Introducción a la Teoría de Grupos (UNED)

Pablo Pallàs

16 de septiembre de 2023

Índice

1. Grupos. Subgrupos. Índice de un subgrupo

1.1. Generalidades. Grupos

Empezaremos por el principio del todo, y como estamos en *Teoría de grupos* qué mejor forma de empezar que por una buena y sencilla definición de lo que son los grupos, los principales protagonistas de este libro.

Definición 1.1. *Un **grupo** es un conjunto no vacío G en el que está definida una operación binaria*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & ab \end{array}$$

que satisface:

1. *$(ab)c = a(bc)$ para cada terna de elementos a, b, c de G. Se dice que la operación es **asociativa**.*
2. *Existe un elemento $e \in G$ tal que*

$$ea = a = ae \quad \forall a \in G.$$

3. *Para cada elemento $a \in G$ existe un $x \in G$ tal que*

$$ax = e = xa.$$

*Diremos que ab es el **producto** de a por b.*

Veamos algunas observaciones respecto a la definición:

Observación 1.1.1. *El elemento e de la segunda condición de la definición anterior es único, ya que si existiese otro e' que verificara esa condición tendríamos*

$$ee' = e' = e'e$$

$$e'e = e = ee'$$

y así $e' = e'e = e$.

*Se dice que e es el **elemento neutro de** G. Usualmente lo denotaremos por 1_G, y si no hay posible confusión con el grupo en el que estemos trabajando simplemente escribiremos 1.*

Observación 1.1.2. *Si la operación en G la notamos por $(a,b) \longmapsto a+b$, entonces la denominaremos **suma** y al elemento neutro 0_G o simplemente 0.*

Observación 1.1.3. *Para cada $a \in G$, el elemento x de la tercera condición es único puesto que si $y \in G$ cumpliese también esa condición tendríamos:*

$$ax = e = xa,$$

$$ay = e = ya.$$

En particular $ax = ay$, luego $x(ax) = x(ay)$, y por la propiedad asociativa $(xa)x = (xa)y$, esto es, $ex = ey$ y así $x = y$.

Al único elemento $x \in G$ que cumple

$$ax = e = xa$$

le denominaremos ***inverso*** *de a y lo notamos por a^{-1}. Nótese que si $a \in G$, como $aa^{-1} = 1_G = a^{-1}a$, a es el inverso de a^{-1}, es decir,*

$$(a^{-1})-1 = a.$$

Por último, apuntar que cuando la operación en G sea la suma escribiremos $-a$ en vez de a^{-1} y se denominará ***opuesto*** *de a.*

Proposición 1.2 (***Simplificación***)**.** *Sean $a, b, c \in G$. Entonces:*

1. *Si $ab = ac$, entonces $b = c$.*
2. *Si $ba = ca$, entonces $b = c$.*

Demostración. Si $ab = ac$, se tiene $a^{-1}(ab) = a^{-1}(ac)$ y así $(a^{-1}a)b = (a^{-1}a)c$, esto es, $b = 1b = 1c = c$. Análogamente con $ba = ca$.

□

Proposición 1.3 (***Asociatividad generalizada***)**.** *Los productos que se obtienen al variar las formas de asociar n elementos $a_1, \ldots, a_n$ de un grupo G, conservando el orden, son iguales. Denotaremos cualquiera de esos productos por $a_1 \ldots a_n$.*

Demostración. Probaremos esto por inducción sobre n. Los casos $n = 1, 2$ son evidentes. Supongamos $n > 2$. Debemos demostrar que, si $1 < k < l < n$,

$$(a_1 \ldots a_k)(a_{k+1} \ldots a_n) = (a_1 \ldots a_l)(a_{l+1} \ldots a_n).$$

Sean $a = a_1 \ldots a_k$, $b = a_{k+1} \ldots a_l, c = a_{l+1} \ldots a_n$. Por la hipótesis de inducción,

$$a_1 \ldots a_l = (a_1 \ldots a_k)(a_{k+1} \ldots a_l) = ab,$$

$$a_{k+1} \ldots a_n = (a_{k+1} \ldots a_l)(a_{l+1} \ldots a_n) = bc.$$

Así, lo que inicialmente queríamos probar equivale a probar que

$$a(bc) = (ab)c,$$

lo cual es cierto por la propiedad asociativa.

□

En particular, esto nos permite dar la siguiente definición:

Definición 1.4. *Dado un elemento $a \in G$, y un natural n, definimos la* ***potencia n-ésima*** *de a*

$$a^n = a \underbrace{\ldots}_{n} a.$$

Y para completar la definición consideraremos $a^0 = 1$, $a^{-n} = (a^{-1})^n$.

Además, la ley de asociatividad generalizada nos permite deducir, con $m, n \in \mathbb{Z}$ y $a \in G$,

$$a^m a^n = a^{m+n},$$
$$(a^m)^n = a^{mn}.$$

Proposición 1.5. *Dados elementos $a_1, \ldots, a_n$ en un grupo G se tiene*

$$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$

Demostración. Lo probaremos por inducción. Si $n = 1$, es evidente. Si $n > 1$, usando la asociatividad generalizada

$$(a_1 \ldots a_n)(a_n^{-1} \ldots a_1^{-1}) = (a_1 \ldots a_{n-1})(a_n a_n^{-1})(a_{n-1}^{-1} \ldots a_1^{-1}) =$$
$$(a_1 \ldots a_{n-1})(a_{n-1}^{-1} \ldots a_1^{-1}) = \ldots = 1 = \ldots = (a_n^{-1} \ldots a_2^{-1})(a_2 \ldots a_n) =$$
$$(a_n^{-1} \ldots a_2^{-1})(a_1^{-1} a_1)(a_2 \ldots a_n) = (a_n^{-1} \ldots a_1^{-1})(a_1 \ldots a_n)$$

□

Ejemplo 1.5.1. *Veamos algunos ejemplos:*

1. *Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ con la suma usual son grupos cuyo neutro es el número cero.*
2. *Los conjuntos $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ obtenidos a partir de $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ quitando el número cero, son grupos con el producto. Sin embargo, no ocurre así con $\mathbb{Z}^*$ ya que no contiene a los inversos.*
3. *Si X es un conjunto no vacío, el conjunto $Biy(X)$, formado por las aplicaciones $X \longrightarrow X$ que son biyectivas, es un grupo con la operación composición de aplicaciones, cuyo elemento neutro es la aplicación identidad:*

$$\begin{array}{rccc} 1_X\colon & X & \longrightarrow & X \\ & x & \longmapsto & x. \end{array}$$

   Esto se puede comprobar fácilmente: si $f, g \in Biy(X)$ entonces $(f \circ g)(X) = f(g(X)) = f(X) = X$, lo que prueba la sobreyectividad. Para la inyectividad, si x, y son elementos distintos de X, la inyectividad de g nos dice que $g(x) \neq g(y)$, y la de f permite concluir que $f(g(x)) \neq f(g(y))$, y así $f \circ g$ también es inyectiva.

■

Definición 1.6 (***El grupo simétrico*** S_n)**.** *Cuando el conjunto X es finito con n elementos, escribiremos S_n en vez de $Biy(X)$. Este grupo tiene $n!$ elementos, ya que si $X = \{a_1, \ldots, a_n\}$ entonces para definir un elemento en S_n tenemos n posibles valores como imágenes de a_1, $n-1$ valores como imagen de a_2 (pues al ser biyecciones las imágenes de a_1 y a_2 deben ser distintas) y, en general, $n-i$ posibles valores como imagen de a_{i+1}, con $i = 0, \ldots, n-1$, por lo que el número de elementos de S_n es*

$$n(n-1)\ldots 3 \cdot 2 \cdot 1 = n!.$$

Ejemplo 1.6.1. *Más ejemplos:*

1. *El conjunto $GL(\mathbb{R})_n$ formado por las matrices de orden n con coeficientes en $\mathbb{R}$ cuyo determinante es no nulo forma un grupo con la operación producto de matrices, con elemento neutro la matriz identidad de orden n, I_n, y cuyos únicos coeficientes no nulos son los de la diagonal principal, que valen uno.*

   De hecho, de la fórmula

   $$det(A \cdot B) = det(A) \cdot det(B)$$

   se deduce en particular que el producto es una operación binaria en $GL(\mathbb{R})_n$ y por otro lado, sabemos ya que las matrices con determinante nulo no tienen inversa.

2. *(**Grupo diédrico**) Sea $n \geq 3$ un número natural y X el polígono regular de n lados, con vértices $a_1, \ldots, a_n$.*

   *Decimos que una biyección $f\colon X \longrightarrow X$ **conserva la distancia** si $d(a,b) = d(f(a), f(b))$ para cada $a, b \in X$. Así, llamaremos n**-ésimo grupo diedral** o **grupo diédrico de orden** n al conjunto*

   $$D_n = \{f \in Biy(X) : f \text{ conserva la distancia}\}.$$

   En efecto, es inmediato comprobar que $\mathcal{D}_n$ con la operación composición es un grupo:

   - *La asociatividad de D_n se desprende de la asociatividad de $Biy(X)$.*
   - *La aplicación identidad $1_X \in \mathcal{D}_n$ (que claramente conserva la distancia) constituye el elemento neutro de $\mathcal{D}_n$.*
   - *Por último, sea $h \in \mathcal{D}_n$, y $h^{-1} \in Biy(X)$ la aplicación inversa. Para ver que h posee inversa en $\mathcal{D}_n$ basta comprobar que $h^{-1} \in \mathcal{D}_n$, es decir, que h^{-1} conserva la distancia. Veámoslo:*

   Sean $a, b \in X$, $p = h^{-1}(a)$, $q = h^{-1}(b)$. Así, $h(p) = a$, $h(q) = b$, y como h conserva la distancia:

   $$d(a,b) = d(h(p), h(q)) = d(p,q) = d(h^{-1}(a), h^{-1}(b)).$$

Si $f \in \mathcal{D}_n$ y p es un punto situado en el segmento que une a_i con a_{i+1}, se cumple

$$d(a_i, a_{i+1}) = d(a_i, p) + d(p, a_{i+1}),$$

luego

$$d(f(a_i), f(a_{i+1})) = d(f(a_i), f(p)) + d(f(p), f(a_{i+1})).$$

Por lo que $f(p)$ pertenece al segmento que une $f(a_i)$ con $f(a_{i+1})$. Como f transforma X en X se deduce de lo anterior que envía lados en lados, y por ello, al ser un vértice un punto común a dos lados, la imagen por f de un vértice de X es otro vértice de X.

Por lo tanto, si $V = \{a_1, \ldots, a_n\}$, $f|_V \in Biy(V)$.

Además, cada $f \in \mathcal{D}_n$ queda determinada por las imágenes $f(a_1), \ldots, f(a_n)$ de los vértices, pues dado un $p \in X$, estará entre dos vértices consecutivos a_i y a_{i+1}, luego $f(p)$ es el único punto del segmento que une $f(a_i)$ con $f(a_{i+1})$, que dista de éstos lo mismo que p dista de a_i y a_{i+1}.

Por lo tanto, la aplicación $f \longrightarrow f|_V$ entre $\mathcal{D}_n$ y $S_n = Biy(V)$ es inyectiva. Así que podemos identificar a $\mathcal{D}_n$ ***como un subconjunto de*** *S_n.*

Ahora calculemos los elementos que tiene $\mathcal{D}_n$. Si $f \in \mathcal{D}_n$ y $f(a_1) = a_i$, necesariamente será $f(a_2) = a_{i-1}$ ó a_{i+1}, $f(a_3) = a_{i-2}$ ó a_{1+2}, etc. pues f conserva la distancia. En consecuencia, por cada elección de la imagen de a_1 (y hay sólo n posibles imágenes) tenemos dos modos, a lo sumo, de elegir imagen para el resto de vértices. Por lo tanto,

$$|\mathcal{D}_n| \leq 2n.$$

Veamos que se da la igualdad, y cuáles son exactamente los elementos de $\mathcal{D}_n$.

Si 0 es el centro del polígono X, el giro f de centro 0 y ángulo $2\pi/n$ es claro que pertenece a $\mathcal{D}_n$ y f^n es la identidad. Por lo que

$$\{1_X = f^n, f, f^2, \ldots, f^{n-1}\} \subseteq \mathcal{D}_n,$$

y estos elementos son distintos ya que $f^i = f^j$, con $1 \leq i < j \leq n$ implicaría que

$$1_X = f^{-j} \circ f^i = f^{-i} \circ f^j = f^{j-i},$$

y así

$$a_1 = 1_X(a_1) = f^{j-i}(a_1) = a_{j-i+1},$$

y esto es absurdo.

Por otro lado, la simetría g respecto de la recta que une 0 con a_1, es también kelemento de $\mathcal{D}_n$ pues conserva la distancia y $g(a_1) = a_1$, $g(a_i) = a_{n-i+2}$, con $2 \leq i \leq n$.

Así que componiendo con las potencias de f, tenemos

$$\{g, g \circ f, \ldots, g \circ f^{n-1}\} \subseteq \mathcal{D}_n,$$

y si añadimos lo que ya teníamos

$$\{1_X, f, f^2, \ldots, f^{n-1}, g, g \circ f, \ldots, g \circ f^{n-1}\} \subseteq \mathcal{D}_n.$$

Veamos ahora que todos los elementos son distintos. Si $g \circ f^i = g \circ f^j$*, con* $1 \leq i < j \leq n$*, tendríamos*

$$f^i = f^j,$$

que ya hemos visto que es falso. Por otro lado, si $g \circ f^i = f^j$*, con* $1 \leq i < j \leq n$ *implicaría*

$$g = f^{j-i},$$

y así

$$a_1 = g(a_1) = f^{j-i}(a_1) = a_{j-i+1},$$

luego $j-i+1 = 1$ *y* $j-i = 0$*,* $g = f^0 = 1_X$*. Entonces* $a_n = g(a_2) = 1_X(a_2) = a_2$*, por lo que* $n = 2$*, y esto es imposible.*

Al probar que son distintos queda definida la igualdad y así

$$\mathcal{D}_n = \{1_X, f, f^2, \ldots, f^{n-1}, g, g \circ f, \ldots, g \circ f^{n-1}\} \text{ y } |\mathcal{D}_n| = 2n.$$

Es por ello que suele escribirse como $\mathcal{D}_{2n}$*. Más adelante se dará una descripción alternativa a este grupo.*

■

Definición 1.7. *Diremos que un grupo* G *es* ***abeliano*** *o* ***conmutativo*** *si* $ab = ba$ *para cada par de elementos* $a, b \in G$*.*

Es claro que los grupos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la suma y los grupos $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con el producto son grupos abelianos.

En particular, todo grupo con dos elementos es claramente abeliano, ya que uno de esos dos elementos tiene que ser necesariamente el elemento neutro, y el otro, denotémoslo por a, cumplirá claramente que $ea = ae$ y $aa = aa$.

Proposición 1.8. *Para* $n \geq 3$*,* S_n *no es abeliano.*

Demostración. En efecto, sea $X = \{1, 2, \ldots, n\}$ y $S_n = Biy(X)$. Sean f, g elementos de S_n definidos tal que así:

$$f(1) = 2, f(2) = 3, f(3) = 1, f(k) = k, k \geq 4$$

$$g(1) = 2, g(2) = 1, g(k) = k, k \geq 3.$$

Como $(g \circ f)(3) = g(1) = 2$, y $(f \circ g)(3) = f(3) = 1$ tenemos que $g \circ f \neq f \circ g$ y S_n no es abeliano.

□

Proposición 1.9. *Para* $n \geq 2$*,* $GL_n(\mathbb{R})$ *no es abeliano.*

Demostración. En efecto, la matriz $A = (a_{ij})$ dada por

$$a_{ij} = \begin{cases} 1 & si\ i \leq j \\ 0 & si\ i > j \end{cases}$$

pertenece a $GL_n(\mathbb{R})$ pues $det(A) = 1 \neq 0$. Como $detA^t = detA$, $A^t \in GL_n(\mathbb{R})$. Ahora,

$$AA^t = \left(\begin{array}{c|c} n & * \\ \hline * & * \end{array}\right), \quad A^tA = \left(\begin{array}{c|c} 1 & * \\ \hline * & * \end{array}\right),$$

con lo que $AA^t \neq A^tA$.

□

Proposición 1.10. *Si $n \geq 3$, D_n no es abeliano.*

Demostración. Si f y g son el giro y la simetría en D_n vistos en el segundo ejemplo de 1.6.1 tenemos que

$$(g \circ f)(a_1) = g(a_2) = a_n \neq a_2 = f(a_1) = (f \circ g)(a_1).$$

□

Veamos otras caracterizaciones de los grupos abelianos:

Proposición 1.11. *Sea G un grupo.*

1. *Si $x^2 = 1$ para cada $x \in G$, G es abeliano.*
2. *Si $(ab)^2 = a^2b^2$ para cada $a, b \in G$, G es abeliano.*

Demostración. Veámoslo por partes:

1. Para cada $x \in G$ se tiene que $x^2 = x \cdot x = 1 = x \cdot x^{-1}$, luego $x = x^{-1}$. Así, sean $a, b \in G$, entonces $a = a^{-1}, b = b^{-1}$ y

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ab.$$

2. Sean $a, b \in G$, entonces

$$a(ba)b = (ab)^2 = a^2b^2 = aabb = a(ab)b.$$

Así, se tiene que $ab = ba$.

□

Definición 1.12 (***Producto directo***)**.** *Sean G y G' dos grupos, cuyas operaciones notaremos por*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & ab \end{array}$$

$$\begin{array}{ccc} G' \times G' & \longrightarrow & G \\ (a', b') & \longmapsto & a'b' \end{array}$$

El producto cartesiano $G'' = G \times G'$ es un grupo con la operación

$$\begin{array}{ccc} G'' \times G'' & \longrightarrow & G \\ ((a, a'), (b, b')) & \longmapsto & (ab, a'b'). \end{array}$$

La asociatividad en G'' es consecuencia inmediata de la asociatividad en G y G' y de que la operación en G'' se ha definido elemento a elemento. Evidentemente, el elemento $1''_G = (1_G, 1'_G)$ es el neutro en G''.

Por último, como

$$(a, b')(a^{-1}, b'^{-1}) = (aa^{-1}, b'b'^{-1}) = (1_G, 1'_G) = 1''_G$$

$$(a^{-1}, b'^{-1})(a, b') = (a^{-1}a, b'^{-1}b') = (1_G, 1'_G) = 1''_G,$$

el elemento (a^{-1}, b'^{-1}) es el inverso, en G'', de (a, b').

Notar además que si G y G' son abelianos, también lo es G''. Recíprocamente, si G'' es abeliano, dados $a, b \in G$ se tiene que

$$(a, 1'_G)(b, 1'_G) = (b, 1'_G)(a, 1'_G)$$

y así $ab = ba$, luego G abeliano. Análogo con G'.

En general, dados grupos $G_1, \ldots, G_r$, definimos por recurrencia

$$G_1 \times \ldots \times G_r = (G_1 \times \ldots \times G_{r-1}) \times G_r.$$

*Y diremos que $G_1 \times \ldots \times G_r$ es el **producto directo** de los grupos $G_1, \ldots, G_r$.*

1.2. Subgrupos

Definición 1.13. *Un subconjunto no vacío H de un grupo G es un **subgrupo** de G si con la misma operación de G es un grupo.*

Proposición 1.14. *Sea H un subgrupo de un grupo G, entonces:*

1. *1_G pertenece a H y es su elemento neutro.*
2. *Si $x \in H$, también $x^{-1} \in H$.*

Demostración. Veamos:

1. Por definición H tiene un elemento neutro al que llamamos e. Desde luego, $ee = e$. Sea $e^{-1} \in G$ el inverso de e en G. Así, operando en G tenemos que $e^{-1}(ee) = e^{-1}e = 1_G$, luego $(e^{-1}e)e = 1_G$ y así $1_G e = 1_G$, o sea, $e = 1_G$.
2. Si $x \in H$ entonces existe $y \in H$ tal que $xy = 1_G = yx$, ya que sabemos que 1_G es el elemento neutro de H. Así, $xx^{-1} = xy$ y aplicando la propiedad cancelativa $x^{-1} = y \in H$.

□

La siguiente proposición es la que se suele usar como caracterización usual de los subgrupos.

Proposición 1.15. *Sea H un subconjunto no vacío de un grupo G. Las siguientes condiciones son equivalentes:*

1. *H es un subgrupo de G.*
2. *Para cada par de elementos $x, y \in H$, $xy^{-1} \in H$.*

Demostración. Veamos:

1. $\Rightarrow$ 2. Dados dos elementos $x, y \in H$, sabemos que entonces $y^{-1} \in H$. El producto es una operación binaria en H, porque H es subgrupo. Así, como $x, y^{-1} \in H$, se sigue que $xy^{-1} \in H$.

2. $\Rightarrow$ 1. Sea $x \in H$ (existe ya que H es no vacío). Ahora, si tomamos $y = x$ tenemos que $xx^{-1} \in H$ y así $1_G \in H$, luego H tiene elemento neutro. Ahora, dado un $y \in H$, si tomamos $x = 1_G \in H$, tenemos que $y^{-1} = 1_G y^{-1} = xy^{-1} \in H$ luego cada elemento de H tiene inverso en H. Finalmente, dados $x, y \in H$ ya sabemos que $z = y^{-1} \in H$, luego $xy = x(y^{-1})^{-1} = xz^{-1} \in H$ y así la operación de G es una operación binaria de H. La asociatividad es evidente, pues lo es para cada terna de elementos de G.

□

Notar que en la proposición se ha usado la notación multiplicativa, en el caso de que estuviésemos usando una aditiva sería $x - y \in H$ en lugar de $xy^{-1} \in H$.

Observación 1.15.1. *Evidentemente, $\{1_G\}$ y G son subgrupos de cualquier grupo G. Llamaremos* ***subgrupos propios*** *de G a aquellos subgrupos distintos de $\{1_G\}$ y G.*

Ejemplo 1.15.1. *Los subgrupos de $\mathbb{Z}$ son de la forma*

$$m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$$

para cada entero no negativo m.

Desde luego $m\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$, pues es no vacío ya que $m = m1 \in m\mathbb{Z}$, y si $a = mx$, $b = my$ pertenecen a $m\mathbb{Z}$, $a - b = mx - my = m(x - y) \in m\mathbb{Z}$. Por 1.15 $m\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$.

Recíprocamente, sea H un subgrupo de $\mathbb{Z}$. Si H consta sólo del número cero, $H = 0\mathbb{Z}$ tiene la forma requerida. Si H tiene algún elemento no nulo, tiene necesariamente alguno positivo ya que $x^{-1} \in H$ para un $x \in H$. Si m es el menor entero positivo en H, cualquier otro $n \in H$ positivo será

$$n = qm + r, \quad 0 \leq r < m.$$

Como $qm = m\underbrace{+\ldots+}_{q}m \in H$, $r = n - qm \in H$ *y es menor que* m, *luego por la elección de* m, *no es positivo. Así,* $r = 0$ *y por lo tanto* $n = qm = mq \in m\mathbb{Z}$. *Igualmente, si* $n \in H$ *es negativo,* $-n \in H$ *es positivo, luego* $-n = mx \in m\mathbb{Z}$ *para algún entero* x. *Así,* $n = m(-x) \in m\mathbb{Z}$. *Como también* $0 = m0 \in m\mathbb{Z}$, *tenemos que* $H \subseteq m\mathbb{Z}$. *Pero como* $m \in H$ *también* $-m \in H$, *y así para cada* $x \in \mathbb{Z}$ *tenemos:*

$$mx = \begin{cases} m\underbrace{+\ldots+}_{x}m \in H & si\ x > 0 \\ 0 \in H & si\ x = 0 \\ (-m)\underbrace{+\ldots+}_{x}(-m) \in H & si\ x < 0 \end{cases}$$

con lo que $H = m\mathbb{Z}$.

■

Ejemplo 1.15.2. *Para cada* $n \geq 3$, D_n *es subgrupo de* S_n. *De hecho, vimos en 1.5.1 que* $D_n \subseteq S_n$ *y que* D_n *es grupo con la misma operación (composición de aplicaciones) que* S_n.

■

Uno de los modos habituales de construir grupos es:

Definición 1.16. *Si* S *es un subconjunto no vacío de un grupo* G, *el conjunto*

$$\langle S\rangle = \{s_1^{h_1} \ldots s_n^{h_n} : n \in \mathbb{N}, s_i \in S, h_i \in \mathbb{Z}, 1 \leq i \leq n\}$$

es un subgrupo de G *que contiene a* S, *llamado* ***subgrupo generado por*** S.

Observación 1.16.1. *Dado* S *un subconjunto no vacío de un grupo* G, *entonces,*

$$\langle S\rangle = \{x_1 \ldots x_m : m \in \mathbb{N}, x_i \in S,\ \acute{o}\ x_i^{-1} \in S, 1 \leq i \leq m\}.$$

Además, si $\mathcal{F}_S$ *es la familia de todos los subgrupos de* G *que contienen a* S,

$$\langle S\rangle = \bigcap_{H \in \mathcal{F}_S} H.$$

En particular, $\langle S\rangle \subseteq H$ *para cada* $H \in \mathcal{F}_S$.

Demostración. Cada $s \in S$ se escribe $s = s^1 \in \langle S\rangle$. Esto prueba que $S \subseteq \langle S\rangle$. En particular $\langle S\rangle$ es no vacío, por no serlo S.

Dados $x = s_1^{h_1} \ldots s_n^{h_n}$, $y = t_1^{l_1} \ldots t_m^{l_m}$, con $x, y \in \langle S\rangle$. Como $y^{-1} = t_m^{-l_m} \ldots t_1^{-l_1}$ tenemos

$$xy^{-1} = s_1^{h_1} \ldots s_n^{h_n} t_m^{-l_m} \ldots t_1^{-l_1} \in \langle S\rangle.$$

Queda probado así que $\langle S\rangle$ es un subgrupo de G.

Ahora, dado $x = x_1 \ldots x_m, m \in \mathbb{N}$, $x_i \in S$ ó $x_i^{-1} \in S$, consideramos, para cada $1 \leq i \leq n$

$$s_i = \begin{cases} x_i & si\ x_i \in S \\ x_i^{-1} & si\ x_i^{-1} \in S \end{cases}$$

$$h_i = \begin{cases} 1 & si\ x_i \in S \\ -1 & si\ x_i^{-1} \in S \end{cases}$$

Evidentemente, para cada $1 \leq i \leq n$, $s_i \in S$, $s_i^{h_i} = x_i$. Así, $x = s_1^{h_1} \dots s_n^{h_n} \in \langle S \rangle$, luego

$$\{x_1 \dots x_m : m \in \mathbb{N}, x_i \in S,\ ó\ x_i^{-1} \in S, 1 \leq i \leq m\} \subseteq \langle S \rangle.$$

Recíprocamente, sea $x = s_1^{h_1} \dots s_n^{h_n} \in \langle S \rangle$, $n \in \mathbb{N}$, $s_i \in S$, $h_i \in \mathbb{Z}$, $1 \leq i \leq n$. Como $s_i^0 = 1$, podemos suponer que cada $h_i \neq 0$. Consideremos, para cada $1 \leq i \leq n$,

$$l_i = \begin{cases} h_i & si\ h_i > 0 \\ -h_i & si\ h_i < 0 \end{cases}$$

y fijado i pongamos para cada $1 \leq k \leq l_i$,

$$x_{ki} = \begin{cases} s_i & si\ h_i > 0 \\ s_i^{-1} & si\ h_i < 0 \end{cases}$$

Desde luego, para cada $1 \leq i \leq n$, $1 \leq k \leq l_i$, bien $x_{ki} \in S$ (si $h_i > 0$), bien $x_{ki}^{-1} = s_i \in S$ (si $h_i < 0$). Además, $s_i^{h_i} = x_{1i} \dots x_{l_i i}$, $1 \leq i \leq n$, luego

$$x = x_{11} \dots x_{l_1 1} \dots x_{1n} \dots x_{l_n n}$$

pertenece a $\{x_1 \dots x_m : m \in \mathbb{N}, x_i \in S,\ ó\ x_i^{-1} \in S, 1 \leq i \leq m\} \subseteq \langle S \rangle$, y así tenemos la igualdad.

Finalmente, ya sabemos que $\langle S \rangle \in \mathcal{F}_S$, de donde

$$\bigcap_{H \in \mathcal{F}_S} H \subseteq \langle S \rangle.$$

Para probar la igualdad bastará pues ver que $\langle S \rangle \subseteq H$ para cada $H \in \mathcal{F}_S$. Dado $x = s_1^{h_1} \dots s_n^{h_n} \in \langle S \rangle$, cada $s_i \in S \subseteq H$ y al ser H subgrupo, también $s_i^{hi} \in H$, de donde $x \in H$.

□

Definición 1.17. *Un caso particular pero muy importante es aquel en el que $S = \{a\}$ para algún $a \in G$. En tal caso escribiremos $\langle a \rangle$ en vez de $\langle \{a\} \rangle$. Es claro que*

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

y se le llama ***subgrupo generado por*** *a.*

Definición 1.18. *Un subconjunto no vacío S de un grupo G se llama* ***sistema generador*** *de G si $G = \langle S \rangle$.*

Como el menor subgrupo de G que contiene a G es el propio G, deducimos que $\langle G \rangle = G$, luego G es un sistema generador de G.

Ejemplo 1.18.1. *En el caso del grupo diédrico tenemos que*

$$D_n = \{1, f, \ldots, f^{n-1}, g, g \circ f, \ldots, g \circ f^{n-1}\}$$

y así $D_n = \langle S \rangle$*, con* $S = \{f, g\}$*.*

■

Definición 1.19. *Un grupo* G *que posee un sistema finito de generadores diremos que es* ***finitamente generado****. Así, todo grupo finito* G *es finitamente generado porque, tal y como se ha visto,* G *es un sistema generador de* G*.*

Sin embargo, el recíproco en general no es cierto. Por ejemplo, el grupo $\mathbb{Z}$ de los números enteros está generado por $\{1\}$, ya que, dado un $n \in \mathbb{Z}$,

$$n = \begin{cases} 1\underbrace{+\ldots+}_{n}1 & si\ n > 0 \\ (-1)\underbrace{+\ldots+}_{n}(-1) & si\ n < 0 \end{cases}$$

Sin embargo, es claro que $\mathbb{Z}$ no es finito.

Observación 1.19.1. *Aunque obvio, lo siguiente es con frecuencia útil. Y es que dado un grupo* G*, y dos subconjuntos* S *y* S' *de* G*, para que los subgrupos* $H = \langle S \rangle$ *y* $K = \langle S' \rangle$ *coincidan es suficiente que* $S \subseteq K$ *y* $S' \subseteq H$*, pues en tal caso si* $x \in H$ *será de la forma* $x = s_1 \ldots s_m$*, con* $s_i \in S \subseteq K$*, luego como* K *es subgrupo,* $x \in K$ *y hemos probado* $H \subseteq K$*.*

Recíprocamente, cada $x \in K$ *se escribe como* $x = s'_1 \ldots s'_n$*, con* $s'_i \in S' \subseteq H$*, luego* $x \in H$*, es decir,* $K \subseteq H$*.*

Definición 1.20. *Si* H *es un subgrupo de* G*, llamaremos* ***centralizador*** *de* H *en* G *a*

$$C_G(H) = \{x \in G : ax = xa \ \ \forall a \in H\}.$$

Al centralizador de G *en* G *lo denotaremos por* $Z(G)$ *y se le denominará* ***centro*** *de* G*. Evidentemente*

$$Z(G) = \{x \in G : ax = xa \ \ a \in G\},$$

y por lo tanto G *es abelianos si y sólo si* $G = Z(G)$*.*

Observación 1.20.1. *El centro es un subgrupo de* G*. De hecho,* $C_G(H)$ *es subgrupo de* G*.*

Demostración. Como $1_G \in C_G(H)$, éste no es vacío. Sean $x, y \in C_G(H)$, $a \in H$. Como $x \in C_G(H)$, $ax = xa$. Como $y \in C_G(H)$, $a^{-1} \in H$, $a^{-1}y = ya^{-1}$. Por lo tanto,

$$a(xy^{-1}) = (ax)y^{-1} = (xa)y^{-1} = x(ay^{-1}) = x(ya^{-1})^{-1} = x(a^{-1}y)^{-1} = x(y^{-1}a) = (xy^{-1})a$$

luego $xy^{-1} \in C_G(H)$. Así, $C_G(H)$ es un subgrupo de G.

□

Observación 1.20.2. *En el caso particular de que $H = \langle a \rangle$ para algún $a \in G$, entonces $x \in C_G(H)$ si y sólo si $xa = ax$.*

Demostración. En efecto, el sólo si es obvio, pues $a \in H$. Para probar el si tenemos que ver que $ax = xa$ implica $a^k x = xa^k$ para cada $k \in \mathbb{Z}$.

Lo haremos por inducción sobre k. Si $k = 1$ no hay nada que probar. Si $k > 1$,

$$a^k x = a(a^{k-1}x) = a(xa^{k-1}) = (ax)a^{k-1} = (xa)a^{k-1} = xa^k$$

donde hemos usado la hipótesis de inducción en la segunda y cuarta igualdades. Antes de abordar el caso $k < 0$, observemos que de $ax = xa$ se deduce $a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$, luego $xa^{-1} = a^{-1}x$. Ahora, si $k = -l < 0$, con $l \in \mathbb{N}$, probaremos por inducción sobre l que $(a^{-1})^l x = x(a^{-1})^l$, de donde $a^k x = xa^k$. Para $l = 1$ no hay nada que probar, y si $l > 1$ $(a^{-1})^l x = a^{-1}(a^{-1})^{l-1}x = a^{-1}x(a^{-1})^{l-1} = xa^{-1}(a^{-1})^{l-1} = x(a^{-1})^l$.

□

Con esto, tenemos

$$C_G(\langle a \rangle) = \{x \in G : ax = xa\}.$$

Por eso se suele esccribir $C_G(a)$ en lugar de $C_G(\langle a \rangle)$. Evidentemente es claro que $Z(G) = \cap_{a \in G} C_G(a)$. Además

Observación 1.20.3. *$a \in Z(G)$ si y sólo si $C_G(a) = G$.*

Demostración. Si $a \in Z(G)$ cada $x \in G$ cumple $ax = xa$, luego $G \subseteq C_G(a) \subseteq G$. Recíprocamente, si $C_G(a) = G$ cada $x \in G$ pertenece a $C_G(a)$, luego $ax = xa$ para cada $x \in G$ y así $a \in Z(G)$.

□

Proposición 1.21. *Si S es un subconjunto no vacío de un grupo G y $a \in G$, llamaremos **conjugado de** S **por** a al conjunto*

$$S^a = \{a^{-1}xa : x \in S\}.$$

Además, es claro que $y \in S^a$ si y sólo si $aya^{-1} \in S$.

Propiedades 1.21.1. *Algunas propiedades del conjugado son:*

1. *Se tiene que*

$$\begin{array}{ccc} S & \longrightarrow & S^a \\ x & \longmapsto & a^{-1}xa \end{array}$$

es biyectiva.

2. $(S^a)^b = S^{ab}$ *para cualesquiera* $a, b \in G$.

3. $S = S^1$.

4. *Si* S *es subgrupo de* G, *también lo es* S^a.

5. *Si* $S \subseteq T$, *entonces* $S^a \subseteq T^a$.

Demostración. Veamos:

1. Basta ver la inyectividad. Pero si $a^{-1}xa = a^{-1}ya$, se sigue que $xa = ya$ y de aquí $x = y$.

2. Como $z \in (S^a)^b$ equivale a $z = b^{-1}yb$, $y \in S^a$ y esto es lo mismo que $z = b^{-1}yb$, $y = a^{-1}xa$, con $x \in S$ entonces
$$z = b^{-1}(a^{-1}xa)b = (b^{-1}a^{-1})x(ab) = (ab)^{-1}x(ab) \in S^{ab}.$$

3. Simplemente, si $x \in S$, entonces $1^{-1}x1 = 1x1 = x$.

4. Cuando S es subgrupo, $1 \in S$ y así $a^{-1}1a \in S^a$, esto es, $1 \in S^a$. Así, S^a es no vacío. Además, dados $u, v \in S^a$ serán $u = a^{-1}xa$, $v = a^{-1}ya$ para algunos $x, y \in S$, y por lo tanto $uv^{-1} = a^{-1}xa(a^{-1}ya)^{-1} = a^{-1}xaa^{-1}y^{-1}a = a^{-1}xy^{-1}a \in S^a$ por ser S subgrupo de G (y así $xy^{-1} \in S$).

5. Si $x \in S^a$ tenemos que $axa^{-1} \in S \subseteq T$, luego $x \in T^a$.

□

Definición 1.22. *Si* S *es un subconjunto no vacío de un grupo* G, *llamaremos* ***normalizador*** *de* S *en* G *a*
$$N_G(S) = \{a \in G : S^a = S\},$$
que además es un subgrupo de G.

Demostración. Veamos que es subgrupo. Ya sabemos que $S = S^1$, luego $1 \in N_G(S)$ y así $N_G(S)$ es no vacío. Por otro lado, si $a, b \in N_G(S)$ tenemos $S^{ab^{-1}} = (S^a)^{b^{-1}} = S^{b^{-1}}$ ya que $a \in N_G(S)$. Como $S = S^1 = S^{bb^{-1}} = (S^b)^{b^{-1}} = S^{b^{-1}}$, ya que $b \in N_G(S)$, tenemos entonces que
$$S^{ab^{-1}} = S,$$
y así $ab^{-1} \in N_G(S)$.

□

Observación 1.22.1. *Si* $\{H_i : i \in I\}$ *es una familia no vacía de subgrupos de un grupo* G, *entonces*
$$H = \bigcap_{i \in I} H_i$$
es un subgrupo de G. *Además, para cada* $a \in G$ *se tiene que*
$$H^a = \bigcap_{i \in I} H_i^a.$$

Demostración. Esto es así puesto que $1 \in H$ y si $x, y \in H$ se sigue que $x, y \in H_i$ para cada $i \in I$ y así $xy^{-1} \in H_i$, por ser H_i subgrupo, para cada $i \in I$. Por lo tanto, $xy^{-1} \in H$.

Para lo segundo, si $x \in H^a$ entonces $axa^{-1} \in H$, luego $axa^{-1} \in H_i$ para cada $i \in I$, o lo que es lo mismo, $x \in H_i^a$ para cada $i \in I$. Así, $H^a \subseteq \cap_{i\in I} H_i^a$. Recíprocamente, si $x \in \cap_{i\in I} H_i^a$ se tiene que $x \in H_i^a$ para todo $i \in I$, o sea, $axa^{-1} \in H_i$ para todo $i \in I$ y así

$$axa^{-1} \in \bigcap_{i\in I} H_i = H,$$

de donde $x \in H^a$. Esto prueba $\cap_{i\in I} H_i^a \subseteq H^a$ y así la igualdad.

□

Definición 1.23 (***Grupo producto***)**.** *Dados dos subgrupos H y K de un grupo G, definimos*

$$HK = \{hk : h \in H, k \in K\}.$$

Sin embargo, este producto no se suele comportar muy bien. En general, el producto de subgrupos no será subgrupo, para que lo sea tendrá que ocurrir lo siguiente:

Proposición 1.24. *HK es subgrupo de G si y sólo si $HK = KH$. Es claro que $H \subseteq HK$, $K \subseteq HK$.*

Demostración. Supongamos que HK es subgrupo de G. Si $x = hk \in HK$ entonces $k^{-1}h^{-1} = x^{-1} \in HK$, luego $k^{-1}h^{-1} = uv$ con $u \in H$, $v \in K$ y así $x = hk = (k^{-1}h^{-1})^{-1} = (uv)^{-1} = v^{-1}u^{-1} \in KH$ y esto prueba $HK \subseteq KH$. Sea ahora $y = kh \in KH$. Entonces $z = h^{-1}k^{-1} \in HK$, y como HK es subgrupo $y = kh = (h^{-1}k^{-1})^{-1} = z^{-1} \in HK$, y así $KH \subseteq HK$.

Recíprocamente, supongamos que $HK = KH$. Evidentemente HK es no vacío, pues $1 = 1 \cdot 1 \in HK$. Además, dados $x = h_1k_1$, $y = h_2k_2$, con $x, y \in HK$,$xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1k_3h_2^{-1}$, con $k_3 = k_1k_2^{-1} \in K$. Como $k_3h_2^{-1} \in KH = HK$, $k_3h_2^{-1} = h_3k$, con $h_3 \in H$, $k \in K$. Así, $xy^{-1} = h_1h_3k = hk \in HK$, con $h = h_1h_3 \in H$.

□

Ejemplo 1.24.1 (***Identidad de Bézout***)**.** *Sean m y n enteros no negativos, $H = m\mathbb{Z}$, $K = n\mathbb{Z}$ dos subgrupos de $\mathbb{Z}$. Como $\mathbb{Z}$ es abeliano es obvio que $H+K = K+H$, luego por el resultado anterior $H + K$ es subgrupo de $\mathbb{Z}$ (notar que aquí la operación es la suma).*

$H + K$ no es el subgrupo $\{0\}$ pues, $m = m + 0 \in H + K$. Y, como ya sabemos, existirá un $d \in \mathbb{Z}$ tal que $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, veamos que $d = mcd(m, n)$:

Como $m = m+0 \in m\mathbb{Z}+n\mathbb{Z} = d\mathbb{Z}$, d divide a m, y como $n = 0+n \in m\mathbb{Z}+n\mathbb{Z} = d\mathbb{Z}$, d divide a n. Además $d \in d\mathbb{Z} = m\mathbb{Z}+n\mathbb{Z}$ luego existen $a, b \in \mathbb{Z}$, tal que $d = ma+nb$. Entonces, dado un c que divida a m y n:

$$m = cu,\ n = cv, u, u \in \mathbb{Z}$$

tenemos $d = (cu)a+(cv)b = c(ua+vb)$ *y* c *divide a* d*. Esto prueba que* $d = mcd(m, n)$*.*

En particular, dos números enteros m, n *son primos entre sí si y sólo si*

$$1 = am + bn \;\; a, b \in \mathbb{Z}.$$

En efecto, si $mcd(m, n) = 1$*, es* $m\mathbb{Z}+n\mathbb{Z} = 1\mathbb{Z}$ *por lo visto ahora. Así,* $1 \in m\mathbb{Z}+n\mathbb{Z}$ *y existirán* $a, b \in \mathbb{Z}$ *tales que* $1 = am + bn$*. Recíprocamente, si* $1 = am + bn$ *y* d *es un divisor de* m *y* n*, tendremos* $m = du$*,* $n = dv$*, luego* $1 = d(au + bv)$ *y así* $d = +1$ *ó* -1*. Y como podemos asumir que* $mcd(m, n)$ *es positivo entonces* $mcd(m, n) = 1$*.*

■

Observación 1.24.1. *Dados dos subgrupos* H *y* K *de un grupo* G *tales que* $H \subseteq K$ *se tiene* $HK = K = KH$*.*

En efecto, cada $x \in HK$ *se escribe como* $x = hk$*, con* $h \in H \subseteq K$ *y* $k \in K$ *y así* $HK = KH \subseteq K$*. Recíprocamente, cada* $k \in K$ *es de la forma* $k = 1 \cdot k \in HK$*, y así* $K \subseteq HK$*. Análogo con* KH*.*

Otra noción importante de un grupo es el número de elementos que tiene, su cardinal si lo vemos como conjunto. Aunque no es exactamente lo mismo, veremos que en algunos grupos podremos tener todos los elementos que queramos pero el orden no será infinito, como es el caso de los *grupos cíclicos*. Además, también vamos a ver cómo extender este concepto a un sólo elemento cualquiera de un grupo G cualquiera, y tendrá una íntima relación con el subgrupo que genera.

1.3. Orden de un grupo

Definición 1.25. *Sea* G *un grupo. Al número de elementos de un subgrupo finito* H *de* G *se le llama* ***orden*** *de* H *y lo notaremos por* $o(H)$*. En particular, cuando* G *es finito, el número de elementos de* G *se llama orden de* G*. En caso contrario, diremos que* G *es un grupo infinito.*

Un elemento $a \in G$ *se llama de* ***torsión*** *si el subgrupo* $\langle a \rangle$ *es finito. En tal caso llamaremos* ***orden de*** a *y lo denotaremos por* $o(a)$ *al orden del subgrupo* $\langle a \rangle$*.*

Es decir, hemos definido también el orden de un elemento como $o(a) = o(\langle a \rangle)$.

Ejemplo 1.25.1. *Tanto* $\mathbb{Z}$ *como todos sus subgrupos son grupos infinitos. Sin embargo, para cada* $n \geq 2$*,* $o(S_n) = n!$ *y, para cada* $n \geq 3$*,* $o(D_n) = 2n$*.*

■

Veamos algunas propiedades interesantes del orden y algunos resultados importantes:

Proposición 1.26. *Sea* G *un grupo y* $a \in G$ *un elemento de torsión (su subgrupo generado es finito). Entonces:*

1. *Existe* $k \geq 1$ *tal que* $a^k = 1$*.*
2. *El orden de* a *es el menor natural* $n \geq 1$ *tal que* $a^n = 1$
3. *Si* $n = o(a)$*, entonces* $\langle a \rangle = \{1, a, \cdots, a^{n-1}\}$*.*

4. *Si $n = o(a)$ y $k \in \mathbb{N}$, $a^k = 1$ si y sólo si k es múltiplo de n.(n divide a m).*
5. *$o(a) = 1$ si y sólo si $a = 1$.*
6. *a^{-1} es un elemento de torsión y $o(a^{-1}) = o(a)$.*
7. *Si $x = a^k \in \langle a \rangle$ y $o(a) = n$, x es de torsión y*

$$o(x) = \frac{n}{mcd(n,k)}.$$

8. *Si $b \in G$ es otro elementos de torsión y $ab = ba$, entonces ab es de torsión y $o(ab)$ es un divisor del $mcm(o(a), o(b))$, con mcm el mínimo común múltiplo.*
9. *En el punto anterior, si $o(a)$ y $o(b)$ son primos entre sí, $o(ab) = o(a)o(b)$.*
10. *Si $b \in G$ y ab es de torsión, también lo es ba, y $o(ab) = o(ba)$.*

Demostración. Lo veremos por partes:

1. Como $\langle a \rangle$ es finito, la aplicación

$$\begin{array}{ccc} \mathbb{N}\backslash\{0\} & \longrightarrow & \langle a \rangle \\ m & \longmapsto & a^m \end{array}$$

no es inyectiva. Así, existen $r < s \in \mathbb{N}$ tales que $a^r = a^s$. Si $k = s - r$, $1 = a^0 = a^r a^{-r} = a^s a^{-r} = a^{s-r} = a^k$.

2. Sea n el menor natural que cumple $a^n = 1$, cuya existencia se deduce de lo que acabamos de demostrar en el punto anterior. Si probamos que

$$\langle a \rangle = \{1, a, \ldots, a^{n-1}\}$$

y que todos los elementos del miembro de la derecha son distintos, entonces tendremos que $o(a) = n$. Evidentemente el elemento de la izquierda de la igualdad contiene al de la derecha. Recíprocamente, si $x = a^k$, $k \in \mathbb{Z}$, dividimos por n y por el algoritmo de la división sabemos que:

$$k = qn + r,\ 0 \leq r \leq n - 1,$$

luego $x = a^{qn+r} = (a^n)^q a^r = 1^q a^r = a^r$, $0 \leq r \leq n - 1$. Por último, si existieran $0 \leq r < s \leq n - 1$ tales que $a^r = a^s$, sería $a^{s-r} = a^s a^{-r} = a^r a^{-r} = a^0 = 1$, $s - r \leq n - 1 < n$, pero esto es absurdo porque hemos definido a n como el menor natural poitivo tal que $a^n = 1$.

3. Queda demostrado con lo visto en el punto anterior.

4. Si $k = nm$ es múltiplo de n, $a^k = a^{nm} = (a^n)^m = 1$. Recíprocamente, si k no es múltiplo de n, $k = nm + r$, $1 \leq r \leq n - 1$, luego $a^k = a^{nm+r} = (a^n)^m a^r = 1^m a^r = a^r \neq 1$ por 2.

5. Si $o(a) = 1$, $a = a^1 = 1$ por 2. Recíprocamente, como $1^1 = 1$, $o(1) = 1$.

6. $\langle a\rangle = \langle a^{-1}\rangle$ puesto que $a^k = (a^{-1})^{-k}$ para cada entero k. Así, $o(a)$ = número de elementos de $\langle a\rangle$ = número de elementos de $\langle a^{-1}\rangle = o(a^{-1})$ y a^{-1} es de torsión.

7. Como $x = a^k$ cada elemento $y = a^l$ de $\langle x\rangle$ cumple que $y = (a^k)^l = a^{kl} \in \langle a\rangle$, luego $\langle x\rangle \subseteq \langle a\rangle$ es finito y así x es de torsión.

   Sea ahora $d = mcd(n,k)$. Como d divide a k, tenemos $k = ed$, para algún $e \in \mathbb{Z}$. Así, $x^{n/d} = a^{kn/d} = a^{ne} = (a^n)^e = 1^e = 1$ luego n/d es múltiplo de $o(x)$. Por otro lado, $a^{ko(x)} = (a^k)^{o(x)} = x^{o(x)} = 1$ y así $ko(x)$ es múltiplo de n. Entonces, podemos expresar $ko(x) = nm$ para un cierto $m \in \mathbb{Z}$, esto es,

   $$k = m\frac{n}{o(x)},\ \textit{es decir}\ ,\frac{n}{o(x)}\ \textit{divide a}\ k.$$

   Como evidentemente $n/o(x)$ divide a n, $n/o(x)$ divide a $d = mcd(n,k)$, es decir, $ln/o(x) = d$ para algún $l \in \mathbb{Z}$. En consecuencia, $ln/d = o(x)$ y así $o(x)$ también es múltiplo de n/d. Por lo tanto, $o(x) = n/d$.

8. Sean $n = o(a), m = o(b)$, $M = pn = qm$, $p,q \in \mathbb{N}$, $M = mcm(m,n)$. Como $ab = ba$, tenemps

   $$(ab)^M = a^M b^M = (a^n)^p (b^m)^q = 1^p 1^q = 1$$

   y $o(ab)$ divide a M por lo que vimos en el punto 4.

9. Como $o(a) = n$ y $o(b) = m$ son primos entre sí, el mínimo común múltiplo de m y n es $M = nm$. Por el punto 8. $o(ab)$ divide a nm. Llamemos s al orden de ab. Así, $(ab)^s = 1$ y como $ab = ba$, $a^s b^s = (ab)^s = 1$, luego $a^s = b^{-s}$. En particular, $o(a^s) = o(b^{-s}) = o((b^s)^{-1}) = o(b^s)$ donde para la último igualdad se ha utilizado el punto 6. Ahora, por 7.,

   $$\frac{n}{mcd(n,s)} = o(a^s) = o(b^s) = \frac{m}{mcd(m,s)}.$$

   Así,

   $$d = \frac{n}{mcd(n,s)} = \frac{m}{mcd(m,s)}\ \textit{divide a}\ m\ \textit{y a}\ n,$$

   luego $d = 1$, es decir, $n = mcd(n,s)$, $m = mcd(m,s)$. Entonces, s es múltiplo de n y de m, luego lo es de $M = nm$. Con esto hemos probado que $o(ab) = s = nm = o(a)o(b)$.

10. Sea $n = o(ab)$. Tendremos $a(ba)^{n-1}b = a(baba...ba)b = (ab)^n = 1$, luego $(ba)^{n-1}b = a^{-1}$, $(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$, de donde $(ba)^n = (ba)^{n-1}ba = (ba)^{-1}ba = 1$, y así el orden de ba divide al de ba. Cambiando los papeles de a y b obtenemos que el orden de ab divide al de ba, luego $o(ab) = o(ba)$.

□

Ejemplo 1.26.1. *Sea $n \geq 3$ y D_n el correspondiente grupo diédrico. Con lo que sabemos, sean $f, g \in D_n$, el giro de ángulo $2\pi/n$ y una simetría respecto de una*

recta. Si $V = \{a_1, \ldots, a_n\}$ *son los vértices del polígono regular de* n *lados, vimos que* $g(a_1) = a_1$ *y* $g(a_i) = a_{n-i+2}$*, con* $2 \leq i \leq n$ *(es decir,* g *es la simetría). Como* $g(a_2) = a_n \neq a_2$*, entonces* $g \neq 1$ *y así* $o(g) > 1$*. Además,* $g^2(a_1) = g(a_1) = a_1$ *y* $g^2(a_i) = g(a_{n-i+2}) = a_{n-(n-i+2)+2} = a_i$*, con* $2 \leq i \leq n$*, luego* $g^2 = 1$ *y así* $o(g) = 2$*.*

En cuanto a f *(el giro), ya sabemos que* $f^n = 1$ *y que* $f^i \neq 1$ *si* $1 \leq i < n$*. Por ello,* $o(f) = n$*.*

■

1.4. Índice de un subgrupo y Teorema de Lagrange

Definición 1.27. *Sea* G *un grupo y* H *un subgrupo de* G*. Llamaremos* R_H *y* R^H *a las siguientes relaciones en* G*:*

$$xR_Hy \text{ si y sólo si } xy^{-1} \in H$$
$$xR^Hy \text{ si y sólo si } x^{-1}y \in H$$

Tanto R_H como R^H son relaciones de equivalencia.

Demostración: Lo haremos para R_H (para R^H es análoga). Tenemos que ver que cumplen con la propiedad *reflexiva* (1), *simétrica* (2) y *transitiva* (3)

(1). Si $x \in G$, $xx^{-1} = 1 \in H$ luego xR_Hx.

(2). Si xR_Hy entonces $xy^{-1} \in H$, luego

$$(xy^{-1})^{-1} \in H,$$

y esto es $yx^{-1} \in H$ así que yR_Hx.

(3). Si xR_Hy, y yR_Hz, entonces,

$$xy^{-1} \in H, \;\; yz^{-1} \in H$$

y así

$$xz^{-1} = (xy^{-1})(yz^{-1}) \in H$$

por lo que xR_Hz.

□

Notar que en las propiedades anteriores se ha tenido en cuenta, y esto resulta de gran importancia, que H es subgrupo.

La demostración era bastante sencilla y casi evidente. El haber definido estas relaciones de equivalencia nos va a permitir estudiar las clases que éstas mismas generan para llegar a unos conjuntos especiales que llamaremos *coclases* ó *clases laterales*. En ocasiones se hace al revés, primero se presentan las coclases y a partir de ahí estudiamos (normalmente en sus demostraciones) las relaciones que definen.

Si $x \in G$, la clase de equivalencia de x respecto de R_H es

$$Hx = \{hx : h \in H\}.$$

En efecto, $y \in G$ está relacionado con x mediante R_H si y sólo si $yx^{-1} = h \in H$, esto es, si $y = hx \in Hx$.

De igual modo, $y \in G$ está relacionado con x mediante R^H si y sólo si $x^{-1}y = h \in H$, o sea, si $y = xh \in xH$.

Proposición 1.28. *La aplicación entre los conjuntos cocientes*

$$\begin{array}{ccc} G/R_H & \longrightarrow & G/R^H \\ Hx & \longmapsto & x^{-1}H \end{array}$$

es biyectiva

Demostración. Veamos primero que está bien definida. Si $Hx = Hy$ tenemos que xR_Hy, y así $xy^{-1} \in H$, luego $(x^{-1})^{-1}y^{-1} \in H$ y así $x^{-1}R^Hy^{-1}$, es decir, $x^{-1}H = y^{-1}H$.

La inyectividad se prueba de modo análogo: si $Hx \neq Hy$ entonces $xy^{-1} \notin H$, luego $(x^{-1})^{-1}y^{-1} \notin H$, es decir, x^{-1} e y^{-1} no están relacionados mediante R^H, y por ello $x^{-1}H \neq y^{-1}H$.

Como cada clase yH de G/R^H es la imagen de Hy^{-1} es claro que también es sobreyectiva.

□

Definición 1.29. *Decimos que H es un subgrupo de G de **índice infinito** si G/R_H (y por ello G/R^H) es un conjunto infinito.*

*Cuando G/R_H es finito, llamamos **índice** de H en G, y lo denotamos $[G : H]$, al número de elementos de G/R_H (que además coincide con el de G/R^H). Es decir, definimos el índice como el número de coclases a derecha (o a izquierda porque es el mismo). En este caso decimos que H es un subgrupo de G de índice finito o que tiene índice finito en G. Por tanto tenemos que*

$$[G : H] = card(G/R_H) = card(G/R^H).$$

Además es claro que si G tiene orden finito, como la aplicación

$$\begin{array}{ccc} G & \longrightarrow & G/R_H \\ x & \longmapsto & Hx \end{array}$$

es sobreyectiva, todo subgrupo de G es de índice finito.

Una consecuencia bastante clara de todo esto es que $[G : 1] = o(G)$ $(= |G|)$ y $[G : H] = 1$ si y sólo si $G = H$.

Ejemplo 1.29.1. *Veamos cómo se relacionan los subgrupos de $\mathbb{Z}$ con el mismo $\mathbb{Z}$ a través de sus respectivos índices:*

Sea $G = \mathbb{Z}$ y $\{0\} \neq H$ un subgrupo de $\mathbb{Z}$. Ya sabemos que H es de la forma $H = m\mathbb{Z}$, con m un entero positivo cualquiera. Como la operación en $\mathbb{Z}$ es la suma, las clases respecto de R_H serán de la forma

$$H + x = m\mathbb{Z} + x,\ x \in \mathbb{Z}.$$

Veamos que

$$\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z} + 0, m\mathbb{Z} + 1, \ldots, m\mathbb{Z} + (m-1)\}.$$

Dado $x \in \mathbb{Z}$ obtenemos, por el algoritmo de la división,

$$x = qm + r,\ 0 \leq r \leq m - 1.$$

Así $x - r = qm \in m\mathbb{Z} = H$, luego xR_Hr, es decir, $m\mathbb{Z} + x = m\mathbb{Z} + r$, lo que prueba la igualdad. Además los elementos del segundo miembro son distintos, pues si $m\mathbb{Z} + k = m\mathbb{Z} + l$, $0 \leq k < l \leq m - 1$, entonces lR_Hk, y por tanto $l - k \in m\mathbb{Z} = H$, $1 \leq l - k < m$, y tenemos que $l - k = qm$, con $q \in \mathbb{Z}$, lo cual implicaría que $l = qm + k > m$ si $q > 0$ ó $k = l - qm > m$ si $q < 0$ (y así $-q > 0$), lo cual es imposible.

Así, $[\mathbb{Z} : m\mathbb{Z}] = m$. Notar que $\mathbb{Z}$ es un grupo infinito cuyos subgrupos no nulos tienen índice finito.

■

Observación 1.29.1. *Si G es un grupo, H un subgrupo de G y $x \in G$, las aplicaciones*

$$\begin{array}{ccc} H & \longrightarrow & Hx \\ h & \longmapsto & hx \end{array}$$

$$\begin{array}{ccc} H & \longrightarrow & xH \\ h & \longmapsto & xh \end{array}$$

son biyectivas. La inyectividad se deduce de las leyes de simplificación que vimos al principio, mientras que la sobreyectividad es obvia.

Observación 1.29.2. *De la observación anterior deducimos que, dado un $x \in G$, existe una biyección entre Hx y xH. Sin embargo, Hx y xH pueden ser distintos (de hecho normalmente así será). Consideremos por ejemplo $G = D_n$ para algún $n \geq 3$, y con las notaciones vistas en 1.6.1*

$$H = \langle g \rangle, x = f.$$

Como $o(g) = 2$ tal y como vimos en 1.26.1, $H = \{1, g\}$, luego $Hf = \{f, g \circ f\}$, $fH = \{f, f \circ g\}$. Y en 1.10 vimos que $f \circ g \neq g \circ f$, luego $Hf \neq fH$.

Teorema 1.30 (***Teorema de Lagrange***)**.** *Sean G un grupo y H un subgrupo de G. Son equivalentes:*

1. *G es finito.*
2. *$o(H)$ es finito y H tiene índice finito en G.*

En tal caso, $o(G) = o(H) \cdot [G : H]$. En particular, el orden de H y el índice de H en G dividen al orden de G.

Demostración. Veámoslo por doble implicación:

1. $\Rightarrow$ 2. Como

$$\begin{array}{ccc} H & \longrightarrow & G \\ x & \longmapsto & x \end{array}$$

es inyectiva la finitud de G implica la de H, y por 1.29 también lo es G/R_H.

2. $\Rightarrow$ 1. Como R_H es relación de equivalencia, G es unión *disjunta* de las clases de equivalencia como ya sabemos. Así, recordamos que

$$|G| = o(G) = \sum_{Hx \in G/R_H} card\,(Hx).$$

Ahora, por 1.29.1, $card\,(Hx) = card\,(H) = o(H)$, luego

$$o(G) = o(H) \cdot card\, G/R_H = o(H) \cdot [G : H],$$

y así G es finito, y se tiene la conocida *fórmula de Lagrange*.

□

Como consecuencia inmediata se tiene que si G grupo y H subgrupo de G son finitos, y es importante recalcar esto, entonces

$$[G : H] = \frac{|G|}{|H|}.$$

Observación 1.30.1. *Sean G un grupo finito, $n = o(G)$ y $a \in G$. Entonces a es elemento de torsión y $a^n = 1$.*

Demostración. Como $\langle a \rangle \subseteq G$, $\langle a \rangle$ es finito, luego a es de torsión. Si $m = o(a) = o(\langle a \rangle)$, el *teorema de Lagrange* nos dice que $n = mp$, con $p \in \mathbb{N}$. Así, $a^n = a^{mp} = (a^m)^p = 1^p = 1$.

□

Una consecuencia sencilla pero útil del *teorema de Lagrange* es la siguiente:

Corolario 1.30.1. *Si H y K son subgrupos finitos de un grupo G con $o(H) = m$, $o(K) = n$ y $mcd(m, n) = 1$, entonces $H \cap K = \{1_G\}$.*

Demostración. $H \cap K$ es subgrupo de H y de K, luego $o(H \cap K)$ debe dividir a m y n. Como $mcd(m, n) = 1$, entonces $o(H \cap K) = 1$ y así $H \cap K = \{1_G\}$.

□

Proposición 1.31 (***Transitividad del índice***)**.** *Sean G un grupo y H y K subgrupos de G tales que $H \subseteq K$. Entonces:*

1. *H es subgrupo de K*
2. *Si el índice de H en G es finito lo son también el índice de K en G y el de H en K, y*
$$[G : H] = [G : K] \cdot [K : H] .$$

Esta propiedad se conoce como transitividad del índice.

Demostración. La primera afirmación es consecuencia obvia de las definiciones. Sea ahora
$$\begin{array}{rccc} \pi\colon & G/R_H & \longrightarrow & G/R_K \\ & Hx & \longmapsto & Kx \end{array}$$
Está bien definida, ya que si $Hx = Hy$ entonces $xy^{-1} \in H \subseteq K$, y así xR_Ky y tenemos $Kx = Ky$.

Como evidentemente es sobreyectiva,
$$G/R_H = \bigcup_{Kx \in G/R_K} \pi^{-1}(Kx).$$

Además esta unión es claramente disjunta.

Notamos también por R_H la restricción de R_H a K. Nótese que la condición $Hy \in \pi^{-1}(Kx)$ equivale a decir que $Ky = Kx$, es decir, $z = yx^{-1} \in K$. De hecho,
$$\begin{array}{ccc} \pi^{-1}(Kx) & \longrightarrow & K/R_H \\ Hy & \longmapsto & H(yx^{-1}) \end{array}$$
es una biyección.

La sobreyectividad de π y la finitud de G/R_H implican la de G/R_K, luego el índice de K en G es finito.

Por otro lado, $\pi^{-1}(Kx) \subseteq G/R_H$ luego también es finito, y así, lo es el índice de H en K. Finalmente,
$$[G : H] = \sum_{Kx \in G/R_K} card\, \pi^{-1}(Kx) = card\, G/R_K \cdot card\, K/R_H.$$

Por lo que
$$[G : H] = [G : K] \cdot [K : H].$$

□

Proposición 1.32. *Sean G un grupo y H, K subgrupos de G de orden finito. Se tiene*
$$card\, HK = \frac{o(H) \cdot o(K)}{o(H \cap K)}.$$

Demostración. La relación $(h,k)R(h',k')$ si $hk = h'k'$ definida en $H \times K$ es, evidentemente, de equivalencia y la aplicación

$$\begin{array}{ccc} (H \times K)/R & \longrightarrow & HK \\ [(h,k)]_R & \longmapsto & hk, \end{array}$$

donde $[(h,k)]_R$ denota la clase de (h,k) respecto de R, es biyectiva ya que

1. Está bien definida, ya que si $[(h,k)]_R = [(h',k')]_R$ entonces $(h,k)R(h',k')$, es decir, $hk = h'k'$.
2. Es inyectiva, ya que $[(h,k)]_R \neq [(h',k')]_R$ quiere decir que (h,k) y (h',k') no están relacionados, luego $hk \neq h'k'$.
3. Es evidentemente sobreyectiva.

Así, tenemos que $card\, HK = card\, (H \times K)/R$.

Como

$$o(H) \cdot o(K) = card\, (H \times K) = \sum_{[(h,k)]_R \in (H \times K)/R} card\, [(h,k)]_R,$$

necesitamos calcular $card\, [(h,k)]_R$.

Veamos que la aplicación

$$\begin{array}{ccc} [(h,k)]_R & \longrightarrow & H \cap K \\ (u,v) & \longmapsto & u^{-1}h \end{array}$$

es una biyección.

Si $(u,v) \in [(h,k)]_R$ entonces $hk = uv$, luego $u^{-1}h = vk^{-1} \in H \cap K$ y la aplicación está bien definida.

Es inyectiva, pues si (u,v) y (w,z) son elementos distintos en $[(h,k)]_R$, se tiene

$$hk = uv = wz, \quad u \neq w \text{ ó } v \neq z.$$

Si $u \neq w$, $u^{-1}h \neq w^{-1}h$. Si $v \neq z$, $u^{-1}h = vk^{-1} \neq zk^{-1} = w^{-1}h$. Así, en cualquier caso $u^{-1}h \neq w^{-1}h$.

También es sobreyectiva ya que, dado $t \in H \cap K$, $(ht^{-1}, tk) \in [(h,k)]_R$ puesto que $ht^{-1} \in H$, $tk \in K$ y $(ht^{-1})(tk) = hk$, y se tiene

$$(ht^{-1})^{-1}h = th^{-1}h = t.$$

Por lo tanto, $card\, [(h,k)]_R = o(H \cap K)$, con lo que

$$o(H) \cdot o(K) = \textstyle\sum_{[(h,k)]_R \in (H \times K)/R} o(H \cap K) = o(H \cap K) \cdot card\, (H \times K)/R = \\ o(H \cap K) \cdot card\, (HK).$$

□

Observación 1.32.1. *Sean $H_1, \ldots, H_t$ subgrupos de índice finito de un grupo G. Entonces $H = H_1 \cap \ldots \cap H_t$ es subgrupo de índice finito de G.*

Demostración. Ya sabemos que H es subgrupo de G. Además la aplicación

$$\begin{array}{ccc} G/R_H & \longrightarrow & G/R_{H_1} \times \ldots \times G/R_{H_t} \\ Ha & \longmapsto & (H_1 a, \ldots, H_t a) \end{array}$$

está bien definida y es inyectiva, pues si $Ha = Hb$, entonces $ab^{-1} \in H = H_1 \cap \ldots \cap H_t$, y se tiene que $H_j a = H_j b$ para cada $1 \leq j \leq t$. Por lo tanto,

$$card(G/R_H) \leq card(G/R_{H_1}) \cdot \ldots \cdot card(G/R_{H_t}) = [G : H_1] \cdot \ldots \cdot [G : H_t]$$

y esto es finito.

□

Ejemplo 1.32.1 (***Subgrupos de*** D_4)**.** *Vamos a calcular todos los subgrupos del grupo diédrico D_4.*

Como $o(D_4) = 8$, salvo los subgrupos triviales $\{1\}$ y D_4, todos los subgrupos de D_4 tienen, por el teorema de Lagrange, orden 2 o 4.

Si H es subgrupo de orden dos será $H = \{1, h\}$, con $h \in D_4$, $h \neq 1$. Y como H es subgrupo, ha de ser $h \circ h \in H$, es decir, $h \circ h = h$ ó bien $h \circ h = 1$. Del primer caso deducimos que $h = 1$, lo cual es falso. Así, $h \circ h = 1$, $h \neq 1$. Con las notaciones de 1.6.1, $h = f^i$ ó $h = g \circ f^i$, para algún $0 \leq i \leq 3$. Recordemos que, tal y como vimos en , $o(f) = 4$ y $o(g) = 2$. Si $h = f^i$, como $1 = h^2 = f^{2i}$, $2i$ ha de ser múltiplo de 4, luego i es par, con $0 \leq i \leq 3$. Así, $i = 0, 2$. Para $i = 0$, $h = f^0 = 1$ y no nos sirve. Para $i = 2$, obtenemos $h = f^2 \neq 1$, pues $o(f) = 4 > 2$, $h^2 = f^4 = 1$. Así, $H = \{1, f^2\}$ es subgrupo de orden dos.

Antes de calcular los demás subgrupos de orden dos necesitaremos:

$$f^k \circ g \circ f^k = g, \text{ para cada } 0 \leq k \leq n-1 \text{ en } D_4.$$

Veámoslo. Por inducción sobre k: si $k = 0$, es obvio. Para $k = 1$, si $V = \{a_1, \ldots, a_n\}$ son los vértices del polígono,

$$(f \circ g \circ f)(a_i) = f(g(a_{i+1})) = f(a_{n-(i+1)+2} = a_{n-(i+1)+2+1} = a_{n-i+2} = g(a_i) \text{ para } 1 \leq i \leq n \text{ (llamando } a_{n+1} = a_1).$$

Así, es claro que $f \circ g \circ f = g$. Ahora, si $k > 1$,

$$f^k \circ g \circ f^k = f \circ (f^{k-1} \circ g \circ f^{k-1}) \circ f = f \circ g \circ f = g,$$

usando la hipótesis de inducción y el caso $k = 1$. Entonces, para cada $0 \leq i \leq n-1$,

$$(g \circ f^i)^2 = (g \circ f^i) \circ (g \circ f^i) = g \circ (f^i \circ g \circ f^i) = g \circ g = g^2 = 1,$$

y como ya vimos que $g \circ f^i \neq 1$ entonces si $H_i = \{1, g \circ f^i = h_i\}$, $0 \leq i \leq n-1$, $o(h_i) = 2$. En particular, $H = \{1, f^2\}$, H_0, H_1, H_2, H_3 son todos subgrupos de orden dos de D_4.

Sólo falta calcular los subgrupos de orden 4. *Sea* H *uno de ellos. Supongamos que* $f \in H$. *Como* $o(f) = 4$ *y* $\langle f \rangle \subseteq H$, *como* $f \in H$ *resulta* $\{1, f, f^2, f^3\} = \langle f \rangle \subseteq H$ *y* $o(H) = 4$. *Por lo tanto, si* $f \in H$, *ha de ser* $H = \langle f \}$, *que evidentemente es un subgrupo de orden* 4.

Calculemos ahora los subgrupos de orden 4 *que no contienen a* f. *Para facilitar los cálculos observemos que si* H *es un subgrupo de un grupo* G, $x, y \in G$, $x \in H$, $xy \notin H$, *entonces* $y \notin H$, *pues si* $y \in H$, *como* $x \in H$ *tendríamos* $xy \in H$.

Sea pues H *un subgrupo de orden* 4 *de* D_4 *que no contiene a* f. *Como* $f^4 = 1$, *entonces* $f \circ f^3 = 1 = f^3 f$, *luego* $f^3 = f^{-1} \notin H$. *Supongamos ahora que* $g \in H$. *Como* $g \circ (g \circ f) = f \notin H$, $g \in H$, *se sigue que* $g \circ f \notin H$. *Si* $f \circ g \in H$ *entonces* $f = (f \circ g) \circ g \in H$, *lo cual es falso. Así,* $f \circ g \notin H$ *y como* $f^3 \circ g \circ f^3 = g$ *y* $f^3 = f^{-1}$, *se tiene que* $f^{-1} \circ g \circ f^3 = g$, *luego* $g \circ f^3 = f \circ g \notin H$. *Por lo tanto,* $H \subseteq D_4 = \{1, f, f^2, f^3, g, g \circ f, g \circ f^2, g \circ f^3\}$, $o(H) = 4$, $f, f^3, g \circ f, g \circ f^3 \notin H$, *luego*

$$H = \{1, f^2, g, g \circ f^2\}.$$

Comprobemos que esto es, efectivamente, un subgrupo de D_4. *Notar que como* $(f^2)^2 = g^2 = (g \circ f^2)^2 = 1$, *se tiene que* $(f^2)^{-1} = f^2$, $g^{-1} = g$, $(g \circ f^2)^{-1} = g \circ f^2$. *Además, como* $f^2 \circ g \circ f^2 = g$, *es* $g \circ f^2 = f^2 \circ g$, *luego*

$$f^2 \circ g^{-1} = f^2 \circ g = g \circ f^2 \in H,$$

$$f^2 \circ (g \circ f^2)^{-1} = f^2 \circ g \circ f^2 = g \in H,$$

$$g \circ (f^2)^{-1} = g \circ f^2 \in H,$$

$$g \circ (g \circ f^2)^{-1} = g \circ (g \circ f^2) = f^2 \in H,$$

$$(g \circ f^2) \circ (f^2)^{-1} = (g \circ f^2) \circ f^2 = g \in H,$$

$$(g \circ f^2) \circ g^{-1} = (g \circ f^2) \circ g = (f^2 \circ g) \circ g = f^2 \in H,$$

lo que prueba que $\{1, f^2, g, g \circ f^2\}$ *es subgrupo de* D_4.

Quedan por calcular los subgrupos H *de orden* 4 *de* D_4 *que no contienen ni a* f *ni a* g. *Por lo tanto,* $f, f^3, g \notin H$. *Si* $f^2 \notin H$, *tendríamos que* $g \circ f, g \circ f^2 \in H$, *luego su producto* $(g \circ f)(g \circ f^2) = g \circ (f \circ g \circ f) \circ f = g^2 \circ f = f \in H$, *que es falso. Así,* $f^2 \in H$ *(luego ó* $g \circ f$ *ó* $g \circ f^2 \notin H$*).*

Si $g \circ f^2 \in H$, $g \circ f^2 \circ f^2 = g \in H$, *que es falso. Así,* $g \circ f^2 \notin H$, *y necesariamente*

$$H = \{1, f^2, g \circ f, g \circ f^3\}.$$

Comprobemos que es un subgrupo de D_4. *Notar que* $(f^2)^2 = (g \circ f)^2 = (g \circ f^3)^2 = 1$, *luego* $(f^2)^{-1} = f^2$, $(g \circ f)^{-1} = g \circ f$, $(g \circ f^3)^{-1} = g \circ f^3$.

Ahora, tenemos

$$f^2 \circ (g \circ f)^{-1} = f^2 \circ g \circ f = f \circ (f \circ g \circ f) = f \circ g = (f \circ g \circ f) \circ f^{-1} = g \circ f^{-1} = g \circ f^3 \in H,$$

$$f^2 \circ (g \circ f^3)^{-1} = f^2 \circ g \circ f^3 = (f^2 \circ g \circ f^2) \circ f = g \circ f \in H,$$

$$(g \circ f) \circ (f^2)^{-1} = g \circ f^3 \in H,$$
$$(g \circ f) \circ (g \circ f^3)^{-1} = (g \circ f) \circ (g \circ f^3) = g \circ (f \circ g \circ f) \circ f^2 = g \circ g \circ f^2 = f^2 \in H,$$
$$(g \circ f^3) \circ (f^2)^{-1} = g \circ f^5 = g \circ f^4 \circ f = g \circ f \in H,$$
$$(g \circ f^3) \circ (g \circ f^{-1}) = g \circ f^3 \circ g \circ f = g \circ (f^3 \circ g \circ f^3) \circ f^2 = g \circ g \circ f^2 = f^2 \in H.$$

Resumiendo, además de $\{1\}$ *y* D_4*, los subgrupos de* D_4 *son:*

1. $\{1, f^2\}$, $\{1, g\}$, $\{1, g \circ f\}$, $\{1, g \circ f^2\}$, $\{1, g \circ f^3\}$, *de orden* 2.
2. $\{1, f, f^2, f^3\}$, $\{1, f^2, g, g \circ f^2\}$, $\{1, f^2, g \circ f, g \circ f^3\}$, *de orden* 4.

■

Ejemplo 1.32.2 (***El grupo cuaternión***)**.** *Consideremos los ocho símbolos siguientes:*

$$Q = \{1, -1, i, j, k, -i, -j, -k\}$$

y una operación $Q \times Q \longrightarrow Q$ *que tiene a* 1 *por elemento neutro, cumple la propiedad asociativa, la regla de los signos que todos conocemos (por ejemplo* $i(-k) = -(ik)$*) y*

$$ij = k, \;\; ji = -k$$
$$jk = i, \;\; kj = -i$$
$$ki = j, \;\; ik = -j$$
$$i^2 = j^2 = k^2 = -1$$

Con esto, está claro que Q *es un grupo de orden* 8*. Sólo queda demostrar que tiene elemento inverso.*

Como se cumple la regla de los signos tenemos que $(-1)^2 = 1$*, luego* $o(-1) = 2$ *y* -1 *es su propio inverso. Como* $i^2 = -1$*, resulta que* $(-i)^4 = (-1)^4 i^4 = i^4 = (-1)^2 = 1$*, luego* $o(i) = o(-i) = 4$*, y así* $i^{-1} = i^3$ *ya que* $ii^3 = i^4 = 1$*, además* $(-i)^{-1} = -i^3$ *ya que* $-i(-i)^3 = (-i)^4 = 1$*.*

Análogamente, $o(j) = o(-j) = 4$*,* $o(k) = o(-k) = 4$ *y* $j^{-1} = j^3$*,* $k^{-1} = k^3$*,* $(-j)^{-1} = -j^3$*,* $(-k)^{-1} = -k^3$*. Luego todos los elementos tienen inverso y así* Q *es un grupo.*

Veamos ahora cuáles son los subgrupos de Q*. Evidentemente,* $\{1\}$ *y* Q *lo son y por el Teorema de Lagrange los demás han de tener orden* 2 *ó* 4*. Como* -1 *es el único elemento de orden* 2 *de* Q*,* $\{1, -1\}$ *es el único subgrupo de orden* 2*.*

Si H *es un subgrupo de orden* 4*, deberá contener algún elemento* x *que no sea el* 1 *ó el* -1*. Entonces* $\langle x \rangle \subseteq H$ *y como* $o(x) = 4 = o(H)$ *tendremos que* $H = \langle x \rangle$*. Además, como* $-x = (-1)x = x^2 x = x^3 \in \langle x \rangle$ *y* $x = (-1)(-x) = (-x)^2(-x) = (-x)^3 \in \langle -x \rangle$*, los subgrupos de orden* 4 *de* Q *serán* $\langle i \rangle$*,* $\langle j \rangle$ *y* $\langle k \rangle$*.*

A este grupo Q lo llamaremos ***grupo cuaternión****. Además estará generado por i y j, es decir, $Q = \langle i, j \rangle$ ya que*

$$\begin{aligned} &i = i, \;\; ij = k \\ &j = j, \;\; i^3 j = i^2 ij = (-1)k = -k \\ &i^0 = 1, \;\; i^3 = i^2 i = (-1)i = -i \\ &i^2 = -1, \;\; i^2 j = (-1)j = -j. \end{aligned}$$

Y así, se tiene que

$$Q = \{1, i, i^2, i^3, j, ij, i^2 j, i^3 j\}.$$

Veremos enseguida que no existe un sistema generador con menos elementos. Para ello basta observar que $x^4 = 1$ para cada $x \in Q$, pues

$$1^4 = 1, \quad (-1)^4 = ((-1)^2)^2 = 1^2 = 1, \quad i^4 = (i^2)^2 = (-1)^2 = 1$$

$$k^4 = (k^2)^2 = (-1)^2 = 1, \quad j^4 = (j^2)^2 = (-1)^2 = 1$$

$$(-i)^4 = i^4 = 1, \quad (-j)^4 = j^4 = 1, \quad (-k)^4 = k^4 = 1$$

Este grupo además se suele presentar como el generado por las siguientes matrices:

$$a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

■

Definición 1.33. *Un grupo G se llama* ***cíclico*** *si existe un elemento $a \in G$ tal que*

$$G = \langle a \rangle.$$

Ejemplo 1.33.1. *El grupo $\mathbb{Z}$ de los números enteros es un grupo cíclico pues $\mathbb{Z} = \langle 1 \rangle$.*

■

Observación 1.33.1. *Un grupo finito G es cíclico si y sólo si existe $a \in G$ tal que $o(a) = o(G)$.*

Demostración. En efecto, si $G = \langle a \rangle$, $o(G) = o(\langle a \rangle) = o(a)$. Recíprocamente, si $a \in G$ y $o(a) = o(G)$, $\langle a \rangle$ es un subconjunto de G con tantos elementos como G, luego

$$\langle a \rangle = G.$$

□

Observación 1.33.2. *El grupo D_4 no es cíclico pues ningún elemento tiene orden 8. De hecho, con las notaciones habituales, vimos en el ejemplo 1.32.1 que*

$$o(f) = o(f^{-1}) = o(f^3) = 4, \;\; o(1) = 1, \;\; o(x) = 2, \;\; \textit{con } x \in D_4 \setminus \{1, f, f^3\}.$$

Tampoco el grupo cuaternión es cíclico, puesto que $x^4 = 1$ para cada $x \in Q$.

De este modo, cuando vimos que $D_4 = \langle f, g \rangle$, $Q = \langle i, j \rangle$ encontramos sistemas generadores de D_4 y Q respectivamente con el menor número posible de elementos.

Proposición 1.34. *Si p es un número primo y G es un grupo de orden p, G es cíclico.*

Demostración. Sea $a \in G$, $a \neq 1$. Por el teorema de Lagrange $o(a)$ divide a p, como $o(a) \neq 1$, será $o(a) = p$, luego G es cíclico.

□

De hecho, se ha probado que $G = \langle a \rangle$ para cada $a \in G$, con $a \neq 1$.

Proposición 1.35. *Todo grupo cíclico es abeliano, pero existen grupos abelianos no cíclicos.*

Demostración. Para la primera parte, sea $G = \langle a \rangle$ un grupo cíclico. Dados $x, y \in G$, serán $x = a^k$, $y = a^l$, para ciertos k, l. Por lo tanto, $xy = a^k a^l = a^{k+l} = a^{l+k} = yx$ y así G es abeliano.

Para la segunda parte, consideremos el subgrupo de D_4:

$$H = \{1, f^2, g, g \circ f^2\}.$$

Como los elementos de H tienen orden 2, salvo $o(1) = 1$, y $o(H) = 4$, H no es cíclico. Sin embargo, H es abeliano:

$$f^2 \circ g = f^2 \circ g \circ f^4 = (f^2 \circ g \circ f^2) \circ f^2 = g \circ f^2,$$

$$f^2 \circ (g \circ f^2) = f^2 \circ g \circ f^2 = g = g \circ f^4 = (g \circ f^2) \circ f^2,$$
$$g \circ (g \circ f^2) = g^2 \circ f^2 = f^2 = (g \circ f^2) \circ (f^2 \circ g \circ f^2) = (g \circ f^2) \circ g.$$

□

Observación 1.35.1. *En los ejemplos anteriores, 1.32.1 y , hemos visto que para los grupos D_4 y Q se cumple una especie de recíproco al teorema de Lagrange:*

Para cada divisor m de $8 = o(D_4) = o(Q)$ existe un subgrupo de D_4 (respectivamente de Q) de orden m.

Este resultado, que como veremos más adelante es en general falso, se cumple para cualquier grupo cíclico finito, con una importante información adicional.

Proposición 1.36. *Sea G un grupo cíclico, $n = o(G)$. Para cada divisor m de n existe un único subgrupo de G de orden m. Además este subgrupo es cíclico.*

Demostración. Sea $a \in G$ tal que $G = \langle a \rangle$. En primer lugar, si $n = kl$, $\langle a^k \rangle$ es un subgrupo de orden l, ya que $o(a^k) = \dfrac{n}{mcd(k,n)} = \dfrac{n}{k} = l$ por 1.26.

Probemos la proposición. Como m divide a n, existe un natural d tal que

$$n = dm.$$

Por lo que acabamos de ver al comienzo de la demostración, $H = \langle a^d \rangle$ tiene orden m. Veamos que es el único subgrupo de orden m. Sea K otro subgrupo de G de orden m. Sea k el menor entero positivo tal que $a^k \in K$ (que existe puesto que $K \subseteq G = \langle a \rangle$).

Si $a^p \in K$, p es múltiplo de k ya que si dividimos p entre k tenemos, por el algoritmo de la división, que

$$p = qk + r,\ 0 \leq r < k, \text{ luego } a^r = a^{p-qk} = a^p(a^k)^{-q} \in K$$

pero por la elección de k (el menor entero positivo tal que $a^k \in K$), ha de ser necesariamente $r = 0$, y así $p = qk$, es decir, p es múltiplo de k.

De esto se deduce que $n = sk$, con $s \in \mathbb{N}$, ya que $a^n = 1 \in K$, además $K = \langle a^k \rangle$ porque para cada $x = a^p \in K$ se tiene que $x = (a^k)^q \in \langle a^k \rangle$.

Ahora, $m = o(K) = o(a^k) = n/k$, con lo que $k = n/m = d$ y así $K = \langle a^d \rangle = H$.

Luego, $\langle a^d \rangle$ es el único subgrupo de G de orden m. Como además es cíclico, hemos acabado.

□

Proposición 1.37. *Todo subgrupo de un grupo cíclico es cíclico.*

Demostración. Sea G un grupo cíclico. Si G es finito, ya hemos probado el resultado en la proposición anterior.

Supongamos así que G no es finito, se razona igual. Si $G = \langle a \rangle$ y H es subgrupo de G, consideramos k el menor entero positivo tal que $a^k \in H$. Así, dado $x \in H \subseteq G$, será $x = a^p$, con $p \in \mathbb{N}$, y dividiendo

$$p = qk + r, \quad 0 \leq r < k.$$

Como $a^r = a^p(a^k)^{-q} \in H$, debe ser $r = 0$ por la elección de k. Por lo tanto, $x = a^p = (a^k)^q \in \langle a^k \rangle$, con lo que $H = \langle a^k \rangle$.

□

Terminamos este capítulo con un resultado que relaciona el orden de un grupo finito con el mínimo número de elementos de un sistema generador del grupo.

Definición 1.38. *Sea G un grupo finitamente generado. Un sistema generador finito S de G se llama* ***minimal*** *si cualquier subconjunto de G con menos elementos que S no es sistema generador de G.*

Evidentemente, todo grupo finitamente generado tiene algún sistema generador minimal.

Proposición 1.39. *Sea G un grupo finito de orden n y $S = \{x_1, \ldots, x_p\}$ un sistema generador minimal de G. Entonces $2^p \leq n$.*

Demostración. Llamemos $S_i = \{x_1, \ldots, x_i\}$ para cada $1 \leq i \leq p$ y $H_i = \langle S_i \rangle$. Desde luego, $H_p = G$.

Evidentemente $H_i \subseteq H_{i+1}$ para cada $1 \leq i \leq p-1$, pues $H_{i+1} \supseteq S_{i+1} \supseteq S_i$ y H_i es el menor subgrupo que contiene a S_i.

Además, el contenido es estricto; en caso contrario, $x_{i+1} \in H_{i+1} = H_i$, luego $x_{i+1} = x_i^{l_i} \ldots$ para ciertos enteros $l_1, \ldots, l_i$.

Consideremos

$$T = \{x_1, \ldots, x_i, x_{i+2}, \ldots, x_p\},$$

que tiene $p-1$ elementos. Si probamos que T es sistema generador de G habremos obtenido una contradicción, pues S no sería minimal.

Dado $x \in G = \langle S \rangle$, se escribe:

$$x = s_1^{h_1} \ldots s_m^{h_m}, \quad m \in \mathbb{N}, s_j \in \{x_1, \ldots, x_p\}, h_j \in \mathbb{Z}, 1 \leq j \leq m.$$

Cada vez que en la expresión anterior aparezca $s_j = x_{i+1}$ lo sustituimos por $x_{i+1} = x_i^{l_i}$. Así, $x \in \langle T \rangle$, y T es sistema generador de G.

Así (volviendo a lo que estábamos viendo), tenemos pues $H_1 \subsetneq H_2 \subsetneq \ldots \subsetneq H_p = G$. Y aplicando reiteradamente la transitividad del índice 1.31 se deduce

$$[G : H_1] = [H_p : H_{p-1}] \cdot [H_{p-1} : H_{p-2}] \cdot \ldots \cdot [H_2 : H_1].$$

Usando el teorema de Lagrange, para cada $1 \leq i \leq p-1$, $[H_{i+1} : H_i] = \dfrac{o(H_{i+1})}{o(H_i)} > 1$ pues $H_i \subsetneq H_{i+1}$, y como $[H_{i+1} : H_i]$ es un número entero, $[H_{i+1} : H_i] \geq 2$. Así, tenemos

$$\frac{o(G)}{o(H_1)} = [G : H_1] \geq 2^{p-1},$$

y por lo tanto $n = o(G) \geq o(H_1) \cdot 2^{p-1}$.

Si $o(H_1) = 1$ sería $H_1 = \{1\}$, luego $x_1 = 1$ y $U = \{x_2, \ldots, x_p\}$ sería un sistema generador de G con menos elementos que S. Esto es absurdo y por lo tanto $o(H_1) \geq 2$. En consecuencia, $n \geq 2 \cdot 2^{p-1} = 2^p$.

□

Observación 1.39.1. *En determinadas situaciones, la cota $2^p \leq n$ es mejorable. Supongamos que q es el menor número primo que divide a n. Como cada $[H_{i+1} : H_i] \neq 1$ tendremos*

$$[H_{i+1} : H_i] \geq q,$$

y análogamente $o(H_1) \geq q$. De este modo obtendremos $q^p \leq n$. Por ejemplo, si n es impar tenemos $q \geq 3$ y así $3^p \leq n$.

2. Subgrupos normales. Grupos cocientes. Homomorfismos

2.1. Subgrupos normales. Propiedades

Al trabajar con cualquier clase de objetos en Matemáticas es importante hallar relaciones de equivalencia tales que los cocientes admitan, de modo natural, una estructura del tipo de la de los objetos iniciales. En el caso de los grupos, si H es un subgrupo de un grupo G, los cocientes G/R_H y G/R^H no admiten, en general, estructura de grupo de modo natural. Estudiaremos aquí los subgrupos H para los que esto es posible.

Posteriormente estudiaremos las aplicaciones entre grupos «compatibles» con la estructura de grupo. De la existencia de una tal aplicación entre dos grupos G y G' obtendremos información sobre G' a partir de información sobre G y recíprocamente.

Proposición 2.1. *Sean G un grupo y H un subgrupo de G. Las siguientes condiciones son equivalentes:*

1. *Para cada $a \in G$, $Ha = aH$.*
2. *$H = H^a$ para cada $a \in G$. Es decir, $a^{-1}Ha = H \ \forall a \in G$.*
3. *Para cada par de elementos $a, b \in G$ tales que $ab \in H$ se verifica que $ba \in H$.*

Demostración. Sigamos una demostración circular:

$1 \Rightarrow 2$. Si $y \in H^a$ entonces $aya^{-1} = h \in H$. Como $ay = ha \in Ha = aH$ existirá un $h' \in H$ con $ay = ah'$. Simplificando tenemos que $y = h' \in H$, luego $H^a \subseteq H$. Y aplicando el contenido que acabamos de probar para a^{-1} se tiene que $H^{a^{-1}} \subseteq H$, y así $H = (H^{a^{-1}})^a \subseteq H^a$, por lo tanto $H = H^a$.

$2 \Rightarrow 3$. Como $ab \in H$ entonces $ba = a^{-1}(ab)a \in H^a = H$.

$3 \Rightarrow 1$. Sea $x \in Ha$. Entonces, $x = ha$ con $h \in H$ y, por ello, $xa^{-1} = h \in H$. Por hipótesis $a^{-1}x = h' \in H$, y así $x = ah' \in aH$, demostrando el primer contenido $Ha \subseteq aH$.

Recíprocamente, si $x = ah \in aH$, resulta que $a^{-1}x = h \in H$, luego $xa^{-1} = h' \in H$, es decir, $x = h'a \in Ha$, demostrando con esto el contenido recíproco $aH \subseteq Ha$, y por lo tanto $aH = Ha$.

□

Definición 2.2. *Un subgrupo H de un grupo G que cumple cualquiera (y por tanto todas) de las condiciones de la propoposición anterior se llama **normal**. Con más precisión, diremos que H es subgrupo normal de G.*

Observación 2.2.1. *Evidentemente la condición (1) de 2.1 equivale a decir que $R_H = R^H$. En particular, si H es normal, $G/R_H = G/R^H$ y denotaremos ambos cocientes por G/H. Más adelante veremos qué es exactamente este cociente.*

Observación 2.2.2. *Para probar que H es un subgrupo normal de G basta ver que $H^a \subseteq H$ para cada $a \in G$. Probado esto y aplicado para a^{-1}, se tendrá $H^{a^{-1}} \subseteq H$, luego $H = (H^{a^{-1}})^a \subseteq H^a$ y por ello $H = H^a$ y así H es normal.*

Observación 2.2.3. *Todo subgrupo de un grupo abeliano es normal, puesto que en un grupo abeliano siempre se cumple $ab = ba$, luego se tiene la condición* (3) *de 2.1.*

Proposición 2.3. *Si G es un grupo y H un subgrupo de G con índice* 2*, H es subgrupo normal de G.*

Demostración. Por hipotesis, G/R_H tiene dos elementos, y también G/R^H.

Entonces, dado $a \in G$ puede ocurrir:

1. $a \in H$. En tal caso, $a1^{-1} = a \in H$, luego aR_H1 y $Ha = H1 = H$. Como $a^{-1}1 = a^{-1} \in H$, también se tiene aR^H1 y así $aH = 1H = H$. Luego, $aH = Ha$.
2. Si $a \notin H$, $aH \neq H$. Como G/R^H tiene dos elementos, será $G = H \cup aH$ (unión disjunta). Así, $aH = G \setminus H = Ha$ y H es normal.

□

Observación 2.3.1. *En cualquier grupo G los subgrupos $\{1_G\}$ y G son normales. En efecto, dado $a \in G$ se tiene $a\{1_G\} = \{1_G\}a$ (de aquí se deduce que $G/\{1_G\} = G$). Y $aG = G = Ga$ (ya que $ax = (axa^{-1})a$).*

Observación 2.3.2. *El recíproco de 2.2.3 es falso. EL grupo cuaternión Q no es abeliano, pero todos sus subgrupos son normales.*

Demostración. Que no es abeliano es claro, pues $ij = k \neq -k = ji$. Los subgrupos $\{1\}$ y Q son normales por lo que acabamos de ver. Los subgrupos de orden 4 tienen índice 2, luego son normales. El único subgrupo de orden 2 es $H = \{1, -1\}$, que es normal porque para cada $a \in Q$,

$$aH = a\{1, -1\} = \{a, -a\} = \{1, -1\}a = Ha.$$

□

Definición 2.4. *Los grupos como Q, cuyos subgrupos son todos normales, se llaman* ***hamiltonianos****.*

Observación 2.4.1. *Existen grupos cuyos subgrupos no son todos normales. Consideremos $G = D_n$, con $n \geq 3$, y, con las notaciones usuales, $H = \{1, g\}$. Vimos en 1.29.2 que $fH \neq Hf$, luego H no es subgrupo normal de D_n.*

Calculemos ahora los subgrupos normales de D_4. Evidentemente, $\{1\}$ y D_4 son normales.

Los subgrupos $\{1, f, f^2, f^3\}$, $\{1, f^2, g, g \circ f^2\}$ y $\{1, f^2, g \circ f, g \circ f^3\}$ son los subgrupos de D_4 de orden 4*. Como todos ellos tienen índice* 2*, son normales.*

Debemos decidir si los subgrupos de orden 2, que son

$$H_1 = \{1, f^2\}, \quad H_2 = \{1, g\}, \quad H_3 = \{1, g \circ f\},$$

$$H_4 = \{1, g \circ f^2\}, \quad H_5 = \{1, g \circ f^3\},$$

son normales.

1. *H_2 y H_4.*

   Tenemos $f \circ g \circ f^{-1} = f \circ g \circ f^3 = (f \circ g \circ f) \circ f^2 = g \circ f^2 \in H_4$, luego $g \in H_4^f$. Como H_4^f es un subgrupo de orden 2 resulta que $H_4^f = \{1, g\} = H_2$. Así, $H_2^{f^{-1}} = (H_4^f)^{f^{-1}} = H_4$. En consecuencia, $H_4^f = H_2 \neq H_4$, luego H_4 no es normal; $H_2^{f^{-1}} = H_4 \neq H_2$, luego H_2 no es normal.

2. *H_3 y H_5.*

   Tenemos $f \circ (g \circ f) \circ f^{-1} = (f \circ g \circ f) \circ f^3 = g \circ f^3 \in H_5$, luego $g \circ f \in H_5^f$ y al ser H_5^f subgrupo de orden 2 resulta que $H_5^f = \{1, g \circ f\} = H_3$ y por lo tanto, $H_5 = H_3^{f^{-1}}$. Así, $H_5^f = H_3 \neq H_5$, luego H_5 no es normal; $H_3^{f^{-1}} = H_5 \neq H_3$, luego H_3 no es normal.

3. *H_1.*

   Veamos, para acabar, que H_1 es subgrupo normal de D_4. En primer lugar, $a^{-1} \circ f^2 \circ a = f^2$ para cada $a \in D_4$, ya que si $a = f^i$ tenemos $a^{-1} \circ f^2 \circ f = f^{-i} \circ f^2 \circ f^i = f^{-i+2+i} = f^2$, y si $a = g \circ f^i$ tenemos $a^{-1} \circ f^2 \circ a = (g \circ f^i)^{-1} \circ f^2 \circ (g \circ f^i) = f^{-i} \circ g^{-1} \circ f^2 \circ g \circ f^i = f^{-i} \circ g^{-1} \circ (f^2 \circ g \circ f^2) \circ f^{i-2} = f^{-i} \circ g^{-1} \circ g \circ f^{i-2} = f^{-i} \circ f^{i-2} = f^{-2} = f^2$.

   Ahora, dado $a \in D_4$, si $x \in H_1^a$ tendremos $axa^{-1} \in H_1$ y por lo tanto, $axa^{-1} = 1$ ó $axa^{-1} = f^2$. En el primer caso, $ax = a$, luego $x = 1 \in H_1$. En el segundo caso, $x = a^{-1}f^2a = f^2 \in H_1$. Así, $H_1^a \subseteq H_1$ para cada $a \in D_4$, con lo que, por 2.2.2, H_1 es subgrupo normal de D_4. Por lo tanto, $H_1 = \{1, f^2\}$ es el único subgrupo normal de orden 2 de D_4.

Proposición 2.5. *Si G es un grupo, todo subgrupo $H \subseteq Z(G)$ es un subgrupo normal de G.*

Demostración. Recordemos que el centro de G es

$$Z(G) = \{x \in G : ax = xa \ \ \forall a \in G\}$$

y es subgrupo de G.

Usando 2.2.2 bastará probar que $H^a \subseteq H$ para cada $a \in G$. Sea $x \in H^a$. Así $axa^{-1} = h \in H$, luego $x = a^{-1}ha$. Como $h \in H \subseteq Z(G)$, $ha = ah$ y así

$$x = a^{-1}ha = h \in H.$$

□

Observación 2.5.1 (***Grupo especial lineal***). *Sea $n \in \mathbb{N}$ (no nulo) y $G = GL_n(\mathbb{R})$ el grupo de las matrices de orden n con coeficientes en $\mathbb{R}$ y determinante no nulo. Ya sabemos que, con la operación producto de matrices, G es un grupo.*

Sea $H = \{A \in G : det\ A = 1\}$. H es subgrupo normal de G, llamado ***grupo especial lineal*** *y que se denota por $SL_n(\mathbb{R})$.*

Dados $A, B \in H$, como $BB^{-1} = I_n$, $det\ B \cdot det\ B^{-1} = 1$, luego $detB^{-1} = \dfrac{1}{det\ B} = 1$ y así

$$det(AB^{-1}) = det\ A \cdot det\ B^{-1} = 1 \cdot 1 = 1.$$

En consecuencia, $AB^{-1} \in H$ y por lo tanto H es subgrupo de G. Para probar que es normal veremos que se cumple la condición (3) *de 2.1.*

Si $A, B \in G$ y $AB \in H$ significa que $det(AB) = 1$. Entonces $det(BA) = det\ B \cdot detA = det\ A \cdot det\ B = det(AB) = 1$, es decir, $BA \in H$.

Proposición 2.6. *Sean G un grupo y H un subgrupo de G.*

1. *H es subgrupo de $N_G(H)$.*
2. *H es subgrupo normal de $N_G(H)$.*
3. *Si K es un subgrupo de G que contiene a H y H es un subgrupo normal de K, entonces $K \subseteq N_G(H)$.*

Demostración. Veámoslo por partes.

1. Basta ver que $H \subseteq N_G(H)$, o lo que es lo mismo, que si $a \in H$ entonces $H = H^a$.

   Pero si $x \in H^a$ es $axa^{-1} = h \in H$, luego $x = a^{-1}ha \in H$. Por lo tanto $H^a \subseteq H$. Recíprocamente, como también $a^{-1} \in H$ tendremos por lo anterior $H^{a^{-1}} \subseteq H$ y así $H = (H^{a^{-1}})^a \subseteq H^a$ y de aquí $H = H^a$.

2. Para cada $a \in N_G(H)$ es $H = H^a$ por definición. Así que H es subgrupo normal de $N_G(H)$.

3. Si $a \in K$, como H es subgrupo normal de K, es $H = H^a$, con lo que $a \in N_G(H)$.

□

Proposición 2.7. *Si H y K son subgrupos de un grupo G decimos que K es un* ***subgrupo conjugado*** *de H si existe $a \in G$ tal que*

$$K = H^a.$$

1. *Si K es conjugado de H, entonces H es conjugado de K, y diremos que H y K son conjugados.*

2. *Si Σ es la familia de subgrupos conjugados de H (distintos) y $N = N_G(H)$ es el normalizador de H en G, la aplicación*

$$\begin{array}{rccc} \varphi\colon & G/R_N & \longrightarrow & \Sigma \\ & Na & \longmapsto & H^a \end{array}$$

es biyectiva.

3. *En particular, si $N_G(H)$ tiene índice finito en G, el número de conjugados de H en G es $[G : N_G(H)]$.*

Demostración. Veámoslo por partes.

1. Es evidente, pues si $K = H^a$, $K^{a^{-1}} = (H^a)^{a^{-1}} = H$.

2. Comencemos por demostrar que φ está bien definida:

   Si $Na = Nb$, entonces $ab^{-1} \in N$, luego $H^{ab^{-1}} = H$ y así

   $$H^b = (H^{ab^{-1}})^b = H^a,$$

   Veamos ahora que es inyectiva:

   Si $H^a = H^b$ se tiene $H^{ab^{-1}} = (H^b)^{b^{-1}} = H$, luego $ab^{-1} \in N$ y $Na = Nb$. Como la sobreyectividad es evidente, queda demostrado.

3. Es claro ya que

   $$card\,\Sigma = card(G/R_N) = [G : N]\,.$$

□

Proposición 2.8. *Sea N un subgrupo normal de un grupo G y sean H y K subgrupos de G tales que H es subgrupo normal de K. Entonces NH es subgrupo normal de NK.*

Demostración. Primeramente veamos que $NH = HN$ y así NH es subgrupo de G:

En particular NH es subgrupo de NK, pues $NH \subseteq NK$. Pero si $x \in NH$ se escribirá $x = nh$, $n \in N$, $h \in H$. Así $x \in Nh = hN \subseteq HN$, la igualdad $Nh = hN$ se tiene por ser N subgrupo normal de G. Esto prueba el contenido $NH \subseteq HN$. El otro es análogo. De igual forma se prueba que $NK = KN$, luego NK es subgrupo de G, y así es grupo. Ahora veamos la normalidad:

Usaremos la condición (1) de 2.1. Veamos que si $a \in NK$, entonces $a(NH) = (NH)a$. Como $a \in NK$ se escribirá $a = nk$, $n \in N$, $k \in K$. Si $x \in a(NH) = a(HN)$ se tendrá $x = ahn_1$, $h \in H$, $n_1 \in N$. Como $x \in (ah)N = N(ah)$ por ser N subgrupo normal de G, tendremos entonces $x = n_2ah = n_2nkh$, $n_2 \in N$. Como $kh \in kH = Hk$ por ser H subgrupo normal de K, $x = n_2nh_1k$, $h_1 \in H$, o también, $x = n_2nh_1n^{-1}nk = n_2nh_1n^{-1}a$. Ahora $h_1n^{-1} \in HN = NH$, con lo que se tiene $h_1n^{-1} = n_3h_2$, $n_3 \in N$, $h_2 \in H$. Finalmente, $x = n_2nn_3h_2a \in (NH)a$. Y así $a(NH) \subseteq (NH)a$. Para el otro contenido se procede de igual forma.

□

Definición 2.9. *Decimos que un grupo G es simple si sus únicos subgrupos normales son $\{1_G\}$ y G. Los ejemplos más sencillos de grupos simples son los de orden primo. De hecho*

Observación 2.9.1. *Si p es un número primo y G un grupo de orden p, los únicos subgrupos de G son $\{1_G\}$ y G. En particular, G es simple.*

Esto se sigue del hecho que si H es un subgrupo de G, su orden debe dividir a p por el teorema de Lagrange. Y como p es primo, ó bien $o(H) = 1$ y así $H = \{1_G\}$, ó bien $o(H) = p$ y así $H = G$.

Observación 2.9.2. *La normalidad no es una propiedad **transitiva**, esto es, existen un grupo G y subgrupos suyos H y K con $H \subseteq K$, H subgrupo normal de K, K subgrupo normal de G, pero H no es subgrupo normal de G.*

Por ejemplo, tomemos $G = D_4$ y con las notaciones usuales,

$$K = \{1, f^2, g, g \circ f^2\}, \quad H = \{1, g\}.$$

Como $[D_4 : K] = 2$, K es subgrupo normal de D_4. Como $[K : H] = \dfrac{o(K)}{o(H)} = 2$, también H es subgrupo normal de K. Sin embargo, ya vimos en 2.4.1 que H no es subgrupo normal de G.

Definición 2.10. *Si H es un subgrupo de un grupo G, se llama **corazón** de H a*

$$K(H) = \bigcap_{a \in G} H^a.$$

Por 1.22.1, $K(H)$ es subgrupo de G. Además, $K(H)$ es subgrupo normal de G.

Demostración. Basta probar que $K(H)^b \subseteq K(H)$ para cada $b \in G$:

Sea $x \in K(H)^b$, tenemos que ver que $x \in H^a$ para cada $a \in G$. Pero $bxb^{-1} \in K(H) \subseteq H^{ab^{-1}}$, luego

$$ab^{-1}(bxb^{-1})(ab^{-1})^{-1} \in H,$$

y por lo tanto $axa^{-1} \in H$, esto es, $x \in H^a$.

□

Veamos por último que

Observación 2.10.1. *Si $N \subseteq H$ es un subgrupo normal de G, entonces $N \subseteq K(H)$, puesto que, para cada $a \in G$,*

$$N = N^a \subseteq H^a, \text{ luego } N \subseteq \bigcap_{a \in G} H^a = K(H).$$

Ahora podemos demostrar:

Teorema 2.11 (***Teorema de Poincaré***)**.** *Si G posee un subgrupo de índice finito, también posee un subgrupo normal de índice finito.*

Demostración. Probemos que si H es un subgrupo de índice finito, $K(H)$, que es normal, tiene índice finito.

Como $[G : H]$ es finito, también lo es

$$[G : N_G(H)] = \frac{[G : H]}{[N_G(H) : H]},$$

luego sabemos que H tiene un número finito de conjugados. Y como $K(H)$ es la intersección de los conjugados de H, y hay una cantidad finita de éstos, para probar que $[G : K(H)]$ es finito basta (ya que la intersección de subgrupos de índice finito es subgrupo de índice finito) demostrar que cada H^a es subgrupo de G de índice finito. De hecho probaremos la igualdad

$$[G : H] = [G : H^a].$$

Para eso es suficiente demostrar que la aplicación

$$\begin{array}{ccc} G/R_{H^a} & \longrightarrow & G/R_H \\ H^a x & \longmapsto & Hax \end{array}$$

es biyectiva.

Está bien definida, y es inyectiva, pues $H^a x = H^a y$ equivale a que $xy^{-1} \in H^a$, y así $axy^{-1}a^{-1} \in H$, o lo que es lo mismo, $ax(ay)^{-1} \in H$ y esto es $Hax = Hay$. Además es sobreyectiva, puesto que $Hy = Hax$ con $x = a^{-1}y$ para cada $y \in G$.

□

Como adelantamos en la introducción, buscamos subgrupos H tales que G/R_H tenga, de modo natural, estructura de grupo. La siguiente proposición pone de manifiesto que los subgrupos normales son los adecuados.

2.2. Grupos cocientes

Proposición 2.12. *Sean G un grupo y H un subgrupo normal de G. El cociente $G/H = G/R_H = G/R^H$ tiene estructura de grupo con la operación*

$$\begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (aH, aH) & \longmapsto & abH. \end{array}$$

El elemento neutro es $H = 1H$. Además, si H es subgrupo de G de índice finito, $o(G/H) = [G : H]$.

Demostración. Ya sabemos que cuando H es normal, los conjuntos cocientes G/R_H y G/R^H coinciden, y los denotaremos por G/H. El único punto problemático, y donde se hace uso de la normalidad de H, es cuando hay que comprobar que la operación está bien definida, es decir, que no dependa de los representantes a y b elegidos.

1. Sea pues $aH = xH$, $bH = yH$, comprobemos que $abH = xyH$, es decir que $(ab)^{-1}xy \in H$, y así $b^{-1}a^{-1}xy \in H$. Como $aH = xH$, $a^{-1}x = h \in H$. Como $bH = yH$, $b^{-1}y = h' \in H$. Por ello,

$$b^{-1}a^{-1}xy = b^{-1}hy = b^{-1}yy^{-1}hy = h'y^{-1}hy.$$

   Si $z = y^{-1}hy$, resulta que $z \in H^y = H$ por ser H normal. Por lo que,

$$b^{-1}a^{-1}xy = h'z \in H.$$

2. Además la operación es asociativa, pues

$$aH((bH)(cH)) = (aH)(bcH) = (a(bc))H = ((ab)c)H = ((ab)H)(cH) = ((aH)(bH))cH.$$

3. Como

$$(aH)H = (aH)(1H) = (a1)H = (aH) \text{ y}$$
$$H(aH) = (1H)(aH) = (1a)H = aH,$$

   la clase H es el elemento neutro.

4. Dado $aH \in G/H$ se verifica

$$(aH)(a^{-1}H) = (aa^{-1}H) = 1H = H,$$

$$(a^{-1}H)(aH) = (a^{-1}aH) = 1H = H,$$

   y así $a^{-1}H$ es el inverso de aH. Es decir

$$(aH)^{-1} = a^{-1}H.$$

5. Finalmente, si H tiene índice finito en G,

$$|G/H| = card(G/R_H) = [G : H].$$

□

Es decir, si tenemos un grupo G y un subgrupo normal H, entonces el cociente G/H es también un grupo. Los subgrupos normales son los adecuados para dotar a un cociente de estructura de grupo.

Observación 2.12.1. *Vamos a estudiar cómo son los subgrupos de un grupo cociente G/H.*

Si K es un subgrupo de G que contiene a H, H es subgrupo normal de K, por serlo de G. Entonces tiene sentido considerar el grupo cociente K/H. Evidentemente $K/H \subseteq G/H$ y es subgrupo de G/H, puesto que dados $aH, bH \in K/H$, $a, b \in K$ se tiene

$$(aH)(bH)^{-1} = (aH)(b^{-1}H) = ab^{-1}H \in K/H,$$

ya que al ser K subgrupo de G, $ab^{-1} \in K$.

Recíprocamente, sea M un subgrupo de G/H, y llamemos

$$K = \{x \in G : xH \in M\}.$$

Veamos que K es un subgrupo de G que contiene a H y que $M = K/H$.

Desde luego, si $h \in H$ se tiene que $hH = H$ que pertenece a M pues M es subgrupo y H es el neutro de G/H. Esto prueba que $h \in K$ y con ello que $H \subseteq K$.

Dados $x, y \in K$, tenemos $xH, yH \in M$ de donde

$$xy^{-1}H = (xH)(y^{-1}H) = (xH)(yH)^{-1} \in M$$

por ser M subgrupo. Esto quiere decir que $xy^{-1} \in K$. Por lo tanto K es subgrupo de G.

Veamos que se cumple la igualdad $M = K/H$. Dado $xH \in K/H$, es $x \in K$ y por tanto $xH \in M$. En el otro sentido, si $xH \in M$, entonces $x \in K$, luego $xH \in K/H$. Es inmediato que si K_1 y K_2 son subgrupos de G que contienen a H y $K_1/H = K_2/H$, entonces $K_1 = K_2$.

Por lo tanto, hemos demostrado que la aplicación

$$\begin{array}{ccc} K & \longrightarrow & K/H \\ x & \longmapsto & xH. \end{array}$$

es una biyección entre los subgrupos de G que contienen a H y los subgrupos de G/H. Este resultado se conoce como ***Teorema de la correspondencia***. Además la biyección preserva la normalidad y por lo tanto tenemos que:

Proposición 2.13. *K es subgrupo normal de G si y sólo si K/H es subgrupo normal de G/H.*

Demostración. Utilizaremos la condición (3) de 2.1. Supongamos que K es normal. Dados aH, bH con $(aH)(bH) \in K/H$, entonces $(ab)H \in K/H$, es decir, $ab \in K$. Como K es normal, y $ab \in K$, deducimos que $ba \in K$, luego $(bH)(aH) = (ba)H \in K/H$, y así K/H es normal. Para el recíproco es análogo.

□

Observación 2.13.1. *Si G es cíclico y H es un subgrupo normal de G, también el cociente G/H es cíclico.*

En efecto, si $G = \langle a \rangle$, es obvio que $G/H = \langle aH \rangle$.

Ejemplo 2.13.1. *Dado un entero positivo m, el subgrupo $H = m\mathbb{Z}$ del grupo $\mathbb{Z}$ es desde luego normal, por ser $\mathbb{Z}$ abeliano. Como aquí la notación es aditiva, la operación en el cociente vendrá dada por*

$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \\ (a + m\mathbb{Z}, b + m\mathbb{Z}) & \longmapsto & a + b + m\mathbb{Z}. \end{array}$$

Además el grupo cociente $\mathbb{Z}/m\mathbb{Z}$ es cíclico de orden m. Y sabemos que

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\},$$

siendo todos los elementos del miembro de la derecha distintos. Visto esto tendremos

$$o(\mathbb{Z}/m\mathbb{Z}) = m, \quad \mathbb{Z}/m\mathbb{Z} = \langle 1 + m\mathbb{Z}\rangle.$$

■

Ejemplo 2.13.2. *Sea m un entero positivo. Denotamos*

$$\mathbb{Z}_m^* = \{a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z} : mcd(a, m) = 1\},$$

y consideremos la operación binaria

$$\begin{array}{ccc} \mathbb{Z}_m^* \times \mathbb{Z}_m^* & \longrightarrow & \mathbb{Z}_m^* \\ (a + m\mathbb{Z}, b + m\mathbb{Z}) & \longmapsto & ab + m\mathbb{Z}. \end{array}$$

Queremos demostrar que, con esta operación, $\mathbb{Z}_m^*$ es un grupo abeliano. En primer lugar hemos de ver que la operación está bien definida, y para ello

1. *Si $a + m\mathbb{Z} = a' + m\mathbb{Z}$ y $b + m\mathbb{Z} = b' + m\mathbb{Z}$, tendremos que $a = a' + mu$, $b = b' + mv$, con $u, v \in \mathbb{Z}$ y así*

   $$ab = a'b' + m(b'u + a'v + muv).$$

   Luego $ab - a'b' \in m\mathbb{Z}$ y por tanto $ab + m\mathbb{Z} = a'b' + m\mathbb{Z}$. Esto demuestra que la definición no depende de los representantes.

2. *Ahora veamos que es interna:*

   Si $mcd(a, m) = mcd(b, m) = 1$, entonces $mcd(ab, m) = 1$. Usando 1.24.1 (Identidad de Bézout) tenemos que

   $$1 = ua + vm,\ 1 = u'b + v'm,\ u, v, u', v' \in \mathbb{Z}.$$

   Por lo que,

   $$1 = (ua + vm)(u'b + v'm) = uu'ab + (auv' + bvu' + mvv')m = u''ab + v''m,$$

   con $u'' = uu'$ y $v'' = auv' + bvu' + mvv'$. Y de nuevo, por 1.24.1, $mcd(ab, m) = 1$ como queríamos ver.

   El resto de las propiedades de grupo son fáciles de comprobar. La asociatividad es obvia, y es claro que $1 + m\mathbb{Z}$ es el elemento neutro. También es inmediato que $\mathbb{Z}_m^*$ es abeliano.

   Por último, para cada $a + m\mathbb{Z}$, como $mcd(a, m) = 1$, se tiene que $1 = au + mv$, $u, v \in \mathbb{Z}$, y así $1 + m\mathbb{Z} = (au + m\mathbb{Z}) + (mv + m\mathbb{Z}) = (a + m\mathbb{Z})(u + m\mathbb{Z})$, por lo que $u + m\mathbb{Z}$ es el inverso de $a + m\mathbb{Z}$.

A la función

$$\begin{array}{rccc} \phi\colon & \mathbb{N}\setminus\{0\} & \longrightarrow & \mathbb{N}\setminus\{0\} \\ & m & \longmapsto & \phi(m) \end{array}$$

que a cada natural positivo m le hace corresponder el orden $\phi(m)$ del grupo $\mathbb{Z}_m^*$ se le llama ***función de Euler****.*

Vamos a dar un procedimiento para calcular $\phi(m)$.

- *Si p es primo, $\phi(p) = p-1$, pues cada natural $1 \leq a \leq p-1$ cumple $mcd(a,p) = 1$.*
- *Si p es un número primo y m un natural positivo,*

  $$\phi(p^m) = p^{m-1}(p-1).$$

  Esto se desprende del hecho de que los naturales $1 \leq a \leq p^m$ que no son primos con p^m son

  $$p, 2p, 3p, \ldots, p^{m-1}p.$$

  Así que hay p^{m-1} que no son primos con p, por lo que

  $$\phi(p^m) = p^m - p^{m-1} = p^{m-1}(p-1).$$

- *Si m y n son primos primos entre sí, $\phi(mn) = \phi(m)\phi(n)$. Para ver esto se trata de encontrar una biyección*

  $$\mathbb{Z}_{mn}^* \longrightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*,$$

  ya que el primer miembro tiene $\phi(mn)$ elementos, y el segundo $\phi(m)\phi(n)$. Y, ¿cúal es esta biyección?, bien pues aquí la tenemos

  $$f\colon \quad a + mn\mathbb{Z} \longrightarrow (a + m\mathbb{Z}, a + n\mathbb{Z}).$$

  Es claro que, si $mcd(a, mn) = 1$, se tendrá

  $$mcd(a,m) = mcd(a,n) = 1.$$

  Además, si $a \in mn\mathbb{Z}$, también $a \in m\mathbb{Z}$ y $a \in n\mathbb{Z}$. Esto prueba que f está bien definida.

  También es inyectiva: si $a + m\mathbb{Z} = b + m\mathbb{Z}$ y $a + n\mathbb{Z} = b + n\mathbb{Z}$, resulta que $a - b$ es múltiplo de m y de n. Y como m y n son primos entre sí, deducimos que $a - b$ es múltiplo de mn, luego $a + mn\mathbb{Z} = b + mn\mathbb{Z}$.

  Lo más sorprendente es que es sobreyectiva. Sea $(x + m\mathbb{Z}, y + n\mathbb{Z}) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Como m y n son primos entre sí, por 1.24.1 existen $u, v \in \mathbb{Z}$ tales que $um + vn = 1$. Sea entonces

  $$a = yum + xvn.$$

  Veamos que si $a + mn\mathbb{Z} \in \mathbb{Z}_{mn}^*$, entonces $f(a + mn\mathbb{Z}) = (x + m\mathbb{Z}, y + n\mathbb{Z})$ probando así la sobreyectividad:

Si $mcd(a, mn) \neq 1$, existirá un primo p que dividirá a ambos. Como p es primo y divide a mn, divide a uno de ellos, digamos m. Entonces también divide a

$$a - yum = xvn,$$

y por ello p ha de dividir a x, v o n. Como $mcd(m, x) = mcd(m, n) = 1$, se sigue que p divide a v. En tal caso dividirá a

$$um + vn = 1,$$

lo cual es absurdo. Por lo tanto, $a + mn\mathbb{Z} \in \mathbb{Z}_{mn}^*$. Como

$$a - x = yum + x(vn - 1) = yum - xum \in m\mathbb{Z},$$

$$a - y = xvn + y(um - 1) = xvn - yvn \in n\mathbb{Z},$$

y así tenemos que

$$f(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z}) = (x + m\mathbb{Z}, y + n\mathbb{Z}).$$

- *Por fin, descomponiendo en factores primos $m = p_1^{a_1} \dots p_k^{a_k}$, resulta*

$$\phi(m) = \phi(p_1^{a_1} \dots p_k^{a_k}) = p_1^{a_1 - 1} \dots p_k^{a_k - 1}(p_1 - 1) \dots (p_k - 1).$$

■

Ya sabemos que los grupos $\mathbb{Z}$ y $\mathbb{Z}/m\mathbb{Z}$, con m un entero positivo, son cíclicos. De hecho, éstos son los únicos grupos cíclicos. Precisaremos enseguida lo que significa esto.

2.3. Homomorfismos

Definición 2.14. *Una aplicación $f\colon G \longrightarrow G'$ entre dos grupos G y G' se llama* ***homomorfismo de grupos*** *si*

$$f(ab) = f(a)f(b) \text{ para cada } a, b \in G.$$

Observación 2.14.1. *Algunas propiedades sobre los homomorfismos de grupos que serán importantes tenerlas en cuenta: (consideraremos f un homomorfismo cualquiera)*

1. *$f(1_G) = 1_{G'}$ ya que*

$$1_{G'} f(1_G) = f(1_G) = f(1_G 1_G) = f(1_G)f(1_G) \Longrightarrow 1_{G'} = f(1_G).$$

2. *$f(a^{-1}) = (f(a))^{-1}$ para cada $a \in G$, puesto que*

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_G) = 1_{G'},$$

$$f(a^{-1})f(a) = f(a^{-1}a) = f(1_G) = 1_{G'}.$$

3. *Se llama* ***núcleo de*** f *a*

$$ker f = \{a \in G : f(a) = 1_{G'}\}.$$

El núcleo es un subgrupo normal de G*. En efecto, dados* $a, b \in ker f$

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1_{G'}(1_{G'})^{-1} = 1_{G'},$$

probando así que $ker f$ *es subgrupo de* G*. Para probar que es normal es suficiente comprobar que* $(ker f)^a \subseteq ker f$ *para cada* $a \in G$*. Si* $x \in (ker f)^a$ *resulta que* $axa^{-1} \in ker f$*, es decir,* $f(axa^{-1}) = 1_{G'}$*, o lo que es lo mismo,* $f(a)f(x)f(a)^{-1} = 1_{G'}$*. Entonces,* $f(a)f(x) = 1_{G'}f(a) = f(a) = f(a)1_{G'}$*, y simplificando* $f(x) = 1_{G'}$*, luego* $x \in ker f$*.*

4. f *es inyectiva si y sólo si* $ker f = \{1_G\}$*.*

Supongamos que f *es inyectiva. Entonces cada* $a \in G$ *distinto de* 1_G *cumplirá*

$$f(a) \neq f(1_G) = 1_{G'}, \text{ luego } a \notin ker f.$$

Como $1_G \in ker f$ *tendremos que* $ker f = \{1_G\}$*.*

Recíprocamente, si $ker f = \{1_G\}$*, dados elementos distintos* $a, b \in G$*, tendremos* $ab^{-1} \neq 1_{G'}$*, luego* $ab^{-1} \notin ker f$*, es decir,*

$$f(ab^{-1}) \neq 1_{G'}.$$

Entonces, $f(a)f(b)^{-1} \neq 1_{G'}$*, de donde* $f(a) \neq f(b)$ *y así* f *es inyectiva.*

5. *Se llama* ***imagen*** *de* f *a la imagen conjuntista, esto es,*

$$im f = \{f(x) : x \in G\}.$$

La imagen es un subgrupo de G' *pues dados* $a = f(x), b = f(y)$*,* $a, b \in im f$*, se tiene*

$$ab^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in im f.$$

6. *Si* $f\colon G \longrightarrow G'$ *es un homomorfismo de grupos y* H' *es un subgrupo de* G'*,*

$$f^{-1}(H') = \{x \in G : f(x) \in H'\}$$

es un subgrupo de G*. Además si* H *es subgrupo normal de* G'*,* $f^{-1}(H')$ *lo es de* G*.*

En efecto, si $x, y \in f^{-1}(H')$*, entonces* $f(x), f(y) \in H'$*, de donde* $f(xy^{-1}) = f(x)f(y)^{-1} \in H'$*, luego* $xy^{-1} \in f^{-1}(H')$*. Para probar la normalidad de* $f^{-1}(H')$ *usamos la condición* (3) *de 2.1: Si* $ab \in f^{-1}(H')$ *se sigue que* $f(a)f(b) = f(ab) \in H'$ *y como* H' *es normal,* $f(ba) = f(b)f(a) \in H'$*. Por lo tanto* $ba \in f^{-1}(H')$*.*

Observemos que $ker f = f^{-1}(\{1_{G'}\})$*.*

7. *Si H es un subgrupo de un grupo G, la inclusión*

$$\begin{array}{rccc} i\colon & H & \longrightarrow & G \\ & x & \longmapsto & x \end{array}$$

es un homomorfismo inyectivo puesto que $i(xy) = xy = i(x)i(y)$ y $x \in ker\, i$ equivale a $i(x) = 1_G$, es decir, $x = 1_G = 1_H$.

8. *Si H es un subgrupo normal de un grupo G, la proyección*

$$\begin{array}{rccc} \pi\colon & G & \longrightarrow & G/H \\ & x & \longmapsto & xH \end{array}$$

es un homomorfismo sobreyectivo. La sobreyectividad es obvia. Además, $\pi(xy) = xyH = (xH)(yH) = \pi(x)\pi(y)$, luego π es homomorfismo.

9. *Si $f\colon G \longrightarrow G'$, $g\colon G' \longrightarrow G''$ son homomorfismos entre grupos, también lo es $g \circ f\colon G \longrightarrow G''$, ya que*

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y).$$

10. *Sean $f\colon G \longrightarrow G'$ un homomorfismo de grupos y $x \in G$ un elemento de orden m.*

    a) *$o(f(x))$ divide a m.*

    b) *Si f es inyectiva, $o(f(x)) = m$.*

    Para lo primero, como $x^m = 1$ se tiene que $1 = f(1) = f(x^m) = f(x)^m$ y así $o(f(x))$ divide a m.

    Para lo segundo, sea $k = o(f(x))$. Entonces $f(x)^k = 1$, luego $f(x^k) = 1$ y $x^k \in kerf = \{1\}$. Así, $x^k = 1$. De nuevo, k ha de ser múltiplo de m. Esto junto con lo visto antes nos da que $k = m$.

11. *Supongamos que $S = \{x_1, \ldots, x_p\}$ es un sistema generador de un grupo G. Entonces, si $f\colon G \longrightarrow G'$, $g\colon G \longrightarrow G'$ son dos homomorfismos tales que $f(x_i) = g(x_i)$, con $1 \leq i \leq p$, se cumple $f = g$. (Abreviadamente diremos que f queda determinado por las imágenes de $x_1, \ldots, x_p$.)*

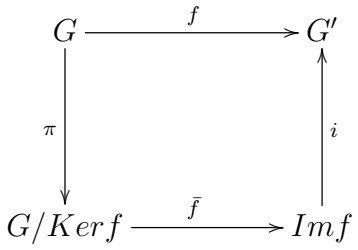
    En efecto: dado $x \in G$ será $x = x_1^{h_1} \ldots x_p^{h_p}, h_1, \ldots, h_p \in \mathbb{Z}$ y así

$$f(x) = f(x_1)^{h_1} \ldots f(x_p)^{h_p} = g(x_1)^{h_1} \ldots g(x_p)^{h_p} = g(x).$$

Proposición 2.15 (***Factorización canónica de un homomorfismo***)**.** *Sea $f\colon G \longrightarrow G'$ un homomorfismo. Entonces existe un homomorfismo biyectivo*

$$\bar{f}\colon G/kerf \longrightarrow imf$$

que hace conmutativo el siguiente diagrama



donde i y π tienen el significado visto en las observaciones 7 y 8 anteriores, notemos que $kerf$ es subgrupo normal, y la conmutatividad del diagrama significa que

$$f = i \circ \bar{f} \circ \pi.$$

Demostración. La última condición nos dice cómo debe ser $\bar{f}$, pues para cada $x \in G$ debe cumplirse:

$$f(x) = (i \circ \bar{f} \circ \pi)(x) = i((\bar{f} \circ \pi)(x)) = i(\bar{f}(\pi(x))) = \bar{f}(\pi(x)) = \bar{f}(xkerf).$$

Y con esto definimos $\bar{f}$. Comprobamos que se cumple lo del enunciado:

1. $\bar{f}$ está bien definida ya que si $xkerf = ykerf$, entonces

   $$x^{-1}y \in kerf \Longrightarrow f(x^{-1}y) = f(x)^{-1}f(y) = 1_{G'}$$

   y así $f(x) = f(y) \Longrightarrow \bar{f}(xkerf) = \bar{f}(ykerf)$.

2. $\bar{f}$ es homomorfismo ya que

   $$\bar{f}((xkerf)(ykerf)) = \bar{f}(xykerf) = f(xy) = f(x)f(y) = \bar{f}(xkerf)\bar{f}(ykerf).$$

3. $\bar{f}$ es inyectiva ya que si $xkerf \in ker\bar{f}$ entonces

   $f(x) = \bar{f}(xkerf) = 1_{imf} = 1_{G'} \Longrightarrow x \in kerf$ y así $xkerf = kerf$, que es el elemento neutro de $G/kerf$ y así $\bar{f}$ es inyectiva.

4. $\bar{f}$ es sobreyectiva, pues cada elemento de imf es de la forma $imf \ni g = f(x) = \bar{f}(xkerf)$ para cierto $x \in G$.

Además la conmutatividad del diagrama es obvia, pues $\bar{f}$ se ha definido para que cumpla esta condición.

□

Definición 2.16. *Un homomorfismo biyectivo entre dos grupos se llama* ***isomorfismo****. Cuando exista un isomorfismo $f\colon G \longrightarrow G'$ diremos que los grupos G y G' son* ***isomorfos****, y escribiremos $G \simeq G'$.*

Observación 2.16.1. *Algunas observaciones:*

1. *El término «G y G' son isomorfos» no es ambiguo, pues si $f\colon G \longrightarrow G'$ es isomorfismo, también lo es $f^{-1}\colon G' \longrightarrow G$.*

   En efecto, como la inversa de toda aplicación biyectiva es biyectiva también, bastará comprobar que f^{-1} es homomorfismo de grupos.

   Ahora bien, si $a, b \in G'$ y $f^{-1}(a) = x$, $f^{-1}(b) = y$, se tiene $f(x) = a, f(y) = b$, luego $f(xy) = f(x)f(y) = ab$, es decir, $xy = f^{-1}(ab)$, de donde $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$.

2. *Dos grupos isomorfos tienen las «mismas propiedades» (siempre que sean propiedades de la teoría de grupos). Por ejemplo*

   a) *Si $G \simeq G'$ y G es abeliano, lo es G' también. En efecto, sean $x, y \in G'$ y $f\colon G \longrightarrow G'$ un isomorfismo. Como f es sobreyectiva, existen $a, b \in G$ con $x = f(a)$, $y = f(b)$. Entonces*

   $$xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx.$$

   b) *Si $G \simeq G'$ y G es cíclico, también G' es cíclico.*

   En efecto, sea $a \in G$ tal que $G = \langle a \rangle$ y $f\colon G \longrightarrow G'$ un isomorfismo. Llamemos $b = f(a)$. Vamos a probar que $G' = \langle b \rangle$.

   Dado $y \in G'$ existe $x \in G$ tal que $y = f(x)$. Como $x \in G = \langle a \rangle$, existe un entero k tal que $x = a^k$. Entonces

   $$y = f(x) = f(a^k) = f(a)^k = b^k \in \langle b \rangle.$$

   c) *Si X e Y son dos conjuntos finitos con n elementos, los grupos $Biy(X)$, $Biy(Y)$ son isomorfos. Esto justifica que llamáramos a ambos S_n en 1.5.1* (3).

   Como X e Y tienen el mismo número de elementos, existe una biyección $f\colon X \longrightarrow Y$. Consideremos

   $$\begin{array}{rccc} \phi\colon & Biy(X) & \longrightarrow & Biy(Y) \\ & g & \longmapsto & f \circ g \circ f^{-1}. \end{array}$$

   Habremos terminado si probamos que ϕ es isomorfismo. Como $\phi(g \circ h) = f \circ (g \circ h) \circ f^{-1} = f \circ g \circ f^{-1} \circ f \circ h \circ f^{-1} = \phi(g) \circ \phi(h)$, ϕ es homomorfismo.

   Si $\phi(g) = \phi(h)$ entonces $f \circ g \circ f^{-1} = f \circ h \circ f^{-1}$, luego $f^{-1} \circ f \circ g \circ f^{-1} \circ f = f^{-1} \circ f \circ h \circ f^{-1} \circ f$, y por lo tanto $g = h$. Así, ϕ es inyectiva.

   Por último, para cada $l \in Biy(Y)$, existe $g = f^{-1} \circ l \circ f \in Biy(X)$ tal que $\phi(g) = f \circ f^{-1} \circ l \circ f \circ f^{-1} = l$, lo que prueba la sobreyectividad de ϕ.

   d) *Dados grupos G_1, G_2, G_3 y G_4 tales que $G_1 \simeq G_3$ y $G_2 \simeq G_4$, se tiene*

      1) $G_1 \times G_2 \simeq G_2 \times G_2$.

      2) $G_1 times G_2 \simeq G_3 \times G_4$.

En efecto, es inmediato que

$$\begin{array}{ccc} G_1 \times G_2 & \longrightarrow & G_2 \times G_1 \\ (x, y) & \longmapsto & (y, x) \end{array}$$

es isomorfismo, lo que prueba la primera parte.

Para la segunda, dejamos al lector que compruebe que si $f\colon G_1 \longrightarrow G_3$ *y* $g\colon G_2 \longrightarrow G_4$ *son isomorfismos, también lo es*

$$h\colon \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & G_3 \times G_4 \\ (x, y) & \longmapsto & (f(x), g(y)). \end{array}$$

Teorema 2.17 (***Primer Teorema de Isomorfía***)**.** *Si* $f\colon G \longrightarrow G$ *es un homomorfismo entre dos grupos* G *y* G*, los grupos* $G/ker f$ *e* imf *son isomorfos. Es decir*

$$G/ker f \simeq imf.$$

Demostración. Consecuencia de la *descomposición canónica.* $\bar{f}\colon G/ker f \longrightarrow imf$ es un isomorfismo como ya se ha visto.

□

Corolario 2.17.1. *Todo grupo cíclico es isomorfo, bien a* $\mathbb{Z}$*, bien a* $\mathbb{Z}/m\mathbb{Z}$*, para algún entero positivo* m*.*

Demostración. Sea $G = \langle a \rangle$ un grupo cíclico. Consideremos

$$f\colon \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & f(k) = a^k. \end{array}$$

Como $f(x+y) = a^{x+y} = a^x a^y = f(x)f(y)$, f es homomorfismo (notar que el grupo $\mathbb{Z}$ tiene operación aditiva).

Cada elemento b de $G = \langle a \rangle$ es de la forma $b = a^k = f(k)$ para algún $k \in \mathbb{Z}$.

Por lo tanto, f es sobreyectiva, es decir, $imf = G$. Por el primer teorema de isomorfía tenemos

$$\mathbb{Z}/ker f \simeq G.$$

Como $ker f$ es un subgrupo de $\mathbb{Z}$, existe un entero no negativo m tal que $ker f = m\mathbb{Z}$.

Si $m = 0$, resulta $ker f = \{0\}$ luego f es inyectiva y como también es sobreyectiva, $\mathbb{Z} = G$.

Si $m > 0$, $\mathbb{Z}/m\mathbb{Z} \simeq G$, lo que termina la demostración.

□

Observación 2.17.1. *Dos grupos finitos isomorfos tienen, evidentemente, el mismo orden* m*. De lo anterior se deduce que para cada entero positivo* m *todos los grupos cíclicos de orden* m *son isomorfos a* $\mathbb{Z}/m\mathbb{Z}$*.*

Ejemplo 2.17.1. *[**Ejemplos de homomorfismos**] Veamos algunos ejemplos de homomorfismos:*

1. *Vamos a calcular todos los homomorfismos $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$.*

   Sea f uno de estos homomorfismos, y $f(1) = a$, con $a \in \mathbb{Z}$, tendremos para cada entero positivo n:

   $$f(n) = f(\underbrace{1 + \ldots + 1}_{n}) = f(1)\underbrace{+ \ldots +}_{n} f(1) = na$$

   mientras que si n es negativo, $m = -n$ será positivo y así

   $$f(n) = f(-m) = -f(m) = -(ma) = (-m)a = na.$$

   Y como $f(0) = 0a$, tenemos que

   $$f(n) = na \text{ para cada } n \in \mathbb{Z}.$$

   Esta aplicación es homomorfismo, ya que

   $$f(n + m) = (n + m)a = na + ma = f(n) + f(m).$$

   Así, los homomorfismos de $\mathbb{Z}$ en $\mathbb{Z}$ son las aplicaciones ($a \in \mathbb{Z}$)

   $$\begin{array}{rccc} f_a\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & n & \longmapsto & na \end{array}$$

2. *Sea $n \geq 3$, X el polígono regular de n lados y $V = \{a_1, \ldots, a_n\}$ el conjunto de vértices de X. Vimos en 1.5.1 (1) que la aplicación*

   $$\begin{array}{rccc} \phi\colon & D_n & \longrightarrow & S_n = Biy(V) \\ & f & \longmapsto & f\big|_V \end{array}$$

   es ineyctiva.

   De hecho, es homomorfismo, ya que

   $$\phi(f \circ g) = (f \circ g)\big|_V = f\big|_V \circ g\big|_V = \phi(f) \circ \phi(g).$$

   Como $ker\phi = \{1\}$, el primer teorema de isomorfía nos dice que

   $$D_n \simeq imf,$$

   y por lo tanto D_n es isomorfo a un subgrupo de S_n, lo cual precisa más 1.15.2. Allí deciamos que D_n era un subgrupo de S_n porque identificabamos f con $f\big|_V$.

3. *La aplicación*

   $$\begin{array}{rccc} f\colon & GL_n(\mathbb{R}) & \longrightarrow & \mathbb{R}^* \\ & A & \longmapsto & \det A \end{array}$$

   es un homomorfismo sobreyectivo de grupos con núcleo $SL_n(\mathbb{R})$ y así, por el primer teorema de isomorfía,

   $$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*.$$

En efecto, $f(AB) = \det(AB) = \det A \cdot \det B = f(A)f(B)$*, luego* f *es homomorfismo. Es evidente que* $kerf = SL_n(\mathbb{R})$ *por definición. Finalmente, si* $a \in \mathbb{R}^*$*, la matriz*

$$A = (a_{ij} : 1 \leq i \leq n,\ 1 \leq j \leq n)$$

definida por

$$a_{ij} = \begin{cases} 0 & si\ i \neq j \\ a & si\ i = j = 1 \\ 1 & si\ i = j > 1 \end{cases}$$

cumple $\det A = a1^{n-1} = a$*, probando la sobreyectividad de* f*.*

4. *Sean* m *y* n *enteros positivos. Anteriormente estudiamos los homomorfismos entre* $\mathbb{Z}$ *y* $\mathbb{Z}$*, ahora vamos a calcular los homomorfismos entre* $\mathbb{Z}/m\mathbb{Z}$ *y* $\mathbb{Z}/n\mathbb{Z}$*. Sea entonces*

$$f\colon \quad \mathbb{Z}/m\mathbb{Z} \ \longrightarrow\ \mathbb{Z}/n\mathbb{Z}$$

uno de ellos. Llamemos

$$f(1 + m\mathbb{Z}) = k + n\mathbb{Z}.$$

Como

$$(m + 1) + m\mathbb{Z} = 1 + m\mathbb{Z},$$

entonces

$$k + n\mathbb{Z} = f((m + 1) + m\mathbb{Z}) = f(\underbrace{(1 + m\mathbb{Z}) + \ldots + (1 + m\mathbb{Z})}_{m+1}) =$$

$$(m + 1)f(1 + m\mathbb{Z}) = (m + 1)(k + n\mathbb{Z}) = k(m + 1) + n\mathbb{Z}.$$

Y así,

$$km \in n\mathbb{Z}.$$

Evidentemente km *es múltiplo de* m *y de* n *luego, si llamamos* $M = mcm(m, n)$*, es claro que* km *es múltiplo de* M*.*

Ahora, si $d = mcd(m, n)$*, entonces* $Md = mn$*. En efecto, sean* $p_1, \ldots, p_k$ *los factores primos comunes a* m *y* n*. Descomponiendo* m *y* n *en producto de números primos será*

$$m = p_1^{\alpha_1} \ldots p_k^{\alpha_k} q_1^{\gamma_1} \ldots q_r^{\gamma_r}$$

$$n = p_1^{\beta_1} \ldots p_k^{\beta_k} l_1^{\delta_1} \ldots l_s^{\delta_s}.$$

Si $\epsilon_j = \max\{\alpha_j, \beta_j\}$ *y* $\mu_j = \min\{\alpha_j, \beta_j\}$ *es claro que*

$$\alpha_j + \beta_j = \epsilon_j + \mu_j,$$

$$d = p_1^{\mu_1} + \ldots + p_k^{\mu_k},$$

$$M = p_1^{\epsilon_1} \ldots p_k^{\epsilon_k} q_1^{\gamma_1} \ldots q_r^{\gamma_r} l_1^{\delta_1} \ldots l_s^{\delta_s},$$

luego

$$Md = p_1^{\epsilon_1+\mu_1} \ldots p_k^{\epsilon_k+\mu_k} q_1^{\gamma_1} \ldots q_r^{\gamma_r} l_1^{\delta_1} \ldots l_s^{\delta_s} =$$
$$p_1^{\alpha_1+\alpha_1} \ldots p_k^{\alpha_k+\beta_k} q_1^{\gamma_1} \ldots q_r^{\gamma_r} l_1^{\delta_1} \ldots l_s^{\delta_s} = mn.$$

Visto esto, como km es múltiplo de M, k es múltiplo de $\frac{M}{m} = \frac{n}{d}$, digamos $k = \frac{n}{d}a$, con $a \in \mathbb{Z}$.

Recíprocamente, si $k = \frac{n}{d}a$, la aplicación

$$\begin{array}{rccc} f_k\colon & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x + m\mathbb{Z} & \longmapsto & kx + n\mathbb{Z}, \end{array}$$

cumple las siguientes propiedades:

a) *Está bien definida, pues si $x + m\mathbb{Z} = y + m\mathbb{Z}$, $x - y \in m\mathbb{Z}$, entonces $x - y = mb$, con algún $b \in \mathbb{Z}$, y en consecuencia,*

$$kx - ky = k(x - y) = \frac{n}{d}a(x - y) = \frac{namb}{d} = \frac{m}{d}abn \in n\mathbb{Z},$$

con lo que $kx + n\mathbb{Z} = ky + n\mathbb{Z}$.

b) *$f_k(1 + m\mathbb{Z}) = k + n\mathbb{Z}$.*

c) *Es homomorfismo ya que*

$$f_k((x + m\mathbb{Z}) + (y + m\mathbb{Z})) = f_k((x + y) + m\mathbb{Z}) = k(x + y) + n\mathbb{Z} = (kx + ky) + n\mathbb{Z} = (kx + n\mathbb{Z}) + (ky + n\mathbb{Z}) = f_k(x + m\mathbb{Z}) + f_k(y + m\mathbb{Z}).$$

Por lo tanto, los homomorfismos entre $\mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ son las aplicaciones f_k vistas ahora, con $k = \frac{n}{d}a$, $d = mcd(m, n)$ y $a \in \mathbb{Z}$.

Una vez visto cómo son, veamos cuántas hay. Es claro que si

$$k = \frac{n}{d}a \text{ y } l = \frac{n}{d}b,$$

las aplicaciones f_k y f_l coincidirán si y sólo si

$$f_k(1 + m\mathbb{Z}) = f_l(1 + m\mathbb{Z}) \ (*),$$

ya que

$$f_k(x + m\mathbb{Z}) = xf_k(1 + m\mathbb{Z}),$$
$$f_l(x + m\mathbb{Z}) = xf_l(1 + m\mathbb{Z}).$$

La condición $(*)$ equivale a

$$k + n\mathbb{Z} = l + n\mathbb{Z},$$

es decir,

$$\frac{n}{d}(a - b) = k - l \in n\mathbb{Z},$$

o lo que es lo mismo

$$a - b \in d\mathbb{Z}.$$

Así, los homomorfismos f_k, con $k = \frac{n}{d}a$, $a = 0, 1, \ldots, d-1$ son todos distintos, mientras que para cualquier otro a, dividiendo tenemos (por el algoritmo de la división)

$$a = dq + r,\ 0 \leq r \leq d - 1,$$

es

$$a - r = dq \in d\mathbb{Z},$$

luego

$$f_{(n/d)a} = f_{(n/d)r}.$$

Por tanto, el número de homomorfismos entre $\mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ es $d = mcd(m, n)$.

Ahora vamos a ver cómo deben ser m y n para que exista algún homomorfismo inyectivo entre $\mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ y, en tal caso, calcular cuáles son.

Si existe un homomorfismo inyectivo $f\colon \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ será, por el primer teorema de isomorfía,

$$\mathbb{Z}/m\mathbb{Z} \simeq imf,$$

luego

$$m = o(imf).$$

Como imf es subgrupo de $\mathbb{Z}/n\mathbb{Z}$, por el teorema de Lagrange,

$$m = o(imf) \text{ divide a } o(\mathbb{Z}/n\mathbb{Z}) = n.$$

Así, n debe ser múltiplo de m. En tal caso, $d = mcd(m, n) = m$ y los homomorfismos entre $\mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ son

$$f_k,\ k = \frac{n}{d}a = \frac{n}{m}a,\ 0 \leq a \leq m - 1.$$

Veamos que f_k es inyectiva si y sólo si $mcd(a, m) = 1$. Desde luego, si $mcd(a, m) = c \neq 1$, escribimos

$$a = cu,$$

$$m = cv,$$

con lo que $av = mu$. Como $c \neq 1$, $v \notin m\mathbb{Z}$, esto es, $v + m\mathbb{Z} \neq 0 + m\mathbb{Z}$. Sin embargo,

$$f_k(v + m\mathbb{Z}) = kv + n\mathbb{Z} = \frac{n}{m}av + n\mathbb{Z} = \frac{n}{m}mu + n\mathbb{Z} = nu + n\mathbb{Z} = 0 + n\mathbb{Z},$$

con lo que $v + m\mathbb{Z} \in ker f_k$ y f_k no es inyectiva.

Recíprocamente, supongamos que $mcd(a, m) = 1$. Si $x + m\mathbb{Z} \in ker f_k$ debe ser $kx \in n\mathbb{Z}$, es decir

$$\frac{n}{m}ax \in n\mathbb{Z},$$

luego

$$ax \in m\mathbb{Z}.$$

Como $mcd(a,m)=1$, *por 1.24.1*

$$1 = as + mt,\ s,t \in \mathbb{Z}$$

y por tanto

$$x = (ax)s + m(tx) \in m\mathbb{Z},$$

y así

$$x + m\mathbb{Z} = 0 + m\mathbb{Z}.$$

Por lo que f_k *es inyectiva.*

Así, para que existan homomorfismos inyectivos $\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, n *debe ser múltiplo de* m *y en tal caso los homomorfismos inyectivos son*

$$\begin{array}{rccc} f_k\colon & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x + m\mathbb{Z} & \longmapsto & kx + n\mathbb{Z}, \end{array}$$

para $k = \dfrac{n}{m}a$, $0 \leq a \leq m-1$, $mcd(a,m) = 1$.

Por lo tanto, el número de homomorfismos inyectivos entre $\mathbb{Z}/m\mathbb{Z}$ *y* $\mathbb{Z}/n\mathbb{Z}$, *cuando* m *divide a* n, *coincide con el orden* $\phi(m)$ *de* $\mathbb{Z}_m^*$.

Terminamos este largo ejemplo estudiando en qué condiciones existen homomorfismos sobreyectivos entre $\mathbb{Z}/m\mathbb{Z}$ *y* $\mathbb{Z}/n\mathbb{Z}$ *y en tal caso, calculando cuántos hay.*

Si existe $f\colon \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ *homomorfismo sobreyectivo, tendremos*

$$(\mathbb{Z}/m\mathbb{Z})/kerf \simeq imf \simeq \mathbb{Z}/n\mathbb{Z},$$

luego $[\mathbb{Z}/m\mathbb{Z} : kerf] = n$ *y por el teorema de Lagrange*

$$\frac{m}{o(kerf)} = n.$$

Por ello, m *debe ser múltiplo de* n. *Entonces* $mcd(n,m) = n$ *con lo que si* f_k *es homomorfismo tendremos*

$$k = \frac{n}{n}a = a,\ \ 0 \leq a \leq n-1,$$

esto es,

$$f_k\colon x + m\mathbb{Z} \longmapsto kx + n\mathbb{Z},\ \ 0 \leq k \leq n-1$$

son, en este caso, los homomorfismos entre $\mathbb{Z}/m\mathbb{Z}$ *y* $\mathbb{Z}/n\mathbb{Z}$.

Para que f_k *sea sobreyectivo es suficiente (y por supuesto necesario) que* $1 + n\mathbb{Z} \in imf_k$, *pues si* $1 + n\mathbb{Z} = f_k(u + m\mathbb{Z})$, *cada* $x + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ *se escribe como*

$$x + n\mathbb{Z} = f_k(xu + m\mathbb{Z}).$$

Así, f_k *es sobreyectiva si y sólo si existe* $u \in \mathbb{Z}$ *tal que* $ku + n\mathbb{Z} = 1 + n\mathbb{Z}$, *o lo que es igual, existe* $v \in \mathbb{Z}$ *tal que* $ku - 1 = nv \in n\mathbb{Z}$.

Llamando $w = -v$, lo anterior se convierte en $1 = ku + nw$, $u, w \in \mathbb{Z}$. Por 1.24.1 esto equivale a decir que $mcd(k, n) = 1$.

Resumiendo, para que exista algún homomorfismo sobreyectivo de $\mathbb{Z}/m\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$, m debe ser múltiplo de n y en tal caso,

$$\begin{array}{rccc} f_k\colon & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x + m\mathbb{Z} & \longmapsto & kx + n\mathbb{Z}, \end{array}$$

con $0 \leq k \leq n-1$, $mcd(k, n) = 1$, son los homomorfismos sobreyectivos entre $\mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$. El número de ellos es, evidentemente, $\phi(n)$.

5. *Sea G un grupo abeliano y*

$$\begin{array}{rccc} f\colon & G & \longrightarrow & G \\ & x & \longmapsto & x^2 \end{array}$$

una aplicación que es homomorfismo ya que

$$f(xy) = (xy)^2 = xyxy = xxyy = x^2y^2 = f(x)f(y).$$

(De hecho, de 1.11 (2) deducimos que G es abeliano si y sólo si f es homomorfismo).

Observar que

$$kerf = \{x \in G : x^2 = 1\}$$

está formado por 1 y todos los elementos de orden 2 de G. Por ejemplo si $G = \mathbb{R}^*$, entonces $x^2 = 1$ equivale a $(x+1)(x-1) = 0$, y así $kerf = \{+1, -1\}$. A este grupo lo denotaremos U_2. En particular, f no es inyectiva. Cuando G es finito, entonces f es inyectiva si y sólo si el orden de G es impar.

Demostración. Supongamos que $o(G) = 2k + 1$ es impar y sea $x \in kerf$. Así $x^2 = 1$ y también $x^{2k+1} = 1$, por ser el orden de G. Entonces

$$x = x1 = x1^k = x(x^2)^k = x^{2k+1} = 1$$

y así f es inyectiva.

Recíprocamente, veamos que si $o(G) = 2k$ es par, sea o no G abeliano, f no es inyectiva. (Esto se deduce directamente del teorema de Cauchy pero lo haremos aquí «artesanalmente»).

Para cada $x \in G$ llamaremos $A_x = \{x, x^{-1}\}$. Los distintos A_x constituyen una partición de G pues como cada $x \in A_x$, la igualdad

$$G = \bigcup_{x \in G} A_x$$

es obvia, además si $A_x \cap A_y \neq \emptyset$ entonces $x \in \{y, y^{-1}\}$ ó $x^{-1} \in \{y, y^{-1}\}$.

Para el primer caso, si $x = y$ entonces $x^{-1} = y^{-1}$ y $A_x = A_y$, y si $x = y^{-1}$ entonces $x^{-1} = y$ y nuevamente $A_x = A_y$. Análogamente para el segundo caso.

Es claro que $A_1 = \{1\}$, pues $1^{-1} = 1$. Si el resto de los A_x (digamos que hay m de ellos) tuviese dos elementos, entonces

$$2k = o(G) = cardA_1 + 2m = 2m + 1, \text{ que es impar.}$$

Esto es absurdo, luego ha de existir $1 \neq a \in G$ tal que $cardA_a = 1$. Esto significaría que $a^{-1} = a$, y así $f(a) = a^2 = aa^{-1} = 1 = f(1)$. Por tanto, f no es inyectiva.

□

Esto se puede reformular diciendo: «Todo grupo finito de orden par posee algún elemento de orden 2».

6. *Sea $n \geq 2$ un número natural, $X = \{1, 2, \ldots, n\}$ y $f \in S_n = Biy(X)$. Llamamos* ***signatura*** *de f y notaremos por $s(f)$ el número de pares $(i, j) \in X \times X$ tales que $i < j$ y $f(i) > f(j)$. La aplicación*

$$\begin{array}{rccc} \epsilon: & S_n & \longrightarrow & U_2 = \{+1, -1\} \\ & f & \longmapsto & \epsilon(f) = (-1)^{s(f)} \end{array}$$

es homomorfismo de grupos; nótese que

$$\epsilon(f) = \prod_{i<j} \frac{f(i) - f(j)}{i - j}$$

pues al ser f biyectiva los factores del numerador son, salvo el signo, los del denominador, y hay tantos factores con signos distintos en numerador y denominador como $s(f)$. Entonces, si $f, g \in S_n$,

$$\epsilon(f \circ g) = \prod_{i<j} \frac{f(g(i)) - f(g(j))}{i - j} =$$
$$\prod_{i<j} \frac{f(g(i)) - f(g(j))}{g(i) - g(j)} \cdot \prod_{i<j} \frac{g(i) - g(j)}{i - j} = \epsilon(f)\epsilon(g).$$

El número $\epsilon(f)$ se suele llamar ***índice*** *de f y el núcleo*

$$ker\epsilon = \{f \in S_n : \epsilon(f) = 1\}$$

es el llamado ***grupo alternado****, que denotaremos A_n.*

Observar que por 2.14.1 (3) A_n es subgrupo normal de S_n y por el primer teorema de isomorfía

$$S_n/A_n \simeq U_2.$$

En particular,

$$[S_n : A_n] = o(S_n/A_n) = o(U_2) = 2$$

y usando el teorema de Lagrange

$$\frac{o(S_n)}{o(A_n)} = 2,$$

de donde $o(A_n) = \dfrac{n!}{2}$.

■

Remarcamos del ejemplo anterior (2.17.1) el apartado (4), que lo podemos resumir en, dados enteros positivos m, n:

1. Los homomorfismos entre $\mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ serán de la forma

$$\begin{array}{rccc} f_k\colon & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x+m\mathbb{Z} & \longmapsto & kx+n\mathbb{Z} \end{array},$$

   con $k = \dfrac{n}{d}a$, $d = mcd(m,n)$ y $a \in \mathbb{Z}$.

2. Para que existan homomorfismos inyectivos entre $\mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ n ha de ser múltiplo de m y los homomorfismos serán de la forma

$$\begin{array}{rccc} f_k\colon & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x+m\mathbb{Z} & \longmapsto & kx+n\mathbb{Z} \end{array}, \quad k = \frac{n}{m}a,\ 0 \le a \le m-1,\ mcd(a,m) = 1.$$

   Habrá $\phi(m)$.

3. Para que existan homomorfismos sobreyectivos entre $\mathbb{Z}/m\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$ m ha de ser múltiplo de n y los homomorfismos serán de la forma

$$\begin{array}{rccc} f_k\colon & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & x+m\mathbb{Z} & \longmapsto & kx+n\mathbb{Z} \end{array}, \quad 0 \le k \le n-1,\ mcd(k,n) = 1.$$

   Habrá $\phi(n)$.

2.4. Teoremas de Isomorfía

Vamos a probar otros teoremas de isomorfía.

Teorema 2.18 (***Segundo teorema de isomorfía***)**.** *Sean N y H subgrupos normales de un grupo G, tales que $N \subseteq H$. Entonces H/N es subgrupo normal de G/N y*

$$(G/N)/(H/N) \simeq G/H.$$

Demostración. Consideremos la aplicación

$$\begin{array}{rccc} f\colon & G/N & \longrightarrow & G/H \\ & aN & \longmapsto & aH \end{array},$$

que está bien definida, pues si $aN = bN$ se tiene

$$ab^{-1} \in N \subseteq H, \text{ luego } aH = bH.$$

Como $f((aN)(bN)) = f(abN) = abH = (aH)(bH) = f(aN)f(bN)$, f es homomorfismo.

Cada $aH \in G/H$ es de la forma $aH = f(aN)$ y así f es sobreyectiva.

Por último, $aN \in kerf \iff aH = f(aN) = H$, es decir,

$$kerf = \{aN \in G/N : a \in H\} = H/N.$$

Y por el primer teorema de isomorfía, $(G/N)/kerf \simeq imf$, y como $imf = G/H$, por ser f sobreyectiva, y $kerf = H/N$ se tiene

$$(G/N)/(H/N) \simeq G/H.$$

□

Este resultado ya lo vimos en 2.12.1.

Teorema 2.19. *[**Tercer teorema de isomorfía**] Sean H y N subgrupos de un grupo G, con N subgrupo normal de G. Entonces:*

1. *$H \cap N$ es subgrupo normal de H.*
2. *HN es subgrupo de G.*
3. *N es subgrupo normal de HN.*
4. *$HN/N \simeq H/(H \cap N)$.*

Demostración. Lo probaremos por partes.

1. Veamos que se cumple la condición (3) de 2.1. Sean $a, b \in H$ tales que $ab \in H \cap N$. Entonces $ab \in N$, $a, b \in G$. Como N es subgrupo normal de G, $ba \in N$. Además $ba \in H$, ya que $b, a \in H$, luego $ba \in H \cap N$.
2. Tenemos que probar que $HN = NH$ (como ya sabemos del primer capítulo). Si $x \in HN$, existen $h \in H$, $n \in N$ tales que $x = hn$. En particular;

   $$x \in hN = Nh \subseteq NH,$$

   ya que N es normal. Esto prueba que $HN \subseteq NH$ y el otro contenido es análogo.
3. Se sigue de
4. Definimos

   $$\begin{array}{rccc} f\colon & H & \longrightarrow & HN/N \\ & h & \longmapsto & hN \end{array}$$

   que evidentemente es un homomorfismo.

   Veamos que $imf = HN/N$. Dado $xN \in HN/N$ será

   $$x = hn,\ h \in H,\ n \in N.$$

   Entonces $x^{-1}h = n^{-1}h^{-1}h = n^{-1} \in N$, luego $xN = hN = f(h)$.

   Veamos que $kerf = H \cap N$.

$x \in kerf$ quiere decir que $x \in H$ y $xN = N$, es decir, $x \in H$, $x \in N$ y, por lo tanto, $x \in H \cap N$.

Así, por el primer teorema de isomorfía,

$$H/kerf \simeq Imf \Longrightarrow H/(H \cap N) \simeq HN/N.$$

□

Antes de probar el cuarto teorema de isomorfía necesitamos:

Lema 2.19.1. *Sean A, B y C tres subgrupos de un subgrupo G, $B \subseteq A$. Entonces*

$$A \cap BC = B(A \cap C).$$

Demostración. $B(A \cap C) \subseteq BC$ porque $A \cap C \subseteq C$. Como $B \subseteq A$ y $A \cap C \subseteq A$, se sigue, al ser A subgrupo, que

$$B(A \cap C) \subseteq A.$$

En consecuencia, $B(A \cap C) \subseteq A \cap BC$.

Recíprocamente, sea $a \in A \cap BC$. Entonces $a \in A$ y existen $b \in B$, $c \in C$, tales que $a = bc$. De este modo, $c = b^{-1}a$, $b^{-1} \in B \subseteq A$. Por ello,

$$c = b^{-1}a \in A \cap C,$$

de donde $a = bc \in B(A \cap C)$, lo que prueba el otro contenido.

□

Teorema 2.20 (***Cuarto teorema de isomorfía***)**.** *Sean G un grupo, H_1 y H_2 subgrupos de G, N_1 subgrupo normal de H_1 y N_2 subgrupo normal de H_2. Entonces*

1. *$N_1(H_1 \cap H_2)$ y $N_2(H_1 \cap H_2)$ son subgrupos, respectivamente, de H_1 y H_2.*
2. *$N_1(H_1 \cap N_2)$ es subgrupo normal de $N_1(H_1 \cap H_2)$ y $N_2(N_1 \cap H_2)$ es subgrupo normal de $N_2(H_1 \cap H_2)$.*
3. *$(H_1 \cap N_2)(N_1 \cap H_2)$ es subgrupo normal de $H_1 \cap H_2$.*
4. *$(N_1(H_1 \cap H_2))/(N_1(H_1 \cap N_2)) \simeq (H_1 \cap H_2)/(H_1 \cap N_2)(N_1 \cap H_2) \simeq (N_2(H_1 \cap H_2))/(N_2(N_1 \cap H_2))$.*

Demostración. Lo haremos por partes:

1. Es consecuencia inmediata de 2.19 (2), pues para $i = 1, 2$, N_i es subgrupo normal del grupo H_i y $H_1 \cap H_2$ es subgrupo de H_i.
2. Por simetría, basta ver la primera parte. Como N_2 es subgrupo normal de H_2 y $H_1 \cap H_2$ es subgrupo de H_2, de (1) de 2.19 se deduce que $(H_1 \cap H_2) \cap N_2$ es subgrupo normal de $H_1 \cap H_2$, es decir, $H_1 \cap N_2$ es subgrupo normal de $H_1 \cap H_2$, y ambos son subgrupos del grupo H_1.

   Ahora el resultado se sigue de 2.8, pues N_1 es subgrupo normal de H_1.

3. Basta demostrar que si $a \in H_1 \cap H_2$,

$$a(H_1 \cap N_2)(N_1 \cap H_2) = (H_1 \cap N_2)(N_1 \cap H_2)a.$$

Probaremos que el primer miembro está contenido en el segundo y dejamos al lector la comprobación del otro contenido.

Si $x \in a(H_1 \cap N_2)(N_1 \cap H_2)$, se escribirá

$$x = auv, u \in H_1 \cap N_2, v \in N_1 \cap H_2.$$

Como $au \in aN_2$, $a \in H_2$ y N_2 es subgrupo normal de H_2, $au = n_2a$, $n_2 \in N_2$.

Además, $n_2 = aua^{-1} \in H_1$, pues $a, u \in H_1$. Así, $x = auv = n_2av$, $n_2 \in H_1 \cap N_2$.

Como $av \in aN_1$, $a \in H_1$ y N_1 es subgrupo normal de H_1, $av = n_1a$, $n_1 \in N_1$.

Además, $n_1 = ava^{-1} \in H_2$, pues $a, v \in H_2$. Por tanto, $x = n_2n_1a$, $n_2 \in H_1 \cap N_2$, $n_1 \in N_1 \cap H_2$, es decir, $x \in (H_1 \cap N_2)(N_1 \cap H_2)a$.

4. Llamemos $H = H_1 \cap H_2$, $N = N_1(H_1 \cap N_2)$, $G' = N_1(H_1 \cap H_2)$. Sabemos que H es subgrupo de G' y, por (2), N es subgrupo normal de G'.

Aplicando el tercer teorema de isomorfía (aquí el grupo «ambiente» es G') se tiene

$$(N_1(H_1 \cap N_2)(H_1 \cap H_2))/(N_1(H_1 \cap N_2)) = NH/N = HN/N \simeq H/(H \cap N) = (H_1 \cap H_2)/(H_1 \cap H_2 \cap N_1(H_1 \cap N_2)). \ (*)$$

Los subgrupos $A = H_1$, $B = H_1 \cap N_2$, $C = H_2$ cumplen $B \subseteq A$. En virtud del lema anterior,

$$A \cap BC = B(A \cap C), \ es\ decir\ , H_1 \cap (H_1 \cap N_2)H_2 = (H_1 \cap N_2)(H_1 \cap H_2).$$

Ahora bien, $H_1 \cap N_2 \subseteq N_2 \subseteq H_2$. Por 1.24.1, $(H_1 \cap N_2)H_2 = H_2$, luego $H_1 \cap H_2 = (H_1 \cap N_2)(H_1 \cap H_2)$ y multiplicando ambos miembros por N_1,

$$N_1(H_1 \cap H_2) = N_1(H_1 \cap N_2)(H_1 \cap H_2).$$

Sustituyendo en $(*)$ obtenemos

$$(N_1(H_1 \cap H_2))/(N_1(H_1 \cap N_2)) \simeq (H_1 \cap H_2)/(H_1 \cap H_2 \cap N_1(H_1 \cap N_2)). \ (**)$$

Aplicamos de nuevo el lema anterior, ahora con

$$A = H_1 \cap H_2, B = H_1 \cap N_2, C = N_1,$$

y obtenemos

$$H_1 \cap H_2 \cap (H_1 \cap N_2)N_1 = A \cap BC = B(A \cap C) = (H_1 \cap N_2)(H_1 \cap H_2 \cap N_1) = (H_1 \cap N_2)(N_1 \cap H_2),$$

pues $N_1 \subseteq H_1$.

Como $N_1(H_1 \cap N_2)$ es subgrupo, se tiene $N_1(H_1 \cap N_2) = (H_1 \cap N_2)N_1$, y así

$$H_1 \cap H_2 \cap N_1(H_1 \cap N_2) = H_1 \cap H_2 \cap (H_1 \cap N_2)N_1 = (H_1 \cap N_2)(N_1 \cap H_2).$$

Sustituyendo en $(**)$ obtenemos finalmente

$$(N_1(H_1 \cap H_2))/(N_1(H_1 \cap N_2)) \simeq (H_1 \cap H_2)/((H_1 \cap N_2)(N_1 \cap H_2)).$$

Esto prueba la primera parte. La segunda se obtiene a partir de ésta por simetría.

□

2.5. Teorema de estructura de los grupos abelianos finitos

Comentario. Terminamos este capítulo utilizando los teoremas de isomorfía para estudiar cuáles son los grupos abelianos finitos. Ya vimos en 1.35 que no todo grupo abeliano es cíclico. Sin embargo, vamos a probar que los finitos son *producto directo de grupos cíclicos.*

Lema 2.20.1. *Sea G un grupo abeliano finito y $x \in G$ un elemento de orden máximo. Entonces, para cada $y \in G$ el orden de y divide al de x.*

Demostración. Sea $n = o(x)$ y sea $y \in G$ con $o(y) = m$. Si m no dividiese a n, en la factorización de ambos como producto de primos aparecería un factor primo p más veces en m que en n, esto es,

$$m = p^k a, \;\; k \geq 1, \; a \text{ no múltiplo de } p,$$

$$n = p^h b, \;\; k > h \geq 0, \; b \text{ no múltiplo de } p.$$

En virtud de 1.26 (7) se deduce

$$o(x^{p^h}) = n/p^h = b, \;\; o(y^a) = m/a = p^k.$$

Como G es abeliano y $mcd(b, p^k) = 1$, se sigue de 1.26 (9) que el orden de $z = x^{p^h} \cdot y^a$ es $o(z) = bp^k > bp^h = o(x)$ en contradicción con la definición de x.

□

3. Grupos abelianos finitamente generados. Acciones de grupos sobre conjuntos

3.1. Grupos abelianos finitamente generados

3.2. Algoritmo para la obtención del número de Betti y los coeficientes de torsión

3.3. Generadores y relaciones

3.4. Acciones de grupos sobre conjuntos