Pequeño Instituto de Matemáticas
2024-2025

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

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

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

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 $a \in A$,

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

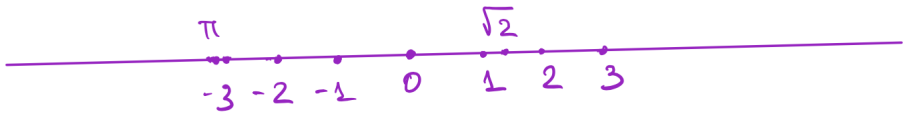
Es decir, $\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha$. Es la propiedad **asociativa** que va a jugar un papel importante.

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 $\mathbb{R}$:

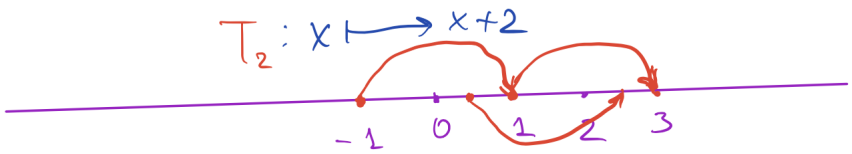
$$\text{para todos } a, b \in \mathbb{R} \text{ se cumple que } d(\phi(a), \phi(b)) = d(a, b).$$

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

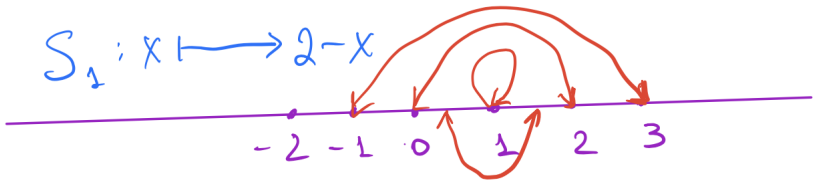
$$\mathrm{Isom}(\mathbb{R}) = \{\phi : \mathbb{R} \to \mathbb{R} \colon |\phi(a) - \phi(b)| = |a - b|, \forall a, b \in \mathbb{R}\}. \tag{1}$$

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



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



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

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

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

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

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

Problema 4. 1. Usando la definición de $\text{Isom}(\mathbb{R})$, 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

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

$(\text{Isom}(\mathbb{R}), \circ)$ 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 $\{(x, y) : x, y \in \mathbb{R}\}$ de pares de elementos de $\mathbb{R}$. La distancia entre dos puntos de $\mathbb{R}^2$ está dada por la fórmula

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

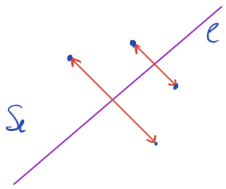
Una **isometría** de $\mathbb{R}^2$ es una aplicación $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ que conserva la distancia:

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

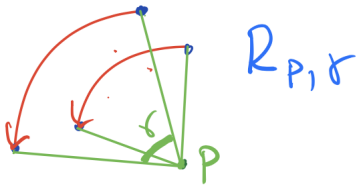
El conjunto de todas las isometrías de $\mathbb{R}^2$ lo denotaremos por $\mathrm{Isom}(\mathbb{R}^2)$. En el siguiente ejercicio vamos a describir todas las isometrías del plano.

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).



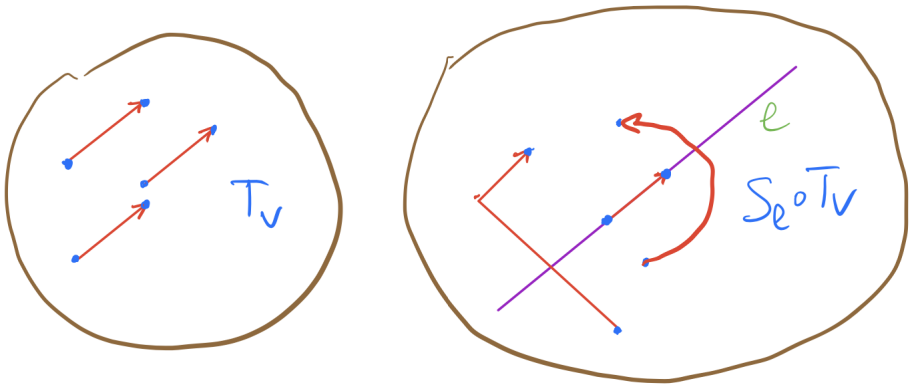
3. Sea $\alpha \in \mathrm{Isom}(\mathbb{R}^2)$. Supongamos que α fija exactamente un punto p. Demuestra que α es un giro con el centro de giro p. (Si γ es el ángulo de giro en dirección contraria a las agujas del reloj, vamos a denotar esta isometría como $R_{p,\gamma}$).



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.



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 $\alpha \circ R_{p,\gamma} \circ \alpha^{-1} = R_{p',\pm\gamma}$.

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 $z \in \mathbb{C}$.

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?

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.

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.

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.

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.

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.

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.

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. $(\mathbb{Q}^*, :)$.

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 $\cdot$.

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.

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

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 $h \in H$, $h^{-1} \in H$.

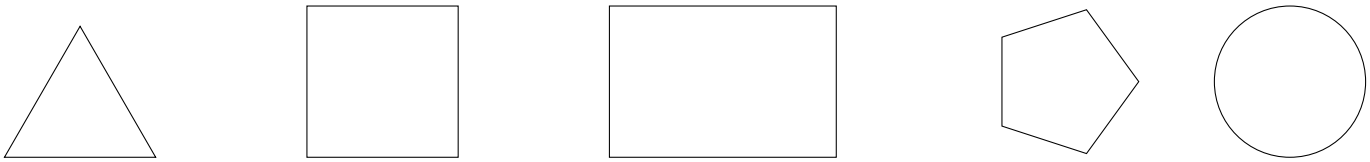
Demuestra que entonces $(H, \cdot)$ es un grupo. (En este caso se dice que H es un **subgrupo** de G).

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.

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

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?

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).

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?

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?

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 $\Phi \in \mathbb{Z}[x_1, \ldots, x_n]$:

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

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 $\text{sign}(\sigma) \in \{1, -1\}$ tal que:
$$\sigma \cdot \Phi = \text{sign}(\sigma)\Phi.$$
2. Calcula $\text{sign}(\sigma)$ para:
$$\sigma = (12345), \quad \sigma = (123)(45), \quad \sigma = (34).$$
3. Demuestra que:
$$\text{sign}(\sigma_1 \circ \sigma_2) = \text{sign}(\sigma_1)\,\text{sign}(\sigma_2),$$
para todas las permutaciones $\sigma_1, \sigma_2 \in \Sigma_n$.
4. Demuestra que:
$$\text{sign}(\sigma) = (-1)^{n-1},$$
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.

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.

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?

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.

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).

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).

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 $\sigma = f^m$.

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.

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 $\mathbb{R}^3$.

Problema 40. Sea $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ una permutación. Un **ciclo** de π es una lista $(a_1, \ldots, a_k)$ con entradas de $\{1, \ldots, n\}$ 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 $\{1, \ldots, n\}$ 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.

.

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).

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

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?