Capítulo 2
Grupos

Después de estudiar el grupo simétrico S_n y el grupo alternante A_n, podemos definir qué es un grupo en general.

2.1 Definición de grupos abstractos

2.1.1. Definición. Un **grupo** es un conjunto G junto con una operación binaria

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

que satisface las siguientes propiedades.

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

$$(g * h) * k = g * (h * k).$$

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

$$e * g = g = g * e$$

para todo $g \in G$.

G3) Para todo elemento $g \in G$ existe su **inverso** $g' \in G$ tal que

$$g * g' = e = g' * g.$$

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

2.1.3. Definición. Además, si la operación $*$ en G es **conmutativa**, es decir

$$g * h = h * g$$

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 ≥ 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.

2.1.4. Ejemplo. Un conjunto de un elemento $\{e\}$ 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 e. ▲

2.1.5. Ejemplo. Hemos visto en el capítulo 1 que el grupo simétrico S_X y en particular S_n es un grupo. La operación es la composición de permutaciones; el elemento neutro es la permutación identidad id. El grupo $S_2 = \{\mathrm{id},\ (1\ 2)\}$ es abeliano. El grupo S_n para $n \geq 3$ no es abeliano. De hecho, este contiene, por ejemplo, las transposiciones $(1\ 2)$ y $(2\ 3)$ que no conmutan:

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

El grupo alternante $A_n \subset S_n$ es también un grupo respecto a las mismas operaciones que S_n. Notamos que

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

es abeliano. En efecto, tenemos

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

Para $n \geq 4$ el grupo A_n no es abeliano: por ejemplo, los 3-ciclos $(1\ 2\ 3)$ y $(1\ 2\ 4)$ no conmutan:

$$(1\ 2\ 3)\,(1\ 2\ 4) = (1\ 3)\,(2\ 4), \quad (1\ 2\ 4)\,(1\ 2\ 3) = (1\ 4)\,(2\ 3).$$

▲

2.2 Algunas observaciones respecto a los axiomas de grupos

2.2.1. Observación (Unicidad del elemento neutro). *En un grupo hay un elemento único $e \in G$ que satisface*

$$e * g = g = g * e$$

para todo $g \in G$.

Demostración. Sea $e' \in G$ otro elemento con la misma propiedad. Entonces,

$$e = e' * e = e'.$$

■

2.2.2. Observación (Unicidad de inversos). *Para $g \in G$ un elemento g' tal que*

$$g * g' = e = g' * g. \tag{2.1}$$

es único.

Demostración. Sea $g'' \in G$ otro elemento tal que

$$g * g'' = e = g'' * g. \tag{2.2}$$

Luego,

$$g' \overset{\text{G2)}}{=} g' * e \overset{(2.2)}{=} g' * (g * g'') \overset{\text{G1)}}{=} (g' * g) * g'' \overset{(2.1)}{=} e * g'' \overset{\text{G2)}}{=} g''.$$

■

2.2.3. Observación (Asociatividad generalizada). *Supongamos que $*$ es una operación asociativa: para cualesquiera $g, h, k \in G$ tenemos*

$$(g * h) * k = g * (h * k).$$

Entonces en una expresión

$$g_1 * g_2 * \cdots * g_n$$

todos los posibles modos de poner los paréntesis dan el mismo resultado.

Demostración. Funciona el mismo argumento que vimos en el capítulo 0 para las composiciones de aplicaciones. ∎

Normalmente vamos a usar la notación **multiplicativa**: escribir "$g \cdot h$" o simplemente "gh" en vez de "$g * h$". En este caso también sería lógico denotar el elemento neutro por 1, o por 1_G para subrayar que es el elemento neutro de un grupo G. En vez de "operación $*$" vamos a decir "producto". Hay que recordar que en general este producto no es conmutativo: en general $gh \neq hg$ (cuando el grupo no es abeliano). También 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 $g^2h^2 = gghh$.

Cuando el grupo es abeliano, es común la notación **aditiva**: en vez de "$g * h$" se escribe "$g + h$". En este caso el elemento neutro se denota por 0.

Puesto que para cada $g \in G$ su inverso $g' \in G$ está definido de modo único, vamos a denotarlo por g^{-1}:

$$gg^{-1} = 1 = g^{-1}g.$$

En la notación aditiva, vamos a denotar los grupos abelianos por las letras A, B, C y sus elementos por a, b, c. En vez del elementos inversos se habla de los elementos **opuestos** que se denotan por $-a$:

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

Se usa la notación

$$n \cdot a := \begin{cases} \underbrace{a + \cdots + a}_{n \text{ veces}}, & \text{si } n > 0, \\ 0, & \text{si } n = 0, \\ -((-n) \cdot a), & \text{si } n < 0. \end{cases} \tag{2.3}$$

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

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

2.2.4. Observación (Cancelación). *En todo grupo se cumple la cancelación:*

$$gh' = gh'' \Rightarrow h' = h'', \quad g'h = g''h \Rightarrow g' = g''.$$

Demostración. Multiplicando la identidad $g\,h' = g\,h''$ por g^{-1} por la izquierda, se obtiene

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

Luego,

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

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

2.2.5. Observación. *Para todo $g \in G$ se tiene $(g^{-1})^{-1} = g$.*

2.2.6. Observación. *Para un producto de dos elementos gh se tiene*

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

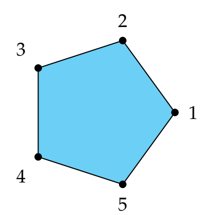
En general,

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

Para entender la fórmula $(gh)^{-1} = h^{-1}g^{-1}$, piense en el siguiente ejemplo: primero nos ponemos los calcetines y luego los zapatos. La operación inversa es primero quitarse los zapatos y luego los calcetines.

2.3 Grupos diédricos

Para un número fijo $n = 3, 4, 5, \ldots$ consideremos un polígono regular P de n vértices centrado en el origen del plano euclidiano $\mathbb{R}^2$. Numeremos sus vértices.



Pentágono regular.

Consideremos las isometrías del plano euclidiano $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ que preservan el polígono; es decir, $f(P) = P$. Estas forman un grupo respecto a la composición. El elemento neutro es la aplicación identidad id. Este grupo se llama el **grupo de simetrías del n-ágono regular** o el **grupo diédrico**[*] D_n[**].

Recordemos que 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

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

[*] 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.

[**] Ojo: en muchos textos el mismo grupo se denota por D_{2n}.

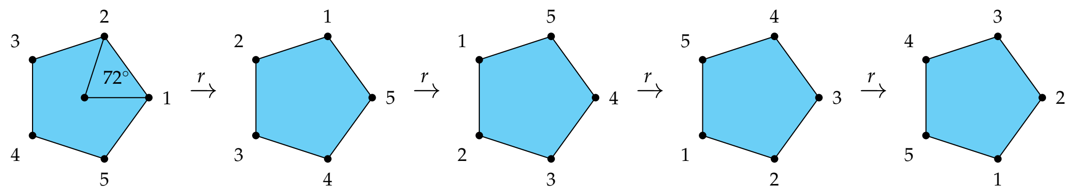
Aquí escribimos

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

Por la definición, $r^0 := \mathrm{id}$ y en este caso está claro que

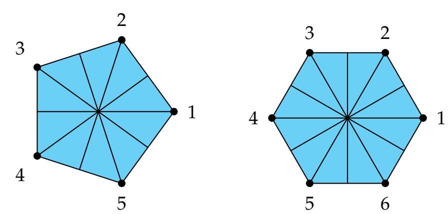
$$r^n = \mathrm{id}$$

(es la rotación de 360°).



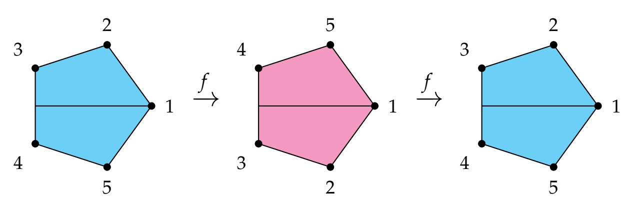
Las reflexiones que preservan P son precisamente las reflexiones respecto a los ejes de simetría de nuestro polígono regular. En total tenemos n ejes de simetría:

- 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.



(Más adelante veremos que de hecho, las propiedades del grupo D_n dependen la paridad de n.)

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 rotaciones:

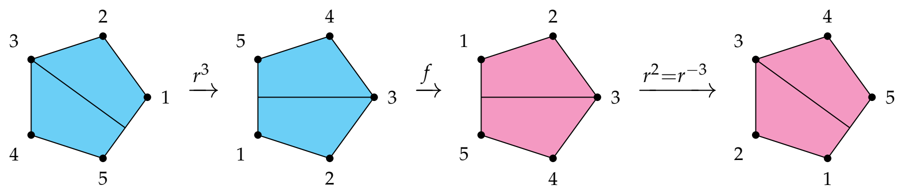
$$f \neq r^i \quad \text{para ningún } i,$$

y en general, los elementos

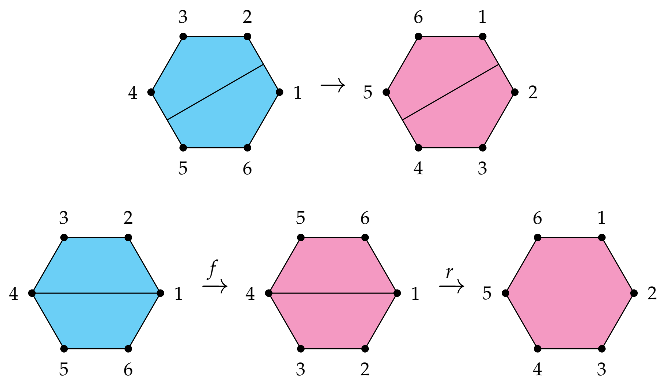
$$f, f \circ r, f \circ r^2, f \circ r^3, \ldots, f \circ r^{n-1}$$

son distintos y no coinciden con los r^i.

Notemos que una reflexión respecto a otro eje puede ser realizada como una rotación seguida por f y otra rotación:



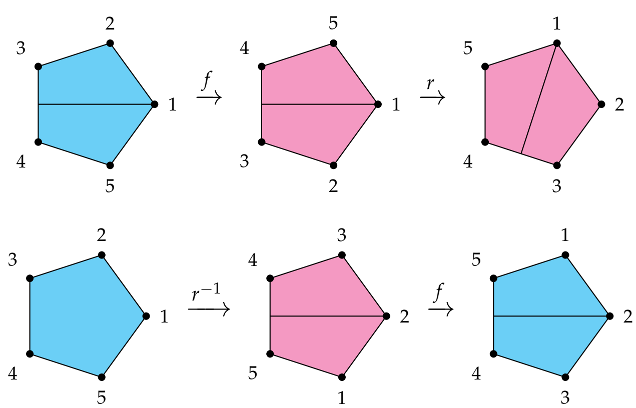
Si n es par, las reflexiones respecto a los ejes que pasan por los lados opuestos también pueden ser expresadas mediante f y r:



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

$$r \circ f = f \circ r^{-1};$$

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



En particular, $r \circ f \neq f \circ r$, y el grupo D_n no es abeliano. Por inducción se sigue que

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

Usando esto, se puede concluir que

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

(a partir de ahora voy a omitir el signo "$\circ$"). Los elementos enumerados son visiblemente distintos, y hemos calculado entonces que

$$|D_n| = 2n.$$

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

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

Por ejemplo,

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

2.3.1. Ejemplo. Consideremos el caso particular de D_3. Este grupo tiene 6 elementos:

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

y la tabla de multiplicación viene dada por

$\cdot$	id	r	r^2	f	fr	fr^2
id	id	r	r^2	f	fr	fr^2
r	r	r^2	id	fr^2	f	fr
r^2	r^2	id	r	fr	fr^2	f
f	f	fr	fr^2	id	r	r^2
fr	fr	fr^2	f	r^2	id	r
fr^2	fr^2	f	fr	r	r^2	id

▲

Los grupos diédricos D_n nos van a servir como un ejemplo importante para varias definiciones y resultados.

2.4 Grupo de cuaterniones

2.4.1. Ejemplo. Consideremos el conjunto de 8 elementos

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Definamos la multiplicación de elementos de la siguiente manera. ± 1 se comporta de modo habitual: para todo $x \in Q_8$ tenemos

$$1 \cdot x = x \cdot 1, \quad (-1) \cdot x = x \cdot (-1) = -x.$$

y

$$(-1)^2 = 1.$$

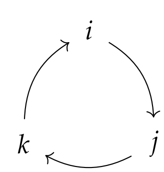
Los cuadrados de i, j, k son iguales a -1:

$$i^2 = j^2 = k^2 = -1.$$

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



El dibujo a la derecha puede ayudar a memorizar las fórmulas: los caminos nos dan $i \to j \to ij = k$, $j \to k \to jk = i$, $k \to i \to ki = j$, y cuando cambiamos el orden de múltiplos, el signo cambia.

Esto define un grupo que se llama el **grupo de cuaterniones**. El elemento neutro es 1, y el lector puede verificar existencia de elementos inversos (es fácil) y asociatividad (esto puede ser un poco tedioso). Este grupo no es abeliano.

$\cdot$	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

▲

2.5 Subgrupos

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

1) $1_G \in H$,

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 $H \neq \emptyset$.

2.5.2. 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. ▲

2.5.3. Ejemplo. Hemos visto que el grupo alternante A_n es un subgrupo de S_n. ▲

2.5.4. Ejemplo. Las isometrías del plano euclidiano $\mathbb{R}^2$ forman un grupo. El grupo diédrico D_n es un subgrupo finito. ▲

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

Demostración. Claro a partir de la definición de subgrupo. ■

Ahora compilemos las listas completas de subgrupos para algunos grupos de cardinalidad pequeña.

2.5.6. Ejemplo. En el grupo Q_8, aparte de los subgrupos triviales $\{1\}$ y Q_8, hay un subgrupo de orden 2, que es $\{\pm 1\}$, y tres subgrupos de orden 4:

$$\{\pm 1, \pm i\},\ \{\pm 1, \pm j\},\ \{\pm 1, \pm k\}.$$

Las inclusiones de subgrupos están dibujados en el diagrama de abajo.

$$
\begin{tikzcd}
& Q_8 & \\
\{\pm 1, \pm i\} \arrow[ur] & \{\pm 1, \pm j\} \arrow[u] & \{\pm 1, \pm k\} \arrow[ul] \\
& \{\pm 1\} \arrow[ul] \arrow[u] \arrow[ur] & \\
& \{1\} \arrow[u] &
\end{tikzcd}
$$

▲

2.5.7. Ejemplo. Consideremos el grupo diédrico

$$D_4 = \{\mathrm{id},\ r,\ r^2,\ r^3,\ f,\ fr,\ fr^2,\ fr^3\}.$$

Al igual que Q_8, este tiene 8 elementos, pero la estructura de sus subgrupos es totalmente diferente. Tenemos 5 subgrupos de orden 2:

$$\{\mathrm{id},\ r^2\},\ \{\mathrm{id},\ f\},\ \{\mathrm{id},\ fr\},\ \{\mathrm{id},\ fr^2\},\ \{\mathrm{id},\ fr^3\}.$$

y 3 subgrupos de orden 4:

$$\{\mathrm{id}, f, r^2, fr^2\},\ \{\mathrm{id}, r, r^2, r^3\},\ \{\mathrm{id},\ fr, r^2, fr^3\}.$$

$$
\begin{tikzcd}
& & D_4 & & \\
& \{\mathrm{id}, f, r^2, fr^2\} \arrow[ur] & \{\mathrm{id}, r, r^2, r^3\} \arrow[u] & \{\mathrm{id},\ fr, r^2, fr^3\} \arrow[ul] & \\
\{\mathrm{id}, fr^2\} \arrow[ur] & \{\mathrm{id}, f\} \arrow[u] & \{\mathrm{id}, r^2\} \arrow[ul] \arrow[u] \arrow[ur] & \{\mathrm{id},\ fr\} \arrow[u] & \{\mathrm{id},\ fr^3\} \arrow[ul] \\
& & \{\mathrm{id}\} \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}
$$

▲

2.5.8. Ejemplo. Revisando los elementos del grupo alternante A_4, se puede compilar la lista de sus subgrupos.

Cada una de las tres permutaciones de la forma $(\bullet\ \bullet)\,(\bullet\ \bullet)$ corresponde a un subgrupo de orden 2:

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

Y junto con id, estas tres permutaciones forman un subgrupo de orden 4:

$$V := \{\mathrm{id}, (1\ 2)\,(3\ 4), (1\ 3)\,(2\ 4), (1\ 4)\,(2\ 3)\}$$

(la letra V viene del alemán “Vierergruppe”, “grupo de cuatro”; el mismo grupo se conoce como el **grupo de Klein**).

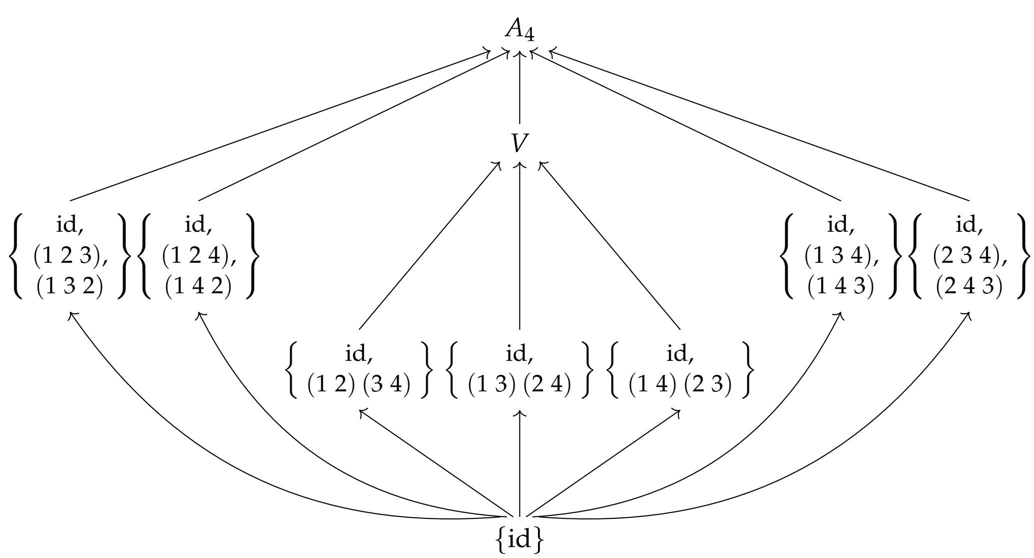
$\circ$	id	$(1\,2)\,(3\,4)$	$(1\,3)\,(2\,4)$	$(1\,4)\,(2\,3)$
id	id	$(1\,2)\,(3\,4)$	$(1\,3)\,(2\,4)$	$(1\,4)\,(2\,3)$
$(1\,2)\,(3\,4)$	$(1\,2)\,(3\,4)$	id	$(1\,4)\,(2\,3)$	$(1\,3)\,(2\,4)$
$(1\,3)\,(2\,4)$	$(1\,3)\,(2\,4)$	$(1\,4)\,(2\,3)$	id	$(1\,2)\,(3\,4)$
$(1\,4)\,(2\,3)$	$(1\,4)\,(2\,3)$	$(1\,3)\,(2\,4)$	$(1\,2)\,(3\,4)$	id

Para los 3-ciclos tenemos

$$\begin{aligned} (1\,2\,3)^2 &= (1\,3\,2), & (1\,3\,2)^2 &= (1\,2\,3),\\ (1\,2\,4)^2 &= (1\,4\,2), & (1\,4\,2)^2 &= (1\,2\,4),\\ (1\,3\,4)^2 &= (1\,4\,3), & (1\,4\,3)^2 &= (1\,3\,4),\\ (2\,3\,4)^2 &= (2\,4\,3), & (2\,4\,3)^2 &= (2\,3\,4), \end{aligned}$$

lo que nos da cuatro subgrupos de orden 3:

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



Hay una manera ingeniosa de ver que en A_4 no hay otros subgrupos, pero todavía no hemos desarrollado el lenguaje adecuado. ▲

2.5.9. Comentario. El número de subgrupos de S_n y A_n crece muy rápido con n. Hemos descrito los subgrupos de A_4, pero en A_5 ya hay 59 subgrupos. De la misma manera, en S_3 hay 6 diferentes subgrupos (haga el ejercicio 2.6 de abajo), pero en S_4 ya son 30.

n:	2	3	4	5	6	7	8	9	10
subgrupos de S_n:	2	6	30	156	1455	11 300	151 221	1 694 723	29 594 446
subgrupos de A_n:	1	2	10	59	501	3786	48 337	508 402	6 469 142

Véanse `http://oeis.org/A005432` y `http://oeis.org/A029725`.

2.6 El centro

Un subgrupo importante es el centro.

2.6.1. 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

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

2.6.2. Observación. *G es abeliano si y solamente si $Z(G) = G$.*

2.6.3. Observación. *$Z(G)$ es un subgrupo de G.*

Demostración. Para la identidad $1 \in G$ obviamente tenemos $1h = h1 = h$ para todo $h \in G$, entonces $1 \in Z(G)$. Luego, si $g, g' \in Z(G)$, entonces para todo $h \in G$

$$(gg')\,h = g\,(g'h) = g\,(hg') = (gh)\,g' = (hg)\,g' = h\,(gg'),$$

así que $gg' \in Z(G)$. Por fin, si $g \in Z(G)$, entonces para todo $h \in G$ tenemos

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

así que $g^{-1} \in Z(G)$. ■

2.6.4. Ejemplo. 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.

De hecho, sea $\sigma \in S_n$ una permutación diferente de id. Entonces existen diferentes índices $i, j \in \{1, \ldots, n\}$ tales que

$$\sigma\colon i \mapsto j.$$

Ya que $n > 2$, podemos elegir otro índice k tal que $k \neq i$ y $k \neq j$. Consideremos la transposición $\tau = (j\ k)$. Tenemos

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

Entonces, $\tau\sigma\tau^{-1} \neq \sigma$ y por lo tanto $\sigma \notin Z(G)$. ▲

2.6.5. Ejemplo. Revisando la tabla de multiplicación del grupo de cuaterniones Q_8, se ve que

$$Z(Q_8) = \{\pm 1\}.$$

▲

2.6.6. 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

$$f\,x = x\,f, \quad r\,x = x\,r.$$

1) Para x de la forma fr^i tenemos

$$r\,x = x\,r \iff rfr^i = fr^i \cdot r \iff fr^{i-1} = fr^{i+1} \iff r^{i-1} = r^{i+1}.$$

La última condición es equivalente a $i - 1 \equiv i + 1 \pmod{n}$, lo que es imposible para $n > 2$. Podemos concluir que los elementos fr^i no están en el centro.

2) Para x de la forma r^i tenemos obviamente $r\,x = x\,r$. Luego,

$$f\,x = x\,f \iff fr^i = r^i f \iff fr^i = fr^{-i} \iff r^i = r^{-i}.$$

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

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

▲

2.7 Ejercicios

Ejercicio 2.1. *Calcule que* $(fr^i)^2 = \mathrm{id}$ *en* D_n *para cualquier* $i \in \mathbb{Z}$. *En general, calcule* $(fr^i)(fr^j)$ *para* $i, j \in \mathbb{Z}$.

Ejercicio 2.2. *Demuestre que* $\mathbb{Q} \setminus \{-1\}$ *es un grupo abeliano respecto a la operación*

$$x * y := xy + x + y.$$

Ejercicio 2.3. *Sea* X *un conjunto y* $\mathbf{2}^X$ *el conjunto de sus subconjuntos. Para* $A, B \subseteq X$, *definamos la* ***diferencia simétrica*** *por*

$$A \Delta B := (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

Demuestre que $\mathbf{2}^X$ *es un grupo abeliano respecto a* Δ.

Ejercicio 2.4. *Para dos parámetros fijos* $a, b \in \mathbb{R}$ *definamos una función*

$$\begin{aligned} \phi_{a,b} \colon \mathbb{R} &\to \mathbb{R}, \\ x &\mapsto ax + b. \end{aligned}$$

Consideremos el conjunto

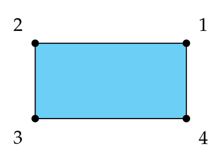
$$\mathrm{Aff}_1(\mathbb{R}) := \{\phi_{a,b} \mid a \in \mathbb{R} \setminus \{0\},\ b \in \mathbb{R}\}.$$

Verifique que $\mathrm{Aff}_1(\mathbb{R})$ *es un grupo respecto a la composición habitual de aplicaciones y que no es abeliano.*

Ejercicio 2.5. *Supongamos que* G *es un grupo donde cada elemento* $g \in G$ *satisface* $g^2 = 1$. *Demuestre que* G *es abeliano.*

Ejercicio 2.6. *Encuentre todos los subgrupos del grupo simétrico* S_3.

Ejercicio 2.7. *Escriba la tabla de multiplicación del grupo de simetrías de un rectángulo que no es un cuadrado. (Note que este tiene menos simetrías que un cuadrado.)*



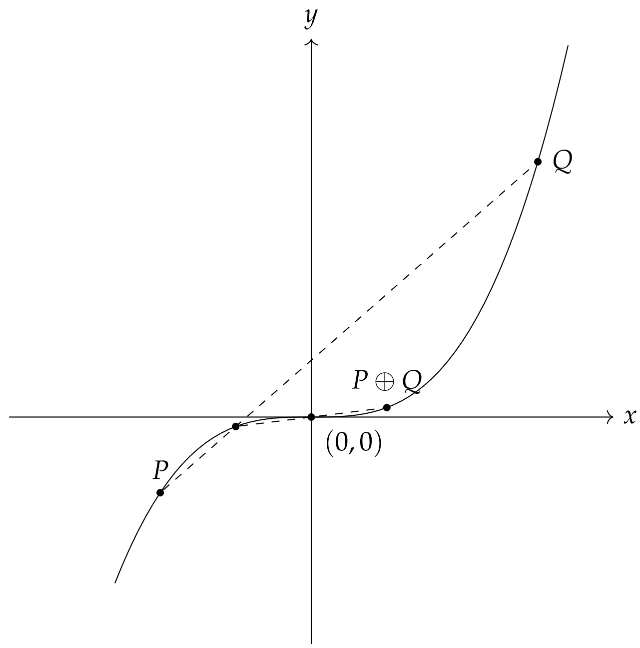
Ejercicio 2.8. *Consideremos el conjunto de puntos* (x, y) *en el plano real que satisfacen la ecuación* $y = x^3$:

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

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

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

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



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

2) *Demuestre que el conjunto*

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

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

Nota: este ejercicio requiere un buen conocimiento del álgebra de nivel de Baldor.

Ejercicio 2.9. *Sea* G *un grupo y* $H, K \subset G$ *dos subgrupos. Demuestre que* $H \cup K$ *es un grupo si y solamente si* $H \subseteq K$ *o* $K \subseteq H$.

Ejercicio 2.10. *Hemos visto que el centro del grupo simétrico es trivial:*

$$Z(S_n) = \{\mathrm{id}\} \quad \textit{para } n \geq 3.$$

Demuestre que para el grupo alternante sobre 4 *elementos*

$$Z(A_4) = \{\mathrm{id}\}.$$

Nota: más adelante veremos en el curso que $Z(A_n) = \{\mathrm{id}\}$ *para* $n \geq 4$.