1H) \cup (x_2H) \cup \ldots \cup (x_mH)$$

donde $x_j \in G$ y $x_iH \cap x_jH = \emptyset$ si $i \neq j$, $i = 1, 2, \ldots, m$. Como todos los conjuntos x_jH poseen $|H|$ elementos (proposición 4.2.3), se tiene

$$|G| = |x_1H| + |x_2H| + \ldots + |x_mH| = m\,|H|$$

y queda demostrado el teorema. ■

Corolario 4.2.6. Si G es un grupo de orden p, con p primo, G es cíclico.

Demostración. Sea $x \in G$ con $x \neq e$; el conjunto $\langle x \rangle$ es un subgrupo de G distinto de $\{e\}$; por el teorema de Lagrange, $|\langle x \rangle|$ divide a p; puesto que p es primo, sus únicos divisores son 1 y p; como $|\langle x \rangle| > 1$ se ha de tener $|\langle x \rangle| = p$ y por tanto x es un generador de G. ■

En las condiciones del teorema de Lagrange, al número entero m tal que $|G| = m\,|H|$ se denomina **índice de H en G** y se representa mediante [G:H]. A los diferentes xH que aparecen en la demostración del teorema de Lagrange se les denomina **clases de equivalencia por la izquierda módulo H.** De manera similar a como se han definido las clases de equivalencia por la izquierda módulo H pueden definirse las **clases de equivalencia por la derecha módulo H** y pueden utilizarse para demostrar el teorema de Lagrange.

EJERCICIOS 4.2

1. Escribir las tablas de multiplicación de todos los grupos de orden 7.
2. Si G es un grupo de orden 2p, con p primo, demostrar que todo subgrupo propio de G es cíclico.
3. Probar que si x tiene orden n en G y d es un entero positivo divisor de n, G tiene un elemento de orden d.
4. Sea G un grupo abeliano y n un número entero positivo; demostrar que $H_n = \{x \in G: \text{orden } (x) \mid n\}$ es un subgrupo de G.

5. Probar que en un grupo G el orden de xy coincide con el orden de yx para cualquier par de elementos x, y de G.

6. Si G es un grupo con n elementos, demostrar que para todo $x \in G$, $x^n = e$.

7. Demostrar que todo subgrupo propio de S_3 es cíclico. (Se tiene así un ejemplo de un grupo **no abeliano** en el que todos sus subgrupos propios son cíclicos.) ¿Es posible encontrar un grupo **abeliano no cíclico** en el que todos sus subgrupos propios sean cíclicos?

8. Demostrar que si [a] es un elemento de $\mathbb{Z}_n^*$, [a] posee inverso en $(\mathbb{Z}_n^*, \cdot)$ si y sólo si el máximo común divisor de a y n es 1.

9. Sea $I(\mathbb{Z}_n^*)$ el conjunto de todos los $[a] \in \mathbb{Z}_n^*$ tales que [a] posee inverso en $(\mathbb{Z}_n^*, \cdot)$. Según el problema 8 de esta misma sección el conjunto $I(\mathbb{Z}_n^*)$ tiene $\varphi(n)$ elementos, donde $\varphi(n)$ es la función de Euler definida en el problema 12 de la sección 2.5. Demostrar que $(I(\mathbb{Z}_n^*), \cdot)$ es un grupo.

10. Demostrar el **teorema de Fermat-Euler:** si a es primo con n, $a^{\varphi(n)} \equiv 1(n)$ (usar el problema 6 de esta misma sección).

11. Usar los problemas 13 y 14 de la sección 2.5 para demostrar que $\varphi(100) = 40$. Demostrar que si a es un entero que no es divisible entre 2 ni entre 5, los últimos dígitos de a^{40} son 01.

12. Dados H y K, subconjuntos de un grupo G, definimos $HK = \{hk : h \in H, k \in K\}$. Demostrar que si H es un subgrupo de G, HH = H.

13. Encontrar dos subgrupos H y K de D_8, tales que HK no sea un subgrupo de D_8.

14. Sean H y K subgrupos de G. Demostrar que HK es un subgrupo de G si y sólo si HK = KH.

15. Sean H y K subgrupos finitos de un grupo G tales que H y K sólo tienen en común el elemento neutro. Demostrar que el número de elementos de HK coincide con |H| |K|.

4.3. SUBGRUPOS NORMALES Y GRUPO COCIENTE

El estudio de un grupo G puede simplificarse si se estudian sus subgrupos propios, que poseen un orden inferior al orden de G, y los conjuntos cocientes de G sobre cada uno de estos subgrupos. Si H es un subgrupo de G podemos considerar el conjunto cociente G/H, que es el conjunto de las clases de equivalencia que se obtienen al definir en G la relación de equivalencia módulo H dada en la definición 4.2.4, a saber,

$$x \equiv y\ (H) \quad \text{si y sólo si} \quad x^{-1}y \in H.$$

Es natural preguntarse si al conjunto G/H se le puede dotar de una estructura de grupo, cuya operación esté relacionada con la operación de G; en este sentido lo más lógico que cabe espe-

rar del resultado de operar las clases de equivalencia xH e yH en G/H es la clase de equivalencia (xy)H. Pero esto no sucede para cualquier subgrupo de un grupo dado como se muestra en el ejemplo siguiente.

★★ EJEMPLO A. Sea $H = \{I, B\}$ un subgrupo de D_6 (véase la sección 3.6 del capítulo 3); tenemos que

$$AH = \{A, AB\} \quad y \quad A^2H = \{A^2, A^2B\}$$

con lo que

$$(AH)(A^2H) = \{I, B, ABA^2, ABA^2B\} = \{I, B, A^2B, A^2\},$$

mientras que

$$AA^2H = A^3H = IH = H.$$

El ejemplo anterior sugiere que únicamente para algunos subgrupos distinguidos de G puede definirse una operación en el conjunto cociente; tales subgrupos reciben el nombre de **"normales".**

Definición 4.3.1. Un subgrupo H de un grupo G se dice **normal,** y escribiremos $H \lhd G$, si $(xH)(yH) = (xy)H$ para todo $x, y \in G$.

★★ EJEMPLO B. En el grupo D_6 de las simetrías de un triángulo, que se ha usado en el ejemplo A, se ha comprobado que $H = \{I, B\}$ no es normal en D_6.

★★ EJEMPLO C. En $(\mathbb{Z}, +)$ el subgrupo $5\mathbb{Z}$ es normal ya que para todo para m y n enteros, $(m + 5\mathbb{Z}) + (n + 5\mathbb{Z}) = \{m + 5z_1 + n + 5z_2 : z_1, z_2 \in \mathbb{Z}\} = \{m + n + 5z : z \in \mathbb{Z}\} = (m + n) + 5\mathbb{Z}$.

El siguiente teorema muestra que si H es un subgrupo normal de G, a G/H se le puede dotar de una estructura de grupo.

Teorema 4.3.2. Sea G un grupo y H un subgrupo normal de G; la operación $(xH)(yH) = (xy)H$ define en el conjunto cociente G/H una estructura de grupo. Este grupo recibe el nombre de **grupo cociente de G sobre H.**

Demostración. Se ha de verificar en primer lugar que la operación de clases de equivalencia está bien definida en G/H, es decir si x' es un representante de xH e y' es un representante de yH, x'y' es un representante de (xy)H. Pero como $x' \in xH$ e $y' \in yH$, $x'y' \in (xH)(yH) = (xy)H$, por ser H un subgrupo normal de G.

La asociatividad de esta nueva operación es una consecuencia de la asociatividad de G puesto que

$$((xH)\,(yH))\,(zH) = ((xy)H)\,(zH) = (xy)zH = x(yz)H = (xH)\,((yH)(zH)).$$

El elemento neutro es $H = eH$, donde e es el neutro de G, puesto que

$$(xH)\,(eH) = (xe)H = xH \quad \text{y} \quad (eH)\,(xH) = (ex)H = xH$$

para todo $xH \in G/H$. Finalmente, si $xH \in G/H$, $x^{-1}H$ es su inverso, donde x^{-1} denota el inverso de x en G, puesto que se tienen las igualdades siguientes:

$$(xH)\,(x^{-1}H) = (xx^{-1})H = eH = H \quad \text{y} \quad (x^{-1}H)\,(xH) = (x^{-1}x)H = eH = H. \qquad \blacksquare$$

Recordamos la definición de índice de un subgrupo.

Definición 4.3.3. Si G es un grupo y H es un subgrupo de G, definimos el **índice de H en G,** y lo representamos mediante [G:H], como el cardinal del conjunto cociente G/H.

Observar que el índice de H en G se puede definir para cualquier subgrupo no necesariamente normal, como se hizo al final de la sección anterior. En este caso el índice de H en G es el número de clases de equivalencia de G bajo la relación dada por H, bien sea por la izquierda o por la derecha.

La definición dada de subgrupo normal de un grupo ha aparecido de manera natural al tratar de definir una estructura de grupo en el conjunto cociente; sin embargo, la verificación de que un subgrupo dado de un grupo es normal resulta bastante engorrosa a partir de la definición. La siguiente proposición nos da condiciones equivalentes de normalidad que permiten determinar más fácilmente los subgrupos normales de un grupo.

Proposición 4.3.4. Si G es un grupo y H es un subgrupo de G, las siguientes condiciones son equivalentes:

i) H es un subgrupo normal de G.
ii) $xHx^{-1} \subset H$ para todo $x \in G$.
iii) $xH = Hx$ para todo $x \in G$, es decir, las clases de equivalencia por la izquierda y por la derecha coinciden.

Demostración. Demostraremos que i) $\Rightarrow$ ii), ii) $\Rightarrow$ iii) y que iii) $\Rightarrow$ i), con lo cual quedará demostrada la proposición.

Sea H un subgrupo normal de G; entonces $(xH)(x^{-1}H) = (xx^{-1})H = eH = H$ para todo $x \in G$; se tiene entonces que si $h \in H$, $xhx^{-1}h \in H$ y, por tanto, $xhx^{-1} \in H\,h^{-1} \in H \subset H$, lo cual demuestra ii).

Supongamos que $xHx^{-1} \subset H$ para todo $x \in G$; operando con x por la derecha se obtiene $xH \subset Hx$; aplicando la hipótesis a x^{-1} se obtiene $x^{-1}Hx \subset H$ y operando con x por la izquierda se obtiene $Hx \subset xH$; esto demuestra que las clases de equivalencia por la izquierda y por la derecha coinciden.

Finalmente, supongamos que $xH = Hx$ para todo $x \in G$; queremos demostrar que $(xH)(yH) = (xy)H$. Sean $x' \in xH$ e $y' \in yH$; se tiene $x' = xh_1$ e $y' = yh_2$ con $h_1, h_2 \in H$; entonces $x'y' = (xh_1)(yh_2)$ y, puesto que $Hy = yH$, existe $h' \in H$ tal que $h_1y = yh'$, con lo cual

$$x'y' = (xh_1)(yh_2) = x(yh')h_2 \in (xy)H.$$

Esto prueba que $(xH)(yH) \subset (xy)H$. Sea ahora $(xy)h \in (xy)H$; entonces

$$(xy)h = (xe)(yh) \in (xH)(yH),$$

con lo cual se prueba la inclusión $(xy)H \subset (xH)(yH)$ y con ella la normalidad de H en G. ■

Una consecuencia sencilla de la proposición 4.3.4 es que todo subgrupo de un grupo abeliano es normal; basta observar que si H es un subgrupo de un grupo abeliano A y $x \in H$, el conjunto xH coincide con el conjunto Hx.

Corolario 4.3.5. Si $(A, \cdot)$ es un grupo abeliano y H es un subgrupo de A, H es normal en A.

★★ EJEMPLO D. Tratemos de encontrar todos los subgrupos normales de S_3; la tabla de S_3 puede encontrarse en la sección 3.4 del capítulo 3. Recordamos que $S_3 = \{I, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ donde $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ y $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; recuérdese también que $\alpha^3 = \beta^2 = I$ y que $\beta\alpha = \alpha^2\beta$. Los subgrupos de S_3 se han encontrado en el problema 2 de la sección 4.1, y son, además de los subgrupos impropios,

$$H_1 = \{I, \beta\}, H_2 = \{I, \alpha\beta\}, H_3 = \{I, \alpha^2\beta\} \text{ y } H = \{I, \alpha, \alpha^2\}.$$

Todo subgrupo impropio de cualquier grupo G es normal, lo que se deduce inmediatamente de examinar los conjuntos xGx^{-1} y $x\{e\}x^{-1}$ para todo $x \in G$ y aplicar la proposición 4.3.4. Tenemos pues que S_3 e $\{I\}$ son subgrupos normales de S_3. Examinemos si H_1 es normal:

$$\alpha H_1\alpha^{-1} = \alpha\{I, \beta\}\alpha^{-1} = \{\alpha, \alpha\beta\}\alpha^{-1} = \{\alpha, \alpha\beta\}\alpha^2$$
$$= \{\alpha^3, \alpha\beta\alpha^2\} = \{I, \alpha^2\beta\} \neq \{I, \beta\} = H_1.$$

Este resultado prueba que H_1 **no** es normal en S_3; de manera similar puede deducirse que H_2 y H_3 **no** son normales en S_3. Estudiemos finalmente si H es normal en S_3:

$$IHI^{-1} = H$$
$$\alpha H\alpha^{-1} = \alpha\{I, \alpha, \alpha^2\}\alpha^2 = \{I, \alpha, \alpha^2\} = H$$
$$\alpha^2 H(\alpha^2)^{-1} = \alpha^2\{I, \alpha, \alpha^2\}\ \alpha = \{I, \alpha, \alpha^2\} = H$$
$$\beta H\beta^{-1} = \beta\{I, \alpha, \alpha^2\}\ \beta = \{I, \beta\alpha\beta, \beta\alpha^2\beta\} = \{I, \alpha^2, \alpha\} = H$$
$$(\alpha\beta)H(\alpha\beta)^{-1} = (\alpha\beta)\ \{I, \alpha, \alpha^2\}\ (\alpha\beta) = \{I, \alpha^2, \alpha\} = H$$
$$(\alpha^2\beta)H(\alpha^2\beta)^{-1} = (\alpha^2\beta)\ \{I, \alpha, \alpha^2\}\ (\alpha^2\beta) = \{I, \alpha^2, \alpha\} = H\ .$$

De estas igualdades se deduce que H es normal en S_3.

Conviene en estos momentos hacer hincapié en dos errores que se pueden cometer cuando se trabaja con subgrupos normales. El primero de ellos es considerar que todo subgrupo abeliano de un grupo cualquiera es normal: esto no es cierto, como se pone de manifiesto si se considera el subgrupo H_1 de S_3 (véase el ejemplo D). El segundo de ellos es considerar que la igualdad $xHx^{-1} = H$ ha de hacerse elemento a elemento, es decir, $xhx^{-1} = h$ para todo $h \in H$: la falsedad de esta consideración es evidente a la vista del ejemplo anterior. De la igualdad $xHx^{-1} = H$ siempre puede asegurarse que dado $h \in H$, existe $h' \in H$ tal que $xhx^{-1} = h'$, pero h' puede no coincidir con h.

Del estudio realizado para encontrar los subgrupos normales de S_3 se deduce que es relativamente sencillo probar que un subgrupo no es normal, mientras que puede resultar bastante engorroso comprobar que es normal, puesto que deben encontrarse todos los conjuntos de la forma xHx^{-1} para cada $x \in G$. Es conveniente, entonces, disponer de algunos criterios para identificar subgrupos normales; este es el objetivo de los siguientes resultados.

Proposición 4.3.6. Si G es un grupo finito y H es un subgrupo de G tal que el índice de H en G es 2, H es un subgrupo normal de G.

Demostración. Basta probar que las clases de equivalencia por la izquierda coinciden con las clases de equivalencia por la derecha. Como sólo hay dos clases de equivalencia por la izquierda y H es una de ellas, la otra es G – H. También hay dos clases de equivalencia por la derecha ya que pueden ponerse en correspondencia biyectiva con las clases de equivalencia por la izquierda. Como H es una clase de equivalencia por la derecha, deducimos que G – H es también una clase de equivalencia por la derecha, y por tanto las clases de equivalencia por la izquierda y por la derecha coinciden. ■

Proposición 4.3.7. Si G es un grupo y H es un subgrupo de G con un número finito de elementos y es el único subgrupo de G de orden |H|, H es un subgrupo normal del G.

Demostración. Observamos primero que para todo $x \in G$, xHx^{-1} es un subgrupo de G (véase el ejercicio 1 al final de esta sección); a continuación observamos que el numero de elementos de xHx^{-1} es |H| (véase el ejercicio 2 al final de esta sección). Dado $x \in G$, como H es el único subgrupo de G de orden |H|, las dos observaciones anteriores implican que $xHx^{-1} = H$, o equivalentemente $xH = Hx$. Basta aplicar ahora la parte iii) de la proposición 4.3.4 para obtener el resultado deseado. ■

Dado un grupo G se define **el centro de G,** y se simboliza mediante Z(G), como el conjunto de los elementos de G que conmutan con todos los elementos de G, es decir:

$$Z(G) = \{g \in G: xg = gx \text{ para todo } x \in G\}.$$

★★ EJEMPLO E. El centro de cualquier grupo abeliano es el mismo grupo y el centro de un grupo no abeliano es un subconjunto del grupo. En cierto sentido, un grupo está lejos de ser abeliano cuando su centro es pequeño en comparación con el tamaño del grupo.

★★ EJEMPLO F. El centro de D_8 es $\{I, A^2\}$ (véase la definición de D_8 en la sección 3.6 del capítulo 3); claramente $I \in Z(D_8)$. Además

$$A^jA^2 = A^{j+2} = A^{2+j} = A^2A^j \quad j = 1,2,3$$

y

$$(A^jB)A^2 = A^j(A^2B) = A^2(A^jB) \quad j = 1, 2, 3$$

con lo que $A^2 \in Z(D_8)$. Ningún otro elemento pertenece al centro de D_8; baste como ejemplo observar que

$$AB \neq BA = A^3B .$$

Proposición 4.3.8. Si G es un grupo y J es un subgrupo de Z(G), se tiene necesariamente que J es un subgrupo normal de G. En particular Z(G) es un subgrupo normal de G.

Demostración. En primer lugar se ha de comprobar que Z(G) es un subgrupo de G, lo que se pide al lector en el ejercicio 3 de esta sección. Sea $x \in G$ y $j \in J$; puesto que $j \in J \subset Z(G)$, $xj = jx$, y entonces

$$xJx^{-1} = \{xjx^{-1} : j \in J\} = \{jxx^{-1} : j \in J\} = \{j : j \in J\} = J.$$

La proposición 4.3.4 demuestra ahora el resultado deseado. ■

EJERCICIOS 4.3

1. Demostrar que si H es un subgrupo de G y x es un elemento de G, xHx^{-1} es un subgrupo de G.
2. Sea G un grupo finito y x un elemento de G. Demostrar que la aplicación $f_x: G \to G$ dada por $f_x(g) = xgx^{-1}$ es biyectiva.
3. Demostrar que Z(G) es un subgrupo de G.

4. Encontrar todos los subgrupos normales de D_8.

5. Si K es un subgrupo normal de H y H es un subgrupo normal de G, ¿es K un subgrupo normal de G? Otra forma de hacer esta pregunta es la siguiente: ¿es la relación de normalidad entre los subgrupos de un grupo una relación transitiva? (Sugerencia: mirar en el retículo de los subgrupos de D_8.)

6. Si N es un subgrupo normal de G y N tiene dos elementos, demostrar que N está incluido en el centro de G.

7. Demostrar que si H y J son subgrupos normales de G, $H \cap J$ es también un subgrupo normal de G.

8. Sean H y J subgrupos normales de G tal que $H \cap J = \{e\}$; demostrar que $hj = jh$ para todo h de H y j de J.

9. Dar un ejemplo de un grupo G que posea un subgrupo normal H tal que H y G/H sean cíclicos, pero G no lo sea.

10. Si x es un elemento de un grupo G, definimos el **centralizador de x en G** mediante $C_G(x) = \{g \in G : xg = gx\}$. Demostrar que el centralizador de x en G es un subgrupo de G (observar que el centralizador de x en G es el conjunto de los elementos de G que conmutan con x).

11. Encontrar el centralizador para cada elemento de S_3, cada elemento de D_8 y para la matriz $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$.

12. Si H es un subgrupo de G definir entonces el **normalizador de H en G** como $N(H) = \{g \in G : gHg^{-1} = H\}$. Demostrar:

    a) N(H) es un subgrupo de G y H es un subgrupo normal de N(H).
    b) Si H es un subgrupo normal de otro subgrupo K de G, K es un subconjunto de N(H) (es decir, N(H) es el más grande de los subgrupos de G en los que H es normal).
    c) H es normal en G si y sólo si N(H) = G.

13. Sean H y K dos subgrupos de G tales que H está incluido en N(K), el normalizador de K en G. Demostrar que HK es un subgrupo de G (puede usarse el ejercicio 14 de la sección 4.2). Deducir que si H es un subgrupo de G y K es normal en G, HK es un subgrupo de G.

14. Sea N un subgrupo normal de G y x un elemento de G; demostrar que el orden de xN en G/N es un divisor del orden de x en G.

15. Sea G un grupo en el cual existe un entero $n > 1$ tal que $(ab)^n = a^n b^n$ para todos los elementos a y b de G. Sean $H_1 = \{x^n : x \in G\}$ y $H_2 = \{x \in G : \text{orden}(x) \mid n\}$. Demostrar que H_1 y H_2 son subgrupos normales de G.

16. Demostrar que

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \; ac \neq 0,\ a,\ b,\ c \in \mathbf{R} \right\},$$

con la operación de multiplicación, es un grupo; si

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G \right\}$$

demostrar que N es un subgrupo normal de G y que G/N es abeliano.

4.4. HOMOMORFISMOS DE GRUPOS

En esta sección daremos la definición de homomorfismo, que es una aplicación que conserva las operaciones de los grupos entre los que está definida, y estudiaremos algunas de sus propiedades en preparación para la sección siguiente en la que se demostrarán los importantes teoremas de isomorfía.

Definición 4.4.1. Sean $(G_1, *)$ y $(G_2, \circ)$ dos grupos y f una aplicación de G_1 en G_2. La aplicación f se dice que es un **homomorfismo de grupos** si para todo $x, y \in G_1$,

$$f(x * y) = f(x) \circ f(y).$$

Si no es necesario especificar las operaciones de los grupos, la propiedad de homomorfismo se escribe $f(xy) = f(x)f(y)$. Supongamos que f es un homomorfismo de grupos; si f es, además, una aplicación inyectiva diremos que f es un **monomorfismo;** si f es una aplicación suprayectiva, f se llamará **epimorfismo;** cuando f es biyectiva, diremos que f es un **isomorfismo.** Cuando existe un isomorfismo entre dos grupos G_1 y G_2, diremos que ambos grupos son **isomorfos** y escribiremos $G_1 \approx G_2$. Los isomorfismos entre un mismo grupo reciben el nombre de **automorfismos.**

★★ EJEMPLO A. La aplicación f dada por $f(x) = e^x$ es un monomorfismo de $(\mathbf{R}, +)$ en $(\mathbf{R}^*, \cdot)$: de la gráfica de f se deduce que es inyectiva y además $f(x + y) = e^{x+y} = e^x e^y = f(x)\, f(y)$. Esta misma aplicación es un isomorfismo de $(\mathbf{R}, +)$ en $(\mathbf{R}^+, \cdot)$.

★★ EJEMPLO B. La aplicación $f: (\mathbf{Z}, +) \to (\{-1, 1\}, \cdot)$ dada por $f(n) = (-1)^n$ es un epimorfismo: la suprayectividad es clara ya que $f(0) = 1$ y $f(1) = -1$; además

$$f(n + m) = (-1)^{n+m} = (-1)^n(-1)^m = f(n)\, f(m).$$

★★ EJEMPLO C. Si A es un grupo abeliano, $f(a) = a^2$ define un homomorfismo de A en A:

$$f(ab) = (ab)^2 = abab = a^2b^2 = f(a)\,f(b)$$

para todo a y b de A.

★★ EJEMPLO D. La aplicación $f: (GL_2(\mathbf{R}), \cdot) \to (\mathbf{R}^*, \cdot)$ dada por

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - cb$$

es un homomorfismo de grupos: recordar que el determinante de un producto de matrices es el producto de los determinantes de cada una de ellas o demostrar este resultado directamente.

★★ EJEMPLO E. Sea G un grupo y g un elemento de G; definimos $f_g: G \to G$ de manera que $f_g(x) = gxg^{-1}$ para todo elemento x de G; f_g es un homomorfismo de grupos puesto que

$$f_g(xy) = gxyg^{-1} = (gxg^{-1})\,(gyg^{-1}) = f_g(x)f_g(y).$$

f_g es, además, un isomorfismo: la propiedad suprayectiva es fácil y la inyectiva se deduce de las propiedades cancelativas del grupo. Como f_g es un isomorfismo de G en sí mismo, f_g es un automorfismo; estos automorfismos, uno para cada g, se llaman **automorfismos internos de G.**

★★ EJEMPLO F. Si V es el grupo de Klein, V y $\mathbf{Z}_4$ no son isomorfos. Escribamos $V = \{e, a, b, c\}$ donde $a^2 = b^2 = c^2 = e$ y $ab = c$; si existiera un isomorfismo f de $\mathbf{Z}_4$ en V, cualquiera que sea el valor de $f([x])$ se ha de tener $f([x] + [x]) = f([x])f([x]) = (f([x]))^2 = e$ para todo elemento [x] de $\mathbf{Z}_4$. En particular,

$$f([0]) = f([0] + [0]) = e \quad \text{y} \quad f([2]) = f([1] + [1]) = e.$$

Puesto que f es un isomorfismo, f es inyectiva y de $f([0]) = f([2])$ se deduce $[0] = [2]$. Esta contradición muestra la imposibilidad de que $\mathbf{Z}_4$ y V sean isomorfos.

Proposición 4.4.2. Sea f un homomorfismo entre los grupos G_1 y G_2; se tiene:

a) $f(e_1) = e_2$, donde e_1 es el elemento neutro de G_1 y e_2 es el elemento neutro de G_2.
b) $f(x^{-1}) = (f(x))^{-1}$ para todo elemento x de G_1.

Demostración. Para demostrar a) observar que si $g \in G$, $f(g)f(e_1) = f(ge_1) = f(g) = f(g)e_2$, de donde se deduce $f(e_1) = e_2$ usando la propiedad cancelativa.

Para demostrar b) utilizaremos a). Cualquiera que sea $x \in G_1$ tenemos

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e_1) = e_2$$

y

$$f(x^{-1})f(x) = f(x^{-1}x) = f(e_1) = e_2.$$

De la definición de inverso se sigue que el inverso de f(x) es $f(x^{-1})$, que era lo que queríamos demostrar. ■

Dado un homomorfismo f entre los grupos G_1 y G_2, definimos el **núcleo de f** mediante

$$N(f) = \{x \in G_1 : f(x) = e_2\},$$

donde e_2 es el elemento neutro de G_2 (en la literatura matemática inglesa el nucleo de f se representa mediante ker(f)). El núcleo de un homomorfismo juega un papel importante en el desarrollo de los teoremas de isomorfía que estudiaremos en la próxima sección.

★★ EJEMPLO G. En el ejemplo A, N(f) = {0}; en el ejemplo B, N(f) es el conjunto de todos los múltiplos enteros de 2; en el ejemplo C, N(f) es el conjunto de todos los elementos del grupo A que tienen orden 1 ó 2; en el ejemplo D, N(f) es el conjunto de todas las matrices de orden 2 con determinante 1; en el ejemplo E, N(f) = {e}. Observar que en aquellos homomorfismos que son inyectivos el núcleo solamente contiene al elemento identidad.

La siguiente proposición nos da algunas propiedades del núcleo de un homomorfismo.

Proposición 4.4.3. Sea f un homomorfismo entre los grupos G_1 y G_2; se tiene:

a) El núcleo de f, N(f), es un subgrupo normal de G_1.
b) f es un monomorfismo si y sólo si $N(f) = \{e_1\}$, donde e_1 es el elemento neutro de G_1.

Demostración. Comenzaremos demostrando que N(f) es un subgrupo de G_1; para ello usaremos la proposición 4.1.1. Si x e y son elementos del núcleo de f, $f(x) = e_2$ y $f(y) = e_2$, de donde se deduce

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y)^{-1}) = e_2e_2 = e_2.$$

En las igualdades anteriores se ha usado la proposición 4.4.2. Para demostrar que el núcleo de f es un subgrupo normal de G_1 sean $g \in G_1$ y $x \in N(f)$; puesto que

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)e_2f(g)^{-1} = e_2,$$

en donde se ha usado de nuevo la proposición 4.4.2, deducimos que gxg^{-1} es un elemento de N(f); esto es suficiente para mostrar que el núcleo de f es un subgrupo normal de G_1 de acuerdo con la proposición 4.3.4. La demostración de la parte a) está terminada.

Para demostrar la parte b) comencemos suponiendo que f es un monomorfismo; puesto que e_1 siempre pertenece al núcleo de f, debido a la proposición 4.4.2, sólo es necesario

demostrar que si x pertenece al núcleo de f, x coincide con el elemento neutro de G_1; si x es un elemento de N(f), $f(x) = e_2 = f(e_1)$, y como f es inyectiva $x = e_1$. Supongamos ahora que el núcleo de f es $\{e_1\}$ y sean x e y dos elementos de G_1 que satisfacen $f(x) = f(y)$; puesto que

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y)^{-1}) = f(y)(f(y)^{-1}) = e_2,$$

se deduce que $xy^{-1} \in N(f) = \{e_1\}$; por tanto $xy^{-1} = e_1$ o equivalentemente $x = y$; esto demuestra que f es un monomorfismo y termina la demostración de b). ■

La siguiente proposición clarifica el comportamiento de los homomorfismos frente a subgrupos y subgrupos normales.

Proposición 4.4.4. (Teorema de correspondencia entre homorfismos y subgrupos). Sea f un homomorfismo entre los grupos G_1 y G_2; se tiene:

a) Si H_1 es un subgrupo de G_1, $f(H_1)$ es un subgrupo de G_2.
b) Si H_2 es un subgrupo de G_2, $f^{-1}(H_2) = \{h \in G_1 : f(h) \in H_2\}$ es un subgrupo de G_1.
c) Si H_2 es un subgrupo normal de G_2, $f^{-1}(H_2)$ es un subgrupo normal de G_1.
d) Si H_1 es un subgrupo normal de G_1 y f es un homomorfismo suprayectivo, $f(H_1)$ es un subgrupo normal de G_2.

Demostración. Para demostrar a) sean h_2 y k_2 elementos de $f(H_1)$ y tratemos de probar que $h_2(k_2)^{-1}$ es un elemento de $f(H_1)$; como $h_2 \in f(H_1)$ existe $h_1 \in H_1$ tal que $f(h_1) = h_2$ y puesto que $k_2 \in f(H_1)$ existe $k_1 \in H_1$ tal que $f(k_1) = k_2$; entonces

$$h_2(k_2)^{-1} = f(h_1)f(k_1)^{-1} = f(h_1)f((k_1)^{-1}) = f(h_1(k_1)^{-1}),$$

en donde se ha usado la proposición 4.4.2 y la definición de homomorfismo. La igualdad anterior muestra que $h_2(k_2)^{-1}$ es un elemento de $f(H_1)$, que era lo que queríamos demostrar.

La demostración de la parte b) se deja para el lector. Para demostrar la parte c) basta observar que para todo g de G_1 y todo h_2 de H_2, si $f(h') = h_2$ se tiene

$$f(gh'g^{-1}) = f(g)f(h')f(g^{-1}) = f(g)(h_2)f(g)^{-1} \in H_2$$

por ser H_2 un subgrupo normal de G_2.

Demostraremos detalladamente la parte d). Tenemos que demostrar que si g_2 es un elemento de G_2, $g_2f(H_1)(g_2)^{-1}$ está incluido en $f(H_1)$; puesto que f es una aplicación suprayectiva, existe un elemento g_1 de H_1 tal que $f(g_1) = g_2$; de aquí se deduce que para todo h_1 de H_1

$$g_2f(h_1)(g_2)^{-1} = f(g_1)f(h_1)f(g_1)^{-1} = f(g_1)f(h_1)f((g_1)^{-1}) = f(g_1h_1(g_1)^{-1}).$$

Como H_1 es un subgrupo normal de G_1, $g_1h_1(g_1)^{-1}$ es un elemento de H_1, y por tanto la igualdad anterior demuestra que $g_2f(h_1)(g_2)^{-1}$ es un elemento de $f(H_1)$ para todo h_1 de H_1. ■

Observar que la parte a) de la proposición 4.4.3 es una consecuencia inmediata de las partes b) y c) de la proposición 4.4.4. puesto que $N(f) = f^{-1}(\{e_2\})$, donde e_2 es el elemento neutro de G_2. La suprayectividad del homomorfismo f en la parte d) de la proposición 4.4.4 es necesaria (véase el ejercicio 7 al final de esta sección).

Para determinar si dos grupos son isomorfos basta exhibir un isomorfismo entre ellos; así por ejemplo $(\mathbf{R}, +)$ y $(\mathbf{R}^+, \cdot)$ son isomorfos ya que entre ellos se ha encontrado un isomorfismo en el ejemplo A de esta misma sección. Para determinar que dos subgrupos no son isomorfos puede utilizarse la proposición que damos a continuación.

Proposición 4.4.5. Sea f un isomorfismo entre los grupos G_1 y G_2; se tiene que:

a) G_1 es abeliano si y sólo si G_2 es abeliano.
b) G_1 es cíclico si y sólo si G_2 es cíclico.

Demostración. Supongamos que G_1 es abeliano; si g_2 y h_2 son elementos de G_2, como f es suprayectiva existen g_1 y h_1 elementos de G_1 tales que $f(g_1) = g_2$ y $f(h_1) = h_2$; entonces

$$g_2h_2 = f(g_1)f(h_1) = f(g_1h_1) = f(h_1g_1) = f(h_1)f(g_1) = h_2g_2,$$

lo que demuestra que G_2 es abeliano. La implicación contraria es consecuencia de que f^{-1} es un isomorfismo si f lo es.

Supongamos ahora que G_1 es cíclico y que está generado por el elemento x; si g es un elemento de G_2, $f^{-1}(g)$ es un elemento de G_1 y por tanto existe un número entero n tal que $f^{-1}(g) = x^n$; de aquí deducimos la igualdad $g = f(x^n) = (f(x))^n$, y en consecuencia G_2 está generado por f(x), siendo, por tanto, cíclico. La implicación contraria se demuestra aplicando este resultado a f^{-1}, que es también un isomorfismo. ■

★★ EJEMPLO H. S_3 no puede ser isomorfo a $\mathbf{Z}_6$ ya que éste es abeliano mientras que el primero no lo es. Aunque $\mathbf{Z}_4$ y el grupo de Klein son ambos abelianos, no son isomorfos ya que el primero de ellos es cíclico y el segundo no lo es.

Dada una aplicación f entre dos conjuntos A y B siempre se cumple la inclusión $S \subseteq f^{-1}(f(S))$ para cualquier subconjunto S de A, donde $f^{-1}(f(S))$ es el conjunto de todos los elementos de A cuya imagen mediante f pertenece a f(S). La inclusión contraria no es cierta ni siquiera cuando f es un homomorfismo. Considerar la aplicación f de $(\mathbf{R}^*, \cdot)$ en $(\mathbf{R}^+ \cdot)$ dada por $f(x) = x^2$, que es un homomorfismo suprayectivo; si $S = \mathbf{R}^+$ se comprueba fácilmente que $f^{-1}(f(S)) = \mathbf{R}^*$, que es un conjunto más grande que S. El siguiente resultado, que se usará en la demostración de la segunda parte del primer teorema de isomorfía, que será tratado en la próxima sección, indica una condición bajo la cual la igualdad de estos dos conjuntos es cierta.

Proposición 4.4.6. Si f es un homomorfismo entre los grupos G_1 y G_2 y J es un subgrupo de G_1 que contiene al núcleo de f, $f^{-1}(f(J)) = J$.

Demostración. Basta demostrar la inclusión $f^{-1}(f(J)) \subset J$ ya que la inclusión contraria es siempre cierta. Si x es un elemento de $f^{-1}(f(J))$ se cumple que f(x) es un elemento de f(J), y por tanto existe un elemento j de J tal que f(x) = f(j); usando las propiedades de homomorfismo deducimos:

$$f(xj^{-1}) = f(x)f(j^{-1}) = f(x)f(j)^{-1} = f(j)f(j)^{-1} = e_2.$$

Por tanto xj^{-1} es un elemento del núcleo de f y en consecuencia de J, ya que este contiene a N(f); se tiene, pues, que xj^{-1} es un elemento de J, y como J es un subgrupo se deduce que x es también un elemento de J.

EJERCICIOS 4.4

1. Sea $f: (\mathbf{R}, +) \to (GL_2(\mathbf{R}), \cdot)$ la aplicación dada por

$$f(x) = \begin{pmatrix} \cos x & \text{sen } x \\ -\text{sen } x & \cos x \end{pmatrix}.$$

   Demostrar que f es un homomorfismo y calcular su núcleo.

2. Demostrar que $G = \{m + \sqrt{2}n : m, n \in \mathbf{Z}\}$ es un grupo con respecto a la suma. Demostrar que $H = \{5^k 3^s : k, s \in \mathbf{Z}\}$ es un grupo con respecto a la multiplicación. ¿Son G y H. isomorfos?

3. ¿Es $(\mathbf{R}^*, \cdot)$ isomorfo a $(\mathbf{R}, +)$? ¿Es $(\mathbf{R}^+, \cdot)$ isomorfo a $(\mathbf{Q}^+, \cdot)$? ¿Es $(\mathbf{Z}, +)$ isomorfo a $(\mathbf{Q}, +)$?

4. Si A es un grupo abeliano con n elementos y k es un entero primo con n, demostrar que la aplicación $f: A \to A$ definida por $f(a) = a^k$ es un isomorfismo.

5. Sea $G_1 = (\mathbf{R}^3, +)$ y $G_2 = (\mathbf{R}^2, +)$ dos grupos. ¿Es f(a, b, c) = (a, b) un homomorfismo de G_1 en G_2?

6. Si $G = (\mathbf{R}^2, +)$ y M es una matriz cuadrada con coeficientes reales, demostrar que $f_M : G \to G$ definida por $f_M((x,y)) = (x,y)M$ es un homomorfismo de grupos. ¿Cuándo es f_M un isomorfismo?

7. Dar un ejemplo en el que se muestre que la suprayectividad es necesaria en la parte d) de la proposición 4.4.4. (Sugerencia: encontrar un homomorfismo no suprayectivo de S_3 en S_3).

8. Si f es un isomorfismo entre los grupos G y G', demostrar que f^{-1} es un isomorfismo entre los grupos G' y G. Probar que en el conjunto $\mathscr{G}$ de todos los grupos la relación $G \approx G'$ (es decir, G y G' son isomorfos) es de equivalencia.

9. a) Demostrar que la aplicación $f: G \to G$ definida por $f(g) = g^{-1}$ es un automorfismo de G si y sólo si G es abeliano.

b) Dado $g \in G$, demostrar que la aplicación $I_g : G \to G$ dada por $I_g(x) = gxg^{-1}$ es un automorfismo (este es el ejemplo E dado en esta sección, del que se pide al lector que complete los detalles de la demostración). Recordar que éstos se llaman **automorfismos internos** de G.

10. Sean B(G), Aut(G) e I(G) los conjuntos de biyecciones, automorfismos y automorfismos internos de G; demostrar que Aut(G) es un subgrupo de B(G) e I(G) es un subgrupo normal de Aut(G) (en todos ellos la operación que se debe considerar es la composición de aplicaciones).

11. Sea $f: G_1 \to G_2$ un monomorfismo de grupos; demostrar que x e y conmutan en G_1 si y sólo si f(x) y f(y) conmutan en G_2; utilizar este resultado para demostrar que si G_2 es abeliano, G_1 es también abeliano.

12. Sea $f: G_1 \to G_2$ un monomorfismo de grupos; demostrar que x y f(x) tienen el mismo orden, cualquiera que sea el elemento x de G_1.

13. Sea N un subgrupo normal de G cuyo índice en G es n; demostrar que si n y m son primos entre sí, la relación $x^m = e$ implica que x es un elemento de N.

14. Se G un grupo abeliano con n elementos y p un entero primo con n; demostrar que para todo $a \in G$ la ecuación $x^p = a$ tiene una solución en G (Sugerencia: utilizar el problema 4 de esta misma sección).

15. Supongamos que existe un entero n tal que la aplicación $f(x) = x^n$ es un automorfismo de G. Demostrar que para todo elemento x de G, x^{n-1} pertenece al centro de G (véase la definición de centro de G al final de la sección 3).

4.5. TEOREMAS DE ISOMORFÍA

Una de las técnicas más fecundas en la teoría de grupos es la relación existente entre subgrupos normales y homomorfismos; tal relación queda plasmada en el **primer teorema de isomorfía,** que es uno de los resultados principales de esta sección. Para demostrarlo es necesario introducir nociones nuevas.

Si H es un subgrupo normal de G, podemos considerar el grupo cociente G/H; la aplicación $\pi : G \to G/H$ dada por $\pi(g) = gH$ es un **homomorfismo suprayectivo**, que recibe el nombre de **homomorfismo canónico con núcleo H**. El hecho de que π es un homomorfismo se deduce de que si $x, y \in G$,

$$\pi(xy) = (xy)H = (xH)\,(yH) = \pi(x)\,\pi(y),$$

donde la igualdad central es debida a que H es un subgrupo normal de G; la suprayectividad de π es consecuencia fácil de su definición.

Supongamos ahora que tenemos un homomorfismo f entre los grupos G_1 y G_2; por la proposición 4.4.3 sabemos que N(f) es un subgrupo normal de G_1; si denominamos π al homomorfismo canónico con núcleo N(f) podemos formar el diagrama de la ilustración 5.

¿Puede definirse un homomorfismo $F : G/N(f) \to G_2$ de manera que $F \circ \pi = f$? Esto puede hacerse definiendo

$$F(xN(f)) = f(x)$$

para todo $x \in G_1$. Puesto que $G_1/N(f)$ es un conjunto de clases de equivalencia, se ha de comprobar en primer lugar que si las clases xN(f) e yN(f) coinciden, f(x) = f(y); esto es cierto puesto que de la igualdad xN(f) = yN(f) se deduce que y = xn con $n \in N(f)$, con lo cual f(y) = f(xn) = = f(x)f(n) = f(x)e = f(x).

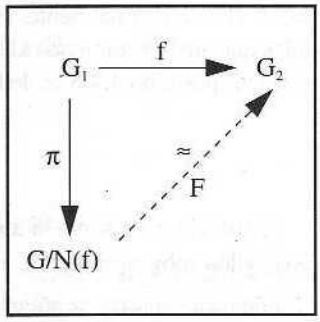


Ilustración 5

F es un homomorfismo puesto que

$$F(xN(f)\ yN(f)) = F(xyN(f)) = f(xy) = f(x)f(y) = F(xN(f))F(yN(f)),$$

igualdades que el lector debe comprobar cuidadosamente.

El homomorfismo F tiene la propiedad adicional de que es inyectivo: si $F(xN(f)) = e_2$ se tiene que $f(x) = e_2$ y por tanto $x \in N(f)$; así pues xN(f) = N(f), lo que prueba que f es inyectiva debido a la parte b) de la proposición 4.4.3.

Si f es un homomorfismo suprayectivo, F también lo es, puesto que si $y \in G_2$ basta tomar $x \in G_1$ tal que f(x) = y, y observar que

$$F(xN(f)) = f(x) = y.$$

Estas propiedades constituyen la primera de las afirmaciones del teorema fundamental de homomorfismos de grupos que se enuncia a continuación:

Primer teorema de isomorfía.

Sea $f : G_1 \to G_2$ un homomorfismo suprayectivo entre los grupos G_1 y G_2 con núcleo N(f).

i) $G_1/N(f)$ es isomorfo a G_2.

ii) Existe una correspondencia biyectiva entre los subgrupos de G_2 y los subgrupos de G_1 que contienen a N(f).

Demostración. La parte i) ha quedado demostrada anteriormente. Demostraremos a continuación la parte ii) del teorema. Sea $\mathscr{C}_N(G_1)$ el conjunto de los subgrupos de G_1 que contienen a N(f), y $\mathscr{C}(G_2)$ el conjunto de los subgrupos de G_2; definimos la aplicación H entre los

conjuntos $\mathscr{C}_N(G_1)$ y $\mathscr{C}(G_2)$ de manera que si J es un subgrupo que contiene al núcleo de f, H(J) = f(J). Observar que por la proposición 4.4.4, f(J) es un subgrupo de G_2 y por tanto H está bien definida; H es suprayectiva ya que si K es un subgrupo de G_2, $J = f^{-1}(K)$ es un subgrupo de G_1 (véase la proposición 4.4.4) que contiene al núcleo de f y satisface $H(J) = f(J) = f(f^{-1}(K)) = K$; finalmente, H es inyectiva, ya que si J_1 y J_2 son dos subgrupos distintos de G_1 tales que ambos contienen al núcleo de f, $H(J_1)$ y $H(J_2)$ no coinciden, puesto que si $f(J_1) = f(J_2)$, de la proposición 4.4.6 se deduce que

$$J_1 = f^{-1}(f(J_1)) = f^{-1}(f(J_2)) = J_2.$$

Esto demuestra que la aplicación H, definida entre los subgrupos de G_1 que contienen a N(f) y los subgrupos de G_2, es la biyección buscada. ∎

★★ EJEMPLO A. En el ejemplo D de la sección 4.4 se demostró que la aplicación $f : (GL_2(\mathbf{R}), \cdot) \to (\mathbf{R}^*, \cdot)$ dada por

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - cb$$

es un homomorfismo; dado un número real r, no nulo, la matriz $\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbf{R})$ y

$$f\left(\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}\right) = r\ ,$$

con lo que queda probado que f es un homomorfismo suprayectivo. Puesto que

$$N(f) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - cd = 1\right\} = SL_2(\mathbf{R})$$

(véase la sección 3.5 del capítulo 3 para la definición de $SL_2(\mathbf{R})$), el primer teorema de isomorfía nos permite deducir el siguiente isomorfismo:

$$GL_2(\mathbf{R})/SL_2(\mathbf{R}) \approx (\mathbf{R}^*, \cdot)\ .$$

★★ EJEMPLO B. Dado un número entero positivo n se define $f_n : (\mathbf{Z}, +) \to (\mathbf{Z}_n, +)$ mediante $f_n(z) = [z]$; f es un homomorfismo debido al teorema 2.4.4 y es claramente suprayectivo. Puesto que

$$N(f) = \{z \in \mathbf{Z} : f_n(z) = [0]\} = \{z \in \mathbf{Z} : z \equiv 0\ (n)\} = n\mathbf{Z},$$

deducimos que

$$\mathbf{Z}/n\mathbf{Z} \approx (\mathbf{Z}_n, +).$$

★★ EJEMPLO C. Dados dos números enteros positivos n y m definir $f : (n\mathbb{Z}, +) \to (\mathbb{Z}_m, +)$ mediante $f(nz) = [z]$; f es un homomorfismo debido al teorema 2.4.4 y es claramente suprayectivo. Puesto que

$$N(f) = \{nz \in n\mathbb{Z} : f(nz) = [0]\} = \{nz \in n\mathbb{Z} : z \equiv 0\ (m)\}$$
$$= \{nz \in n\mathbb{Z} : z = km, k \in \mathbb{Z}\} = \{nmk : k \in \mathbb{Z}\} = nm\mathbb{Z},$$

deducimos que

$$n\mathbb{Z}/nm\mathbb{Z} \approx \mathbb{Z}_m,$$

que es una generalización del resultado obtenido en el ejemplo B.

★★ EJEMPLO D. Sea $f : D_8 \to V$ dada por $f(A) = a$ y $f(B) = b$, donde $A^4 = B^2 = I$ y $BA = A^3B$ en D_8 y $a^2 = b^2 = (ab)^2 = e$ en el grupo de Klein V; esta aplicación se extiende a un homomorfismo entre los grupos dados ya que A y B generan D_8. Se tiene que f es un homomorfismo suprayectivo ya que $f(AB) = f(A)f(B) = ab$ y su núcleo es $N(f) = \{I, A^2\}$ como puede comprobar el lector si calcula las imágenes mediante f de todos los elementos de D_8. Por la primera parte del primer teorema de isomorfía obtenemos $D_8/\{I, A^2\} \approx V$.

Si miramos al retículo de los subgrupos de D_8 (véase el ejercicio 2 de la sección 4.1 y la ilustración 6) y al de V, se observa que el retículo de los subgrupos de V está en correspondencia biyectiva con el retículo de los subgrupos de D_8 que contienen a $\langle A^2\rangle = \{I, A^2\} = N(f)$. Esto sirve para ilustrar la segunda parte del primer teorema de isomorfía.

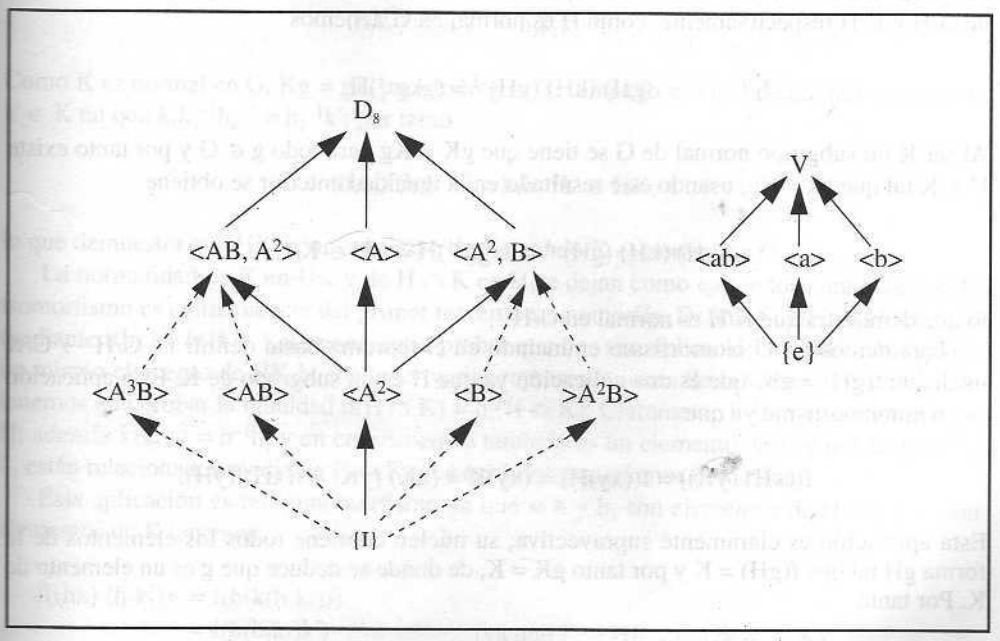


Ilustración 6. Retículos de D_8 y del grupo de Klein

★★ EJEMPLO E. ¿Cuáles son los posibles núcleos de homomorfismos suprayectivos de D_8 en V que contengan exactamente dos elementos? Mirando al retículo de los subgrupos de D_8 (véase la ilustración 6) se observa que los posibles núcleos de este homomorfismo son

$$\langle A^3B\rangle, \quad \langle AB\rangle, \quad \langle A^2\rangle, \quad \langle B\rangle \quad \text{y} \quad \langle A^2B\rangle.$$

El retículo de los subgrupos de D_8 que contienen a uno cualquiera de los subgrupos $\langle A^3B\rangle$, $\langle AB\rangle$, $\langle B\rangle$ o $\langle A^2B\rangle$ no se "corresponde" con el retículo de los subgrupos de V; por la segunda parte del primer teorema de isomorfía no pueden existir homomorfismos de D_8 en V que tengan como núcleo estos subgrupos; así pues, el único subgrupo de D_8 que puede ser núcleo de un homomorfismo de D_8 en V es $\{I, A^2\}$.

Para terminar esta sección enunciamos dos teoremas que también se conocen con el nombre de teoremas de isomorfía y que tienen varias aplicaciones en la teoría de grupos. Ambos son consecuencia del primer teorema de isomorfía.

Segundo teorema de isomorfía. Sea G un grupo, H y K subgrupos normales de G y H subgrupo de K. Entonces K/H es un subgrupo normal de G/H y

$$G/H\Big/_{K/H} \approx G/K$$

Demostración. Puesto que K es un subgrupo de G se deduce inmediatamente que K/H es un subgrupo de G/H. Demostraremos que K/H es normal en G/H. Sean gH y kH elementos de G/H y K/H respectívamente; como H es normal en G, tenemos

$$(gH)\,(kH)\,(gH)^{-1} = (gkg^{-1})H.$$

Al ser K un subgrupo normal de G se tiene que $gK = Kg$ para todo $g \in G$ y por tanto existe $k' \in K$ tal que $gk = k'g$; usando este resultado en la igualdad anterior se obtiene

$$(gH)\,(kH)\,(gH)^{-1} = (k'gg^{-1})H = k'H \in K/H,$$

lo que demuestra que K/H es normal en G/H.

Para demostrar el isomorfismo enunciado en el teorema basta definir $f : G/H \to G/K$ mediante $f(gH) = gK$, que es una aplicación ya que H es un subgrupo de K. Esta aplicación es un homomorfismo ya que

$$f((xH)\,(yH)) = f((xy)H) = (xy)K = (xK)\,(yK) = f(xH)f(yH).$$

Esta aplicación es claramente suprayectiva; su núcleo contiene todos los elementos de la forma gH tal que $f(gH) = K$ y por tanto $gK = K$, de donde se deduce que g es un elemento de K. Por tanto

$$N(f) = \{gH: g \in K\} = K/H.$$

Aplicando el primer teorema de isomorfía se demuestra el resultado deseado (véase la ilustración 7). ■

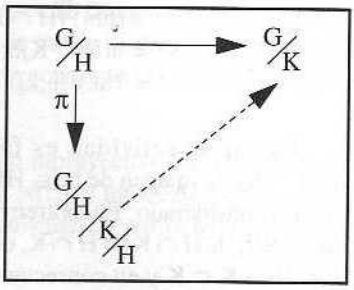


Ilustración 7

★★ EJEMPLO F. Si n y m son dos enteros positivos y en todos los grupos que escribimos a continuación usamos la adición, se tienen los siguientes isomorfismos:

$$\mathbf{Z}_{mn}/\mathbf{Z}_m \approx \mathbf{Z}/mn\mathbf{Z}\Big/_{n\mathbf{Z}/mn\mathbf{Z}} \approx \mathbf{Z}/n\mathbf{Z} \approx \mathbf{Z}_n.$$

En el primer y tercer isomorfismo se han usado los ejemplos C y B de esta misma sección y en el del centro se ha usado el segundo teorema de isomorfía.

Tercer teorema de isomorfía. Sea G un grupo y H y K subgrupos de G con K normal en G. Entonces HK es un subgrupo de G, K es normal en HK y $H \cap K$ es normal en H. Además,

$$HK/K \approx H/(H \cap K).$$

Demostración. En general HK no es un subgrupo de G (véase el ejercicio 13 de la sección 4.2), pero en este caso la normalidad de K en G nos permite demostrar que sí lo es. Para probarlo, elegir h_1k_1 y h_2k_2 dos elementos de HK y considerar

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}.$$

Como K es normal en G, $Kg = gK$ para todo $g \in G$; tomando $g = h_2^{-1}$ deducimos que existe $k' \in K$ tal que $k_1k_2^{-1}h_2^{-1} = h_2^{-1}k'$; por tanto

$$(h_1k_1)(h_2k_2)^{-1} = h_1h_2^{-1}k' \in HK,$$

lo que demuestra que HK es un subgrupo de G cuando K es normal en G.

La normalidad de K en HK y de $H \cap K$ en H se dejan como ejercicios para el lector. El isomorfismo es consecuencia del primer teorema de isomorfía. Definir $f : HK \to H/(H \cap K)$ mediante $f(hk) = h(H \cap K)$; es necesario probar que f es una aplicación bien definida ya que un mismo elemento de HK puede tener varias representaciones de la forma hk: si $hk = h_1k_1$ tenemos que probar la igualdad $h(H \cap K) = h_1(H \cap K)$. Claramente $h^{-1}h_1$ es un elemento de H; además $k(k_1)^{-1} = h^{-1}h_1$ y en consecuencia también es un elemento de K y por tanto h^{-1} y h_1 están relacionados mediante $H \cap K$, que era lo que queríamos demostrar.

Esta aplicación es un homomorfismo ya que si h y h_1 son elementos de H y k y k_1 son elementos de K tenemos:

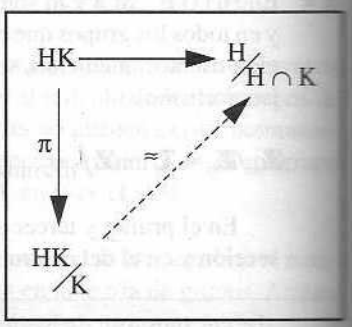
$$\begin{aligned} f((hk)(h_1k_1)) &= f(h(k(h_1k_1))) \\ &= f(h(h_1k_1)k') \qquad \text{(ya que } K \lhd HK \text{ y donde } k' \in K) \\ &= f((hh_1)(k_1k')) \end{aligned}$$

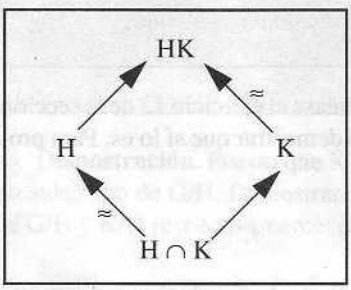
$= (hh_1)(H \cap K)$
$= h(H \cap K)h_1(H \cap K)$ (debido a la operación de $H/(H \cap K)$)
$= f(hk)f(h_1k_1)$ (debido a la definición de f).

La suprayectividad es fácil ya que, elegido $h(H \cap K)$, la imagen de $he \in HK$ mediante f es el elemento considerado. Encontremos ahora su núcleo. Si $hk \in N(f)$, $h(H \cap K) = H \cap K$, de donde se deduce que $h \in H \cap K \subset K$ y en consecuencia $hk \in K$. Por tanto N(f) está incluido en K. Por otro lado, si $k \in K$,

$$f(k) = f(ke) = e(H \cap K) = (H \cap K)$$

y por tanto K está incluido en N(f). Esto demuestra que N(f) = K y el resultado se deduce del primer teorema de isomorfía. ■





Si en el retículo de los subgrupos de G se dibujan solamente los subgrupos H, K, HK y $H \cap K$ y sus correspondientes inclusiones, se obtiene un gráfico en forma de rombo como en la ilustración de la izquierda, en donde se han marcado con dos líneas paralelas los cocientes que son isomorfos. La figura que se obtiene es la base para que, en algunas ocasiones, el tercer teorema de isomorfía reciba el nombre de "teorema del rombo".

★★ EJEMPLO G. Si n y m son números enteros, $n\mathbf{Z}$ y $m\mathbf{Z}$ son subgrupos del grupo $(\mathbf{Z}, +)$. Escribiendo el tercer teorema de isomorfía para estos subgrupos con notación aditiva se obtiene el isomorfismo

$$(n\mathbf{Z} + m\mathbf{Z})/m\mathbf{Z} \approx n\mathbf{Z}/(n\mathbf{Z} \cap m\mathbf{Z}).$$

EJERCICIOS 4.5

1. Si H y K son subgrupos de G y K es normal en G, demostrar que K es normal en HK.
2. Si H y K son subgrupos de G y K es normal en G, demostrar que $H \cap K$ es normal en H.
3. Escribir el isomorfismo que se obtiene al aplicar la primera parte del primer teorema de isomorfía al homomorfismo suprayectivo del ejercicio 5 de la sección 4.4.
4. Sea f un homomorfismo suprayectivo de G en $\mathbf{Z}$. Demostrar que para todo número entero positivo n, G tiene un subgrupo normal de índice n (Sugerencia: definir un homomorfismo suprayectivo de G en $\mathbf{Z}_n$ y usar el primer teorema de isomorfía).

5. Sea G un grupo y N un subgrupo normal de G tal que $G/N \approx \mathbb{Z}$. Demostrar que para todo número entero positivo n, G tiene un subgrupo normal de índice n. (Sugerencia: usar el isomorfismo dado para definir un homomorfismo suprayectivo de G en $\mathbb{Z}$ y aplicar el resultado del problema 4.)

6. Sean G_1 y G_2 dos grupos y $f : G_1 \to G_2$ un homomorfismo suprayectivo con núcleo N(f). Demostrar que si J es un subgrupo de G_1 que contiene a N(f), el índice de J en G_1 coincide con el índice de f(J) en G_2 (considerar clases de equivalencia por la izquierda para hacer la demostración).

7. Dar un ejemplo en el que el resultado del problema anterior no sea cierto cuando J no contiene a N(f). (Sugerencia: mirar el ejemplo D de esta sección.)

8. Sean G_1, G_2, f y N(f) como en el ejercicio 6 de esta sección. Si J_1 y J_2 son dos subgrupos de G_1 que contienen a N(f) y J_1 contiene a J_2, demostrar que

$$[J_1 : J_2] = [f(J_1) : f(J_2)].$$

(No trabajar demasiado: aplicar el ejercicio 6).

9. Sea D_{2n} el grupo diédrico de orden 2n (véase la sección 3.6 del capítulo 3). Demostrar que $N = \{I, A, A^2, \ldots, A^{n-1}\}$ es un subgrupo normal de G y que $G/N \approx \{-1, 1\}$, donde $\{-1, 1\}$ es un grupo con respecto a la multiplicación.

10. Dado un grupo G y un subgrupo normal N tal que G/N es cíclico de orden 6, describir el retículo de los subgrupos de G que contienen a N.

11. Sea G un grupo finito, N y M subgrupos normales de G y H subgrupo de G de órdenes n, m y h respectivamente. Si (n, h) = 1 y (m, h) = 1, demostrar que

$$HM/M \approx HN/N.$$

12. Probar que si K es un subgrupo normal de G de índice primo p, para todo subgrupo H de G se tiene que o bien H es un subgrupo de K o bien G = HK con $[H : H \cap K] = p$. (Sugerencia: usar los dos últimos teoremas de isomorfía.)

4.6. CLASIFICACIÓN DE LOS GRUPOS CÍCLICOS

El concepto de grupo cíclico fue introducido en la sección 4.1; recordemos que un grupo es cíclico si está generado por un sólo elemento, es decir existe un elemento g del grupo tal que todos los demás se obtienen operando este elemento repetidas veces con sí mismo; en notación multiplicativa todos los elementos del grupo son de la forma g^n con n un número entero; si la operación del grupo es la adición, todos los elementos son de la forma ng. Recordar que $(\mathbb{Z}, +)$ y $(\mathbb{Z}_n, +)$ son grupos cíclicos con generadores 1 y [1] respectívamente . En esta sección demostraremos que, salvo isomorfismos, éstos son todos los grupos cíclicos que existen.

Teorema 4.6.1. (Clasificación de los grupos cíclicos).

i) Si G es un grupo cíclico con infinitos elementos, G es isomorfo a $(\mathbb{Z}, +)$.
ii) Si G es un grupo cíclico con n elementos, G es isomorfo a $(\mathbb{Z}_n, +)$.

Demostración. Comenzamos demostrando la parte i) del teorema. Si g es un generador de G, definimos $f : \mathbb{Z} \to G$ mediante $f(k) = g^k$. Se tiene que f es un homomorfismo puesto que para cualquier par de números enteros k y s se tiene

$$f(k + s) = g^{k+s} = g^k g^s = f(k)f(s) .$$

El homomorfismo f es suprayectivo puesto que G es cíclico y es inyectivo ya que si $g^k = e$ para algún entero k, $k = 0$ debido a que G posee infinitos elementos (en caso contrario $G = \langle g \rangle$ no podría poseer más de k elementos). Esto prueba que G es isomorfo a $(\mathbb{Z}, +)$.

Demostramos ahora la segunda parte del teorema; la demostración se basa en el primer teorema de isomorfía. Escribir $G = \langle g \rangle = \{g, g^2, \ldots, g^{n-1}, g^n = e\}$ con $g^j \neq g^k$ si $j \neq k$. La aplicación $f : \mathbb{Z} \to G$ dada por $f(k) = g^k$ es un homomorfismo suprayectivo al igual que en la parte primera. Sin embargo, f no es inyectiva ya que

$$N(f) = \{k \in \mathbb{Z} : f(k) = e\} = \{k \in \mathbb{Z} : g^k = e\} = \{m : m \text{ es múltiplo de } n\} = n\mathbb{Z} .$$

Utilizando el primer teorema de isomorfía deducimos que $G \approx \mathbb{Z}/n\mathbb{Z}$; por el ejemplo B de la sección 4.5 se tiene que $\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$, con lo cual $G \approx \mathbb{Z}_n$, que era lo que queríamos demostrar.

■

★★ EJEMPLO A **Todos los subgrupos de $(\mathbb{Z}, +)$ son cíclicos.** En efecto, si H es un subgrupo de $\mathbb{Z}$ y $H \neq \{0\}$, considerar

$$m = \inf\{h : h \in H \cap \mathbb{Z}^+\}$$

(es decir, m es el menor entero positivo de H); demostraremos que $H = \langle m \rangle$. Puesto que $m \in H$ se tiene que $\langle m \rangle \subset H$. Por otro lado, si $h \in H$, dividiendo entre m se tiene $h = cm + r$ con $0 \leq r < m$; entonces $r = h - cm \in H + \langle m \rangle \subset H$. Como r es un entero positivo menor que m o cero, y m se había elegido como el menor entero positivo de H, se tiene $r = 0$, con lo cual $h = cm \in \langle m \rangle$. Esto prueba que $H = \langle m \rangle$, y por tanto que H es cíclico.

También puede demostrarse, haciendo uso del resultado del ejemplo A y del primer teorema de isomorfía, que todos los subgrupos de $(\mathbb{Z}_n, +)$ son cíclicos; este es el contenido del ejercicio 5 propuesto al final de esta sección. Una vez hechas estas observaciones y teniendo

en cuenta el teorema 4.6.1 no es de extrañar que todo subgrupo de un grupo cíclico sea cíclico; este es el contenido del resultado que se expone a continuación.

Proprosición 4.6.2. Todo subgrupo de un grupo cíclico es cíclico.

Demostración. Sea G un grupo generado por el elemento g y H un subgrupo de G; consideremos m como el más pequeño de los enteros positivos k tal que g^k es un elemento de H; observar que este ínfimo existe debido al principio del mínimo enunciado en la sección 2.1 del capítulo 2. Demostraremos que H coincide con el subgrupo generado por g^m.

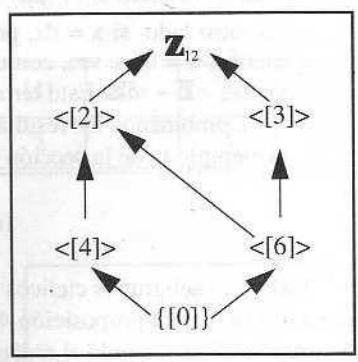
Como $g^m \in H$ y H es un subgrupo de G, se deduce inmediatamente que $\langle g^m \rangle \subset H$. Para demostrar la otra inclusión consideremos un elemento h de H; como h es también un elemento de G y G es cíclico, existe un entero s tal que $h = g^s$; por el algoritmo de la división podemos escribir $s = cm + r$ con $0 \leq r < m$; entonces $h = g^s = g^{cm}g^r$, de donde se deduce $g^r = g^s(g^m)^{-c} = h(g^m)^{-c}$; como tanto h como g^m son elementos de H, deducimos que g^r es también un elemento de H. Como r es un entero no negativo más pequeño que m, de la definición de m se deduce que $r = 0$; por tanto

$$h = g^s = g^{cm} = (g^m)^c \in \langle g^m \rangle.$$

Esto demuestra que $H = \langle g^m \rangle$ y, en consecuencia, H es cíclico. ■

★★ EJEMPLO B. Todos los subgrupos de $(\mathbf{Z}_{12}, +)$ son cíclicos; para hallarlos todos basta con mirar los subgrupos que generan cada uno de los elementos de este grupo. Estos son:

$$\langle [1] \rangle = \mathbf{Z}_{12}$$
$$\langle [2] \rangle = \{[2], [4], [6], [8], [10], [0]\}$$
$$\langle [3] \rangle = \{[3], [6], [9], [0]\}$$
$$\langle [4] \rangle = \{[4], [8], [0]\}$$
$$\langle [5] \rangle = \{[5], [10], [3], [8], [1], [6], [11], [4], [9], [2], [7], [0]\} = \mathbf{Z}_{12}$$
$$\langle [6] \rangle = \{[6], [0]\}$$
$$\langle [7] \rangle = \mathbf{Z}_{12}, \quad \langle [8] \rangle = \langle [4] \rangle, \quad \langle [9] \rangle = \langle [3] \rangle,$$
$$\langle [10] \rangle = \langle [2] \rangle \quad \text{y} \quad \langle [11] \rangle = \mathbf{Z}_{12}.$$



El retículo de los subgrupos de este grupo se muestra en la ilustración de la derecha.

★★ EJEMPLO C. Sean $n\mathbf{Z}$ y $m\mathbf{Z}$ dos subgrupos de $(\mathbf{Z}, +)$. Los subconjuntos $n\mathbf{Z} \cap m\mathbf{Z}$ y $n\mathbf{Z} + m\mathbf{Z}$ son subgrupos de este grupo como puede comprobarse fácilmente; como $(\mathbf{Z}, +)$ es cíclico, ambos deben estar generados por un solo elemento, es decir han de ser de la forma $k\mathbf{Z}$ y $d\mathbf{Z}$, respectivamente, con k y d números enteros. El lector debe hacer algunas pruebas antes de continuar y así no le parecerán desacertados los siguientes resultados.

El subgrupo $n\mathbb{Z} \cap m\mathbb{Z}$ está generado por [n, m], donde [n, m] es el mínimo común múltiplo de n y m, y por tanto

$$n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z}.$$

Si x es un elemento de la intersección podemos escribir $x = nu$ y $x = mv$ con u y v enteros; por tanto x es un múltiplo común de n y m y ha de ser por tanto un múltiplo de [n, m]. Por otro lado, si $x = [n, m]z$, con z entero, y d es el máximo común divisor de n y m, podemos escribir

$$x = [n, m]z = n(m/d)z \in n\mathbb{Z}, \quad \text{y}$$
$$x = [n, m]z = m\,(n/d)z \in m\mathbb{Z},$$

de donde se deduce que x pertenece a la intersección. De esta manera queda demostrado el resultado deseado.

El subgrupo $n\mathbb{Z} + m\mathbb{Z}$ está generado por (n, m), donde (n, m) es el máximo común divisor de n y m, y por tanto

$$n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}.$$

Si d es el máximo común divisor de n y m se tiene que $n = ld$ y $m = sd$ con l y s números enteros; además, si x es un elemento del conjunto suma se tiene $x = nu + mv$ con u y v números enteros; por tanto:

$$x = nu + mv = ldu + sdv = d(lu + sv) \in (n, m)\mathbb{Z}.$$

Por otro lado, si $x = dz$, por la propiedad lineal del máximo común divisor podemos escribir $d = un + vm$, con u y v enteros (véase el corolario 2.2.3); por tanto $x = unz + vmz \in n\mathbb{Z} + m\mathbb{Z}$. Esto termina la demostración del resultado enunciado.

Combinando los resultados que acabamos de exponer y el isomorfismo obtenido en el ejemplo G de la sección 4.5 tenemos

$$(n, m)\mathbb{Z}/m\mathbb{Z} \approx n\mathbb{Z}/[n, m]\mathbb{Z}.$$

Todos los subgrupos cíclicos han quedado caracterizados, salvo isomorfismos, en el teorema 4.6.1, y en la proposición 4.6.2 se ha descrito cómo deben ser todos los subgrupos de un grupo cíclico. Cuando el orden del grupo cíclico es finito se puede decidir el orden de cada uno de sus elementos a partir del orden del grupo; además, en este caso, el número de subgrupos del grupo coincide con el número de divisores del orden del grupo. Este es el contenido de los dos resultados siguientes.

Proposición 4.6.3. Sea G un grupo y x un elemento de G de orden n; el orden de x^k es n/(n, k), donde (n, k) es el máximo común divisor de n y k. En particular, si k divide a n, x^k tiene orden n/k.

Demostración. Sea d el máximo común divisor de n y k; existen, por tanto, dos números enteros a y b tales que n = ad y k = bd. A partir de aquí podemos escribir

$$(x^k)^{n/d} = x^{ka} = x^{bda} = (x^n)^b = e;$$

de aquí se deduce que el orden de x^k es un divisor de n/d.

Sea c el orden de x^k; como $x^{kc} = e$, deducimos que n es un divisor de kc y por tanto n/d es un divisor de (k/d)c; puesto que n/d y k/d son primos entre sí (véase ejercicio 3 de la sección 2.2), se ha de tener que n/d divide a c. De esta manera queda probado el resultado deseado. ■

Proposición 4.6.4. Sea G un grupo cíclico de orden n. Si k es un entero positivo que divide a n, existe un **único** subgrupo H de G con k elementos. Por tanto, el conjunto de todos los subgrupos de G está en correspondencia biyectiva con todos los divisores positivos de n.

Demostración. Sea x un generador de G. Si k divide a n, $x^{(n/k)}$ es un elemento de orden k según la proposición anterior y por tanto el subgrupo H generado por este elemento tiene orden k. Así queda probada la existencia de un subgrupo de orden k.

Para demostrar la unicidad supongamos que K es otro subgrupo de G con k elementos; como G es cíclico, K también lo es y por tanto está generado por un elemento x^m, con m el menor entero positivo tal que $x^m \in K$. Por la proposición anterior k = n/(n, m) y por tanto

$$x^m = x^{(n,\,m)(m/(n,\,m))} \in \langle x^{(n,\,m)}\rangle = \langle x^{n/k}\rangle,$$

de donde se deduce que $K = \langle x^m\rangle$ es un subgrupo de $H = \langle x^{n/k}\rangle$. Como ambos tienen k elementos ha de cumplirse la igualdad. ■

★★ EJEMPLO D. Los órdenes de todos los elementos de $(\mathbb{Z}_8, +)$ se obtienen usando la proposición 4.6.3 y se dan en la siguiente tabla:

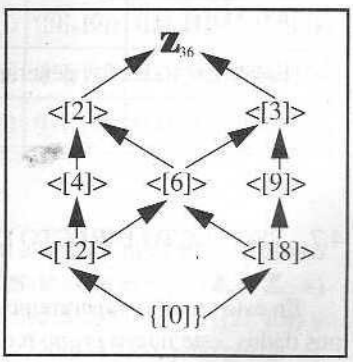
Elementos	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
Orden	1	8	4	8	2	8	4	8

★★ EJEMPLO E. Los subgrupos de $(\mathbb{Z}_{36}, +)$ se corresponden con los divisores de 36, de acuerdo con la proposición 4.6.4. Los divisores de 36 son

36, 18, 12, 9, 6, 4, 3, 2 y 1.

Los subgrupos de este grupo son nueve, incluidos los impropios, y, según los resultados anteriores, el subgrupo de orden k estará generado por [36/k]. Así pues, tenemos los subgrupos

$\langle[1]\rangle = \mathbb{Z}_{36}$, $\langle[2]\rangle$, $\langle[3]\rangle$, $\langle[4]\rangle$, $\langle[6]\rangle$, $\langle[9]\rangle$, $\langle[12]\rangle$, $\langle[18]\rangle$, $\langle[36]\rangle = \langle[0]\rangle$



El retículo de los subgrupos de este grupo se muestra en la ilustración que acompaña a este ejemplo.

EJERCICIOS 4.6

1. Encontrar el retículo de los subgrupos de $(\mathbb{Z}_{50}, +)$ y de $(\mathbb{Z}_{13}, +)$.
2. Dar un ejemplo de un grupo no abeliano en el que todos sus subgrupos propios sean cíclicos.
3. Dar un ejemplo de un grupo abeliano no cíclico en el que todos sus subgrupos propios sean cíclicos.
4. Si G es un grupo cíclico y N un subgrupo normal de G, demostrar que G/N es también un grupo cíclico.
5. Sea H un subgrupo de $\mathbb{Z}_n$; demostrar que existe un entero positivo m que divide a n tal que H es isomorfo a $m\mathbb{Z}/n\mathbb{Z}$. Deducir de este resultado y del ejercicio 4 que todo subgrupo de $(\mathbb{Z}_n, +)$ es cíclico.
6. Sea H un subgrupo de $\mathbb{Z}_n$; demostrar que existe un entero positivo m que divide a n tal que H es isomorfo a $\mathbb{Z}_{n/m}$.
7. Si G es un grupo no abeliano, demostrar que G/Z(G) no es cíclico. Utilizar este resultado para demostrar que si G es un grupo no abeliano de orden pq, con p y q primos distintos, entonces $Z(G) = \{e\}$.
8. ¿Cuáles son los posibles núcleos de un homomorfismo suprayectivo de $\mathbb{Z}_{36}$ en el grupo de Klein?
9. Encontrar el orden de todos los elementos de $(\mathbb{Z}_6, +)$. Demostrar que $(\mathbb{Z}_7^*, \cdot)$ es un grupo cíclico y encontrar el orden de todos sus elementos.
10. Si G es un grupo cíclico y $|G| = n$, probar que G posee tantos generadores como enteros positivos hay menores que n y relativamente primos con n (usar la proposición 4.6.3).
11. Encontrar todos los generadores de $(\mathbb{Z}_{32}, +)$.

4.7. PRODUCTO DIRECTO DE GRUPOS

En esta sección mostraremos un método para obtener un nuevo grupo a partir de dos grupos dados; este nuevo grupo recibe el nombre de **producto directo** de los grupos dados.

Sean G y H dos grupos con operaciones $\circ$ y $*$ respectivamente; en el producto cartesiano $G \times H = \{(g, h): g \in G, h \in H\}$ puede definirse la siguiente operación:

$$(g, h) \circ (g', h') = (g \circ g', h * h').$$

Proposición 4.7.1. Si G y H son grupos, $(G \times H, \circ)$ es un grupo con la operación definida anteriormente. Este grupo recibe el nombre de **producto directo** de G y H.

Demostración. La operación es cerrada por definición. De la asociatividad de las operaciones de G y H se deduce la asociatividad de $\circ$, que se deja como ejercicio para el lector. El elemento neutro es (e_G, e_H), donde e_G, e_H son los elementos neutros de G y H respectivamente. Finalmente, si $(g, h) \in G \times H$, g^{-1} denota el inverso de g en G y h^{-1} denota el inverso de h en H, se tiene que $(g, h)^{-1} = (g^{-1}, h^{-1}) \in G \times H$. ■

★★ EJEMPLO A. $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ es un ejemplo de producto directo de $(\mathbf{R}, +)$ y $(\mathbf{R}, +)$; sus elementos son de la forma (a, b) con $a, b \in \mathbf{R}$ y la operación queda definida mediante $(a, b) + (c, d) = (a + c, b + d)$.

★★ EJEMPLO B. Cuando n y m son enteros positivos siempre podemos considerar el producto directo de $(\mathbf{Z}_n, +)$ y $(\mathbf{Z}_m, +)$, para obtener el grupo $(\mathbf{Z}_n \times \mathbf{Z}_m, +)$, que será abeliano ya que cada uno de los grupos anteriores lo es. La tabla del grupo $(\mathbf{Z}_4 \times \mathbf{Z}_2, +)$ se describe a continuación:

+	([0], [0])	([0], [1])	([1], [0])	([1], [1])	([2], [0])	([2], [1])	([3], [0])	([3], [1])
([0], [0])	([0], [0])	([0], [1])	([1], [0])	([1], [1])	([2], [0])	([2], [1])	([3], [0])	([3], [1])
([0], [1])	([0], [1])	([0], [0])	([1], [1])	([1], [0])	([2], [1])	([2], [0])	([3], [1])	([3], [0])
([1], [0])	([1], [0])	([1], [1])	([2], [0])	([2], [1])	([3], [0])	([3], [1])	([0], [0])	([0], [1])
([1], [1])	([1], [1])	([1], [0])	([2], [1])	([2], [0])	([3], [1])	([3], [0])	([0], [1])	([0], [0])
([2], [0])	([2], [0])	([2], [1])	([3], [0])	([3], [1])	([0], [0])	([0], [1])	([1], [0])	([1], [1])
([2], [1])	([2], [1])	([2], [0])	([3], [1])	([3], [0])	([0], [1])	([0], [0])	([1], [1])	([1], [0])
([3], [0])	([3], [0])	([3], [1])	([0], [0])	([0], [1])	([1], [0])	([1], [1])	([2], [0])	([2], [1])
([3], [1])	([3], [1])	([3], [0])	([0], [1])	([0], [0])	([1], [1])	([1], [0])	([2], [1])	([2], [0])

Tabla del grupo $(\mathbf{Z}_4 \times \mathbf{Z}_2, +)$

Este es un grupo de 8 elementos que no es isomorfo ni a $(\mathbf{Z}_8, +)$, ni al grupo diédrico D_8; esto se deduce comparando los órdenes de los elementos de estos grupos. $(\mathbf{Z}_4 \times \mathbf{Z}_2, +)$ tiene 1 elemento de orden 1 (el ([0], [0])), 3 elementos de orden 2 (([0], [1]), ([2], [0]) y ([2], [1])) y los 4 restantes son todos de orden 4. No es, por tanto cíclico, y no puede ser

isomorfo a $(\mathbf{Z}_8, +)$. D_8 solamente tiene dos elementos de orden 4, A y A^3, con lo que tampoco puede ser isomorfo al grupo descrito en la tabla anterior.

De ahora en adelante, los símbolos $\circ$ y $*$, que se han utilizado en la definición de producto directo, quedarán suprimidos siempre que no sea necesaria su utilización.

En el ejemplo A se observa que $\mathbf{R} \times \{0\} \approx \mathbf{R}$ y que $\{0\} \times \mathbf{R} \approx \mathbf{R}$; esto sucede en cualquier producto directo de grupos. El resultado general se enuncia y demuestra a continuación.

Proposición 4.7.2. Sean G y H grupos.

a) Si G y H son finitos, $|G \times H| = |G|\,|H|$.
b) G es isomorfo a $\underline{G} = \{(g, e_H): g \in G\}$ y $\underline{G}$ es un subgrupo normal de $G \times H$.
c) H es isomorfo a $\underline{H} = \{(e_G, h): h \in H\}$ y $\underline{H}$ es un subgrupo normal de $G \times H$.

Demostración. La parte a) resulta evidente ya que el número de elementos del conjunto producto es el número de elementos de G multiplicado por el número de elementos de H.

Para demostrar b) sea $f : G \to \underline{G}$ dada por $f(g) = (g, e_H)$; f es un isomorfismo, con lo cual se tiene que G es isomorfo a $\underline{G}$; además, si $(g, h) \in G \times H$ y $(g', e_H) \in \underline{G}$, se tiene que

$$(g, h) \circ (g', e_H) \circ (g, h)^{-1} = (g, h) \circ (g', e_H) \circ (g^{-1}, h^{-1}) = (gg'g^{-1}, e_H),$$

con lo cual $\underline{G}$ es un subgrupo normal de $G \times H$. La demostración de c) es análoga a la demostración de b). ∎

De manera análoga a como se definió el producto directo de dos grupos, puede procederse para definir el **producto directo** de un número finito de grupos $G_1, G_2, \ldots, G_n$, el cual se escribirá mediante $G_1 \times G_2 \times \ldots \times G_n$; la operación en el producto directo está definida como sigue:

$$(x_1, x_2, \ldots, x_n) \circ (y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n)\,.$$

★★ EJEMPLO C. Si escribimos el grupo de Klein V como $V = \{e, a, b, c\}$ con $a^2 = b^2 = c^2 = e$, $ab = c$ y observamos que $f : V \to (\mathbf{Z}_2 \times \mathbf{Z}_2, +)$ dado por $f(e) = ([0], [0])$, $f(a) = ([1], [0])$, $f(b) = ([0], [1])$ y, en consecuencia, $f(c) = f(a) + f(b) = ([1], [1])$, es un isomorfismo, se tiene que $V \approx (\mathbf{Z}_2 \times \mathbf{Z}_2, +)$. Es conveniente que el lector escriba las tablas de ambos grupos, dibuje sus retículos y determine el orden de cada uno de sus elementos para convencerse de su similitud.

El ejemplo B sugiere que en algunas ocasiones un grupo puede escribirse como producto directo de otros dos grupos; estas ocasiones serán descritas en la proposición 4.7.3. Observar que escribir un grupo G como producto directo de grupos H_1 y H_2 posee la ventaja de que varios subgrupos de G pueden encontrarse estudiando separadamente los subgrupos de H_1 y de H_2.

Proposición 4.7.3. Sea G un grupo con N y M subgrupos normales de G; si $M \cap N = \{e\}$ y $MN = G$, se tiene que G es isomorfo a $M \times N$.

Demostración. Puesto que $G = MN$, dado $g \in G$ existen $m \in M$ y $n \in N$ de manera que $g = mn$; debido a que $M \cap N = \{e\}$, esta representación es única, puesto que si $mn = m'n'$ se tiene que $(m')^{-1} m = n'n^{-1} \in M \cap N = \{e\}$, y por tanto $m' = m$ y $n' = n$. Entonces, la aplicación $f: G \to M \times N$ dada por $f(g) = (m, n)$, con $g = mn$, está bien definida. La aplicación f es suprayectiva e inyectiva. Falta demostrar que f es un homomorfismo de grupos; para demostrar esto observemos primero que si $n \in N$ y $m \in M$, $nm = mn$: puesto que N es un subgrupo normal de G,

$$n^{-1}m^{-1}nm = n^{-1}(m^{-1}nm) \in NN = N,$$

y puesto que M es un subgrupo normal de G,

$$n^{-1}m^{-1}nm = (n^{-1}m^{-1}n)m \in MM = M;$$

puesto que $N \cap M = \{e\}$, se deduce que $n^{-1}m^{-1}nm = e$, que era lo que queríamos demostrar. Con esta observación puede finalizarse fácilmente la prueba de que f es un isomorfismo y en consecuencia quedará demostrada la proposición: si $g = mn$ y $g' = m'n'$,

$$\begin{aligned} f(gg') &= f((mn)(m'n')) \\ &= f(m(nm')n') && \text{(propiedad asociativa)} \\ &= f(m(m'n)n') && \text{(ya que n y m' conmutan)} \\ &= f((mm')(nn')) && \text{(propiedad asociativa)} \\ &= (mm',nn') && \text{(definición de f)} \\ &= (m,n) \circ (m'n') && \text{(definición de producto directo)} \\ &= f(g) \circ f(g'). \end{aligned}$$

■

★★ EJEMPLO D. Sea $V = \{e, a, b, c\}$ con $a^2 = b^2 = e$ y $ab = c$ el grupo de Klein; $M = \{e, a\}$ es un subgrupo normal de V y $N = \{e, b\}$ también lo es; además $M \cap N = \{e\}$ y $MN = V$, por lo que aplicando el resultado que acabamos de demostrar deducimos que V es isomorfo a $M \times N \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$.

★★ EJEMPLO E. En $(\mathbf{R}^*, \cdot)$ los subgrupos $(\mathbf{R}^+, \cdot)$ y $(\{1,-1\}, \cdot)$ son normales y su intersección es $\{1\}$; como todo número real no nulo es positivo o negativo, se tiene que

$$(\mathbf{R}^*, \cdot) \simeq \mathbf{R}^+ \times \{-1,1\}.$$

★★ EJEMPLO F. En $(\mathbf{Z}_6, +)$ los subgrupos $M = \{[0], [2], [4]\}$ y $N = \{[0], [3]\}$ son normales ya que el grupo es abeliano, su intersección es el elemento neutro y $M + N = \{[0], [2], [4], [3], [5], [1]\} = \mathbf{Z}_6$; por tanto $(\mathbf{Z}_6, +)$ es isomorfo a $(M \times N, +)$ y éste es, a su vez, isomorfo a $(\mathbf{Z}_2 \times \mathbf{Z}_3, +)$.

★★ EJEMPLO G. En la demostración de la proposición 4.7.3 se ha probado que si M y N son subgrupos normales de G y $M \cap N = \{e\}$, los elementos de M conmutan con los elementos de N. Este resultado no es cierto si alguno de los subgrupos no es normal; tomar en D_6 los subgrupos $M = \{I, B\}$ y $N = \{I, A, A^2\}$, el primero de los cuales no es normal, y mostrar que A y B no conmutan.

EJERCICIOS 4.7

1. Demostrar que si A y B son grupos, $A \times B$ es abeliano si y sólo si A y B son abelianos.

2. Demostrar que $D_{12} \approx \mathbf{Z}_2 \times D_6$. ¿Cómo puede generalizarse este resultado para escribir D_{4m}, $m \geq 5$ y m impar, como producto directo?

3. Encontrar el centro de $\mathbf{Z}_2 \times S_3$.

4. i) Encontrar el retículo de los subgrupos de $\mathbf{Z}_4 \times \mathbf{Z}_2$.
   ii) Si $N = \{([0], [0]), ([0], [1])\}$, identificar $\mathbf{Z}_4 \times \mathbf{Z}_2/N$.
   iii) Si f es un epimorfismo de $\mathbf{Z}_4 \times \mathbf{Z}_2$ en $\mathbf{Z}_4$, ¿cuáles son los posibles núcleos de f?

5. Sea $G = \{(a, b): a, b \in \mathbf{Z}\}$ y $*$ la operación dada en G por $(a, b) * (c, d) = (a + c(-1)^b, b + d)$; demostrar que $(G, *)$ es un grupo. ¿Es G abeliano? ¿Es G isomorfo a $\mathbf{Z} \times \mathbf{Z}$?

6. Si A y B son grupos, demostrar que $A \times B$ es isomorfo a $B \times A$.

7. Sea G un grupo y considerar el producto directo $M = G \times G$.

   (a) Demostrar que $D = \{(g, g) \in G \times G: g \in G\}$ es un grupo isomorfo a G.
   (b) Demostrar que D es normal en M si y sólo si G es abeliano.

8. Sean $M = \langle x \rangle$ y $N = \langle y \rangle$ grupos cíclicos de órdenes m y n respectivamente, con m y n primos entre sí; demostrar que $M \times N$ es un grupo cíclico y encontrar un generador.

9. Sean M y N grupos cíclicos de órdenes m y n respectivamente; demostrar que $M \times N$ es cíclico si y sólo si m y n son primos entre sí.

10. Utilizar el problema 8 para demostrar el **teorema chino del resto,** a saber, si m y n son enteros primos entre sí y u,v son dos enteros cualesquiera, el sistema de ecuaciones $x \equiv u \pmod{m}$ y $x \equiv v \pmod{n}$ tiene al menos una solución entera.

11. Decir cuáles de los siguientes grupos puede escribirse como suma directa de subgrupos propios: $(\mathbf{Z}_{12}, +)$, $(\mathbf{Z}_5, +)$, $(\mathbf{Z}_4, +)$.

12. Sea A subgrupo normal de G y B subgrupo normal de H. Demostrar que $A \times B$ es un subgrupo normal de $G \times H$ y que $(G \times H)/(A \times B)$ es isomorfo a $(G/A) \times (H/B)$.

4.8. GRUPOS DE PERMUTACIONES

En la sección 3.4 del capítulo 3 se comenzaron a estudiar los grupos de permutaciones; en esta sección ampliaremos su estudio por la importancia que tienen en la teoría de resolución de ecuaciones algebraicas y por los importantes ejemplos de grupos que originan.

Recordemos que el grupo de las permutaciones de n elementos, o grupo simétrico de n elementos, es el conjunto de todas las aplicaciones biyectivas del conjunto $\{1, 2, \ldots, n\}$ en sí mismo. Una permutación α queda determinada, por tanto, por la imagen de cada uno de los elementos 1, 2, ..., n y para designarla utilizamos la notación

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}$$

Esta notación es redundante puesto que la primera fila se repite siempre. Por esta razón, introduciremos una nueva notación, que recibe el nombre de notación **cíclica.** Expondremos esta nueva notación con un ejemplo. Sea

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 5 & 1 & 8 & 6 & 3 \end{pmatrix}$$

un elemento de S_8. Calculamos las imágenes sucesivas de 1 mediante α; escribiendo α^0 = Identidad, tenemos:

$$\alpha^0(1) = 1; \quad \alpha^1(1) = 4; \quad \alpha^2(1) = \alpha(4) = 5; \quad \alpha^3(1) = \alpha(5) = 1$$

y

$$\alpha^j(1) = \alpha^{j-3}(1) \quad \text{para todo } j \geq 4 .$$

A los elementos que son imágenes sucesivas del 1 mediante α los escribimos de la forma $\sigma_1 = (1\ 4\ 5)$.

Si $\{\sigma_1\}$ es el conjunto de los elementos de σ_1, es decir $\{\sigma_1\} = \{1, 4, 5\}$, tomamos el menor elemento de $\{1, 2, \ldots, n\}$ que no esté en $\{\sigma_1\}$ y calculamos sus imágenes mediante α; en este caso se tiene

$$\alpha(2) = 2,$$

con lo cual escribiremos $\sigma_2 = (2)$. Este proceso se continúa hasta que los elementos de $\{1, 2, \ldots, n\}$ se han agotado, en nuestro caso

$$\alpha(3) = 7, \quad \alpha^2(3) = 6, \quad \alpha^3(3) = 8, \quad \alpha^4(3) = 3 ,$$

con lo cual se tiene $\sigma_3 = (3\ 7\ 6\ 8)$ y se agotan los ocho primeros números naturales. Este proceso nos permite escribir $\alpha = \sigma_3 \circ \sigma_2 \circ \sigma_1$; cada uno de los σ_j se denomina un **ciclo** y α se dice que está escrita en notación **cíclica.** Puesto que el ciclo $\sigma_2 = (2)$ no cambia nada, se conviene en suprimirlo en la notación, con lo cual se tiene $\alpha = \sigma_3 \circ \sigma_1$.

★★ EJEMPLO A. La permutación $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 6 & 5 \end{pmatrix} \in S_6$ se escribe en notación cíclica de la forma $\alpha = (5\ 6)\ (1\ 3\ 4\ 2)$.

★★ EJEMPLO B. Si $\sigma_1 = (1\ 3\ 5)$ y $\sigma_2 = (3\ 5\ 6)$ son dos ciclos en S_6, se tiene que

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 1 & 3 \end{pmatrix} = (3\ 6)(1\ 5),$$

mientras que

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 6 & 5 \end{pmatrix} = (5\ 6)(1\ 3),$$

con lo que queda probado que, en general, dos ciclos no conmutan; pero si los ciclos tienen la particularidad de que son "disjuntos" (véase la definición 4.8.1), puede invertirse el orden de su composición sin alterar el resultado (proposición 4.8.2).

Obsérvese que los ciclos (1 4 5) y (4 5 1) son el mismo a pesar de que comienzan con elementos distintos.

Definición 4.8.1. Dos ciclos $\sigma = (a_1 \dots a_n)$ y $\gamma = (b_1 \dots b_m)$ se dicen **disjuntos** si $\{a_1, \dots, a_n\} \cap \{b_1, \dots, b_m\} = \emptyset$.

Proposición 4.8.2. Si σ y γ son dos ciclos disjuntos de S_n, $\gamma \circ \sigma = \sigma \circ \gamma$.

Demostración. Sean $\sigma = (a_1 \dots a_n)$ y $\gamma = (b_1 \dots b_m)$. Si $1 \le j < n$, $\gamma \circ \sigma(a_j) = \gamma(a_{j+1}) = a_{j+1}$ y $\sigma \circ \gamma(a_j) = \sigma(a_j) = a_{j+1}$ puesto que $a_j, a_{j+1} \notin \{b_1, \dots, b_m\}$; de manera similar $\gamma \circ \sigma(a_n) = \gamma(a_1) = a_1$ y $\sigma \circ \gamma(a_n) = \sigma(a_n) = a_1$. El mismo resultado se obtiene para los b_j. Finalmente, si $x \notin \{a_1, \dots, a_n\} \cup \{b_1, \dots, b_m\}$, x queda fijo mediante σ y γ, con lo cual queda probada la proposición. ■

El proceso seguido para descomponer una permutación en ciclos sugiere que toda permutación puede descomponerse en ciclos disjuntos; éste es el contenido del siguiente teorema:

Teorema 4.8.3. Toda permutación α de S_n puede descomponerse en **ciclos disjuntos de manera única,** salvo el orden de los ciclos y su primer elemento.

Demostración. Demostraremos primero que α puede descomponerse en un producto de ciclos. Si formamos

$$1, \alpha(1), \alpha^2(1), \dots, \alpha^n(1),$$

como hay $n + 1$ elementos y sólo n posibles imágenes, se tendrá alguna repetición; si, por ejemplo, $\alpha^j(1) = \alpha^k(1)$ con $0 \le j < k \le n$, se tiene que $\alpha^{k-j}(1) = 1$ con $0 < k - j \le n$. Elegir m_1 como el menor entero positivo tal que $\alpha^{m_1}(1) = 1$ y sea

$$\sigma_1 = (1\ \alpha(1) \dots \alpha^{m_1 - 1}(1)).$$

Sea a un elemento de $\{1, \ldots, n\}$ que no esté en $\{1, \alpha(1), \ldots, \alpha^{m_1-1}(1)\}$ y repetir el proceso para obtener un entero positivo m_2 tal que $\alpha^{m_2}(a) = a$ y m_2 sea el menor entero positivo que satisfaga esta igualdad. Escribir

$$\sigma_2 = (a, \alpha(a), \ldots, \alpha^{m_2-1}(a)) .$$

Este proceso se realiza cuantas veces sea necesario hasta agotar los n elementos de $\{1, \ldots, n\}$; se obtiene de esta manera una cantidad finita, digamos k, de ciclos $\sigma_1, \sigma_2, \ldots, \sigma_k$ tal que $\alpha = \sigma_k \circ \ldots \circ \sigma_2 \circ \sigma_1 = \sigma_k \ldots \sigma_2 \sigma_1$.

A continuación demostraremos que dos ciclos cualesquiera obtenidos de esta manera son disjuntos; para fijar los ciclos utilizamos σ_1 y σ_2. Si $\alpha^j(1) = \alpha^s(a)$ se tiene que $\alpha^{j-s}(1) = a$, y por tanto $a \in \{1, \alpha(1), \ldots, \alpha^{m_1-1}(1)\}$ en contra de la elección realizada. Como dos ciclos cualesquiera en los que se descompone α son disjuntos, estos conmutan debido a la proposición 4.8.2, con lo cual el orden de los ciclos no influye en la descomposición de α.

Finalmente, demostraremos que la elección del primer elemento no afecta a la descomposición en ciclos; en efecto, si $b = \alpha^j(a)$ con $0 < j < m_2$, basta probar que $\sigma_2 = (a\ \alpha(a) \ldots \alpha^{m_2-1}(a))$ coincide con $\tilde{\sigma}_2 = (b\ \alpha(b) \ldots \alpha^{m_2-1}(b))$:

$$\tilde{\sigma}_2(b) = \alpha(b) = \alpha^{j+1}(a) = \sigma_2(\alpha^j(a)) = \sigma_2(b)$$

y en general para todo s, $1 \leq s \leq m_2 - 1$,

$$\tilde{\sigma}_2(\alpha^s(b)) = \alpha^{s+1}(b) = \alpha^{s+1+j}(a) = \sigma_2(\alpha^{s+j}(a)) = \sigma_2(\alpha^s(b)).$$ ■

Definición 4.8.4. Si σ es un ciclo, se denomina **longitud** de σ, y se escribe $\ell(\sigma)$, al número de elementos que aparecen en σ. Un ciclo de longitud 2 se denomina una **trasposición.**

La longitud de un ciclo está ligada al orden de la permutación σ, considerada como un elemento de S_n; recuérdese que el orden del elemento σ en S_n se definió como el número de elementos que posee el subgrupo generado por σ y que coincidía con el menor entero positivo m tal que σ^m = Identidad. Supongamos que el ciclo σ tiene longitud r y orden m; entonces $\sigma = (a\ \sigma(a)\ \sigma^2(a) \ldots \sigma^{r-1}(a))$ y para todo j con $0 \leq j \leq r - 1$,

$$\sigma^r(\sigma^j(a)) = \sigma^{r+j}(a) = \sigma^j\,\sigma^r(a) = \sigma^j(a),$$

con lo cual σ^r = Identidad; como m es el menor entero que satisface esta igualdad se tiene que $m \leq r$. Por otro lado $m \geq r$ puesto que $\sigma^j(a) \neq a$ para todo $j < r$, con lo cual se tiene la igualdad. En resumen, **el orden de un ciclo coincide con su longitud.**

Una vez obtenida una respuesta sencilla al problema de calcular el orden de un ciclo, cabe preguntarse si podrá encontrarse un método sencillo para calcular el orden de una permutación cualquiera α de S_n. Puesto que por el teorema 4.8.3, α puede descomponerse en un producto de ciclos disjuntos es razonable pensar que la respuesta a esta pregunta viene dada en

función del orden de los ciclos en los que se descompone. La respuesta queda plasmada en la siguiente proposición:

Proposición 4.8.5. Sea α una permutación de S_n y $\alpha = \sigma_r \dots \sigma_2 \sigma_1$ una descomposición de α en ciclos disjuntos. El orden de α coincide con el mínimo común múltiplo de los órdenes de cada σ_i.

Demostración. Sea m el orden de α y $s = m.c.m\{m_1, \dots, m_r\}$, donde cada m_j es el orden de σ_j; debido a que los ciclos σ_i son disjuntos, conmutan, y por tanto $\alpha^s = (\sigma_r)^s \dots (\sigma_2)^s(\sigma_1)^s$; para cada j, $1 \le j \le r$, podemos escribir $s = p_j m_j$ con p_j entero positivo y entonces obtenemos

$$\sigma^s = (\sigma_r)^{p_r m_r} \dots (\sigma_2)^{p_2 m_2}(\sigma_1)^{p_1 m_1} = ((\sigma_r)^{m_r})^{p_r} \dots ((\sigma_2)^{m_2})^{p_2}((\sigma_1)^{m_1})^{p_1},$$

que es la permutación identidad . Tenemos, por tanto, $m \le s$. Si demostramos que $\alpha^j \ne$ Identidad para todo $j = 1, \dots, s-1$, quedará probado que $m = s$. Para demostrar esto observar que si $j < s$, existe $k \in \{1, 2, \dots, r\}$ tal que j no es múltiplo de m_k; si $\sigma_k = (a\ \sigma_k(a) \dots \sigma_k^{m_k - 1}(a))$ se tiene que $\alpha^j(a) = (\sigma_k)^j(a) \ne a$. ■

★★ EJEMPLO C. a) La permutación $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 6 & 5 \end{pmatrix}$ del ejemplo A tiene orden 4 puesto que $\alpha = (5\ 6)(1\ 3\ 4\ 2)$.

b) Para calcular el orden de $\beta = (3\ 4\ 5)\ (1\ 5\ 2\ 4)$ es necesario realizar su descomposición en ciclos disjuntos; ésta es $\beta = (1\ 3\ 4)\ (2\ 5)$ y por tanto su orden es 6.

La descomposición de un objeto en partes elementales permite deducir propiedades del objeto a partir de propiedades de sus partes; así ha ocurrido al estudiar el orden de una permutación mediante su descomposición en ciclos disjuntos. Sin embargo, los ciclos más sencillos son las trasposiciones, por lo que cabría preguntarse si toda permutación puede descomponerse en trasposiciones y poder deducir propiedades de aquélla a partir de las propiedades de éstas. Puesto que toda permutación puede descomponerse en ciclos disjuntos, es suficiente demostrar que todo ciclo puede descomponerse en trasposiciones. El ejemplo $(1\ 3\ 4\ 6) = (16)\ (14)\ (13)$ marca la pauta para la demostración de la siguiente proposición.

Proposición 4.8.6. Todo ciclo puede descomponerse en un producto de trasposiciones.

Demostración. Sea $\sigma = (a\ \sigma(a) \dots \sigma^k(a))$ un ciclo y escribir $\tau = (a\ \sigma^k(a)) \dots (a\ \sigma^2(a))(a\ \sigma(a))$. Tenemos que

$$\tau(a) = \sigma(a), \qquad \tau^2(a) = \tau(\tau(a)) = \tau(\sigma(a)) = \sigma^2(a),$$

y en general $\tau^j(a) = \sigma^j(a)$, $1 \le j \le k$, con lo que $\sigma = \tau$. Observar que τ es un producto de trasposiciones. ■

El teorema 4.8.3 y la proposición 4.8.6 tienen como consecuencia inmediata el resultado que se enuncia a continuación.

Corolario 4.8.7. Toda permutación de S_n puede escribirse como una composición de trasposiciones o, equivalentemente, las trasposiciones generan S_n.

★★ EJEMPLO D. La permutación del ejemplo C puede descomponerse en trasposiciones de la forma $\alpha = (5\ 6)\ (1\ 3\ 4\ 2) = (5\ 6)\ (1\ 2)\ (1\ 4)\ (1\ 3)$. La permutación β del mismo ejemplo puede descomponerse en trasposiciones de la forma $= (1\ 4)\ (1\ 3)\ (2\ 5)$.

La forma de escribir una permutación como un producto de trasposiciones no es única; por ejemplo,

$$(2\ 3)\ (1\ 3)\ (1\ 2)\ (1\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (1\ 4\ 3) = (1\ 3)\ (1\ 4).$$

Demostraremos a continuación que si una permutación α puede descomponerse en un número par (impar) de trasposiciones, cualquier otra descomposición de α en trasposiciones debe de poseer un número par (impar) de éstas. Se tiene así que el número de trasposiciones en que una permutación puede descomponerse determina dos clases disjuntas de permutaciones.

El número de trasposiciones en las que un ciclo σ se ha descompuesto de acuerdo con el procedimiento seguido en la proposición 4.8.6 se escribe $N(\sigma)$; por tanto, si σ tiene longitud r, $N(\sigma) = r - 1$. Si α es una permutación de S_n y $\alpha = \sigma_k \dots \sigma_2\sigma_1$ es una descomposición de α en ciclos disjuntos obtenida mediante el procedimiento seguido en el teorema 4.8.3 definimos

$$N(\alpha) = \sum_{j=1}^{k} N(\sigma_j).$$

Convenimos en escribir $N(Id) = 0$. Observar que $N(\alpha)$ mide el número de trasposiciones en las que se ha descompuesto α siguiendo el procedimiento del teorema 4.8.3 y de la proposición 4.8.6. Nuestro próximo objetivo es demostrar que cualquier otro procedimiento de descomposición de α produce un número m de trasposiciones que posee la misma paridad que $N(\alpha)$, es decir, m es par o impar de acuerdo con que $N(\alpha)$ sea par o impar.

Lema 4.8.8. Si σ es un ciclo de S_n y (a b) es una transposición de S_n, $N((a\ b)\sigma) = N(\sigma) \pm 1$.

Demostración. Sea $\sigma = (c_1\ c_2 \dots c_r)$ de manera que $N(\sigma) = r - 1$; varios casos han de ser tratados de manera diferente dependiendo de la intersección de $\{a, b\}$ con $\{c_1, c_2, \dots, c_r\}$. Supongamos primero que $\{a, b\} \subset \{c_1, c_2, \dots, c_r\}$; entonces

$$(a\ b)\sigma = (a\ b)(c_1 \dots c_{s-1}\ a\ c_{s+1} \dots c_{j-1}\ b\ c_{j+1} \dots c_r) =$$
$$= (c_1 \dots c_{s-1}\ b\ c_{j+1} \dots c_r)\ (a\ c_{s+1} \dots c_{j-1}) = \sigma_1\sigma_2,$$

de donde se deduce que $N((a\ b)\sigma) = N(\sigma_1) + N(\sigma_2)$, puesto que σ_1 y σ_2 son disjuntos. Puesto que $N(\sigma_1) = [s - 1 + 1 + r - j] - 1$ y $N(\sigma_2) = [1 + j - s - 1] - 1$ se tiene que

$$N((a\ b)\sigma) = s + r - j - 1 + j - s - 1 = (r - 1) - 1 = N(\sigma) - 1.$$

En el caso en que $a \in \{c_1, \ldots, c_r\}$ y $b \notin \{c_1, \ldots, c_r\}$ se tiene

$$(a\ b)\sigma = (a\ b)(c_1 \ldots c_{s-1}\ a\ c_{s+1} \ldots c_r) = (c_1 \ldots c_{s-1}\ b\ a\ c_{s+1} \ldots c_r) = \mu\ ,$$

de donde se deduce que $N((a\ b)\sigma) = N(\mu) = [s - 1 + 2 + r - s] - 1 = r = (r - 1) + 1 = N(\sigma) + 1$.

El caso en que $b \in \{c_1, \ldots, c_r\}$ y $a \notin \{c_1, \ldots, c_r\}$ es similar al anterior. Finalmente, si ambos conjuntos son disjuntos, se tiene que $N((ab)\sigma) = N((a\ b)) + N(\sigma) = 1 + N(\sigma)$. ■

Un resultado similar al que se acaba de demostrar para ciclos es cierto para permutaciones.

Proposición 4.8.9. Si α es una permutación de S_n y $(a\ b)$ es una trasposición de S_n, $N((a\ b)\alpha) = N(\alpha) \pm 1$.

Demostración. Al igual que en el lema anterior, es necesario distinguir varios casos. Supongamos primero que $\{a, b\} \subset \{\sigma_j\}$ para algún j, donde $\alpha = \sigma_k \ldots \sigma_1$ es la descomposición de α en ciclos disjuntos según el teorema 4.8.3 y $\{\sigma_j\}$ representa el conjunto de los elementos de σ_j. Del primer caso estudiado en el lema 4.8.8 se deduce

$$\begin{aligned} N((a\ b)\alpha) &= N(\sigma_1) + \ldots + N((a\ b)\sigma_j) + \ldots + N(\sigma_k) = \\ &= N(\sigma_1) + \ldots + N(\sigma_j) - 1 + \ldots + N(\sigma_k) = N(\alpha) - 1. \end{aligned}$$

Del resto de los casos sólo merece especial atención aquél en que $a \in \{\sigma_j\}$ y $b \in \{\sigma_i\}$, con $i \neq j$ (¡comprobar esta afirmación!). Supongamos, para trabajar en un caso concreto, que $j > i$ y escribamos $\sigma_j = (c_1 \ldots c_{s-1}\ a\ c_{s+1} \ldots c_{n_j})$, $\sigma_i = (d_1 \ldots d_{k-1}\ b\ d_{k+1} \ldots d_{m_i})$. Como los ciclos disjuntos conmutan, deducimos

$$N((a\ b)\alpha) = \sum_{\substack{r \neq i \\ r \neq j}} N(\sigma_r) + N((a\ b)\ \sigma_j\sigma_i)\ . \qquad (*)$$

Además

$$\begin{aligned} (a\ b)\sigma_j\sigma_i &= (a\ b)\ (c_1 \ldots c_{s-1}\ a\ c_{s+1} \ldots c_{n_j}) \circ (d_1 \ldots d_{k-1}\ b\ d_{k+1} \ldots d_{m_i}) = \\ &= (a\ c_{s+1} \ldots c_{n_j}\ c_1 \ldots c_{s-1}\ b\ d_{k+1} \ldots d_{m_i}\ d_1 \ldots d_{k-1})\ , \end{aligned}$$

de donde se deduce

$$\begin{aligned} N((a\ b)\sigma_j\sigma_i) &= [1 + n_j - s + s - 1 + 1 + m_i - k + k - 1] - 1 = n_j + m_i - 1 = \\ &= (n_j - 1) + (m_i - 1) + 1 = N(\sigma_j) + N(\sigma_i) + 1\ . \end{aligned}$$

Sustituyendo este resultado en la igualdad (*) queda demostrada la proposición. ■

Teorema 4.8.10. Sean $\alpha = \sigma_s \dots \sigma_1$ y $\alpha = \tau_m \dots \tau_1$ dos descomposiciones de α en producto de trasposiciones; entonces m y s son ambos pares o impares (es decir, $(-1)^m = (-1)^s$). En particular, $(-1)^{N(\alpha)} = (-1)^s$.

Demostración. Como la inversa de una trasposición es la misma trasposición, de la cadena de igualdades

$$\text{Identidad} = \alpha \circ \alpha^{-1} = (\sigma_s \dots \sigma_1)(\tau_m \dots \tau_1)^{-1} = (\sigma_s \dots \sigma_1)(\tau_1^{-1} \dots \tau_m^{-1}) = (\sigma_s \dots \sigma_1)(\tau_1 \dots \tau_m)$$

se deduce que $0 = N(\tau_1 \dots \tau_m) \pm 1 \pm \dots \pm 1$, donde el número de ± 1 es s. Sea k el número de $+1$ y t el de -1 de manera que $k + t = s$; entonces, $0 = m + k - t$ y por tanto $m = t - k$; así pues,

$$(-1)^m = (-1)^t (-1)^{-k} = (-1)^{s-k}(-1)^{+k} = (-1)^s . \qquad \blacksquare$$

Dada una permutación α de S_n, el teorema anterior nos permite definir la **signatura** de α, que simbolizaremos mediante **sig**(α), como

$$\text{sig}(\alpha) = (-1)^m ,$$

donde m es el número de trasposiciones en que se ha descompuesto la permutación α. De acuerdo con el teorema anterior el número sig(α) no varía con la descomposición de α en trasposiciones y en particular se tiene que

$$\text{sig}(\alpha) = (-1)^{N(\alpha)} .$$

Los elementos de S_n que pueden descomponerse en un número par de trasposiciones reciben el nombre de **permutaciones pares;** aquellos que se descomponen en un numero impar de trasposiciones se llaman **permutaciones impares.**

Si definimos $f : S_n \to \{-1, 1\}$ mediante $f(\alpha) = (-1)^{N(\alpha)}$, f es un homomorfismo de grupos cuando $\{-1, 1\}$ se considera con la operación de multiplicación. En efecto, si $\alpha, \beta \in S_n$ se tiene que

$$\begin{aligned} f(\beta\alpha) &= (-1)^{N(\beta\alpha)} \\ &= \text{sig}(\beta\alpha) \\ &= (-1)^{\#\text{ trasp. }(\beta\alpha)} \\ &= (-1)^{\#\text{ trasp. }\alpha}(-1)^{\#\text{ trasp. }\beta} \qquad \text{(por el teorema 4.8.10)} \\ &= f(\beta)f(\alpha). \end{aligned}$$

Obsérvese, además, que f es suprayectiva si $n \geq 2$ (¿por qué?). Por el primer teorema de isomorfía $S_n / N(f) \approx (\{-1, 1\}, \cdot)$. N(f) es un subgrupo normal de S_n (proposición 4.4.3) que está formado por todas aquellas permutaciones α tales que sig(α) = 1, es decir las permutaciones pares; este subgrupo normal de S_n se denomina **subgrupo alternado de n elementos** y se simboliza **Alt(n)**. Puesto que $S_n / \text{Alt}(n) \approx \{-1, 1\}$ se tiene que $|\text{Alt}(n)| = n!/2$. Este subgrupo está generado por todos los ciclos de longitud 3 de S_n (véase ejercicio 7 al final de esta sección).

★★ EJEMPLO E. Queremos encontrar el orden y la signatura de $\alpha = (1\ 3\ 5\ 6)\ (2\ 3\ 4\ 6)\ (2\ 1)$. Puesto que

$$\alpha = (1\ 6)\ (1\ 5)\ (1\ 3)\ (2\ 6)\ (2\ 4)\ (2\ 3)\ (2\ 1)$$

se tiene que $\text{sig}(\alpha) = (-1)^7 = -1$. Para calcular el orden es necesario descomponer α en ciclos disjuntos: $\alpha = (1\ 5\ 6\ 2\ 3\ 4)$. Entonces, orden $(\alpha) = 6$.

Como ya se ha comentado al comienzo de esta sección, el estudio de las permutaciones tiene especial importancia por su aplicación a la teoría de la resolución de ecuaciones algebraicas. Dada una ecuación algebraica de segundo grado de la forma $ax^2 + bx + c = 0$, es bien conocido que sus soluciones pueden encontrarse mediante una expresión que involucra los coeficientes a, b y c y operaciones tales como suma, resta, multiplicación, división, potenciación y extracción de raíces, a saber

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Las operaciones arriba mencionadas se dice que son operaciones con radicales. Durante la Edad Media se trató de encontrar fórmulas semejantes a la anterior que sirvieran para resolver ecuaciones algebraicas de grado 3 y superior. El primer resultado positivo para las ecuaciones de grado 3 se atribuye a **N. Fontana** (más conocido como **Tartaglia**) y a **G. Cardano**, que utilizaron la fórmula

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

para calcular las soluciones de la ecuación $x^3 + px + q = 0$. Puesto que la ecuación $y^3 + by^2 + cy + d = 0$ puede reducirse a una ecuación del tipo $x^3 + px + q = 0$ mediante el cambio de variable $y = x - b/3$, la ecuación general de tercer grado queda resuelta. Diez años después, **Ludovico Ferrari** publicó una fórmula para resolver las ecuaciones algebraicas de grado 4. (El lector interesado en estas fórmulas puede consultar el libro de A.D. Aleksandrov, A. N. Kolmogorov y M. A. Laurentiev, Matemáticas: su contenido, métodos y significado, Alianza Editorial, Vol. 1.)

Durante varios siglos los matemáticos trataron infructuosamente de encontrar una fórmula con radicales que sirviera para resolver ecuaciones de grado 5. Como consecuencia de esta búsqueda infructuosa el matemático **Paolo Ruffini** anunció, a comienzos del siglo XIX, la imposibilidad de encontrar una fórmula para resolver estas ecuaciones; su artículo, publicado en 1813, contenía afirmaciones imprecisas. La primera demostración de que las ecuaciones de quinto grado no podían resolverse mediante radicales es atribuida al matemático noruego **N. H. Abel,** quien en 1823 publicó una demostración de este hecho que contenía afirmaciones precisas pero con demostraciones vagas.

La teoría dentro de la cual podía demostrarse la imposibilidad de resolver ecuaciones de quinto grado o superior fue desarrollada por el matemático francés **Evariste Galois** (1811-

1832). La idea de Evariste Galois se expone a continuación. Dada una ecuación algebraica de grado n de la forma

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0\,,$$

con soluciones $r_1, r_2, \ldots, r_n$, se le puede asociar un subgrupo del grupo de las permutaciones de los elementos $r_1, r_2, \ldots, r_n$; en particular, toda ecuación algebraica $f(x) = 0$ lleva asociada un subgrupo del grupo S_n; el estudio de la resolución mediante radicales de $f(x) = 0$ puede llevarse a cabo estudianto ciertas propiedades de los grupos de permutaciones S_n. (Una exposición clara de la teoría de E. Galois puede encontrarse en los libros de I. Stewart, Galois Theory, Chapman & Hall (1973) y de C. H. Hadlock, Field Theory and its Classical Problems, The Carus Math. Monographs, 19, MAA (1978).)

Durante el siglo XIX se consideró que el estudio de los grupos de permutaciónes era también importante porque permitiría conocer la estructura de **todos** los grupos finitos. Esto se debía al hecho, demostrado por el matemático inglés **Arthur Cayley** (1821-1895), de que todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones. La posible importancia de este resultado queda mermada por la dificultad que presenta el estudiar los subgrupos de los grupos de permutaciones S_n para $n \geq 5$. A pesar de esto, expondremos a continuación el resultado de Arthur Cayley:

Teorema de Cayley. Todo grupo G es isomorfo a un subgrupo del grupo de las biyecciones de G. En particular, si G es finito, G es isomorfo a un subgrupo de un grupo de permutaciones.

Demostración. Sea B(G) el conjunto de todas las biyecciones de G; definimos $F: G \to (B(G), \circ)$ mediante $F(g)(x) = gx$ para todo $x \in G$. Demostramos primero que si $g \in G$, $F(g) \in B(G)$: si $F(g)(x) = F(g)(y)$ se tiene que $gx = gy$, y de la propiedad cancelativa se deduce que $x = y$, con lo que F(g) es inyectiva; además, si $y \in G$, $F(g)(g^{-1}y) = g(g^{-1}y) = y$, con lo que F(g) es también suprayectiva.

F es un homomorfismo de G en $(B(G), \circ)$ puesto que si $g_1, g_2 \in G$, para todo $x \in G$ se tiene que

$$F(g_1g_2)(x) = (g_1g_2)x = g_1(g_2x) = F(g_1) \circ F(g_2)(x)\,.$$

Puesto que $N(F) = \{g : F(g) = \text{Identidad}\} = \{g : gx = x, \text{ para todo } x \in G\} = \{e\}$, G es isomorfo a F(G); puesto que F(G) es un subgrupo de $(B(G), \circ)$ (proposición 4.4.4), el teorema queda probado. ■

EJERCICIOS 4.8

1. Descomponer en ciclos la permutación

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}$$

de S_{10}, calcular su orden, su signatura y encontrar α^{100}.

2. Calcular el orden y la signatura de cada una de las permutaciones siguientes:

   $\alpha = (4\ 5\ 6)\ (5\ 6\ 7)\ (6\ 7\ 1)\ (1\ 2\ 3)\ (2\ 3\ 4)\ (3\ 4\ 5)$
   $\beta = (4\ 5)\ (4\ 3\ 1)$
   $\gamma = (3\ 4\ 5)\ (2\ 3\ 4)\ (1\ 2\ 3)\ (6\ 7\ 1)\ (5\ 6\ 7)\ (4\ 5\ 6)$.

3. Sean

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 12 & 8 & 11 & 6 & 7 & 5 & 3 & 2 & 4 & 10 & 1 \end{pmatrix} \text{ y}$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 3 & 4 & 6 & 8 & 5 & 10 & 12 & 11 & 9 & 7 & 2 \end{pmatrix}$$

   dos permutaciones de S_{12}.

   a) Calcular $\beta^4\gamma^8$.
   b) Encontrar el orden y la signatura de $\beta^4\gamma^8$.

4. Calcular el orden y la signatura de la permutación σ de S_9 dada por $\sigma = (5\ 7\ 3\ 9)\ (4\ 2)\ (3\ 8\ 5)\ (1\ 6\ 4)$. Calcular σ^{26} y σ^{-1}.

5. Demostrar que las trasposiciones de la forma $(k, k + 1)$ generan todas las trasposiciones.

6. Utilizar el problema 5 para demostrar que si G es un subgrupo de S_n que contienen el ciclo $(1\ 2\ \ldots\ n)$ y la trasposición $(1\ 2)$, se tiene que $G = S_n$.

7. Demostrar que Alt(n) está generado por todos los ciclos de S_n de longitud 3 (usar el problema 5).

8. Encontrar la descomposición en ciclos disjuntos de todas las potencias del ciclo $(1\ 2\ 3\ 4\ 5\ 6)$.

9. i) Dadas las permutaciones $\alpha = (1\ 2)\ (3\ 4)$ y $\beta = (5\ 6)\ (1\ 3)$, encontrar una permutación γ tal que $\gamma^{-1}\alpha\,\gamma = \beta$.
   ii) Demostrar que no existe ninguna permutación α tal que $\alpha^{-1}(1\ 2\ 3)\ \alpha = (1\ 3)\ (5\ 7\ 8)$.

10. Demostrar que S_n no es abeliano si $n \geq 3$.

11. Demostrar que, si $n \geq 3$, el centro de S_n es únicamente la permutación identidad, es decir, si σ es una permutación de S_n y satisface $\sigma \circ \alpha = \alpha \circ \sigma$ para toda permutación α de S_n, se ha de tener $\sigma = I$, la permutación identidad.

12. Comprobar que en S_n, $n \geq 3$, se cumple $(i\ j\ k) = (1\ i\ j)\ (1\ j\ k)$ y $(1\ i\ j) = (1\ 2\ j)\ (1\ 2\ i)\ (1\ 2\ i)$. Usar estos resultados para demostrar que todo elemento del grupo alternado Alt (n) es producto de ciclos de longitud 3 de la forma $(1\ 2\ i)$, $3 \leq i \leq n$.

4.9. COMENTARIOS HISTÓRICOS

Las ideas que contiene la definición de grupo estaban presentes en algunos trabajos de matemáticos realizados durante la segunda mitad del siglo XVIII y todo el siglo XIX. Todas ellas se referían a casos particulares de grupos, principalmente grupos de permutaciones.

El estudio de la resolución de ecuaciones algebraicas fue el que aglutinó más trabajos y desde donde más tarde germinarían las ideas que servirían para definir el concepto abstracto de grupo. El matemático que más contribuyó durante el siglo XVIII a este tema fue **Joseph Louis Lagrange** (1736-1813). Fue un matemático francés nacido en Italia que a los 19 años ya era Profesor en la Escuela Real de Artilleria de Turín y acabó trabajando en los grandes centros matemáticos de su época. En 1776 aceptó la invitación de Federico el Grande de Prusia para ocupar la vacante que había dejado **Leonhard Euler** (1707-1783) en la Academia de Ciencias de Berlín y en 1797 fue nombrado Profesor de Matemáticas de la Escuela Politécnica de París. En un artículo publicado en 1771 en la revista de la Academia de Ciencias de Berlín trató de sistematizar los resultados conocidos sobre la resolución de las ecuaciones de grados 2, 3 y 4. En el proceso, encontró que las fórmulas para resolver las ecuaciones de estos grados estaban relacionadas con la cantidad de valores distintos que pueden tomar ciertas expresiones de las raíces de la ecuación. Por ejemplo, en la ecuación de grado 4 con raíces x_1, x_2, x_3 y x_4, la función $y = f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$ sólo toma tres valores distintos cuando se permutan las raíces de las 4!=24 maneras posibles. Esto, encontró Lagrange, estaba ligado con el hecho de que la resolución de la ecuación de cuarto grado pudiera reducirse a encontrar las raíces de una de grado 3.

La exposición anterior tiene relación con los grupos tal como los entendemos actualmente. En el ejemplo anterior, el conjunto de las permutaciones que producen el mismo valor de f constituyen un subgrupo del grupo de todas las permutaciones. Precisamente, hay tantos subgrupos distintos de este tipo como valores distintos toma f: en nuestro ejemplo 3. Lagrange denominó a este tipo de razonamientos **"teoría de las sustituciones"** y todos sus trabajos están escritos en el lenguaje de los valores que puede tomar una función de las raíces de una ecuación. Así por ejemplo logró probar que el número de valores diferentes que puede tomar una función de las raíces es un divisor del total de sustituciones que pueden hacerse, lo que es una formulación particular del que nosotros hemos denominado **teorema de Lagrange** (sección 4.2).

La "teoría de las sustituciones" de Lagrange influyó en los trabajos del matemático italiano **Paolo Ruffini** (1765-1822), quien creyó haber demostrado que las ecuaciones de quinto grado no pueden resolverse mediante radicales, y en los del matemático noruego **Niels Henrik Abel** (1802-1829), a quien se le reconoce la primera demostración correcta del resultado que creyó haber demostrado Ruffini.

Todos estos trabajos fueron superados por los de **Evariste Galois** (1811-1832) quien en su juventud sentó las bases de la resolución de las ecuaciones algebraicas, enlazando las solución de éstas con propiedades de los grupos de sustituciones. Mientras tanto, usó por primera vez las palabras "grupo", "normal", "isomorfismo" y "simple" (esto último aparecerá en el capítulo siguiente), siempre referidas a permutaciones.

Evariste Galois nació en un pueblo cercano a París y tuvo una corta, pero azarosa, vida. A la muerte de su padre, ocurrida en 1829, se sumó el rechazo para entrar en la Escuela

Politécnica de París, con lo que tuvo que conformarse con ingresar en la Escuela Normal Superior. Sus ideas revolucionarias le valieron la prisión en dos ocasiones, lo que aprovechó para continuar trabajando en sus ideas acerca de la teoría de la resolución de ecuaciones algebraicas.

Poco después de salir de su segundo período en la cárcel, Galois se vio envuelto en un duelo, no se sabe si por razones políticas o amorosas. Temiendo no sobrevivir en el duelo, dedicó los últimos días de su vida a escribir los principales resultados de sus investigaciones matemáticas. El manuscrito, que envió a su amigo Auguste Chevalier, contenía las ideas principales para resolver el problema de la solubilidad mediante radicales de las ecuaciones de quinto grado o superior. Permaneció olvidado hasta que **Joseph Liouville** (1809-1882) lo presentó en 1843 a la Academia de Ciencias de París y fue aceptado para publicarlo.

Mientras tanto, el matemático francés **Augustin-Louis Cauchy** (1789-1857) continuó trabajando en la teoría de los valores que puede tomar una función de las raíces de una ecuación, como había sido descrita por Lagrange. Sus artículos sobre este tema comenzaron en 1815, pero fue en 1846 cuando apareció el resultado que hoy lleva su nombre y que nosotros expondremos en el capítulo 5 de manera general: todo grupo de permutaciones cuyo orden es divisible por un primo p tiene al menos un subgrupo de orden p.

También en el contexto de las permutaciones, el matemático noruego **Mejdell Ludwig Sylow** (1832-1918) publicó en 1873 uno de los trabajos que supuso el mayor avance en esta teoría desde los resultados de Cauchy. Sylow logró demostrar, escrito en lenguaje moderno, que no sólo todo grupo de orden n tiene un subgrupo de orden p si p es primo y divide a n, sino que los tiene de todos los órdenes p^s siempre que p^s divida a n y para el mayor s para el que esto suceda solamente hay uno de ellos. Estos resultados, que se conocen con el nombre de **teoremas de Sylow**, serán expuestos en la sección 5.5.

En el proceso de gestación de la definición abstracta de grupo hay que mencionar al matemático británico **Arthur Cayley** (1821-1895) quién en 1854 propuso una definición abstracta de estructuras que satisfacían algunas propiedades que se asemejaban a la definición de grupo. Ni sus contemporáneos estaban preparados para manejar una definición tan abstracta, ni Cayley estaba convencido de que fuera necesaria, puesto que él continuó trabajando con las permutaciones y además sabía que sus estructuras abstractas podían considerarse grupos de permutaciones (véase su resultado al final de la sección 4.8).

A comienzos del siglo XX las ideas ya estaban maduras para que una definición abstracta de grupo no ofreciera problemas. Varios matemáticos publicaron artículos durante la primera década de este siglo en donde, con ligeras modificaciones, aparecía el concepto abstracto de grupo tal como nosotros lo hemos definido en la sección 2 del capítulo 3.

A partir de aquí los matemáticos comenzaron a trasladar a este contexto más general las definiciones y los resultados de sus antepasados sobre grupos de permutaciones. El teorema de Lagrange, el de Cauchy y los de Sylow fueron generalizados. En lugar de buscar propiedades de algún grupo concreto y después tratar de demostrarlas en la estructura más general, se definieron conceptos directamente para esta estructura y se obtuvieron resultados con ellos. Los conmutadores de dos elementos de un grupo, que expondremos en el capítulo 5, y los automorfismos de un grupo son ejemplos de ello.

El siglo XX ha vivido una gran actividad en torno a la teoría de grupos. La clasificación de todos los grupos finitos, de la que hablaremos en el capítulo 5, ha ocupado gran parte de los trabajos de muchos de los matemáticos que se han dedicado a esta rama. Muchos de los conceptos y de las teorías aparecidas han podido parafrasearse en el lenguaje de los grupos y se han encontrado aplicaciones en cristalografía. Siendo demasiado optimista, según nuestra opinión, el matemático francés **Jules Henri Poincaré** (1854-1912) afirmaba que la teoría de grupos permitiría reducir toda la matemática a su forma más pura.

CAPÍTULO 5

GRUPOS: RESULTADOS SOBRE SU ESTRUCTURA Y CLASIFICACIÓN

5.1. Introducción
5.2. Producto directo y producto semidirecto de grupos
5.3. Estructura de los grupos abelianos finitos
5.4. Invariantes y clasificación de los grupos abelianos finitos
5.5. Teoremas de Sylow
5.6. Grupos simples y grupos solubles
5.7. Grupos de orden pequeño

5.1. INTRODUCCIÓN

Tener una descripción detallada de todos los grupos que pueden existir de un cierto orden, salvo isomorfismos, ha sido el deseo de muchos matemáticos que han trabajado en este tema una vez que se generalizó la definición de grupo. Esta tarea de describir todos los grupos (repetimos de nuevo: salvo isomorfismos) ha resultado costosa. Presentaremos en este capítulo algunos resultados sobre su clasificación a la vez que vamos profundizando en su estructura.

Algo hemos avanzado sobre este asunto en el capítulo anterior dedicado a las propiedades básicas de los grupos. En la sección 4.8, dedicada a permutaciones, demostramos que todo grupo G es isomorfo a un subgrupo del grupo B(G) de sus biyecciones. Si el grupo tiene n elementos, este resultado, que se conoce con el nombre de **Teorema de Cayley**, establece que todo grupo de n elementos es isomorfo a un subgrupo de S_n. En teoría, el problema queda

resuelto con este resultado, pero en la práctica no, ya que el número de elementos de S_n crece rápidamente cuando n aumenta.

En el caso de grupos cíclicos, el problema de su clasificación está totalmente resuelto: en la sección 4.6 se demostró que sólo existen, salvo isomorfismos, los grupos $\mathbf{Z}$ y $\mathbf{Z}_n$, $n \in \mathbf{Z}^+$ que sean cíclicos. Para grupos cíclicos finitos su estructura quedó completamente esclarecida en la misma sección: hemos demostrado que para cada divisor k del orden de un grupo cíclico finito, hay un subgrupo, y sólo uno, cuyo orden es k.

Este resultado es un recíproco del teorema de Lagrange para grupos cíclicos. Recuérdese que el teorema de Lagrange establece que todo subgrupo de un grupo G de orden finito tiene que tener un número de elementos que divide al orden de G. Obsérvese, por tanto, que el teorema es un resultado acerca de la estructura de los grupos, puesto que establece que no pueden existir subgrupos cuyo orden no sea un divisor del orden del grupo. Su recíproco establecería que si G es un grupo finito y k divide al orden de G, este grupo tiene un subgrupo de orden k. Hemos visto que este recíproco es cierto para grupos cíclicos, y también puede demostrarse que es cierto para grupos abelianos, pero no es cierto en general, como muestra el ejemplo que se expone a continuación.

★★ EJEMPLO A. Sea T el siguiente conjunto de simetrías de un tetraedro regular. Cada eje que pasa por el vértice 1 y por el centro del triángulo opuesto a él produce dos simetrías S_{11}, S_{12}, al girar el tetraedro alrededor de este eje $2\pi/3$ o $4\pi/3$ radianes en sentido positivo. Para el resto de los vértices escribimos

$$S_{j1}, S_{j2} \quad j = 2, 3, 4,$$

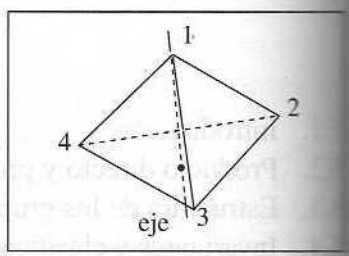


Ilustración 1

con lo cual tenemos 8 elementos en este conjunto. Todos ellos son de orden 3. Además podemos considerar 3 ejes de giro que producen 3 simetrías de orden 2, e_1, e_2, e_3. Cada uno de estos ejes es una recta que pasa por el centro de dos lados opuestos, como en la ilustración 2.

Añadiendo la identidad, este grupo tiene 12 elementos. El lector puede intentar hacer la tabla del grupo directamente, o bien recurrir a numerar los vértices y asociar a cada movimiento de este conjunto una permutación. En cualquier caso es necesario comprobar que la composición de dos de estos elementos no produce ningún movimiento nuevo del tetraedro.

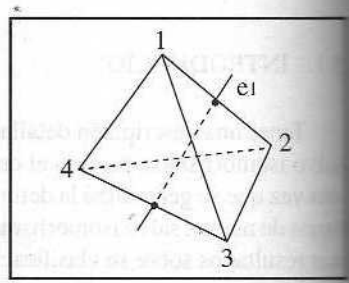


Ilustración 2

Con la operación $\circ$ de composición es fácil demostrar que $(T, \circ)$ es un grupo. El inverso de cada uno de los elementos descritos es fácil de obtener.

$(T, \circ)$ es un ejemplo de grupo en el que **no se cumple el recíproco del teorema de Lagrange.** Demostraremos que $(T, \circ)$ no tiene ningún subgrupo con 6 elementos. Supongamos que T tuviera un subgrupo H de orden 6; como $|T|/|H| = 2$, H ha de ser

normal en T y T/H sería isomorfo a $(\mathbb{Z}_2, +)$. Entonces, los elementos de T/H tienen orden 1 ó 2 y, en consecuencia, para todo $x \in T$, $(xH)^2 = H$; de aquí se deduce que para todo $x \in T$ ha de cumplirse $x^2 \in H$.

Si y es un elemento de T de orden 3, $y = (y^2)^2 \in H$ y por tanto todos los elementos de orden 3 de T deben ser elementos de H. Como hemos visto que hay 8 elementos de orden 3 en T, H no puede tener solamente 6 elementos. Esto muestra que $(T, \circ)$ no puede tener subgrupos de 6 elementos.

Un caso particular del recíproco del teorema de Lagrange es el teorema de Cauchy. Este establece que si G es un grupo finito y p es un primo que divide al orden de G, G tiene un elemento de orden p y, por tanto, también un subgrupo de este mismo orden. Con nuestros conocimientos, este resultado es fácil demostrar para grupos **abelianos** finitos.

Teorema 5.1.1. (Teorema de Cauchy para grupos abelianos finitos) Si G es un grupo abeliano de orden n y p es un primo que divide a n, G contiene un elemento de orden p, y por tanto, un subgrupo con p elementos

Demostración. La demostración se realiza por inducción sobre el orden del grupo. Si $n = 1$ el resultado es claramente cierto. Supongamos que el resultado es cierto para todo grupo G de orden inferior a n, $n > 1$. Como G tiene al menos dos elementos, existe $x \in G$ tal que $x \neq e$. Si $n = p$, x tiene orden p por el teorema de Lagrange, y el resultado queda probado.

Supongamos, por tanto, que $p < n$. Si llamamos s al orden de x y p divide a s, $x^{s/p}$ es de orden p (proposición 4.6.3) y también en este caso hemos demostrado el resultado.

Supongamos entonces que $n > p$ y que p no divide al orden de x. Sea $N = \langle x \rangle$; como G es abeliano, N es un subgrupo normal de G. Puesto que $N \neq \{e\}$,

$$|G/N| = |G|/|N| < |G| = n.$$

Además, como p divide a n y no divide a $|N|$, de la igualdad $n = (n/|N|)\,|N|$ se deduce que p divide a $n/|N| = |G/N|$. Se puede, por tanto, aplicar la hipótesis de inducción a G/N para encontrar un elemento $[y] = yN$ de orden p en G/N. Sea k el orden de y en G. Como yN es de orden p en G/N, $yN \neq N$, $y^2N \neq N$, ..., $y^{p-1}N \neq N$, $y^pN = N$. Se obtiene fácilmente que si $j = 1, 2, 3, \ldots, y^jN = N$ si y sólo si j es un múltiplo de p. Como $y^k = e \in N$ se tiene $y^kN = N$ y, por tanto, k es un múltiplo de p. Así pues, $y^{k/p} \in G$ y tiene orden p (proporción 4.6.3). También en este caso hemos encontrado un elemento de orden p. ■

Muchos resultados son más fáciles demostrar para grupos abelianos. El teorema de Cauchy que acabamos de probar es un ejemplo. En el caso de grupos abelianos finitos hay una caracterización completa de estos grupos que se expone en las secciones 5.3 y 5.4. En ellas se demuestra que todo grupo abeliano finito es isomorfo a un producto directo de grupos $(\mathbb{Z}_k, +)$ donde los órdenes de estos grupos están relacionados con el orden del grupo.

El teorema de Cauchy también es cierto para grupos no necesariamente abelianos; esto será una consecuencia de los teoremas de Sylow que se exponen en la sección 5.5. Estos teoremas son los más clásicos que se conocen acerca de la estructura de los grupos finitos.

Si se analiza detenidamente la demostración que hemos realizado del teorema de Cauchy para grupos abelianos finitos se observa que la idea principal es dividir G en dos grupos N y G/N, ambos de orden inferior al orden de G, para poder aplicar la hipótesis de inducción. Esto ha sido posible ya que todo grupo abeliano cuyo orden no sea primo tiene un subgrupo normal propio. Esto no sucede en todos los grupos: los grupos alternados de n elementos, Alt(n), con $n \geq 5$, son ejemplos de ello, lo que se demostrará en la sección 5.6.

Esto sugiere que los grupos que no tengan subgrupos propios normales son los más sencillos, a partir de los cuales podrían obtenerse el resto de los grupos que sí los poseen. Estos grupos, que se llaman **simples**, constituyen los átomos que aparecen en la descomposición de un grupo en factores elementales: este resultado se conoce con el nombre de teorema de Jordan-Hölder y se expone en la sección 5.6. Encontrar todos los grupos simples ha sido una tarea costosa, de la que también hablaremos en este capítulo. También aquí estudiaremos los grupos solubles, que juegan un papel principal en los resultados sobre la imposibilidad de resolver ecuaciones algebraicas de grado cinco o superior mediante radicales.

La última sección se dedica a estudiar los grupos de orden pequeño. Se pueden apreciar aquí las dificultades que entraña la clasificación de todos los grupos finitos.

EJERCICIOS 5.1

1. Escribir la tabla completa del grupo $(T, \circ)$ descrito en el ejemplo A de esta sección usando como operación la composición de aplicaciones.
2. Encontrar subgrupos de órdenes 2, 3 y 4 en el grupo $(T, \circ)$ del ejemplo A (véase ejercicio 1).
3. Encontrar subgrupos de órdenes 2, 3, 4 y 6 en el grupo D_{12} de las simetrías de un hexágono regular.

5.2. PRODUCTO DIRECTO Y PRODUCTO SEMIDIRECTO DE GRUPOS

Uno de nuestros próximos resultados nos permitirá afirmar que todo grupo abeliano de orden finito es isomorfo a un producto directo de grupos cíclicos. Por esta razón, expondremos en esta sección el concepto de producto directo de varios grupos. Para el caso de dos grupos este concepto fue ampliamente estudiado en la sección 4.7 del capítulo 4.

Definición 5.2.1. Dados los grupos $G_1, G_2, \ldots, G_k$ definimos su producto directo como el grupo formado por los elementos de la forma $(g_1, g_2, \ldots, g_k)$ con $g_j \in G_j$ para todo $j = 1, 2, \ldots, k$, con la operación

$$(g_1, g_2, \ldots, g_k)(g'_1, g'_2, \ldots, g'_k) = (g_1 g'_1, g_2 g'_2, \ldots, g_k g'_k).$$

Se deja para el lector la comprobación de que la operación dada cumple todas las propiedades de grupo (ejercicio 1 al final de esta sección); el elemento neutro es $(e_1, e_2, \ldots, e_k)$ donde e_j es el elemento neutro de G_j, j= 1, 2, ..., k. El inverso del elemento $(g_1, g_2, \ldots, g_k)$ es $(g_1^{-1}, g_2^{-1}, \ldots, g_k^{-1})$.

Los símbolos que utilizaremos para describir el producto directo de varios grupos serán

$$G_1 \times G_2 \times \ldots \times G_k \quad \text{o} \quad \bigtimes_{j=1}^{k} G_j .$$

Observar que la operación de cada grupo G_j no es necesariamente la misma, aunque se haya usado el mismo signo en la definición anterior para simbolizarla.

Si todos los grupos tienen como operación la "suma", el producto directo se llama **suma directa**, y en este caso los símbolos que se usan son

$$G_1 \oplus G_2 \oplus \ldots \oplus G_k \quad \text{o} \quad \bigoplus_{j=1}^{k} G_j .$$

★★ EJEMPLO A. $\mathbf{Z}_2 \times \mathbf{Z}_4$ es un grupo cuyos elementos son ([0], [0]), ([0], [1]), ([0], [2]), ([0], [3]), ([1], [0]), ([1], [1]), ([1], [2]), ([1], [3]). Obsérvese que este grupo **no** es isomorfo a $(\mathbf{Z}_8, +)$ ya que no tiene ningún elemento de orden 8.

★★ EJEMPLO B. $(\mathbf{R}^n, +) = (\mathbf{R} \oplus \ldots \oplus \mathbf{R}, +)$ donde en la suma directa hay n factores y $((\mathbf{Q}^*)^n, \cdot) = (\mathbf{Q}^* \times \ldots \times \mathbf{Q}^*, \cdot)$ donde en el producto directo hay n factores.

Estamos interesados en conocer bajo qué condiciones un grupo dado es isomorfo a un producto directo de algunos de sus subgrupos. En la proposición 4.7.3 se demostró que esto ocurre para dos subgrupos H_1 y H_2 si ambos son normales y satisfacen $H_1 \cap H_2 = \{e\}$ y $H_1H_2 = G$ donde $H_1H_2 = \{h_1h_2 : h_1 \in H_1, h_2 \in H_2\}$. Para varios subgrupos tenemos el resultado que se enuncia y demuestra a continuación.

Teorema 5.2.2. Un grupo G es isomorfo a un producto directo de sus subgrupos H_1, H_2, ..., H_k si

1) todos los H_j son subgrupos normales de G;

2) $H_j \cap (\prod_{i \neq j} H_i) = \{e\}$ para todo j = 1, 2, ..., k;

3) $\prod_{i=1}^{k} H_i = G$.

Aquí, $\prod_{i=1}^{m} H_i = \{h_1h_2 \ldots h_m : h_j \in H_j, j = 1 \ldots m\}$.

Demostración. El teorema quedará demostrado si exhibimos un isomorfismo f de G en $H_1 \times H_2 \times \ldots \times H_k$. Debido a la condición tercera, dado $g \in G$ podemos encontrar elementos $h_1 \in H_1$, $h_2 \in H_2$, ..., $h_k \in H_k$ de manera que $g = h_1h_2 \ldots h_k$. Por lo tanto parece razonable definir $f(g) = (h_1, h_2, \ldots, h_k)$.

La correspondencia f será una aplicación si logramos probar que la representación de g como producto de $h_1, h_2, \ldots, h_k$ es única. Para ello, suponer que tuviéramos dos representaciones de la forma

$$h_1h_2 \ldots h_k = g = h'_1h'_2 \ldots h'_k ,$$

con $h_j, h'_j \in H_j$, $j = 1, 2, \ldots, k$. De la igualdad anterior deducimos

$$(h'_1)^{-1}h_1 = (h'_2 \ldots h'_k)(h_k^{-1} \ldots h_2^{-1}) .$$

La parte izquierda de esta igualdad es un elemento de H_1. La parte derecha es un elemento de $\prod_{j \neq 1} H_j$ ya que los H_j son subgrupos normales de G; para demostrar esto observar que

$$(h'_2 \ldots h'_k)(h_k^{-1} \ldots h_2^{-1}) = h'_2(h'_3 \ldots h'_kh_k^{-1} \ldots h_3^{-1})h_2^{-1} = (h'_2h''_2)(h'_3 \ldots h'_kh_k^{-1} \ldots h_3^{-1}) =$$
$$= \ldots = (h'_2h''_2)(h'_3h''_3) \ldots (h'_kh''_k) \in \prod_{j \neq 1} H_j .$$

Por la segunda condición del enunciado del teorema

$$(h'_1)^{-1}h_1 = e = (h'_2 \ldots h'_k)(h_k^{-1} \ldots h_2^{-1})$$

y por tanto $h_1 = h'_1$ y $h'_2 \ldots h'_k = h_2 \ldots h_k$. A partir de esta última igualdad y observando que $\prod_{i \neq 1,2} H_j \subset \prod_{i \neq 1} H_j$ se demuestra, de manera análoga a como se hizo anteriormente, que $h_2 = h'_2$. Después de realizar este razonamiento $k - 1$ veces se consigue demostrar las igualdades $h_1 = h'_1$, $h_2 = h'_2, \ldots, h_k = h'_k$, que era lo deseado.

Puede comprobarse fácilmente que f es biyectiva. El teorema quedará demostrado si probamos que f es un homomorfismo de grupos. Sean $g, g' \in G$ con representaciones

$$g = h_1h_2 \ldots h_k , \quad g' = h'_1h'_2 \ldots h'_k .$$

Si fuera cierto que

$$gg' = (h_1h_2 \ldots h_k)(h'_1h'_2 \ldots h'_k) = (h_1h'_1)(h_2h'_2) \ldots (h_kh'_k) \qquad (*)$$

tendríamos

$$f(gg') = (h_1h'_1, h_2h'_2, \ldots, h_kh'_k) = (h_1, h_2, \ldots, h_k)(h'_1, h_2, \ldots, h'_k) = f(g)f(g') ,$$

lo cual completaría la demostración. La igualdad (*) se ha demostrado para $k = 2$ en la proposición 4.7.3. Para el caso $k > 2$ véase el ejercicio 4 al final de esta sección. ■

★★ EJEMPLO C. En $(\mathbf{Z}_{30}, +)$ tenemos los subgrupos

$$H_1 = \{[0], [15]\}, \quad H_2 = \{[0], [10], [20]\}, \quad H_3 = \{[0], [6], [12], [18], [24]\} ,$$

que son normales ya que $(\mathbf{Z}_{30},+)$ es abeliano. Puede comprobarse que

$$H_1 \cap (H_2 + H_3) = \{[0]\}\ ,\ H_2 \cap (H_1 + H_3) = \{[0]\} \text{ y } H_3 \cap (H_1 + H_2) = \{[0]\}.$$

Por ejemplo, $H_1 + H_2 = \{[0], [10], [15], [20], [25], [5]\}$ y por tanto solamente posee el elemento [0] en común con H_3. Además $H_1 + H_2 + H_3 = \mathbf{Z}_{30}$. Por el teorema 5.2.2, $(\mathbf{Z}_{30}, +) \approx H_1 \oplus H_2 \oplus H_3$. Puesto que H_1, H_2 y H_3 son grupos cíclicos de órdenes 2, 3 y 5, respectivamente, se tiene

$$\mathbf{Z}_{30} \approx \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5\ .$$

★★ EJEMPLO D. Sea G = {e, a, b, c, d, f, g, h} un grupo **abeliano** de 8 elementos en el que todo elemento, salvo la identidad, es de orden 2, y tal que

$$df = a, \quad dg = b, \quad dh = c, \quad fg = c, \quad fh = b, \quad gh = a\ .$$

Estas relaciones son suficientes para escribir la tabla del grupo:.

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	e	a	g	h	d	f
c	c	b	a	e	h	g	f	d
d	d	f	g	h	e	a	b	c
f	f	d	h	g	a	e	c	b
g	g	h	d	f	b	c	e	a
h	h	g	f	d	c	b	a	e

Invitamos al lector a comporbar esta tabla. Demostraremos

$$G \approx \langle d\rangle \times \langle f\rangle \times \langle g\rangle\ .$$

En efecto, los subgrupos <d>, <f> y <g> son normales ya que G es abeliano. Además

$$\langle d\rangle \cap (\langle f\rangle\langle g\rangle) = \{d, e\} \cap \{f, g, c, e\} = \{e\}\ ,$$

y análogamente se comprueban las restantes intersecciones. Finalmente, <d> <f> <g> = = {d, e} {f, g ,c, e} = {a, b, dc, d, f, g, c, e}; puesto que dc = d(dh) = d^2h = h, se tiene que <d> <f> <g> = G. Obsérvese que

$$G \approx \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2\ .$$

No siempre puede escribirse un grupo como producto directo de sus subgrupos de **manera única**. En este ejemplo puede comprobarse que $G \approx \langle d\rangle \times \langle f\rangle \times \langle h\rangle$.

El producto directo es una forma de construir un grupo más grande a partir de dos o más grupos dados. En este caso cada uno de los subgrupos es isomorfo a un subgrupo normal del grupo grande (véase el ejercicio 2 al final de esta sección). A continuación mostraremos una forma de construir un grupo más grande a partir de dos dados, donde uno de ellos no es necesariamente isomorfo a un subgrupo normal del grupo más grande. Esto producirá nuevos ejemplos de grupos.

Para hacer esto necesitamos dos grupos G_1 y G_2 y un homomorfismo φ de G_2 en $\mathrm{Aut}(G_1)$. Varios conceptos han aparecido súbitamente sobre los que conviene recapacitar, aunque ninguno de ellos es nuevo para quien haya trabajado las secciones y los ejercicios de los capítulos anteriores.

$\mathrm{Aut}(G_1)$, que es el conjunto de todos los isomorfismos de G_1 en G_1, apareció en el ejercicio 10 de la sección 4.4, y se pidió demostrar que era un grupo con la composición de aplicaciones. Si no se hizo antes, ahora es una buena oportunidad para demostrar que $(\mathrm{Aut}(G_1), \circ)$ es un grupo cuando G_1 lo es; su elemento neutro es el isomorfismo identidad I_{G_1} que deja invariantes todos los elementos de G_1, y si $f \in \mathrm{Aut}(G_1)$, f^{-1} es también un elemento de $\mathrm{Aut}(G_1)$ que es el inverso de f en este grupo.

Lo que necesitamos es una aplicación $\varphi: G_2 \to \mathrm{Aut}(G_1)$ que sea un homomorfismo entre el grupo G_2 y el grupo $(\mathrm{Aut}(G_1), \circ)$. Es necesario aclararse con la notación: para cada g_2 de G_2, $\varphi(g_2)$ es un automorfismo de G_1 y por tanto tiene sentido calcular $\varphi(g_2)(g_1)$ para todo $g_1 \in G_1$. Conviene recordar algunas consecuencias inmediatas del hecho de que φ y $\varphi(g_2)$ sean homomorfismos, que se usarán en los resultados que se exponen más adelante.

Lema 5.2.3. Sean G_1, G_2 grupos y $\varphi: G_2 \to \mathrm{Aut}(G_1)$ un homomorfismo de grupos:

i) Si e_2 es el neutro de G_2, $\varphi(e_2) = I_{G_1}$.
ii) Para todo $x_2, y_2 \in G_2$, $\varphi(x_2) \circ \varphi(y_2) = \varphi(x_2 y_2)$.
iii) Para todo $g_2 \in G_2$, $\varphi(g_2) \circ \varphi(g_2^{-1}) = I_{G_1}$.
iv) Para todo $g_2 \in G_2$, $\varphi(g_2)(e_1) = e_1$, donde e_1 es el elemento neutro de G_1.
v) Para todo $g_2 \in G_2$, $\varphi(g_2)(x_1 y_1) = \varphi(g_2)(x_1)\,\varphi(g_2)(y_1)$ para todo x_1, y_1 de G_1.

Demostración. i) es debida a que e_2 es el neutro de G_2, I_{G_1} es el neutro de $(\mathrm{Aut}(G_1), \circ)$ y φ es un homomorfismo. La propiedad ii) únicamente expresa que φ es un homomorfismo. Para demostrar iii) tomar $x_2 = g_2$ e $y_2 = g_2^{-1}$ en ii) y aplicar las dos propiedades anteriores. Finalmente iv) y v) son consecuencia de que $\varphi(g_2)$ es un automorfismo de G_1 para todo $g_2 \in G_2$. ∎

★★ EJEMPLO E. Sea G_1 abeliano y $G_2 = \langle g\rangle$ cíclico. Definimos $\varphi(g): G_1 \to G_1$ mediante $\varphi(g)(x) = x^{-1}$ para todo $x \in G_1$; como G_1 es abeliano, $\varphi(g)$ es un homomorfismo de grupos y la biyectividad es fácil de probar. Como G_2 es cíclico podemos definir $\varphi: G_2 \to \mathrm{Aut}(G_1)$ de manera que sea un homomorfismo, es decir

$$\varphi(g^k) = \varphi(g)^k .$$

Así pues si $x \in G_1$

$$\varphi(g^k)(x) = \varphi(g)^k(x),$$

y por tanto $\varphi(g^k)(x) = x$ si k es par o cero y $\varphi(g^k)(x) = x^{-1}$ si k es impar.

★★ EJEMPLO F. Dado un grupo G, definir φ: $G \to \text{Aut}(G)$ mediante $\varphi(g)(x) = gxg^{-1}$, que son los automorfismos internos de G que ya han aparecido en el ejemplo E de la sección 4.4. En el problema 9 de aquella sección se pidió demostrar que $\varphi(g) \in \text{Aut}(G)$ para todo $g \in G$; si no se ha comprobado este resultado, ahora es una buena ocasión para hacerlo. Vamos a demostrar que φ es un homomorfismo; si $g_1, g_2 \in G$ y $x \in G$

$$\varphi(g_1g_2)(x) = g_1g_2x(g_1g_2)^{-1} = g_1g_2xg_2^{-1}g_1^{-1} = \varphi(g_1)(g_2xg_2^{-1}) = \varphi(g_1) \circ \varphi(g_2)(x).$$

Este homomorfismo jugará un papel importante cuando queramos saber si un grupo es isomorfo a un producto semidirecto de dos de sus subgrupos.

Estamos ya preparados para poder definir el producto semidirecto de dos grupos.

Definición 5.2.4. Sean G_1 y G_2 dos grupos y φ un automorfismo de G_2 en $\text{Aut}(G_1)$. En el conjunto producto $G_1 \times G_2$ definimos

$$(a, b) \times_\varphi (a', b') = (a\,\varphi(b)(a'), bb').$$

★★ EJEMPLO G. Si $\varphi : G_2 \to \text{Aut}(G_1)$ es tal que $\varphi(x) = I_{G_1}$ para todo $x \in G_2$, la operación de la definición 5.24 es la del producto directo.

★★ EJEMPLO H. Si $\varphi : G \to \text{Aut}(G)$ está definida mediante $\varphi(g)(x) = gxg^{-1}$ (véase ejemplo F) se tiene

$$(a, b) \times_\varphi (a', b') = (a\,\varphi(b)(a'), bb') = (aba'b^{-1}, bb'),$$

y cuando G es abeliano esta operación se reduce a la del producto directo en $G \times G$.

Teorema 5.2.5. Sean G_1, G_2 grupos y φ como en 5.2.4. La operación $\times_\varphi$ definida en 5.2.4 hace de $G_1 \times G_2$ un grupo que se llama **producto semidirecto** de G_1 y G_2 con respecto a φ y se simboliza mediante $G_1 \times_\varphi G_2$.

Demostración. La operación es claramente cerrada en $G_1 \times G_2$. La propiedad asociativa se demuestra cuidadosamente:

$$[(a, b) \times_\varphi (c, d)] \times_\varphi (e, f) = (a\,\varphi(b)(c), bd)(e, f) \qquad \text{Def. de } \times_\varphi$$
$$= (a\,\varphi(b)(c)\,\varphi(bd)(e), (bd)f) \qquad \text{Def. de } \times_\varphi$$

$$= (a\ \varphi(b)\ (c)\ \varphi(b)\ (\varphi(d)\ (e)),\ b(df)) \qquad \varphi \text{ automorfismo}$$
$$= (a\ \varphi(b)\ (\ c\varphi(d)\ (e),\ b(df)) \qquad \varphi(b) \text{ aut. en } G_1$$
$$= (a, b) \times_\varphi (c\ \varphi(d)\ (e),\ df) \qquad \text{Def. de } \times_\varphi$$
$$= (a, b) \times_\varphi [(c, d) \times_\varphi (e,f)] \qquad \text{Def. de } \times_\varphi$$

Es claro que (e_1, e_2) es el neutro de esta operación ya que

$$(a, b) \times_\varphi (e_1, e_2) = (a\ \varphi(b)\ (e_1),\ be_2) = (a, b),$$

donde se ha hecho uso de la parte iv) del lema 5.2.3, y además

$$(e_1, e_2) \times_\varphi (a, b) = (e_1\ \varphi(e_2)\ (a),\ e_2 b) = (a, b),$$

debido a la parte i) del mismo lema.

El inverso de (a, b) es $(\varphi(b^{-1})\ (a^{-1}),\ b^{-1})$. Comprobaremos que es cierto solamente por la derecha dejando la comprobación por la izquierda como ejercicio:

$$(a, b) \times_\varphi (\varphi(b^{-1})\ (a^{-1}),\ b^{-1}) = (a\ \varphi(b)\ (\varphi(b^{-1})\ (a^{-1})),\ bb^{-1}) =$$
$$= (a\ \varphi(bb^{-1})\ (a^{-1}),\ e_2) = (aa^{-1},\ e_2) = (e_1,\ e_2)\ ,$$

en donde se ha hecho uso de algunos de los resultados contenidos en el lema 5.2.3. ■

Proposición 5.2.6. Sean G_1 y G_2 dos grupos finitos y φ como en 5.2.4.

1) El grupo $G_1 \times_\varphi G_2$ definido en 5.2.5 tiene $|G_1|\,|G_2|$ elementos.
2) G_1 es isomorfo a $\underline{G}_1 = \{(a, e_2) : a \in G_1\}$ y $\underline{G}_1$ es normal en $G_1 \times_\varphi G_2$.
3) G_2 es isomorfo a $\underline{G}_2 = \{(e_1, b) : b \in G_2\}$.

Demostración. Es claro que $G_1 \times_\varphi G_2$ tiene los mismos elementos que $G_1 \times G_2$. Para demostrar 2) definimos $f : G_1 \to \underline{G}_1$ mediante $f(a) = (a, e_2)$, que es una biyección. Además es un homomorfismo ya que

$$f(aa') = (aa', e_2) = (a\ \varphi(e_2)\ (a'),\ e_2) = (a, e_2) \times_\varphi (a', e_2) = f(a) \times_\varphi f(a').$$

Eligiendo $(a, b) \in G_1 \times G_2$ y $(g, e_2) \in G_1$, el siguiente razonamiento muestra que $\underline{G}_1$ es normal en $G_1 \times G_2$:

$$(a, b) \times_\varphi (g, e_2) \times_\varphi (a, b)^{-1} = (a\ \varphi(b)\ (g),\ b) \times_\varphi (\varphi(b^{-1})\ (a^{-1}),\ b^{-1}) =$$
$$= (a\ \varphi(b)\ (g)\ \varphi(b)\ (\varphi(b^{-1})\ (a^{-1})),\ e_2) = (a\ \varphi(b)\ (g)a^{-1},\ e_2) \in \underline{G}_1\ .$$

La parte 3) es similar a la anterior definiendo $g(b) = (e_1, b)$. ■

★★ EJEMPLO I. Definir $\varphi: \mathbf{Z}_2 \to \mathrm{Aut}(\mathbf{Z}_3)$ mediante $\varphi([0]) = I$, $\varphi([1])\ (k) = -k$; comprobar que $\varphi([1])$ es un automorfismo de $\mathbf{Z}_3$ y que φ es un homomorfismo. La proposición

5.2.6 nos permite afirmar que el grupo $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_2$ tiene 6 elementos y el subgrupo $H = \{([n], [0]) : n \in \mathbf{Z}_3\}$ es un subgrupo normal con 3 elementos. La tabla de este grupo y el orden de cada uno de sus elementos se muestran a continuación:

$\mathbf{Z}_3 \times_\varphi \mathbf{Z}_2$	([0], [0])	([0], [1])	([1], [0])	([1], [1])	([2], [0])	([2], [1])
([0], [0])	([0], [0])	([0], [1])	([1], [0])	([1], [1])	([2], [0])	([2], [1])
([0], [1])	([0], [1])	([0], [0])	([2], [1])	([2], [0])	([1], [1])	([1], [0])
([1], [0])	([1], [0])	([1], [1])	([2], [0])	([2], [1])	([0], [0])	([0], [1])
([1], [1])	([1], [1])	([1], [0])	([0], [1])	([0], [0])	([2], [1])	([2], [0])
([2], [0])	([2], [0])	([2], [1])	([0], [0])	([0], [1])	([1], [0])	([1], [1])
([2], [1])	([2], [1])	([2], [0])	([1], [1])	([1], [0])	([0], [1])	([0], [0])

$\mathbf{Z}_3 \times_\varphi \mathbf{Z}_2$	([0], [0])	([0], [1])	([1], [0])	([1], [1])	([2], [0])	([2], [1])
Orden	1	2	3	2	3	2

Por tanto, este grupo tiene dos elementos de orden 3, tres elementos de orden 2 y no es conmutativo. Si identificamos ([0], [1]) con B en el grupo diédrico D_6 de las simetrías de un triángulo equilátero y ([1], [0]) con A en el mismo grupo, es fácil probar que $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_2$ es isomorfo a D_6. Recordar que D_6 es también isomorfo a S_3, el grupo de las permutaciones de tres elementos.

★★ EJEMPLO J. El ejemplo anterior puede generalizarse para definir $\mathbf{Z}_n \times_\varphi \mathbf{Z}_2$ usando el mismo homomorfismo φ que en el ejemplo I. La aplicación $F([k], [s]) = F(k([1], [0]) + s([0], [1])) = A^k B^s$ permite demostrar que $\mathbf{Z}_n \times_\varphi \mathbf{Z}_2$ es isomorfo a D_{2n}.

★★ EJEMPLO K. Los resultados de los dos ejemplos anteriores pueden generalizarse para construir $G \times_\varphi \mathbf{Z}_2$ donde G es un grupo abeliano. Para ello, definir φ: $\mathbf{Z}_2 \to \text{Aut}(G)$ mediante

$$\varphi([0]) = I$$
$$\varphi([1])(x) = x^{-1}.$$

$\varphi([1])$ es un automorfismo de G ya que G es abeliano:

$$\varphi([1])(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi([1])(x)\,\varphi([1])(y).$$

Cuando $G = \mathbf{Z}_n$ se obtiene el ejemplo J. Si $G = \mathbf{Z}$ el grupo $\mathbf{Z} \times_\varphi \mathbf{Z}_2$ se simboliza mediante D_∞ y es un grupo que no es isomorfo a $\mathbf{Z}$ ya que no es abeliano:

$$(6, [1]) \times_\varphi (2, [0]) = (6 + \varphi([1])(2), [1]) = (4, [1])$$

y

$$(2, [0]) \times_\varphi (6, [1]) = (2 + \varphi([0])(6), [1]) = (8, [1]) .$$

★★ EJEMPLO L. Considerar $\varphi: \mathbf{Z}_4 \to \text{Aut}(\mathbf{Z}_3)$ dado por $\varphi([0]) = I$, $\varphi([1])([k]) = -k$, $\varphi([2]) = I$ y $\varphi([3])([k]) = -k$. Observar que basta definir $\varphi([1])$ y el resto queda definido usando que φ debe ser homomorfismo y que $\mathbf{Z}_4 = \langle [1] \rangle$. El grupo $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$ tiene 12 elementos y no es abeliano ya que

$$([1], [1]) \times_\varphi ([2], [0]) = ([1] - [2], [1]) = ([2], [1])$$

y

$$([2], [0]) \times_\varphi ([1], [1]) = ([2] + [1], [1]) = ([0], [1]) .$$

Conocemos dos grupos de 12 elementos no abelianos; uno de ellos es el grupo diédrico D_{12} de las simetrías de un hexágono regular y otro es el grupo T de simetrías de un tetraedro regular descrito en el ejemplo A de la sección 5.1. ¿Será alguno de éstos isomorfo a $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$? La respuesta a esta pregunta es negativa y la forma más fácil de probarlo es estudiando los órdenes de los elementos de estos grupos.

Los grupos D_{12} y T no tienen elementos de orden 4, mientras que $([0], [1])$ es de orden 4 en $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$, ya que

$$([0], [1]) \times_\varphi ([0], [1]) = ([0], [2])$$

y

$$([0], [1]) \times_\varphi ([0], [1]) \times_\varphi ([0], [1]) \times_\varphi ([0], [1]) = ([0], [2]) \times_\varphi ([0], [2]) = ([0], [0]) .$$

$\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$ es, por tanto, un nuevo grupo de 12 elementos.

Finalizamos esta sección estableciendo un resultado que permite reconocer en qué ocasiones un grupo es producto semidirecto de dos de sus subgrupos; es un resultado análogo al de la proposición 4.7.3 (cuya generalización se ha dado en el teorema 5.2.2 de esta sección) para el producto directo. Más adelante este resultado se usará para caracterizar todos los grupos de orden pequeño (sección 5.7).

Teorema 5.2.7. Sea G un grupo con M y N subgrupos de G tal que M es normal en G. Si $M \cap N = \{e\}$ y $MN = G$, G es isomorfo al producto semidirecto de M y N mediante el homomorfismo $\varphi: N \to \text{Aut}(M)$ dado por $\varphi(n)(m) = nmn^{-1}$.

Demostración. Al igual que en la demostración de la proposición 4.7.3, todo elemento de G es de la forma $g = mn$, $m \in M$, $n \in N$, de manera única, ya que $M \cap N = \{e\}$. La aplicación

$$f : G \to M \times_\varphi N$$

dada por $f(g) = f(mn) = (m, n)$ está bien definida y, al igual que en la proposición 4.7.3, es suprayectiva e inyectiva.

Sólo falta demostrar que f es un homomorfismo de grupos. Sean $g_1 = m_1n_1$ y $g_2 = m_2n_2$ dos elementos de G y su descomposición en elementos de M y N respectivamente. Entonces

$$g_1g_2 = (m_1n_1)(m_2n_2) = m_1n_1m_2(n_1^{-1}n_1)n_2 = m_1\varphi(n_1)(m_2)n_1n_2$$

donde $m_1\,\varphi(n_1)\,(m_2)$ es de M y n_1n_2 es de N; ésta es, por tanto, la descomposición de g_1g_2 en elementos de M y N. Así pues,

$$\begin{aligned} f(g_1g_2) &= (m_1\,\varphi(n_1)\,(m_2),\, n_1n_2) \\ &= (m_1,\, n_1) \times_\varphi (m_2,\, n_2) \qquad \text{Def. de } \times_\varphi \\ &= f(g_1) \times_\varphi f(g_2)\,, \end{aligned}$$

lo que muestra que f es un isomorfismo y por tanto $G \approx M \times_\varphi N$. ■

★★ EJEMPLO M. En $S_3 = \{I, \alpha = (1\,2\,3), \alpha^2 = (1\,3\,2), \beta = (1\,2), \alpha\beta = (1\,3), \alpha^2\beta = (2\,3)\}$, el subgrupo $M = \{I, \alpha, \alpha^2\}$ es de orden 3 y, por tanto, normal en S_3, y el subgrupo N generado por β es de orden 2. Claramente $M \cap N = \{I\}$ y $MN = S_3$. Por el teorema 5.2.7, S_3 es isomorfo a $M \times_\varphi N$. Como $M \approx \mathbf{Z}_3$ y $N \approx \mathbf{Z}_2$, del ejercicio 15 del final de esta sección se deduce que S_3 es isomorfo a un producto semidirecto de $\mathbf{Z}_3$ y $\mathbf{Z}_2$:

$$S_3 \approx \mathbf{Z}_3 \times_\varphi \mathbf{Z}_2\,.$$

EJERCICIOS 5.2

1. Demostrar que $G_1 \times G_2 \times \ldots \times G_k$ es un grupo con la operación dada en la definición 5.2.1.
2. Demostrar que $H_j = \{(e_1, \ldots, g_j, \ldots, e_k)\colon g_j \in G_j\}$ es un subgrupo normal de $G_1 \times G_2 \times \ldots \ldots \times G_k$ para todo $j = 1, 2, \ldots, k$.
3. Demostrar que las clases de restos módulo 16 cuyos representantes son primos con 16 es un grupo abeliano de 8 elementos con respecto a la **multiplicación**. Escribir este grupo como producto directo de algunos de sus subgrupos.
4. Sea G un grupo y $H_1, H_2, \ldots, H_k$ subgrupos normales de G tales que $H_j \cap \left(\prod_{i \neq j} H_i \right) = \{e\}$. Demostrar
   i) $H_i \cap H_j = \{e\}$ para todo $i \neq j$.
   ii) Si $a \in H_i$, $b \in H_j$, $i \neq j$, a y b conmutan.
   iii Demostrar la igualdad (*) que se ha usado en la demostración del teorema 5.2.2. (Esto completará la demostración de este teorema.)
5. Demostrar que $(\mathbf{Z}_{12}, +)$ es isomorfo a $\mathbf{Z}_4 \oplus \mathbf{Z}_3$, pero no es isomorfo a $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$.
6. Dar un ejemplo de un grupo G y subgrupos normales $H_1, H_2, \ldots, H_k$ tal que $G = H_1H_2 \ldots H_k$ y $H_i \cap H_j = \{e\}$ si $i \neq j$, pero G no sea isomorfo al producto directo de $H_1, H_2, \ldots, H_k$.

7. Sea $(g_1, g_2, \ldots, g_n) \in \bigtimes_{i=1}^{n} G_i$; si cada g_j es de orden r_j en G_j, demostrar que $(g_1, g_2, \ldots, g_n)$ tiene orden $[r_1, r_2, \ldots, r_n]$ (es decir, el mínimo común múltiplo) en $\bigtimes_{i=1}^{n} G_i$.

8. Demostrar que $\bigoplus_{i=1}^{m} \mathbf{Z}_{m_i}$ es cíclico e isomorfo a $\mathbf{Z}_{m_1 \ldots m_n}$ si y sólo si los m_i son primos entre sí.

9. Encontrar todos los subgrupos propios no triviales de $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$.

10. Sea G un grupo abeliano de orden $n > 1$. Si $k \in \mathbf{Z}$ y $(n, k) = 1$, demostrar que $f_k(x) = x^k$ es un automorfismo de G.

11. Sea G un grupo cíclico de orden $n > 1$ y para $k \in \mathbf{Z}$ definir $f_k(x) = x^k$. Demostrar que f_k es un automorfismo de G si y sólo si n y k son primos entre sí (usar que si x tiene orden n, x^k tiene orden $n/(n, k)$).

12. Demostrar que $(\mathrm{Aut}(G), \circ)$, con $|G| = n$ y G cíclico, es un grupo isomorfo a $(I(\mathbf{Z}_n^*), \cdot)$. (Véase la definición de este grupo en el ejercicio 9 de la sección 4.2.)

13. Demostrar que las siguientes condiciones son equivalentes cuando G_1 y G_2 son grupos y φ es un homomorfismo de G_2 en $\mathrm{Aut}(G_1)$:

    a) La aplicación identidad de $G_1 \times_\varphi G_2$ en $G_1 \times G_2$ es un homomorfismo de grupos;
    b) $\varphi(z)$ es la identidad en G_1 para todo $z \in G_2$;
    c) $\underline{G}_2$ es normal en $G_1 \times_\varphi G_2$, donde $\underline{G}_2 = \{(e_1, g) : g \in G_2\}$.

14. Encontrar dos subgrupos M y N de D_{2n} tal que D_{2n} sea isomorfo al producto semidirecto de M y N.

15. Sean H, H', K, K' grupos tales que H es isomorfo a H' y K es isomorfo a K'; sea φ un homomorfismo de K en Aut(H). Demostrar que existe un homomorfismo χ de K' en Aut(H') tal que $H \times_\varphi K$ es isomorfo a $H' \times_\chi K'$.

5.3. ESTRUCTURA DE LOS GRUPOS ABELIANOS FINITOS

En esta sección y en la siguiente estudiaremos la estructura de los grupos abelianos finitos llegando a una descripción satisfactoria de todos ellos en términos del producto directo de grupos $(\mathbf{Z}_k, +)$.

Sea A un grupo abeliano con un número finito de elementos n. Si p es un factor primo de n, definimos $\mathbf{S_p = \{a \in A: a \text{ tiene como orden una potencia de p}\}}$. Evidentemente, $e \in S_p$ ya que su orden es $1 = p^0$; además, si $a, b \in S_p$ con $\mathrm{orden}(a) = p^n$, $\mathrm{orden}(b) = p^m$ se tiene que

$$(ab^{-1})^{p^{n+m}} = a^{p^n p^m} (b^{-1})^{p^m p^n} = e$$

ya que A es abeliano; por tanto, $ab^{-1} \in S_p$ y S_p es un subgrupo de A.

El subgrupo S_p recibe el nombre de **p-subgrupo de Sylow** asociado con el grupo abeliano A.

★★ EJEMPLO A. Si A es un grupo abeliano tal que $|A| = p^n$ con p primo, se tiene que $S_p = A$ ya que todo elemento es de orden p^s con $0 \leq s \leq n$.

★★ EJEMPLO B. Sea A un grupo abeliano generado por los elementos a y c tales que $a^3 = e$, $c^4 = e$. Sus elementos son

$$\{e, a, a^2, c, c^2, c^3, ac, a^2c, ac^2, a^2c^2, ac^3, a^2c^3\}.$$

Se tiene que $S_2 = \{e, c, c^2, c^3\}$ y $S_3 = \{e, a, a^2\}$, como puede comprobarse fácilmente. Observar que $G \approx S_2 \oplus S_3$.

★★ EJEMPLO C. En $(\mathbf{Z}_{10}, +)$ los elementos cuyo orden es una potencia de 2 son $S_2 = \{[0], [5]\}$ y los elementos cuyo orden es una potencia de 5 son $S_5 = \{[0], [2], [4], [6], [8]\}$. De nuevo observar que $\mathbf{Z}_{10} \approx S_2 \oplus S_5$.

El primer resultado importante de esta sección es que todo grupo abeliano de orden finito es isomorfo al producto directo de todos sus subgrupos de Sylow. Antes de dar la demostración de este resultado necesitamos demostrar dos lemas que son válidos para cualquier grupo.

Lema 5.3.1. Sea G un grupo y $x \in G$ un elemento de orden mn con $(m, n) = 1$. El elemento x puede escribirse de manera única como el producto de dos elementos y, z, que conmutan entre sí, con órdenes n y m, respectivamente. Además, y, z son "potencias" de x.

Demostración. Puesto que $1 = (m, n)$, existen $u, v \in \mathbf{Z}$ tal que $1 = um + vn$. Entonces, $x = x^{um+vn} = x^{um}x^{vn}$, y tomando $y = x^{um}$, $z = x^{vn}$, se tiene que y, z conmutan entre sí y ambos son "potencias" de x.

Sea $n' = \text{orden}(y)$, $m' = \text{orden}(z)$; puesto que $y^n = x^{umn} = e$ y $z^m = x^{vnm} = e$, tenemos que $n' \mid n$, $m' \mid m$. Puesto que $x = yz$, y ambos conmutan entre sí, se tiene que

$$x^{n'm'} = (yz)^{n'm'} = y^{n'm'}z^{n'm'} = e\,,$$

y por tanto $mn \mid m'n'$. Esto prueba que $n' = n$ y $m' = m$.

Para demostrar la unicidad, supongamos que podemos escribir $x = y_1z_1 = z_1y_1$; entonces y_1 y z_1 conmutan con x, ya que

$$xy_1 = y_1z_1y_1 = y_1x \quad \text{y} \quad xz_1 = z_1y_1z_1 = z_1x.$$

Por tanto y_1 y z_1 conmutan con y y z puesto que estos elementos son "potencias" de x.

Por otro lado, de $yz = x = y_1z_1$ deducimos $w = y_1^{-1}y = z_1z^{-1}$. Puesto que y e y_1 son elementos que conmutan y de orden n, y z y z_1 son elementos que conmutan y de orden m, se tiene que

$$w^n = (y_1^{-1})^n y^n = e, \qquad w^m = z_1^m (z_1^{-1})^m = e.$$

Puesto que (n, m) = 1, deducimos que w = e y por tanto $y = y_1$, $z = z_1$. ∎

Mediante sucesivas aplicaciones del lema 5.3.1 obtenemos

Lema 5.3.2. Sea G un grupo y $x \in G$ con $\text{orden}(x) = (p_1)^{n_1} (p_2)^{n_2} \dots (p_k)^{n_k}$, donde los p_j son primos distintos. El elemento x puede escribirse de manera única de la forma $x = x_1x_2 \dots x_k$ de manera que $x_ix_j = x_jx_i$ y cada x_i es una "potencia" de x de orden $(p_i)^{n_i}$.

Ya estamos en condiciones de demostrar el resultado anteriormente anunciado que nos permitirá afirmar que todo grupo abeliano de orden finito es isomorfo al producto directo de todos sus p–subgrupos de Sylow. Es una consecuencia del lema 5.3.2.

Teorema 5.3.3. Todo grupo abeliano de orden finito es isomorfo al producto directo de todos sus p-subgrupos de Sylow.

Demostración. En la demostración usaremos el teorema 5.2.2. Sea A un grupo abeliano con

$$|A| = n = (p_1)^{n_1} (p_2)^{n_2} \dots (p_k)^{n_k},$$

donde los p_j son primos distintos. Cada S_p es un subgrupo normal de A ya que A es abeliano. Además, si

$$a \in S_{p_i} \cap \left(\prod_{i \neq j} S_{p_i}\right)$$

su orden es $(p_j)^{m_j}$, con $0 \leq m_j \leq n_j$; por otro lado $a = \prod_{i \neq j} y_i$, y $\text{orden}(a) = \text{m.c.m.}\{\text{orden}(y_i)\} = \prod_{i \neq j} \text{orden}(y_i) = \prod_{i \neq j} (p_i)^{m_i}$. Puesto que $((p_j)^{m_j}, \prod_{i \neq j} (p_i)^{m_i}) = 1$, se tiene que $a = e$.

Finalmente, del lema 5.3.2 deducimos que $A = S_{p_1} S_{p_2} \dots S_{p_k}$. El teorema 5.2.2 de la sección 5.2 nos permite deducir el resultado deseado. ∎

En el resto de este capítulo utilizaremos la **notación aditiva**, ya que todos los grupos que consideraremos serán abelianos; en consecuencia el **elemento neutro será simbolizado por 0.**

Dado un grupo abeliano A diremos que $a_1, a_2, \ldots, a_r$ es un **sistema de generadores** de A si todo elemento de A puede escribirse de la forma $x = n_1a_1 + n_2a_2 + \ldots + n_ra_r$ con $n_j \in \mathbf{Z}$ para todo $j = 1, 2, \ldots, r$. Un sistema de generadores de A es una **base de A** si la expresión $x = n_1a_1 + n_2a_2 + \ldots + n_ra_r$ que expresa x como combinación de $a_1, a_2, \ldots, a_r$ es única; es decir, si escribiéramos $x = n'_1a_1 + n'_2a_2 + \ldots + n'_ra_r$ se tendría necesariamente $n_ja_j = n'_ja_j$ para todo $j = 1, 2, \ldots, r$.

★★ EJEMPLO D. En $(\mathbf{Z}_{16}, +)$, [1] es una base ya que todo elemento $[a] \in \mathbf{Z}_{16}$ puede escribirse de la forma [a] = a[1], donde $a \in \mathbf{Z}$ es un representante de la clase [a], y si [a] = a'[1] tendríamos a [1] =a'[1], y por tanto la representación es única en el sentido anteriormente descrito. Observar que de aquí no se puede deducir la igualdad de a y a'. En general, todo grupo cíclico tiene a uno de sus generadores como base.

★★ EJEMPLO E. En $(\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2, +)$, a = ([1], [0], [0]), b = ([0], [1], [0]) y c = ([0], [0], [1]) forman un sistema de generadores ya que si ([k], [n], [m]) es un elemento de $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$,

$$([k], [n], [m]) = ka + nb + mc.$$

Es, además, una base de este grupo ya que si

$$([k], [n], [m]) = k'a + n'b + m'c,$$

se tendría ([k], [n], [m]) = (k'[1], n'[1], m'[1]) y por tanto [k] = k'[1], [n] = n'[1] y [m] = = m'[1] de donde se deduce ka = (k[1], [0], [0]) = (k'[1], [0], [0]) = k'a y nb=n'b, mc=m'c de manera similar.

Cuando se tiene una base en un grupo abeliano, éste es isomorfo a una suma directa de los subgrupos generados por los elementos de la base. A demostrar esto nos dedicaremos en los dos próximos lemas.

Lema 5.3.4. Sea A un grupo abeliano y $\{a_1, \ldots, a_r\}$ un sistema de generadores de A. Las siguientes condiciones son equivalentes:

1) $\{a_1, a_2, \ldots, a_r\}$ es una base de A.
2) Si existen $n_1, n_2, \ldots, n_r \in \mathbf{Z}$ tal que $n_1a_1 + n_2a_2 + \ldots + n_ra_r = 0$, se debe tener $n_ja_j = 0$ para todo $j = 1, 2, \ldots, r$.

Demostración. Comenzaremos demostrando que 1) implica 2). Supongamos, por tanto, que $\{a_1, a_2, \ldots, a_r\}$ es una base de A y que $n_1a_1 + n_2a_2 + \ldots + n_ra_r = 0$. Como podemos escribir

$$n_1a_1 + n_2a_2 + \ldots + n_ra_r = 0a_1 + 0a_2 + \ldots + 0a_r,$$

de la unicidad de la descomposición se deduce $n_ja_j = 0$ para todo $j = 1, 2, \ldots, r$.

Para demostrar que 2) implica 1), supongamos que tenemos dos descomposiciones de x de la forma

$$n_1a_1 + n_2a_2 + \ldots + n_ra_r = x = n'_1a_1 + n'_2a_2 + \ldots + n'_ra_r.$$

Por tanto

$$(n_1 - n'_1)a_1 + (n_2 - n'_2)a_2 + \ldots + (n_r - n'_r)a_r = 0,$$

y de la hipótesis deducimos $(n_j - n'_j)a_j = 0$ para todo $j = 1, 2, \ldots, r$, que es lo que queríamos demostrar. ■

Lema 5.3.5. Si $\{a_1, a_2, \ldots, a_r\}$ es una base de un grupo abeliano A, se tiene que A es isomorfo a la suma directa $\langle a_1\rangle \oplus \langle a_2\rangle \oplus \ldots \oplus \langle a_r\rangle$ donde $\langle a_j\rangle$ es el grupo cíclico generado por a_j.

Demostración. En esta demostración usaremos el teorema 5.2.2. Cada $\langle a_j\rangle$ es normal en A puesto que A es abeliano. Además, puesto que $\{a_1, a_2, \ldots, a_r\}$ es un sistema de generadores de A, $A = \langle a_1\rangle + \langle a_2\rangle + \ldots + \langle a_r\rangle$. Finalmente, si

$$x \in \langle a_j\rangle \cap \left(\prod_{i \neq j} \langle a_i\rangle\right)$$

tenemos

$$x = n_j a_j = \sum_{i \neq j} n_i a_i ;$$

por tanto $x = 0a_1 + \ldots + n_j a_j + \ldots + 0a_r = n_1 a_1 + \ldots + 0a_j + \ldots + n_r a_r$, y puesto que la representación de x es única se tiene que $x = n_j a_j = 0$. El teorema 5.2.2 de la sección 5.2 termina la demostración. ■

★★ EJEMPLO F. Sea $V = \{e, a, b, c\}$ el grupo abeliano caracterizado por las relaciones $2a = 2b = e$ y $a + b = c$. El subconjunto $\{a, b\}$ es un sistema de generadores de V. Es, además, una base; por ejemplo, si $c = na + mb$, tendríamos $a + b = na + mb$, de donde se deduce que n y m tienen que ser impares estudiando los cuatro casos posibles; como $2a = 2b = e$, si n y m son impares $na = a$ y $mb = b$.

El lema 5.3.5 nos permite deducir $V \approx \langle a\rangle \oplus \langle b\rangle$ y como $\langle a\rangle \approx \mathbf{Z}_2$ y $\langle b\rangle \approx \mathbf{Z}_2$ se tiene $V \approx \mathbf{Z}_2 \oplus \mathbf{Z}_2$, es decir, V es isomorfo al grupo de Klein.

Estamos en condiciones de demostrar el resultado principal de esta sección acerca de la estructura de los grupos abelianos finitos.

Teorema 5.3.6. (Teorema de estructura para grupos abelianos finitos.) Todo grupo abeliano finito es isomorfo a una suma directa de grupos cíclicos de órdenes potencias de primos.

Demostración. Por el teorema 5.3.3 y el lema 5.3.5, basta demostrar que cualquier p – subgrupo de Sylow S_p tiene una base.

Sea pues $A = S_p$ un grupo abeliano con la propiedad de que todos sus elementos tienen un orden que es una potencia de un número primo p.

Para tener una base de A comenzamos eligiendo un elemento a_1 de A de orden p^{m_1} máximo. Sea $A_1 = \langle a_1 \rangle$. Si $A_1 = A$, $\{a_1\}$ es una base de A y hemos terminado la demostración.

Supongamos, entonces, que $A_1 \subseteq A$ y A_1 es distinto de A; procedamos por inducción para elegir el resto de los elementos. Aceptemos, por tanto, que hemos encontrado k elementos a_1, a_2, ..., a_k de órdenes p^{m_1}, p^{m_2}, ..., p^{m_k} tales que

1) $m_1 \geq m_2 \geq \ldots \geq m_k$ y todo elemento de A que no está en $A_k = \langle a_1 \rangle + \langle a_2 \rangle + \ldots + \langle a_k \rangle$ tiene orden p^t con $t \leq m_k$.
2) $\{a_1, a_2, \ldots, a_k\}$ es una base de A_k.

Si $A_k \subseteq A$ y A_k es distinto de A, tomemos $b \in A - A_k$; algún múltiplo de b está contenido en A_k, ya que si p^t es el orden de b, $p^t b = 0 \in A_k$. Sea r el menor entero positivo tal que $rb \in A_k$. Demostraremos que r es una potencia de p. En efecto, dividiendo p^t entre r se tiene $p^t = cr + r'$ con $0 \leq r' < r$. Por tanto $r'b = p^t b - crb \in A_k$. Puesto que r es el menor entero positivo tal que $rb \in A_k$, hemos de tener $r' = 0$. Por tanto, r es un factor de p^t, digamos $r = p^{m_{k+1}}$ y puesto que $m_{k+1} \leq t$ se tiene $m_1 \geq m_2 \geq \ldots \geq m_k \geq m_{k+1}$.

Puesto que $rb \in A_k$ tenemos que

$$r\,b = \sum_{i=1}^{k} n_i a_i .$$

Demostraremos a continuación que cada n_i es divisible entre r; multiplicando la igualdad anterior por $p^t/r = p^{t-m_{k+1}}$ se tiene

$$p^t b = 0 = \sum_{i=1}^{k} n_i \ (p^t/r) a_i .$$

De esta igualdad y 2), deducimos $(n_i p^t/r)a_i = 0$, y por tanto $n_i p^t/r$ es un múltiplo de p^{m_i}, $i = 1, 2, \ldots, k$; es decir

$$n_i p^t/r = n'_i p^{m_i}, \qquad n'_i \in \mathbb{Z}^+, \qquad i = 1, 2, \ldots, k.$$

Por tanto $n_i = r(n'_i p^{m_i - t}) = r\, n''_i$, en donde n''_i es un entero positivo ya que $m_i \geq t$.

Definimos

$$a_{k+1} = b - \sum_{i=1}^{k} n''_i a_i .$$

Tenemos que $ra_{k+1} = rb - \sum_{i=1}^{k} rn''_i a_i = rb - \sum_{i=1}^{k} n_i a_i = 0$, y por tanto el orden de a_{k+1} divide a r. Por otro lado cualquier ecuación de la forma $sa_{k+1} = 0$ implica $sb \in A_k$, y por tanto $r \leq s$; así pues $r = \text{orden}(a_{k+1}) = p^{m_{k+1}}$.

Finalmente hemos de probar que la igualdad

$$0 = \sum_{i=1}^{k+1} c_i a_i \qquad (*)$$

implica $c_i a_i = 0$, $i = 1, 2, \ldots, k+1$. De esta igualdad deducimos que $c_{k+1} a_{k+1} \in A_k$, y de la definición de a_{k+1} se deduce que $c_{k+1} b \in A_k$.

Dividiendo c_{k+1} entre r, se tiene $c_{k+1} = cr + r''$, con $0 \leq r'' < r$, y por tanto $r'' = 0$ ya que $r''b = c_{k+1} b - crb \in A_k$. Así pues c_{k+1} es un múltiplo de $r = p^{m_{k+1}}$ y podemos escribir

$$c_{k+1} = p^{m_{k+1}} c'_{k+1}.$$

Por tanto, $c_{k+1} a_{k+1} = 0$ y la igualdad (*) se transforma en $0 = \sum_{i=1}^{k} c_i a_i$; de 2) deducimos que $c_i a_i = 0$, $i = 1, 2, \ldots, k$.

Por tanto, $\{a_1, \ldots, a_{k+1}\}$ es una base de $A_{k+1} = \langle a_1 \rangle + \ldots + \langle a_k \rangle + \langle a_{k+1} \rangle = \langle a_1 \rangle + \ldots + \langle a_k \rangle + \langle b \rangle$. Puesto que S_p es un grupo finito, este procedimiento nos permite encontrar una base de S_p después de un número finito de pasos. Esto completa la demostración. ∎

★★ EJEMPLO G. Sea A un grupo abeliano generado por los elementos a, b y c tal que $a^2 = e$, $b^3 = c^3 = e$. El grupo A posee 18 elementos y puesto que $18 = 2 \cdot 3^2$ podemos encontrar S_2 y S_3. Fácilmente se comprueba que

$$S_2 = \langle a \rangle \approx \mathbf{Z}_2$$

$$S_3 = \{e, b, b^2, c, c^2, bc, b^2c, bc^2, b^2c^2\} = \langle b \rangle \oplus \langle c \rangle \approx \mathbf{Z}_3 \oplus \mathbf{Z}_3.$$

Si el p_i – subgrupo de Sylow S_{p_i} cumple $S_{p_i} = \langle a_{i1} \rangle + \langle a_{i2} \rangle + \ldots + \langle a_{is} \rangle$ con los a_{ij} de orden $p^{m_{ij}}$, se tiene que

$$|S_{p_i}| = p_i^{m_{i1}} p_i^{m_{i2}} \ldots p_i^{m_{is}} = p_i^{m_{i1} + m_{i2} + \ldots + m_{is}}$$

Si

$$|A| = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$$

es la descomposición de A en factores primos, se tiene que

$$p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k} = |A| = |S_{p_1}| \, |S_{p_2}| \ldots |S_{p_k}| =$$

$$= p_1^{m_{11} + m_{12} + \ldots + m_{1s}} p_2^{m_{21} + m_{22} + \ldots + m_{2s}} \ldots p_k^{m_{k1} + m_{k2} + \ldots + m_{ks}}.$$

De la unicidad de la descomposición de un número en factores primos se deduce

$$m_j = m_{j1} + m_{j2} + \ldots + m_{js}, \qquad j = 1, 2, \ldots, k,$$

con lo que se tiene el siguiente resultado:

Corolario 5.3.7. Si A es un grupo abeliano finito con $|A| = p^r m$ y $(p, m) = 1$, el p-subgrupo de Sylow de A, S_p, posee p^r elementos.

Puesto que todos los grupos cíclicos de un orden dado m son isomorfos a $(\mathbf{Z}_m, +)$ del teorema 5.3.6 se deduce que todo grupo abeliano finito es isomorfo a una suma directa de grupos de la forma $(\mathbf{Z}_m, +)$ donde m es una potencia de un número primo.

Esto ayudará al lector a demostrar los siguiente resultados (véase ejercicio 3). El primero de ellos es el **teorema de Cauchy para grupos abelianos finitos** que ya fue demostrado en 5.1.1 y que ahora se puede demostrar más fácilmente. El segundo demuestra que el recíproco del teorema de Lagrange es cierto para grupos abelianos finitos.

Corolario 5.3.8.(Teorema de Cauchy para grupos abelianos finitos). Todo grupo abeliano de orden n posee un elemento de orden p para todo primo p que divide a n.

Corolario 5.3.9. Si A es un grupo abeliano de orden n y r un divisor de n, A posee un subgrupo de orden r.

EJERCICIOS 5.3

1. Dar un ejemplo de un grupo no abeliano en el que S_p no sea subgrupo.
2. En $(\mathbf{Z}_{15}, +)$ y en $(\mathbf{Z}_{12}, +)$ encontrar todos sus p-subgrupos.
3. Demostrar los corolarios 5.3.8 y 5.3.9 enunciados al final de esta sección.
4. Demostrar que el grupo $A = \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ posee siete subgrupos de orden 2.
5. Encontrar todos los automorfismos de $\mathbf{Z}_{2p}$ con p primo impar.
6. Sea $G \approx A \oplus B$, donde A y B son cíclicos de orden 2. Encontrar C y D subgrupos de G tales que $G \approx C \oplus D$, con C y D cíclicos de orden 2 y $C \neq A$, $D \neq B$.
7. Escribir los grupos abelianos dados por las relaciones siguientes como suma directa de grupos cíclicos

   i) $13A = 0, 5B = 0$
   ii) $15A = 0, 10B = 0, 4C = 0$
   iii) $8A = 0, 10B = 0, 6C = 0$

   (Los grupos anteriores han sido escritos con notación aditiva.)
8. Encontrar todos los subgrupos de orden p^2 del grupo $\mathbf{Z}_p \oplus \mathbf{Z}_{p^2}$, donde p es un número primo.

5.4. INVARIANTES Y CLASIFICACIÓN DE LOS GRUPOS ABELIANOS FINITOS

En esta sección demostraremos que la descomposición de todo grupo abeliano de orden finito en una suma directa de grupos cíclicos de órdenes potencias de un primo es única salvo isomorfismos. Esto nos permitirá definir los invariantes de un grupo abeliano finito y poder determinar la lista completa, salvo isomorfismos, de todos los grupos abelianos finitos de cualquier orden. Puesto que los subgrupos de Sylow de un grupo abeliano quedan unívocamente determinados por su definición, basta demostrar la unicidad para grupos abelianos con las características de un subgrupo de Sylow. Puesto que los subgrupos de Sylow tienen orden p^t, con p primo (ver corolario 5.3.7 de la sección anterior), basta demostrar la unicidad para grupos abelianos cuyo orden es una potencia de un número primo. Un grupo de orden p^t, con p primo, se denomina un **p-grupo**.

Teorema 5.4.1. (Unicidad). Si A es un p-grupo abeliano que puede escribirse como suma directa de grupos cíclicos de dos formas diferentes

$$A \approx A_1 \oplus A_2 \oplus \ldots \oplus A_r,$$
$$A \approx B_1 \oplus B_2 \oplus \ldots \oplus B_s,$$

con $|A_j| = p^{e_j}$, $j = 1, 2, \ldots, r$, $|B_i| = p^{f_i}$, $i = 1, 2, \ldots, s$ y

$$e_1 \geq e_2 \geq \ldots \geq e_r, \qquad f_1 \geq f_2 \geq \ldots \geq f_s,$$

se tiene que $r = s$ y $e_j = f_j$ para todo $j = 1, 2, \ldots, r$.

Demostración. Sea $|A| = p^t$; si $t=1$ el resultado es cierto puesto que A es cíclico. Para $t > 1$ procedemos por inducción. Supongamos que el resultado es cierto para todo p-grupo de orden p^k con $k < t$.

Sea $pA = \{py: y \in A\}$ que es un subgrupo de A. Si $pA = \{e\}$, todo elemento (salvo e) de A es de orden p y por tanto $A_j \approx (\mathbb{Z}_p, +)$, $j = 1, 2, \ldots, r$, y $B_i \approx (\mathbb{Z}_p, +)$, $i = 1, 2, \ldots, s$; en este caso $p^t = |A| = p^r = p^s$, de donde se deduce el resultado.

Si $pA \neq \{e\}$, demostraremos que

$$pA \approx \langle pa_1 \rangle \oplus \langle pa_2 \rangle \oplus \ldots \oplus \langle pa_r \rangle$$

y

$$pA \approx \langle pb_1 \rangle \oplus \langle pb_2 \rangle \oplus \ldots \oplus \langle pb_s \rangle$$

donde a_j es un generador del grupo cíclico A_j y b_i es un generador del grupo cíclico B_i.

Si $px \in pA$, $x \in A$ y por tanto $x = \sum_{i=1}^{r} n_i a_i$; entonces $px = \sum_{i=1}^{r} n_i (pa_i)$; además, si $\sum_{i=1}^{r} n_i (pa_i) = 0$, se tiene que $n_i pa_i = 0$ y por tanto $\{pa_i\}$ es una base de pA. El resultado se obtiene aplicando el lema 5.3.5 de la sección anterior. Similarmente se demuestra el segundo isomorfismo.

Por tanto

$$|pA| = p^{e_1 - 1}p^{e_2 - 1} \dots p^{e_r - 1} = p^{t-r}$$

y

$$|pA| = p^{f_1 - 1}p^{f_2 - 1} \dots p^{f_r - 1} = p^{t-s}.$$

Puesto que $r \geq 1$, por la hipótesis de inducción $r = s$ y $e_1 - 1 = f_1 - 1$, $e_2 - 1 = f_2 - 1$, ..., $e_r - 1 = f_r - 1$, de donde se deduce el resultado deseado. ■

Los números $(p^{e_1}, p^{e_2}, \dots, p^{e_n})$ se denominan **invariantes** del p-grupo A. Del teorema anterior se deduce que dos p-grupos con invariantes distintos no pueden ser isomorfos. Para un grupo abeliano finito A se denominan **invariantes** a los invariantes de cada uno de sus subgrupos de Sylow. De nuevo dos grupos abelianos finitos con invariantes distintos no pueden ser isomorfos.

★★ EJEMPLO A. Los posibles invariantes de un grupo abeliano con p^4 elementos y p primo son

$$(p, p, p, p), \quad (p^2, p, p), \quad (p^2, p^2), \quad (p^3, p), \quad (p^4)$$

y por tanto existen únicamente, salvo isomorfismos, 5 grupos abelianos de p^4 elementos. Estos son isomorfos a uno y sólo uno de los siguientes grupos:

$$\mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p, \quad \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p \oplus \mathbf{Z}_p, \quad \mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}, \quad \mathbf{Z}_{p^3} \oplus \mathbf{Z}_p, \quad \mathbf{Z}_{p^4}.$$

★★ EJEMPLO B. Para averiguar cuántos grupos abelianos existen de 360 elementos, descomponemos 360 en factores primos: $360 = 2^3 \cdot 3^2 \cdot 5$. Como $|S_2| = 2^3$ sus posibles invariantes son

$$(2, 2, 2), \quad (2^2, 2), \quad (2^3)$$

y por tanto existen tres grupos abelianos distintos de 2^3 elementos.

Similarmente, puesto que $|S_3| = 3^2$, tenemos dos grupos abelianos esencialmente distintos de 3^2 elementos.

Finalmente, sólo existe un grupo abeliano de orden 5 salvo isomorfismos.

Combinando todos los posibles grupos anteriores, deducimos que, salvo isomorfismos, solamente existen $3 \cdot 2 \cdot 1 = 6$ grupos abelianos de 360 elementos.

La lista completa, salvo isomorfismos, es

$$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5, \quad \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_5$$
$$\mathbf{Z}_4 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5, \quad \mathbf{Z}_4 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_5$$
$$\mathbf{Z}_8 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5, \quad \mathbf{Z}_8 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_5$$

★★ EJEMPLO C. ¿Está el grupo $\mathbf{Z}_{360}$ incluido en la lista dada en el ejemplo B? Se tiene que $\mathbf{Z}_{360} \approx \mathbf{Z}_8 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_5$ ya que se recordará que $\mathbf{Z}_{mn}$ es isomorfo a $\mathbf{Z}_m \oplus \mathbf{Z}_n$ si y sólo si $(m, n) = 1$. (Véase el ejercicio 9 del final de la sección 4.7.)

El grupo $\mathbf{Z}_{60} \oplus \mathbf{Z}_6$, de 360 elementos, está incluido también en la lista del ejemplo B, ya que

$$\mathbf{Z}_{60} \oplus \mathbf{Z}_6 \approx \mathbf{Z}_4 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \approx \mathbf{Z}_4 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5 .$$

★★ EJEMPLO D. El grupo abeliano $(\mathbf{Z}^*_{13}, \cdot)$ tiene 12 elementos y por tanto es isomorfo a $\mathbf{Z}_4 \oplus \mathbf{Z}_3$ o $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$. Para averiguar a cuál de ellos es isomorfo, estudiamos el orden de sus elementos. $\mathbf{Z}_4 \oplus \mathbf{Z}_3$ posee un elemento de orden 4, mientras que $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$ no posee ningún elemento de orden 4.

Puesto que en $(\mathbf{Z}^*_{13}, \cdot)$, $[5]^4 = [5]^2 \cdot [5]^2 = ([-1])\,([-1]) = [1]$, este grupo no puede ser isomorfo a $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3$. Por tanto

$$(\mathbf{Z}^*_{13}, \cdot) \approx \mathbf{Z}_4 \oplus \mathbf{Z}_3 \approx \mathbf{Z}_{12}.$$

Ahora podemos hacer una tabla de todos los grupos abelianos que existen, salvo isomorfismos. En la tabla siguiente se indican todos los grupos abelianos finitos de orden menor o igual que 16.

n	Grupos abelianos finitos de orden n
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$, $\mathbf{Z}_2 \times \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_6 \approx \mathbf{Z}_2 \times \mathbf{Z}_3$
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$, $\mathbf{Z}_4 \times \mathbf{Z}_2$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$
9	$\mathbf{Z}_9$, $\mathbf{Z}_3 \times \mathbf{Z}_3$
10	$\mathbf{Z}_{10} \approx \mathbf{Z}_2 \times \mathbf{Z}_5$
11	$\mathbf{Z}_{11}$
12	$\mathbf{Z}_{12} \approx \mathbf{Z}_4 \times \mathbf{Z}_3$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$
13	$\mathbf{Z}_{13}$
14	$\mathbf{Z}_{14} \approx \mathbf{Z}_2 \times \mathbf{Z}_7$
15	$\mathbf{Z}_{15} \approx \mathbf{Z}_3 \times \mathbf{Z}_5$
16	$\mathbf{Z}_{16}$, $\mathbf{Z}_8 \times \mathbf{Z}_2$, $\mathbf{Z}_4 \times \mathbf{Z}_4$, $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$

EJERCICIOS 5.4

1. Encontrar los invariantes del grupo abeliano generado por los elementos a, b y c tal que $6a = 0$, $4b = 0$, $12c = 0$.

2. ¿Cuántos grupos abelianos existen de 10^6 elementos?

3. Dar una lista completa, salvo isomorfismos, de todos los grupos abelianos de los siguientes órdenes: i) 48, ii) 108, iii) 3528, iv) 625.

4. Demostrar que si el orden de un grupo abeliano no es divisible por un cuadrado, el grupo tiene que ser cíclico.

5. Sea $I(\mathbb{Z}_n^*)$ el conjunto de todos los $[a] \in \mathbb{Z}_n^*$ tales que $[a]$ posee inverso en $(\mathbb{Z}_n^*, \cdot)$. En el problema 9 de la sección 4.2 se pidió demostrar que $(I(\mathbb{Z}_n^*), \cdot)$ es un grupo. Es claramente abeliano.

   i) Encontrar los invariantes de $I(\mathbb{Z}_8^*)$ y de $I(\mathbb{Z}_{16}^*)$
   ii) Probar que los invariantes de $I(\mathbb{Z}_{24}^*)$ son (2, 2, 2)

5.5. TEOREMAS DE SYLOW

Los grupos abelianos finitos han sido caracterizados de manera precisa en las secciones 5.3 y 5.4 en donde se estableció que todos ellos son producto directo de grupos cíclicos. Se conoce, por tanto, su estructura y cuántos hay no isomorfos de un orden determinado. Este problema es más complicado cuando el grupo no es abeliano. Los teoremas de Sylow son algunos de los resultados sobre este problema. Comenzaremos con un resultado que se llama la **"ecuación de las clases conjugadas"** y que jugará un papel esencial en la demostración de los teoremas de Sylow.

Definición 5.5.1. Dado un grupo G, dos elementos x e y de G se dicen **conjugados** si existe $g \in G$ tal que $g\,x\,g^{-1} = y$.

Dado un elemento x de G deseamos contar cuántos elementos de G son conjugados con x; este número está relacionado con el **centralizador** de x que fue expuesto en el ejercicio 10 de la sección 4.3 y cuya definición repetimos a continuación.

Definición 5.5.2. Si x es un elemento de un grupo G, el **centralizador de x en G** es $C_G(x) = \{g \in G: gx = xg\}$.

En el ejercicio que mencionamos antes de dar esta definición se pidió demostrar que **$C_G(x)$ es un subgrupo de G, cualquiera que sea x.** Si no se hizo antes, es el momento de ponerse a trabajar para demostrarlo. (¡No es difícil!)

★★ EJEMPLO A. Si G es un grupo **abeliano** y $x \in G$, el único elemento conjugado con x es él mismo, ya que para todo $g \in G$, $gxg^{-1} = xgg^{-1} = x$. Como todo elemento conmuta con x, $C_G(x) = G$ para todo $x \in G$.

★★ EJEMPLO B. Sea G un grupo y $x \in Z(G)$, el centro de G. Entonces x conmuta con todos los elementos de G y por tanto $C_G(x) = G$; además x es el único elemento conjugado con él mismo.

★★ EJEMPLO C. Sea $S_3 = \{I, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ el grupo de las permutaciones de 3 elementos, que se definió en la sección 3.4 del capítulo 3. Calcularemos los conjugados de cada uno de sus elementos, su centralizador y el índice del centralizador en el grupo, entendiendo éste como el número de clases de equivalencia por la izquierda que hay en $G/C_G(x)$.

x	Conjugados	$C_{S_3}(x)$	$[S_3 : C_{S_3}(x)]$
I	I	S_3	1
α	α, α^2	$<\alpha>=\{I, \alpha, \alpha^2\}$	2
α^2	α, α^2	$<\alpha> = \{I, \alpha, \alpha^2\}$	2
β	$\beta, \alpha\beta, \alpha^2\beta$	$<\beta> = \{I, \beta\}$	3
$\alpha\beta$	$\beta, \alpha\beta, \alpha^2\beta$	$<\alpha\beta> = \{I, \alpha\beta\}$	3
$\alpha^2\beta$	$\beta, \alpha\beta, \alpha^2\beta$	$<\alpha^2\beta> = \{I, \alpha^2\beta\}$	3

El lector debe comprobar con cuidado esta tabla. Obsérvese que el número de conjugados de x coincide con el índice del centralizador de x en S_3.

★★ EJEMPLO D. Ya conocemos varios grupos de 8 elementos. $\mathbf{Z}_8$, $\mathbf{Z}_4 \oplus \mathbf{Z}_2$ y $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ son, salvo isomorfismos, los únicos grupos abelianos que existen de 8 elementos; además, el grupo de las simetrías de un cuadrado, D_8, tiene también 8 elementos y no es abeliano. He aquí otro grupo de 8 elementos. Se llama el grupo de los **cuaterniones** y se simboliza por Q_8. Está formado por los elementos

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\},$$

sometidos a las relaciones

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j.$$

Además, 1 es el elemento neutro y la operación que se considera en Q_8 es la multiplicación.

No es difícil, aunque pueda resultar tedioso, comprobar la asociatividad de esta operación. El resto de los axiomas de grupo son fáciles de comprobar: 1 es el neutro, el inverso de –1 es –1, i y –i son inversos entre sí, y lo mismo sucede con j, –j y k, –k.

El lector puede hacer la tabla de este grupo (ejercicio 2 al final de esta sección). Se comprueba fácilmente que este grupo **no es abeliano** ($ij \neq ji$) y que tiene un elemento de orden 2, (–1), y 6 elementos de orden 4: i, –i, j, –j, k, –k.

El retículo de sus subgrupos es el que se muestra en la ilustración de la derecha, donde

$$\begin{aligned} \langle -1\rangle &= \{1, -1\} \\ \langle i\rangle = \langle -i\rangle &= \{1, i, -1, -i\} \\ \langle j\rangle = \langle -j\rangle &= \{1, j, -1, -j\} \\ \langle k\rangle = \langle -k\rangle &= \{1, k, -1, -k\}. \end{aligned}$$

Mirando los retículos se observa que Q_8 no puede ser isomorfo a D_8 y por tanto es un nuevo elemento para nuestra colección de grupos.

Se puede hacer con este grupo un cuadro similar al del ejemplo C:

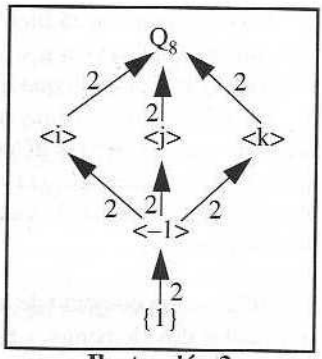


Ilustración 3
Retículo de Q_8

x	Conjugados	$C_{Q_8}(x)$	$[Q_8 : C_{Q_8}(x)]$
1	1	Q_8	1
–1	–1	Q_8	1
i	i, –i	<i>	2
–i	i, –i	<i>	2
j	j, –j	<j>	2
–j	j, –j	<j>	2
k	k, –k	<k>	2
–k	k, –k,	<k>	2

En los dos últimos ejemplos que hemos realizado el número de conjugados de x coincide con el índice del centralizador de x en el grupo. Este es el resultado que se demuestra a continuación.

Proposición 5.5.3. Sea G un grupo y $x \in G$; el número de conjugados de x coincide con el índice del centralizador de x en G.

Demostración. Sea $\zeta(x)$ el conjunto de los conjugados de x, es decir, $\zeta(x) = \{gxg^{-1}: g \in G\}$. El índice del centralizador de x en G, $[G: C_G(x)]$, es el número de clases de equivalencia por la izquierda de $C_G(x)$ en G, es decir $|G/C_G(x)|$. Basta, por tanto, establecer una aplicación biyectiva entre $\zeta(x)$ y $G/C_G(x)$.

Definir $f: \zeta(x) \to G/C_G(x)$ mediante

$$f(gxg^{-1}) = gC_G(x).$$

Esta aplicación está bien definida: si $gxg^{-1} = g_1xg_1^{-1}$ hemos de mostrar la igualdad de los conjuntos $gC_G(x) = g_1C_G(x)$. De $gxg^{-1} = g_1xg_1^{-1}$ deducimos $(g_1^{-1}g)x = x(g_1^{-1}g)$ y por tanto $g_1^{-1}g \in C_G(x)$, lo que implica la igualdad $gC_G(x) = g_1C_G(x)$.

La aplicación es suprayectiva ya que dada la clase $gC_G(x)$ basta tomar $gxg^{-1} \in \zeta(x)$ y observar que $f(gxg^{-1}) = gC_G(x)$. Para probar que es inyectiva supongamos que $f(gxg^{-1}) = f(g_1xg_1^{-1})$, es decir, $gC_G(x) = g_1C_G(x)$; por tanto $g_1^{-1}g \in C_G(x)$, de donde se deduce $(g_1^{-1}g)x = x(g_1^{-1}g)$; esta igualdad es equivalente a $gxg^{-1} = g_1xg_1^{-1}$. Esto termina la demostración de la proposición 5.5.3. ■

Si $\zeta(x)$ es el conjunto de los elementos conjugados de x, en los ejemplos C y D se observa que, dados dos elementos x e y de G, o bien $\zeta(x) = \zeta(y)$ o $\zeta(x) \cap \zeta(y) = \emptyset$. Cada uno de estos conjuntos $\zeta(x)$ se dice que es una **clase conjugada** y demostraremos en el siguiente resultado que las clases conjugadas establecen una partición de G.

Proposición 5.5.4. Dado un grupo G, las clases conjugadas de dos elementos cualesquiera de G o bien son iguales o bien no tienen elementos en común. Además, G es la unión de todas sus clases conjugadas.

Demostración. Sean x e y elementos de G y supongamos que $\zeta(x) \cap \zeta(y) \neq \emptyset$; tomar $z \in \zeta(x) \cap \zeta(y)$, de manera que podamos encontrar $g_1, g_2 \in G$ tales que $z = g_1xg_1^{-1}$ y $z = g_2yg_2^{-1}$. Por tanto $(g_2^{-1}g_1)x = y(g_2^{-1}g_1)$. Queremos demostrar la igualdad $\zeta(x) = \zeta(y)$. Sea $t \in \zeta(x)$, de manera que existe $g \in G$ tal que $t = gxg^{-1}$; por tanto

$$t = gxg^{-1} = g(g_2^{-1}g_1)^{-1} \text{ y } (g_2^{-1}g_1)g^{-1} = (gg_1^{-1}g_2)y(gg_1^{-1}g_2)^{-1}.$$

Esto muestra que $t \in \zeta(y)$ y por tanto se tiene la inclusión $\zeta(x) \subset \zeta(y)$. Intercambiando los papeles de x y de y en la demostración anterior se deduce la igualdad de las clases conjugadas.

Finalmente, si $x \in G$, $x \in \zeta(x)$ ya que $x = exe^{-1}$, donde e es el neutro de G, y en consecuencia la unión de todas las clases conjugadas debe ser G. ■

Tenemos ya suficientes herramientas para poder demostrar la ecuación de las clases conjugadas, que será fundamental en la demostración de los teoremas de Sylow.

Teorema 5.5.5. (Ecuación de las clases conjugadas). Sea G un grupo finito y sean $x_1, x_2, \ldots, x_r$ representantes de distintas clases conjugadas de G que no sean elementos del centro de G. Entonces

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$$

donde Z(G) es el centro de G y $C_G(x_i)$ es el centralizador de x_i en G, $i = 1, 2, \ldots, r$.

Demostración. En el ejemplo B se ha observado que si $x \in Z(G)$, $\zeta(x) = \{x\}$; sea $Z(G) = \{e, z_2, \ldots, z_m\}$ y sean $\zeta_1, \zeta_2, \ldots, \zeta_r$ las clases conjugadas de G no contenidas en el centro de G; elegir $x_i \in \zeta_i$, $i = 1, 2, \ldots, r$. Todas las clases conjugadas de G son

$$\{e\}, \{z_2\}, \ldots, \{z_m\}, \zeta_1, \zeta_2, \ldots, \zeta_r$$

Puesto que estas clases forman una partición de G, de acuerdo con la proposición 5.5.4,

$$|G| = \sum_{1}^{m} 1 + \sum_{i=1}^{r} |\zeta_i| = |Z(G)| + \sum_{i=1}^{r} [G: C_G(x_i)]$$

ya que $|\zeta_i| = [G: C_G(x_i)]$ según la proposición 5.5.3. ■

★★ EJEMPLO E. En el grupo S_3 (véase ejemplo C de esta misma sección) el centro tiene un sólo elemento, la identidad, y si tomamos α y β como representantes de las dos clases conjugadas que existen, la ecuación de clases se cumple ya que $|Z(S_3)| + [S_3: \langle\alpha\rangle] + [S_3: \langle\beta\rangle] = 1 + 2 + 3 = 6 = |S_3|$.

★★ EJEMPLO F. En el grupo Q_8 del ejemplo D de esta misma sección se tiene $Z(G) = \{1, -1\}$ y hay tres clases de equivalencia diferentes $\langle i\rangle$, $\langle j\rangle$ y $\langle k\rangle$. Entonces

$$|Z(G)| + [G: \langle i\rangle] + [G: \langle j\rangle] + [G: \langle k\rangle] = 2 + 2 + 2 + 2 = 8 = |Q_8|.$$

Antes de adentrarnos en la exposición de los teoremas de Sylow mostraremos la potencia del teorema que acabamos de probar deduciendo resultados acerca de la estructura de algunos grupos.

Corolario 5.5.6. Si p es primo y P es un grupo con p^n elementos, $n \geq 1$, P tiene un centro no trivial, es decir $Z(P) \neq \{e\}$.

Demostración. La ecuación de las clases conjugadas (teorema 5.5.5) es

$$|P| = |Z(P)| + \sum_{i=1}^{r} [P: C_P(x_i)]$$

donde los x_i son representantes de distintas clases conjugadas no contenidas en el centro de P. Como P tiene p^n elementos y $C_P(x_i)$ es distinto de P, ya que x_i no está en el centro de P, cada $[P : C_P(x_i)]$ es un múltiplo de p. Por tanto, $|Z(P)|$ tiene que ser también un múltiplo de p, lo que muestra que $Z(P) \neq \{e\}$. ■

Corolario 5.5.7. Todo grupo P de orden p^2, con p primo, es abeliano. En particular P es isomorfo a $\mathbf{Z}_{p^2}$ o a $\mathbf{Z}_p \oplus \mathbf{Z}_p$.

Demostración. Por el corolario 5.5.6, $Z(P) \neq \{e\}$; por tanto $Z(P) = P$ o $Z(P)$ tiene p elementos. Si $Z(P)$ tuviera p elementos, P no sería abeliano, pero $P/Z(P)$ sería cíclico, ya que tiene p elementos y p es primo; esto contradice el ejercicio 7 de la sección 4.6. Por tanto, $Z(P) = P$

y P tiene que ser abeliano. La última parte del corolario se deduce de los resultados de la sección 5.4 sobre la estructura de los grupos abelianos finitos. ■

★★ EJEMPLO G. Para grupos de orden $4 = 2^2$ el corolario anterior asegura que todos ellos deben ser abelianos y que, salvo isomorfismos, éstos son $\mathbf{Z}_4$ y $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. Este es un resultado ya conocido.

Es menos conocido cuando se aplica a grupos de $9 = 3^2$ elementos. En este caso podemos asegurar que solamente hay dos grupos de 9 elementos y ambos son abelianos; sus modelos son $\mathbf{Z}_9$ y $\mathbf{Z}_3 \oplus \mathbf{Z}_3$.

Obsérvese que el corolario anterior caracteriza todos los grupos de orden p^2, cuando p es primo.

En los corolarios anteriores, la ecuación de clases se usó para decidir resultados acerca de la estructura de grupos de orden p^2 y p^n. En lo que sigue la usaremos para deducir resultados para grupos finitos de cualquier orden. Estos resultados se conocen con el nombre de **Teoremas de Sylow**.

Definición 5.5.8. Sea G un grupo de orden $p^n m$ con p primo que no divide a m; todo subgrupo de G de orden p^n se dice que es un **p-subgrupo de Sylow de G**.

★★ EJEMPLO H. Como $12 = 2^2 \cdot 3$, en $\mathbf{Z}_{12}$ el subgrupo H generado por [3] es un 2-subgrupo de Sylow de $\mathbf{Z}_{12}$ y el subgrupo K generado por [4] es un 3-subgrupo de Sylow de $\mathbf{Z}_{12}$.

★★ EJEMPLO I. En D_{10} $(10 = 5 \times 2)$, el grupo de las simetrías de un pentágono, el subgrupo $H = \langle A \rangle$ es un 5-subgrupo de Sylow y $K = \langle B \rangle$ es un 2-subgrupo de Sylow. El retículo de los subgrupos de D_{10} es

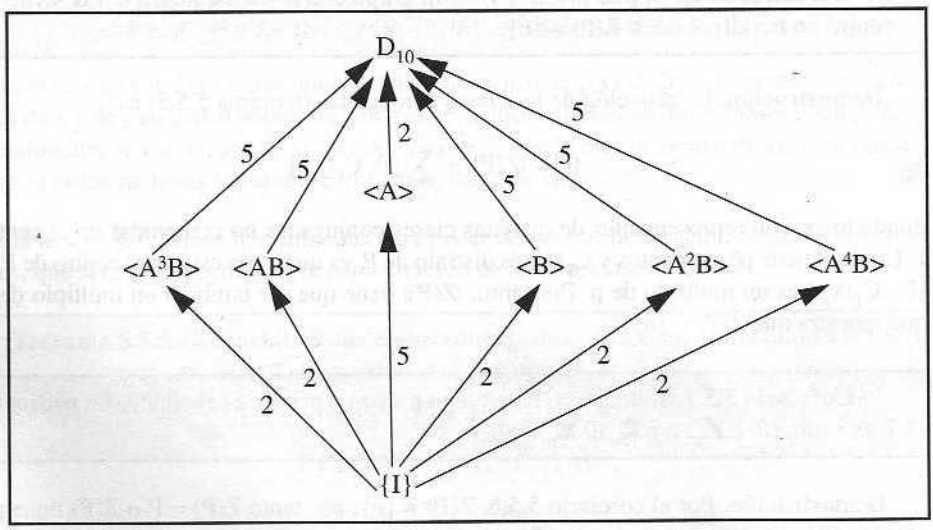


Ilustración 4. Retículo de D_{10}

Por tanto <B>, <AB>, <A^2B>, <A^3B> y <A^4B> son todos los 2-subgrupos de Sylow de D_{10}.

El primer teorema de Sylow, que expondremos a continuación, afirma, precisamente, que en todo grupo hay subgrupos de Sylow.

Teorema 5.5.9. (Primer teorema de Sylow). Sea G un grupo de orden $p^n m$ con p primo que no divide a m; en G existe al menos un p-subgrupo de Sylow.

Demostración. Realizamos la demostración por inducción en el orden de G. Si $|G| = 1$ el resultado es trivial. Supongamos que $|G| > 1$ y separemos los casos en que p divida o no al orden del centro de G, $|Z(G)|$.

Si p divide a $|Z(G)|$, por el teorema de Cauchy para grupos abelianos finitos (teorema 5.1.1), Z(G) tiene un subgrupo N de orden p. Sea G' = G/N, cuyo orden es $p^{n-1}m$; por la hipótesis de inducción G' tiene un subgrupo P' de orden p^{n-1}. Sea π: G $\rightarrow$ G' = G/N el homomorfismo canónico que transforma cada elemento en su clase de equivalencia, definido en la sección 4.3; sea $P = \pi^{-1}(P')$, que es un subgrupo de G por la proposición 4.4.4(b) y observar que P/N = P'. Por tanto, $|P| = |N|\,|P'| = p^{n-1} = p^n$, lo que prueba que P es un p-subgrupo de Sylow.

Supongamos ahora que p no divide a $|Z(G)|$. La ecuación de las clases conjugadas para G es

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G: C_G(x_i)]$$

donde los x_i son representantes de distintas clases conjugadas de G y no están en el centro de G. Si p dividiera a todos los $[G: C_G(x_i)]$, i = 1, 2, ..., r, p sería también un divisor de $|Z(G)|$ ya que p divide a |G|. Podemos, por tanto, asegurar que existe i tal que p no divide a $[G: C_G(x_i)]$. Sea $H = C_G(x_i)$ para este i; como p no divide a [G:H] = $p^n m/|H|$, hemos de tener $|H| = p^n k$ con p y k primos entre sí; como $x_i \notin Z(G)$, H es un subgrupo propio de G y por tanto $|H| < |G|$. Podemos aplicar la hipótesis de inducción a H y obtener un p-subgrupo de Sylow de H que tendrá orden p^n; éste es, también, un p-subgrupo de Sylow de G. ■

En la sección 5.1 demostramos que todo grupo abeliano finito cuyo orden es un múltiplo de un primo p tiene un elemento de orden p. El resultado, como ya anunciamos anteriormente, es cierto para cualquier grupo finito.

Teorema 5.5.10 (Teorema de Cauchy). Sea G un grupo finito y p un primo que divide a |G|. Entonces G tiene algún elemento de orden p y, por tanto, un subgrupo de orden p.

Demostración. Sea P un p-subgrupo de Sylow de G con $|P| = p^n$. Tomando $h \in P$, $h \neq e$, el orden de h es p^α, $1 \leq \alpha \leq n$. Si $\alpha = 1$, h es de orden p, y hemos encontrado el elemento deseado. Si $\alpha > 1$, sea $x = h^{p^{\alpha-1}}$, entonces $x \neq e$ y

$$x^p = (h^{p^{\alpha-1}})^p = h^{p^\alpha} = e.$$

Por tanto, x es de orden p, ya que p es primo. ■

Para demostrar el resto de los resultados de Sylow necesitamos usar el concepto de **subgrupos conjugados y de normalizador de un subgrupo.**

Definición 5.5.11. Sea G un grupo.

a) Dos subgrupos H y K de G se dicen **conjugados** si existe $g \in G$ tal que $gHg^{-1} = K$.

b) Si H es un subgrupo de G definimos el **normalizador de H en G** como $N(H) = \{g \in G: gHg^{-1} = H\}$.

c) Si Q y H son subgrupos de G, el **normalizador de H en Q** es

$$N_Q(H) = \{g \in Q: gHg^{-1} = H\} = Q \cap N_G(H).$$

El normalizador de un subgrupo H en G se definió con anterioridad en el ejercicio 12 de la sección 4.3; en ese ejercicio se pidió demostrar que N(H) es un subgrupo de G y que **H es un subgrupo normal de N(H)**; además, **H es normal en G si y sólo si N(H)=G**. Si no se han demostrado estos resultados anteriormente, es el momento de hacerlo. (¡No son difíciles!) También puede demostrarse que $N_Q(H)$ es un subgrupo de G.

★★ EJEMPLO J. Sea $S_3 = \{I, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ el grupo de las permutaciones de 3 elementos, que se definió en la sección 3.4 del capítulo 3 (véase, además, el ejemplo C de esta sección). Calcularemos los subgrupos conjugados de cada uno de sus subgrupos, sus normalizadores y el índice del normalizador en el grupo, para ilustrar el resultado que enunciaremos después.

Subgrupos H	Subgrupos conjugados	Normalizadores N(H)	$[S_3 : N(H)]$
$\{I\}$	$\{I\}$	S_3	1
$\langle\alpha\rangle$	$\langle\alpha\rangle$	S_3	1
$\langle\beta\rangle$	$\langle\beta\rangle, \langle\alpha\beta\rangle, \langle\alpha^2\beta\rangle$	$\langle\beta\rangle$	3
$\langle\alpha\beta\rangle$	$\langle\beta\rangle, \langle\alpha\beta\rangle, \langle\alpha^2\beta\rangle$	$\langle\alpha\beta\rangle$	3
$\langle\alpha^2\beta\rangle$	$\langle\beta\rangle, \langle\alpha\beta\rangle, \langle\alpha^2\beta\rangle$	$\langle\alpha^2\beta\rangle$	3

En el ejemplo anterior se observa que el número de subgrupos conjugados de un subgrupo H de un grupo G coincide con el índice del normalizador de H en G. La siguiente proposición es una generalización de este hecho.

Proposición 5.5.12. Sea G un grupo finito y sean H y Q subgrupos de G; el número de subgrupos conjugados de H mediante elementos de Q coincide con $[Q: N_Q(H)]$, el índice del normalizador de H en Q.

Demostración. Sea $\zeta(H)$ el conjunto de los subgrupos conjugados de H mediante elementos de Q; la proposición quedará demostrada si establecemos una aplicación biyectiva entre $\zeta(H)$ y $Q/N_Q(H)$. Para ello, definir $f: \zeta(H) \to Q/N_Q(H)$ mediante

$$f(gHg^{-1}) = gN_Q(H).$$

La comprobación de que f está bien definida y es biyectiva se deja como ejercicio. ■

El siguiente resultado cuenta los elementos de HK, para dos subgrupos cualesquiera de un grupo en función de los elementos de H, de K y de $H \cap K$. Cuando $H \cap K = \{e\}$ este resultado se pidió demostrar en el ejercicio 15 de la sección 4.2.

Lema 5.5.13. Si H y K son subgrupos finitos de un grupo G,

$$|HK| = |H|\,|K| / |H \cap K|.$$

Demostración. Como K es un subgrupo de G, en HK puede definirse la relación de equivalencia que produce clases de equivalencia módulo K; tenemos entonces $HK = \bigcup_{h \in H} hK$. Pero las clases de equivalencia hK no son todas disjuntas; de hecho, si $h_1K = h_2K$ se tiene $h_2^{-1}h_1 \in K$, y como $h_2^{-1}h_1 \in H$ se deduce $h_2^{-1}h_1 \in H \cap K$. Por tanto, $h_1(H \cap K) = h_2(H \cap K)$ y, en consecuencia, las clases de equivalencia h_1K y h_2K coinciden si y sólo si coinciden $h_1(H \cap K)$ y $h_2(H \cap K)$. Así pues, hay $|H| / |H \cap K|$ clases de equivalencia disjuntas en HK módulo K, y por tanto $|HK| = (|H| / |H \cap K|)\,|K|$. ■

En el siguiente resultado usaremos el concepto de **p-subgrupo. Un p-subgrupo de G** es cualquier subgrupo de G cuyo orden sea una potencia de p.

Lema 5.5.14. Sea G un grupo de orden $p^n m$ con p primo que no divide a m y sea P un p-subgrupo de Sylow de G. Si Q es un p-subgrupo cualquiera de G,

$$Q \cap N_G(P) = Q \cap P.$$

Demostración. Ya sabemos que P es un subgrupo de $N_G(P)$ (véase ejercicio 12 de la sección 4.3) y por tanto $Q \cap P \subseteq Q \cap N_G(P)$. Basta probar la inclusión $Q \cap N_G(P) \subseteq P$. Como $Q \cap N_G(P)$ es un subgrupo de $N_G(P)$, el ejercicio 13 de la sección 4.3 nos permite afirmar que $P(Q \cap N_G(P))$ es un subgrupo de G. Usamos ahora el lema 5.5.13 para escribir

$$|P(Q \cap N_G(P))| = |P|\,|Q \cap N_G(P)| / |P \cap Q \cap N_G(P)| = |P|\,|Q \cap N_G(P)| / |P \cap Q|$$

Como Q es un p-subgrupo, $|Q \cap N_G(P)|$ y $|P \cap Q|$ son de la forma p^α, $0 \leq \alpha \leq n$; como $|P| = p^n$ se tiene que $P(Q \cap N_G(P))$ tiene p^s elementos; como $P(Q \cap N_G(P))$ contiene a P y p no divide a m, $|P(Q \cap N_G(P))| = p^n$. Esto prueba que $P(Q \cap N_G(P)) = P$, y por tanto $Q \cap N_G(P) \subseteq P$, que era lo que queríamos demostrar. ■

Teorema 5.5.15. Sea G un grupo de orden $p^n m$ con p primo que no divide a m.

(a) **(Segundo teorema de Sylow).** Si P es un p-subgrupo de Sylow de G y Q es un p-subgrupo de G, existe $g \in G$ tal que Q es un subgrupo de gPg^{-1}; en particular dos cualesquiera p-subgrupos de Sylow de G son conjugados.

(b) **(Tercer teorema de Sylow).** El número n_p de p-subgrupos de Sylow de G satisface $n_p \equiv 1(p)$ (es decir, n_p es congruente con 1 módulo p) y n_p divide a m.

Demostración. Sea P un p-subgrupo de Sylow de G; sea $\mathrm{L} = \{P_1, P_2, \ldots, P_r\}$ el conjunto de todos los conjugados de P, es decir, $\mathrm{L} = \{gPg^{-1}: g \in G\}$ donde hemos tomado $P_1 = P$. Sea Q un p-subgrupo de G y definir en L la siguiente relación: $P_i \sim P_j$ si y sólo si existe $q \in Q$ tal que $qP_iq^{-1} = P_j$. Es fácil comprobar que $\sim$ es una relación de equivalencia en L; sean $\zeta_1, \zeta_2, \ldots, \zeta_s$ sus clases de equivalencia, de manera que

$$\bigcup_{i=1}^{s} \zeta_i = \mathrm{L} \quad \text{y} \quad \zeta_i \cap \zeta_j = \emptyset \text{ si } i \neq j.$$

Por tanto $r = |\mathrm{L}| = |\zeta_1| + |\zeta_2| + \ldots + |\zeta_s|$. Sea P_{ij} un representante de ζ_i y tomar ζ_1 la clase de $P = P_1$; por la proposición 5.5.12, $|\zeta_i| = [Q: N_Q(P_{ij})]$. Puesto que $N_Q(P_{ij}) = N_G(P_{ij}) \cap Q$, del lema 5.5.14 se deduce

$$|\zeta_i| = [Q: N_Q(P_{ij})] = [Q: N_G(P_{ij}) \cap Q] = [Q: Q \cap P_{ij}].$$

Queremos demostrar que $r \equiv 1(p)$. Tomando $Q = P$ se obtiene $|\zeta_1| = [P: P \cap P_1] = 1$; además, si $i \neq 1$, $P_{ij} \neq P$ y por tanto $P \cap P_{ij}$ es un subgrupo de P distinto de éste, por lo que $|\zeta_i| = [P: P \cap P_{ij}] > 1$; como $|P| = p^n$, $|\zeta_i|$ debe ser un múltiplo de p si $i = 2, 3, \ldots, s$. Por tanto $r = |\zeta_1| + |\zeta_2| + \ldots + |\zeta_s| = 1 + mp$, con $m \in \mathbf{N}$, lo que prueba $r \equiv 1(p)$.

Ya podemos demostrar el segundo teorema de Sylow. Sea Q un p-subgrupo de G y supongamos, para argumentar por contradicción, que Q no es un subgrupo de gPg^{-1} para cualquier $g \in G$. En particular, Q no es un subgrupo de P ni de P_{ij} para todo $i = 2, \ldots, s$ ya que éstos son todos los subgrupos conjugados de P; por tanto $|\zeta_1| = [Q: Q \cap P] > 1$ y $|\zeta_i| = [Q: Q \cap P_{ij}] > 1$, $i = 2, \ldots, s$, de donde se deduce que p divide a $|\zeta_i|$, $i = 1, 2, \ldots, s$. Como $r = |\zeta_1| + |\zeta_2| + \ldots + |\zeta_s|$ deducimos que p divide a r, lo cual es imposible ya que $r \equiv 1(p)$.

Esto muestra que existe g tal que Q es un subgrupo de gPg^{-1}. Como todos los p-subgrupos de Sylow tienen el mismo número de elementos, se deduce inmediatamente que dados P_1 y P_2, p-subgrupos de Sylow de G, existe $g \in G$ tal que $gP_1g^{-1} = P_2$.

Ahora es fácil probar el tercer teorema de Sylow. Todo p-subgrupo de Sylow de G es conjugado con P y por tanto L contiene todos los p-subgrupos de Sylow de P; así pues $r = n_p$ y como $r \equiv 1(p)$ se deduce que n_p es congruente con 1 módulo p.

Aplicamos ahora la proposición 5.5.12 con $H = P$ y $Q = G$ de manera que $n_p = [G: N_G(P)]$; por tanto

$$n_p = |G|/|N_G(P)| = p^n m/|N_G(P)|.$$

Pero P es un subgrupo de $N_G(P)$ y $|P| = p^n$; por lo tanto $|N_G(P)| = p^n k$, para algún número entero positivo k, de donde se deduce que n_p divide a m. ■

A continuación mostraremos, en algunos ejemplos, resultados sobre la estructura de los grupos finitos, que se deducirán de los teoremas de Sylow. Varias consecuencias más aparecerán en las dos secciones siguientes.

★★ EJEMPLO K. En un grupo G de $10 = 5 \times 2$ elementos el número n_5 de 5-subgrupos de Sylow satisface $n_5 \equiv 1(5)$ y n_5 divide a 2; por tanto $n_5 = 1$ y sólo hay un 5-subgrupo de

Sylow de este grupo. Si llamamos P a este subgrupo, gPg^{-1} es otro 5-subgrupo de Sylow de P para todo $g \in G$ y por tanto $gPg^{-1} = P$ para todo $g \in G$; esto muestra que P es un subgrupo normal de G.

El número n_2 de 2-subgrupos de Sylow satisface $n_2 \equiv 1(2)$ y n_2 divide a 5; por tanto $n_2 = 1$ o $n_2 = 5$. Para el caso $n_2 = 5$ tenemos un modelo en el ejemplo I, a saber D_{10}; en la sección 5.7 mostraremos que este es el único grupo de 10 elementos con estas características, salvo isomorfismos.

Si $n_2 = 1$, G sólo tiene un 2-subgrupo de Sylow que tendrá que ser normal debido a la proposición 4.3.7 o al segundo teorema de Sylow. Si P es el 5-subgrupo de Sylow y Q es el 2-subgrupo de Sylow y llamamos x e y a sus generadores, tenemos $P \cap Q = \{e\}$ por el teorema de Lagrange. Como P y Q son normales, x e y conmutan y por tanto xy tiene orden 10 (véase ejercicio 8 de la sección 4.3). En este caso $G \approx P \times Q \approx \mathbf{Z}_5 \oplus \mathbf{Z}_2 \approx \mathbf{Z}_{10}$.

★★ EJEMPLO L. En todo grupo G de orden 20 hay un subgrupo normal de orden 5; en efecto $20 = 5 \times 2^2$ y por tanto $n_5 \equiv 1(5)$ y n_5 divide a 4. La única posibilidad es $n_5 = 1$. Así pues, solamente existe un 5-subgrupo de Sylow, que, por el segundo teorema de Sylow, será normal en G.

★★ EJEMPLO M. Mostraremos que todo grupo G de orden 30 tiene un subgrupo normal. Como $30 = 2 \times 3 \times 5$, $n_5 \equiv 1(5)$ y n_5 divide a 6, por lo que n_5 es 1 ó 6; además, $n_3 \equiv 1(3)$ y n_3 divide a 10, y por tanto n_3 es 1 ó 10. Si n_5 fuera 6 a la vez que n_3 fuera 10, tendríamos 24 elementos de orden 5 y 20 elementos de orden 2, todos distintos, con lo que tendríamos más de 44 elementos en G. Esto muestra que G tiene un subgrupo normal de orden 5 o de orden 3.

★★ EJEMPLO N. En un grupo G de 48 elementos hay un subgrupo normal de orden 16 o de orden 8. Como $48 = 3 \times 2^4$, $n_2 \equiv 1(2)$ y n_2 divide a 3; por tanto $n_2 = 1$ ó 3. Si $n_2 = 1$ hay un subgrupo normal de orden 16. Si $n_2 = 3$, sean H y K dos 2-subgrupos de Sylow de G. Entonces $H \cap K$ debe tener 8 elementos, pues si $|H \cap K| \leq 4$, de la proposición 5.5.13 deducimos $|HK| \geq 16 \times 16/4 = 64$, lo que es imposible. Por tanto, $H \cap K$ es normal en H y en K, por lo que el normalizador de $H \cap K$ contiene a $H \cup K$ y debe tener un orden que sea múltiplo de 16 y divisor de 48, es decir, 48; en este caso $H \cap K$ es normal en G (ya que $N(H \cap K) = G$).

Corolario 5.5.16. Sean p y q primos distintos con $p < q$. Todo grupo G de orden pq tiene un sólo subgrupo de orden q que será normal en G. Si q no es congruente con 1 módulo p, G es abeliano y cíclico.

Demostración. Por el tercer teorema de Sylow, $n_q \equiv 1(q)$ y n_q divide a p; como $p < q$, deducimos $n_q = 1$ y la primera parte del resultado se sigue del segundo teorema de Sylow. Si q no es congruente con 1 módulo p, del tercer teorema de Sylow se deduce $n_p = 1$ y por tanto sólo hay un p-subgrupo de Sylow, que será normal.

En este caso, sean Q y P los subgrupos de Sylow de G de órdenes q y p respectivamente. Como $(p, q) = 1$, $P \cap Q = \{e\}$, y como son normales en G los elementos de Q conmutan con los de P. Por tanto $G \approx Q \times P \approx \mathbf{Z}_q \times \mathbf{Z}_p \approx \mathbf{Z}_{pq}$. ■

EJERCICIOS 5.5

1. Hallar las clases conjugadas de todos los elementos de D_8, el grupo de las simetrías de un cuadrado, y sus centralizadores. Establecer un cuadro como el del ejemplo C y comprobar que se cumple la ecuación de las clases conjugadas.
2. Escribir la tabla del grupo Q_8 descrito en el ejemplo D.
3. Sea P un grupo abeliano de orden p^2, con p primo, en el que todos sus elementos distintos de la identidad tienen orden p. Demostrar que P es isomorfo a $\mathbf{Z}_p \oplus \mathbf{Z}_p$.
4. Sea G un grupo de orden p^n, donde p es primo, tal que $|Z(G)| \geq p^{n-1}$. Demostrar que G es abeliano (usar el ejercicio 7 de la sección 4.6.)
5. Encontrar todos los p-subgrupos de Sylow de D_{12} (sería conveniente dibujar el retículo de sus subgrupos).
6. Encontrar todos los p–subgrupos de Sylow del grupo T de simetrías del tetraedro regular del ejemplo A de la sección 5.1 (véase también el ejercicio 1 de la misma sección). Sería conveniente dibujar el retículo de sus subgrupos.
7. Encontrar los conjugados y los normalizadores de todos los subgrupos de orden 4 de D_{12} y de todos los subgrupos de orden 3 de T (véanse problemas 5 y 6). En cada caso verificar que se cumple la proposición 5.5.12 para $Q = D_{12}$ y $Q = T$ respectivamente.
8. Demostrar que la aplicación f definida en la demostración de la proposición 5.5.12 está bien definida y es biyectiva.
9. Encontrar todos los subgrupos de Sylow de T, grupo de simetrías del tetraedro del ejemplo A de la sección 5.1 y mostrar que son conjugados entre sí si tienen el mismo orden. Comprobar que $T \approx Alt(4)$.
10. Demostrar que todo grupo de orden $5^3 \times 7^3$ tiene un subgrupo normal de orden 125.
11. Demostrar que todo grupo de orden 312 tiene un p-subgrupo de Sylow normal para algún primo p que divide al orden.
12. Probar que en todo grupo de orden 36 hay un subgrupo normal de orden 9, o de orden 18 o de orden 3.

En el texto se ha presentado una demostración de los teoremas de Sylow sin recurrir al concepto de acción de un grupo sobre un conjunto. Varios libros de texto utilizan este concepto para explicar los mencionados teoremas. En los siguientes ejercicios daremos una idea de esta técnica y pediremos al lector que la use para probar varios resultados, algunos de los cuales ya han sido probados en el texto.

Sea X un conjunto y G un grupo. Diremos que **G actúa en X mediante la aplicación** $\varphi : \mathbf{G} \times \mathbf{X} \to \mathbf{X}$ si φ satisface:

1) $\varphi(e, x) = x$ para todo $x \in X$
2) $\varphi(ab, x) = \varphi(a, \varphi(b, x))$ para todo $a, b \in G$, $x \in X$.

13. Sea $G_x = \{a \in G: \varphi(a, x) = x\}$ el subgrupo de **isotropía** de $x \in X$. Demostrar que G_x es un subgrupo de G para cada $x \in X$.

14. En el conjunto X definimos la relación $x \sim y$ si y sólo si existe $a \in G$ tal que $\varphi(a, x) = y$. Demostrar que $\sim$ es una relación de equivalencia en X.

En el conjunto cociente $X/\sim$ la clase de equivalencia de X se llama **órbita de x** y la simbolizaremos mediante O[x]; es decir $O[x] = \{x_1 \in X:$ existe $a \in G$ y $\varphi(a, x) = x_1\}$.

15. Demostrar la igualdad $|O[x]| = |G/G_x|$ (Sugerencia: definir una aplicación biyectiva entre O[x] y G/G_x).

16. Sea G un grupo y $\varphi: G \times G \to G$ una aplicación dada por $\varphi(a, g) = gag^{-1}$.
    i) Demostrar que G actua sobre sí mismo mediante la aplicación φ.
    ii) Demostrar que G_a es el centralizador de a en G.
    iii) Deducir la proposición 5.5.3 usando este resultado y el ejercicio 15.

Sean $x_1, x_2, \ldots, x_r$ representantes distintos de cada una de las órbitas de X. Por el problema 14

$$|X| = \sum_{i=1}^{r} |O[x_i]| .$$

Sea $X_G = \{x \in X: \varphi(g, x) = x$ para todo $g \in G\}$, es decir el conjunto de los elementos de X cuya órbita solamente tiene un elemento. Si hay s de éstos,

$$|X| = |X_G| + \sum_{i=s+1}^{r} |O[x_i]| .$$

17. Si G es un grupo de orden p^n demostrar que $|X| \equiv |X_G|$ (p).

18. Sean P y Q dos subgrupos de un grupo G de orden finito. Sea $\mathrm{P} = G/P$ el conjunto de las clases de equivalencia por la izquierda de P en G. Demostrar que Q actua en P mediante la aplicación $\delta : Q \times \mathrm{P} \to \mathrm{P}$ dada por $\delta(y, xP) = (yx)P$.

19. Si P y Q son dos p-subgrupos de Sylow de un grupo G de orden finito, demostrar que P y Q son conjugados (usar los ejercicios 17 y 18). Este resultado es una parte del segundo teorema de Sylow enunciado en el teorema 5.5.15.

20. Sea H un p–subgrupo de un grupo finito G.
    i) Demostrar que $[N(H):H] \equiv [G:H]$ (p) (usar los ejercicios 17 y 18, este último con $P = Q = H$)
    ii) Deducir de i) que si p divide a [G:H] se tiene que p divide a [N(H):H] y en consecuencia $H \neq N(H)$.

21. Demostrar que todo grupo finito G de orden $p^n m$, con p primo que no divide a m, tiene un subgrupo de orden p^i para cada i = 1, 2, ..., n (para i = 1 es el teorema de Cauchy; proceder por inducción en i).

5.6. GRUPOS SIMPLES Y GRUPOS SOLUBLES

Si un grupo G tiene un subgrupo propio normal N distinto de {e}, algunas de las propiedades del grupo G pueden deducirse a partir de las propiedades de N y del grupo cociente G/N. Un resultado de estas características está contenido en el primer teorema de isomorfía: el retículo de los subgrupos de G que contienen a N es "isomorfo" al retículo de los subgrupos de G/N, de manera que conociendo la estructura de G/N se conoce la estructura de los subgrupos de G que contienen a N.

En este capítulo hemos tenido ocasión de presenciar cómo se utiliza este argumento en dos demostraciones por inducción. En la sección 5.1 la demostración del teorema de Cauchy para grupos abelianos finitos tiene como razonamiento principal el encontrar un subgrupo propio normal N y aplicar la hipótesis de inducción a G/N. El mismo argumento usamos en la demostración de uno de los casos del primer teorema de Sylow desarrollado en la sección 5.5.

Se presenta una dificultad insalvable para hacer este tipo de razonamientos cuando el grupo G no tiene subgrupos normales propios. En este caso, podemos decir que el grupo es "sencillo" o, como se dice en matemáticas, **simple**.

Definición 5.6.1. Un grupo G es **simple** si no tiene subgrupos normales propios distintos de {e}.

Todo grupo de orden p, con p primo, es simple. No sólo no tiene subgrupos normales propios no triviales, sino que ni siquiera tiene subgrupos propios no triviales como consecuencia del teorema de Lagrange.

Por otro lado, si G es un grupo abeliano cuyo orden no es un primo, G tiene subgrupos de orden cada uno de los primos que aparecen en la descomposición de |G| (véase teorema 5.3.9). Como G es abeliano todos estos subgrupos son normales y, por tanto, todo grupo abeliano cuyo orden **no** es primo **no es un grupo simple**.

Entre los grupos no abelianos esta cuestión es sencilla si sus órdenes son muy pequeños. En $S_3 = \{I, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ el subgrupo generado por α es normal y por tanto S_3 **no es simple**. Como S_3 es isomorfo a D_6, éste tampoco es simple. En general, **ningún** D_{2n}, el grupo de las simetrías de un polígono regular de n lados (véase la sección 3.6) **es simple**, ya que el subgrupo generado por A, giro de $2\pi/n$ radianes alrededor del origen, es un subgrupo normal propio de D_{2n}. **El grupo** Q_8 del ejemplo D de la sección 5.5 **tampoco es simple** ya que tiene tres subgrupos de orden 4 que son normales en Q_8.

Los teoremas de Sylow junto con el lema 5.5.13 se utilizan para demostrar que los grupos de ciertos órdenes no pueden ser simples. Si se repasan los ejemplos K, L, M y N de la sección 5.5, se concluirá que ninguno de los grupos de órdenes 10, 20, 30 ó 48 pueden ser simples. El corolario 5.5.16 es también un resultado acerca de la no simplicidad de grupos cuyo orden es pq con p y q primos distintos y $p < q$. Los razonamientos realizados en los ejemplos que acabamos de mencionar son los que se pueden usar para realizar los tres primeros ejercicios del final de esta sección en los que se pide demostrar la no simplicidad de todos los grupos de un cierto orden.

En 1963 los matemáticos W. Feit y J. W. Thompson lograron probar un resultado, conjeturado por Burnside, acerca de los grupos finitos simples no abelianos.

Teorema 5.6.2. (Feit–Thompson). Todo grupo finito simple no abeliano es de orden par.

Los autores publicaron este resultado en un artículo titulado "On the solvability of groups of odd order", que ocupó las 255 páginas del número 13 de la revista "Pacific Journal of Mathematics" publicada en 1963.

Hemos encontrado una familia infinita de grupos simples, la de los grupos (abelianos) de orden primo. Los otros ejemplos que hemos puesto son todos de grupos no simples. Para encontrar otra familia de grupos simples es necesario estudiar algunos subgrupos de los grupos de permutaciones de n elementos, S_n. Convendría repasar, antes de continuar, la sección 4.8 dedicada a los grupos de permutaciones. Toda permutación es par o impar; el conjunto de las permutaciones pares forma un subgrupo de S_n que se llama el grupo **alternado** de n elementos y que hemos simbolizado mediante Alt(n). Como $|Alt(n)| = n!/2$ y $|S_n| = n!$, Alt(n) es un subgrupo normal de S_n y, en consecuencia, ninguno de los grupos de permutaciones S_n es simple.

La historia es diferente con los grupos Alt(n). Alt(3) tiene 3 elementos y, por tanto, es simple. Alt(4) está formado por todas las permutaciones pares de 4 elementos; es un grupo isomorfo al grupo T de simetrías del tetraedro regular descrito en el ejemplo A de la sección 5.1. Está formado por 8 elementos de orden 3 que son los giros alrededor de rectas que pasan por cada uno de sus vértices y el centro del triángulo equilátero opuesto y que como permutaciones son

$$\alpha = (1\ 2\ 3), \quad \alpha^2 = (1\ 3\ 2), \quad \beta = (1\ 2\ 4), \quad \beta^2 = (1\ 4\ 2),$$
$$\gamma = (1\ 3\ 4), \quad \gamma^2 = (1\ 4\ 3), \quad \delta = (2\ 3\ 4), \quad \delta^2 = (2\ 4\ 3).$$

Además tiene cuatro elementos de orden 2 que son simetrías con respecto a ejes que pasan por los puntos medios de dos lados opuestos:

$$\sigma_1 = (1\ 2)\ (3\ 4), \quad \sigma_2 = (1\ 3)\ (2\ 4), \quad \sigma_3 = (1\ 4)\ (2\ 3).$$

Alt(4) tiene un subgrupo de orden 4 que es normal (véase el ejercicio 4 al final de esta sección); por tanto Alt(4) **no es simple.**

La situación es diferente para **Alt(n) si n≥ 5: todos ellos son simples.** Esta será nuestra segunda familia infinita de grupos simples, lo que demostraremos en los resultados que siguen.

Lema 5.6.3. Los ciclos de longitud 3 generan Alt(n) si $n \geq 3$.

Demostración. Todas las permutaciones de Alt(n) pueden escribirse como un producto de un número par de transposiciones (véase corolario 4.8.7 y téngase en cuenta la definición de Alt(n)). Agrupamos las transposiciones de dos en dos. Los casos que pueden darse son (i j) (k l) o (i j) (i l). En el primer caso

$$(i\ j)\ (k\ l) = (i\ k\ j)\ (i\ k\ l),$$

y en el segundo

$$(i\ j)\ (i\ l) = (i\ l\ j).$$

Por tanto, todo elemento de Alt(n) puede escribirse como un producto de ciclos de longitud 3. ■

Lema 5.6.4. Sean $r_0, s_0 \in \{1, 2, \ldots, n\}$, $r_0 \neq s_0$. Los 3-ciclos especiales de la forma $(r_0\ s_0\ i)$, $i = 1, 2, \ldots, n$, $i \neq r_0$, $i \neq s_0$, generan Alt(n) si $n \geq 3$.

Demostración. Si (i j k) es un 3-ciclo podemos escribir

$$(i\ j\ k) = (r_0\ i\ j)\ (r_0\ j\ k).$$

Ahora

$$(r_0\ i\ j) = (r_0\ s_0\ j)\ (r_0\ s_0\ i)\ (r_0\ s_0\ i),$$

lo que prueba el resultado deseado. ■

Proposición 5.6.5. Si N es un subgrupo normal de Alt(n), $n \geq 3$, que contiene un 3-ciclo, N = Alt(n).

Demostración. Sea $r = (r_0\ s_0\ i)$ un 3-ciclo de N. Basta demostrar que los 3-ciclos $(r_0\ s_0\ j)$ son elementos de N para todo j distinto de r_0 y s_0 y aplicar el lema 5.6.4. Es suficiente con hacer el siguiente cálculo si $i \neq j$:

$$((i\ j)(r_0\ s_0))^{-1}\ (r_0\ s_0\ i)^2\ ((i\ j)\ (r_0\ s_0)) = (r_0\ s_0\ j),$$

y observar que la parte izquierda es un elemento de N por ser N normal en Alt(n). ■

Proposición 5.6.6. Alt(5) es simple.

Demostración. Sea N un subgrupo normal de Alt(5) distinto de {I}; la estrategia es demostrar que N ha de contener un 3-ciclo y aplicar la proposición 5.6.5. Sea $\sigma \in N$, $\sigma \neq I$; σ es una composición de ciclos **disjuntos** y con signatura par. Los casos que pueden presentarse, esencialmente diferentes, son:

$$\text{i) } \sigma = (a\ b)\ (c\ d) \quad \text{ii) } \sigma = (a\ b\ c) \quad \text{ii) } \sigma = (a\ b\ c\ d\ e)$$

Observar que σ no puede ser de la forma (a b c) (d e) ya que ésta es una permutación impar y por la misma razón no puede ser de la forma (a b c d).

En el caso i) tomar $e \neq a, b, c, d$ (aquí usamos $n = 5$ y observar que si $\beta = (a\ b\ e)$

$$\alpha[\beta\alpha\beta^{-1}] = (a\ b)\ (c\ d)\ (a\ b\ e)\ (a\ b)\ (c\ d)\ (e\ b\ a) = (a\ b\ e) \in N,$$

ya que N es normal. En este caso N contiene un 3-ciclo. No hay nada que mostrar en el caso ii), ya que σ es un 3 ciclo. Para el caso iii) observamos que

$$\sigma^{-1}[(a\ b\ c)\ \sigma\ (a\ b\ c)^{-1}] = (e\ d\ c\ b\ a)\ (a\ b\ c)\ (a\ b\ c\ d\ e)\ (a\ c\ b) = (a\ c\ e) \in N,$$

ya que N es normal. También en este caso N contiene un 3-ciclo. ■

Teorema 5.6.7. Alt(n) es simple si $n \geq 5$.

Demostración. Habiendo mostrado ya que Alt(5) es simple, procedemos por inducción en n. Sea $n \geq 6$ y N un subgrupo normal de Alt(n) distinto de {I}. Supongamos que existe $\sigma \in N$ tal que $\sigma \neq I$ y $\sigma(i) = i$ para algún $i \in \{1, 2, \ldots, n\}$. Sea $G_i = \{\alpha \in \text{Alt}(n): \alpha(i) = i\}$, que es un subgrupo de Alt(n) isomorfo a Alt(n – 1) ya que todos sus elementos dejan i fijo. Por la hipótesis de inducción, G_i es simple. Si definimos $N' = N \cap G_i$, N' es un subgrupo normal de G_i no trivial ya que $\sigma \in N'$. Entonces $N' = G_i$ por la hipótesis de inducción y por tanto G_i es un subgrupo de N. Por otro lado, si $j \neq i$, $G_j = (i\ j)\ G_i(i\ j)^{-1}$, ya que si $\alpha \in G_i$, $\beta = (i\ j)\ \alpha\ (i\ j)^{-1} = (i\ j)\ \alpha\ (i\ j)$ satisface $\beta(j) = j$. Como $(i\ j)\ G_i(i\ j)^{-1} \leq N$, ya que G_i es subgrupo de N y N es normal, tenemos que $G_j \leq N$ para todo $j = 1, 2, \ldots, n$.

Sea $\tau \in \text{Alt}(n)$ y escribamos $\tau = (\sigma_1 \circ \sigma_2) \circ (\sigma_3 \circ \sigma_4) \circ \ldots \circ (\sigma_{2s-1} \circ \sigma_{2s})$ como una composición de un número par de transposiciones. Como $n > 4$, cada par de transposiciones deja al menos un elemento fijo (el que no está en ninguna de ellas), de donde se deduce que cada par es un elemento de algún G_j, $j = 1, 2, \ldots, n$. Como Alt(n) coincide con el subgrupo generado por $\bigcup_{j=1}^{n} G_j$ y cada G_j es un subgrupo de N, se tiene que Alt(n) = N, lo que prueba, en este caso, que Alt(n) es simple.

La demostración se terminará si logramos probar que para $n \geq 6$ existe $\mu \in N$ que deja fijo al menos un elemento i entre 1 y n. Si $\sigma \in N$, escribimos σ como una composición de ciclos disjuntos; puede suceder que σ contenga un ciclo de longitud superior a 2 o que todos sus ciclos sean transposiciones.

Supongamos en primer lugar que $\sigma = (a_1\ a_2\ a_3\ \ldots)\sigma'$ tiene un ciclo $(a_1\ a_2\ a_3\ \ldots)$ de longitud 3 o superior. Sea $\tau \in G$ tal que $\tau(a_1) = a_1$, $\tau(a_2) = a_2$ y $\tau(a_3) \neq a_3$, lo que es posible ya que $n \geq 4$. Entonces $\tau\sigma\tau^{-1} \in N$ y

$$\tau\sigma\tau^{-1} = \tau(a_1\ a_2\ a_3\ \ldots)\sigma'\tau^{-1} = (a_1\ a_2, \tau(a_3), \ldots).$$

Al calcular $\mu = \sigma^{-1}[\tau\sigma\tau^{-1}]$, que es un elemento de N, se obtiene $\mu(a_1) = a_1$, y hemos conseguido el objetivo de que N tenga una permutación que deja fijo un i entre 1 y n.

Supongamos, para finalizar, que $\sigma \in N$, $\sigma \neq I$, es un producto de transposiciones disjuntas; si $\sigma = (a_1\ a_2)\ (a_3\ a_4)$, σ deja fijo a_5 y el resultado está probado. Si

$$\sigma = (a_1\ a_2)\ (a_3\ a_4)\ (a_5\ a_6)\ \ldots$$

(aquí se necesita $n \geq 6$) sea $\tau = (a_1\ a_2)\ (a_3\ a_5) \in \mathrm{Alt}(n)$; como $\tau\sigma\tau^{-1} \in N$ y

$$\tau\sigma\tau^{-1} = (a_1\ a_2)\ (a_3\ a_6)\ (a_4\ a_5)\ \ldots$$

se tiene que $\mu = \sigma^{-1}[\tau\sigma\tau^{-1}] \in N$ y $\mu(a_1) = a_1$, con lo que también en este caso hay una permutación de N que deja fijo un elemento. Esto termina la demostración de que Alt(n) es simple si $n \geq 5$. ■

En cierto sentido los grupos simples son los "átomos" a partir de los cuales se pueden "construir" el resto de los grupos finitos; juegan un papel análogo en la descomposición de un grupo al que tienen los primos en el teorema fundamental de la aritmética.

Definición 5.6.8. En un grupo G una cadena de subgrupos

$$\{I\} = H_0 \leq H_1 \leq H_2 \leq \ldots \leq H_{k-1} \leq H_k = G$$

se dice que es una **serie de composición** si H_i es un subgrupo normal de H_{i+1} y H_{i+1}/H_i es un grupo simple para todo $i = 0, 1, 2, \ldots, k-1$. En una serie de composición los grupos cociente H_{i+1}/H_i se denominan **factores de composición**.

★★ EJEMPLO A. En $\mathbf{Z}_{20}$ las siguientes cadenas

$$\{[0]\} \leq \langle[4]\rangle \leq \langle[2]\rangle \leq \mathbf{Z}_{20}$$

$$\{[0]\} \leq \langle[10]\rangle \leq \langle[5]\rangle \leq \mathbf{Z}_{20}$$

son series de composición ya que todos los subgrupos son normales en $\mathbf{Z}_{20}$ (este grupo es abeliano) y los factores de composición son grupos cíclicos de orden primo, y por tanto simples. Observar que los factores de composición de la primera cadena son

$$\mathbf{Z}_{20}/\langle[2]\rangle \approx \mathbf{Z}_2, \quad \langle[2]\rangle/\langle[4]\rangle \approx \mathbf{Z}_2, \quad \langle[4]\rangle/\{[0]\} \approx \mathbf{Z}_5$$

y que los correspondientes de la segunda cadena son

$$\mathbf{Z}_{20}/\langle[5]\rangle \approx \mathbf{Z}_5, \quad \langle[5]\rangle/\langle[10]\rangle \approx \mathbf{Z}_2, \quad \langle[10]\rangle/\{[0]\} \approx \mathbf{Z}_2.$$

En ambos casos los factores de composición son los mismos salvo isomorfismos.

★★ EJEMPLO B. En el grupo D_8 de las simetrías de un cuadrado, $D_8 = \{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$ con $A^4 = I$, $B^2 = I$ y $BA = A^3B$ (véase la sección 3.6 para recordar la definición, y el ejemplo D de la sección 4.5 para encontrar su retículo), las cadenas

$$\{I\} \lhd \langle AB\rangle \lhd \langle AB, A^2\rangle \lhd D_8$$

y

$$\{I\} \lhd \langle A^2\rangle \lhd \langle A\rangle \lhd D_8$$

son dos series de composición cuyos factores de composición son

$$D_8/\langle AB, A^2\rangle \approx \mathbf{Z}_2, \quad \langle AB, A^2\rangle/\langle AB\rangle \approx \mathbf{Z}_2, \quad \langle AB\rangle/\{I\} \approx \mathbf{Z}_2$$

y

$$D_8/\langle A\rangle \approx \mathbf{Z}_2, \quad \langle A\rangle/\langle A^2\rangle \approx \mathbf{Z}_2, \quad \langle A^2\rangle/\{I\} \approx \mathbf{Z}_2 .$$

De nuevo los factores de composición son los mismos salvo isomorfismos.

Observar que no es necesario que, en una serie de composición, H_i sea un subgrupo normal de G, sino solamente de H_{i+1}. En los dos ejemplos anteriores puede observarse que se cumple el resultado que enunciamos a continuación en el que se establece que todo grupo finito tiene una serie de composición "esencialmente única" en el sentido de que dos series de composición de G tienen factores de composición isomorfos.

Teorema 5.6.9. (Teorema de Jordan–Hölder). Sea G un grupo finito.

(i) G tiene una serie de composición.

(ii) Sean $\{I\} = H_0 \leq H_1 \leq \ldots \leq H_k = G$ y $\{I\} = J_0 \leq J_1 \leq \ldots \leq J_r = G$ dos series de composición de G; se tiene que $k = r$ y existe una permutación α de $\{0, 1, \ldots, k-1\}$ tal que

$$J_{\alpha(i)+1}/J_{\alpha(i)} \approx H_{i+1}/H_i, \quad i = 0, 1, 2, \ldots, k-1.$$

La primera parte de este teorema es fácil demostrar y se propone como ejercicio al final de esta sección. La segunda parte requiere comprobar un resultado técnico que recibe el nombre de lema de Zassenhaus o "de la mariposa" debido a que la figura que suele trazarse durante su demostración semeja a uno de estos insectos. No demostraremos estos resultados, que no

son más que una aplicación larga, pero sencilla, de los teoremas de isomorfía descritos y demostrados en la sección 4.5. El lector interesado puede consultar la bibliografía al final de este libro.

Una vez conocido el teorema de Jordan-Hölder, la clasificación de todos los grupos finitos requiere tener una lista completa de todos los grupos simples finitos posibles. Numerosos matemáticos de todo el mundo han dedicado su esfuerzo a descubrir grupos simples. Nosotros ya hemos encontrado dos familias infinitas de grupos simples: los grupos cíclicos de orden primo y los grupos Alt(n) si $n \geq 5$. Hay 16 familias infinitas más de grupos simples finitos, lo que con las dos anteriores constituyen la lista completa de las 18 familias infinitas de grupos simples finitos.

Pero también hay otros grupos finitos simples que no pertenecen a ninguna de estas familias. El primero de ellos fue descubierto por Emile Mathieu en el decenio de 1860, y tenía $7.920 = 8 \times 9 \times 10 \times 11$ elementos. El sexto de estos grupos, que comenzaron a llamarse **esporádicos**, fue encontrado por Zvonimir Janko, que trabajaba en la Monash University (Australia), un siglo después que el anterior y tenía 175.560 elementos. A partir de aquí se comenzaron a descubrir vertiginosamente varios grupos esporádicos simples nuevos, que culminaron cuando en 1982 Robert Griess Jr., que trabajaba en el Institute for Advanced Study de Princeton, encontró un grupo simple de

808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000

($\approx 8{,}08 \times 10^{53}$) elementos, al que se le conoce con el nombre de **"el monstruo"**. El "monstruo" hace el número 26 de los grupos esporádicos simples, algunos de los cuales fueron descubiertos después que éste.

Encontrar grupos simples esporádicos puede ser tarea tediosa. Pero diseñar un método que permita encontrar **todos** ellos y llevarlo a buen puerto es una tarea mucho más complicada. En 1972, Daniel Gorenstein proponía, en unas conferencias impartidas en la Universidad de Chicago, un programa para determinar todos los grupos finitos simples. Pensaba este matemático que su programa no estaría terminado hasta finales del siglo XX. Nadie contaba entonces con M. Aschbacher, quien, recién terminada su carrera universitaria, dedicaría un gran esfuerzo a trabajar en el programa de Gorenstein; logró demostrar varios teoremas sorprendentes en poco tiempo y, aunque en el resultado final también trabajaron otras personas, Aschbacher fue el principal responsable de que el programa propuesto en la Universidad de Chicago tardase solamente diez años en completarse.

El resultado final es que **sólo existen 18 familias infinitas de grupos simples finitos y 26 grupos simples esporádicos**, todos ellos completamente descritos en la actualidad. Conseguir esto requirió más de 500 artículos de investigación publicados en aproximadamente 15.000 páginas. Cuando Daniel Gorenstein escribió un artículo de divulgación sobre esta saga, que se publicó en Scientific American (edición española, Febrero 1982), lo tituló, y con razón, "El teorema enorme". El lector interesado puede consultar este artículo, y si desea adentrarse en este fascinante problema puede leer el libro de M. Aschbacher reseñado en la bibliografía.

Otra clase de grupos que estudiaremos, debido a la importancia que tienen en la resolución de ecuaciones algebraicas mediante radicales, es la de los grupos **solubles**.

Definición 5.6.10. Un grupo G es soluble si existe una cadena de subgrupos de G que satisfacen

$$\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_k = G,$$

y en la que todos sus factores H_{i+1}/H_i, $i = 0, 1, 2, \ldots, k-1$, son abelianos.

★★ EJEMPLO C. El grupo D_8 es soluble ya que en el ejemplo B se encontró una serie con factores isomorfos a $(\mathbf{Z}_2, +)$, que es abeliano.

★★ EJEMPLO D. Todo grupo abeliano G es soluble ya que $\{e\} \lhd G$ es una serie con factor abeliano.

★★ EJEMPLO E. El **grupo S_3**, de las permutaciones de 3 elementos, **es soluble** ya que

$$\{I\} \lhd \text{Alt}(3) \lhd S_3$$

es una serie con factores $S_3/\text{Alt}(3) \approx \mathbf{Z}_2$ y $\text{Alt}(3)/\{I\} \approx \mathbf{Z}_3$ (Recuérdese que S_3 es isomorfo a D_6).

El **grupo S_4** de las permutaciones de 4 elementos, también **es soluble** ya que

$$\{I\} \lhd \langle(1\,2)(3\,4), (1\,3)(2\,4)\rangle \lhd \text{Alt}(4) \lhd S_4$$

es una serie con factores

$$S_4/\text{Alt}(4) \approx \mathbf{Z}_2, \qquad \text{Alt}(4)/\langle(1\,2)(3\,4), (1\,3)(2\,4)\rangle \approx \mathbf{Z}_3$$

y

$$\langle(1\,2)(3\,4), (1\,3)(2\,4)\rangle / \{I\} \approx \mathbf{Z}_2 \times \mathbf{Z}_2,$$

que son abelianos (consúltese el retículo de los subgrupos de Alt(4) en el problema 4 al final de esta sección). Claramente, **Alt(4) es también un grupo soluble.**

En el ejemplo anterior se muestra que S_3 y S_4 son grupos solubles. No sucede así para S_n si $n \geq 5$, lo que es una consecuencia del teorema 5.6.7, en el que se muestra que Alt(n) es simple si $n \geq 5$.

Teorema 5.6.11. Si $n \geq 5$, S_n y Alt(n) no son solubles.

Demostración. La única serie que podría tener S_n, si $n \geq 5$, es $\{I\} \lhd Alt(n) \lhd S_n$ debido a que Alt(n) es simple (teorema 5.6.7); pero esta serie no tiene factores abelianos ya que Alt(n) es un grupo **no** abeliano si $n > 3$. Un razonamiento similar sirve para Alt(n). ■

El ejemplo E y el teorema 5.6.11 son la clave que permite probar que las ecuaciones algebraicas de grado inferior a 5 pueden resolverse mediante radicales, pero no así las de grado superior o igual a 5. El resultado fundamental, que se enmarca dentro de la teoría de Galois, establece que una ecuación algebraica es soluble mediante radicales sólo cuando un cierto grupo asociado con la ecuación es soluble.

En los ejercicios al final de esta sección se pide demostrar algunas propiedades de los grupos solubles. Terminaremos esta sección dando una caracterización de los grupos solubles en términos del subgrupo conmutador de un grupo.

Definición 5.6.12. Sea G un grupo y $x, y \in G$; el **conmutador de x e y** se define mediante $[x, y] = x^{-1}y^{-1}xy$ y el subgrupo G' generado por todos los conmutadores de elementos de G, es decir $G' = \langle \{[x, y]: x, y \in G\} \rangle$, se llama **el subgrupo conmutador de G.**

★★ EJEMPLO F. Si G es un grupo abeliano, $[x, y] = e$ para todo par x, y de elementos de G; por tanto $G' = \{e\}$. El subgrupo conmutador de S_3, $(S_3)'$ es Alt(3), lo que en este momento puede hacerse calculando todos los conmutadores de elementos de S_3 (alguno puede obviarse ya que si dos elementos conmutan, su conmutador es la identidad).

Proposición 5.6.13. Sea G un grupo; el subgrupo conmutador G' de G es normal en G y G/G' es abeliano. Además, si N es un subgrupo normal de G, G/N es abeliano si y sólo si G' es un subgrupo de N.

Demostración. Comenzaremos demostrando que G' es normal en G. Sea $g \in G$ y $x \in G'$, tenemos que probar que $gxg^{-1} \in G'$. El elemento x es un producto de conmutadores; insertando entre cada uno de los conmutadores que forman este producto el elemento $e = g^{-1}g$, basta probar que $g[a, b]g^{-1} \in G'$ para cada par $a, b \in G$. Esto resulta sencillo:

$$[gag^{-1}, gbg^{-1}] = (ga^{-1}g^{-1})(gb^{-1}g^{-1})(gag^{-1})(gbg^{-1}) = ga^{-1}b^{-1}abg^{-1} = g[a, b]g^{-1}.$$

Para mostrar que G/G' es abeliano sean xG' e yG' dos clases de equivalencia de G/G'. El cálculo

$$(xG')(yG') = (xy)G' = (xy)[y, x]G' = (yx)G' = (yG')(xG')$$

muestra el resultado deseado.

Supongamos ahora que N es un subgrupo normal de G y que G/N es abeliano; entonces, si $x, y \in G$, $(xy)N = (xN)(yN) = (yN)(xN) = (yx)N$ y, por tanto, $x^{-1}y^{-1}xyN = N$, de donde se deduce $[x, y] \in N$; como G' es el más pequeño de los subgrupos de G que contienen a todos los conmutadores, G' es un subgrupo de N.

Recíprocamente, supongamos que G' es un subgrupo de N; entonces.

$$(xN)\,(yN) = (xy)\,N = xy[y, x]N = (yx)\,N = (yN)\,(xN)$$

y por tanto G/N es abeliano. ■

★★ EJEMPLO G. En ocasiones es posible encontrar el subgrupo conmutador de un grupo sin necesidad de calcular los conmutadores. Para el grupo D_8 de las simetrías de un cuadrado sabemos que $Z(D_8) = \langle A^2 \rangle$ es un subgrupo normal de D_8; como $D_8 / Z(D_8)$ es abeliano, ya que tiene orden 4, de la proposición 5.6.13 se deduce que $(D_8)'$ es un subgrupo de $Z(D_8)$. Por otro lado, $(D_8)'$ no es $\{I\}$ ya que D_8 no es abeliano y por tanto $(D_8)' = Z(D_8) = \{I, A^2\}$.

Usando el concepto de subgrupo conmutador se puede construir una serie de subgrupos de un grupo G. Sea $G^{(0)} = G$, $G^{(1)} = G'$, $G^{(2)} = (G')'$, y en general $G^{(i+1)} = (G^{(i)})'$ es el subgrupo conmutador de $G^{(i)}$. Por la proposición 5.6.13, $G^{(i+1)}$ es un subgrupo normal de $G^{(i)}$, $i = 0, 1, 2, \ldots$ La serie

$$G = G^{(0)}, G^{(1)}, \ldots, G^{(k)}, \ldots$$

se llama **serie de conmutadores** o **serie derivada de G**. Si existe un $k \in$ tal que $G^{(k)} = \{e\}$ la cadena finita

$$\{e\} = G^{(k)} \lhd G^{(k-1)} \lhd \ldots \lhd G^{(1)} \lhd G^{(0)} = G$$

tiene factores, $G^{(i)}/G^{(i+1)}$, abelianos según la proposición 5.6.13, y por tanto el grupo G es soluble. Esta condición es una caracterización para los grupos solubles.

Teorema 5.6.14. Un grupo G es soluble si y sólo si $G^{(k)} = \{e\}$ para algún $k \geq 0$.

Demostración. Ya hemos comentado antes de enunciar el teorema la razón por la que un grupo G es soluble si $G^{(k)} = \{e\}$ para algún $k \geq 0$: es una consecuencia de la proposición 5.6.13.

Supongamos ahora que G es soluble, de manera que existe una cadena de subgrupos

$$\{e\} = H_n \lhd H_{n-1} \lhd \ldots \lhd H_1 \lhd H_0 = G$$

en donde cada factor H_{i-1}/H_i es abeliano, $i = 1, 2, \ldots, n$. Demostraremos por inducción que $G^{(i)}$ es un subgrupo de H_i. Esto es cierto para $i = 0$ y para $i = 1$ por la segunda parte de la proposición 5.6.13. En general, si suponemos que $G^{(i-1)}$ es un subgrupo de H_{i-1}, G^i es un subgrupo de $(H_{i-1})'$; como H_{i-1}/H_i es abeliano, la segunda parte de la proposición 5.6.13 nos permite deducir que $(H_{i-1})'$ es un subgrupo de H_i y por tanto $G^{(i)} \leq (H_{i-1})' \leq H_i$, que era lo que queríamos demostrar. Como $H_n = \{e\}$ tenemos $G^{(n)} = \{e\}$ y el teorema queda probado. ■

★★ EJEMPLO H. Como Alt(n) es simple si $n \geq 5$, $(\text{Alt}(n))'$ es un subgrupo normal de Alt(n) que no es $\{I\}$ ya que Alt(n) no es abeliano y por tanto $(\text{Alt}(n))' = \text{Alt}(n)$. En general $(\text{Alt}(n))^{(k)} = \text{Alt}(n)$ para todo $k = 1, 2, \ldots$, si $n \geq 5$. Por el teorema 5.6.14, Alt(n) no puede ser soluble si $n \geq 5$.

Este resultado puede deducirse sin recurrir al teorema en el que se demuestra la simplicidad de Alt(n) si $n \geq 5$ (teorema 5.6.7); se indica cómo puede hacerse esto en algunos ejercicios al final de esta sección.

EJERCICIOS 5.6

1. Demostrar que no hay grupos simples de orden $255 = 3 \cdot 5 \cdot 17$
2. Demostrar que no hay grupos simples de orden $p^r m$ con p primo y $m < p$.
3. Demostrar que si $|G| = 365$, G no es simple.
4. Dibujar el retículo de los subgrupos de Alt(4). (Véase ejercicio 5.5.6. Para demostrar que solamente hay un subgrupo de orden 4, que por el segundo teorema de Sylow será normal, usar un argumento para contar los elementos de Alt(4) si hubiera más de un subgrupo de orden 4.)
5. Demostrar que $(\mathbf{Z}, +)$ no puede tener una serie de composición.
6. Encontrar una serie de composición en S_n, el grupo de las permutaciones de n elementos, para cada $n \geq 3$.
7. Encontrar un serie de composición en $\mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_5$.
8. Un **subgrupo normal maximal de un grupo G** es un subgrupo normal M de G que no coincide con G y tal que ningún subgrupo normal propio de G contiene propiamente a M. Demostrar que M es un subgrupo normal maximal de G si y sólo si G/M es simple. (Sugerencia: usar el homomorfismo canónico π: $G \to G/M$ y el teorema de correspondencia entre homomorfismos y subgrupos de la sección 4.4)
9. Usar el ejercicio 8 para demostrar la parte i) del teorema de Jordan–Hölder (teorema 5.6.9).
10. Demostrar que el grupo D_{2n} de las simetrías de un polígono regular de n lados es soluble para todo $n \geq 3$.
11. i) Sea G un grupo soluble y φ: $G \to G'$ un homomorfismo de grupos que sea suprayectivo; demostrar que G' es soluble.
    ii) Si N es un subgrupo normal de G y G es soluble, demostrar que G/N es soluble.
12. Sea G un grupo y N un subgrupo normal de G; demostrar que si N y G/N son solubles, G es soluble (este resultado puede probarse manejando cuidadosamente el segundo teorema de isomorfía expuesto en la sección 4.5).
13. Encontrar una serie de composición de $S_3 \times S_3$. ¿Es este grupo soluble?
14. Si G y H son dos grupos solubles, demostrar que el grupo producto directo $G \times H$ es también soluble.

15. Sean A y B dos subconjuntos no vacíos de G; definir [A, B] como el subgrupo generado por los conmutadores de la forma [a, b] con $a \in A$ y $b \in B$. Sea H un subgrupo de G; demostrar que H es normal en G si y sólo si [H, G] es un subgrupo de H.

16. Encontrar el subgrupo conmutador del grupo de los cuaterniones Q_8, descrito en el ejemplo D de la sección 5.5.

17. Demostrar que si G es un grupo no abeliano de orden p^3, con p primo, $G' = Z(G)$ (Usar el ejercicio 7 de la sección 4.6, el corolario 5.5.6 y un argumento similar al del ejemplo G de esta sección).

18. Sea $D_{2n} = \langle \{A, B: A^n = I, B^2 = I, AB = BA^{n-1}\} \rangle$ el grupo de las simetrías de un polígono regular de n lados. Demostrar que $(D_{2n})'$ es de índice 4 ó 2 en D_{2n} según que n sea par o impar.

19. Si $x, y, z \in G$ demostrar que $[x, yz] = [x, z](z^{-1}[x, y]z)$, y $[xy, z] = (y^{-1}[x, z]y)[y, z]$.

20. Encontrar los subgrupos conmutadores de S_4 y Alt(4). Encontrar la serie de los conmutadores de Alt(4).

21. Para cada par de elementos $x, y \in G$ demostrar que $[x, y] = [y, x]^{-1}$ y deducir de aquí que $[A, B] = [B, A]$ para cada par de subconjuntos A y B no vacíos de G (véase la definición de [A, B] en el ejercicio 15 de esta sección).

Los siguientes ejercicios han sido diseñados para poder demostrar que Alt(n) y S_n **no son solubles si** $n \geq 5$ sin necesidad de conocer que Alt(n) es simple en estos casos.

22. Sea $n \geq 5$ y N un subgrupo de S_n que contiene a los 3-ciclos $\alpha = (1\ 2\ 3)$ y $\beta = (1\ 4\ 5)$. Demostrar que (1 3 5) pertenece al subgrupo conmutador N' de N (Sugerencia: calcular $[\alpha, \beta]$).

23. Sea $n \geq 5$ y $\delta \in S_n$ tal que $\delta(1) = a$, $\delta(3) = b$ y $\delta(5) = c$. Demostrar que $\delta(1\ 3\ 5)\delta^{-1} = (a\ b\ c)$.

24. Sea G un grupo y N un subgrupo normal de G; demostrar que N', el subgrupo conmutador de N, es normal en G.

25. Sea N un subgrupo normal de S_n, $n \geq 5$, que contiene a todo 3-ciclo de S_n. Usar los tres problemas anteriores para deducir que el subgrupo conmutador N' de N contiene a todo 3-ciclo (a b c) de S_n.

26. i) Deducir del ejercicio 25 que si $n \geq 5$, los subgrupos conmutadores $(S_n)^{(k)}$, $k \geq 1$, de S_n contienen a todo 3-ciclo de S_n.
    ii) Deducir del resultado anterior que S_n y Alt(n) no son solubles si $n \geq 5$.

5.7. GRUPOS DE ORDEN PEQUEÑO

En las secciones anteriores hemos probado varios resultados acerca de la estructura de los grupos finitos. En el caso de los grupos abelianos conseguimos una clasificación completa en las secciones 5.3 y 5.4. En esta sección nos ayudaremos de los resultados que hemos obtenido anteriormente para describir, en algunos casos, todos los grupos de un cierto orden y, en otros, para descifrar el retículo de sus subgrupos. En todos los casos el orden del grupo no superará a 15, dejando para los ejercicios resultados acerca de algunos grupos de orden superior a este número.

Ya sabemos que todo grupo G de orden primo p es cíclico y por tanto abeliano. En este caso G es isomorfo a $(\mathbf{Z}_p, +)$ y el retículo de sus subgrupos se describe en la ilustración 5.

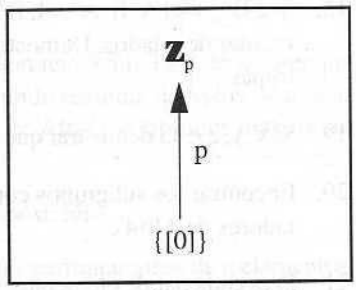


Ilustración 5. Retículo de $(\mathbf{Z}_p, +)$, p primo

Si el orden de G es pq, con p y q primos, $p < q$ y q no es congruente con 1 módulo p, G es cíclico y por tanto abeliano; esto se deduce de los teoremas de Sylow y está contenido en el corolario 5.5.16. Para los grupos de orden menor o igual que 15 esto sólo sucede si $|G| = 3 \cdot 5 = 15$ y por el teorema de clasificación de los grupos abelianos finitos G es isomorfo a $(\mathbf{Z}_{15}, +)$; el retículo de sus subgrupos se describe en la ilustración 6.

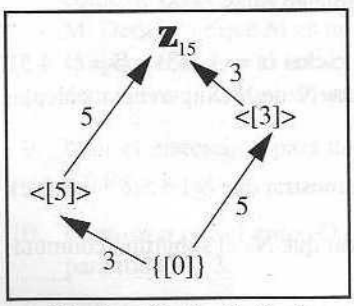


Ilustración 6. Retículo de $(\mathbf{Z}_{15}, +)$

Si el orden de G es p^2, con p primo, el corolario 5.5.7 muestra que G debe ser abeliano. Por tanto G es isomorfo a $\mathbf{Z}_p$ o a $\mathbf{Z}_p \times \mathbf{Z}_p$. Si el orden de G es menor o igual que 15 este resultado se aplica a $|G| = 4 = 2^2$ y $|G| = 9 = 3^2$. Los retículos de los subgrupos de $\mathbf{Z}_4$ y de $\mathbf{Z}_2 \times \mathbf{Z}_2$ son conocidos. Los de $\mathbf{Z}_9$ y $\mathbf{Z}_3 \times \mathbf{Z}_3$ se describen en la ilustración 7. Obsérvese que todo elemento de $\mathbf{Z}_3 \times \mathbf{Z}_3$ distinto del neutro ha de ser de orden 3.

Grupos de orden 6.

Conocemos dos grupos de orden 6: **el grupo abeliano** $\mathbf{Z}_6 \approx \mathbf{Z}_2 \times \mathbf{Z}_3$ y el grupo $S_3 \approx D_6$. Los retículos de sus subgrupos se indican en la ilustración 8.

Demostraremos a continuación que no hay, salvo isomorfismos, más subgrupos de orden 6. Sea G un grupo de orden $6 = 2 \cdot 3$. Por el tercer teorema de Sylow (véase el teorema 5.5.15) $n_3 = 1$ y $n_2 = 1$ ó 3. Si $n_2 = 1$, G tiene un subgrupo normal Q de orden 3 y otro subgrupo normal P de orden 2; por el teorema de Lagrange $Q \cap P = \{e\}$ y por el lema 5.5.13 $QP = G$; de la proposición 4.7.3, deducimos $G \approx Q \times P \approx \mathbf{Z}_3 \times \mathbf{Z}_2 \approx \mathbf{Z}_6$.

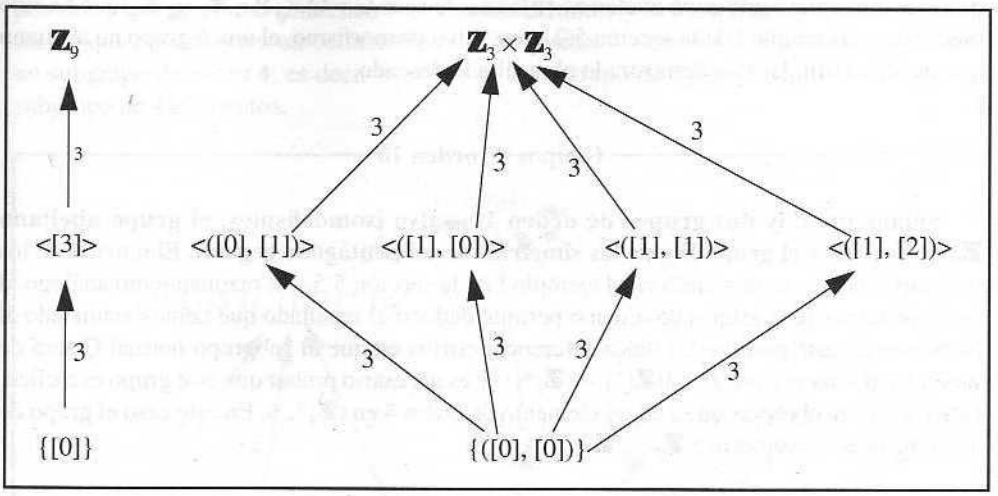


Ilustración 7. Retículos de $\mathbf{Z}_9$ y de $\mathbf{Z}_3 \times \mathbf{Z}_3$

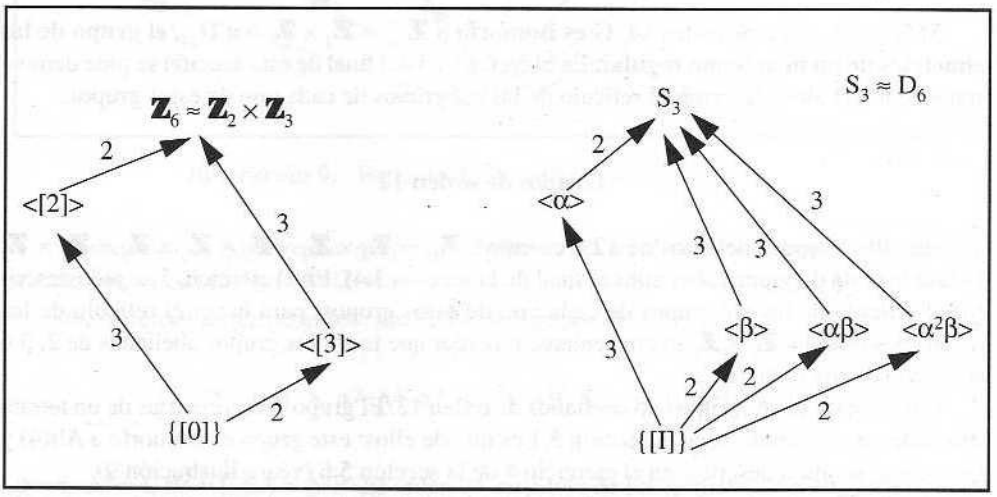


Ilustración 8. Retículos de $\mathbf{Z}_6 \approx \mathbf{Z}_2 \times \mathbf{Z}_3$ y de $S_3 \approx D_6$

Supongamos que $n_2 = 3$; sea Q un subgrupo normal de orden 3 de G ($n_3 = 1$) y P un subgrupo de orden 2, que no será normal en G. Por el teorema de Lagrange $Q \cap P = \{e\}$ y por el lema 5.5.13, $QP = G$. Por el teorema 5.2.7, G es isomorfo a $Q \times_\varphi P$ para algún homomorfismo φ: $P \to \text{Aut}(Q)$. Como $Q \approx \mathbf{Z}_3$, $\text{Aut}(Q) \approx I(\mathbf{Z}_3^*) \approx (\mathbf{Z}_3^*, \cdot) \approx (\mathbf{Z}_2, +)$, de acuerdo con el ejercicio 12 de la sección 5.2 y el 9 de la sección 4.2; por tanto Aut(Q) tiene un generador a de orden 2. Como P es de orden 2, $P = \langle y \rangle$ donde y es un elemento de orden 2. Como P solamente tiene dos subgrupos, $\{e\}$ y $P = \langle y \rangle$, solamente puede haber dos homomorfismos cuyos núcleos sean estos subgrupos. Uno es el homomorfismo φ_0, cuyo núcleo es P; por tanto, φ_0 es el trivial $\varphi_0(e) = \varphi_0(y) = I$; en este caso $G \approx Q \times P$ (véase el ejemplo G de la sección 5.2).

Sea φ el homomorfismo cuyo núcleo es $\{e\}$; en este caso $G \approx Q \times_\varphi P \approx \mathbf{Z}_3 \times_\varphi \mathbf{Z}_2$, que ha sido descrito en el ejemplo I de la sección 5.2, y es, salvo isomorfismo, el único grupo no abeliano que puede existir. Hemos demostrado el resultado deseado.

Grupos de orden 10

Solamente hay dos grupos de orden 10, salvo isomorfismos, el grupo abeliano $\mathbf{Z}_{10} \approx \mathbf{Z}_2 \times \mathbf{Z}_5$ y el grupo D_{10} de las simetrías de un pentágono regular. El retículo de los subgrupos de D_{10} se describió en el ejemplo I de la sección 5.5. Un razonamiento análogo al que realizamos para grupos de orden 6 permite deducir el resultado que hemos enunciado al comienzo de este párrafo. La única diferencia estriba en que el subgrupo normal Q será de orden 5 y por tanto $\mathrm{Aut}(Q) \approx I(\mathbf{Z}_5^*) \approx (\mathbf{Z}_5^*, \cdot)$ y es necesario probar que este grupo es cíclico. Para ello basta observar que 2 es un elemento de orden 4 en $(\mathbf{Z}_5^*, \cdot)$. En este caso el grupo de 10 elementos es isomorfo a $\mathbf{Z}_5 \times_\varphi \mathbf{Z}_2$.

Grupos de orden 14

Si G es un grupo de orden 14, **G es isomorfo a $\mathbf{Z}_{14} \approx \mathbf{Z}_2 \times \mathbf{Z}_7$ o a D_{14}, el grupo de las simetrías de un heptágono regular.** En el ejercicio 3 del final de esta sección se pide demostrar este resultado y describir el retículo de los subgrupos de cada uno de estos grupos.

Grupos de orden 12

Hay dos grupos abelianos de 12 elementos, $\mathbf{Z}_{12} \approx \mathbf{Z}_3 \times \mathbf{Z}_4$ y $\mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \approx \mathbf{Z}_6 \times \mathbf{Z}_2$ (véase la tabla de grupos abelianos al final de la sección 5.4). En el ejercicio 5 se pide describir el retículo de los subgrupos de cada uno de estos grupos; para hacer el retículo de los subgrupos de $\mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ es conveniente recordar que todos los grupos abelianos de 2, 3 ó 6 elementos son cíclicos.

Conocemos varios grupos no abelianos de orden 12. El grupo T de simetrías de un tetraedro dado en el ejemplo A de la sección 5.1 es uno de ellos; este grupo es isomorfo a Alt(4) y su retículo se pidió describir en el ejercicio 4 de la sección 5.6 (véase ilustración 9).

Otro es D_{12}, el grupo de las simetrías de un hexágono regular y otro, que no es isomorfo a ninguno de los anteriores, es $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$ que fue descrito en el ejemplo L de la sección 5.2.

Antes de describir los retículos de estos grupos hacemos una observación sobre los grupos de orden 12, que es una consecuencia de los teoremas de Sylow.

Proposición 5.7.1. Todo grupo G de orden 12 tiene o bien un sólo subgrupo de orden 4, que será normal en G, o bien un sólo subgrupo de orden 3 que será normal en G.

Demostración. Como $12 = 2^2 \cdot 3$, $n_2 \equiv 1(2)$ y divide a 3, por lo que n_2 puede ser 1 ó 3; de la misma manera $n_3 \equiv 1(3)$ y divide a 4, por lo que n_3 puede ser 1 ó 4. Si $n_3 = 1$ el 3-subgrupo de Sylow de G es normal y es un subgrupo de 3 elementos. Si $n_3 = 4$ tenemos cuatro 3-subgru-

pos de Sylow de G que contienen 8 elementos distintos y la identidad, que es el único elemento que pueden tener en común. Como sólo quedan 3 elementos, solamente puede haber un subgrupo de orden 4, es decir $n_2 = 1$, y el 2-subgrupo de Sylow es normal en G y es un subgrupo de 4 elementos. ■

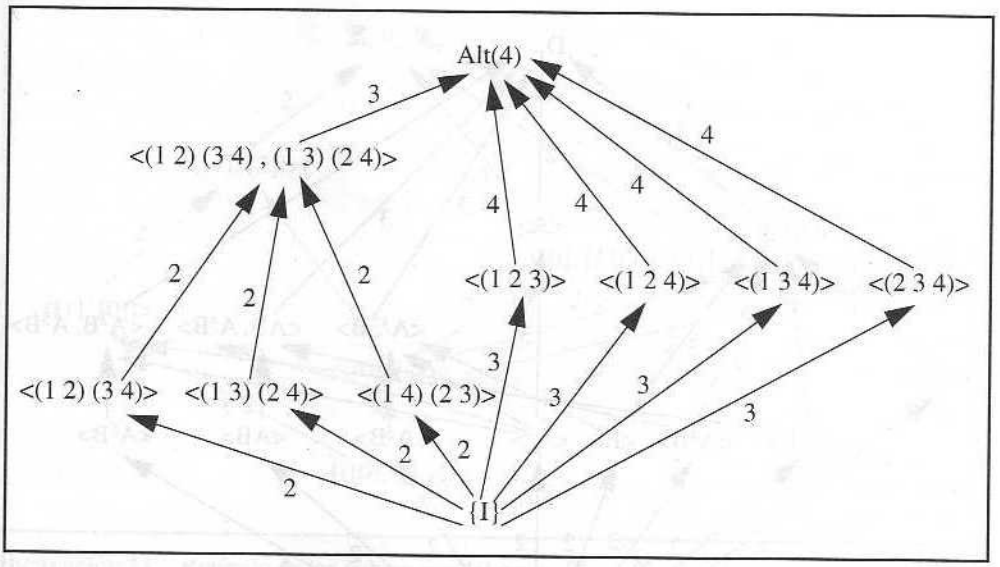


Ilustración 9. Retículo de los subgrupos de Alt(4)

Obsérvese que Alt(4) es un grupo de 12 elementos en el que sólo hay un subgrupo de 4 elementos, <(1 2) (3 4), (1 3) (2 4)>.

Intentaremos descifrar el retículo de los subgrupos de

$$D_{12} = \{I, A, A^2, A^3, A^4, A^5, B, AB, A^2B, A^3B, A^4B, A^5B\}$$

donde $A^6 = I$, $B^2 = I$, $BA = A^5B$. El orden de cada uno de los elementos de este grupo se describe en la tabla siguiente:

D_{12}	I	A	A^2	A^3	A^4	A^5	B	AB	A^2B	A^3B	A^4B	A^5B
Orden	1	6	3	2	3	6	2	2	2	2	2	2

Tenemos, por tanto, siete subgrupos de orden 2 y un subgrupo de orden 3, que es $\langle A^2 \rangle = \{I, A^2, A^4\}$. Por tanto $n_3 = 1$. Como D_{12} no es abeliano, $n_2 = 3$ (si $n_2 = 1$ tendríamos $G \approx \mathbf{Z}_3 \times \mathbf{Z}_4$) y, como no hay elementos de orden 4 en D_{12}, los tres subgrupos de orden 4 deben ser isomorfos al grupo de Klein. Esto ayuda a encontrar estos subgrupos. Hay, además, un subgrupo de 6 elementos, <A>, que tiene un subretículo lineal.

Finalmente tenemos el subgrupo $<A^2, B>$ que es de 6 elementos e isomorfo a S_3, por lo que su subretículo debe ser similar al de la derecha de la ilustración 8. El retículo de los subgrupos de D_{12} se describe en la ilustración 10.

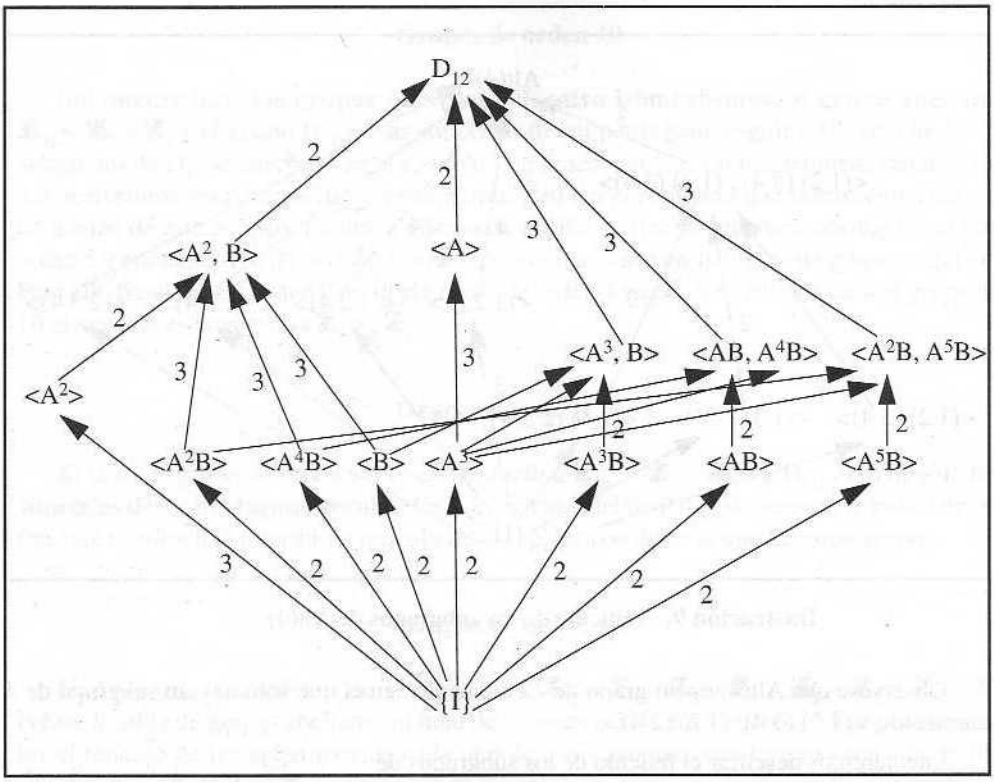


Ilustración 10. Retículo de los subgrupos de D_{12}, el grupo diédrico de las simetrías de un hexágono regular

Intentemos descifrar ahora el retículo de los subgrupos del grupo $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$ descrito en el ejemplo L de la sección 5.2. El orden de cada uno de sus elementos es:

$\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$	([0], [0])	([0], [1])	([0], [2])	([0], [3])	([1], [0])	([1], [1])	([1], [2])	([1], [3])	([2], [0])	([2], [1])	([2], [2])	([2], [3])
Orden	1	4	2	4	3	4	6	4	3	4	6	4

Como solamente hay dos elementos de orden 3, y ambos pertenecen al subgrupo generado por ([1], [0]) tenemos $n_3 = 1$. Por tanto $n_2 = 3$ ya que en caso contrario el grupo sería abeliano. Como solamente hay un elemento de orden 2, no puede haber ningún subgrupo isomorfo al grupo de Klein: los tres subgrupos de orden 4 serán cíclicos. Estos son $<([0], [1])>$, $<([1], [1])>$ y $<([2], [1])>$. Finalmente, sólo hay un subgrupo de orden 6, $<([2], [2])>$, que es

cíclico, ya que si hubiera otro subgrupo de orden 6 sería isomorfo a S_3 y necesitaríamos 3 elementos de orden 2, que no los hay en este grupo. El retículo de los subgrupos de $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$ se describe en la ilustración 11.

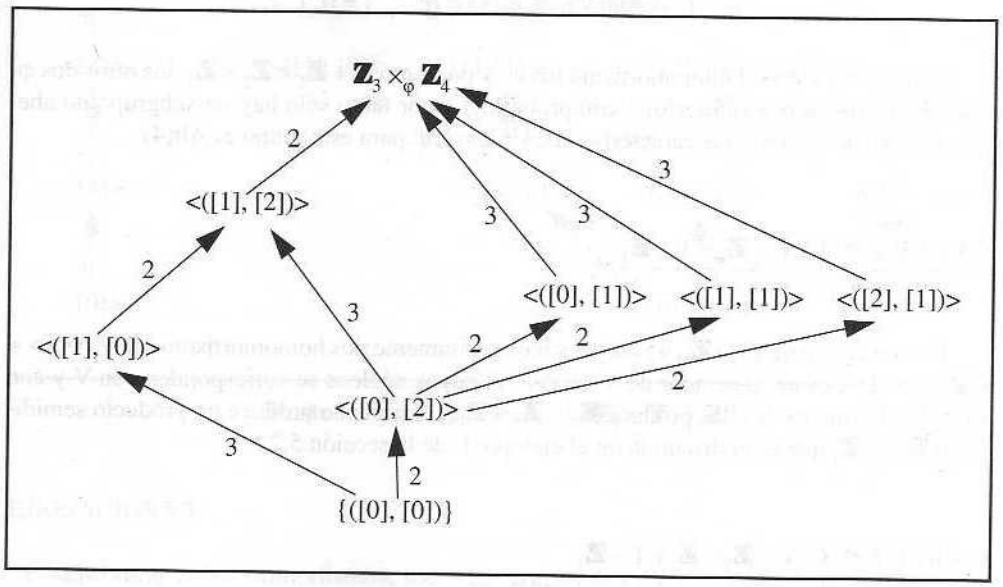


Ilustración 11. Retículo de los subgrupos del grupo $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$ descrito en el ejemplo L de la sección 5.2

Los descritos anteriormente son todos los grupos de 12 elementos, salvo isomorfismos. Esbozaremos la demostración de este resultado y dejaremos algunos detalles como ejercicios.

Sea G un grupo de 12 elementos, sea V un subgrupo de G de 4 elementos (un 2-subgrupo de Sylow de G) y T un subgrupo de G de 3 elementos (un 3-subgrupo de Sylow de G). Al menos uno de ellos es normal en G por la proposición 5.7.1. Además, $V \approx \mathbf{Z}_4$ o $V \approx \mathbf{Z}_2 \times \mathbf{Z}_2$ y $T \approx \mathbf{Z}_3$. Se pueden presentar varios casos que estudiaremos a continuación.

CASO 1: $V \lhd G$, $V \approx \mathbf{Z}_4$ y $T \approx \mathbf{Z}_3$

En este caso $\mathrm{Aut}(V) \approx (\mathbf{Z}_2, +)$ y solamente podemos tener el homomorfismo trivial de $T \approx \mathbf{Z}_3$ en Aut(V). En este caso $G \approx V \times T \approx \mathbf{Z}_4 \times \mathbf{Z}_3 \approx \mathbf{Z}_{12}$.

CASO 2: $V \lhd G$, $V \approx \mathbf{Z}_2 \times \mathbf{Z}_2$ y $T \approx \mathbf{Z}_3$

En este caso es más difícil obtener todos los automorfismos de V; se propone como ejercicio mostrar que $\mathrm{Aut}(V) \approx S_3$; por tanto solamente hay un subgrupo de orden 3 en Aut(V) y

supongamos que está generado por α. Si T = <y>, hay tres posibles homomorfismos de T en Aut(V), a saber

$$\varphi_i : T \to \mathrm{Aut}(V), \quad \varphi_i(y) = \alpha^i, \quad i = 0, 1, 2.$$

Con φ_0 se obtiene el homomorfismo trivial y por tanto $G \approx \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$; los otros dos φ_1 y φ_2 producen grupos isomorfos (¡comprobarlo!) y por tanto sólo hay un subgrupo no abeliano de orden 12 con estas características. Un modelo para este grupo es Alt(4).

CASO 3: $T \lhd G$, $V \approx \mathbf{Z}_4$ y $T \approx \mathbf{Z}_3$

En este caso $\mathrm{Aut}(T) \approx (\mathbf{Z}_2, +) = <\sigma>$ y hay exactamente dos homomorfismos de $V = <x> \approx \mathbf{Z}_4$, donde x es un generador de V, en Aut(T) cuyos núcleos se corresponden con V y con $\{e, x^2\}$. El primero de ellos produce $\mathbf{Z}_3 \times \mathbf{Z}_4 \approx \mathbf{Z}_{12}$; el segundo produce un producto semidirecto $\mathbf{Z}_3 \times_\varphi \mathbf{Z}_4$ que es el discutido en el ejemplo L de la sección 5.2.

CASO 4: $T \lhd G$, $V \approx \mathbf{Z}_2 \times \mathbf{Z}_2$ y $T \approx \mathbf{Z}_3$

En este caso $\mathrm{Aut}(T) \approx \mathbf{Z}_2 \approx <\sigma>$ y hay exactamente cuatro homomorfismos de $V \approx \mathbf{Z}_2 \times \mathbf{Z}_2$ en Aut(T) cuyos núcleos corresponden a V, {a}, {b} y {c} donde $V = \{e, a, b, c\}$, $a^2 = b^2 = e$, $ab = c$. El primero de ellos produce el homomorfismo trivial y genera $G \approx \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$. Los otros tres producen grupos isomorfos entre sí. Un modelo para ellos es D_{12}.

Grupos de orden 8

Como $8 = 2^3$ los teoremas de Sylow no producen mucha información. Esto sucede, en general, con todos los grupos cuyo orden es la potencia de un primo.

Hay tres grupos abelianos, no isomorfos entre sí, de 8 elementos: $\mathbf{Z}_8$, $\mathbf{Z}_4 \times \mathbf{Z}_2$ y $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$. El retículo de los subgrupos de $\mathbf{Z}_8$ es fácil de realizar; para hacer el retículo de los subgrupos de $\mathbf{Z}_4 \times \mathbf{Z}_2$ comprobar que este grupo tiene cuatro elementos de orden 4 y tres elementos de orden 2. Sus retículos se describen en la ilustración 12. En $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ todos los elementos, excepto el neutro, son de orden 2; describir gráficamente su retículo es complicado por la cantidad de flechas que se entrelazan.

Conocemos dos grupos no abelianos: el grupo diédrico D_8 de las simetrías de un cuadrado y el grupo Q_8 descrito en el ejemplo D de la sección 5.5. Estos son todos los grupos no abelianos de orden 8, salvo isomorfismos. El retículo de los subgrupos de Q_8 puede verse en el ejemplo que acabamos de mencionar y el de D_8 en la sección 4.5 (ilustración 6 en el ejemplo D).