Grupos

Este segundo cuatrimestre lo dedicaremos al estudio de estructuras algebraicas. Primero, las estructuras de grupo, anillo y cuerpo, y más adelante, la estructura de espacio vectorial y todo lo que se refiere al Álgebra lineal.

Empezamos con la estructura de grupo. Es la más sencilla, porque solo interviene una operación, aunque tiene gran importancia.

Definición

Decimos que un conjunto G, con una operación binaria $\star$, tiene estructura de *grupo* si se cumplen estas propiedades:

(g1) La operación $\star$ es una *ley de composición interna*, o tiene la propiedad de *clausura*:

$$a, b \in G \Rightarrow a \star b \in G$$

(g2) La operación $\star$ es *asociativa*:

$$a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c \in G$$

(g3) La operación $\star$ tiene *elemento neutro*. Es un elemento $e \in G$ tal que:

$$a \star e = e \star a = e \quad \forall a \in G$$

(g4) Todo elemento de G tiene *elemento simétrico* para la operación $\star$:

$$\forall a \in G \quad \exists a' \in G \text{ tal que } a \star a' = a' \star a = e$$

Así pues, un grupo es un conjunto con una operación, $(G, \star)$, que satisface las propiedades (g1), (g2), (g3) y (g4). Se tendría que decir que la operación $\star$ da al conjunto G una estructura de grupo, o que G tiene estructura de grupo con la operación $\star$. Pero diremos simplemente que G es un grupo, porque el contexto suele dejar clara la operación que se está considerando.

Si G tiene infinitos elementos, decimos que es un *grupo infinito*. Si G tiene n elementos, decimos que es un grupo de *orden* n.

Puede haber una quinta propiedad:

(g5) La operación $\star$ es *conmutativa*:

$$a \star b = b \star a \quad \forall a, b \in G$$

En este caso, decimos que G es un *grupo conmutativo* o *abeliano*.

Ejemplos

Grupos infinitos, con la operación suma

- Los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son grupos infinitos conmutativos con la operación suma. El elemento neutro es 0 y el simétrico de un elemento a es el opuesto, $-a$.
- En cambio, $\mathbb{N}$ no lo es, porque no cumple la propiedad (g4) (si consideramos que $0 \in \mathbb{N}$, se cumple (g3); si $0 \notin \mathbb{N}$ no se cumple).

Grupos infinitos, con la operación producto

En los conjuntos del ejemplo anterior tenemos que quitar el 0 porque este elemento no tiene simétrico (o inverso) para el producto.

- Los conjuntos $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$ son grupos conmutativos. El elemento neutro es 1 y el simétrico de a es $1/a$.
- En cambio, los conjuntos $\mathbb{N}$ y $\mathbb{Z} - \{0\}$ no lo son porque falla la propiedad (g4).

Con el resto de las operaciones habituales estos conjuntos no tienen estructura de grupo.

Ejercicio 1. *Determina cuáles de las cinco propiedades tienen las operaciones* diferencia *y* división *en los conjuntos* $\mathbb{N}$*,* $\mathbb{Z}$ *y* $\mathbb{R}$*, y cuáles no.*

Grupos finitos de la aritmética modular

- Los conjuntos $\mathbb{Z}_m$, con la operación suma, son grupos conmutativos de orden m, cualquiera que sea m. Vimos que la suma es una ley de composición interna, que es conmutativa y asociativa, que 0 es elemento neutro y que cada elemento a tiene simétrico, que es $-a = m - a$.

  Ejemplo 2. *Tomando el conjunto* $\mathbb{Z}_4 = \{0, 1, 2, 3\}$*, la tabla de la suma sería:*

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

  Ejercicio 3. *Haz la tabla de los grupos* Z_3 *y* Z_5*, con la operación suma.*

- Con el producto, en cambio, no todos los elementos de $\mathbb{Z}_m$ tienen simétrico, o inverso. Si nos quedamos con el conjunto de elementos invertibles, que denotaremos por $U(\mathbb{Z}_m)$, podemos comprobar que, con la operación producto, este conjunto tiene estructura de grupo conmutativo, y su orden es $\phi(m)$.

  Si p es primo, $U(\mathbb{Z}_p) = \mathbb{Z}_p - \{0\}$, que es un grupo de orden $p - 1$.

  Ejemplo 4. *Por ejemplo, si* $m = 9$*, hay* $\phi(9) = 6$ *elementos invertibles en* $\mathbb{Z}_9$*. El conjunto que forman,* $U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$*, es un grupo conmutativo de orden* 6*. La tabla del producto es:*

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

  Ejercicio 5. *Haz la tabla de los grupos* $U(\mathbb{Z}_7)$*,* $U(\mathbb{Z}_8)$ *y* $U(\mathbb{Z}_{10})$*, con la operación producto.*

Grupos de Matrices

- Consideramos un conjunto de números C, que con la suma tenga estructura de grupo ($\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z}_m$, ...). El conjunto de matrices de m filas y n columnas con coeficientes en C, que denotaremos por $\mathcal{M}_{m\times n}(C)$, con la suma habitual de matrices, es un grupo conmutativo, que será finito o infinito según lo sea C. Si C tiene k elementos, el orden de $\mathcal{M}_{m\times n}(C)$ es k^{mn}.

  Ejemplo 6. *El conjunto de matrices $\mathcal{M}_{2\times 3}(\mathbb{Z}_3)$ tiene $3^{2\cdot 3} = 729$ elementos. Con la suma tiene estructura de grupo conmutativo y su orden es 729. El elemento neutro es la matriz nula $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ y, por ejemplo, la matriz simétrica de $\begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \end{pmatrix}$ es la matriz $\begin{pmatrix} 2 & 1 & 2 \\ 0 & 1 & 1 \end{pmatrix}$.*

- Partimos ahora de un conjunto de números C que sea grupo con la suma y, quitando el 0, con el producto ($\mathbb{R}$, $\mathbb{Z}_p$ con p primo,...). El conjunto $U(\mathcal{M}_n(C))$ formado por las matrices cuadradas invertibles (las que tiene determinante no nulo) de dimensión n, con coeficientes en C, tiene estructura de grupo con el producto habitual de matrices. Es un grupo no conmutativo.

  Ejercicio 7. *Enumera las seis matrices invertibles de $U(\mathcal{M}_2(\mathbb{Z}_2))$. Halla la matriz inversa de cada una de ellas.*

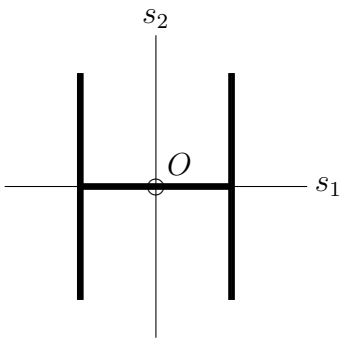
  Ejercicio 8. *Sea G_M el conjunto de matrices cuadradas de dimensión 2 que tienen la forma $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$, donde α y β son elementos de $\mathbb{Z}_3$ y $\alpha \neq 0$. Demuestra que G_M tiene estructura de grupo, con el producto de matrices.*

  Enumera sus elementos y halla los inversos.

Grupo de simetrías de una figura plana

Consideramos una figura plana $\mathcal{F}$. Los movimientos que la dejan fija, que pueden ser giros y simetrías, forman un conjunto que es fácil comprobar que tiene estructura de grupo con la composición de movimientos. El elemento neutro de este grupo, que podemos denotar por $G_{\mathcal{F}}$, es la identidad (o el giro de 0°, g_{0°); el elemento simétrico de una simetría es ella misma, y el de un giro g_α es $g_{360^\circ-\alpha}$.

Ejemplo 9. *El grupo de simetrías de la letra H está formada por dos simetrías, s_1 y s_2, y dos giros respecto del centro O, g_{0° y g_{180°.*



Así pues, el grupo es $G_H = \{g_{0^\circ}, g_{180^\circ}, s_1, s_2\}$; la tabla de la operación es:

	g_{0°	g_{180°	s_1	s_2
g_{0°	g_{0°	g_{180°	s_1	s_2
g_{180°	g_{180°	g_{0°	s_2	s_1
s_1	s_1	s_2	g_{0°	g_{180°
s_2	s_2	s_1	g_{180°	g_{0°

El grupo de simetrías de un polígono regular de n lados está formado por n giros y n simetrías, con lo que es un grupo de orden $2n$.

Ejercicio 10. *Enumera los seis elementos del grupo $G_\triangle$ de simetrías de un triángulo equilátero (tres giros y tres simetrías) y haz la tabla de la operación. Enumera los ocho elementos del grupo $G_\square$.*

Grupo de las aplicaciones biyectivas

Consideramos ahora un conjunto cualquiera X, y el conjunto $\mathcal{F}$ de las aplicaciones biyectivas de X en sí mismo. El conjunto $\mathcal{F}$, con la composición de aplicaciones $\circ$, tiene estructura de grupo no conmutativo.

(g1) La operación $\circ$ es una ley de composición interna, porque la composición de dos aplicaciones biyectivas es otra aplicación biyectiva.

(g2) La composición de aplicaciones es siempre asociativa.

(g3) El elemento neutro de la composición de aplicaciones es la aplicación identidad Id, que pertenece a $\mathcal{F}$: $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$.

(g4) El elemento simétrico de una aplicación biyectiva $f \in \mathcal{F}$ es, en este caso, la aplicación inversa f^{-1}, que sabemos que existe y que también es biyectiva. Se cumple $f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}$.

El conjunto $\mathcal{F}$, con la composición, es, por tanto un grupo. En general no es conmutativo, porque no lo es la composición (solo lo es si X tiene uno o dos elementos). Es un grupo finito o infinito, según lo sea X.

El caso que más nos interesa, que es cuando X es finito, lo veremos en la última sección de este tema.

Propiedades de los grupos

Emplearemos una notación multiplicativa. Pondremos xy para denotar $x \star y$. El inverso de un elemento será x^{-1} y el neutro, 1.

Estas son algunas de las propiedades que tienen los grupos:

- El neutro es único. El inverso de cada elemento también es único.
- El inverso del inverso de un elemento es el propio elemento: $(x^{-1})^{-1} = x$.
- El inverso de un producto es el producto de los inversos, pero cambiado de orden: $(xy)^{-1} = y^{-1}x^{-1}$.
- En un grupo siempre se puede simplificar:

  $xy = xz \Rightarrow y = z$ (simplificación por la izquierda)

  $yx = zx \Rightarrow y = z$ (simplificación por la derecha)

- En un grupo la ecuación $ax = b$ siempre tiene solución, que es única: $x = a^{-1}b$. Análogamente, $x = ba^{-1}$ es la única solución de $xa = b$.
- La tabla de la operación de un grupo es un *cuadrado latino*, es decir, en cada fila y en cada columna están todos los elementos del grupo, sin repetir.

  Obviamente, no todos los cuadrados latinos corresponden a la tabla de la operación de un grupo.

Ejemplo 11. *Con la última propiedad vamos a ver que, en esencia, solo hay un grupo de orden 3. Tomamos un conjunto G de tres elementos: el neutro, 1, y otros dos que llamaremos b y c. En la tabla de la operación la fila y la columna del neutro son obligadas:*

	1	a	b
1	1	a	b
a	a		
b	b		

Pero en los cuatro sitios que quedan los elementos que tenemos que poner están también determinados porque la tabla tiene que ser un cuadrado latino:

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

Ejercicio 12. *Demuestra que solo hay dos grupos de orden 4 esencialmente diferentes.*

Ejercicio 13. *Demuestra las propiedades de los grupos que hemos visto en esta sección.*

El orden de los elementos de un grupo

Consideramos las potencias de un elemento $x \in G$: $x^1 = x$, $x^2 = xx$, $x^3 = xxx$, ... Si todas estas potencias son diferentes, decimos que x tiene *orden infinito*.

Vamos a ver el caso en que se repitan algunas de estas potencias (cosa que pasa necesariamente si G es de orden finito). Suponemos $x^a = x^b$, con $a > b$. Entonces, $x^{a-b} = 1$, es decir, hay alguna potencia de x que da como resultado el elemento neutro. Decimos que el *orden* de x es el menor entero positivo k que verifica $x^k = 1$.

Ejemplo 14. *En el grupo $G_H = \{g_{0^\circ}, g_{180^\circ}, s_1, s_2\}$ del ejemplo 9 el orden del neutro es 1, mientras que los otros tres elementos tienen orden 2, porque $g_{180^\circ}^2 = s_1^2 = s_2^2 = g_{0^\circ}$.*

Ejemplo 15. *En el grupo $U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$, con el producto, el neutro tiene orden 1 y el elemento 9 tiene orden 2 porque $9^2 = 1$. Los otros dos elementos tienen orden 4 porque hasta la potencia cuarta no obtenemos la unidad: $3^2 = 9$, $3^3 = 7$ y $3^4 = 1$; $7^2 = 9$, $7^3 = 3$ y $7^4 = 1$.*

Ejercicio 16. *Determina el orden de los elementos de los grupos $\mathbb{Z}_8$ (con la suma) y $U(\mathbb{Z}_9)$ (con el producto).*

El orden del elemento neutro de un grupo es siempre 1 (de hecho, es el único elemento de orden 1). Del orden de los demás elementos podemos decir lo que afirma el siguiente resultado.

Teorema 17. *El orden de un elemento de un grupo es un divisor del orden del grupo.*

Este teorema afirma que dado un grupo de orden n, el orden de los elementos tiene que ser obligatoriamente un divisor de n, pero esto no quiere decir que, dado un divisor k de n, exista algún elemento de orden k. El grupo de orden 4 del ejemplo 14 hemos visto que tiene elementos de orden 1 y 2, pero no de orden 4. En cambio, en el ejemplo 15, el grupo, que es de orden 4, tiene elementos de orden 1, 2 y 4.

Ejemplo 18. *En el grupo $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ con la suma, que tiene orden 5, los posibles órdenes de los elementos son 1 y 5. Sin hacer ningún cálculo, podemos afirmar que el elemento neutro 0 tiene orden 1 y todos los demás tienen orden 5.*

Isomorfismo de grupos

Dos grupos, G_1, con la operación $\star$, y G_2, con la operación $\triangledown$, decimos que son *isomorfos* si existe una biyección $f : G_1 \to G_2$ compatible con las operaciones, es decir,

$$f(g \star g') = f(g) \triangledown f(g'),\ \forall g, g' \in G_1$$

A esta aplicación la llamaremos *isomorfismo*. Pondremos $G_1 \approx G_2$ para denotar que tal aplicación existe y que los grupos son isomorfos.

Que dos grupos sean isomorfos quiere decir que, en esencia, si abstraemos la notación de sus elementos y la operación, tienen la misma estructura, la misma tabla de la operación.

Ejemplo 19. *En el ejemplo 11 vimos que, planteando una notación genérica, solo aparecía un grupo de orden 3, que denotábamos por $G = \{1, a, b\}$, lo que quiere decir que cualquier otro grupo de orden 3 que tengamos tiene que ser obligatoriamente isomorfo a él. Por ejemplo, el grupo $\mathbb{Z}_3 = \{0, 1, 2\}$, con la suma, tiene esta tabla:*

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

que es idéntica a la del ejemplo 11. El paso de una a otra lo hacemos con el isomorfismo $f : G \to \mathbb{Z}_3$ definido por $f(1) = 0$, $f(a) = 1$ y $f(b) = 2$.

La imagen del elemento neutro de un grupo por un isomorfismo es siempre el elemento neutro del otro grupo, y la imagen de un elemento de orden k tiene también orden k. Esto nos sirve para ver que los grupos de los ejemplos 14 y 15 no son isomorfos, porque el primero no tiene elementos de orden 4 y el segundo sí.

Ejercicio 20. *Los grupos $\mathbb{Z}_4$ con la suma, $U(\mathbb{Z}_5)$, $U(\mathbb{Z}_8)$ y $U(\mathbb{Z}_12)$ con el producto, y el grupo de raíces cuartas complejas de la unidad $\{1, -1, i, -i\} \in \mathbb{C}$, también con el producto, tienen todos ellos orden 4. Halla el orden de sus elementos y decide a cuál de los grupos de los ejemplos 14 y 15 son isomorfos cada uno de ellos.*

Ejercicio 21. *Demuestra que la imagen del neutro de un grupo por un isomorfismo es el neutro del otro grupo.*

Ejercicio 22. *Demuestra que un elemento y su imagen por un isomorfismo tienen el mismo orden.*

Grupos cíclicos

Decimos que un grupo G es *cíclico* si todos sus elementos se pueden expresar como potencias de un elemento $x \in G$. Llamaremos *generador* de G a este elemento x, y escribiremos $G =< x >$.

Si todas las potencias son distintas, el grupo es $G = \{..., x^{-3}, x^{-2}, x^{-1}, 1, x^1, x^2, x^3, ...\}$; decimos que es un grupo cíclico *infinito* y lo denotaremos por C_∞.

Ejemplo 23. *El conjunto $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$, con la operación suma, es un grupo cíclico infinito.*

En cambio, si las potencias no son todas distintas, x tiene orden *finito* m y $G = \{1, x, x^2, ..., x^{m-1}\}$. Cualquier otra potencia x^k se puede reducir a una de ellas, tomando el resto de dividir k por m: $x^k = x^{mq+r} = (x^m)^q x^r = 1^q x^r = x^r$, $0 \leq r < m$.

En este caso decimos que el grupo G es un grupo cíclico de orden m, y lo denotaremos por C_m. El generador $x \in G$ es un elemento que tiene también orden m y esta es la manera de distinguir si un grupo es cíclico o no:

- Si un grupo de orden m tiene algún elemento de orden m es cíclico.
- Si todos los elementos de un grupo de orden m tienen orden menor estrictamente que m, entonces no es cíclico.

Ejemplo 24. *El conjunto $\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}$ de la aritmética modular, con la operación suma, es un grupo cíclico de orden m. El elemento 1 es un generador de $\mathbb{Z}_m$, pero puede haber otros.*

Ejemplo 25. *El conjunto de las raíces cuartas de 1, $\{1, -1, i, -i\} \subset \mathbb{C}$, con el producto habitual, es un grupo cíclico de orden 4 generado por i, porque todos los elementos se pueden poner como potencias de i: $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -1$.*

Ejercicio 26. *Comprueba que el elemento $-i$ es también un generador del grupo del ejemplo anterior y que, en cambio, -1 no lo es.*

Existe un grupo cíclico de orden m, para cualquier $m \in \mathbb{Z}$. Además este grupo es único, salvo isomorfismos. O dicho de otra forma, podemos asegurar que dos grupos cíclicos del mismo orden son isomorfos.

Producto de grupos cíclicos

Consideramos dos grupos cíclicos $C_m = \{1, x, x^2, ..., x^{m-1}\}$ y $C_n = \{1, y, y^2, ..., y^{n-1}\}$.

Definimos el *producto*, o *producto directo* de estos dos grupos como el conjunto $C_m \times C_n = \{(x^a, y^b) | x^a \in C_m, y^b \in C_n\}$, que es el producto cartesiano y tiene $m \cdot n$ elementos, con esta operación: $(x^a, y^b)(x^{a'}, y^{b'}) = (x^{a+a'}, y^{b+b'})$, donde tenemos que reducir los exponentes módulos m y n respectivamente.

Este conjunto $C_m \times C_n$ con esta operación tiene estructura de grupo y su orden es $m \cdot n$. Nos interesa ver cuándo es a su vez cíclico, y cuándo no. Vemos primero un ejemplo de cada caso y después damos el resultado general.

Ejemplo 27. *El producto de dos grupos cíclicos de órdenes 2 y 3, $C_2 = \{1, x\}$ y $C_3 = \{1, y, y^2\}$ es el conjunto $C_2 \times C_3 = \{(1,1), (1,y), (1,y^2), (x,1), (x,y), (x,y^2)\}$, con la operación dada por la tabla:*

	$(1,1)$	$(1,y)$	$(1,y^2)$	$(x,1)$	(x,y)	(x,y^2)
$(1,1)$	$(1,1)$	$(1,y)$	$(1,y^2)$	$(x,1)$	(x,y)	(x,y^2)
$(1,y)$	$(1,y)$	$(1,y^2)$	$(1,1)$	(x,y)	(x,y^2)	$(x,1)$
$(1,y^2)$	$(1,y^2)$	$(1,1)$	$(1,y)$	(x,y^2)	$(x,1)$	(x,y)
$(x,1)$	$(x,1)$	(x,y)	(x,y^2)	$(1,1)$	$(1,y)$	$(1,y^2)$
(x,y)	(x,y)	(x,y^2)	$(x,1)$	$(1,y)$	$(1,y^2)$	$(1,1)$
(x,y^2)	(x,y^2)	$(x,1)$	(x,y)	$(1,y^2)$	$(1,1)$	$(1,y)$

Los órdenes de los elementos son:

- $(1,1)$*, que es el elemento neutro, tiene orden 1.*
- $(x,1)$ *tiene orden 2.*
- $(1,y)$ *y* $(1,y^2)$ *tienen orden 3.*
- (x,y) *y* (x,y^2) *tienen orden 6, es decir, son generadores.*

Por tanto $C_2 \times C_3$ *es un grupo cíclico. Es isomorfo a* C_6*.*

Ejercicio 28. *Enumera los ocho elementos del grupo* $C_2 \times C_4$ *y haz la tabla de la operación. Determina el orden de cada elemento y deduce que no es un grupo cíclico.*

El producto de grupos cíclicos puede ser, a su vez, un grupo cíclico, como en el caso $C_2 \times C_3$, o un grupo no cíclico, como $C_2 \times C_4$. En general podemos afirmar lo siguiente:

Teorema 29. *Si* m *y* n *son enteros positivos primos entre sí, entonces el producto* $C_m \times C_n$ *es cíclico:* $C_m \times C_n \approx C_{mn}$*. En caso contrario, si no son primos entre sí, entonces* $C_m \times C_n$ *no es cíclico.*

El siguiente teorema permite caracterizar todos los grupos finitos conmutativos.

Teorema 30. *Si* G *es un grupo finito conmutativo, entonces o es cíclico o es un producto de grupos cíclicos.*

Con este teorema podemos asegurar lo siguiente:

- Si p es número primo, el único grupo conmutativo de orden p es el grupo cíclico C_p.
- Los grupos conmutativos de orden 4 son C_4 y $C_2 \times C_2$, que no son isomorfos.
- El único grupo conmutativo de orden 6 es C_6, porque el otro que podemos plantear, $C_2 \times C_3$, es isomorfo a él.
- Hay tres grupos conmutativos de orden 8: C_8, $C_4 \times C_2$ y $C_2 \times C_2 \times C_2$. Ninguno de ellos es isomorfo a otro.

Ejemplo 31. *Para hallar los grupos conmutativos de orden* 20*, tenemos que hallar las formas de expresar este número como producto de enteros positivos mayores que* 1 *y plantear los grupos correspondientes:*

$$\begin{array}{ll} 20 & C_{20} \\ 2 \cdot 10 & C_2 \times C_{10} \\ 4 \cdot 5 & C_4 \times C_5 \\ 2 \cdot 2 \cdot 5 & C_2 \times C_2 \times C_5 \end{array}$$

Pero 4 *y* 5 *son coprimos, con lo que* $C_4 \times C_5 \approx C_{20}$*; y* 2 *y* 5 *también, con lo que* $C_2 \times C_5 \approx C_{10}$ *y, por tanto,* $C_2 \times C_2 \times C_5 \approx C_2 \times C_{10}$*. Es decir, solo hay dos grupos conmutativos de orden* 20*:* C_{20} *y* $C_2 \times C_{10}$*.*

Ejercicio 32. *Halla los grupos conmutativos que hay de orden* 10*,* 25 *y* 40*.*

Grupo de permutaciones

Consideramos un conjunto finito de n elementos, que por comodidad, escribiremos $X = \{1, 2, \ldots, n\}$. El conjunto de las aplicaciones biyectivas de X en sí mismo, como vimos anteriormente, es un grupo.

Vamos a representar una aplicación biyectiva cualquiera $f : X \to X$ con una notación especial. Ponemos una fila con los elementos de X y, debajo, otra fila con sus imágenes, y cerramos estas dos filas entre paréntesis:

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ f(1) & f(2) & f(3) & \ldots & f(n) \end{pmatrix}$$

o, simplemente, pondremos $f(1)f(2)f(3)\ldots f(n)$, que puede interpretarse como una permutación de los elementos de X.

Ejemplo 33. *La aplicación* $f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ *definida por* $f(1) = 3$, $f(2) = 2$, $f(3) = 4$ *y* $f(4) = 1$ *la representamos con la matriz* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$, *o simplemente como la permutación* 3241.

Así pues, entenderemos las aplicaciones como *permutaciones*, que representaremos con letras griegas: α, β, γ, ... , σ, ... Al conjunto que forman lo denotaremos por S_n, y lo llamaremos *grupo simétrico* de orden n. Tiene orden $n!$ y, salvo el caso $n = 2$, no es conmutativo.

Ejemplo 34. *Veamos los casos más sencillos, que son* $n = 2$ *y* $n = 3$*:*

- *Si* $n = 2$, $S_2 = \{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\} = \{12, 21\}$, *que es un grupo de dos elementos, isomorfo a* C_2.
- *Si* $n = 3$, $S_2 = \{123, 132, 213, 231, 312, 321\}$, *que es un grupo de seis elementos, no conmutativo.*

A la composición de aplicaciones biyectivas la llamaremos *producto* de permutaciones. Para hacer este producto solo tenemos que considerar que estamos componiendo aplicaciones.

Ejemplo 35. *Si queremos hacer el producto* $\beta\alpha$ *de las permutaciones de* S_5 $\alpha = 34512$ *y* $\beta = 15234$, *hacemos lo siguiente: el primer elemento es la imagen de 1, que hallamos así:* $\beta\alpha(1) = \beta(3) = 2$*; la imagen de 2, que es el segundo elemento de la permutación, es* $\beta\alpha(2) = \beta(4) = 3$. *Los otros tres elementos son* $\beta\alpha(3) = \beta(5) = 4$, $\beta\alpha(4) = \beta(1) = 1$ *y* $\beta\alpha(5) = \beta(2) = 5$, *con lo que* $\beta\alpha = 23415$.

Para hallar la permutación inversa de, por ejemplo, α, *basta darse cuenta de que si* $\alpha(1) = 3$, $\alpha^{-1}(3) = 1$. *Haciendo esto con todos los elementos y poniéndolos en su orden, resulta* $\alpha^{-1} = 45123$.

Ejercicio 36. *Dadas las permutaciones* $\alpha = 365142$ *y* $\beta = 451623$, *halla* $\beta\alpha$, $\alpha\beta$, α^{-1} *y* β^{-1}.

De la misma forma, podríamos hacer operaciones como α^2, β^{-3}, $\alpha\beta\alpha$ (que no es $\alpha^2\beta$ porque el producto de permutaciones no es conmutativo) o $\beta^6\alpha^{-5}\beta^{17}$.

Expresión de una permutación como producto de ciclos

Esta es una forma de expresar las permutaciones que resulta de mucha utilidad. Vamos a explicarla con un ejemplo.

Consideramos la permutación $\sigma = 259317486 \in S_9$. La imagen de 1 es 2, la de 2 es 5 y la de 5 vuelve a ser 1, con lo que se cierra un *ciclo* de *longitud* 3, que denotaremos por (125). Lógicamente, también podríamos poner (251) o (512), si hubiéramos empezado por 2 o por 5. Lo que no sería lo mismo es el ciclo (152).

Ahora nos fijamos en el primer elemento que no ha salido, que es 3. Su imagen es 9, la de 9 es 6, la de 6 es 7, la de 7 es 4 y la de 4 es 3, con lo que se cierra el ciclo, que es (39674) y tiene longitud 5. Queda el elemento 8 cuya imagen es él mismo, con lo que formaría un ciclo él solo que denotaríamos por (8).

Tenemos, por tanto,

$$\sigma = (125)(39674)(8),$$

que es la expresión de σ como *producto de ciclos disjuntos*. Esta expresión es única salvo que podemos expresar los ciclos de formas diferentes, como hemos explicado en el caso (125), y salvo el orden en que pongamos los ciclos, porque el producto de ciclos disjuntos sí es conmutativo. Por último, señalemos que los ciclos con un elemento no se suelen poner; se entiende que los números que no aparecen forman ciclos de longitud 1. Por ejemplo, $(134)(67) \in S_8$ entendemos que es la permutación $(134)(67)(2)(5)(8)$.

Ejercicio 37. *Expresa la permutación $\alpha = 42516387 \in S_8$ como producto de ciclos disjuntos y la permutación $\beta = (176)(285)$, también de S_8, en la notación habitual de las permutaciones.*

Ejercicio 38. *Multiplica los ciclos* (35496) *y* (152798)*, que no son disjuntos, y expresa la permutación resultante como producto de ciclos disjuntos.*

Clasificación de las permutaciones según su tipo

Vamos a hacer en este apartado una primera clasificación de las permutaciones: según su tipo. En el apartado siguiente veremos otra: según su signo o su paridad.

Decimos que una permutación es del *tipo* $[1^{\alpha_1}2^{\alpha_2}\dots n^{\alpha_n}]$ si en su expresión como producto de ciclos disjuntos hay α_1 ciclos de longitud 1, α_2 de longitud 2, ... y α_n de longitud n. Por ejemplo, la permutacion $(143)(28)(67) \in S_8$ es del tipo $[1\ 2^2\ 3]$ porque tiene un ciclo de longitud 1 (cuando el exponente es 1 no hace falta ponerlo), que es (5), dos de longitud 2, (28) y (67), y uno de longitud 3, (143).

Esto permite hacer una clasificación de las permutaciones, como vemos en el siguiente ejemplo.

Ejemplo 39. *En S_5 hay $5! = 120$ permutaciones, que pueden tener estos tipos:* $[1^5]$, $[1^3\ 2]$, $[1^2\ 3]$, $[1\ 2^2]$, $[1\ 4]$, $[2\ 3]$ *y* $[5]$.

Ejercicio 40. *Enumera los once tipos de permutaciones que hay en S_6.*

El número de permutaciones que hay del tipo $[1^{\alpha_1}2^{\alpha_2}\dots n^{\alpha_n}]$ viene dado por esta expresión:

$$\frac{n!}{1^{\alpha_1}2^{\alpha_2}\dots n^{\alpha_n}\alpha_1!\alpha_2!\dots\alpha_n!},$$

aunque a veces resulta más sencillo calcularlo empleando las técnicas de contar vistas en el primer cuatrimestre.

Ejercicio 41. *Halla el número de permutaciones de S_5 que hay de cada uno de los siete tipos listados en el ejemplo 39. Comprueba que, en total, han salido 120. Enumera las quince que hay del tipo* $[1\ 2^2]$.

Orden de una permutación

El orden de un ciclo c de longitud l, entendido como un elemento del grupo S_n, es también l. Es decir, $c^l = \mathrm{Id}$, siendo este l el menor exponente que lo verifica. Además podemos afirmar que $c^k = \mathrm{Id}$ si y solo si k es un múltiplo de l.

Ejemplo 42. *Queremos hallar el orden del ciclo $c = (2734)$. Si hacemos sus potencias, resulta $c^2 = (23)(74)$, $c^3 = (2437)$ y $c^4 = \mathrm{Id}$. A partir de la quinta potencia se repetirían, de forma que para hallar una potencia cualquiera c^k deberíamos dividir por cuatro y quedarnos con el resto r, con lo que nos quedaría $c^k = c^r$. Por ejemplo,* $(2734)^{4567} = (2734)^3 = (2437)$.

Consideramos ahora una permutación cualquiera $\alpha = c_1 c_2 \dots c_r$, expresada como producto de ciclos disjuntos c_i de longitudes l_i.

Las potencias son $\alpha^k = c_1^k c_2^k \dots c_r^k$, porque el producto en este caso es conmutativo y podemos agrupar los ciclos iguales. Entonces, $\alpha^k = \mathrm{Id}$ si para todo i $c_i^k = \mathrm{Id}$, y esto sucede si k es múltiplo de l_i. Por tanto, k tiene que ser múltiplo de todas las longitudes l_i y el orden sería el mínimo común múltiplo: $\mathrm{ord}(\alpha) = \mathrm{mcm}(l_1, l_2, \dots, l_r)$.

Esta sería una de las formas de hallar el orden de una permutación.

Ejemplo 43. *Podemos hallar el orden de una permutación de varias formas.*

- *Haciendo las potencias de la permutación hasta obtener la identidad. Por ejemplo, si $\alpha = 562143 \in S_6$, $\alpha^2 = 436512$ y $\alpha^3 = 123456 = \mathrm{Id}$, con lo que el orden de α es 3.*
- *Descomponiendo en producto de ciclos disjuntos y hallando el mínimo común múltiplo de sus longitudes. Por ejemplo, si $\beta = 642971583 \in S_9$, la descomposición es $(16)(2493)(57)(8)$, con lo que ord$(\beta)(mcm(1, 2, 4) = 4$.*
- *A partir de su tipo. Si una permutacion $\gamma \in S_{10}$ es, por ejemplo, del tipo $[1\ 2^2 5]$, su orden es ord$(\gamma) = mcm(1, 2, 5) = 10$.*

Recordemos finalmente que el orden de una permutación de S_n tiene que ser un divisor del orden de S_n, que es $n!$.

Permutaciones pares e impares

Es esta otra clasificación de las permutaciones.

Vamos a ver primero que todo ciclo se puede poner como producto de ciclos de longitud 2, o *trasposiciones*.

Consideramos un ciclo cualquiera de longitud r, $(x_1 x_2 x_3 \dots x_{r-1} x_r)$. Se puede comprobar que se puede expresar como producto de $r - 1$ trasposiciones así:

$$(x_1 x_2 x_3 \dots x_{r-1} x_r) = (x_1 x_r)(x_1 x_{r-1}) \dots (x_1 x_3)(x_1 x_2)$$

A diferencia de la expresión de una permutación como producto de ciclos disjuntos, ahora esta descomposición no es única. Por ejemplo, se puede plantear esta otra, que tiene también $r-1$ trasposiciones:

$$(x_1x_2x_3\dots x_{r-1}x_r) = (x_1x_2)(x_2x_3)\dots(x_{r-2}x_{r-1})(x_{r-1}x_r)$$

Pero todas las descomposiciones que se puedan hacer de un ciclo tienen o un número par de trasposiciones o un número impar.

Ejemplo 44. *Para el ciclo* (35178)*, las dos descomposiciones que hemos planteado son:*

$$(35178) = (38)(37)(31)(35) = (35)(51)(17)(78),$$

pero hay muchas otras:

$$(35178) = (38)(37)(12)(31)(25)(32) = (71)(75)(73)(78)(12)(12)(45)(45) = \dots$$

En cualquier caso, el número de trasposiciones es par.

Habíamos visto que toda permutación se puede expresar como producto de ciclos disjuntos, y ahora hemos visto que todo ciclo se puede descomponer como producto de trasposiciones. Por tanto, podemos asegurar que *toda permutación se puede expresar como producto de trasposiciones.*

Esta descomposición no es única pero, por lo que hemos dicho en un párrafo anterior, todas las descomposiciones que se puedan hacer de una permutación tienen o un número par de trasposiciones o un número impar. En el primer caso, decimos que la permutación es *par*; en el segundo, que es *impar.*

Ejemplo 45. *La descomposición en ciclos disjuntos de* $15384162 \in S_8$ *es* $(176)(2548)$ *y en trasposiciones, según el primero de los procedimientos, es* $(16)(17)(28)(24)(25)$*, con lo que la permutación es impar.*

Para ver la paridad de una permutación no es imprescindible hacer la descomposición como producto de trasposiciones; basta conocer su tipo. Basándonos en el hecho de que un ciclo de longitud r descompone en producto de $r-1$ trasposiciones, podemos afirmar que una permutación del tipo $[1^{\alpha_1}2^{\alpha_2}\dots n^{\alpha_n}]$ es par o impar según lo sea el número $\alpha_2 + 2\alpha_3 + 3\alpha_4 + \dots + (n-1)\alpha_n$.

De las $n!$ permutaciones de S_n, se puede demostrar que la mitad son pares y la mitad impares. Proponemos una demostración en el siguiente ejercicio.

Ejercicio 46. *Demuestra que la función* $f : S_n \to S_n$ *definida por* $f(\sigma) = (12)\sigma$ *es una biyección. La imagen por* f *de una permutación par es una impar, y viceversa. Deduce de esto que hay tantas permutaciones pares como impares.*

El conjunto de las permutaciones pares, que denotaremos por A_n, con la operación producto, tiene estructura de grupo y se llama *grupo alternado.* El orden de A_n es $\frac{n!}{2}$ y, salvo el caso $n = 3$, no es conmutativo.

Ejemplo 47. *El conjunto de las permutaciones pares de* S_3 *es* $A_3 = \{123, 231, 312\}$*. La permutacion* 123 *es la identidad, que es par, y las otras son* $231 = (123) = (13)(12)$ *y* $312 = (132) = (12)(13)$*, que también son pares.* A_3 *es isomorfo a* C_3*.*

Ejercicio 48. *El grupo* A_4 *tiene* $\frac{4!}{2} = 12$ *elementos. Enuméralos y calcula el inverso y el orden de cada uno de ellos. Comprueba que no es conmutativo.*

Ejercicio 49. *Demuestra que* A_n *es un grupo.*