Capítulo 6
Generadores

En este capítulo veremos más ejemplos concretos de grupos y subgrupos. Un caso muy importante es el subgrupo generado por una colección de elementos. Cuando un grupo puede ser generado por un solo elemento, se dice que es cíclico. Ya conocimos a los grupos cíclicos (son precisamente los grupos aditivos $\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}$), pero ahora vamos a investigar sus propiedades de manera más sistemática.

6.1 Subgrupos generados

6.1.1. Observación. *Sea G un grupo y $X \subset G$ algún subconjunto. Entonces existe un subgrupo mínimo de G que contiene a X. Este se denota por $\langle X \rangle$ y consiste precisamente en todos los productos finitos de la forma*

$$g_1^{\epsilon_1} \cdots g_k^{\epsilon_k}, \quad k \geq 0,$$

donde $g_i \in X$ y $\epsilon_i = \pm 1$. Para $k = 0$ el producto vacío se considera como la identidad $1 \in G$.

Demostración. Evidentemente, tenemos

$$\langle X \rangle = \bigcap_{\substack{H \subseteq G \text{ subgrupo} \\ X \subseteq H}} H.$$

Este es un subgrupo, siendo una intersección de subgrupos. Luego, junto con todos los elementos de X, este debe contener todos sus inversos y sus productos, de donde el conjunto de productos finitos $g_1^{\epsilon_1} \cdots g_k^{\epsilon_k}$ está contenido en $\langle X \rangle$. Pero este conjunto es un subgrupo, y por lo tanto coincide con $\langle X \rangle$. ■

6.1.2. Comentario. Escribamos el resultado de arriba para los grupos abelianos usando la notación aditiva. Si A es un grupo aditivo y $X \subset A$ es su subconjunto, entonces tenemos

$$\langle X \rangle = \{ \sum_{a \in X} n_a \, a \mid n_a \in \mathbb{Z},\ a \in X,\ n_a \neq 0 \text{ solo para un número finito de } a \}$$

(en otras palabras, tenemos combinaciones $\mathbb{Z}$-lineales *finitas* de los elementos de X.)

6.1.3. Definición. Se dice que $\langle X \rangle$ es el subgrupo de G **generado** por X. Si $\langle X \rangle = G$, se dice que los elementos de X son **generadores** de G.

Por supuesto, $X = G$ es un conjunto de generadores para cualquier grupo G. Pero en realidad, muchos grupos pueden ser generados por pocos elementos, muchos grupos infinitos se generan por un número finito de elementos, etc.

6.1.4. Definición. Si G posee un conjunto finito de generadores, se dice que G es **finitamente generado**.

6.1.5. Ejemplo. Hemos visto que el grupo diédrico D_n es generado por dos elementos r (rotación) y f (reflexión):

$$D_n = \langle r, f \rangle.$$

▲

6.1.6. Ejemplo. En el capítulo sobre los grupos simétricos y alternantes hemos visto que los siguientes son conjuntos de generadores para S_n:

- todas las transposiciones $(i\ j)$ para $1 \leq i < j \leq n$,
- las transposiciones $(1\ 2)$, $(2\ 3)$, $(3\ 4)$, …, $(n-1\ n)$,
- las transposiciones $(1\ 2)$, $(1\ 3)$, …, $(1\ n)$,
- una transposición $(1\ 2)$ y un n-ciclo $(1\ 2\ \cdots\ n)$.

De modo similar, para el grupo alternante A_n con $n \geq 3$, tenemos los siguientes conjuntos de generadores:

- todos los 3-ciclos $(i\ j\ k)$,
- los 3-ciclos de la forma $(1\ 2\ i)$,
- los 3-ciclos de la forma $(i\ i+1\ i+2)$,
- el 3-ciclo $(1\ 2\ 3)$ y el ciclo

$$\begin{cases} (2\ 3\ \cdots\ n), & \text{si } n \text{ es par,} \\ (1\ 2\ 3\ \cdots\ n), & \text{si } n \text{ es impar.} \end{cases}$$

▲

6.1.7. Ejemplo. El grupo

$$\mathrm{SL}_2(\mathbb{Z}) := \{A \in M_2(\mathbb{Z}) \mid \det A = 1\}$$

puede ser generado por dos matrices:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Calculamos que

$$S^2 = -I, \quad T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \text{para todo } n \in \mathbb{Z}.$$

Si tenemos una matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ con $c = 0$, entonces $ad = 1$ y luego $A = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}$. Pero

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = T^b, \quad \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} = S^2\, T^{-b}.$$

Ahora vamos a ver que toda matriz en $\mathrm{SL}_2(\mathbb{Z})$ puede ser "reducida" a una matriz con $c = 0$ mediante multiplicaciones por S y T. Calculamos el efecto de la multiplicación por S y T^n para $n \in \mathbb{Z}$:

$$S \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix},$$
$$T^n \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}.$$

Si en una matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tenemos $c \neq 0$ y $|a| < |c|$, podemos pasar a $S \cdot A$ donde $|a| \geq |c|$. Entonces, se puede asumir que $|a| \geq |c|$. La división con resto nos da

$$a = cq + r, \quad \text{para } 0 \leq r < |c|.$$

Luego,

$$T^{-q}A = \begin{pmatrix} a-qc & b-qd \\ c & d \end{pmatrix} = \begin{pmatrix} r & b-qd \\ c & d \end{pmatrix}.$$

Multipliquemos esta matriz por S:

$$ST^{-q}A = S \cdot \begin{pmatrix} r & b-qd \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ r & b-qd \end{pmatrix}.$$

Hemos obtenido una matriz donde el valor absoluto del primer elemento en la segunda fila se volvió estrictamente más pequeño. Podemos continuar de esta manera hasta que este se vuelva nulo. Esto quiere decir que para alguna matriz $B \in \langle S, T \rangle$, la matriz BA es de la forma $\begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix} \in \langle S, T \rangle$. Podemos concluir que $A \in \langle S, T \rangle$.

Lo que acabamos de describir es un *algoritmo* que a partir de toda matriz en $\mathrm{SL}_2(\mathbb{Z})$ produce su expresión en términos se S y T. ▲

6.1.8. Ejemplo. Los números racionales $\mathbb{Q}$ respecto a la adición forman un grupo que no es finitamente generado. De hecho, sea $X \subset \mathbb{Q}$ un subconjunto finito:

$$X = \left\{ \frac{a_1}{b_1}, \ldots, \frac{a_k}{b_k} \right\}.$$

Entonces,

$$\langle X \rangle = \left\{ n_1 \frac{a_1}{b_1} + \cdots + n_k \frac{a_k}{b_k} \;\middle|\; n_1, \ldots, n_k \in \mathbb{Z} \right\}.$$

Sin embargo,

$$n_1 \frac{a_1}{b_1} + \cdots + n_k \frac{a_k}{b_k} = \frac{\text{algún entero}}{b_1 \cdots b_k}.$$

En particular, si p es algún primo que no divide a ningún denominador $b_1, \ldots, b_k$, entonces $\frac{1}{p} \notin \langle X \rangle$. ▲

6.2 Orden de un elemento

Un caso muy particular de subgrupos generados $\langle X \rangle \subseteq G$ es cuando el conjunto X tiene solo un elemento g. En este caso el subgrupo generado por g es

$$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}.$$

Hay dos posibilidades diferentes.

1) Si todas las potencias g^n son diferentes, entonces $\langle g \rangle$ es un subgrupo infinito.

2) Si tenemos $g^k = g^\ell$ para algunos $k \neq \ell$, entonces sin pérdida de generalidad $k > \ell$, luego $g^{k-\ell} = 1$ y se ve que la sucesión $(g^n)_{n\in\mathbb{Z}}$ es periódica y el subgrupo $\langle g \rangle$ es finito.

6.2.1. Definición. Para un elemento $g \in G$, el mínimo número $n = 1, 2, 3, \ldots$ tal que $g^n = 1$ se llama el **orden** de g y se denota por $\operatorname{ord} g$. Si $g^n \neq 1$ para ningún n, se dice que g tiene orden infinito.

(Como siempre, vamos a usar la notación multiplicativa para la teoría general, pero no olvidemos que para un grupo abeliano con notación aditiva, en lugar de "$g^n = 1$" se escribe "$n \cdot a = 0$".)

6.2.2. Observación. *Si G es un grupo finito, entonces todos sus elementos tienen orden finito.*

Demostración. Si g tuviera orden infinito, entre los elementos g^n para $n \in \mathbb{Z}$ no habría repeticiones. Esto no es posible si G es finito. ■

6.2.3. Ejemplo. La identidad $1 \in G$ es el único elemento de orden 1. ▲

6.2.4. Ejemplo. Un elemento g tiene orden 2 si y solamente si $g \neq 1$ y $g^{-1} = g$. ▲

6.2.5. Ejemplo. En el grupo diédrico la reflexión f tiene orden 2, ya que $f^2 = \mathrm{id}$ y la rotación r tiene orden n. ▲

6.2.6. Ejemplo. La matriz $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ tiene orden 4 en $\mathrm{SL}_2(\mathbb{Z})$. De hecho,

$$S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I,\ S^3 = -S,\ S^4 = (S^2)^2 = I.$$

La matriz $R = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ tene orden 3:

$$R^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},\ R^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Sin embargo, el producto

$$SR = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} =: T$$

tiene orden infinito: para todo $n \in \mathbb{Z}$ tenemos

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Recordamos que hemos visto en 6.1.7 que las matrices S y T generan el grupo $\mathrm{SL}_2(\mathbb{Z})$. Ya que $T = SR$, se sigue que S y R generan $\mathrm{SL}_2(\mathbb{Z})$. ▲

Este ejemplo demuestra que en general, en un grupo no abeliano, no hay ninguna relación entre $\operatorname{ord} g$, $\operatorname{ord} h$ y $\operatorname{ord}(gh)$: puede ser que $\operatorname{ord} g < \infty$, $\operatorname{ord} h < \infty$, pero $\operatorname{ord} gh = \infty$. Esto sucede solamente para grupos no abelianos. El caso de grupos abelianos es más sencillo y más adelante vamos a describir la estructura de grupos abelianos finitamente generados.

Examinemos algunas propiedades básicas de órdenes.

6.2.7. Observación. *Si g es un elemento de orden finito, entonces para todo número entero m tenemos*

$$g^m = 1 \quad \textit{si y solamente si} \quad \operatorname{ord} g \mid m.$$

(En la notación aditiva: $m \cdot a = 0$ si y solamente si $\operatorname{ord} a \mid m$.)

Demostración. Sea $n = \operatorname{ord} g$. Podemos dividir con resto m por n:

$$m = qn + r, \quad \text{para algún } 0 \leq r < n.$$

Luego,

$$g^m = g^{qn+r} = (g^n)^q \cdot q^r = g^r = 1,$$

pero puesto que $r < n$ y n es el mínimo número positivo tal que $g^n = 1$, se sigue que $r = 0$. ■

6.2.8. Ejemplo. El orden de un k-ciclo $(i_1\ i_2\ \cdots\ i_k)$ en el grupo simétrico S_n es igual a k. En general, para toda permutación $\sigma \in S_n$ podemos considerar su descomposición en ciclos disjuntos

$$\sigma = \tau_1 \cdots \tau_s.$$

Luego, los τ_i conmutan entre sí, así que

$$\sigma^k = \tau_1^k \cdots \tau_s^k.$$

Los τ_i^k son también disjuntos para cualquier k, así que $\sigma^k = \mathrm{id}$ si y solamente si $\tau_i^k = \mathrm{id}$ para todo i. Entonces,

$$\operatorname{ord}(\sigma) = \min\{k \mid \tau_1^k = \mathrm{id},\ \ldots,\ \tau_s^k = \mathrm{id}\} = \min\{k \mid \operatorname{ord}\tau_1 \mid k,\ \ldots,\ \operatorname{ord}\tau_s \mid k\} = \operatorname{mcm}(\tau_1, \ldots, \tau_s).$$

Por ejemplo, para la permutación $\sigma = (1\ 2)\,(3\ 4)\,(5\ 6\ 7)$ tenemos

$$\sigma^2 = (5\ 7\ 6),\ \sigma^3 = (1\ 2)\,(3\ 4),\ \sigma^4 = (5\ 6\ 7),\ \sigma^5 = (1\ 2)\,(3\ 4)\,(5\ 7\ 6),\ \sigma^6 = \mathrm{id}.$$

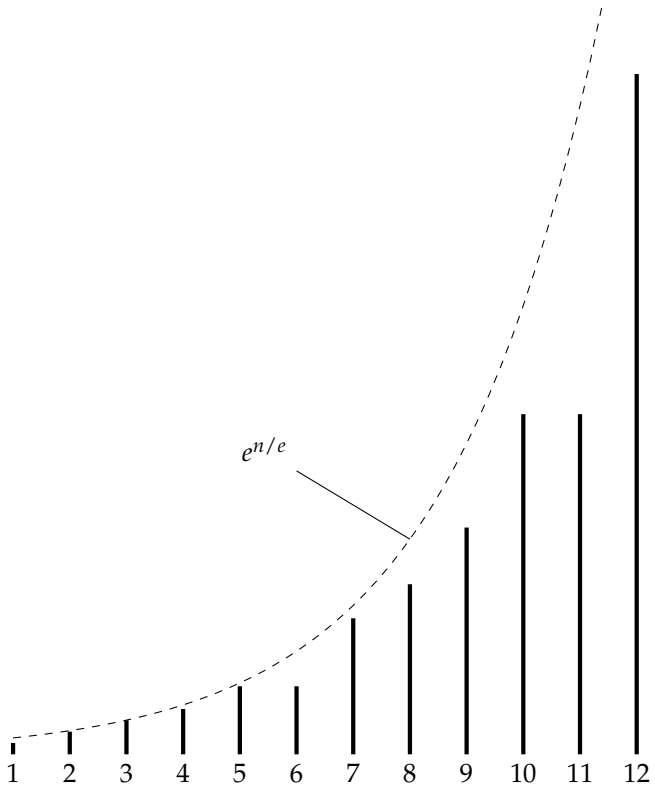
El número

$$g(n) := \max\{\operatorname{ord}\sigma \mid \sigma \in S_n\} = \max\{\operatorname{mcm}(n_1, \ldots, n_s) \mid n_1 + \cdots + n_s = n\}$$

se llama la **función de Landau**. He aquí algunos de sus valores (véase http://oeis.org/A000793):

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$g(n)$:	1	2	3	4	6	6	12	15	20	30	30	60	60	84	105

Hay varias expresiones asintóticas y desigualdades, por ejemplo $g(n) \leq e^{n/e}$.



▲

6.2.9. Corolario. *Si* $\operatorname{ord} g = n$*, entonces*

$$g^k = g^\ell \iff k \equiv \ell \pmod{n}.$$

Demostración. La igualdad $g^k = g^\ell$ es equivalente a $g^{k-\ell} = 1$ y luego a $n \mid (k - \ell)$ gracias a la observación 6.2.7; es decir, $k \equiv \ell \pmod{n}$. ■

6.2.10. Corolario. *Si* $\operatorname{ord} g = n$*, entonces el subgrupo* $\langle g \rangle$ *tiene n elementos.*

Demostración. Tenemos

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{n-1}\},$$

ya que $0, 1, 2, \ldots, n-1$ representan todos los restos módulo n. ■

6.2.11. Observación. *Si g es un elemento de orden finito, entonces*

$$\operatorname{ord} g^k = \frac{\operatorname{ord} g}{\operatorname{mcd}(\operatorname{ord} g, k)}.$$

Demostración. Sea $n = \operatorname{ord} g$. Si $\operatorname{mcd}(k, n) = d$, entonces podemos escribir

$$n = n'd, \quad k = k'd, \quad \text{donde } \operatorname{mcd}(n', k') = 1.$$

Luego,

$$n \mid km \iff n'd \mid k'dm \iff n' \mid k'm \iff n' \mid m,$$

y tenemos

$$\operatorname{ord} g^k = \min\{m \mid (g^k)^m = 1\} = \min\{m \mid n \mid km\} = \min\{m \mid n' \mid m\} = n' = n/d.$$

■

6.3 Grupos cíclicos

6.3.1. Definición. Se dice que un grupo G es **cíclico** si existe un elemento $g \in G$ que genera todo G; es decir $G = \langle g \rangle$.

En la situación de arriba, si g tiene orden finito, entonces, como hemos notado en 6.2.10, tenemos $|\langle g \rangle| = \operatorname{ord} g$. Esto significa que un grupo finito es cíclico si y solamente si este posee un elemento de orden $n = |G|$. En este caso los elementos de G son

$$\{1, g, g^2, \ldots, g^{n-1}\}.$$

6.3.2. Observación. *Sea $G = \langle g \rangle$ un grupo cíclico finito de orden n. Entonces, otro elemento $g^k \in G$ es un generador de G si y solamente si* $\operatorname{mcd}(k, n) = 1$.

Demostración. g^k es un generador si y solamente si $\operatorname{ord} g^k = n$. Para el orden de g^k tenemos la fórmula

$$\operatorname{ord} g^k = \frac{n}{\operatorname{mcd}(k, n)}$$

(véase 6.2.11). ■

6.3.3. Ejemplo. El grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ es generado por $[1]_n$.

$$\begin{aligned}
[0]_n &= 0 \cdot [1]_n, \\
[1]_n &= [1]_n, \\
[2]_n &= 2 \cdot [1]_n := [1]_n + [1]_n, \\
[3]_n &= 3 \cdot [1]_n := [1]_n + [1]_n + [1]_n, \\
&\vdots
\end{aligned}$$

En general, $[k]_n$ es un generador de $\mathbb{Z}/n\mathbb{Z}$ si y solamente si $\operatorname{mcd}(k, n) = 1$. El número de generadores de $\mathbb{Z}/n\mathbb{Z}$ coincide con el valor de la función de Euler $\phi(n)$. ▲

6.3.4. Ejemplo. El grupo aditivo $\mathbb{Z}$ es cíclico, generado por 1, ya que todo número entero puede ser escrito como $\pm(1 + \cdots + 1)$. Otro generador de $\mathbb{Z}$ es -1.

En general, si $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ es un grupo cíclico infinito, se ve que los únicos generadores son g y g^{-1}. ▲

Los ejemplos de arriba son de hecho todos los grupos cíclicos posibles, salvo isomorfismo.

6.3.5. Proposición. *Todo grupo cíclico finito de orden n es isomorfo a $\mathbb{Z}/n\mathbb{Z}$.*
Todo grupo cíclico infinito es isomorfo a $\mathbb{Z}$.

Demostración. Si G es un grupo cíclico finito de orden n, entonces

$$G = \langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}.$$

para algún $g \in G$. Definamos la aplicación

$$\begin{aligned}
f \colon G &\to \mathbb{Z}/n\mathbb{Z}, \\
g^k &\mapsto [k]_n.
\end{aligned}$$

Esta aplicación está bien definida: $g^k = g^\ell$ si y solamente si $k \equiv \ell \pmod{n}$ (véase 6.2.9). Note que esto también demuestra que f es una biyección. Es un homomorfismo, ya que

$$f(g^k \cdot g^\ell) = f(g^{k+\ell}) = [k+\ell]_n = [k]_n + [\ell]_n = f(g^k) + f(g^\ell).$$

Ahora si

$$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

es un grupo cíclico infinito, entonces la aplicación

$$\begin{aligned} G &\to \mathbb{Z}, \\ g^n &\mapsto n \end{aligned}$$

es visiblemente un isomorfismo. ■

6.3.6. Ejemplo. El grupo de las raíces n-ésimas de la unidad $\mu_n(\mathbb{C})$ es cíclico, generado por $\zeta_n := e^{2\pi i/n}$:

$$\mu_n(\mathbb{C}) = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}.$$

Tenemos un isomorfismo

$$\begin{aligned} \mu_n(\mathbb{C}) &\to \mathbb{Z}/n\mathbb{Z}, \\ \zeta_n^k &\mapsto [k]_n. \end{aligned}$$

En general, ζ_n^k es un generador si y solamente si $\mathrm{mcd}(k, n) = 1$. Los generadores de $\mu_n(\mathbb{C})$ se llaman las raíces n-ésimas **primitivas** de la unidad. ▲

Note que el isomorfismo construido en 6.3.5 no es canónico: para construirlo, hemos *escogido* un generador $g \in G$. Diferentes generadores nos dan diferentes isomorfismos. Los grupos específicos $\mathbb{Z}/n\mathbb{Z}$, $\mu_n(\mathbb{C})$, $\mathbb{Z}$ vienen con un generador canónico: $[1]_n$, $\zeta_n := e^{2\pi i/n}$, $+1$ respectivamente.

6.3.7. Ejemplo. El grupo alternante

$$A_3 = \{\mathrm{id},\ (1\ 2\ 3),\ (1\ 3\ 2)\}$$

es cíclico, generado por $(1\ 2\ 3)$ o por $(1\ 3\ 2)$. Es isomorfo a $\mathbb{Z}/3\mathbb{Z}$. ▲

6.3.8. Proposición. *Sea G un grupo cíclico. Si $H \subset G$ es un subgrupo, entonces H es también cíclico.*

Demostración. Sea g un generador de G:

$$G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

Sin pérdida de generalidad $H \neq \{\mathrm{id}\}$ (en el caso contrario, la proposición es obvia). Entonces existe un número mínimo positivo $k_0 = 1, 2, 3, \ldots$ tal que $g^{k_0} \in H$ (siendo un subgrupo, H contiene g^{-k} junto con g^k, así que este g^{k_0} siempre existe). Vamos a ver que g^{k_0} es un generador de H; es decir, $H = \langle g^{k_0} \rangle$. De hecho, para todo $g^k \in H$ podemos dividir con resto k por k_0:

$$k = qk_0 + r, \quad 0 \leq r < k_0.$$

Ahora, ya que H es un subgrupo, tenemos $g^{-k_0} = (g^{k_0})^{-1} \in H$ y $g^{-qk_0} = (g^{-k_0})^q \in H$, y luego

$$g^{-qk_0} \cdot g^k = g^{-qk_0} \cdot g^{qk_0+r} = g^r \in H,$$

pero nuestra elección de k_0 implica que $r = 0$. Entonces, $k = qk_0$ y $g^k = (g^{k_0})^q$. ■

6.3.9. Ejemplo. Todos los subgrupos de $\mathbb{Z}$ son de la forma

$$n\mathbb{Z} := \{0, \pm n, \pm 2n, \pm 3n, \dots\}.$$

Son cíclicos, generados por n. ▲

6.3.10. Proposición. *Sea G es un grupo cíclico finito de orden n. Para todo subgrupo $H \subset G$ se tiene $|H| \mid n$. Además, para todo $d \mid n$ el grupo G contiene precisamente un subgrupo de orden d.*

Demostración. Todo subgrupo $H \subset G$ es necesariamente cíclico según 6.3.8, generado por g^k para algún k. Luego,

$$|H| = |\langle g^k \rangle| = \operatorname{ord} g^k = n/d, \quad \text{donde } d = \operatorname{mcd}(k, n).$$

De hecho, se tiene $\langle g^k \rangle = \langle g^d \rangle$. En efecto, $d \mid k$ implica que $\langle g^k \rangle \subseteq \langle g^d \rangle$. Por otro lado,

$$|\langle g^d \rangle| = \operatorname{ord} g^d = \frac{n}{\operatorname{mcd}(d, n)} = n/d,$$

ya que $d \mid n$. Esto significa que $\langle g^k \rangle = \langle g^d \rangle$. Entonces,

$$H = \langle g^d \rangle.$$

Viceversa, a partir de cualquier $d \mid n$ podemos considerar el subgrupo $\langle g^d \rangle$. Su orden es n/d. Para diferentes $d, d' \mid n$ los subgrupos $\langle g^d \rangle$ y $\langle g^{d'} \rangle$ son diferentes, siendo grupos de diferente orden. ■

6.3.11. Ejemplo. En el grupo de las n-ésimas raíces de la unidad $\mu_n(\mathbb{C})$ para todo $m \mid n$ tenemos el subgrupo $\mu_m(\mathbb{C}) \subset \mu_n(\mathbb{C})$, y todos los subgrupos surgen de este modo. ▲

6.3.12. Corolario. *Para la función ϕ de Euler se cumple la identidad*

$$\sum_{d \mid n} \phi(d) = n$$

donde la suma es sobre todos los divisores de n.

Demostración. Todo elemento $x \in \mathbb{Z}/n\mathbb{Z}$ tiene orden $d = |\langle x \rangle|$ donde $d \mid n$ y en total hay $\phi(d)$ diferentes elementos de orden d que corresponden a diferentes generadores del único subgrupo de orden d. Entonces, la suma $\sum_{d \mid n} \phi(d)$ nada más cuenta todos los n elementos de $\mathbb{Z}/n\mathbb{Z}$. ■

6.3.13. Ejemplo. $\phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2 = 6$. ▲

Los grupos cíclicos son los grupos más simples que se pueden imaginar (¡salvo los grupos triviales!). Sin embargo, son de mucha importancia en aritmética.

6.4 Ejercicios

Ejercicio 6.1. *Sea G un grupo. Supongamos que para dos elementos de grupo $g, h \in G$ se cumple $h = k\,g\,k^{-1}$ para algún $k \in G$ (en este caso se dice que g y h son **conjugados**). Demuestre que el orden de g es finito si y solamente si el orden de h es finito, y en este caso* $\operatorname{ord} g = \operatorname{ord} h$.

Ejercicio 6.2. *Describa todos los tipos de ciclo posibles en el grupo simétrico S_5 y encuentre los ordenes correspondientes.*

Ejercicio 6.3. *Exprese la matriz* $\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}$ *como un producto de matrices* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *y* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Ejercicio 6.4. *Demuestre que el conjunto* $X = \{1/p^k \mid p \text{ primo}, k = 0, 1, 2, 3, \dots\}$ *genera el grupo aditivo* $\mathbb{Q}$.

Ejercicio 6.5. *Encuentre los elementos de orden finito en el grupo de isometrías del plano euclidiano* $\mathbb{R}^2 \to \mathbb{R}^2$.

Ejercicio 6.6. *Supongamos que G es un grupo finito de orden par. Demuestre que G tiene un elemento de orden 2.*

Ejercicio 6.7. *Supongamos que G es un grupo no trivial que no tiene subgrupos propios. Demuestre que G es un grupo cíclico finito de orden p, donde p es un número primo.*

El ejemplo de $R = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ y $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ en $\mathrm{SL}_2(\mathbb{Z})$ demuestra que para dos elementos de orden finito, su producto puede tener orden infinito y además que un número finito de elementos de orden finito pueden generar un grupo infinito. Esto sucede gracias a la nonconmutatividad. La situación en grupos abelianos es más sencilla.

Ejercicio 6.8. *Sea A un grupo abeliano (escrito en la notación aditiva).*

1) *Sea $m = 1, 2, 3, \dots$ un número fijo. Demuestre que los elementos $a \in A$ tales que $m \cdot a = 0$ forman un subgrupo de A. Este se denota por $A[m]$ y se llama el **subgrupo de m-torsión** en A.*

2) *Demuestre que todos los elementos de orden finito en A forman un subgrupo. Este se llama el **subgrupo de torsión** y se denota por A_{tors}:*
$$A_{tors} = \bigcup_{m \geq 1} A[m].$$

3) *Encuentre los grupos $A[m]$ y A_{tors} para $A = \mathbb{R}, \mathbb{C}, \mathbb{R}^\times, \mathbb{C}^\times$.*

Ejercicio 6.9. *Sea A un grupo abeliano.*

1) *Demuestre que para todo homomorfismo $f\colon \mathbb{Z}/m\mathbb{Z} \to A$ se tiene necesariamente $f([1]_m) \in A[m]$.*

2) *Demuestre que*
$$\operatorname{Hom}(\mathbb{Z}/m\mathbb{Z}, A) \to A[m], \quad f \mapsto f([1]_m)$$
es una biyección.

3) *Describa todos los homomorfismos de grupos abelianos*
$$\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}, \quad \mathbb{Z}/m\mathbb{Z} \to \mathbb{Q}, \quad \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
para diferentes $m, n = 2, 3, 4, 5, \dots$

Ejercicio 6.10. *Demuestre que* $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.