# Capítulo 6
# Grupos

En este capítulo vamos a introducir otra estructura algebraica fundamental que es grupo, investigar sus propiedades básicas y ver varios ejemplos importantes.

## 6.1 Definición de grupo

**6.1.1. Definición.** Un **grupo** es un conjunto $G$ dotado de una operación binaria

$$\begin{aligned} G \times G &\to G, \\ (g, h) &\mapsto g \cdot h \end{aligned}$$

que satisface las siguientes propiedades.

G1) La operación $\cdot$ es **asociativa**: para cualesquiera $g, h, k \in G$ tenemos

$$(g \cdot h) \cdot k = g \cdot (h \cdot k).$$

G2) Existe un **elemento neutro** $1 \in G$ tal que

$$1 \cdot g = g = g \cdot 1$$

para todo $g \in G$.

G3) Para todo elemento $g \in G$ existe su **inverso** $g^{-1} \in G$ tal que

$$g \cdot g^{-1} = 1 = g^{-1} \cdot g.$$

Desde el principio será conveniente omitir el símbolo $\cdot$ y escribir simplemente "$gh$" en lugar de $g \cdot h$.

**6.1.2. Definición.** Si $G$ es un conjunto finito, el número $|G|$ se llama el **orden** de $G$.

**6.1.3. Definición.** Si la operación en $G$ es **conmutativa**, es decir

$$gh = hg$$

para cualesquiera $g, h \in G$, entonces se dice que $G$ es un grupo **abeliano**[*] o **conmutativo**.



[*] Niels Henrik Abel (1802–1829), matemático noruego, conocido por sus contribuciones en análisis (estudio de las series y de las integrales elípticas) y álgebra. Usando la teoría de grupos demostró su célebre teorema que dice que las ecuaciones polinomiales generales de grado $\geq 5$ no pueden resolverse por radicales. Murió de tuberculosis a los 26 años. El lector puede buscar en internet más información sobre su trágica biografía para enterarse de cómo era la vida de los matemáticos del siglo XIX.

Como siempre, el primer ejemplo es trivial.

**6.1.4. Ejemplo.** Un conjunto de un elemento $\{1\}$ puede ser dotado de manera única de estructura de un grupo. Este se llama el **grupo trivial**. Es abeliano (*trivialmente*). Por abuso de notación este también se denota por $1$. ▲

Para dar alguna motivación, aquí están varios grupos no triviales.

**6.1.5. Ejemplo.** Para un conjunto $X$ las biyecciones $\sigma\colon X \to X$ forman un grupo. Esto se sigue de la discusión en el capítulo 0. Este grupo no es abeliano si $X$ tiene más de dos elementos. Para más detalles sobre este tipo de grupos, véase la sección §6.3. ▲

**6.1.6. Ejemplo.** Las matrices invertibles de $n \times n$ con coeficientes en un cuerpo $k$ (o en general en cualquier anillo conmutativo $A$) forman un grupo. Este grupo tampoco es abeliano cuando $n > 1$. Este ejemplo será considerado en la sección §6.4. ▲

**6.1.7. Ejemplo.** Un ejemplo típico de grupos abelianos son los números enteros $\mathbb{Z}$ respecto a la operación de la suma $+$. En este caso el elemento neutro es $0$ y el elemento "inverso" para $a \in \mathbb{Z}$ es $-a$. De la misma manera, los restos módulo $n$ forman un grupo abeliano $\mathbb{Z}/n\mathbb{Z}$ respecto a la suma. ▲

Para más ejemplos interesantes, el lector debe tener paciencia y esperar la siguiente sección. Hagamos primero algunas observaciones sobre las propiedades que se siguen inmediatamente de los axiomas de grupo.

1) En un grupo hay un elemento neutro único $1 \in G$.

   De hecho, asumamos que $1$ y $1'$ son dos elementos que cumplen

   $$1 \cdot g = g = g \cdot 1, \quad 1' \cdot g = g = g \cdot 1'$$

   para todo $g \in G$. Luego, $1 = 1' \cdot 1 = 1'$.

2) Para $g \in G$ un elemento inverso $g^{-1}$ tal que $gg^{-1} = 1 = g^{-1}g$ es único. Esto justifica la notación "$g^{-1}$".

   De hecho, si tenemos dos elementos inversos $g'$ y $g''$:

   $$gg' = 1 = g' \cdot g, \quad gg'' = e = g''g,$$

   entonces

   $$g' = g' \cdot 1 = g'(gg'') = (g'g)\,g'' = 1 \cdot g'' = g''.$$

3) Se cumple la **asociatividad generalizada**: en una expresión

   $$g_1\, g_2\, g_3 \cdots g_n$$

   todos los posibles modos de poner los paréntesis dan el mismo resultado. Aquí funciona el mismo argumento inductivo que vimos en el capítulo 0 para las composiciones de aplicaciones.

4) Se tiene $(g^{-1})^{-1} = g$ para todo $g \in G$.

5) Para un producto de dos elementos $gh$ se tiene

   $$(gh)^{-1} = h^{-1}g^{-1},$$

   y en general,

   $$(g_1 g_2 \cdots g_{n-1} g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_2^{-1} g_1^{-1}.$$

6) Se cumple la **cancelación**:

$$gh' = gh'' \Longrightarrow h' = h'', \quad g'h = g''h \Longrightarrow g' = g''$$

para cualesquiera $g, g', g'', h, h', h'' \in G$.

Por ejemplo, el el primer caso, multiplicando la identidad $g\,h' = g\,h''$ por $g^{-1}$ por la izquierda, se obtiene

$$g^{-1}\,(gh') = g^{-1}\,(gh'')$$

Luego,

$$h' = 1 \cdot h' = (g^{-1}g)\,h' = g^{-1}\,(g\,h') = g^{-1}\,(g\,h'') = (g^{-1}g)\,h'' = 1 \cdot h'' = h''.$$

De la misma manera, la identidad $g'h = g''h$ puede ser multiplicada por $h^{-1}$ por la derecha.

**6.1.8. Comentario.** Nuestra definición de grupo usa la notación **multiplicativa**: la operación se denota por "$g \cdot h$" o simplemente "$gh$" porque la consideramos como una especie de producto. (Solo hay que recordar que a priori este producto no es conmutativo: en general $gh \neq hg$ cuando el grupo no es abeliano.) Por este motivo el elemento neutro se denota por $1$.

Si el grupo es abeliano, es común la notación **aditiva**: en vez de "$gh$" se escribe "$g + h$". En este caso el elemento neutro se denota por $0$. Los grupos abelianos suelen denotarse por las letras $A, B, C$, y sus elementos por $a, b, c$. En vez de elementos inversos se habla de los elementos **opuestos** que se denotan por $-a$:

$$a + (-a) = 0 = (-a) + a.$$

**6.1.9. Notación.** Será útil la notación para $g \in G$ y $n \in \mathbb{Z}$

$$g^n := \begin{cases} \underbrace{g \cdots g}_{n \text{ veces}}, & \text{si } n > 0, \\ 1, & \text{si } n = 0, \\ (g^{-n})^{-1}, & \text{si } n < 0. \end{cases}$$

Note que se tiene la identidad

$$(g^m)^n = g^{mn}.$$

No olvidemos que la multiplicación no es conmutativa en general, así que, por ejemplo, $(gh)^2 = ghgh$, y en general no es lo mismo que $g^2h^2 = gghh$.

En el caso aditivo se usa la notación correspondiente

$$n \cdot a := \begin{cases} \underbrace{a + \cdots + a}_{n \text{ veces}}, & \text{si } n > 0, \\ 0, & \text{si } n = 0, \\ -((-n) \cdot a), & \text{si } n < 0. \end{cases}$$

Note que si $A$ es un grupo abeliano, entonces para cualesquiera $m, n \in \mathbb{Z}$, $a, b \in A$ se tiene

$$\begin{gathered} (m+n) \cdot a = m \cdot a + n \cdot a, \\ m \cdot (a+b) = m \cdot a + m \cdot b, \\ (mn) \cdot a = m \cdot (n \cdot a), \\ 1 \cdot a = a. \end{gathered}$$

Desde el principio sería oportuno introducir la noción de subgrupo.

**6.1.10. Definición.** Sea $G$ un grupo. Se dice que un subconjunto $H \subseteq G$ es un **subgrupo** de $G$ si

1) $1 \in H$,

2) para cualesquiera $h_1, h_2 \in H$ tenemos $h_1 h_2 \in H$,

3) para todo $h \in H$ tenemos $h^{-1} \in H$.

Las condiciones 1)–3) implican que $H$ es también un grupo respecto a la misma operación. Ya que $h\,h^{-1} = 1$ para todo $h \in H$, la condición 1) sirve solo para decir que $H \neq \emptyset$.

**6.1.11. Ejemplo.** Todo grupo $G$ tiene por lo menos dos subgrupos: el subgrupo trivial $1$ y el mismo $G$. Los subgrupos distintos de estos dos se llaman **subgrupos propios** de $G$. ▲

**6.1.12. Observación.** *Si $H_i \subseteq G$ es una familia de subgrupos de $G$, entonces su intersección $\bigcap_i H_i$ es también un subgrupo.* □

**6.1.13. Observación.** *Si*

$$H_1 \subseteq H_2 \subseteq H_3 \subseteq \cdots \subseteq G$$

*es una cadena de subgrupos de $G$, entonces la unión $\bigcup_i H_i$ es también un subgrupo.* □

## 6.2 Primeros ejemplos de grupos

Ya hemos visto algunos grupos cuando estábamos hablando de anillos.

**6.2.1. Ejemplo.** Si $A$ es un anillo, entonces por la definición, este es un grupo abeliano respecto a la suma. La definición de ideal $\mathfrak{a} \subseteq A$ implica que $\mathfrak{a}$ es un subgrupo de $A$. ▲

**6.2.2. Comentario.** Cuando algo forma un grupo respecto a la suma, se dice que es un grupo **aditivo**.

**6.2.3. Ejemplo.** Los números enteros $\mathbb{Z}$ forman un grupo abeliano respecto a la suma. Los números divisibles por $n$ forman un subgrupo

$$n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\} \subset \mathbb{Z}.$$

Notamos que si $m \mid n$, entonces $n\mathbb{Z}$ es un subgrupo de $m\mathbb{Z}$. ▲

**6.2.4. Ejemplo.** Por la definición, todo espacio vectorial es un grupo abeliano respecto a la adición de vectores. Por ejemplo, para todo cuerpo $k$, el espacio vectorial $k^n$ es un grupo abeliano. ▲

**6.2.5. Ejemplo.** Si $A$ es un anillo, entonces los elementos invertibles $A^\times$ forman un grupo respecto a la multiplicación, también conocido como el **grupo de unidades** de $A$. Notamos que si $A \subseteq B$ es un subanillo, entonces $A^\times \subseteq B^\times$ es un subgrupo. ▲

**6.2.6. Comentario.** Cuando algo forma un grupo respecto a la multiplicación, se dice que es un grupo **multiplicativo**.

**6.2.7. Ejemplo.** En un cuerpo todo elemento no nulo $x \in k$ tiene su inverso $x^{-1}$, así que el grupo de unidades viene dado por

$$k^\times = k \setminus \{0\}.$$

Es abeliano (por nuestra definición, la multiplicación en un cuerpo es conmutativa). ▲

**6.2.8. Ejemplo.** Tenemos $\mathbb{Z}^\times = \{\pm 1\}$ con la tabla de multiplicación

| $\cdot$ | $+1$ | $-1$ |
|---|---|---|
| $+1$ | $+1$ | $-1$ |
| $-1$ | $-1$ | $+1$ |

▲

**6.2.9. Ejemplo.** Tenemos una cadena de subgrupos aditivos

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

que nos da la cadena correspondiente de subgrupos multiplicativos

$$\{\pm 1\} \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times.$$ ▲

**6.2.10. Ejemplo.** El grupo $\mathbb{Q}^\times$ tiene como su subgrupo el conjunto $\mathbb{Q}_{>0}$ formado por los números racionales positivos. De la misma manera, los números reales positivos $\mathbb{R}_{>0}$ forman un subgrupo de $\mathbb{R}^\times$. ▲

**6.2.11. Ejemplo.** Tenemos

$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}.$$

La multiplicación de estos elementos viene dada por

$$(u(1+\sqrt{2})^m) \cdot (v(1+\sqrt{2})^n) = uv(1+\sqrt{2})^{m+n},$$

donde $u, v = \pm 1$. ▲

**6.2.12. Ejemplo.** Tenemos $\mathbb{Z}[i]^\times = \{+1, +i, -1, -i\}$ con la tabla de multiplicación

| $\cdot$ | $+1$ | $+i$ | $-1$ | $-i$ |
|---|---|---|---|---|
| $+1$ | $+1$ | $+i$ | $-1$ | $-i$ |
| $+i$ | $+i$ | $-1$ | $-i$ | $+1$ |
| $-1$ | $-1$ | $-i$ | $+1$ | $+i$ |
| $-i$ | $-i$ | $+1$ | $+i$ | $-1$ |

Notamos que aquí se trata nada más de las raíces cuartas de la unidad:

$$\mathbb{Z}[i]^\times = \{1, \zeta_4, \zeta_4^2, \zeta_4^3\}.$$

La tabla de arriba puede ser reescrita como

| $\cdot$ | $1$ | $\zeta_4$ | $\zeta_4^2$ | $\zeta_4^3$ |
|---|---|---|---|---|
| $1$ | $1$ | $\zeta_4$ | $\zeta_4^2$ | $\zeta_4^3$ |
| $\zeta_4$ | $\zeta_4$ | $\zeta_4^2$ | $\zeta_4^3$ | $1$ |
| $\zeta_4^2$ | $\zeta_4^2$ | $\zeta_4^3$ | $1$ | $\zeta_4$ |
| $\zeta_4^3$ | $\zeta_4^3$ | $1$ | $\zeta_4$ | $\zeta_4^2$ |

▲

**6.2.13. Ejemplo.** Si $A = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, entonces tenemos

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]^\times = \{1, \zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5\}$$

con la multiplicación

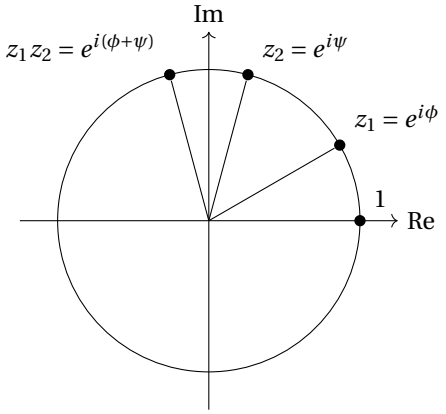
$$\zeta_6^k \cdot \zeta_6^\ell = \zeta_6^{k+\ell}.$$ ▲

Los últimos ejemplos sugieren considerar los grupos formados por las raíces de la unidad. Primero notamos que $|\zeta_n^k| = 1$, así que todas las raíces de la unidad están en el círculo unitario en el plano complejo.

**6.2.14. Ejemplo.** El conjunto de los números complejos de valor absoluto 1

$$\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{i\phi} \mid 0 \le \phi < 2\pi\}$$

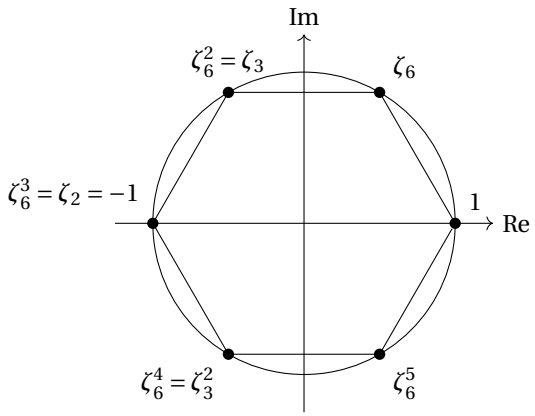
es un subgrupo de $\mathbb{C}^\times$ respecto a la multiplicación. Este grupo se llama el **grupo del círculo**.




Notamos que el producto $e^{i\phi} \cdot e^{i\psi} = e^{i(\phi+\psi)}$ corresponde a la suma de ángulos $\phi + \psi$, solo que hay que sumarlos módulo $2\pi$. ▲

**6.2.15. Ejemplo.** Las raíces $n$-ésimas de la unidad forman un subgrupo

$$\mu_n(\mathbb{C}) = \{z \in \mathbb{C} \mid z^n = 1\} = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} \subset \mathbb{S}^1.$$



Si $m \mid n$, entonces $z^m = 1$ implica $z^n = 1$ y se ve que $\mu_m(\mathbb{C})$ es un subgrupo de $\mu_n(\mathbb{C})$. Por ejemplo, en el dibujo de arriba tenemos

$$\mu_2(\mathbb{C}) \subset \mu_6(\mathbb{C}) \quad \text{y} \quad \mu_3(\mathbb{C}) \subset \mu_6(\mathbb{C}).$$

Todas las raíces de la unidad forman un subgrupo del grupo del círculo

$$\mu_\infty(\mathbb{C}) = \{z \in \mathbb{C}^\times \mid z^n = 1 \text{ para algún } n = 1,2,3,\ldots\} = \bigcup_{n\geq 1} \mu_n(\mathbb{C}) = \{e^{2\pi i\phi} \mid \phi \in \mathbb{Q}\}.$$

Tenemos entonces una cadena de subgrupos

$$\mu_m(\mathbb{C}) \overset{\text{si } m|n}{\subset} \mu_n(\mathbb{C}) \subset \mu_\infty(\mathbb{C}) \subset \mathbb{S}^1 \subset \mathbb{C}^\times. \qquad \blacktriangle$$

## 6.3 Grupo simétrico

Un ejemplo fundamental son grupos de permutación, también conocidos como grupos simétricos.

**6.3.1. Definición.** Sea $X$ un conjunto. Si $\sigma\colon X \to X$ es una biyección, se dice también que $\sigma$ es una **permutación** de los elementos de $X$. El conjunto de todas estas permutaciones se denota por $S_X$ y se llama el **grupo simétrico** sobre los elementos de $X$.

En particular, si $X = \{1,\ldots,n\}$, entonces se usa la notación

$$S_n := S_{\{1,\ldots,n\}}.$$

La discusión en el capítulo 0 significa que $S_X$, y en particular $S_n$, son grupos respecto a la composición $\circ$. Desde el principio será conveniente omitir el símbolo de la composición: para dos permutaciones $\sigma, \tau\colon X \to X$ la composición $\tau \circ \sigma$ será denotada simplemente por $\tau\sigma$. Esta es una especie de multiplicación, pero en general $\tau\sigma \neq \sigma\tau$.

**6.3.2. Observación.** *Tenemos* $|S_n| = n!$ □

**6.3.3. Ejemplo.** Los grupos $S_0$ y $S_1$ son triviales. El grupo $S_2$ consiste en dos permutaciones: la permutación identidad $\mathrm{id}$ y la permutación que intercambia $1$ y $2$:

$$\sigma\colon 1 \mapsto 2,\ 2 \mapsto 1. \qquad \blacktriangle$$

**6.3.4. Notación.** Una permutación $\sigma \in S_n$ puede representarse mediante una tabla donde en la primera fila están los números $i = 1,2,\ldots,n$ y en la segunda fila están sus imágenes correspondientes $\sigma(i)$:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Notamos que el hecho de que $\sigma$ sea una biyección significa precisamente que los números en la segunda fila no se repiten.

**6.3.5. Ejemplo.** Los elementos de $S_2$ pueden ser representados por las tablas

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

El grupo simétrico $S_3$ consiste en $6$ elementos

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \tag{6.1}$$

Notamos que en general, dos permutaciones $\sigma, \tau \in S_n$ no conmutan; es decir,

$$\sigma\tau \neq \tau\sigma.$$

En el caso de $S_3$ tenemos

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tag{6.2}$$

mientras que

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \tag{6.3}$$

Este ejemplo demuestra que $S_n$ no es abeliano para $n \geq 3$. ▲

## Permutaciones cíclicas

Una clase importante de permutaciones son las permutaciones cíclicas.

**6.3.6. Definición.** Para $1 \leq k \leq n$ sean $i_1, i_2, i_3, \ldots, i_k$ algunos números distintos entre 1 y $n$. Definamos una permutación $\sigma$ por

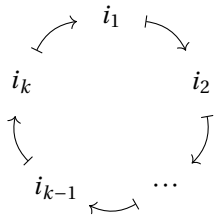
$$\sigma(i_1) := i_2, \quad \sigma(i_2) := i_3, \quad \ldots, \quad \sigma(i_{k-1}) := i_k, \quad \sigma(i_k) := i_1$$

y

$$\sigma(j) = j \quad \text{para } j \notin \{i_1, i_2, i_3, \ldots, i_k\}.$$

Entonces, se dice que $\sigma$ es una **permutación cíclica de orden** $k$ o un $k$**-ciclo** y se escribe

$$\sigma = (i_1\ i_2\ \cdots\ i_{k-1}\ i_k).$$




La permutación identidad id se considera como la permutación cíclica de orden 1, ya que esta corresponde a $(i)$ para cualquier $i \in \{1, \ldots, n\}$.

**6.3.7. Definición.** Los 2-ciclos $\sigma = (i\ j)$ reciben el nombre especial de **transposiciones**.

Note que la transposición $(i\ j)$ intercambia $i$ con $j$ y deja otros elementos intactos.

En un ciclo, los índices en paréntesis pueden ser *permutados cíclicamente* y el resultado no cambia:

$$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2).$$

Por esto normalmente se escoge la presentación $(i_1\ i_2\ \cdots i_{k-1}\ i_k)$ donde $i_1$ es el número mínimo (en el ejemplo de arriba es $(1\ 2\ 3)$).

**6.3.8. Ejemplo.** El grupo simétrico $S_3$ consiste en permutaciones cíclicas; sus elementos, enumerados en (6.1), también pueden ser escritos como

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

Compilemos la tabla de composición de permutaciones en $S_3$ en términos de ciclos. Por ejemplo, las fórmulas (6.2) y (6.3) pueden ser escritas como

$$(1\ 2)\,(2\ 3) = (1\ 2\ 3), \quad (2\ 3)\,(1\ 2) = (1\ 3\ 2).$$

Haciendo cálculos similares, se obtiene

| $\circ$ | id | (1 2) | (2 3) | (1 3) | (1 2 3) | (1 3 2) |
|---|---|---|---|---|---|---|
| id | id | (1 2) | (2 3) | (1 3) | (1 2 3) | (1 3 2) |
| (1 2) | (1 2) | id | (1 2 3) | (1 3 2) | (2 3) | (1 3) |
| (2 3) | (2 3) | (1 3 2) | id | (1 2 3) | (1 3) | (1 2) |
| (1 3) | (1 3) | (1 2 3) | (1 3 2) | id | (1 2) | (2 3) |
| (1 2 3) | (1 2 3) | (1 3) | (1 2) | (2 3) | (1 3 2) | id |
| (1 3 2) | (1 3 2) | (2 3) | (1 3) | (1 2) | id | (1 2 3) |

▲

**6.3.9. Observación.** *La permutación inversa a un $k$-ciclo es también un $k$-ciclo, dado por*

$$(i_1\ i_2\ \cdots\ i_k)^{-1} = (i_k\ i_{k-1}\ \cdots\ i_1) = (i_1\ i_k\ i_{k-1}\ \cdots\ i_2).$$ □

**6.3.10. Definición.** Se dice que dos ciclos $\sigma = (i_1\ i_2\ \cdots\ i_k)$ y $\tau = (j_1\ j_2\ \cdots\ j_\ell)$ en $S_n$ son **disjuntos** si $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_\ell\} = \emptyset$.

**6.3.11. Observación.** *Si $\sigma$ y $\tau$ son ciclos disjuntos, entonces $\sigma\tau = \tau\sigma$.* □

No todas las permutaciones son cíclicas. Por ejemplo, en el grupo $S_4$ se tiene

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

En general, tenemos el siguiente resultado.

**6.3.12. Proposición.** *Toda permutación $\sigma \in S_n$ puede ser escrita como una composición de ciclos disjuntos.*

*Demostración.* Fijemos una permutación $\sigma \in S_n$ y consideremos sus potencias

$$\mathrm{id}, \sigma, \sigma^2, \sigma^3, \ldots \in S_n.$$

Dado que $S_n$ es finito, en esta lista necesariamente hay repeticiones: se tiene $\sigma^p = \sigma^q$ para algunos $0 \le q < p$. Luego, $\sigma^{p-q} = \mathrm{id}$, y en particular $\sigma^{p-q-1} = \sigma^{-1}$. Esto significa que la permutación inversa $\sigma^{-1}$ puede ser escrita como $\sigma^m$ para algún $m \in \mathbb{N}$.

Consideremos la siguiente relación sobre $\{1, 2, \ldots, n\}$: pongamos

$$i \sim j \iff i = \sigma^p(j) \text{ para algún } p \in \mathbb{N}.$$

Notamos que la relación es reflexiva: $i = \sigma^0(i)$. Además, es simétrica:

$$i = \sigma^p(j) \Longrightarrow j = \sigma^{-p}(i) = \sigma^{mp}(i).$$

En fin, la relación es transitiva: tenemos

$$i = \sigma^p(j),\ j = \sigma^q(k) \Longrightarrow i = \sigma^{p+q}(k).$$

Podemos concluir que $\{1, 2, \dots, n\}$ se descompone en una unión disjunta de clases de equivalencia. Ahora para la clase

$$[i] = \{\sigma^p(i) \mid p \in \mathbb{N}\}$$

consideremos la lista

$$i, \sigma(i), \sigma^2(i), \dots, \sigma^p(i).$$

Sea $p$ el mínimo número natural tal que en esta lista hay repeticiones. Si $\sigma^p(i) = \sigma^q(i)$ para algún $0 < q < p$, entonces tenemos $\sigma^{p-q}(i) = i$, lo que contradice la minimalidad de $p$. Podemos concluir que se tiene $\sigma^p(i) = i$ y los números

$$i \mapsto \sigma(i) \mapsto \sigma^2(i) \mapsto \cdots \mapsto \sigma^{p-1}(i) \mapsto \sigma^p(i) = i$$

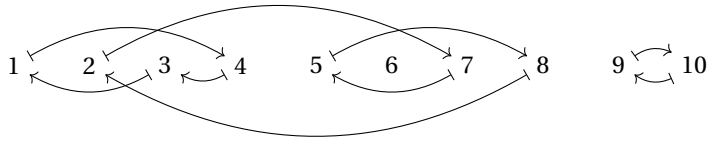
forman un ciclo. ■

**6.3.13. Ejemplo.** Analizando la permutación

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

se obtiene la descomposición

$$\sigma = (1\ 4\ 3)\,(2\ 7\ 5\ 8)\,(9\ 10).$$




▲

**6.3.14. Definición.** Para $\sigma \in S_n$, consideremos su descomposición en ciclos disjuntos. La sucesión de órdenes de estos ciclos se llama el **tipo de ciclo** de $\sigma$.

Todos los tipos de ciclo posibles en $S_n$ corresponden a las particiones de $n$ en una suma de números positivos. Por ejemplo, para $n = 4$ tenemos las siguientes opciones.

$$\begin{aligned} 1+1+1+1 &\leftrightarrow (\bullet)\,(\bullet)\,(\bullet)\,(\bullet) = \mathrm{id} \\ 1+1+2 &\leftrightarrow (\bullet)\,(\bullet)\,(\bullet\ \bullet) = (\bullet\ \bullet) \\ 2+2 &\leftrightarrow (\bullet\ \bullet)\,(\bullet\ \bullet) \\ 1+3 &\leftrightarrow (\bullet)\,(\bullet\ \bullet\ \bullet) = (\bullet\ \bullet\ \bullet) \\ 4 &\leftrightarrow (\bullet\ \bullet\ \bullet\ \bullet) \end{aligned}$$

**6.3.15. Ejemplo.** Con un poco de cuidado para no olvidar ninguna permutación y no escribirla dos veces, encontramos la lista completa de los elementos de $S_4$:

$$\begin{gathered} \mathrm{id}, \\ (1\ 2), \quad (1\ 3), \quad (1\ 4), \quad (2\ 3), \quad (2\ 4), \quad (3\ 4), \\ (1\ 2\ 3), \quad (1\ 2\ 4), \quad (1\ 3\ 2), \quad (1\ 3\ 4), \quad (1\ 4\ 2), \quad (1\ 4\ 3), \quad (2\ 3\ 4), \quad (2\ 4\ 3), \\ (1\ 2)\,(3\ 4), \quad (1\ 3)\,(2\ 4), \quad (1\ 4)\,(2\ 3), \\ (1\ 2\ 3\ 4), \quad (1\ 2\ 4\ 3), \quad (1\ 3\ 2\ 4), \quad (1\ 3\ 4\ 2), \quad (1\ 4\ 2\ 3), \quad (1\ 4\ 3\ 2). \end{gathered}$$

(Notamos que el número total es $1 + 6 + 8 + 3 + 6 = 24 = 4!$) ▲

**6.3.16. Proposición.** *En $S_n$ hay*

$$\frac{n!}{\prod_\ell M_\ell! \cdot \ell^{M_\ell}}$$

*permutaciones con la descomposición en ciclos disjuntos de la forma*

$$\sigma = \underbrace{(\bullet)\cdots(\bullet)}_{M_1 \text{ puntos fijos}} \quad \underbrace{(\bullet\ \bullet)\cdots(\bullet\ \bullet)}_{M_2 \text{ transposiciones}} \quad \underbrace{(\bullet\ \bullet\ \bullet)\cdots(\bullet\ \bullet\ \bullet)}_{M_3 \text{ ciclos de orden } 3}\cdots \tag{6.4}$$

*(aquí $M_1 + M_2 \cdot 2 + M_3 \cdot 3 + \cdots = n$).*

*Demostración.* Hay $n!$ posibilidades de colocar los números $\{1,\dots,n\}$ en lugar de $\bullet$ en (6.4). En cada serie de $M_\ell$ ciclos de longitud $\ell$, podemos escribir los ciclos en otro orden, y el resultado no cambia, así que hay que dividir $n!$ por $\prod_\ell M_\ell!$. También para cada ciclo de longitud $\ell$, hay $\ell$ modos equivalentes de escribirlo permutando los índices cíclicamente. Por esto hay que dividir todo por $\prod_\ell \ell^{M_\ell}$. ■

**6.3.17. Ejemplo.** Si nos interesan los $k$-ciclos en $S_n$ (donde $1 \le k \le n$), tenemos

$$M_1 = (n-k), \quad M_2 = \cdots = M_{k-1} = 0, \quad M_k = 1, \quad M_{k+1} = M_{k+2} = \cdots = 0$$

y la fórmula nos da

$$\frac{n!}{(n-k)! \cdot k}.$$

En particular, hay $\binom{n}{2}$ transposiciones. ▲

**6.3.18. Ejemplo.** En $S_5$ tenemos

- la permutación identidad id,
- $10 = \frac{5!}{3!\cdot 2}$ transposiciones $(\bullet\ \bullet)$,
- $20 = \frac{5!}{2!\cdot 3}$ ciclos $(\bullet\ \bullet\ \bullet)$,
- $30 = \frac{5!}{4}$ ciclos $(\bullet\ \bullet\ \bullet\ \bullet)$,
- $24 = \frac{5!}{5}$ ciclos $(\bullet\ \bullet\ \bullet\ \bullet\ \bullet)$,
- $15 = \frac{5!}{2!\cdot 2^2}$ permutaciones $(\bullet\ \bullet)(\bullet\ \bullet)$,
- $20 = \frac{5!}{2\cdot 3}$ permutaciones $(\bullet\ \bullet)(\bullet\ \bullet\ \bullet)$. ▲

**6.3.19. Definición.** Para $\sigma, \tau \in S_n$ la permutación $\tau\sigma\tau^{-1} \in S_n$ se llama la **conjugación de $\sigma$ por $\tau$**.

**6.3.20. Observación.** *Para dos permutaciones $\sigma, \tau \in S_n$, si*

$$\sigma\colon i \mapsto j,$$

*entonces*

$$\tau\sigma\tau^{-1}\colon \tau(i) \mapsto \tau(j).$$ □

**6.3.21. Corolario.** *Para un $k$-ciclo $\sigma = (i_1\ i_2\ \cdots\ i_k)$ y permutación $\tau \in S_n$, la conjugación de $\sigma$ por $\tau$ es también un $k$-ciclo dado por*

$$\tau\,(i_1\ i_2\ \cdots\ i_k)\,\tau^{-1} = (\tau(i_1)\ \tau(i_2)\ \cdots\ \tau(i_k)).$$

*En general, la conjugación no cambia el tipo de ciclo de una permutación. Dos permutaciones $\sigma, \sigma' \in S_n$ son conjugadas ($\sigma' = \tau\sigma\tau^{-1}$ para alguna permutación $\tau \in S_n$) si y solamente si tienen el mismo tipo de ciclo.*

*Demostración.* Todo esto está claro de la observación precedente: la conjugación nada más cambia la numeración de nuestros elementos $\{1,2,\dots,n\}$. Para una permutación

$$\sigma = (\bullet\ \bullet\ \cdots\ \bullet)(\bullet\ \bullet\ \cdots\ \bullet)\cdots(\bullet\ \bullet\ \cdots\ \bullet)$$

la conjugación por $\tau$ nos da

$$\tau\sigma\tau^{-1} = \tau(\bullet\ \bullet\ \cdots\ \bullet)\tau^{-1}\tau(\bullet\ \bullet\ \cdots\ \bullet)\tau^{-1}\cdots\tau(\bullet\ \bullet\ \cdots\ \bullet)\tau^{-1},$$

y aquí para cada $k$-ciclo $(\bullet\ \bullet\ \cdots\ \bullet)$ en la descomposición su conjugado $\tau(\bullet\ \bullet\ \cdots\ \bullet)\tau^{-1}$ es también un $k$-ciclo. Si al principio los ciclos son disjuntos, los conjugados son también disjuntos, puesto que $\tau$ es una biyección.

Ahora si $\sigma$ y $\sigma'$ son dos permutaciones que tienen el mismo tipo de ciclo, esto significa que son idénticas salvo renumeración de los elementos $\{1,2,\dots,n\}$. Esta renumeración se realiza por cierta permutación $\tau \in S_n$ y $\sigma' = \tau\sigma\tau^{-1}$. ■

## 6.4 Grupo lineal general

En los cursos básicos de álgebra lineal mucho tiempo se dedica a multiplicación e inversión de matrices. De hecho, detrás de todo esto hay un grupo.

**6.4.1. Definición.** Sea $V$ un espacio vectorial sobre un cuerpo. Consideremos todas las aplicaciones lineales invertibles $f\colon V \to V$. Estas forman un grupo respecto a la composición habitual de aplicaciones. El elemento neutro es la aplicación identidad y los elementos inversos son las aplicaciones inversas[*]. Este grupo se denota por $\mathrm{GL}(V)$ y se llama el **grupo lineal general** de $V$.

Note que este es un análogo lineal del grupo simétrico $S_X$. De hecho, $\mathrm{GL}(V)$ es un subconjunto de $S_V$, pero no tiene sentido considerar todas las biyecciones de conjuntos $V \to V$—son muchas—y por esto restringimos nuestra atención a las biyecciones lineales; es decir, las biyecciones que preservan la estructura algebraica de $V$.

En general, todas las aplicaciones lineales $f\colon V \to V$ forman un anillo $\mathrm{End}(V)$ que se llama el **anillo de endomorfismos** de $V$. La adición en este anillo viene dada por

$$(f+g)(v) := f(v) + g(v)$$

y la multiplicación de $f$ por $g$ es la composición $f \circ g$. Este anillo no es conmutativo si $\dim V > 1$. El grupo lineal general es el grupo de unidades correspondiente:

$$\mathrm{GL}(V) = \mathrm{End}(V)^\times.$$

El procedimiento habitual para hacer cálculos con aplicaciones lineales es fijar una base y usar matrices. Entonces, podemos considerar el grupo de unidades en el anillo de matrices.

**6.4.2. Observación.** *Los elementos invertibles en el anillo de matrices $M_n(A)$ son precisamente las matrices con determinante invertible:*

$$M_n(A)^\times = \{a \in M_n(A) \mid \det a \in A^\times\}.$$

*Demostración.* Recordemos que el determinante satisface

$$\det(ab) = \det(a)\cdot\det(b)$$

para cualesquiera $a, b \in M_n(A)$. Luego, si para $a \in M_n(A)$ existe su matriz inversa $a^{-1} \in M_n(A)$, entonces

$$1 = \det(1) = \det(a\,a^{-1}) = \det(a)\cdot\det(a^{-1}) = \det(a^{-1})\cdot\det(a),$$

[*] Recuerde (o verifique ahora) que para una aplicación lineal $f\colon V \to V$ su inversa $f^{-1}\colon V \to V$ es también lineal.

lo que demuestra que para toda matriz invertible en $M_n(A)$ se tiene necesariamente $\det(a) \in A^\times$. En la otra dirección, si $\det(a) \in A^\times$, podemos usar la fórmula (también conocida como la "regla de Cramer")

$$a^{-1} = \det(a)^{-1} \operatorname{adj}(a),$$

donde $\operatorname{adj}(a)$ es la **matriz adjunta**. ■

**6.4.3. Definición.** El grupo

$$\mathrm{GL}_n(A) := M_n(A)^\times = \{a \in M_n(A) \mid \det a \in A^\times\}$$

se llama el **grupo lineal general** sobre $A$.

**6.4.4. Ejemplo.** Si $A = k$ es un cuerpo, entonces

$$\mathrm{GL}_n(k) = \{a \in M_n(k) \mid \det a \neq 0\}.$$ ▲

**6.4.5. Ejemplo.** Para las matrices con elementos enteros, tenemos

$$\mathrm{GL}_n(\mathbb{Z}) = \{a \in M_n(\mathbb{Z}) \mid \det a = \pm 1\}.$$ ▲

**6.4.6. Ejemplo.** Para $n = 1$ tenemos

$$\mathrm{GL}_1(A) = A^\times.$$

Para $n \geq 2$ y $A \neq 0$ el grupo $\mathrm{GL}_n(A)$ no es abeliano (es fácil encontrar un par de matrices invertibles que no conmutan). ▲

Notamos que para un cuerpo finito $\mathbb{F}_q$, el anillo de matrices $M_n(\mathbb{F}_q)$ es finito, de orden $q^{n^2}$, y en particular el grupo $\mathrm{GL}_n(\mathbb{F}_q)$ es también finito. ¿Cuál es su orden?

**6.4.7. Proposición.** $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1) \cdot (q^n - q) \cdots (q^n - q^{n-1})$.

*Demostración.* El grupo $\mathrm{GL}_n(\mathbb{F}_p)$ consiste de matrices invertibles de $n \times n$. Para contarlas, podemos escribirlas fila por fila (o columna por columna), recordando que entre estas no podemos tener dependencias lineales.

En la primera fila podemos escribir cualquier vector $v_1 \in \mathbb{F}_q^n$, salvo el vector nulo $(0, 0, \ldots, 0)$. Tenemos $|\mathbb{F}_q|^n - 1 = q^n - 1$ posibilidades.

Luego, en la segunda fila podemos poner cualquier vector $v_2 \in \mathbb{F}_q^n$, salvo los $q = |\mathbb{F}_q|$ vectores linealmente dependientes con $v_1$:

$$\lambda_1 v_1, \quad \lambda_1 \in \mathbb{F}_q.$$

En la tercera fila se puede poner cualquier vector, salvo los vectores linealmente dependientes con $v_1$ y $v_2$:

$$\lambda_1 v_1 + \lambda_2 v_2, \quad \lambda_1, \lambda_2 \in \mathbb{F}_q.$$

Continuando de este modo notamos que para la $i$-ésima fila hay $q^n - q^{i-1}$ posibilidades. Entonces, el número de matrices invertibles de $n \times n$ con elementos en un cuerpo finito $\mathbb{F}_q$ es

$$(q^n - 1) \cdot (q^n - q) \cdots (q^n - q^{n-1}).$$ ■

**6.4.8. Ejemplo.** El grupo $\mathrm{GL}_2(\mathbb{F}_2)$ consiste en 6 matrices:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ a := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ b := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ c := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ d := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\ e := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

He aquí su tabla de multiplicación[*].

[*] La compilé con ayuda de computadora para no equivocarme. Favor de no hacer estos cálculos otra vez; verifique alguna fila para ver cómo se multiplican las matrices sobre $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Por ejemplo,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \pmod 2.$$

| · | 1 | $a$ | $b$ | $c$ | $d$ | $e$ |
|---|---|---|---|---|---|---|
| 1 | 1 | $a$ | $b$ | $c$ | $d$ | $e$ |
| $a$ | $a$ | 1 | $d$ | $e$ | $b$ | c |
| $b$ | $b$ | $e$ | 1 | $d$ | $c$ | $a$ |
| $c$ | $c$ | $d$ | $e$ | 1 | $a$ | $b$ |
| $d$ | $d$ | $c$ | $a$ | $b$ | $e$ | 1 |
| $e$ | $e$ | $b$ | $c$ | $a$ | 1 | $d$ |

El siguiente caso no trivial sería de $\mathrm{GL}_2(\mathbb{F}_3)$, y este grupo ya tiene $(3^2-1)\cdot(3^2-3)=48$ elementos y no es muy instructivo enumerarlos todos...

Sería interesante comparar la tabla de multiplicación de arriba con la tabla de multiplicación en el grupo simétrico $S_3$.

| ∘ | id | (1 2) | (2 3) | (1 3) | (1 2 3) | (1 3 2) |
|---|---|---|---|---|---|---|
| id | id | (1 2) | (2 3) | (1 3) | (1 2 3) | (1 3 2) |
| (1 2) | (1 2) | id | (1 2 3) | (1 3 2) | (2 3) | (1 3) |
| (2 3) | (2 3) | (1 3 2) | id | (1 2 3) | (1 3) | (1 2) |
| (1 3) | (1 3) | (1 2 3) | (1 3 2) | id | (1 2) | (2 3) |
| (1 2 3) | (1 2 3) | (1 3) | (1 2) | (2 3) | (1 3 2) | id |
| (1 3 2) | (1 3 2) | (2 3) | (1 3) | (1 2) | id | (1 2 3) |

▲

## 6.5 Grupo de cuaterniones

En los grupos $\mathrm{GL}_n$ hay muchos subgrupos interesantes. Vamos a ver un ejemplo de grupo finito que puede ser realizado como cierto grupo de matrices complejas.

**6.5.1. Ejemplo.** En el grupo $\mathrm{GL}_2(\mathbb{C})$ consideremos las matrices

$$1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I := \begin{pmatrix} +i & 0 \\ 0 & -i \end{pmatrix}, \quad J := \begin{pmatrix} 0 & +1 \\ -1 & 0 \end{pmatrix}, \quad K := \begin{pmatrix} 0 & +i \\ +i & 0 \end{pmatrix}.$$

Notamos que

$$I^{-1} = -I, \quad J^{-1} = -J, \quad K^{-1} = -K.$$

Los cálculos verifican que las 8 matrices

$$Q_8 := \{\pm 1, \pm I, \pm J, \pm K\}$$

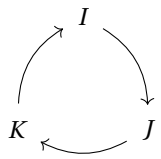
forman un subgrupo de $\mathrm{GL}_2(\mathbb{C})$, llamado el **grupo de cuaterniones**. (Aquí el índice 8 significa que $Q_8$ consiste en 8 elementos.) Primero, se ve que los cuadrados de $I, J, K$ son iguales a $-1$:

$$I^2 = J^2 = J^2 = -1.$$

La multiplicación de $I, J, K$ entre ellos es dada por

$$IJ = K,\ JI = -K,$$
$$JK = I,\ KJ = -I,$$
$$KI = J,\ IK = -J.$$

| $\cdot$ | $1$ | $I$ | $J$ | $K$ |
|---|---|---|---|---|
| $1$ | $1$ | $I$ | $J$ | $K$ |
| $I$ | $I$ | $-1$ | $K$ | $-J$ |
| $J$ | $J$ | $-K$ | $-1$ | $I$ |
| $K$ | $K$ | $J$ | $-I$ | $-1$ |




En particular, la multiplicación no es conmutativa. El dibujo a la derecha puede ayudar a memorizar las fórmulas: los caminos nos dan

$$I \to J \to IJ = K, \quad J \to K \to JK = I, \quad K \to I \to KI = J,$$

y cuando cambiamos el orden de múltiplos, el signo cambia. He aquí la tabla de multiplicación completa.

| $\cdot$ | $+1$ | $-1$ | $+I$ | $-I$ | $+J$ | $-J$ | $+K$ | $-K$ |
|---|---|---|---|---|---|---|---|---|
| $+1$ | $+1$ | $-1$ | $+I$ | $-I$ | $+J$ | $-J$ | $+K$ | $-K$ |
| $-1$ | $-1$ | $+1$ | $-I$ | $+I$ | $-J$ | $+J$ | $-K$ | $+K$ |
| $+I$ | $+I$ | $-I$ | $-1$ | $+1$ | $+K$ | $-K$ | $-J$ | $+J$ |
| $-I$ | $-I$ | $+I$ | $+1$ | $-1$ | $-K$ | $+K$ | $+J$ | $-J$ |
| $+J$ | $+J$ | $-J$ | $-K$ | $+K$ | $-1$ | $+1$ | $+I$ | $-I$ |
| $-J$ | $-J$ | $+J$ | $+K$ | $-K$ | $+1$ | $-1$ | $-I$ | $+I$ |
| $+K$ | $+K$ | $-K$ | $+J$ | $-J$ | $-I$ | $+I$ | $-1$ | $+1$ |
| $-K$ | $-K$ | $+K$ | $-J$ | $+J$ | $+I$ | $-I$ | $+1$ | $-1$ |

Aunque podríamos tomar las fórmulas de multiplicación de arriba como la *definición* del grupo $Q_8$, sin representar sus elementos por matrices, en este caso sería tedioso verificar la asociatividad. ▲

## 6.6 Grupos diédricos

En la sección anterior hemos considerado las biyecciones $f\colon V \to V$ que preservan la estructura lineal. Ahora vamos a considerar las aplicaciones $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ que preservan otra estructura que es la distancia.

**6.6.1. Definición.** Consideremos el plano $\mathbb{R}^2$ con la distancia euclidiana

$$d((x_1, y_1), (x_2, y_2)) := \sqrt{(x_1 - x_2)^2 - (y_1 - y_2)^2}.$$

Una **isometría** de $\mathbb{R}^2$ es una aplicación $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ que preserva las distancias:

$$d(f(\underline{a}), f(\underline{b})) = d(\underline{a}, \underline{b})$$

para cualesquiera $\underline{a}, \underline{b} \in \mathbb{R}^2$.

**6.6.2. Ejemplo.** Hay tres tipos fundamentales de isometrías del plano:

1) **rotación** por un ángulo $\phi$ alrededor de un punto $\underline{o} \in \mathbb{R}^2$;

2) **traslación** por un vector $v \in \mathbb{R}^2$;

3) **reflexión** respecto a una recta $\ell$.

En cursos de geometría se demuestra que toda isometría del plano es una composición de esta tres. El lector puede tratar de probarlo por su cuenta o consultar algún libro de texto. ▲

**6.6.3. Observación.** *Las isometrías de* $\mathbb{R}^2$ *forman un grupo* $\mathrm{Isom}(\mathbb{R}^2)$ *respecto a la composición.*

*Demostración.* Primero, notamos que si $f, g$ son isometrías, entonces $g \circ f$ es también una isometría: para cualesquiera $\underline{a}, \underline{b}$ tenemos

$$d(g(f(\underline{a})), g(f(\underline{b}))) = d(f(\underline{a}), f(\underline{b})) = d(\underline{a}, \underline{b}).$$

La aplicación identidad id es obviamente una isometría y es neutra respecto a la composición. Nos queda ver que toda isometría $f$ posee una aplicación inversa $f^{-1}$ que es también una isometría. Primero notamos que toda isometría $f$ es inyectiva:

$$f(\underline{a}) = f(\underline{b}) \Longrightarrow d(f(\underline{a}) = f(\underline{b})) = d(\underline{a}, \underline{b}) = 0 \Longrightarrow \underline{a} = \underline{b}.$$

Sin embargo, en general una isometría de un espacio métrico $(X, d)$ no es sobreyectiva: por ejemplo, sobre el intervalo $X = [0, \infty) \subset \mathbb{R}$ con la distancia habitual, la aplicación $f\colon x \mapsto x + 1$ es una isometría, pero $[0, 1)$ no pertenece a su imagen[*]. En el caso del plano euclidiano $\mathbb{R}^2$, las isometrías sí son sobreyectivas. Esto se sigue de que toda isometría de $\mathbb{R}^2$ es una composición de traslaciones, rotaciones y reflexiones, y estas aplicaciones son evidentemente invertibles.

Ahora si $f$ es una isometría de $\mathbb{R}^2$ y $f^{-1}$ es su aplicación inversa, entonces

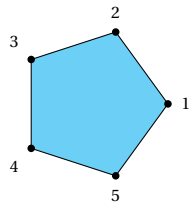
$$d(f^{-1}(\underline{a}), f^{-1}(\underline{b})) = d(ff^{-1}(\underline{a}), ff^{-1}(\underline{b})) = d(\underline{a}, \underline{b}).$$ ■

En el grupo $\mathrm{Isom}(\mathbb{R}^2)$ hay varios subgrupos interesantes; en particular los grupos diédricos.

**6.6.4. Definición.** Para un número fijo $n = 3, 4, 5, \ldots$ consideremos un polígono regular $P$ de $n$ vértices centrado en el origen del plano euclidiano $\mathbb{R}^2$. Las isometrías del plano euclidiano que preservan $P$ forman el subgrupo

$$D_n := \{f\colon \mathbb{R}^2 \to \mathbb{R}^2 \text{ isometría} \mid f(P) = P\} \subset \mathrm{Isom}(\mathbb{R}^2),$$

llamado el **grupo diédrico**[**] $D_n$.




Pentágono regular.

[*] Por este motivo algunos autores definen una isometría de espacios métricos como una *biyección* que preserva la distancia.

[**] Del griego "di-", "dos" y "edra", que en este caso significa "cara". Por ejemplo, de la misma manera la palabra "dilema" significa "dos lemas [proposiciones]". El término "poliedro" significa una figura que tiene varias caras. En este caso $P$ es una figura plana y entonces se puede decir que $P$ tiene dos caras.

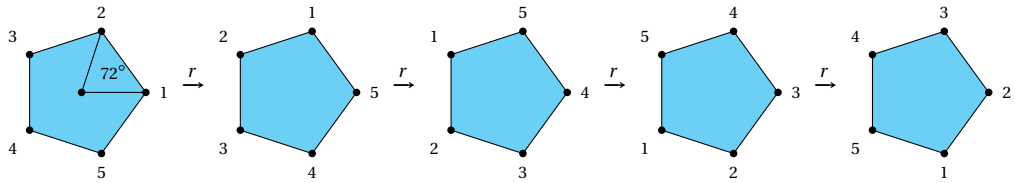
Las isometrías pueden ser descompuestas en aplicaciones de tres tipos: traslación, rotación y reflexión (simetría). Podemos descartar las traslaciones, ya que solo la traslación trivial (identidad) preserva $P$. Para las rotaciones, está claro que solo las rotaciones por los múltiplos de $360°/n$ preservan $P$. Por ejemplo, sea $r\colon \mathbb{R}^2 \to \mathbb{R}^2$ la rotación de $360°/n$ grados en sentido antihorario. Su aplicación inversa $r^{-1}$ es la rotación de $360°/n$ grados en sentido horario, que también puede ser realizada como la rotación de $(n-1)\,360°/n$ grados. Todas las rotaciones distintas son

$$r, r^2, r^3, \ldots, r^{n-1}.$$

Aquí escribimos

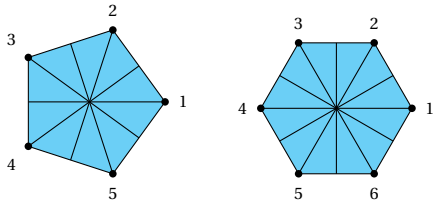
$$r^i := \underbrace{r \circ \cdots \circ r}_{i}.$$

Por la definición, $r^0 := \mathrm{id}$ y en este caso está claro que $r^n = \mathrm{id}$ (es la rotación de $360°$).

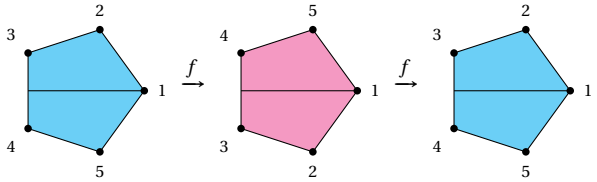



Las reflexiones que preservan $P$ son precisamente las reflexiones respecto a los ejes de simetría de nuestro polígono regular. En total tenemos $n$ ejes de simetría:

- si $n$ es impar, cada uno de ellos pasa por el origen y uno de los vértices;
- si $n$ es par, hay $n/2$ ejes de simetría que pasan por los vértices opuestos y $n/2$ que pasan por los lados opuestos.




Sea $f$ la reflexión respecto al eje que pasa por el origen y el vértice 1.




Tenemos

$$f^2 = \mathrm{id}.$$

Obviamente, $f$ no se expresa en términos de las rotaciones:

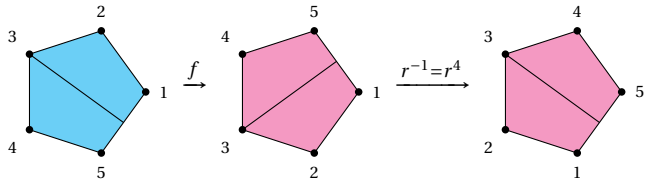
$$f \neq r^i \quad \text{para ningún } i,$$

y los elementos

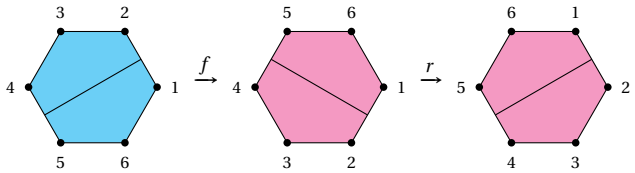
$$f, rf, r^2 f, r^3 f, \ldots, r^{n-1} f$$

son distintos y no coinciden con los $r^i$.

Notamos que una reflexión respecto a cualquier eje de simetría puede ser realizada como la reflexión $f$ seguida por una rotación $r^i$:



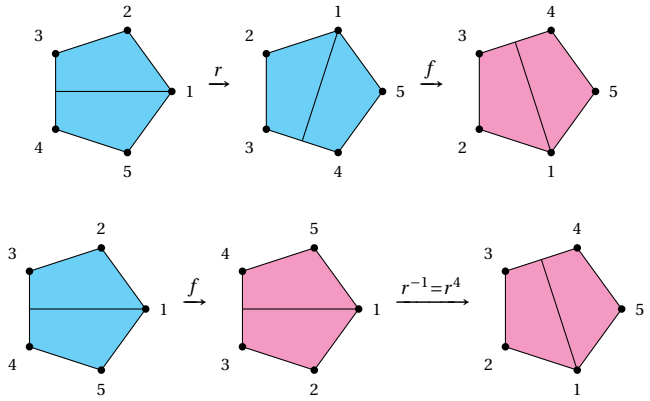

Si $n$ es par, las reflexiones respecto a los ejes que pasan por los lados opuestos también pueden ser expresadas mediante $f$ y $r$:




Entonces, hemos visto que todas las simetrías del $n$-ágono regular pueden ser expresadas como sucesiones de aplicaciones de $r$ y $f$. Notamos que

$$fr = r^{-1}f;$$

en palabras: una reflexión seguida por una rotación de $360°/n$ es lo mismo que la rotación de $360°/n$ en el sentido opuesto seguida por la reflexión respecto a la misma recta en el plano.




En particular, $rf \neq fr$, y el grupo $D_n$ no es abeliano. Por inducción se sigue que

$$fr^i = r^{-i}f \quad \text{para todo } i.$$

Nuestra discusión de arriba nos lleva a la conclusión que el grupo $D_n$ consiste en $2n$ elementos que pueden ser escritos como

$$D_n = \{\mathrm{id},\ r,\ r^2,\ \ldots,\ r^{n-1},\ f,\ rf,\ r^2f,\ \ldots,\ r^{n-1}f\}$$

Note que la tabla de multiplicación de $D_n$ puede ser resumida en las fórmulas

$$r^n = f^2 = \mathrm{id},\ fr = r^{-1}f.$$

Por ejemplo,

$$(r^i f)\cdot(r^j f) = r^i f^2 r^{-j} = r^{i-j}.$$

**6.6.5. Ejemplo.** Consideremos el caso particular de $D_3$. Este grupo tiene 6 elementos:

$$D_3 = \{\mathrm{id},\ r,\ r^2,\ f,\ rf,\ r^2f\}$$

y la tabla de multiplicación viene dada por

| $\cdot$ | id | $r$ | $r^2$ | $f$ | $rf$ | $r^2f$ |
|---|---|---|---|---|---|---|
| id | id | $r$ | $r^2$ | $f$ | $rf$ | $r^2f$ |
| $r$ | $r$ | $r^2$ | id | $rf$ | $r^2f$ | $f$ |
| $r^2$ | $r^2$ | id | $r$ | $r^2f$ | $f$ | $rf$ |
| $f$ | $f$ | $r^2f$ | $rf$ | id | $r^2$ | $r$ |
| $rf$ | $rf$ | $f$ | $r^2f$ | $r$ | id | $r^2$ |
| $r^2f$ | $r^2f$ | $rf$ | $f$ | $r^2$ | $r$ | id |

▲

## 6.7 El centro

Un subgrupo importante de un grupo no abeliano es el centro.

**6.7.1. Definición.** Para un grupo $G$, se dice que $g$ está en su **centro** si $g$ conmuta con todos los elementos de $G$: tenemos $gh = hg$ para todo $h \in G$. El conjunto de los elementos del centro se denota por

$$Z(G) := \{g \in G \mid gh = hg \text{ para todo } h \in G\} = \{g \in G \mid g = hgh^{-1} \text{ para todo } h \in G\}.$$

**6.7.2. Observación.** *$Z(G)$ es un subgrupo de $G$. El grupo es abeliano si y solamente si $Z(G) = G$.* □

**6.7.3. Ejemplo.** Según el ejercicio 6.9, para el grupo simétrico tenemos $Z(S_n) = \{\mathrm{id}\}$ para $n \geq 3$, y en este sentido $S_n$ está muy lejos de ser abeliano. ▲

**6.7.4. Ejemplo.** Revisando la tabla de multiplicación del grupo de cuaterniones, se ve que $Z(Q_8) = \{\pm 1\}$. ▲

**6.7.5. Ejemplo.** Calculemos el centro del grupo diédrico $D_n$ para $n \geq 3$. Tenemos

$$D_n = \{\mathrm{id},\ r,\ r^2,\ \ldots,\ r^{n-1},\ f,\ fr,\ fr^2,\ \ldots,\ fr^{n-1}\}.$$

Ya que todos los elementos de $D_n$ son productos de $f$ y $r$, tenemos $x \in Z(D_n)$ si y solamente si

$$fx = xf, \quad rx = xr.$$

1) Si $x = r^i f$ es una reflexión, entonces $r \cdot r^i f = r^{i+1} f$, mientras que $r^i f \cdot r = r^{i-1} f$. Esto quiere decir que $rx = xr$ si y solamente si $i + 1 \equiv i - 1 \pmod{n}$, lo que no sucede si $n \geq 3$. Podemos concluir que las reflexiones no están en el centro.

2) Si $x = r^i$ es una reflexión, entonces $x$ claramente conmuta con $r$. Luego,

$$fx = xf \iff fr^i = r^i f \iff fr^i = fr^{-i} \iff r^i = r^{-i}.$$

Esto es equivalente a $i \equiv -i \pmod{n}$; es decir, $2i \equiv 0 \pmod{n}$. Esto es posible solamente si $n$ es par e $i = n/2$.

Resumiendo nuestros cálculos, tenemos

$$Z(D_n) = \begin{cases} \{\mathrm{id}\}, & \text{si } n \geq 3 \text{ es impar,} \\ \{\mathrm{id}, r^{n/2}\}, & \text{si } n \geq 4 \text{ es par.} \end{cases}$$

▲

**6.7.6. Ejemplo.** Para $1 \leq i, j \leq n$, denotemos por $e_{ij}$ la matriz de $n \times n$ cuyos coeficientes son nulos, salvo el coeficiente $(i, j)$ que es igual a 1. Ahora para $i \neq j$ la matriz $1 + e_{ij}$ tiene 1 en la diagonal y 1 en la posición $(i, j)$. Dejo al lector calcular que

$$\det(1 + e_{ij}) = 1,$$

y en particular las matrices $1 + e_{ij}$ son invertibles. Además, para una matriz $a \in M_n(A)$ se tiene

$$a\, e_{ij} = e_{ij}\, a \text{ para todo } i \neq j$$

si y solamente si $a$ es una matriz escalar.

Ahora si una matriz $a \in \mathrm{GL}_n(A)$ está en el centro, en particular para todo $i \neq j$, en particular para todo $i \neq j$ debe cumplirse

$$a\,(1 + e_{ij}) = (1 + e_{ij})\, a.$$

Esta identidad en $\mathrm{GL}_n(A)$ es equivalente a la identidad

$$a\, e_{ij} = e_{ij}\, a$$

en el anillo de matrices $M_n(A)$. Esto nos permite concluir que el centro de $\mathrm{GL}_n(A)$ consiste en las matrices escalares invertibles:

$$Z(\mathrm{GL}_n(A)) = \left\{ \begin{pmatrix} a & & \\ & \ddots & \\ & & a \end{pmatrix} \;\middle|\; a \in A^\times \right\}.$$

Para los detalles de este argumento, haga el ejercicio 6.14. ▲

## 6.8 Subgrupos generados

**6.8.1. Observación.** *Sean $G$ 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 $\langle X \rangle$. ■

**6.8.2. 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 $X$.)

**6.8.3. 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 bastante largos pueden ser generados por pocos elementos, varios grupos infinitos importantes se generan por un número finito de elementos, etc.

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

**6.8.5. Ejemplo.** Hemos visto que el grupo diédrico $D_n$ es generado por dos elementos $r$ (rotación) y $f$ (reflexión): $D_n = \langle r, f\rangle$. ▲

**6.8.6. Ejemplo.** Hemos visto que toda permutación $\sigma \in S_n$ puede ser escrita como un producto de ciclos disjuntos. Esto significa que las permutaciones cíclicas $(i_1 \cdots i_k)$ generan el grupo simétrico $S_n$. En realidad, se pueden encontrar conjuntos de generadores más pequeños.

1) Toda permutación cíclica puede ser escrita como una composición de transposiciones gracias a la fórmula
$$(i_1\ i_2 \cdots i_k) = (i_1\ i_2)\,(i_2\ i_3)\cdots(i_{k-1}\ i_k).$$
Entonces, $S_n$ está generado por todas las transposiciones $(i\ j)$ para $1 \le i < j \le n$. En total hay $\binom{n}{2}$ de ellas.

2) Toda transposición $(i\ j)$ puede ser expresada como una combinación de las transposiciones $(1\ 2)$, $(2\ 3)$, …, $(n{-}1\ n)$. Esto puede ser visto por inducción: si $j = i+1$, no hay que probar nada, y en el caso contrario notamos que
$$(i\ j-1) = (j-1\ j)\,(i\ j)\,(j-1\ j).$$
De esta observación y 1) se sigue que las $n-1$ transposiciones de la forma $(i\ i+1)$ generan $S_n$.

3) También como el conjunto de generadores funcionarían las $n-1$ transposiciones $(1\ 2)$, $(1\ 3)$, …, $(1\ n)$. Esto se sigue de la fórmula
$$(1\ i)\,(1\ j)\,(1\ i) = (i\ j).$$

4) En fin, para generar $S_n$ bastan solo dos permutaciones: la transposición $(1\ 2)$ y la permutación cíclica $\sigma := (1\ 2 \cdots n)$. Esto se sigue de 2) y la fórmula
$$\sigma^i\,(1\ 2)\,\sigma^{-i} = (i+1\ i+2).$$ ▲

**6.8.7. 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 $T$. Para dar un ejemplo específico, consideremos la matriz

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Siguiendo el argumento de arriba, primero encontramos que

$$ST^{-2} \cdot \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & -3 \\ 0 & -1 \end{pmatrix} = S^2 T^3.$$

Luego,

$$\begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} = (ST^{-2})^{-1} S^2 T^3 = T^2 S T^3. \qquad \blacktriangle$$

**6.8.8. 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 $\frac{1}{p} \notin \langle X \rangle$. $\blacktriangle$

## 6.9 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 distintas, 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.

**6.9.1. 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 denotará 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 la notación aditiva, en lugar de "$g^n = 1$" se escribe "$n \cdot a = 0$".)

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

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

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

**6.9.5. Ejemplo.** En el grupo diédrico todas las reflexiones $f, rf, \ldots, r^{n-1}f$ tienen orden $2$, y la rotación $r$ tiene orden $n$. ▲

**6.9.6. 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 6.8.7 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.

Examinemos algunas propiedades básicas de órdenes.

**6.9.7. 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 $n$:

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

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 $r = 0$. ■

**6.9.8. 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 $\tau_i$ conmutan entre sí, así que

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

Los $\tau_i^k$ 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

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

**6.9.9. 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 6.9.7; es decir, $k \equiv \ell \pmod{n}$. ■

**6.9.10. 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 $n$. ■

**6.9.11. 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

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

## 6.10 Grupos cíclicos

**6.10.1. 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 6.9.10, 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

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

**6.10.2. 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.* El elemento $g^k$ es un generador si y solamente si $\operatorname{ord} g^k = n$. Basta entonces revisar la fórmula de 6.9.11. ■

**6.10.3. Ejemplo.** El grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ es generado por $[1]_n$: se tiene

$$[a]_n = a \cdot [1]_n.$$

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 $\phi(n)$. ▲

**6.10.4. 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 $g^{-1}$. ▲

**6.10.5. Ejemplo.** En el grupo de las $n$-ésimas raíces de la unidad $\mu_n(\mathbb{C})$ es cíclico, generado por $\zeta_n$. En general, $\zeta_n^k$ es un generador si y solo si $\operatorname{mcd}(k, n) = 1$. ▲

**6.10.6. 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 $g^k = (g^{k_0})^q$. ■

**6.10.7. Comentario.** Compare el último argumento con nuestra prueba en el capítulo 3 de que todo dominio euclidiano es un dominio de ideales principales.

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

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

Son cíclicos, generados por $n$. ▲

**6.10.9. Proposición.** *Sea $G$ es un grupo cíclico finito de orden $n$. Para todo subgrupo $H \subseteq G$ 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 6.10.6, 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 $d \mid n$. 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. ■

**6.10.10. 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. ▲

Del último resultado se puede recuperar una identidad bien conocida para la función $\phi$ de Euler.

**6.10.11. Corolario.** *Para la función $\phi$ 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 $\mathbb{Z}/n\mathbb{Z}$. ■

## 6.11 Ejercicios

**Ejercicio 6.1.** Demuestre que $\mathbb{Q} \setminus \{-1\}$ es un grupo abeliano respecto a la operación $x * y := xy + x + y$.

**Ejercicio 6.2.** Sea $k$ un cuerpo. Para dos parámetros fijos $a, b \in k$, definamos una función

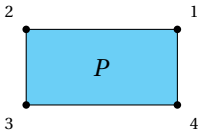
$$\phi_{a,b} \colon k \to k, \quad x \mapsto ax + b.$$

Demuestre que

$$\mathrm{Aff}_1(\mathbb{R}) := \{\phi_{a,b} \mid a \in k^\times,\ b \in k\}$$

es un grupo respecto a la composición habitual de aplicaciones. ¿Es abeliano?

**Ejercicio 6.3.** Sea $P$ un rectángulo en $\mathbb{R}^2$ que no es un cuadrado.




a) Describa todas las isometrías $f \colon \mathbb{R}^2 \to \mathbb{R}^2$ que cumplen $f(P) = P$.

b) Demuestre que estas isometrías forman un subgrupo de $\mathrm{Isom}(\mathbb{R}^2)$ y escriba la tabla de multiplicación en este subgrupo.

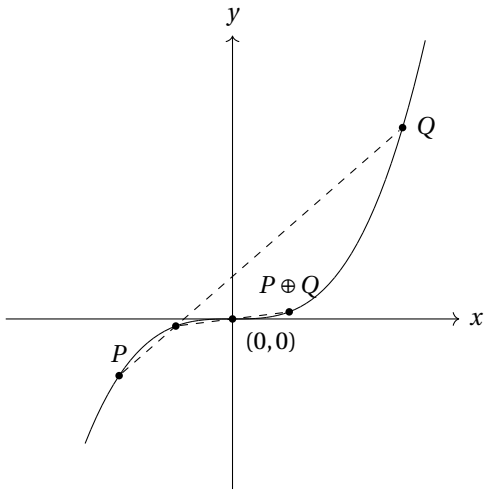
**Ejercicio 6.4.** Consideremos el conjunto de puntos $(x, y)$ en el plano real que satisfacen la ecuación $y = x^3$:

$$C(\mathbb{R}) := \{(x, y) \in \mathbb{R}^2 \mid y = x^3\}.$$

Definamos la siguiente operación sobre $C(\mathbb{R})$: para dos puntos $P, Q \in C(\mathbb{R})$, consideremos la recta $\ell$ que pasa por $P$ y $Q$, o la tangente si $P = Q$. Sea $R$ la intersección de $\ell$ con otro punto de $C(\mathbb{R})$. Entonces, definimos la suma de $P$ y $Q$ como

$$P \oplus Q := -R;$$

es decir, el punto simétrico a $R$ respecto al origen.




a) Demuestre que $C(\mathbb{R})$ es un grupo abeliano respecto a $\oplus$.

b) Demuestre que el conjunto

$$C(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 \mid y = x^3\}$$

(cuyos elementos se denominan "puntos racionales" de la curva $C$) forman un subgrupo de $C(\mathbb{R})$.

**Ejercicio 6.5.** Sea $G$ un grupo y $H \subseteq G$ un subconjunto no vacío.

a) Demuestre que $H$ es un subgrupo si y solamente si para cualesquiera $h_1, h_2 \in H$ se cumple $h_1 h_2^{-1} \in H$.

b) Demuestre que si $H$ es finito y para cualesquiera $h_1, h_2 \in H$ se cumple $h_1 h_2 \in H$, entonces $H$ es un subgrupo.

**Ejercicio 6.6.** Para el grupo $G = S_3$ y $Q_8$ encuentre todos los subgrupos $H \subseteq G$ y las inclusiones entre ellos.

**Ejercicio 6.7.** Calcule la descomposición en ciclos disjuntos del producto de ciclos

$$(1\ 2)\,(2\ 5\ 3)\,(1\ 5\ 7\ 3\ 2\ 6\ 4)\,(4\ 7\ 6) \in S_7.$$

**Ejercicio 6.8.** ¿Cuántas permutaciones $\sigma \in S_n$ cumplen la propiedad de que $\sigma(i) \neq i$ para todo $i = 1, \ldots, n$?

**Ejercicio 6.9.** Demuestre que si $n \geq 3$, entonces para toda permutación $\sigma \in S_n$, $\sigma \neq \mathrm{id}$ existe una permutación $\tau \in S_n$ tal que $\sigma\tau \neq \tau\sigma$.

**Ejercicio 6.10.** Consideremos las matrices de $n \times n$ que tienen 1 en las entradas diagonales, ceros debajo de la diagonal y elementos arbitrarios arriba de la diagonal.

$$\{(x_{ij}) \mid x_{ii} = 1 \text{ para todo } i,\ x_{ij} = 0 \text{ para } i > j\}.$$

Por ejemplo, para $n = 3$ son de la forma

$$\begin{pmatrix} 1 & x_{12} & x_{13} \\ 0 & 1 & x_{23} \\ 0 & 0 & 1 \end{pmatrix}$$

Demuestre que estas matrices forman un subgrupo de $\mathrm{GL}_n(A)$.

**Ejercicio 6.11.** Consideremos el conjunto de matrices

$$O_n(k) = \{a \in \mathrm{GL}_n(k) \mid a^t\, a = a\, a^t = 1\},$$

donde $a^t$ denota la matriz transpuesta.

a) Demuestre que $O_n(k)$ es un subgrupo de $\mathrm{GL}_n(k)$. Este se llama el **grupo ortogonal** sobre $k$.

b) Para $n = 2$ y $k = \mathbb{R}$ demuestre que los elementos de $O_2(\mathbb{R})$ son de la forma

$$\begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix} \quad \text{o} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\alpha & -\operatorname{sen}\alpha \\ \operatorname{sen}\alpha & \cos\alpha \end{pmatrix}.$$

**Ejercicio 6.12.** Supongamos que $G$ es un grupo donde cada elemento $g \in G$ satisface $g^2 = 1$. Demuestre que $G$ es abeliano.

**Ejercicio 6.13.** Sea $G$ un grupo y $H, K \subseteq G$ dos subgrupos. Demuestre que $H \cup K$ es un grupo si y solamente si $H \subseteq K$ o $K \subseteq H$.

**Ejercicio 6.14.** Para $1 \leq i, j \leq n$, denotemos por $e_{ij}$ la matriz de $n \times n$ cuyos coeficientes son nulos, salvo el coeficiente $(i, j)$ que es igual a 1.

a) Demuestre que para $i \neq j$ se tiene

$$\det(1 + e_{ij}) = 1.$$

b) Demuestre que para una matriz $a \in M_n(A)$ se cumple

$$a\,e_{ij} = e_{ij}\,a \text{ para todo } i \neq j$$

si y solamente si $a$ es una matriz escalar.

**Ejercicio 6.15.** Sea $G$ un grupo. Supongamos que para dos elementos $g, h \in G$ 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 6.16.** Supongamos que $G$ es un grupo finito de orden par. Demuestre que $G$ tiene un elemento de orden 2.

**Ejercicio 6.17.** Demuestre que si $G$ es un grupo finito de orden impar, entonces para todo $g \in G$ existe $x \in G$ tal que $x^2 = g$.

**Ejercicio 6.18.** Supongamos que para algún número $n = 1, 2, 3, 4, \ldots$ un grupo $G$ posee único elemento de orden $n$. Demuestre que $n = 1$ o 2.

**Ejercicio 6.19.** Sea $G$ un grupo tal que todo elemento $g \neq 1$ tiene el mismo orden $p$. Demuestre que $p$ es primo.

**Ejercicio 6.20.** Sean $g, h \in G$ dos elementos tales que $gh = hg$ y se tiene $\operatorname{ord} g = m$, $\operatorname{ord} h = n$.

a) Demuestre que $\operatorname{mcm}(\operatorname{ord} g, \operatorname{ord} h) \mid \operatorname{ord}(gh)$.

b) Demuestre que si $\operatorname{mcd}(m, n) = 1$, entonces $\langle g, h\rangle$ es un subgrupo cíclico de $mn$ elementos.

**Ejercicio 6.21.** Describa todos los tipos de ciclo posibles en el grupo simétrico $S_n$ para $n \leq 7$ y encuentre los órdenes correspondientes.

**Ejercicio 6.22.** Demuestre que para $\sigma \in S_n$ se tiene $\operatorname{ord}\sigma < e^{n/e}$.

**Ejercicio 6.23.** Encuentre el orden de cada uno de los elementos del grupo diédrico $D_n$.

**Ejercicio 6.24.** Encuentre los elementos de orden 2 en el grupo $\mathrm{GL}_2(\mathbb{C})$ y $\mathrm{SL}_2(\mathbb{C})$.

**Ejercicio 6.25.** Encuentre los órdenes de las siguientes matrices en $\mathrm{SL}_2(\mathbb{Z})$:

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

**Ejercicio 6.26.** Demuestre que si $p$ es un primo impar, entonces el grupo $(\mathbb{Z}/p^n\mathbb{Z})^\times$ es cíclico. Demuestre que el grupo $(\mathbb{Z}/2^n\mathbb{Z})^\times$ no es cíclico para $n \geq 3$.

**Ejercicio 6.27.** Demuestre que el conjunto

$$X = \{1/p^k \mid p \text{ primo}, k = 0, 1, 2, 3, \ldots\}$$

genera el grupo aditivo $\mathbb{Q}$.

**Ejercicio 6.28.** Consideremos $\mathbb{Q}$, el grupo de los números racionales respecto a la adición. Demuestre que todo subgrupo finitamente generado de $\mathbb{Q}$ es cíclico.

**Ejercicio 6.29.** Encuentre un subgrupo propio $G \subset \mathbb{Q}$ que no sea cíclico.

**Ejercicio 6.30.** Encuentre los elementos de orden finito en el grupo de isometrías del plano euclidiano $\mathbb{R}^2 \to \mathbb{R}^2$.

**Ejercicio 6.31.** 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.

**Ejercicio 6.32.** Sea $A$ un grupo abeliano (escrito en la notación aditiva).

1) Sea $m = 1,2,3,\ldots$ 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 6.33.** Demuestre que el grupo simétrico $S_{15}$ contiene un subgrupo cíclico de orden $105$.

**Ejercicio 6.34.** Demuestre que el grupo de todas las raíces complejas de la unidad

$$\mu_\infty(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1 \text{ para algún } n = 1,2,3,\ldots\}$$

no puede ser generado por un número finito de elementos.