Pequeño Instituto de Matemáticas
2024-2025

Fechas: 31 de enero, 7, 14 de febrero de 2025
Teoría de Grupos I
Grupo: Mercurio (Soluciones)

Un **grupo** es un conjunto con una operación que cumple una serie de propiedades. A los conjuntos con operaciones y propiedades los solemos llamar estructuras algebraicas.

Conjuntos y aplicaciones

Quizás ya sepas qué es un conjunto y qué es una aplicación (o función, es lo mismo), pero por si acaso lo repasaremos aquí. Puedes comenzar con la siguiente sección y volver a esta más tarde si lo necesitas.

Por un **conjunto** entenderemos una colección bien definida de objetos. Pueden ser cualquier cosa: números, letras, palabras, etc.. Cuando os dan un conjunto es muy importante tratar de entender qué elementos lo forman.

Ejemplo.

1. El conjunto $A = \{x \in \mathbb{R} : x^2 = 1\}$ de lo números reales cuyo cuadrado es igual a 1 está formado por dos elementos 1 y -1. Como vemos en este caso hemos podido determinar explícitamente todos los elementos del conjunto: $A = \{-1, 1\}$.

2. $\mathbb{N} = \{1, 2, 3, \ldots\}$ el conjunto de números naturales.

3. Sea
$$B = \{p^k q^l r^n \in \mathbb{N} \colon p, q, r \text{ son primos distintos}, k, r, n \in \mathbb{N}\}$$
el conjunto de los números naturales en cuya factorización en producto de primos aparecen exactamente 3 primos distintos.

   No vamos a poder enumerar todos los elementos de B de forma explícita. Sin embargo, si nos dan un número natural $n \in \mathbb{N}$ sabremos si pertenece a B o no (aunque nos pueda llevar un tiempo calcularlo). Por ejemplo, el número 123456789 se factoriza en producto de primos como $123456789 = 3^2 \cdot 3607 \cdot 3803$ y por lo tanto pertenece al conjunto B.

Una **aplicación** o **función** entre de un conjunto A en otro conjunto B es una regla que a cada elemento de A se le asigna un único elemento de B. Se dice que A es el **dominio** de la función.

Ejemplo.

1. Sea $A = \{(x, y) \colon x, y \in \mathbb{R}\}$ el conjunto de todos los pares de los números reales. Este conjunto se denota normalmente como $\mathbb{R}^2$. Su representación geométrica es el plano: cada punto del plano tiene dos coordinadas reales. Sea $B = \mathbb{R}$ el conjunto de todos los números reales. Entonces la regla que manda un elemento (x, y) del conjunto A al elemento $|x - y|$ de B es una aplicación de A en B.

2. Sea A el conjunto de todas las personas y B el conjunto de todos los colores. Entonces la regla que asigna a una persona el color de sus ojos, es una aplicación de A en B,

Para decir que ϕ es una aplicación de un conjunto A en un conjunto B escribiremos $\phi : A \to B$. Entonces, la imagen de $a \in A$ denotaremos como $\phi(a)$.

Dado un conjunto A, siempre existe la aplicación identidad de A. Es una aplicación $\mathrm{Id}_A : A \to A$ que manda cada elemento $a \in A$ a si mismo: $\mathrm{Id}_A(a) = a$.

Si tenemos dos aplicaciones $\alpha : A \to B$ y $\beta : B \to C$, denotemos por $\beta \circ \alpha : A \to C$ la aplicación que manda $a \in A$ a $\beta(\alpha(a)) \in C$, es decir, aplicar primero α y luego β (observa que se escribe $\beta \circ \alpha$, al revés, y se lee "α compuesto con β"). La operación $\circ$ se llama **composición**.

Sea $\alpha : A \to B$ una aplicación entre dos conjuntos. La aplicación α se llama **inyectiva** si para dos elementos distintos $a_1 \neq a_2 \in A$ sus imágenes $\alpha(a_1)$ y $\alpha(a_2)$ son también distintas: $\alpha(a_1) \neq \alpha(a_2)$. La aplicación α se llama **sobreyectiva** si para cualquier $b \in B$ existe $a \in A$ tal que $\alpha(a) = b$. Cuando se cumplen ambas condiciones para α inyectiva y sobreyectiva, diremos que α es **biyectiva**. En otras palabra α es biyectiva si para cualquier $b \in B$ existe un único elemento a tal que $\alpha(a) = b$. Esta condición nos permite "invertir" la aplicación α. Definamos la aplicación $\alpha^{-1} : B \to A$ tal que $\alpha^{-1}(b)$ es el único $a \in A$ que satisface $\alpha(a) = b$. Notemos que α^{-1} satisface la siguiente propiedad:

$$\alpha^{-1} \circ \alpha = \mathrm{Id}_A \text{ y } \alpha \circ \alpha^{-1} = \mathrm{Id}_B .$$

De hecho está propiedad caracteriza las aplicaciones biyectivas.

Problema 1. Encuentra ejemplos cotidianos de funciones inyectivas, no inyectivas, sobreyectivas, no sobreyectivas y biyectivas. Por ejemplo, la aplicación que a cada persona asigna su número de DNI es inyectiva. ¿Cuál es su dominio?

Problema 2. Sea $\alpha : A \to B$ una aplicación. Entonces α es biyectiva si y sólo si existe $\beta : B \to A$ tal que

$$\beta \circ \alpha = \mathrm{Id}_A \text{ y } \alpha \circ \beta = \mathrm{Id}_B .$$

Solución. La existencia de β si α es biyectiva está demostrada antes del ejercicio.

Ahora suponemos que existe β tal que

$$\beta \circ \alpha = \mathrm{Id}_A \text{ y } \alpha \circ \beta = \mathrm{Id}_B .$$

Probamos primero que α es sobreyectiva. Dado $b \in B$ si ponemos $a = \beta(b)$, entonces

$$\alpha(a) = \alpha(\beta(b)) = b.$$

Es decir, α es sobreyectiva.

Ahora veamos que α es inyectiva. Dados $a_1, a_2 \in A$, si $\alpha(a_1) = \alpha(a_2)$, obtendremos que

$$a_1 = \beta(\alpha(a_1)) = \beta(\alpha(a_2)) = a_2.$$

esto prueba que α es inyectiva. □

Dados cuatro conjuntos A, B, C y D y tres aplicaciones $\alpha : A \to B$, $\beta : B \to C$ y $\gamma : C \to D$, para cualquier $a \in A$,

$$(\gamma \circ (\beta \circ \alpha))(a) = \gamma((\beta \circ \alpha)(a)) = \gamma(\beta(\alpha(a))) = (\gamma \circ \beta)(\alpha(a)) = ((\gamma \circ \beta) \circ \alpha)(a).$$

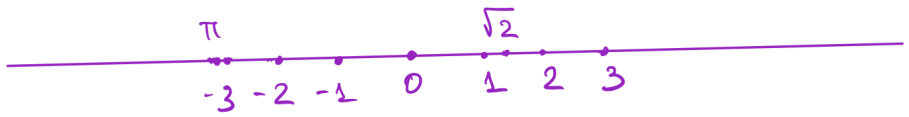
Es decir, $\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha$. Es la propiedad **asociativa** que va a jugar un papel importante.

Primeros ejemplos de grupos

Antes de introducir la definición formal de un grupo estudiaremos distintos ejemplos.

El grupo de isometrías de la recta real

Denotamos por $\mathbb{R}$ el conjunto de los número reales. Vamos a representar $\mathbb{R}$ de forma geométrica, como una recta.



Entonces podemos medir la distancia entre dos puntos $a, b \in \mathbb{R}$:

$$d(a,b) = |a-b|.$$

El grupo de **isometrías** de $\mathbb{R}$ es el conjunto de aplicaciones $\phi : \mathbb{R} \to \mathbb{R}$ que conservan la distancia en $\mathbb{R}$:

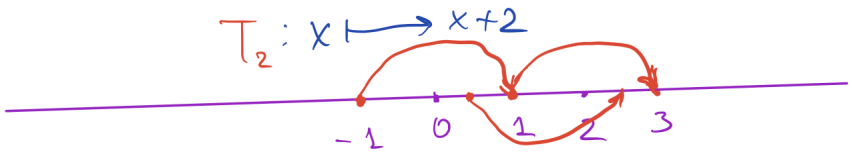
$$\text{para todos } a, b \in \mathbb{R} \text{ se cumple que } d(\phi(a), \phi(b)) = d(a,b).$$

Este conjunto lo denotaremos como $\mathrm{Isom}(\mathbb{R})$. En la notación matemática

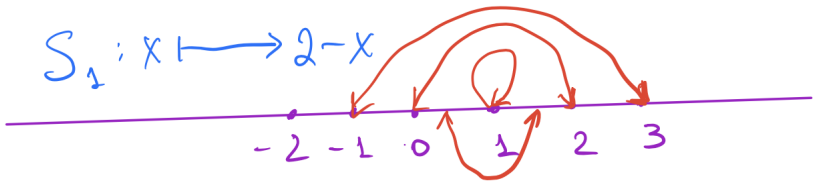
$$\mathrm{Isom}(\mathbb{R}) = \{\phi : \mathbb{R} \to \mathbb{R} \colon |\phi(a) - \phi(b)| = |a-b|, \forall a, b \in \mathbb{R}\}. \tag{1}$$

Problema 3. 1. Sea $\phi : \mathbb{R} \to \mathbb{R}$, tal que $\phi(x) = x^2$. ¿Es $\phi \in \mathrm{Isom}(\mathbb{R})$? (¿Es ϕ una isometría de $\mathbb{R}$?)

2. Sea $a \in \mathbb{R}$ y $T_a : \mathbb{R} \to \mathbb{R}$ tal que $T_a(x) = x + a$. ¿Es $T_a \in \mathrm{Isom}(\mathbb{R})$?



3. Sea $a \in \mathbb{R}$ y $S_a : \mathbb{R} \to \mathbb{R}$ tal que $S_a(x) = 2 \cdot a - x$. ¿Es $S_a \in \mathrm{Isom}(\mathbb{R})$? Dar una interpretación geométrica para $S_a(x)$.



4. Sean $a, b \in \mathbb{R}$ dos puntos de la recta distintos y $\alpha \in \mathrm{Isom}(\mathbb{R})$. Supongamos que α fija a y b. Demostrar que α fija todos los puntos de $\mathbb{R}$ (es decir, $\alpha = T_0 = \mathrm{Id}$).

5. Sea $a \in \mathbb{R}$ y $\alpha \in \mathrm{Isom}(\mathbb{R})$. Supongamos que α fija sólo el punto a, es decir, $\alpha(a) = a$. Demostrar que $\alpha = S_a$.

6. Sea $\alpha \in \mathrm{Isom}(\mathbb{R})$. Supongamos que α no fija ningún punto en $\mathbb{R}$. Demostrar que existe $0 \neq a \in \mathbb{R}$ tal que $\alpha = T_a$.

Solución. 1. No lo es. La distancia entre 2 y 1 es 1, pero la distancia entre sus imágenes es 3.

2. Sí lo es. Sean $x_1, x_2 \in \mathbb{R}$. Entonces,

$$|T_a(x_1) - T_a(x_2)| = |(x_1 + a) - (x_2 + a)| = |x_1 - x_2|.$$

3. Sí lo es. Sean $x_1, x_2 \in \mathbb{R}$. Entonces,

$$|S_a(x_1) - S_a(x_2)| = |(2a - x_1) - (2a - x_2)| = |x_1 - x_2|.$$

La interpretación geométrica: S_a es la reflexión de R respecto al punto a.

4. Sea $x \in \mathbb{R}$. Como

$$|\alpha(x) - a| = |\alpha(x) - \alpha(a)| = |x - a|,$$

obtenemos que $\alpha(x) = x$ o $\alpha(x) = 2a - x$. De la misma forma $\alpha(x) = x$ o $\alpha(x) = 2b - x$. Por lo tanto, si $\alpha(x) \neq x$, entonces $2a - x = 2b - x$ y por lo tanto $a = b$. Pero los puntos a y b son distintos. Entonces $\alpha(x) = x$.

5. Argumentamos como en el apartado 4.

6. Sea $a = \alpha(0)$. Está claro que $a \neq 0$. Entonces para cualquier $0 \neq x \in R$,

$$|\alpha(x) - a| = |\alpha(x) - \alpha(0)| = |x - 0| = |x|.$$

Por lo tanto $\alpha(x) = x + a$ o $\alpha(x) = a - x$. Si siempre ocurre el primer caso, obtendremos que $\alpha = T_a$.

Supongamos que para algún $0 \neq x \in \mathbb{R}$, $\alpha(x) = a - x$. Primero observemos que $x \neq \frac{a}{2}$, porque en el caso contrario $\alpha(\frac{a}{2}) = \frac{a}{2}$. Por lo tanto, $\alpha(\frac{a}{2}) = \frac{3a}{2}$.

Por lo tanto

$$|x + \frac{a}{2}| = |a - x - \frac{3a}{2}| = |\alpha(x) - \alpha(\frac{a}{2})| = |x - \frac{a}{2}|.$$

Es decir $x = 0$, una contradicción.

□

Como consecuencia del ejercicio obtenemos la descripción explícita del conjunto $\mathrm{Isom}(\mathbb{R})$:

$$\mathrm{Isom}(\mathbb{R}) = \{T_a, S_a \colon a \in \mathbb{R}\}.$$

Problema 4. 1. Usando la definición de $\mathrm{Isom}(\mathbb{R})$, demuestra que la composición de dos isometrías de $\mathbb{R}$ es también una isometría de $\mathbb{R}$.

2. Demuestra que una isometría de $\mathbb{R}$ es biyectiva y su inversa es también una isometría.

3. Demuestra que si dos isometrías coinciden en dos puntos distintos, entonces son iguales. Pista: lo más fácil, con diferencia, es usar el apartado 2 de este problema, luego el 1, y por último el apartado 4 del problema 3.

4. Sean $a, b \in \mathbb{R}$. Calcula

$$T_a \circ T_b, S_a \circ S_b, T_a \circ S_b, S_a \circ T_b.$$

Solución. 1. Sean α and β sos isometrias de $\mathbb{R}$. Tenemos que comprobar que para cualquier par $x_1, x_2 \in \mathbb{R}$ se cumple

$$|(\alpha \circ \beta)(x_1) - (\alpha \circ \beta)(x_2)| = |x_1 - x_2|.$$

En efecto,

$$|(\alpha \circ \beta)(x_1) - (\alpha \circ \beta)(x_2)| = |\alpha(\beta(x_1)) - \alpha(\beta(x_2))| = |\beta(x_1) - \beta(x_2)| = |x_1 - x_2|.$$

2. Hemos descrito todas las isometrías de $\mathbb{R}$: $\mathrm{Isom}(\mathbb{R}) = \{T_a, S_a \colon a \in \mathbb{R}\}$ y son todas biyectivas. Ahora $T_a^{-1} = T_{-a}$ y $S_a^{-1} = S_a$.

Notemos que, a partir de la definición de isometría, se deduce fácilmente que esta es inyectiva. La demostración de que es sobreyectiva requiere consideraciones más avanzadas sobre la topología de $\mathbb{R}$.

3. Sean $\alpha, \beta \in \mathrm{Isom}(\mathbb{R})$ y supongamos $\alpha(x_1) = \beta(x_1)$ y $\alpha(x_2) = \beta(x_2)$ para $x_1 \neq x_2 \in \mathbb{R}$. Por el apartado anterior podemos considerar $\gamma = \beta^{-1} \circ \alpha \in \mathrm{Isom}(\mathbb{R})$. Entonces, $\gamma(x_1) = x_1$ y $\gamma(x_2) = x_2$. Por lo tanto, $\gamma = \mathrm{Id}_{\mathbb{R}}$. Entonces $\alpha = \beta$.

4. Por el apartado anterior para determinar una isometría de $\mathbb{R}$ basta ver como esta actúa sobre dos puntos destintos de $\mathbb{R}$. Por ejemplo, consideramos $\gamma = T_a \circ S_b$. Supongamos por un momento que $b \neq 0$. Entonces

$$\gamma(0) = (T_a \circ S_b)(0) = T_a(S_b(0)) = T_a(2b) = 2b + a, \ \gamma(b) = (T_a \circ S_b)(b) = T_a(S_b(b)) = T_a(b) = b + a.$$

Si $\gamma = T_c$ para algún $c \in \mathbb{R}$, entonces $c = 2b + a$ y $b + c = b + a$. Es decir, $b = 0$, que contradice nuestra suposición.

Por lo tanto, la única posibilidad es que $\gamma = S_c$ para algún $c \in \mathbb{R}$. Entonces, $2c = 2b+a$ y $2c-b = b+a$. Por lo tanto, $c = \frac{a+2b}{2}$ y

$$T_a \circ S_b = S_{\frac{a+2b}{2}}$$

si $b \neq 0$. Un argumento similar muestra que la misma formula se cumple si $b = 0$. □

$(\mathrm{Isom}(\mathbb{R}), \circ)$ es nuestro primer ejemplo de grupo.

El grupo de isometrías del plano real

En esta sección vamos a estudiar de forma similar el grupo de isometrías del plano real. El plano real $\mathbb{R}^2$ es el conjunto $\{(x, y) \colon x, y \in \mathbb{R}\}$ de pares de elementos de $\mathbb{R}$. La distancia entre dos puntos de $\mathbb{R}^2$ está dada por la fórmula

$$d((a, b), (c, d)) = \sqrt{(a - c)^2 + (b - d)^2}.$$

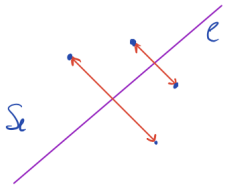
Una **isometría** de $\mathbb{R}^2$ es una aplicación $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ que conserva la distancia:

$$d(\phi(p), \phi(q)) = d(p, q), \text{ para todos } p, q \in \mathbb{R}^2.$$

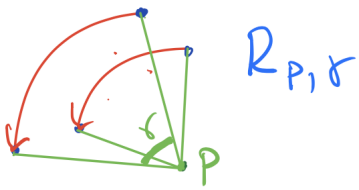
El conjunto de todas las isometrías de $\mathbb{R}^2$ lo denotaremos por $\mathrm{Isom}(\mathbb{R}^2)$. En el siguiente ejercicio vamos a describir todas las isometrías del plano.

Problema 5. 1. Sean $p, q, r \in \mathbb{R}^2$ tres puntos del plano que no están en una misma recta y sea $\alpha \in \mathrm{Isom}(\mathbb{R}^2)$. Supongamos $\alpha(p) = p$, $\alpha(q) = q$ y $\alpha(r) = r$. Entonces α es la isometría que deja todos los puntos fijos (es decir, $\alpha = \mathrm{Id}_{\mathbb{R}^2}$).

2. Sea $\alpha \in \mathrm{Isom}(\mathbb{R}^2)$. Tenemos dos puntos p y q, por los que pasa una recta l. Supongamos que $\mathrm{Id} \neq \alpha$ fija p y q, y ningún otro punto que no esté en l. Demuestra que α manda cualquier punto a su simétrico con respecto a l. (Vamos a denotar esta isometría por S_l).



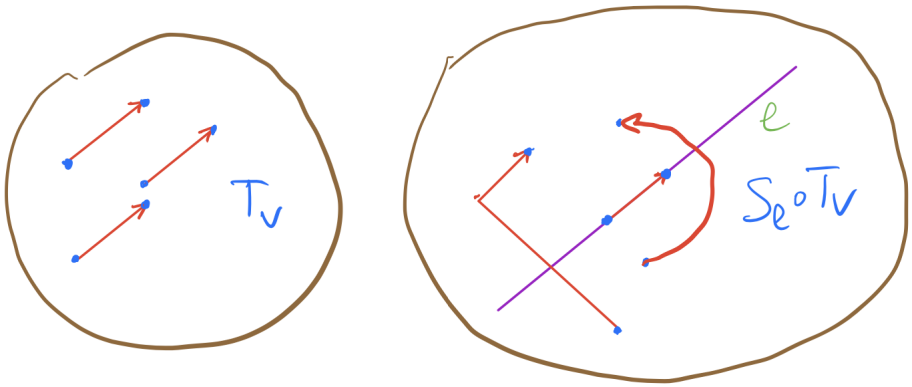
3. Sea $\alpha \in \mathrm{Isom}(\mathbb{R}^2)$. Supongamos que α fija exactamente un punto p. Demuestra que α es un giro con el centro de giro p. (Si γ es el ángulo de giro en dirección contraria a las agujas del reloj, vamos a denotar esta isometría como $R_{p,\gamma}$).



4. Sea $\alpha \in \mathrm{Isom}(\mathbb{R}^2)$. Supongamos que α no fija ningún punto del plano. Demuestra que existe $v = (v_1, v_2) \in \mathbb{R}^2$, tal que pasa uno de los dos siguientes casos

(a) $\alpha = T_v$, donde $T_v((a,b)) = (a+v_1, b+v_2)$ ó

(b) $\alpha = T_v \circ S_l$, donde l es una recta paralela al vector v.



Solución. 1. y 2. Supongamos que una isometría α fija dos puntos distintos $p, q \in \mathbb{R}^2$. Entonces α fija todos los puntos de la recta. l que pasa por p y q. Por lo tanto, α puede ser o la identidad o S_l.

3. Sea q un punto distinto de p. Existe un ángulo γ tal que $R_{\gamma,p}(q)) = \alpha(q)$. Pongamos, $\beta = R_{-\gamma,p} \circ \alpha$. Entonces, $\beta(p) = p$ y $\beta(q) = q$. Sea l la recta que pasa por p y q. Por dos apartados anteriores, se cumple $\beta = \mathrm{Id}_{\mathbb{R}^2}$ o $\beta = S_l$. Si se cumple el primer caso, entonces

$$R_{\gamma,p} = R_{\gamma,p} \circ \beta = R_{\gamma,p} \circ (R_{-\gamma,p} \circ \alpha) = (R_{\gamma,p} \circ R_{-\gamma,p}) \circ \alpha = \mathrm{Id}_{\mathbb{R}^2} \circ \alpha = \alpha.$$

(Es importante notar que aquí hemos usado la propiedad asociativa.)

Nos queda comprobar que el segundo caso $\beta = S_l$ no puede ocurrir. En este caso, $\alpha = R_{\gamma,p} \circ S_l$ y se puede comprobar que α fija todos los puntos de la recta $R_{\frac{\gamma}{2},p}(l)$ que contradice a que α sólo tiene un punto fijo.

4. Sea p un punto de $\mathbb{R}^2$ y v' un vector tal que $T_{v'}(p) = \alpha(p)$. Pongamos $\beta = T_{-v'} \circ \alpha$. Entonces β fija el punto p. Entonces por los apartados anteriores puede pasar tres posibilidades.

(a) $\beta = \mathrm{Id}_{\mathbb{R}^2}$.

(b) $\beta = S_{l'}$, donde l' es una recta que contiene a p.

(c) $\beta = R_{p,\gamma}$ para algún ángulo γ.

En el caso (a), $\alpha = T_v$, donde $v = v'$.

En el caso (b), $\alpha = T_{v'} \circ S_{l'}$. We decompose $v' = v + u$, donde v es paralelo a l' y u es perpendicular a l'. Consideramos la recta $l = \frac{u}{2} + l'$. Vemos que si $x \in l$, entonces $\alpha(x) = x + v \in l$ y para $x \in \mathbb{R}^2$ arbitrario, $\alpha(x) = (T_v \circ S_l)(x)$.

Nos queda comprobar que el caso (c) no puede ocurrir. En este caso $\alpha = T_{v'} \circ R_{p,\gamma}$. Consideramos el triángulo equilátero $\triangle pqr$ tal que $v' = qr$ y $\angle qpr = \gamma$. Ahora vemos que

$$\alpha(q) = (T_{v'} \circ R_{p,\gamma})(q) = T_{v'}(R_{p,\gamma}(q)) = T_{v'}(r) = q.$$

Es decir α fija un punto. Entonces, este caso no es posible. □

Como en el caso de la recta real una composición de dos isometrías de $\mathbb{R}^2$ es también una isometría de $\mathbb{R}^2$. Nuestra clasificación de isometrías implica que todas las isometrías del plano son biyectivas y sus inversas son también isometrías. Como vamos a ver más tarde $(\mathrm{Isom}(\mathbb{R}^2), \circ)$ es otro ejemplo de grupo.

Problema 6. Sea $\alpha \in \mathrm{Isom}(\mathbb{R}^2)$. Prueba las siguientes afirmaciones:

1. Sea l una recta y $l' = \alpha(l)$. Entonces $\alpha \circ S_l \circ \alpha^{-1} = S_{l'}$.
2. Sea p un punto, $p' = \alpha(p)$ y γ un ángulo. Entonces $\alpha \circ R_{p,\gamma} \circ \alpha^{-1} = R_{p',\pm\gamma}$.

Solución. 1. Observa que la isometría $\alpha \circ S_l \circ \alpha^{-1}$ fija la recta l' y no es la identidad.

2. Observa que la isometría $\alpha \circ R_{p,\gamma} \circ \alpha^{-1}$ sólo fija el punto p'. Por lo tanto $\alpha \circ R_{p,\gamma} \circ \alpha^{-1} = R_{p',\gamma'}$ para algún ángulo γ'. Es decir, $\alpha \circ R_{p,\gamma} = R_{p',\gamma'} \circ \alpha$. Como α conserva los ángulos, $\gamma' = \pm\gamma$. □

Si conoces los números complejos $\mathbb{C}$, entonces se puede dar otra descripción al conjunto $\mathrm{Isom}(\mathbb{R}^2)$. Cada elemento $(a, b) \in \mathbb{R}^2$ lo identificamos con el elemento $a + b \cdot i \in \mathbb{C}$. Observa que con esta notación la distancia entre dos puntos $z_1, z_2 \in \mathbb{C}$ es $|z_1 - z_2|$ donde $|z| = \sqrt{z\overline{z}}$ y $\overline{a + bi} = a - bi$.

Problema 7. Demuestra que $\phi : \mathbb{C} \to \mathbb{C}$ es una isometría si y sólo si existen $\alpha, \beta \in \mathbb{C}$ con $|\alpha| = 1$ tales que $\phi(z) = \alpha z + \beta$ ó $\phi(z) = \alpha\overline{z} + \beta$, donde $\overline{z}$ denota la conjugación compleja de $z \in \mathbb{C}$.

Solución. Es una comprobación directa verificar que, con $|\alpha| = 1$ y $\beta \in \mathbb{C}$, las aplicaciones $\phi_{\alpha,\beta}(z) = \alpha z + \beta$ y $\psi_{\alpha,\beta}(z) = \alpha\overline{z} + \beta$ son isometrías.

Damos una idea de cómo ver que cualquier isometría tiene una de estas dos formas. Para esto, podemos usar la clasificación que hemos obtenido. Por ejemplo, si queremos representar S_l, procedemos de la siguiente manera: Observamos que, si l es la recta OX, entonces $S_l(z) = \overline{z}$. Para presentar cualquier S_l, debemos encontrar una $\phi_{\alpha,\beta}$ que lleve la recta OX a l y aplicar el ejercicio anterior:

$$S_l = \phi_{\alpha,\beta} \circ \psi_{1,0} \circ \phi_{\alpha,\beta}^{-1}.$$ □

Grupos de permutaciones

Sea X un conjunto, definamos por Σ_X el conjunto de todas las aplicaciones biyectivas de X en X. Los elementos de Σ_X también se llaman **permutaciones** de X.

Problema 8. 1. Demuestra que si $\alpha, \beta \in \Sigma_X$, entonces $\alpha^{-1} \in \Sigma_X$ y $\alpha \circ \beta \in \Sigma_X$.

2. Cuando $X = \{1, \ldots, n\}$, Σ_X se denota simplemente Σ_n. ¿Cuántos elementos tiene Σ_n?

Solución. 1. Tenemos que demostrar que el inverso de una aplicación biyectiva es biyectivo, y que la composición de dos aplicaciones biyectivas también es biyectiva. Es decir, en ambos casos, debemos verificar que son inyectivas y sobreyectivas.

Por ejemplo, demostremos que α^{-1} es inyectiva. Supongamos que $\alpha^{-1}(x_1) = \alpha^{-1}(x_2)$. Al aplicar α en ambos lados, obtenemos que $x_1 = x_2$.

2. Una permutación de Σ_n manda 1 a cualquier número entre 1 y n, 2 a cualquier número entre 1 y n excepto $\sigma(1)$, 3 a cualquier número entre 1 y n excepto $\sigma(1)$ y $\sigma(2)$, y así sucesivamente. De este modo, hay $n \cdot (n-1) \cdot (n-2) \cdot \ldots = n!$ posibilidades. □

Como veremos más tarde, $(\Sigma_X, \circ)$ es otro ejemplo de grupo. Ahora, vamos a explicar una forma cómoda de trabajar con los elementos de Σ_n.

Problema 9. Sea n un número natural, $\sigma \in \Sigma_n$ y $1 \leq k \leq n$. Escribamos:

$$k, \sigma(k), \sigma^2(k) = \sigma(\sigma(k)), \sigma^3(k), \ldots$$

Como n es finito, en algún momento aparecerá un número que ya está en la sucesión. Demuestra que esta primera repetición es igual a k.

Solución. Supongamos que la primera repetición ocurre cuando $\sigma^i(k) = \sigma^j(k)$, donde $0 \leq i < j$. Si $i \neq 0$, podemos aplicar σ^{-1} a ambos lados y obtener que $\sigma^{i-1}(k) = \sigma^{j-1}(k)$ con $0 \leq i-1 < j-1$. Esto contradice nuestra elección de j. Por lo tanto, $i = 0$. □

Un **ciclo** de una permutación Σ_n es una cadena $(k_1, k_2, \ldots, k_s)$ tal que $k_{i+1} = \sigma(k_i)$ para $i = 1, \ldots, s-1$ y $\sigma(k_s) = k_1$. Llamaremos a s la **longitud** del ciclo $(k_1, k_2, \ldots, k_s)$. Entendemos que los ciclos $(k_1, k_2, \ldots, k_s)$ y $(k_2, \ldots, k_s, k_1)$ son iguales. Entonces está claro que cada elemento de 1 a n pertenece sólo a un ciclo. Para conocer como actúa una permutación es suficiente conocer todos sus ciclos. Por eso a partir de ahora vamos a representar una permutación escribiendo sus ciclos de longitud mayor que 1, entendiendo que si un número k no aparece, la permutación lo fija.

Ejemplo. Consideramos la permutación $\sigma = (214)(79) \in \Sigma_9$ representada como unión de sus ciclos. Esta permutación fija los números 3, 5, 6 y 8, manda 1 a 4, 2 a 1, 4 a 2, 7 a 9 y 9 a 7. Esta claro que podemos representar σ de varias formas como unión de sus ciclos. Por ejemplo, (142)(97) o (97)(214) también representa a σ.

Problema 10. Escribe las permutaciones de Σ_3 como unión de ciclos.

Solución.

$$\mathrm{Id}, (12), (13), (23), (123), (132)$$

□

Problema 11. Sea $\sigma_1 = (23)(78145)$ y $\sigma_2 = (123)(987)$ dos permutaciones en Σ_9. Calcula σ_1^{-1} y $\sigma_1^{-1} \circ \sigma_2$ y representa estas dos permutaciones como unión de ciclos.

Solución. Invertiendo los ciclos en σ_1, obtenemos que $\sigma_1^{-1} = (32)(54187)$.

Para calcular $\sigma_1^{-1} \circ \sigma_2$, primero aplicamos σ_2 y luego σ_1^{-1}. Por ejemplo, σ_2 manda 1 a 2 y luego σ_1^{-1} manda 2 a 3, es decir, $\sigma_1^{-1} \circ \sigma_2(1) = 3$. Siguiendo este proceso, escribimos los ciclos de $\sigma_1^{-1} \circ \sigma_2$:

$$1 \to 3 \to 8 \to 5 \to 4 \to 1, \quad 2 \to 2, \quad 6 \to 6, \quad 7 \to 9 \to 7.$$

Por lo tanto, $\sigma_1^{-1} \circ \sigma_2 = (13854)(79)$. □

Problema 12. Hay 20 tarjetas, cada una con un número del 1 al 20 escrito en cada uno de sus lados. Si consideramos todos los números que aparecen en los dos lados de las 20 tarjetas, cada número del 1 al 20 aparece dos veces. Demuestra que las tarjetas se pueden organizar de manera que todos los números en la parte superior sean diferentes.

Solución. Separaremos las tarjetas en las que está escrito el mismo número dos veces. Tomaremos una de las tarjetas restantes. Supongamos que los números escritos en ella son a y b. Colocaremos la tarjeta con el número a hacia arriba. Luego buscaremos la tarjeta en la que está escrito el segundo número b y la colocaremos con el número b hacia arriba. Continuaremos de esta manera hasta llegar a la tarjeta en la que está escrito el segundo número a. En este punto, el ciclo se detiene. Si aún quedan tarjetas, comenzaremos un nuevo ciclo y así sucesivamente.

□

Problema 13. En una agencia secreta trabajan n agentes: 001, 002, ..., 007, ..., n. Cada agente vigila exactamente un agente. El primer agente vigila a quien vigila al segundo, el segundo vigila a quien vigila al tercero, y así sucesivamente, el n-ésimo vigila a quien vigila al primer agente. Demuestra que n es un número impar.

Solución. Denotemos a los agentes con vértices y tracemos una arista dirigida desde el agente A hasta el agente B en caso de que A vigile a B. Dado que cada agente vigila exactamente un agente, obtendremos algún ciclo (o varios ciclos). Según la condición, si comenzamos a seguir las aristas desde el primer agente y pasamos por dos aristas a la vez, encontraremos consecutivamente a todos los agentes con números 2, 3, ..., n, y al final regresaremos al primer agente (esto significa, en particular, que hay solo un ciclo). Pero en el caso de un número par de agentes, de esta manera solo recorreremos la mitad del ciclo. Así que n es un número impar. □

La definición de grupo

En esta sección vamos a definir el concepto de grupo.

Operación interna

Sea G un conjunto. Denotamos por G^2 el conjunto de todos los pares de elementos de G:

$$G^2 = \{(a, b) \colon a, b \in G\}.$$

Una **operación interna** en G es una aplicación $G^2 \to G$. Es decir, es una regla que a un par $(a, b) \in G^2$ de elementos de G proporciona un elemento de G que en la mayoría de los ejemplos vamos a denotar por $a \cdot b$. Esta notación se llama **multiplicativa**. En vez de $\cdot$ podemos usar otros símbolos: $*$, $+$, $\circ$, etc.

Ejemplo. La composición de aplicaciones es una operación interna en $\mathrm{Isom}(\mathbb{R})$ y $\mathrm{Isom}(\mathbb{R}^2)$.

Problema 14. ¿Cuáles de estas son operaciones internas? Si el conjunto G no está especificado, tendrás que decir cuál es. Si son ambiguas, ten un debate de una duración moderada, en el que el foco debería ser entender qué significa "operación interna".

1. La suma de $\mathbb{R}$.
2. La resta de $\mathbb{R}$.
3. La multiplicación de $\mathbb{R}$.
4. La división de $\mathbb{R}$.
5. Las 4 anteriores, pero en $\mathbb{R} \setminus \{0\}$.
6. Si estás en 2º de bachillerato, la suma y producto de matrices.
7. La suma de vectores.
8. El producto escalar.
9. El producto vectorial de $\mathbb{R}^3$.
10. La reproducción humana.
11. La concatenación de palabras.
12. La mezcla de colores.
13. La composición de aplicaciones.

Solución. La suma, resta y multiplicación en $\mathbb{R}$ son operaciones internas. La división no, porque no se puede dividir por 0, y una operación tiene que estar definida en todo el conjunto. Si quitamos el 0, la multiplicación y división sí son operaciones internas, pero la suma y resta no, porque se pueden salir del conjunto.

La suma de matrices no es una operación interna, sino muchas, una para cada tamaño de matriz: no se pueden sumar matrices de distinto tamaño. El producto es una operación interna para el conjunto de matrices cuadradas de un tamaño fijo.

La suma de vectores (de tamaño fijo) es una operación interna, y lo mismo para el producto vectorial. El producto escalar no lo es, porque no da vectores.

La reproducción humana no es una operación, porque la **inmensa** mayoría de pares ordenados de personas no se reproducen, por lo que la operación no está bien definida.

La concatenación de palabras es una operación si entendemos que "palabra" una sucesión cualquiera de letras. Si tiene que estar en el diccionario, entonces no es una operación, porque *viseracoco* no está en el diccionario.

La mezcla de colores sí es una operación, si es que hay definida una única manera de mezclar dos colores dados (¿a partes iguales?).

La composición de aplicaciones no es una operación, porque hay operaciones que no se pueden componer (por ejemplo, una aplicación $\mathbb{R} \to \mathbb{R}^2$ y otra $\varnothing \to \mathbb{R}^4$). Sí es una operación en el conjunto de aplicaciones de un conjunto fijo en sí mismo. □

La propiedad asociativa

Sea $(G, \cdot)$ un conjunto G con una operación interna $\cdot$. Decimos que $\cdot$ es **asociativa** si para todos $a, b, c \in G$ se cumple que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

La importancia de esta propiedad viene del hecho visto anteriormente de que la composición de aplicaciones es una operación interna asociativa.

Problema 15. Decide si las siguientes operaciones internas son asociativas.

1. $(\mathbb{N}, +)$;
2. $(\mathbb{Z}, +)$;
3. $(\mathbb{Z}, -)$;
4. $(\mathbb{Z}, \cdot)$;
5. $(\mathbb{Q}^*, :)$.

Solución.
1. $(\mathbb{N}, +)$: Sí.
2. $(\mathbb{Z}, +)$: Sí.
3. $(\mathbb{Z}, -)$: No. $(3-2)-1 \neq 3-(2-1)$.
4. $(\mathbb{Z}, \cdot)$: Sí.
5. $(\mathbb{Q}^*, :)$: No. $(3/1)/2 \neq 3/(1/2)$.

□

El elemento neutro

Sea $(G, \cdot)$ un conjunto G con una operación interna $\cdot$. Decimos que $e \in G$ es un elemento neutro con respecto de $\cdot$ si para cualquier $g \in G$, $e \cdot g = g$ y $g \cdot e = g$.

Ejemplo.

1. 0 es neutro en $(\mathbb{Z}, +)$;
2. $(\mathbb{N}, +)$; no tiene un elemento neutro;
3. 1 es neutro en $(\mathbb{Z}, \cdot)$;
4. $(\mathbb{Z}, -)$ no tiene un elemento neutro;
5. $(\mathbb{Q}^*, :)$ no tiene un elemento neutro.
6. la aplicación $\mathrm{Id}_{\mathbb{R}^2}$ es neutro en $\mathrm{Isom}(\mathbb{R}^2)$.

Problema 16. Sea $(G, \cdot)$ un conjunto G con una operación interna $\cdot$. Demuestra que G tiene como mucho un neutro con respecto de $\cdot$.

Solución. Supongamos que existen dos elementos neutros, e_1 y e_2. Consideremos el elemento $e_1 \cdot e_2$. Como e_1 es neutro, se tiene que $e_1 \cdot e_2 = e_2$, y como e_2 es neutro, se cumple que $e_1 \cdot e_2 = e_1$. Por lo tanto, $e_1 = e_2$. □

Por lo tanto a partir de ahora vamos a hablar d**el elemento neutro** (si existe). Cuando la operación interna en G se denota por $\cdot$, $\circ$ o $*$ es habitual denotar el elemento neutro por 1 o e. Cuando la operación se denota por $+$, es habitual denotar el elemento neutro por 0. Vamos. a usar esta notación en adelante.

El inverso de un elemento

Sea $(G, \cdot)$ un conjunto G con una operación interna $\cdot$. Sea $e \in G$ el elemento neutro con respecto de $\cdot$. Si $x \in G$ decimos que $y \in G$ es un inverso de x (con respecto de $\cdot$) si $x \cdot y = e$ y $y \cdot x = e$.

Ejemplo.

1. -2 es el inverso de 2 con respecto de la suma en $\mathbb{Z}$;
2. $\frac{1}{2}$ es el inverso de 2 con respecto de la multiplicación en $\mathbb{Q}^*$.
3. 2 no tiene inverso con respecto de la multiplicación en $\mathbb{N}$.

Problema 17. Calcula los inversos de los siguientes elementos de $\mathrm{Isom}(\mathbb{R}^2)$ con respecto de la composición:

1. S_l, donde l es una recta;
2. $R_{p,\gamma}$, donde p es un punto de $\mathbb{R}^2$ y γ es un ángulo;
3. T_v, donde $v \in \mathbb{R}^2$.

Podemos observar que con los ejemplos anteriores los elementos tienen un único inverso. Como nos demuestra el siguiente ejercicio no es algo casual.

Problema 18. Sea $(G, \cdot)$ un conjunto G con una operación interna $\cdot$. Supongamos que $\cdot$ es asociativa. Entonces cada $x \in G$ puede tener como mucho un inverso.

Solución. Sea $g \in G$ y supongamos que g tiene dos inversos, h_1 y h_2. Consideremos el elemento $t = (h_1 \cdot g) \cdot h_2$. Sea e el elemento neutro. Como h_1 es inverso de g, tenemos que

$$t = (h_1 \cdot g) \cdot h_2 = e \cdot h_2 = h_2.$$

Por la propiedad asociativa, se cumple que $t = h_1 \cdot (g \cdot h_2)$, y como h_2 es inverso de g, obtenemos que

$$t = h_1 \cdot (g \cdot h_2) = h_1 \cdot e = h_1.$$

Por lo tanto, $h_1 = h_2$. Concluimos que el inverso de un elemento en G es único. □

Cuando la operación interna en G se denota por $\cdot$, $\circ$ o $*$ y es asociativa, el único inverso de $x \in G$ (si existe) se denota x^{-1}. Cuando la operación se denota por $+$, el inverso de $g \in G$ normalmente se denota por $-x$.

Problema 19. Sea $(G, \cdot)$ un conjunto G con una operación interna $\cdot$. Supongamos que $\cdot$ es asociativa. Sean $x, y \in G$ y existen $x^{-1} \in G$ e $y^{-1} \in G$. Demuestra que $(x \cdot y)^{-1}$ existe y $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

Solución. Como sólo puede haber un inverso, debemos comprobar que

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = 1 \quad \text{y} \quad (y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = 1.$$

Por ejemplo, comprobemos la primera igualdad. Usando que la operación $\cdot$ es asociativa, obtenemos:

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = ((x \cdot y) \cdot y^{-1}) \cdot x^{-1} = (x \cdot (y \cdot y^{-1})) \cdot x^{-1} = x \cdot x^{-1} = 1.$$

□

Definición de grupo

Por fin hemos llegado al momento cuando podemos definir qué es un grupo. Decimos que $(G, \cdot)$ (un conjunto G con una operación interna $\cdot$) es un **grupo** si

1. la operación $\cdot$ es asociativa:
2. existe el elemento neutro con respecto de $\cdot$.
3. para cada $g \in G$ existe $g^{-1} \in G$.

Ejemplo. Estos son ejemplos de grupos. Comprueba que todas las condiciones de la definición de grupo se cumplen.

1. $(\mathbb{Z}, +)$;
2. $(\mathbb{Q}, +)$;
3. $(\mathbb{Q}^*, \cdot)$;
4. $(\{\pm 1\}, \cdot)$;
5. $(\mathrm{Isom}(\mathbb{R}), \circ)$;
6. $(\mathrm{Isom}(\mathbb{R}^2), \circ)$.
7. $(\Sigma_X, \circ)$
8. $(\mathbb{R}^2, +)$

El siguiente ejercicio nos muestra como a partir de grupos existentes construir grupos nuevos.

Problema 20. Sea $(G, \cdot)$ un grupo y $\emptyset \neq H \subseteq G$ (H un subconjunto no vacío de G). Supongamos que se cumplen dos cosas:

1. Para todos $a, b \in H$, $a \cdot b \in H$.
2. Para cada $h \in H$, $h^{-1} \in H$.

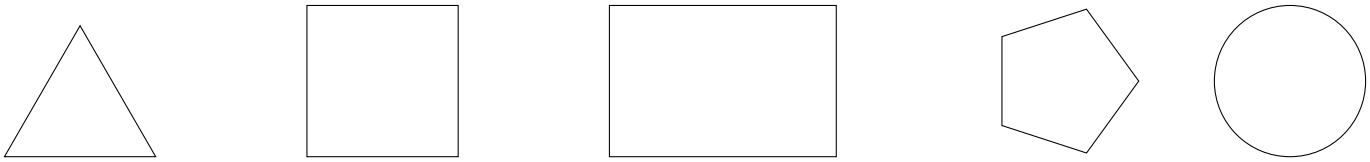
Demuestra que entonces $(H, \cdot)$ es un grupo. (En este caso se dice que H es un **subgrupo** de G).

Problema 21. Sea $(G, \cdot)$ un grupo y $\emptyset \neq H \subseteq G$ (H un subconjunto no vacío de G). Supongamos que para todos $a, b \in H$, $a \cdot b^{-1} \in H$. Demuestra que entonces H es un subgrupo de G.

Problema 22. Encuentra todos los subgrupos de Σ_3.

Más ejemplos de grupos: Grupos de simetría

En esta sección veremos y analizaremos varios ejemplos de subgrupos de $\mathrm{Isom}(\mathbb{R}^2)$. Antes de ver estos ejemplos vamos a intentar contestar la siguiente pregunta informal: ¿Cuáles de estas figuras es la más simétrica?



Claramente podemos tener distintas opiniones al respecto. Intentemos buscar un criterio. Una propuesta lógica puede ser la siguiente: una figura es más simétrica si tiene más simetrías, donde por el conjunto de simetrías de una figura F en $\mathbb{R}^2$ entenderemos el conjunto de isometrías de $\mathbb{R}^2$ que fijan F:

$$\mathrm{Sym}(F) = \{\phi \in \mathrm{Isom}(\mathbb{R}^2) \colon \phi(F) = F\}.$$

Problema 23. 1. Demuestra que $\mathrm{Sym}(F)$ es un subgrupo de $\mathrm{Isom}(\mathbb{R}^2)$.

2. Calcula el grupo $\mathrm{Sym}(F)$ cuando F es una de las figuras anteriores.

Solución. 1. Debemos comprobar que si $\alpha, \beta \in \mathrm{Sym}(F)$, entonces $\alpha^{-1}, \alpha \circ \beta \in \mathrm{Sym}(F)$.

Por ejemplo, veamos que $\alpha^{-1} \in \mathrm{Sym}(F)$. La inversa de una isometría es una isometría. Nos queda ver que $\alpha^{-1}(F) = F$.

Si $p \in F$, existe $q \in F$ tal que $\alpha(q) = p$. Entonces, $\alpha^{-1}(p) = q \in F$. Es decir, $\alpha^{-1}(F) \subseteq F$. Por otro lado, si $p \in F$, entonces $q = \alpha(p) \in F$ y, por lo tanto, $p = \alpha^{-1}(q)$. Es decir, $F \subseteq \alpha^{-1}(F)$. Estas dos implicaciones nos dan que $\alpha^{-1}(F) = F$.

2. Las isometrías que conservan un triángulo regular, un cuadrado o un pentágono regular están consideradas en el siguiente ejercicio. Veamos el caso de un rectángulo con dos lados diferentes y una circunferencia.

Rectángulo. Notemos que, una vez que sabemos la imagen de un vértice, las imágenes de los otros vértices están determinadas. Por lo tanto, como mucho hay 4 isometrías que fijan al rectángulo. Sean l_1 y l_2 las rectas paralelas a los lados y que pasan por la mitad de los lados, y sea O el centro del rectángulo. Entonces, las cuatro isometrías buscadas son $\{\mathrm{Id}_{\mathbb{R}^2}, S_{l_1}, S_{l_2}, R_{O,\pi}\}$.

Observemos que $S_{l_1}^2 = S_{l_2}^2 = R_{O,\pi}^2 = \mathrm{Id}_{\mathbb{R}^2}$ y $R_{O,\pi} = S_{l_1} \circ S_{l_2}$. Este grupo se llama el grupo de **Klein**.

Circunferencia. Supongamos que nuestra circunferencia es la circunferencia $S = \{z \in \mathbb{C} : |z| = 1\}$. Entonces, en la notación del Problema 7, se ve que $\mathrm{Sym}(S) = \{\phi_{\alpha,0}, \psi_{\alpha,0} : |\alpha| = 1\}$, donde las isometrías $\phi_{\alpha,0}$ son rotaciones con centro en 0 y las isometrías $\psi_{\alpha,0}$ son reflexiones respecto de las rectas que pasan por 0. □

Problema 24. Sea P_k un polígono regular de k lados (todos los ángulos son iguales y todos los lados son iguales). Describe $\mathrm{Sym}(P_k)$.

Solución. Observemos primero que, como mucho, puede haber $2k$ isometrías que fijan al polígono. En efecto, sea $\alpha \in \mathrm{Sym}(P_k)$ y A un vértice de P_k. El vértice $\alpha(A)$ puede ser cualquiera de los k vértices. Sea B un vértice vecino de A. Entonces $\alpha(B)$ debe ser un vecino de $\alpha(A)$. Es decir, como mucho, hay 2 posibilidades para $\alpha(B)$.

Notemos que, una vez fijadas las imágenes de A y B, las imágenes de los demás vértices están determinadas de forma única. Por lo tanto, como mucho puede haber $2k$ isometrías.

Ahora vamos a demostrar que existen exactamente $2k$ isometrías que fijan P_k. Sea O el centro del polígono P_k. Entonces tenemos k isometrías de rotación, $R_{O,\frac{2i\pi}{k}}$ con $0 \leq i \leq k-1$ que están en $\mathrm{Sym}(P_k)$.

Además, observemos que P_k tiene k ejes de simetría $l_1, \ldots, l_k$. Las otras k isometrías de P_k son las k reflexiones correspondientes S_{l_i} para $i = 1, \ldots, k$. □

Problema 25. Describe el grupo de simetrías de un cubo. ¿Cuántas de estas simetrías conservan la orientación (es decir, aquellas que se pueden realizar moviendo el cubo con las manos)? ¿Forman estas últimas un subgrupo? ¿Y las que no?

Solución. Sea C un cubo y A uno de sus ocho vértices. Sea $\alpha \in \mathrm{Sym}(C)$. Hay 8 posibilidades para $\alpha(A)$. Entonces, los tres vecinos de A deben ir biyectivamente a los tres vecinos de $\alpha(A)$, lo que proporciona 6 posibilidades. Una vez que tenemos fijadas las imágenes de A y sus vecinos, la isometría del espacio está completamente determinada. Por lo tanto, como mucho puede haber 48 simetrías del cubo. El mismo razonamiento nos da que puede haber como mucho 24 simetrías que se pueden realizar moviendo el cubo con las manos, porque, una vez fijada la imagen de A y de uno de sus vecinos, el resto de las imágenes están determinadas de forma única.

Vamos a ver que el cubo tiene 48 simetrías, de las cuales 24 se pueden realizar moviendo el cubo con las manos. Primero describiremos las 24 que se pueden realizar moviendo el cubo con las manos.

1. La identidad (1 isometría).
2. Para cada par de caras paralelas, tenemos giros de $\frac{\pi}{2}$, π y $\frac{3\pi}{2}$ grados con respecto a la recta perpendicular a estas caras y que pasa por sus centros (9 isometrías).
3. Para cada par de vértices opuestos, tenemos giros de $\frac{2\pi}{3}$ y $\frac{4\pi}{3}$ grados con respecto a la recta que conecta estos vértices (8 isometrías).
4. Hay 6 rectángulos formados por dos lados y dos diagonales de dos caras paralelas. Tenemos los giros de π grados con respecto a la recta perpendicular a cada rectángulo y que pasa por su centro (6 isometrías).

Si O es el centro del cubo, existe la isometría que corresponde a la simetría con respecto a O. La composición de esta isometría con las 24 descritas anteriormente nos da otras 24 simetrías del cubo. No forman un subgrupo, porque no contienen al neutro. □

Problema 26. En la superficie de un cubo están marcados con tiza 100 puntos diferentes. Demuestra que hay dos formas diferentes de colocar el cubo sobre una mesa negra (y exactamente en el mismo lugar) de modo que las marcas de tiza en la mesa sean diferentes en estas formas. (Si se marca un punto en un borde o en un vértice, también deja rastro en la mesa).

Solución. **Pista:** Describir las simetrías del cubo y las órbitas de los puntos del cubo.

Hay 24 simetrías del cubo que conservan la orientación. La orbita del vértice tiene 8 puntos. La orbita de un punto en una arista (que no sea vértice) tiene 12 puntos. La órbita del centro de una cara tiene 6 puntos. Las demás órbitas tienen 24 puntos.

Si todas marcas son iguales, el conjunto de puntos tiene que tener toda la orbita si tiene un punto de ella. Es decir $100 = 8 \cdot a + 12 \cdot b + 24 \cdot c + 6 \cdot d$, donde $a, d \in \{0, 1\}$, porque sólo hay una orbita de vértices y una órbita de centros de las caras. Como 100 y 92 no son divisible por 6, esto no es posible. □

Problema 27. Según Goodyear, "Para garantizar un desgaste uniforme de los neumáticos, es importante rotarlos según las recomendaciones del fabricante del vehículo o a intervalos máximos de 10,000 km.". Recuerda que si se gasta completamente el 10% de la superficie de una rueda, suspendes el 100% la itv.

En los talleres saben que la manera de asegurarse que todas las ruedas pasan por todos los lugares es realizando la misma operación en cada visita. ¿Cuántas maneras hay de intercambiar las 4 ruedas que aseguran que cada 4 visitas cada rueda ha estado en todas las posiciones?

Solución. Si numeramos las ruedas, estamos buscando una permutación, que podemos escribir como un ciclo $(1abc)$, donde $\{a, b, c\} = \{2, 3, 4\}$. Hay 3!, una por cada permutación de 2,3,4.

□

Problema 28. Dicen los magos que 8 mezclas faro perfectas de una baraja la vuelven a colocar como empezó. Una mezcla faro consiste en separar la baraja en dos mitades, e intercalar una carta de cada mitad (la primera y la última no se mueven). ¿Es verdad esto? ¿Con qué barajas funciona?

Solución. Con una baraja española (42 cartas) hay que repetir 12 veces. Con una francesa (52) hay que repetir 8, y con una francesa con comodines (54) hay que repetir 52 veces. □

El signo de una permutación

Hemos visto que existen isometrías del espacio que pueden realizarse con las manos (a estas las llamamos *isometrías que conservan la orientación*) y otras que no lo hacen. Este fenómeno también se observa en dimensiones 1 y 2, y, de hecho, puede generalizarse a dimensiones más altas. Sin embargo, esta generalización requiere el uso de determinantes, razón por la cual no la describiremos aquí.

En esta sección describiremos este fenómeno en el caso de las permutaciones. Definiremos el *signo* de una permutación. Cada permutación en Σ_n se puede interpretar de manera canónica como una isometría: dada una permutación $\sigma \in \Sigma_n$, se puede asociar la isometría $f_\sigma : \mathbb{R}^n \to \mathbb{R}^n$ definida por:

$$f_\sigma(r_1, \ldots, r_n) = (r_{\sigma(1)}, \ldots, r_{\sigma(n)}).$$

Entonces, las permutaciones σ con signo positivo son exactamente aquellas para las que f_σ conserva la orientación.

Para definir el signo de $\sigma \in \Sigma_n$, consideremos la acción de Σ_n sobre los polinomios en $\mathbb{Z}[x_1, \ldots, x_n]$. Dado $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, definimos:

$$(\sigma \cdot p)(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Por ejemplo, si $\sigma = (142)(35)$ y $p = x_1^2 - x_4^3 x_5$, entonces:

$$(\sigma \cdot p) = x_4^2 - x_2^3 x_3.$$

Problema 29. Demuestra que si $\sigma \in \Sigma_n$ y $p_1, p_2 \in \mathbb{Z}[x_1, \ldots, x_n]$, entonces:

$$\sigma \cdot (p_1 + p_2) = \sigma \cdot p_1 + \sigma \cdot p_2, \quad \sigma \cdot (p_1 p_2) = (\sigma \cdot p_1)(\sigma \cdot p_2).$$

Introducimos el siguiente polinomio $\Phi \in \mathbb{Z}[x_1, \ldots, x_n]$:

$$\Phi(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Es decir, Φ es, salvo el signo, el producto de $(x_i - x_j)$ para cada pareja $\{i, j\}$ con $i \neq j$. En total, hay $\binom{n}{2} = \frac{n(n-1)}{2}$ factores.

Problema 30.

1. Demuestra que, para cada $\sigma \in \Sigma_n$, existe $\operatorname{sign}(\sigma) \in \{1, -1\}$ tal que:
$$\sigma \cdot \Phi = \operatorname{sign}(\sigma)\Phi.$$
2. Calcula $\operatorname{sign}(\sigma)$ para:
$$\sigma = (12345), \quad \sigma = (123)(45), \quad \sigma = (34).$$
3. Demuestra que:
$$\operatorname{sign}(\sigma_1 \circ \sigma_2) = \operatorname{sign}(\sigma_1)\operatorname{sign}(\sigma_2),$$
para todas las permutaciones $\sigma_1, \sigma_2 \in \Sigma_n$.
4. Demuestra que:
$$\operatorname{sign}(\sigma) = (-1)^{n-1},$$
si σ es un ciclo de longitud n.

Diremos que una permutación es **par** si su signo es 1 y **impar** si es -1.

Problema 31. Demuestra que en el juego del 15 no se pueden intercambiar la 14 y la 15 sin alterar las demás fichas.

Solución. Basta notar que el intercambio de las fichas 14 y 15, sin alterar las demás, constituye una permutación impar. Sin embargo, todas las permutaciones básicas que podemos realizar en el juego son ciclos de longitud impar y, por lo tanto, su composición resulta en una permutación par. □

Problemas

Problema 32. ¿De cuántas maneras se puede colocar un mismo colchón sobre un somier? Para distribuir el desgaste, hay que rotar los colchones de vez en cuando.

1. Demuestra que no existe una rotación que, aplicada sucesivamente, coloque el colchón en todas las posiciones posibles.
2. Encuentra dos rotaciones a y b tales que, aplicando a, luego b, luego a, etc, se pasa por todas las posiciones posibles.

Solución. Un colchón tiene tres ejes alrededor de los que se puede girar 180 grados: uno vertical (llamémoslo G, o guiñada), y dos horizontales: uno paralelo al durmiente (llamémoslo A, o alabeo), y otro perpendicular al durmiente (llamémoslo C, o cabeceo). Esto da tres rotaciones y, con la identidad, 4 rotaciones. Cada rotación de 180 grados aplicada dos veces da ella misma, y dos rotaciones distintas, compuestas, dan la tercera. Es decir, es el grupo con esta tabla de multiplicar (se llama el grupo de Klein):

$\circ$	Id	G	A	C
Id	Id	G	A	C
G	G	Id	C	A
C	C	A	Id	G
A	A	C	G	Id

Podemos ver que cada una de las tres rotaciones sólo coloca el colchón de dos posibles maneras, con lo que no nos sirve. Sin embargo, si elegimos 2 distintas, por ejemplo, G y A (¡las dos más fáciles de ejecutar!), tenemos

$$\text{Id} \xrightarrow{G\circ} G \xrightarrow{C\circ} A \xrightarrow{G\circ} C \xrightarrow{C\circ} \text{Id}.$$

□

Problema 33. n amigos entran en un bar y cuelgan sus n sombreros. Al abandonar el bar no se recuerdan cuál de los sombreros es de cada uno y cada amigo coge uno al azar. ¿Qué probabilidad hay que ninguno vuelva a casa con su sombrero?

Solución. Se trata de buscar el número D_n de permutaciones de un conjunto de n elementos que no fijan ningún elemento (se llaman **desbarajustes**).

Desbarajustes satisfacen la recurrencia

$$D_n = (n-1)(D_{n-1} + D_{n-2}).$$

De esta recurrencia se obtiene $D_n = nD_{n-1} + (-1)^n$. Por lo tanto, si $p_n = \frac{D_n}{n!}$, obtenemos

$$p_n = p_{n-1} + \frac{(-1)^n}{n!} (n > 1), p_1 = 0.$$

Entonces si $n > 0$,

$$p_n = \sum_{i=0}^{n} \frac{(-1)^i}{i!}.$$

En particular, p_n tiende a $\frac{1}{e}$ cuando n tiende al infinito.

□

Problema 34. Pensamos en una permutación de $\{1, 2, \ldots, n\}$ como una función f, que lleva cada número x a uno distinto $f(x)$. Llamamos $P(n)$ al número de permutaciones de $\{1, 2, \ldots, n\}$ que cumplen que $xf(x)$ es un cuadrado perfecto para todo x. Encuentra el mínimo n tal que $P(n)$ es múltiplo de 2024.

Solución. Cualquier número natural x se puede escribir como $x = ly^2$, donde l no tiene ningún primo repetido en su factorización (es su parte **libre de cuadrados**). Si $xf(x)$ es un cuadrado, signifca que x y $f(x)$ tienen la misma parte libre de cuadrados. Es decir, que los cuadrados se tienen que permutar entre ellos, y lo mismo ocurre con los números de la forma $2y^2, 3y^2, 5y^2, 6y^2, \ldots$ (para todas las posibles partes l, es decir, para todos los números libres de cuadrados). Por ejemplo, una permutación con $n = 20$ tiene que preservar cada uno de estos conjuntos:

$$\{1,4,9,16\},\{2,8,18\},\{3,12\},\{5,20\},\{6\},\{7\},\{10\},\{11\},\{13\},\{14\},\{15\},\{17\},\{19\}.$$

Es decir, consiste en elegir una permutación de cada conjunto: las maneras de elegir una permutación para cada conjunto son el producto de las maneras de elegir cada permutación, es decir,

$$P(20) = 4! \cdot 3! \cdot 2! \cdot 2! \cdot 1! \cdot 1! \cdots = 576.$$

En general, tenemos que contar cuántos elementos hay en cada subconjunto: convéncete de que el número de cuadrados menores que n es $\lfloor \sqrt{n} \rfloor$ (el mayor entero menor o igual que $\sqrt{n}$). El segundo conjunto contiene el doble de los cuadradados: estos son $\left\lfloor \sqrt{\frac{n}{2}} \right\rfloor$. Y así sucesivamente, con lo que en total,

$$P(n) = \lfloor \sqrt{n} \rfloor ! \cdot \left\lfloor \sqrt{\frac{n}{2}} \right\rfloor ! \cdot \left\lfloor \sqrt{\frac{n}{3}} \right\rfloor ! \cdot \left\lfloor \sqrt{\frac{n}{5}} \right\rfloor ! \cdot \left\lfloor \sqrt{\frac{n}{6}} \right\rfloor ! \cdots$$

Como $2024 = 2^3 \cdot 11 \cdot 23$, este número tiene que ser múltiplo de 23, con lo que $\sqrt{n} \geq 23$ (es el factorial más grande que aparece). Si $n = 23^2 = 529$, vemos que $P(n)$ es múltiplo de 23!, que contiene 2^3, 11 y 23 en su factorización, así que $n = 529$.

□

Problema 35. En una cierta ciudad solo se permiten intercambios de apartamentos por pares (si dos propietarios intercambian apartamentos, ese mismo día no pueden participar en otro intercambio). Demuestra que cualquier intercambio complejo de apartamentos (en que participan varios apartamentos) puede realizarse en dos días. (Se supone que en cualquier intercambio cada propietario ocupa un apartamento tanto antes como después del intercambio).

Solución. **Pistas:**

Un intercambio complejo de apartamentos se representa como union de ciclos. Es suficiente considerar un sólo ciclo. Imaginemos este ciclo como una rotación de un polígono regular, cuyas vértices corresponden a los apartamentos involucrados en el intercambio. Esta rotación puede descomponerse en una composición de dos simetrías axiales (respecto a las mediatrices de dos lados consecutivos).

Cada simetría axial define varios intercambios por pares; todos ellos pueden realizarse en un solo día.

Observación: En el lenguaje de permutaciones hemos demostrado que cada permutación $\sigma \in \Sigma_n$ se puede representar como composición $\sigma = \sigma_2 \circ \sigma_1$ con $\sigma_1^2 = \sigma_2^2 = \mathrm{Id}$. □

Problema 36. En el episodio de Futurama "El prisionero de Benda" (no es broma), el profesor Farnsworth inventa una máquina que intercambia los cuerpos de dos personas, pero no funciona dos veces en los cuerpos de las mismas personas. A lo largo del episodio, se suceden muchos intercambios de cuerpos, hasta que en el desenlace dos jugadores de los Harlemn Globetrotters ayudan a los protagonistas a volver a sus respectivos cuerpos.

Demuestra el teorema de Futurama: si un grupo de personas tiene intercambiados los mentes de alguna manera, es posible devolver a cada uno a su cuerpo con la ayuda de dos personas adicionales (que no han usado la máquina).

Solución. Una permutación se puede escribir como un producto de ciclos. Vamos a ver cómo se deshace el ciclo $(123\cdots n)$: Si x e y son los ayudantes, una solución es ésta:

$$P = (1y) \circ (2x) \circ (ny) \cdots (3y)(2y) \circ (1x).$$

Tenemos que $P \circ (123\cdots n) = (xy)$. Entonces, podemos deshacer un ciclo con estas permutaciones entre un personaje de Futurama y un Globetrotter. Hacemos esto con todos los ciclos. Si hay un número par, habremos terminado. Si hay un número impar, al final quedan intercambiados x e y, y sólo tenemos que intercambiarlos.

□

Problema 37. Sea $\sigma : \mathbb{Z} \to \mathbb{Z}$ la permutación de $\mathbb{Z}$ definida mediante $\sigma(z) = z + 2025$. Encuentra para que valores de m naturales existe una aplicación $f : \mathbb{Z} \to \mathbb{Z}$ tal que $\sigma = f^m$.

Solución. Sea $f : \mathbb{Z} \to \mathbb{Z}$ tal que $\sigma = f^m$. Como σ es biyectiva, f debe ser biyectiva. Por lo tanto, f es una permutación de $\mathbb{Z}$. Observemos que

$$f \circ \sigma = f^{m+1} = \sigma \circ f.$$

Por lo tanto,

$$f(n + 2025) = f(n) + 2025.$$

Es decir, si $a \equiv b \pmod{2025}$, entonces $f(a) \equiv f(b) \pmod{2025}$. Por lo tanto, si $\mathbb{Z}_{2025} = \{[1], \ldots, [2025]\}$ denota el conjunto de congruencias módulo 2025, podemos definir $\overline{f} : \mathbb{Z}_{2025} \to \mathbb{Z}_{2025}$ por $\overline{f}([n]) = [f(n)]$. Como f es una permutación de $\mathbb{Z}$, $\overline{f}$ es una permutación de $\mathbb{Z}_{2025}$.

La condición $f^m = \sigma$ implica que $\overline{f}^m = \mathrm{Id}$. En particular, si $([a_1], \ldots, [a_k])$ es un ciclo de $\overline{f}$, entonces k divide a m.

Para cada $1 \leq a \leq 2025$, existen $1 \leq b \leq 2025$ y $t_a \in \mathbb{Z}$ tales que $f(a) = b + 2025t_a$. Entonces, si $([a_1], \ldots, [a_k])$ es un ciclo de $\overline{f}$, tenemos que

$$f^k(a_i) = a_i + 2025 \cdot (t_{a_1} + \ldots + t_{a_k}) \quad \text{y} \quad f^m(a_i) = a_i + 2025 \cdot \frac{m}{k} \cdot (t_{a_1} + \ldots + t_{a_k}).$$

Esto implica que

$$\frac{m}{k} \cdot (t_{a_1} + \ldots + t_{a_k}) \in \mathbb{Z}.$$

Por lo tanto, $m = k$. Concluimos que todos los ciclos de $\overline{f}$ tienen longitud m, y por lo tanto m divide a 2025.

Por otro lado, si m divide a 2025, podemos definir $f(n) = n + \frac{2025}{m}$. En este caso, se verifica que $f^m = \sigma$.

Respuesta: m es un divisor natural de 2025. □

Problemas para hacer en casa

7 de febrero

Problema 38. A un cubo de Rubik se le aplicó una secuencia de giros. Demuestra que, aplicando esta secuencia varias veces, es posible llevar el cubo a su estado inicial.

Solución. **Pistas:** El número de estados del cubo de Rubik es finito; para cada giro existe su inverso.

Denotemos el estado inicial del cubo de Rubik como A. Sea $P = P_1P_2 \ldots P_n$ una secuencia de giros. Denotemos por $P(X)$ el resultado de aplicar la secuencia de giros P al estado X, y por $P^m(X)$ el resultado de aplicar m veces la secuencia de giros P al estado X. Consideremos la secuencia de estados $A, P(A), P^2(A), P^3(A), \ldots$.

Dado que el número de estados del cubo de Rubik es finito, en esta secuencia habrá una repetición, es decir, $P^k(A) = P^n(A) = B$ para algunos k, n con $k < n$. Para cada giro P_i del cubo, existe un giro inverso P_i^{-1} (es decir, un giro tal que $P_i^{-1}(P_i) = P_i(P_i^{-1})$ es la transformación identidad).

De este modo, para la secuencia de giros $P = P_1P_2 \ldots P_n$, existe una transformación inversa P^{-1}, que se define como la ejecución secuencial de los giros $P_n^{-1}, P_{n-1}^{-1}, \ldots, P_1^{-1}$. Aplicando la transformación P^{-1} al estado $B = P^k(A) = P^n(A)$, obtenemos que $P^{-1}(B) = P^{k-1}(A) = P^{n-1}(A)$. Continuando este razonamiento de forma similar, encontramos que los estados coinciden de la siguiente manera: $P^{k-2}(A) = P^{n-2}(A), \ldots, P^1(A) = P^{n-k+1}(A)$.

Por lo tanto, el estado inicial se repetirá después de $(n-k+1)$ ejecuciones de la secuencia de giros P. □

Problema 39. En este ejercicio te proponemos clasificar algunas subfamilias de isometrías de $\mathbb{R}^3$.

1. Sea l una recta en $\mathbb{R}^3$. Describe todas las isometrías de $\mathbb{R}^3$ que fijan la recta l. (¡Ojo! Fijar una recta no es lo mismo que fijar todos los puntos de esta recta).

2. (*) Describe todas las isometrías de $\mathbb{R}^3$ que fijan un punto $p \in \mathbb{R}^3$.

3. (*) Describe todas las isometrías de $\mathbb{R}^3$.

Solución. 1. Sea α una isometría del espacio que fija la recta l. Entonces, la restricción de α sobre l es una isometría de l. Por la clasificación de las isometrías de una recta, pueden ocurrir dos casos:

(a) Existe un vector v paralelo a l tal que la restricción de α sobre l consiste en sumar a cada punto el vector v. Sea T_v la isometría del espacio que consiste en sumar a cada punto el vector v. Consideremos $\beta = T_{-v} \circ \alpha$. Entonces, β fija todos los puntos de l y fija todos los planos perpendiculares a l.

(b) Existe un punto p de la recta l tal que la restricción de α sobre l es la reflexión respecto a este punto. En este caso, α fija el plano perpendicular a l que pasa por este punto.

Ahora podemos describir todas las isometrías de $\mathbb{R}^3$ que fijan la recta l.

Consideremos una isometría γ de $\mathbb{R}^2$ que fija el punto $(0,0)$. Sea π un plano perpendicular a l. Identificamos π con $\mathbb{R}^2$ de tal forma que la intersección de π con l se identifica con $(0,0)$ y pensamos que γ actúa sobre π. Sea v un vector paralelo a l. Dado un punto $x \in \mathbb{R}^3$, existen un punto único $p \in \pi$ y un escalar $r \in \mathbb{R}$ tales que $x = p + rv$.

(a) Sea $t \in \mathbb{R}$. Definimos
$$\phi_{\gamma,v,t}(x) = \gamma(p) + (r+t)v.$$

(b) Definimos
$$\psi_{\pi,\gamma}(x) = \gamma(p) - rv.$$

2. Usando matemáticas más avanzadas, se puede probar que una isometría del espacio que fija un punto también fija una recta que pasa por este punto. Por lo tanto, podemos usar el apartado anterior. En este caso,
$$\alpha = \phi_{\gamma,v,0} \quad \text{o} \quad \alpha = \psi_{\pi,\gamma}.$$

3. Para cada isometría α del espacio, podemos encontrar un vector u tal que $\beta = T_{-u} \circ \alpha$ fija el punto $(0,0,0)$. Por lo tanto,
$$\alpha = T_u \circ \beta,$$
y las posibilidades para β están descritas en el apartado anterior. □

Problema 40. Sea $\pi : \{1,\dots,n\} \to \{1,\dots,n\}$ una permutación. Un **ciclo** de π es una lista $(a_1,\dots,a_k)$ con entradas de $\{1,\dots,n\}$ tal que $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, …, $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$. El número k es la **longitud** del ciclo.

1. ¿Cuantas permutaciones de $\{1,\dots,n\}$ tienen un ciclo de longitud n?

2. Sea $l > 50$. Calcula el número de permutaciones de un conjunto de 100 elementos que tienen un ciclo de longitud l.

3. El director de una prisión ofrece una última oportunidad a 100 condenados a muerte, que están numerados del 1 al 100. Una habitación contiene un armario con 100 cajones. El director pone al azar el número de un preso en cada cajón cerrado. Los prisioneros entran en la habitación, uno tras otro. Cada preso puede abrir y mirar en 50 cajones en cualquier orden. Los cajones se cierran de nuevo después. Si, durante esta búsqueda, cada preso encuentra su número en uno de los cajones, todos los presos son indultados. Si un solo preso no encuentra su número, todos los presos mueren. Antes de que el primer preso entre en la habitación, los presos pueden discutir la estrategia (los presos también tienen acceso a la habitación con los cajones), pero no pueden comunicarse una vez que el primer preso entra para mirar en los cajones. Encuentra una estrategia para los presos con la cual tengan por lo menos 30% de probabilidad de salir de la prisión.

.

Solución. 1. Cada permutación así se puede representar de forma única como un ciclo

$$1 \to a_2 \to a_3 \to \ldots \to a_{n-1} \to a_n \to 1,$$

donde $\{a_2, \ldots, a_n\} = \{2, \ldots, n\}$. Entonces hay $(n-1)!$ permutaciones de este tipo.

2. Una permutación de los números del 1 al 100 puede contener como máximo un ciclo de longitud $l > 50$. Hay exactamente $\binom{100}{l}$ formas de seleccionar los números de dicho ciclo. Por el apartado anterior, dentro de este ciclo, estos números se pueden ordenar en $(l-1)!$ permutaciones. Para los números restantes hay $(100-l)!$ posibles permutaciones. Por tanto, el número de permutaciones de los números del 1 al 100 con un ciclo de longitud $l > 50$ es igual a

$$\binom{100}{l} \cdot (l-1)! \cdot (100-l)! = \frac{100!}{l}.$$

3. Para describir la estrategia, no sólo los presos, sino también los cajones, se numeran del 1 al 100; por ejemplo, fila por fila comenzando con el cajón superior izquierdo. La estrategia ahora es la siguiente:

1. Cada preso primero abre el cajón etiquetado con su propio número.
2. Si este cajón contiene su número, termina porque ha encontrado su número.
3. De lo contrario, el cajón contiene el número de otro preso, y luego abren el cajón etiquetado con este número.
4. El preso repite los pasos 2 y 3 hasta encontrar su propio número, o falla porque el número no se encuentra en los primeros cincuenta cajones abiertos.

La distribución de los números en los cajones lo vemos como una permutación π de $\{1, \ldots .100\}$. Al comenzar con su propio número, el prisionero garantiza que está en el ciclo de π que contienen su número. Encontrará su número si y sólo si la longitud de este ciclo es ≤ 50. Por lo tanto, los prisioneros saldrán de la cárcel si la π no tiene ciclos longitud > 50. Por el apartado anterior la probabilidad de este suceso es

$$\frac{1}{100!}(100! - \sum_{l=51}^{100} \frac{100!}{l}) = 1 - \sum_{l=51}^{100} \frac{1}{l} > 0.3.$$

□

14 de febrero

Problema 41. Un texto ha sido cifrado asignando a cada letra otra letra (posiblemente la misma), de tal manera que el texto puede ser descifrado de manera inequívoca. Demuestra que existe un número N tal que después de aplicar el cifrado N veces, se obtenga el texto original. Encuentra el menor valor de N que sea válido para todos los cifrados (suponiendo que el alfabeto tiene 27 letras).

Solución. **Pistas:** Si la letra a_1 se cifra como la letra a_2, la letra a_2 se cifra como la letra a_3, ..., y la letra a_k se cifra como a_1, entonces, después de aplicar el cifrado k veces, se obtiene el texto original.

Según la condición, el cifrado permite un descifrado inequívoco. Esto significa que el cifrado es simplemente una permutación de las 27 letras del alfabeto (es decir, cada letra se cifra en otra letra). Supongamos que la letra a_1 se cifra como a_2, la letra a_2 como a_3, y así sucesivamente, de manera que a_k se cifra como a_{k+1}, ... En la secuencia de letras $a_1, a_2, \ldots$, en algún momento aparecerá la primera repetición, es decir, a_{k+1} coincidirá con alguna de las letras $a_1, a_2, \ldots, a_k$, y las letras $a_1, a_2, \ldots, a_k$ serán todas distintas. Sin embargo, a_{k+1} no puede coincidir con ninguna de las letras $a_2, \ldots, a_k$, ya que estas se cifran como $a_1, a_2, \ldots, a_{k-1}$ respectivamente, mientras que a_{k+1} se cifra como a_k. Por lo tanto, $a_{k+1} = a_1$.

Así, tenemos el siguiente ciclo: a_1 se cifra como a_2, a_2 se cifra como a_3, ..., a_k se cifra como a_1. Después de k aplicaciones del cifrado, las letras $a_1, a_2, \ldots, a_k$ estarán en las mismas posiciones que en el

texto original. De esta manera, toda la permutación de letras se descompone en ciclos. La longitud de un ciclo puede variar de 1 a 27. Si tomamos un N divisible por cada uno de los números $1, 2, \ldots, 27$ y aplicamos el cifrado N veces, las letras de cada ciclo estarán en sus posiciones originales, es decir, obtendremos el texto original. Por el contrario, si N no es divisible por uno de los números k de 1 a 27, entonces, si el cifrado contiene un ciclo de longitud k, después de aplicar el cifrado N veces, no se obtendrá el texto original.

Por lo tanto, el número buscado N es el mínimo común múltiplo de los números $1, 2, \ldots, 27$. Este número es muy grande, igual a

$$16 \cdot 27 \cdot 25 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 80313433200. \quad \square$$

Problema 42. En un cierto conjunto no vacío A se ha definido una operación $*$, que para cada par de elementos a y b de A calcula algún elemento $a * b$ de A. Se sabe que:

(1) Para cualesquiera tres elementos a, b y c, se cumple:

$$a * (b * c) = b * (c * a).$$

(2) Si $a * b = a * c$, entonces $b = c$.

Demuestra que la operación $*$

(a) es conmutativa, es decir, para cualesquiera elementos a y b se cumple $a * b = b * a$;

(b) es asociativa, es decir, para cualesquiera elementos a, b y c se cumple $(a * b) * c = a * (b * c)$.

Solución. **Pistas:**

De las condiciones (1) y (2) se deduce la conmutatividad: al sustituir en (1) a en lugar de b, obtenemos que para cualesquiera a y c:

$$a * (a * c) = a * (c * a),$$

y de acuerdo con (2), se sigue que $a * c = c * a$.

De la condición (1) y la conmutatividad se deduce la asociatividad: para cualesquiera a, b y c, de acuerdo con (1), se cumple:

$$a * (b * c) = b * (c * a) = c * (a * b),$$

y, utilizando la conmutatividad, obtenemos:

$$a * (b * c) = c * (a * b) = (a * b) * c. \quad \square$$

Problema 43. Describe el grupo de simetrías de un tetraedro regular. ¿Cuántas de estas simetrías conservan la orientación (es decir, aquellas que se pueden realizar moviendo el tetraedro con las manos)? ¿Forman estas últimas un subgrupo?

Solución. Conocemos una isometría del tetraedro al saber cómo actúa sobre sus vértices. Por lo tanto, hay como mucho 4!=24 isometrías. Estas isometrías se pueden obtener a partir de las isometrías del cubo (Problema 26).

Sea C el cubo en $\mathbb{R}^3$ con vértices en el conjunto $\{(a, b, c) \mid a, b, c \in \{0, 1\}\}$. Consideremos el tetraedro regular con vértices en

$$(0, 0, 0), \quad (1, 1, 0), \quad (0, 1, 1), \quad (1, 0, 1).$$

Exactamente 24 isometrías del cubo fijan este tetraedro. De estas, 12 se pueden realizar moviendo el tetraedro con las manos. Estas 12 isometrías forman un subgrupo. $\square$