Estructuras Algebraicas (UNED)

Pablo Pallàs

8 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 $H = m\mathbb{Z}$.

■

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

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

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

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

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. *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,

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

   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,

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

   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

$$\begin{array}{ccc} G/R_H & \longrightarrow & G/R_{H_1} \times \ldots \times G/R_{H_t} \\ Ha & \longmapsto & (H_1a, \ldots, H_ta) \end{array}$$

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 $H_ja = H_jb$ 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*

$$\begin{aligned} ij &= k, \;\; ji = -k \\ jk &= i, \;\; kj = -i \\ ki &= j, \;\; ik = -j \\ i^2 &= j^2 = k^2 = -1 \end{aligned}$$

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.*

2. Subgrupos normales. Grupos cocientes. Homomorfismos

2.1. Subgrupos normales

2.2. Grupos cocientes

2.3. Homomorfismos

2.4. Teorema de estructura de los grupos abelianos finitos

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