

Álgebra II

FACULTAD
DE
CIENCIAS
UNIVERSIDAD DE GRANADA



Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Eres libre de compartir y redistribuir el contenido de esta obra en cualquier medio o formato, siempre y cuando des el crédito adecuado a los autores originales y no persigas fines comerciales.

Álgebra II

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Arturo Olivares Martos

Granada, 2025

Índice general

| | |
|--|-----------|
| 1. Grupos: definición, generalidades y ejemplos | 5 |
| 1.1. Grupos diédricos D_n | 17 |
| 1.1.1. Motivación | 18 |
| 1.1.2. Definición y primeras propiedades | 23 |
| 1.2. Generadores de un grupo | 24 |
| 1.3. Grupos Simétricos S_n | 27 |
| 1.3.1. Signatura | 37 |
| 1.3.2. Grupos Alternados A_n | 40 |
| 1.4. Grupos de matrices | 43 |
| 1.4.1. Grupo lineal $GL_n(\mathbb{F})$ | 43 |
| 1.4.2. Grupo lineal especial $SL_n(\mathbb{F})$ | 45 |
| 1.5. Homomorfismos de grupos | 46 |
| 1.6. Resumen de grupos | 53 |
| 2. Subgrupos, Generadores, Retículos y Grupos cíclicos | 55 |
| 2.1. Generadores de subgrupos | 58 |
| 2.2. Retículo de subgrupos de un grupo | 59 |
| 2.2.1. Ejemplos | 63 |
| 2.3. Índice y Teorema de Lagrange | 70 |
| 2.4. Propiedades de grupos cíclicos | 76 |
| 3. Relaciones de Ejercicios | 81 |
| 3.1. Combinatoria y Teoría de Grafos | 81 |
| 3.2. Grupos: generalidades y ejemplos | 121 |
| 3.3. Subgrupos, Generadores, Retículos y Grupos cíclicos | 145 |

En Álgebra I el objeto principal de estudio fueron los anillos conmutativos, conjuntos en los que teníamos definidas dos operaciones, una usualmente denotada con notación aditiva y otra con notación multiplicativa.

Posteriormente, el estudio se centró en los dominios de integridad (DI), anillos conmutativos donde teníamos más propiedades con las que manejar nuestros elementos (como la tan característica propiedad cancelativa). Después, el objeto de estudio fueron los dominios euclídeos (DE), donde ya podíamos realizar un estudio sobre la divisibilidad de los elementos del conjunto.

Finalmente, nos centramos en los dominios de factorización única (DFU), donde realizamos una breve introducción a la irreducibilidad de los polinomios.

En esta asignatura el principal objeto de estudio serán los grupos, conjuntos en los que hay definida una sola operación que entendemos por “buena¹”. Por tanto, los grupos serán estructuras menos restrictivas que los anillos conmutativos, aunque su estudio no será menos interesante.

¹La operación cumplirá ciertas propiedades deseables.

1. Grupos: definición, generalidades y ejemplos

Comenzamos realizando la primera definición necesaria para entender el concepto de grupo, que es entender qué es una operación dentro de un conjunto.

Definición 1.1 (Operación binaria). Sea G un conjunto, una operación binaria en G es una aplicación

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a * b \end{aligned}$$

Ejemplo. Ejemplos de operaciones binarias sobre conjuntos que ya conocemos son:

1. La suma y el producto de números en $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
2. Dado un conjunto X , los operadores \cap y \cup son operaciones binarias sobre el conjunto $\mathcal{P}(X)$.

Antes de dar la definición de grupo, daremos la de monoide, que es menos restrictiva que la de grupo.

Definición 1.2 (Monoide). Un monoide es una tripleta $(G, *, e)$ donde G es un conjunto no vacío, $*$ es una operación binaria en G y e es un elemento destacado de G de forma que se verifica:

- i) La propiedad asociativa de $*$:

$$(x * y) * z = x * (y * z) \quad \forall x, y, z \in G$$

- ii) La existencia de un elemento neutro (el elemento destacado de G):

$$\exists e \in G \mid e * x = x * e = x \quad \forall x \in G$$

Proposición 1.1. En un monoide, el elemento neutro es único.

Demostración. Sea $(G, *, e)$ un monoide y sea $f \in G$ tal que $f * x = x * f = x$ $\forall x \in G$:

$$f = f * e = e$$

□

Ejemplo. Ejemplos de monoides ya conocidos son:

1. $(\mathbb{N}, +, 0), (\mathbb{N}, \cdot, 1)$

2. Dado un conjunto X : $(\mathcal{P}(X), \cap, X)$, $(\mathcal{P}(X), \cup, \emptyset)$

Definición 1.3 (Grupo). Un grupo es una tripleta $(G, *, e)$ donde G es un conjunto no vacío, $*$ es una operación binaria en G y e es un elemento destacado de G de forma que se verifica:

i) La propiedad asociativa de $*$:

$$(x * y) * z = x * (y * z) \quad \forall x, y, z \in G$$

ii) La existencia de un elemento neutro por la izquierda (el elemento destacado de G):

$$\exists e \in G \mid e * x = x \quad \forall x \in G$$

iii) La existencia de un elemento simétrico por la izquierda para cada elemento de G :

$$\forall x \in G \quad \exists x' \in G \mid x' * x = e$$

Si además se cumple:

iv) La propiedad conmutativa de $*$:

$$x * y = y * x \quad \forall x, y \in G$$

Entonces, diremos que $(G, *, e)$ es un grupo conmutativo o abeliano.

Notación. Para una mayor comodidad a la hora de manejar grupos, introducimos las siguientes notaciones:

1. Cuando dado un conjunto no vacío G sepamos por el contexto a qué grupo $(G, *, e)$ nos estamos refiriendo, indicaremos simplemente G (o en algunos casos $(G, *)$, para hacer énfasis en la operación binaria) para referirnos al grupo $(G, *, e)$.
2. En algunos casos, usaremos (por comodidad) la notación multiplicativa de los grupos. De esta forma, dado un grupo $(G, \cdot, 1)$, en ciertos casos notaremos la operación binaria \cdot simplemente por yuxtaposición:

$$x \cdot y = xy \quad \forall x, y \in G$$

Además, nos referiremos al elemento neutro como “uno” y al simétrico de cada elemento como “inverso”, sustituyendo la notación de x' por la de x^{-1} .

3. Otra notación que también usaremos (aunque de forma menos frecuente que la multiplicativa) será la aditiva. Dado un grupo $(G, +, 0)$, nos referiremos al elemento neutro como “cero” y al simétrico de cada elemento como “opuesto”, sustituyendo la notación de x' por la de $-x$.

Ejemplo. Ejemplos de grupos que se usarán con frecuencia en la asignatura son:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con su respectiva suma son grupos abelianos.

2. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con su respectivo producto son grupos abelianos.

Notemos la importancia de eliminar el 0 de cada conjunto para que todo elemento tenga inverso, así como que \mathbb{Z}^* no es un grupo, ya que el inverso de cada elemento (para el producto al que estamos acostumbrados) no está dentro de \mathbb{Z}^* .

3. $\{1, -1, i, -i\} \subseteq \mathbb{C}$ con el producto heredado¹ de \mathbb{C} también es un grupo abeliano.
4. $(\mathcal{M}_2(\mathbb{R}), +)$ es un grupo abeliano.
5. Dado un cuerpo \mathbb{K} , el grupo lineal de orden 2 con coeficientes en dicho cuerpo:

$$\mathrm{GL}_2(\mathbb{K}) = \{M \in \mathcal{M}_2(\mathbb{K}) : \det(M) \neq 0\}$$

con el producto heredado de $\mathcal{M}_2(\mathbb{K})$ es un grupo que no es conmutativo.

6. \mathbb{Z}_n con su suma es un grupo abeliano, $\forall n \in \mathbb{N}$.
7. $\mathcal{U}(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n \mid \mathrm{mcd}(a, n) = 1\}$ con el producto es un grupo abeliano, $\forall n \in \mathbb{N}$. También lo notaremos por \mathbb{Z}_n^\times .
8. Dado $n \geq 1$, consideramos:

$$\begin{aligned} \mu_n &= \{\text{raíces complejas de } x^n - 1\} = \left\{ \xi_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} : k \in \{0, \dots, n-1\} \right\} \\ &= \left\{ 1, \xi, \xi^2, \dots, \xi^{n-1} : \xi = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right\} \end{aligned}$$

Este conjunto es un grupo abeliano con el producto heredado de \mathbb{C} .

9. Dado un cuerpo \mathbb{K} , el grupo lineal especial de orden 2 sobre dicho cuerpo:

$$\mathrm{SL}_2(\mathbb{K}) = \{M \in \mathcal{M}_2(\mathbb{K}) : \det(M) = 1\}$$

con el producto heredado de $\mathcal{M}_2(\mathbb{K})$ es un grupo que no es conmutativo.

10. Sean $(G, \square, e), (H, \triangle, f)$ dos grupos, si consideramos sobre $G \times H$ la operación binaria $*$: $(G \times H) \times (G \times H) \rightarrow G \times H$ dada por:

$$(x, u) * (y, v) = (x \square y, u \triangle v) \quad \forall (x, u), (y, v) \in G \times H$$

Entonces, $G \times H$ es un grupo, al que llamaremos grupo directo de G y H . Este será abeliano si y solo si G y H lo son.

11. Si X es un conjunto no vacío y consideramos

$$S(X) = \{f : X \rightarrow X \mid f \text{ biyectiva}\} = \mathrm{Perm}(X)$$

es un grupo no abeliano con la operación de composición de funciones \circ .

En el caso en el que X sea finito y tenga n elementos: $X = \{x_1, x_2, \dots, x_n\}$, notaremos:

$$S_n = S(X)$$

¹Será común hablar de “operación heredada” cuando consideramos un subconjunto de un conjunto en el que ya hay definida una operación interna, haciendo referencia a la restricción en dominio y recorrido de dicha operación interna al subconjunto considerado.

12. Sea $(G, *, e)$ un grupo y X un conjunto, consideramos el conjunto:

$$\text{Apl}(X, G) = G^X = \{f : X \rightarrow G \mid f \text{ aplicación}\}$$

junto con la operación binaria $*$: $G^X \times G^X \rightarrow G^X$ dada por:

$$(f * g)(x) = f(x) * g(x) \quad \forall x \in X, \quad \forall f, g \in G^X$$

Entonces, $(G^X, *, g)$ es un grupo, con elemento neutro:

$$g(x) = e \quad \forall x \in X$$

de esta forma, dada $f \in G^X$, la aplicación simétrica de f será:

$$f'(x) = (f(x))' \quad \forall x \in X$$

Casos a destacar son:

- a) Si $X = \emptyset$, entonces $G^X = \{\emptyset\}$.
- b) Si $X = \{1, 2\}$, entonces G^X se identifica con $G \times G$.

13. El grupo más pequeño que se puede considerar es el único grupo válido sobre un conjunto unitario $X = \{e\}$. Es decir, el grupo $(X, *, e)$ con $X = \{e\}$ y $*$: $X \times X \rightarrow X$ dada por:

$$e * e = e \quad e \in X$$

A este grupo (independientemente de cual sea el conjunto X , ya que todos tendrán la misma² estructura) lo llamaremos grupo trivial.

Ejemplo. Consideramos en \mathbb{Z} la operación binaria $*$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ dada por:

$$a * b = a + b + 1 \quad \forall a, b \in \mathbb{Z}$$

Donde usamos $+$ para denotar la suma de \mathbb{Z} . Se pide demostrar que $(\mathbb{Z}, *)$ es un grupo abeliano.

Demostración. Demostramos cada una de las propiedades de la definición de grupo abeliano:

- La propiedad asociativa de $*$ es consecuencia de las propiedades asociativa y conmutativa de $+$:

$$\begin{aligned} (a * b) * c &= (a + b + 1) * c = a + b + 1 + c + 1 = a + b + c + 2 \\ a * (b * c) &= a * (b + c + 1) = a + b + c + 1 + 1 = a + b + c + 2 \\ &\forall a, b, c \in \mathbb{Z} \end{aligned}$$

²Concepto que luego formalizaremos.

- Buscamos $x \in \mathbb{Z}$ de forma que $x * a = a$ para todo $a \in \mathbb{Z}$, por lo que queremos resolver la ecuación:

$$X * a = a \iff X + a + 1 = a \implies X = -1$$

Por lo que $-1 \in \mathbb{Z}$ es el elemento neutro para $*$:

$$-1 * a = -1 + a + 1 = a \quad \forall a \in \mathbb{Z}$$

- Fijado $x \in \mathbb{Z}$, tratamos de buscar un elemento simétrico para x , por lo que buscamos resolver la ecuación:

$$X * x = -1 \iff X + x + 1 = -1 \iff X = -x - 2$$

Por lo que dado $x \in \mathbb{Z}$, su elemento simétrico es $-x - 2 \in \mathbb{Z}$:

$$(-x - 2) * x = -x - 2 + x + 1 = -1 \quad \forall x \in \mathbb{Z}$$

- La propiedad conmutativa de $*$ es consecuencia de la propiedad conmutativa de $+$:

$$a * b = a + b + 1 = b + a + 1 = b * a \quad \forall a, b \in \mathbb{Z}$$

□

Propiedades

Aunque estas propiedades parezcan ya conocidas y familiares (por ejemplo para el caso $(\mathbb{Z}, +, 0)$), es una buena observación darnos cuenta de que son válidas para **cualquier grupo** que consideremos, por raros y difíciles que sean sus elementos y operación interna.

Proposición 1.2. Sea $(G, *, e)$ un grupo, destacamos sus primeras propiedades:

i) $x * x' = e \quad \forall x \in G$.

ii) $x * e = x \quad \forall x \in G$.

iii) El elemento neutro de $*$ es único. Simbólicamente:

$$\exists_1 e \in G \mid e * x = x \quad \forall x \in G$$

iv) Fijado $x \in G$, el simétrico de x es único. Simbólicamente:

$$\forall x \in G \quad \exists_1 x' \in G \mid x' * x = e$$

Demostración. Demostramos cada una a partir de la anterior:

i) En primer lugar, observemos que:

$$x' * (x * x') = (x' * x) * x' = e * x' = x' \quad (1.1)$$

Ahora:

$$x * x' = e * (x * x') = ((x')' * x') * (x * x') = (x')' * (x' * (x * x')) \stackrel{(*)}{=} (x')' * x' = e$$

Donde en $(*)$ hemos usado (1.1).

ii) Usando $i)$ en $(*)$:

$$x * e = x * (x' * x) = (x * x') * x \stackrel{(*)}{=} e * x = x$$

iii) Sea $f \in G$ de forma que $f * x = x \ \forall x \in G$, entonces:

$$f = f * e \stackrel{(*)}{=} e$$

Donde en $(*)$ hemos usado $ii)$.

De otra forma, podríamos haber argumentado que gracias a $ii)$, todo grupo es un monoide, por lo que podemos aplicar la Proposición 1.1 y ya habríamos terminado.

iv) Dado $x \in G$, sea $x'' \in G$ de forma que $x'' * x = e$, entonces:

$$x'' = x'' * e \stackrel{(*)}{=} x'' * (x * x') = (x'' * x) * x' = e * x' = x'$$

Donde en $(*)$ hemos usado $i)$.

□

Notación. A partir de ahora, dado un grupo $(G, *, e)$, comenzaremos a usar (por comodidad) la notación multiplicativa de los grupos:

$$xy = x * y \quad \forall x, y \in G$$

Y denotando a x' (el elemento simétrico de x) por x^{-1} .

Proposición 1.3. *En un grupo G se verifica la propiedad cancelativa (tanto a la izquierda como a la derecha):*

$$\forall x, y, z \in G : \begin{cases} xy = xz \implies y = z \\ xy = zy \implies x = z \end{cases}$$

Demostración. Para la primera, supongamos que $xy = xz$:

$$y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$$

Ahora, para la segunda, supongamos que $xy = zy$ y la demostración es la misma que la anterior pero en el otro sentido y tomando $e = yy^{-1}$.

$$x = xe = x(yy^{-1}) = (xy)y^{-1} = (zy)y^{-1} = z(yy^{-1}) = z$$

□

Proposición 1.4. *Sea G un grupo, entonces:*

1. $e^{-1} = e$.
2. $(x^{-1})^{-1} = x, \forall x \in G$.
3. $(xy)^{-1} = y^{-1}x^{-1}, \forall x, y \in G$.

Demostración. Cada caso se demuestra observando sencillamente que:

1. $ee = e$.
2. $xx^{-1} = e$.
3. $(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}ey = e$.

□

Proposición 1.5. *Sea G un conjunto no vacío con una operación binaria $*$ asociativa, son equivalentes:*

- i) G es un grupo.
- ii) Para cada par de elementos $a, b \in G$, las ecuaciones³:

$$aX = b \quad Xa = b$$

Tienen solución en G , es decir: $\exists c, d \in G \mid ac = b \wedge da = b$.

Demostración. Demostramos las dos implicaciones:

- i) \Rightarrow ii) Tomando $c = a^{-1}b, d = ba^{-1} \in G$ se tiene.
- ii) \Rightarrow i) Basta demostrar que $\exists e \in G$ con $ex = x \forall x \in G$ y que fijado $x \in G$, entonces $\exists x' \in G$ con $x'x = e$:

1. Dado $a \in G$, sabemos que la ecuación $Xa = a$ tiene solución, por lo que existe $e \in G$ de forma que $ea = a$.

Veamos que no depende de la elección de a ; es decir, que es un elemento neutro para cualquier elemento de G . Para ello, dado cualquier $b \in G$, sabemos que la ecuación $aX = b$ tiene solución, por lo que existirá un $x_b \in G$ de forma que $ax_b = b$. Finalmente:

$$eb = e(ax_b) = (ea)x_b = ax_b = b \quad \forall b \in G$$

2. Fijado $x \in G$, sabemos que la ecuación $Xx = e$ tiene solución, por lo que existe $x' \in G$ de forma que $x'x = e$, para cualquier $x \in G$.

□

Proposición 1.6 (Ley asociativa general). *Sea G un grupo, dados $n, m \in \mathbb{N}$ con $n > m > 0$, se tiene que:*

$$\left(\prod_{i=1}^m x_i \right) \left(\prod_{i=m+1}^n x_i \right) = \prod_{i=1}^n x_i \quad \forall x_i \in G, \quad i \in \{1, \dots, n\}$$

Demostración. Por inducción sobre $n \in \mathbb{N}$:

- Para $n = 0, n = 1$: No hay nada que probar: $\nexists m \in \mathbb{N}$ con $0 < m < n$.

³Donde hemos usado X para denotar la incógnita y que no se confunda con un elemento de G .

- Para $n = 2$: Dado $m \in \mathbb{N}$ con $0 < m < n$ (entonces $m = 1$):

$$\left(\prod_{i=1}^m x_i \right) \left(\prod_{i=m+1}^n x_i \right) = x_1 x_2 = \prod_{i=1}^n x_i \quad \forall x_1, x_2 \in G$$

- Supuesto para n , veámoslo para $n + 1$: Dado $m \in \mathbb{N}$ con $0 < m < n + 1$:

$$\begin{aligned} \left(\prod_{i=1}^m x_i \right) \left(\prod_{i=m+1}^{n+1} x_i \right) &= \left[x_1 \left(\prod_{i=2}^m x_i \right) \right] \left[\left(\prod_{i=m+1}^n x_i \right) x_{n+1} \right] \\ &= x_1 \left(\prod_{i=2}^m x_i \prod_{i=m+1}^n x_i \right) x_{n+1} \stackrel{(*)}{=} x_1 \left(\prod_{i=2}^n x_i \right) x_{n+1} = \prod_{i=1}^{n+1} x_i \\ &\forall x_i \in G, \quad i \in \{1, \dots, n+1\} \end{aligned}$$

Donde en $(*)$ hemos usado la hipótesis de inducción, ya que $0 < m - 1 < n$.

□

Definición 1.4 (Potencia). Sea (G, \cdot, e) un grupo, dado $x \in G$ y $n \in \mathbb{Z}$, podemos definir:

$$x^n = \begin{cases} \prod_{i=1}^n x & \text{si } n > 0 \\ e & \text{si } n = 0 \\ (x^{-1})^{-n} & \text{si } n < 0 \end{cases}$$

Notación. En grupos aditivos $(G, +, 0)$, en lugar de x^n escribiremos $n \cdot x$, que se define de igual forma pero en el caso $n > 0$, en lugar de escribir \prod , escribiremos \sum .

Proposición 1.7. Sea G un grupo, se verifica que:

$$x^{n+m} = x^n \cdot x^m \quad \forall x \in G, \quad n, m \in \mathbb{Z}$$

Demostración. Aunque la demostración es sencilla, hemos de distinguir bastantes casos, pues hemos de asegurarnos de que el límite superior de cada producto sea siempre un número positivo. Fijado $x \in G$, distinguimos en función de los valores de $n, m \in \mathbb{Z}$:

1. $n > 0$:

- a) $m > 0$:

$$x^{n+m} = \prod_{i=1}^{n+m} x = \left(\prod_{i=1}^n x \right) \cdot \left(\prod_{i=n+1}^{n+m} x \right) = \left(\prod_{i=1}^n x \right) \cdot \left(\prod_{i=1}^m x \right) = x^n \cdot x^m$$

- b) $m = 0$:

$$x^{n+0} = x^n = x^n \cdot e = x^n \cdot x^0$$

- c) $m < 0$:

En este caso, no sabemos el signo de $n+m$. Por tanto, hemos de distinguir casos:

1) $n + m > 0$: Entonces, $n > -m$. Tenemos:

$$x^n \cdot x^m = \left(\prod_{i=1}^n x \right) \cdot (x^{-1})^{-m} = \left(\prod_{i=1}^n x \right) \cdot \left(\prod_{i=1}^{-m} x^{-1} \right) = \prod_{i=1}^{n-(-m)} x = \prod_{i=1}^{n+m} x = x^{n+m}$$

2) $n + m = 0$: Entonces, $n = -m$. Tenemos:

$$x^{n+m} = x^0 = e = \left(\prod_{i=1}^n x \right) \cdot \left(\prod_{i=1}^n x^{-1} \right) = x^n \cdot \left(\prod_{i=1}^{-m} x^{-1} \right) = x^n \cdot (x^{-1})^{-m} = x^n \cdot x^m$$

3) $n + m < 0$: Entonces, $n < -m$. Tenemos:

$$\begin{aligned} x^n \cdot x^m &= \left(\prod_{i=1}^n x \right) \cdot (x^{-1})^{-m} = \left(\prod_{i=1}^n x \right) \cdot \left(\prod_{i=1}^{-m} x^{-1} \right) = \prod_{i=1}^{-m-n} x^{-1} = \\ &= \prod_{i=1}^{-(n+m)} x^{-1} = (x^{-1})^{-(n+m)} = x^{n+m} \end{aligned}$$

2. $n = 0$:

$$x^{0+m} = x^m = e \cdot x^m = x^0 \cdot x^m$$

3. $n < 0$:

a) $m > 0$:

$$x^{n+m} = x^{m+n} = x^m \cdot x^n = \prod_{i=1}^m x \cdot \prod_{i=1}^{-n} x^{-1} = x^n \cdot x^m$$

donde en la primera igualdad hemos usado la propiedad conmutativa de la suma en \mathbb{Z} , en la segunda hemos empleado el caso anteriormente demostrado, y en la última igualdad hemos empleado que $xx^{-1} = e = x^{-1}x$.

b) $m = 0$:

$$x^{n+0} = x^n = x^n \cdot e = x^n \cdot x^0$$

c) $m < 0$:

$$\begin{aligned} x^n \cdot x^m &= (x^{-1})^{-n} \cdot (x^{-1})^{-m} = \left(\prod_{i=1}^{-n} x^{-1} \right) \cdot \left(\prod_{i=1}^{-m} x^{-1} \right) = \\ &= \prod_{i=1}^{-n-m} x^{-1} = (x^{-1})^{-(n+m)} = x^{n+m} \end{aligned}$$

□

Definición 1.5 (Grupos finitos e infinitos). Sea G un grupo, si G como conjunto tiene⁴ $n \in \mathbb{N} \setminus \{0\}$ elementos, diremos que es un grupo finito. En dicho caso, diremos que n es el “orden del grupo”, notado por: $|G| = n$.

Si G no fuera finito, decimos que es un grupo infinito.

⁴Excluimos $n = 0$ ya que en la definición de grupo exigimos que $G \neq \emptyset$.

Definición 1.6 (Tabla de Cayley). En un grupo finito $G = \{x_1, x_2, \dots, x_n\}$, se llama tabla de Cayley (o de multiplicar⁵) a la matriz $n \times n$ de forma que su entrada (i, j) es $x_i x_j$.

Ejemplo. A continuación, mostramos ejemplos de posibles tablas de Cayley para ciertas operaciones sobre determinados grupos. Como podemos ver, la finalidad de la tabla es mostrar en cada caso cómo se comporta la operación binaria cuando se aplica a distintos elementos del grupo.

1. Si $G = \{0, 1\}$, podemos considerar sobre G las operaciones $*_1$ y $*_2$, cuya definición puede obtenerse a partir de sus tablas de Cayley:

| $*_1$ | 0 | 1 | $*_2$ | 0 | 1 |
|-------|---|---|-------|---|---|
| 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 |

2. Si $G = \{0, 1, 2\}$, podemos considerar sobre G la siguiente operación binaria:

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

3. Si $G = \{0, 1, 2, 3\}$, podemos considerar sobre G las siguientes operaciones binarias:

| | 0 | 1 | 2 | 3 | | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 | 1 | 1 | 0 | 3 | 2 |
| 2 | 2 | 3 | 0 | 1 | 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 | 3 | 3 | 2 | 1 | 0 |

A partir de la definición de la tabla de Cayley para la operación binaria de un grupo pueden deducirse ciertas propiedades que estas tienen, las cuales no demostraremos, entendiendo que pueden deducirse de fórmula fácil a partir de la definición de grupo:

- Si consideramos un grupo abeliano, su tabla de Cayley será una matriz simétrica.
- Todos los elementos del grupo aparecen en todas las filas o columnas de la tabla de Cayley, ya que en la Proposición 1.5 vimos que las ecuaciones $aX = b$ y $XA = b$ tenían que tener solución $\forall a, b \in G$, para que G fuese un grupo.
- Como para que G sea un grupo tiene que haber un elemento que actúe de neutro, esto se refleja en la tabla con un elemento que mantiene igual los encabezados en una fila y en una columna.

Definición 1.7 (Orden de un elemento). Sea $(G, \cdot, 1)$ un grupo, el orden de un elemento $x \in G$ es el menor $n \in \mathbb{N} \setminus \{0\}$ (en caso de existir) que verifica: $x^n = 1$. En cuyo caso, notaremos⁶: $O(x) = \text{ord}(x) = n$.

Si para un elemento $x \in G$ dicho n no existe, se dice que su orden es infinito: $O(x) = +\infty$.

⁵Entendiendo que en este caso hacemos uso de la notación multiplicativa.

⁶Podremos encontrarnos cualquiera de las dos notaciones.

Notación. Si consideramos un grupo con notación aditiva, $(G, +, 0)$, interpretando la anterior definición con esta notación diremos que $x \in G$ tendrá orden $n \in \mathbb{N} \setminus \{0\}$ si n es el menor natural no negativo de forma que verifica $n \cdot x = \sum_{i=1}^n x = 0$.

Proposición 1.8. Sea G un grupo, $x \in G$ con $O(x) = n$ y sea $m \in \mathbb{N} \setminus \{0\}$:

$$x^m = 1 \iff n \mid m$$

Demostración. Demostramos las dos implicaciones:

\implies) Si $O(x) = n$, entonces no puede ser $m < n$, ya que si no el orden de x no sería n sino m , por lo que $m \geq n$. En cuyo caso, $\exists q, r \in \mathbb{N}$ de forma que:

$$m = nq + r \quad \text{con } 0 \leq r < n$$

Pero entonces:

$$1 = x^m = x^{nq+r} = x^{nq}x^r = x^r \xrightarrow{(*)} r = 0$$

Donde en $(*)$ hemos usado que $r < n$, ya que si r no fuese 0, tendríamos que $O(x) = r$.

\impliedby) Si $n \mid m$, entonces $\exists q \in \mathbb{N}$ de forma que $m = qn$, luego:

$$x^m = x^{qn} = (x^n)^q = 1^q = 1$$

□

Proposición 1.9. Sea G un grupo, se verifica que:

1. $O(x) = 1 \iff x = 1$.
2. $O(x) = O(x^{-1}) \forall x \in G$.
3. Si $O(x) = +\infty$ para cierto $x \in G$, entonces todas las potencias de x son elementos distintos de G .
4. Si G es finito, entonces $O(x) \neq +\infty$ para todo $x \in G$.
5. Si $O(x) = n \in \mathbb{N} \setminus \{0\}$ para cierto $x \in G$, entonces x tiene n potencias distintas. Más aún, sean $p, q \in \mathbb{N}$ de forma que $x^p = x^q$ con $q > p$, entonces:

$$x^{q-p} = 1 \iff n \mid (q - p)$$

Demostración. Demostramos todas las propiedades:

1. Por doble implicación:

\impliedby) Trivial.

\implies) Si aplicamos la definición de $O(x)$ y de x^1 :

$$1 = x^1 = \prod_{i=1}^1 x = x$$

2. Distinguiamos dos casos:

- Fijado $x \in G$ con $O(x) = n$, entonces $x^n = 1$, por lo que:

$$x^{-1} = x^{n-1}$$

Veamos en primer lugar que $O(x^{-1}) \leq n$. Para ello, vemos que $(x^{-1})^n = 1$:

$$(x^{-1})^n = (x^{n-1})^n = x^{n(n-1)} = (x^n)^{n-1} = 1$$

Veamos ahora que $O(x^{-1}) \geq n$. Supongamos ahora que $O(x^{-1}) = k$, entonces:

$$(x^{-1})^k = 1 \implies x^{(n-1)k} = 1 \implies n \mid (n-1)k$$

Por tanto, como $n \nmid (n-1)$ y $\text{mcd}(n, n-1) = 1$, entonces $n \mid k$, por lo que $n \leq k = O(x^{-1})$. Por tanto, tenemos que:

$$n \leq O(x^{-1}) \leq n \implies O(x^{-1}) = n$$

- Si tenemos que $O(x) = +\infty$, por reducción al absurdo, supongamos que $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(x^{-1}) = n$.

Que $O(x) = +\infty$ significa que $\nexists m \in \mathbb{N} \setminus \{0\}$ de forma que $x^m = 1$.

Como $O(x^{-1}) = n$, tenemos que:

$$(x^{-1})^n = 1 \implies x = (x^{-1})^{-1} = (x^{-1})^{n-1}$$

De donde llegamos a que:

$$x^n = \left((x^{-1})^{n-1} \right)^n = ((x^{-1})^n)^{n-1} = 1^{n-1} = 1$$

Contradicción, puesto que $O(x) = +\infty$. Deducimos que si $O(x) = +\infty$, entonces ha de ser $O(x^{-1}) = +\infty$.

3. Por reducción al absurdo, supongamos que existen $p, q \in \mathbb{N}$ con $p < q$ de forma que $x^p = x^q$, luego:

$$x^{q-p} = 1$$

De donde deducimos que $O(x) < +\infty$, contradicción, luego $x^p \neq x^q$ para todo $p, q \in \mathbb{N}$ con $p \neq q$.

4. Por reducción al absurdo, supongamos que $\exists x \in G$ con $O(x) = +\infty$. En este caso, podemos construir una aplicación $\phi : \mathbb{N} \rightarrow G$ dada por $\phi(n) = x^n \forall n \in \mathbb{N}$. Esta aplicación es inyectiva gracias al punto 3, lo que contradice que G sea un grupo finito. Concluimos que $O(x) = n \in \mathbb{N} \setminus \{0\}$ para todo $x \in G$.

5. Si $O(x) = n$, consideramos la sucesión:

$$x, x^2, x^3, \dots, x^{n-1}, x^n = 1$$

Si seguimos calculando potencias, está claro que se repetirá este patrón, por lo que tratamos de ver que todos los elementos de la sucesión son distintos

entre sí. Por reducción al absurdo, supuesto que existen $p, q \in \mathbb{N}$ de forma que $p < q \leq n$ con $x^p = x^q$, entonces $x^{q-p} = 1$ con $q - p \leq n$, lo que contradice que $O(x) = n$.

Para ver que si $p, q \in \mathbb{N}$ con $x^p = x^q$, entonces:

$$x^{q-p} = 1 \iff n \mid (q - p)$$

Basta aplicar la Proposición 1.8 con $m = q - p$.

□

Ejemplo. Mostramos ahora ejemplos de órdenes de ciertos elementos en distintos grupos, entendiendo que cuando consideramos conjuntos susceptibles de ser anillos (conjuntos con suma y multiplicación), si dejamos el 0 en el conjunto consideramos el grupo con su suma ($e = 0$) y que cuando quitamos el 0 del conjunto consideramos el grupo con su multiplicación ($e = 1$).

1. Si cogemos $x \neq 1$ en $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con la multiplicación: $O(x) = +\infty$.
2. Si consideramos \mathbb{C} con su multiplicación: $O(i) = 4$, ya que $i^4 = 1$.
3. En \mathbb{Z}_9 , $O(\bar{6}) = 3$:

$$\begin{aligned}\bar{6} &\neq \bar{0} \\ \overline{6+6} &= \overline{12} = \bar{3} \neq \bar{0} \\ \overline{6+6+6} &= \overline{18} = \bar{0}\end{aligned}$$

4. En $\mathbb{Z}_7^* = \mathcal{U}(\mathbb{Z}_7)$:

$$\blacksquare O(\bar{2}) = 3:$$

$$\begin{aligned}\bar{2} &\neq \bar{1} \\ \overline{2 \cdot 2} &= \bar{4} \neq \bar{1} \\ \overline{2 \cdot 2 \cdot 2} &= \bar{8} = \bar{1}\end{aligned}$$

$$\blacksquare O(\bar{3}) = 6.$$

$$\begin{aligned}\bar{3} &\neq \bar{1} \\ \overline{3 \cdot 3} &= \bar{9} = \bar{2} \neq \bar{1} \\ \overline{3 \cdot 3 \cdot 3} &= \overline{27} = \bar{6} \neq \bar{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3} &= \overline{81} = \bar{3} \neq \bar{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} &= \overline{243} = \bar{5} \neq \bar{1} \\ \overline{3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3} &= \overline{729} = \bar{1}\end{aligned}$$

1.1. Grupos diédricos D_n

A continuación, estaremos interesados en el estudio de una familia⁷ de grupos conocida como los “grupos diédricos”, cuyo estudio se desarrollará a lo largo de la asignatura.

⁷Donde con “familia” hacemos referencia a un conjunto de grupos que guardan cierta similitud entre ellos.

1.1.1. Motivación

Para entender estos grupos, conviene destacar la forma en la que surgieron ciertos objetos geométricos que luego fueron interesantes desde el punto de vista algebraico, por formar un grupo.

Ejemplo. Si pensamos en un triángulo rectángulo (el menor polígono regular) sobre el plano centrado en el origen como el de la Figura 1.1, donde hemos numerado los vértices del mismo, es interesante preguntarnos sobre las isometrías del plano en el plano que dejan invariante al mismo.

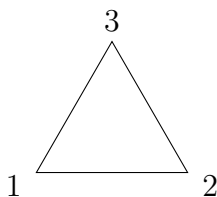


Figura 1.1: Triángulo equilátero con centro en el origen de coordenadas.

En Geometría II se vio que las únicas isometrías que podemos considerar en el plano son los giros y las simetrías axiales o centrales, por lo que procedemos a distinguir casos:

Giros. Como vemos en la Figura 1.2, de forma intuitiva vemos que giros (pensando que todos son en sentido antihorario) que dejan el triángulo invariante solo hay 3:

- El giro de ángulo $\frac{2\pi}{3}$.
- El giro de ángulo $\frac{4\pi}{3}$.
- El giro de ángulo 2π .

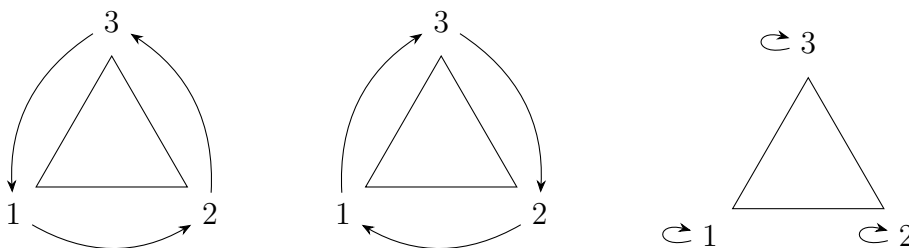


Figura 1.2: Todos los giros que dejan invariante al triángulo.

Simetrías. Como vemos en la Figura 1.3, de forma intuitiva vemos que hay 3 simetrías axiales que dejan invariante al triángulo y que no hay ninguna simetría central que lo deje invariante:

- La simetría respecto a la mediatriz del segmento 2, 3.
- La simetría respecto a la mediatriz del segmento 3, 1.

- La simetría respecto a la mediatriz del segmento 1, 2.

Notemos la forma en la que hemos nombrado las rectas respecto a las cuales se hace la simetría: la recta l_i contiene al vértice i -ésimo.

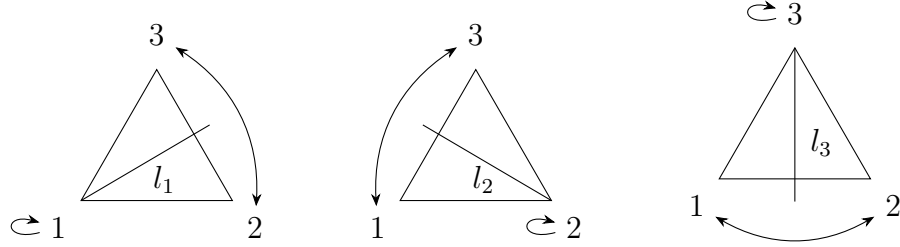


Figura 1.3: Todas las reflexiones que dejan invariante al triángulo.

Con el fin de estudiar las isometrías que mantienen polígonos regulares en el plano, conviene introducir las siguientes definiciones y notaciones:

Definición 1.8 (Permutación). Sea X un conjunto, una permutación del mismo es cualquier aplicación biyectiva $f : X \rightarrow X$.

Si X es el conjunto $\{1, 2, \dots, n\}$, es usual notar:

$$S_n = \text{Perm}(X) = \{f : X \rightarrow X \mid f \text{ es una permutación}\}$$

Definición 1.9 (Ciclo). Sea $\{a_1, a_2, \dots, a_m\} \subseteq \{1, 2, \dots, n\}$, un ciclo de longitud $m \leq n$ es una permutación $\sigma \in S_n$ de forma que:

1. $\sigma(a_i) = a_{i+1}$ para todo $i \in \{1, \dots, m-1\}$.
2. $\sigma(a_m) = a_1$.
3. $\sigma(a_j) = a_j$ para todo $a_j \notin \{a_1, a_2, \dots, a_m\}$.

En dicho caso, representaremos a σ por:

$$\sigma = (a_1 \ a_2 \ \dots \ a_m)$$

Observación. Notemos que podemos notar a un ciclo de longitud m , σ , de m formas distintas:

$$\sigma = (a_1 \ a_2 \ \dots \ a_m) = (a_2 \ \dots \ a_m \ a_1) = \dots = (a_m \ a_1 \ a_2 \ \dots \ a_{m-1})$$

De esta forma, el número de ciclos de longitud m son todas las posibles combinaciones de los m elementos entre n , pero como cada vez aparecen m :

$$\frac{V_m^n}{m}$$

A los 2-ciclos los llamaremos transposiciones.

Ejemplo. Para familiarizarnos con los ciclos, observamos que:

- En S_3 , los ciclos de longitud 2 que podemos considerar son: $(1\ 2)$, $(1\ 3)$ y $(2\ 3)$. Estos se interpretan respectivamente como:
 - Mantener el 3 fijo e intercambiar el 1 con el 2.
 - Mantener el 2 fijo e intercambiar el 1 con el 3.
 - Mantener el 1 fijo e intercambiar el 2 con el 3.
- En S_3 , los únicos ciclos de longitud 3 que podemos considerar son: $(1\ 2\ 3)$ y $(3\ 2\ 1)$, cuya definición debe estar clara.

Notación. Es claro que no toda permutación es un ciclo, basta considerar la aplicación identidad. Sin embargo, hay ciertas permutaciones como por ejemplo la aplicación $\sigma : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ dada por:

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

Que restringida a $\{1, 2\}$ da el ciclo $(1\ 2)$ y que restringida al $\{3, 4\}$ da el ciclo $(3\ 4)$. Será usual denotar permutaciones como esta por⁸:

$$\sigma = (1\ 2)(3\ 4)$$

Aprovechando la notación para los ciclos previamente definida, si por ejemplo extendemos σ a $\{1, 2, 3, 4, 5\}$ definiendo:

$$\sigma(5) = 5$$

Entonces, la notación para σ será la misma: $(1\ 2)(3\ 4)$, ya que el 5 “no se mueve”.

Ejemplo. Volviendo al ejemplo anterior del triángulo y de las isometrías que lo dejan invariante, si notamos por:

- r al giro de ángulo $\frac{2\pi}{3}$.
- s a la simetría axial cuya recta pasa por el vértice 1.

Puede comprobarse de forma geométrica que a partir de composiciones de r y de s obtenemos los otros 4 movimientos restantes (notaremos la composición de aplicaciones por yuxtaposición, ya que estamos buscando un grupo con estas aplicaciones):

- El giro de ángulo $\frac{4\pi}{3}$ es $r^2 = rr$.
- El giro de ángulo 2π es r^3 .
- La simetría respecto a la recta l_2 es sr^2 .

⁸Más adelante formalizaremos bien esta notación, aunque por ahora empecemos a usarla desde un punto de vista más intuitivo.

- La simetría respecto a la recta l_3 es sr .

Notemos que el giro de ángulo 2π es la identidad, que es el elemento neutro para la composición, por lo que el elemento neutro del futuro grupo que definamos será r^3 , que podemos denotar por 1. Además, la composición de aplicaciones es una operación asociativa y se deja como ejercicio demostrar que cada elemento del conjunto:

$$D_3 = \{1, r, r^2, s, sr, sr^2\}$$

Tiene un elemento simétrico respecto de la composición. Podemos ver que $(D_3, \circ, 1)$ es un grupo.

Ejemplo. Continuando con la motivación para los grupos diédricos, nos preguntamos ahora qué pasa si en vez de considerar las isometrías que mantienen invariante a un triángulo equilátero, consideramos las isometrías del plano que mantienen invariantes los vértices de un cuadrado sobre el plano; un cuadrado como el de la Figura 1.4.

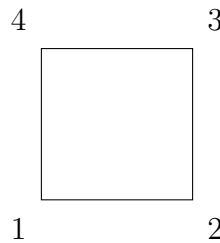


Figura 1.4: Cuadrado con centro en el origen de coordenadas.

Es fácil ver que las únicas isometrías que dejan invariante al cuadrado son (Véase la Figura 1.5):

- Los giros de ángulos $\frac{\pi}{2}$, π , $\frac{3\pi}{2}$ y 2π .
- Las simetrías axiales respecto a las rectas:
 - La recta que une los vértices 1 y 3.
 - La recta que une los vértices 2 y 4.
 - La recta que es mediatriz del segmento 1, 2.
 - La recta que es mediatriz del segmento 2, 3.

Todos estos movimientos pueden verse como aplicaciones lineales $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ tal y como se hace en geometría o aprovecharnos de que todas ellas mantienen el cuadrado invariante, por lo que podemos pensar en ellas como si fueran permutaciones del conjunto $\{1, 2, 3, 4\}$. Aprovechando esta dualidad, vemos que:

- El giro de ángulo $\frac{\pi}{2}$ es $(1\ 2\ 3\ 4)$.
- El giro de ángulo π es $(1\ 3)(2\ 4)$.
- El giro de ángulo $\frac{3\pi}{2}$ es $(1\ 4\ 3\ 2)$.



Figura 1.5: Giros y simetrías que dejan invariante al cuadrado

- El giro de ángulo 2π es la identidad, (1).
- La simetría respecto a la recta que une 1 y 3 es (2 4).
- La simetría respecto a la recta que une 2 y 4 es (1 3).
- La simetría respecto a la mediatriz de 1 y 2 es (1 2)(3 4).
- La simetría respecto a la mediatriz de 2 y 3 es (1 4)(2 3).

Dejamos como ejercicio hacer esta correspondencia (notar las isometrías como su correspondiente permutación) con los movimientos que teníamos en el triángulo. Si ahora hacemos como hicimos anteriormente con el triángulo y notamos por:

- r al giro de ángulo $\frac{\pi}{2}$.
- s a la reflexión respecto a la recta que pasa por el vértice 1.

Podemos obtener los otros 6 movimientos (o permutaciones desde el punto de vista algebraico) con la composición de r y s :

- r^2 es (1 3)(2 4).
- r^3 es (1 4 3 2).
- r^4 es 1 (la aplicación identidad).
- sr es (1 4)(2 3).
- sr^2 es (1 3).
- sr^3 es (1 2)(3 4).

De esta forma, si consideramos el conjunto:

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

Tenemos que $(D_4, \circ, 1)$ es un grupo. Más aún, podemos completar su tabla de Cayley para observar cómo se comporta \circ dentro de D_4 :

| \circ | 1 | r | r^2 | r^3 | s | sr | sr^2 | sr^3 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|
| 1 | 1 | r | r^2 | r^3 | s | sr | sr^2 | sr^3 |
| r | r | r^2 | r^3 | 1 | sr^3 | s | sr | sr^2 |
| r^2 | r^2 | r^3 | 1 | r | sr^2 | sr^3 | s | sr |
| r^3 | r^3 | 1 | r | r^2 | sr | sr^2 | sr^3 | s |
| s | s | sr | sr^2 | sr^3 | 1 | r | r^2 | r^3 |
| sr | sr | sr^2 | sr^3 | s | r^3 | 1 | r | r^2 |
| sr^2 | sr^2 | sr^3 | s | sr | r^2 | r^3 | 1 | r |
| sr^3 | sr^3 | s | sr | sr^2 | r | r^2 | r^3 | 1 |

1.1.2. Definición y primeras propiedades

Una vez comprendida la motivación de los grupos diédricos, estamos preparados para dar su definición. No demostraremos que, dado $n \in \mathbb{N}$, el conjunto de isometrías que dejan invariante al polígono regular de n lados forma un grupo si consideramos sobre dicho conjunto la composición de aplicaciones, ya que no es interesante para esta asignatura.

Sin embargo, aceptaremos la definición como válida (animamos al lector a investigar más sobre los grupos diédricos y su definición) y procedemos a destacar las propiedades algebraicas de estos grupos, que es lo que nos interesa.

Definición 1.10 (Grupos diédricos D_n). Sea D_n el conjunto de isometrías que dejan invariante al polígono regular de n lados. Sabemos que D_n tiene $2n$ elementos:

- n rotaciones de ángulo $\frac{2k\pi}{n}$, con $k \in \{1, \dots, n\}$.
- n simetrías axiales:
 - Si n es par, tenemos:
 - $n/2$ simetrías respecto a las mediatrices.
 - $n/2$ simetrías respecto a unir vértices opuestos.
 - Si n es impar, tenemos n simetrías respecto a las mediatrices.

Se verifica que $(D_n, \circ, 1)$ es un grupo. Además, destacamos dos elementos suyos:

- r , la rotación de ángulo $\frac{2\pi}{n}$.
- s , la simetría axial respecto a la recta que pasa por el origen de coordenadas y el vértice nombrado 1.

De esta forma, todos los elementos de D_n son:

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

Proposición 1.10. Dado $n \in \mathbb{N}$, en D_n se cumple que:

1. $1, r, r^2, \dots, r^{n-1}$ son todos distintos y $r^n = 1$, es decir, $O(r) = n$.

2. $s^2 = 1$.
3. $s \neq r^i, \forall 0 \leq i \leq n-1$.
4. sr^i con $0 \leq i \leq n-1$ son simetrías.
5. $sr^i \neq sr^j$ para todo $i \neq j$, con $i, j \in \{1, \dots, n-1\}$.
6. $sr = r^{-1}s$.
7. $sr^i = r^{-i}s$.

Demostración. Demostramos cada una de las propiedades:

1. La primera parte es competencia de Geometría. Para la segunda, basta ver que r^n es componer n veces el giro de ángulo $\frac{2\pi}{n}$, que es lo mismo que considerar el giro de ángulo $n \cdot \frac{2\pi}{n} = 2\pi$, que es la identidad.
2. Es competencia de Geometría.
3. Es competencia de Geometría, que puede probarse de distintas formas:
 - Viendo que s tiene puntos fijos y r^i no.
 - Viendo que s es un movimiento inverso y que r^i es directo.
4. Es competencia de Geometría.
5. Basta aplicar 1.
- 6, 7. Son competencia de Geometría.

□

Usaremos los resultados de la Proposición 1.10 con frecuencia, como las propiedades básicas de los grupos diédricos. Notemos que a partir de estas puede construirse la tabla de Cayley para cualquier grupo diédrico D_n .

Ejercicio. Construya la tabla de Cayley para D_4 y D_5 usando los resultados de la Proposición 1.10.

1.2. Generadores de un grupo

Definición 1.11 (Conjunto de generadores de un grupo). Sea G un grupo, diremos que $S \subseteq G$ es un conjunto de generadores de G si todo elemento $x \in G$ puede escribirse como producto finito de elementos de S y de sus inversos. En dicho caso, notaremos: $G = \langle S \rangle$.

Si S es un conjunto finito, $S = \{x_1, x_2, \dots, x_n\} \subseteq G$, podemos escribir:

$$G = \langle x_1, x_2, \dots, x_n \rangle$$

Y diremos que G es finitamente generado.

Si S está formado solo por un elemento, diremos que G es un grupo cíclico.

Observación. Sea G un grupo y $S \subseteq G$, equivalen:

i) S es un conjunto de generadores de G .

ii) Dado $x \in G$, $\exists x_1, x_2, \dots, x_p \in S$ de forma que:

$$x = x_1^{\gamma_1} x_2^{\gamma_2} \dots x_p^{\gamma_p} \quad \gamma_i \in \mathbb{Z}, \quad i \in \{1, \dots, p\}$$

Ejemplo. Como ejemplos a destacar, vemos que:

1. $\mathbb{Z} = \langle 1 \rangle$ si pensamos en $(\mathbb{Z}, +, 0)$, ya que dado $x \in \mathbb{Z}$:

■ Si $x > 0$, entonces:

$$x = \underbrace{1 + 1 + \dots + 1}_{x \text{ veces}}$$

■ Si $x < 0$, entonces (-1 es el simétrico de 1):

$$x = \underbrace{-1 - 1 - \dots - 1}_{x \text{ veces}}$$

■ Si $x = 0$, consideramos la suma de 0 elementos.

2. $D_n = \langle r, s \rangle$.

Definición 1.12 (Presentación de un grupo). Sea G un grupo y $S \subseteq G$, si $G = \langle S \rangle$ y existe un conjunto de relaciones R_1, R_2, \dots, R_m (igualdades entre elementos de S , $\{1\}$ y los elementos simétricos de S) tal que cualquier relación entre los elementos de S puede deducirse de estas, entonces, decimos que estos generadores y relaciones constituyen una presentación de G , notado:

$$G = \langle S \mid R_1, R_2, \dots, R_n \rangle$$

Ejemplo. Veamos algunos ejemplos de presentaciones, observando que dar una presentación es equivalente a dar la definición del propio grupo, ya que a partir de la presentación pueden deducirse todos los elementos del grupo y las relaciones que estos guardan entre sí.

1. En el diédrico D_n , tenemos que:

$$D_n = \langle r, s \mid rs = sr^{-1}, r^n = 1, s^2 = 1 \rangle$$

2. $D_1 := \langle s \mid s^2 = 1 \rangle$.

En este caso, vemos que $D_1 = \{s\}$.

3. $D_2 := \langle r, s \mid r^2 = s^2 = 1, sr = rs \rangle$.

Ahora, tenemos: $D_2 = \{1, r, s, rs\}$.

4. $C_n = \langle x \mid x^n = 1 \rangle$ es un grupo cíclico de orden n .

Vemos que: $C_n = \{1, x, x^2, x^3, \dots, x^{n-1}\}$

5. $V^{\text{abs}} = \langle x, y \mid x^2 = 1, y^2 = 1, (xy)^2 = 1 \rangle$ es el grupo de Klein abstracto.

En primer lugar, sabemos que $\{1, x, y\} \subseteq V^{\text{abs}}$. Como x e y son de orden 2, sabemos que $x^{-1} = x$ y que $y^{-1} = y$. Además, vemos que $xy \in V^{\text{abs}}$ y que:

$$(xy)^2 = 1 \iff xyxy = 1 \iff xy = yx$$

Por lo que xy también está en V^{abs} , con $(xy)^{-1} = yx$. Vemos que no hay más elementos que puedan estar en V^{abs} , con lo que:

$$V^{\text{abs}} = \{1, x, y, xy\}$$

Observamos que el grupo nos recuerda a D_2 .

6. $Q_2^{\text{abs}} = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$.

Inicialmente, $\{1, x, y\} \subseteq Q_2^{\text{abs}}$. De la primera relación vemos que también tenemos $\{x^2, x^3\} \subseteq Q_2^{\text{abs}}$. Reescribimos la última relación, para buscar más elementos de forma cómoda:

$$yxy^{-1} = x^{-1} \iff yx = x^{-1}y$$

Como yx no guarda ninguna relación con x e y , sabemos que también está en el grupo, junto con yx^2 y yx^3 . De esta forma:

$$Q_2^{\text{abs}} = \{1, x, x^2, x^3, y, yx, yx^2, yx^3\}$$

Observamos también que el grupo nos recuerda a D_4 .

Ejemplo. Las similitudes que hemos encontrado entre distintos grupos como entre V^{abs} y D_2 o entre Q_2^{abs} y D_4 las formalizaremos con ayuda de un concepto algebraico que luego definiremos, pero merece la pena destacar ahora una similitud entre Q_2^{abs} , el grupo de los cuaternios $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ y unos elementos del grupo $\text{SL}_2(\mathbb{C})$. Para familiarizarnos con los cuaternios, estos cumplen que:

$$\begin{aligned} i^2 &= j^2 = k^2 = -1 \\ ij &= k & jk &= i & ki &= j \\ ji &= -k & kj &= -i & ik &= -j \end{aligned}$$

Productos que pueden recordarse observando la Figura 1.6

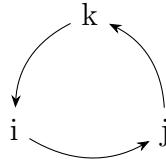


Figura 1.6: Dirección en la que se multiplican los cuaternios de forma positiva.

Se deja como ejercicio ver en qué forma podemos entender que los grupos Q_2 , Q_2^{abs} y el subconjunto de matrices de $\text{SL}_2(\mathbb{C})$ con la operación heredada del mismo:

$$C = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\} \subseteq \text{SL}_2(\mathbb{C})$$

Si pensamos en relacionar los elementos de la Tabla 1.1.

| Q_2^{abs} | C | Q_2 |
|--------------------|--|-------|
| 1 | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | 1 |
| x | $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ | i |
| y | $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ | j |
| x^2 | $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ | -1 |
| x^3 | $\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$ | $-i$ |
| xy | $\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ | k |
| x^2y | $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ | $-j$ |
| x^3y | $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ | $-k$ |

Tabla 1.1: Elementos que se relacionan.

1.3. Grupos Simétricos S_n

Recordamos que dado un conjunto X , podemos considerar el conjunto de todas sus permutaciones:

$$S(X) = \{f : X \rightarrow X \mid f \text{ biyectiva}\}$$

Definición 1.13 (Grupos Simétricos S_n). Dado $n \in \mathbb{N}$, consideramos $X = \{1, 2, \dots, n\}$ y definimos $S_n = S(X)$, el conjunto de todas las permutaciones de X . Se verifica que S_n junto con la operación de composición de aplicaciones es un grupo:

- La composición de aplicaciones es asociativa.
- La aplicación $id : X \rightarrow X$ es el elemento neutro.
- Como las permutaciones son biyecciones, cada una tiene su elemento simétrico.

Llamaremos a (S_n, \circ, id) el n -ésimo grupo simétrico, que recordamos tiene orden:

$$|S_n| = n!$$

Notación. Estaremos interesados en ver cómo se comportan de forma algebraica las permutaciones de conjuntos de n elementos, por lo que tendremos que conocer en cada caso cuáles son las aplicaciones con las que estamos trabajando.

Para abreviar, en muchos casos usaremos la notación matricial de las permutaciones. Sea $\sigma \in S_n$, sabemos que dar σ es equivalente a dar $\sigma(a)$ para cualquier $a \in X$. De esta forma, podemos dar una matriz $n \times n$ de la forma:

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

Observemos que, conocida la matriz anterior, conocemos σ .

Ejemplo. En este ejemplo, vemos los grupos simétricos más pequeños:

1. Si consideramos S_0 , son todas las permutaciones del \emptyset en el \emptyset , que solo hay una: $\sigma : \emptyset \rightarrow \emptyset$.
2. Si consideramos S_1 , solo hay una permutación: $id : \{1\} \rightarrow \{1\}$.
3. En S_2 , tenemos $S_2 = \{\sigma_1, \sigma_2\}$, con:

$$\sigma_1 = id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Hasta ahora, todos estos grupos son abelianos.

4. En S_3 , tenemos:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Que ya es un ejemplo de grupo simétrico no abeliano, ya que si tomamos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Vemos que $\sigma\tau \neq \tau\sigma$:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \tau\sigma$$

De esta forma, acabamos de probar que S_n con $n \geq 3$ no es abeliano, ya que si estamos en S_n , podemos considerar las extensiones de σ y τ a S_n :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$$

Y tendremos que $\sigma\tau \neq \tau\sigma$.

Ejemplo. Sean $s_1, s_2 \in S_7$ dadas por:

$$s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 4 & 3 \end{pmatrix}, \quad s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 1 & 7 & 6 \end{pmatrix}$$

Se pide calcular s_1s_2 , s_2s_1 y s_2^2 .

$$s_1s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 2 & 3 & 5 & 4 \end{pmatrix} \\ s_2s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 1 & 5 & 3 & 4 \end{pmatrix} \\ s_2^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 7 & 5 & 2 & 6 \end{pmatrix}$$

Proposición 1.11. *Se verifica que:*

1. Dado $\sigma \in S_n$, existe $m \in \mathbb{N}$ de forma que $\sigma^{m+1}(x) = x$, $\forall x \in X = \{1, \dots, n\}$.
2. Todo ciclo es una permutación.
3. El orden de un ciclo de longitud m es m .
4. Si $\sigma = (x_1 \ x_2 \ \dots \ x_{m-1} \ x_m)$, entonces: $\sigma^{-1} = (x_m \ x_{m-1} \ \dots \ x_2 \ x_1)$.

Demostración. Demostramos cada propiedad:

1. Por la Proposición 1.9, como S_n es un grupo finito, sabemos que $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(\sigma) = n$. Tomando $m = n - 1$, tenemos que:

$$\sigma^{m+1}(x) = \sigma^n(x) = x \quad \forall x \in X$$

2. Se tiene directamente por la definición de ciclo.
3. Sea $\sigma \in S_n$ un ciclo de longitud m :

$$\sigma = (x_1 \ x_2 \ \dots \ x_m) \quad x_1, x_2, \dots, x_m \in X$$

Queremos ver que $O(\sigma) = m$. Para ello:

- En primer lugar, veamos que $\sigma^m = 1$:
 - Si $x \in X$ con $x \neq x_i$ para todo $i \in \{1, \dots, m\}$, entonces $\sigma(x) = x$, luego:

$$\sigma^m(x) = \sigma^{m-1}(\sigma(x)) = \sigma^{m-1}(x) = \sigma^{m-2}(\sigma(x)) = \dots = x$$

- Si ahora consideramos x_i con $i \in \{1, \dots, m\}$, tendremos que:

$$x_i \xrightarrow{\sigma} x_{i+1} \xrightarrow{\sigma} \dots \xrightarrow{\sigma} x_{m-1} \xrightarrow{\sigma} x_m \xrightarrow{\sigma} x_1 \xrightarrow{\sigma} \dots \xrightarrow{\sigma} x_{i-1} \xrightarrow{\sigma} x_i$$

$\underbrace{\hspace{10em}}_{\sigma^{m-i}} \qquad \underbrace{\hspace{10em}}_{\sigma^i}$

$$\text{Luego: } 1 = \sigma^{m-i} \sigma^i = \sigma^{m-i+i} = \sigma^m$$

- Supongamos ahora que existe $k < m$ de forma que $\sigma^k = 1$, esto significaría que $\sigma^k(x_1) = x_1$, pero como σ es un ciclo de longitud m , se tiene que $\sigma^k(x_1) = x_k$ y $x_k \neq x_1$, contradicción, con lo que $k \geq m$.
4. Recordamos por la definición de ciclo que si $\sigma = (a_1 \ a_2 \ \dots \ a_{m-1} \ a_m)$, entonces se ha de cumplir que:

$$\begin{aligned} \sigma(x) &= x & x \neq x_i, \quad i \in \{1, \dots, m\} \\ \sigma(x_i) &= x_{i+1} & i \in \{1, \dots, m-1\} \\ \sigma(x_m) &= x_1 \end{aligned}$$

Si vemos σ como aplicación y tratamos de buscarle su aplicación inversa σ^{-1} , esta ha de cumplir que:

$$\begin{aligned} \sigma^{-1}(x) &= x & x \neq x_i, \quad i \in \{1, \dots, m\} \\ \sigma^{-1}(x_{i+1}) &= x_i & i \in \{1, \dots, m-1\} \\ \sigma^{-1}(x_1) &= x_m \end{aligned}$$

Sin embargo, vemos que entonces σ^{-1} también es un ciclo:

$$\sigma^{-1} = (x_m \ x_{m-1} \ \dots \ x_2 \ x_1)$$

□

Con el siguiente teorema veremos que los ciclos son una parte interesante de los grupos simétricos, tanto que cualquier permutación pueda expresarse como una composición de ciertos ciclos de longitud mayor o igual que 2. Para ello, será necesario primero realizar una definición:

Definición 1.14 (Ciclos disjuntos). Sean $\sigma_1, \sigma_2 \in S_n$ ciclos, decimos que son disjuntos si no existe $i \in X = \{1, 2, \dots, n\}$ de forma que:

$$\sigma_1(i) = j, \quad \sigma_2(i) = k \quad \text{con } j, k \in X, i \neq j \neq k \neq i$$

Es decir, si no hay ningún elemento que se mueva en ambos ciclos.

Ejemplo. Ejemplos de ciclos disjuntos son:

$$\sigma_1 = (1 \ 3 \ 5), \quad \sigma_2 = (2 \ 4 \ 6), \quad \sigma_3 = (7 \ 8)$$

Un ejemplo de dos ciclos que no son disjuntos son:

$$\tau_1 = (1 \ 3 \ 5 \ 8), \quad \tau_2 = (2 \ 4 \ 5 \ 9)$$

Ya que $\tau_1(5) = 8$ y $\tau_2(5) = 9$, con $5 \neq 8 \neq 9 \neq 5$. Es decir, el 5 se mueve en ambos ciclos.

Teorema 1.12. Toda permutación $\sigma \in S_n$ con $\sigma \neq 1$ se expresa en la forma:

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_k$$

siendo los γ_i con $i \in \{1, \dots, k\}$ ciclos disjuntos de longitud mayor o igual que 2. Además, dicha descomposición es única, salvo el orden de los factores.

Demostración. Supuesto que estamos trabajando con permutaciones sobre el conjunto $X = \{1, 2, \dots, n\}$, sea $\sigma \in S_n$ con $\sigma \neq 1$, definimos la relación:

$$yRx \iff \exists m \in \mathbb{Z} \mid y = \sigma^m(x)$$

Que es una relación de equivalencia:

- Propiedad reflexiva. Se tiene gracias a la Proposición 1.11.
- Propiedad simétrica. Sean $x, y \in X$ de forma que yRx , tenemos que $\exists m \in \mathbb{Z}$ de forma que $y = \sigma^m(x)$, pero entonces:

$$\sigma^{-m}(y) = \sigma^{-m}(\sigma^m(x)) = x \implies xRy$$

- Propiedad transitiva. Sean $x, y, z \in X$ de forma que yRx y que zRx , entonces: $\exists p, q \in \mathbb{Z}$ de forma que:

$$\left. \begin{array}{l} y = \sigma^p(x) \\ z = \sigma^q(y) \end{array} \right\} \implies z = \sigma^q(\sigma^p(x)) = \sigma^{p+q}(x) \implies zRx$$

De esta forma, dado $x \in X$, podemos considerar su clase de equivalencia:

$$\bar{x} = \{\sigma^m(x) \mid m \in \mathbb{Z}\} \in X/R$$

Que es un conjunto finito, ya que gracias a la Proposición 1.11, existe $m \in \mathbb{N}$ de forma que $\sigma^{m+1}(x) = x$, con lo que:

$$C_x = \bar{x} = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^m(x)\}$$

Si consideramos ahora el ciclo:

$$\gamma_x = (x \ \sigma(x) \ \sigma^2(x) \ \dots \ \sigma^m(x)) \in S_n$$

Tenemos que:

$$\gamma_x(y) = \begin{cases} \sigma(y) & \text{si } y \in C_x \\ y & \text{si } y \notin C_x \end{cases}$$

De esta forma, tenemos una partición de X en clases de equivalencia, cada una de las C_x con $x \in X$, que llevan asociado un ciclo γ_x .

1. Sean $\bar{i}, \bar{j} \in X/R$ con $\bar{i} \neq \bar{j}$, entonces los elementos que se mueven en γ_i son los elementos de C_i , mientras los elementos que se mueven en γ_j son los de C_j . Como se tiene que $C_i \cap C_j = \emptyset$ por ser C_i y C_j clases de equivalencia distintas, llegamos a que γ_i y γ_j son ciclos disjuntos, para $\bar{i} \neq \bar{j}$.
2. Sea $\tau = \gamma_1 \gamma_2 \dots \gamma_n$, sea $y \in X$, entonces:

$$\tau(y) = \gamma_1 \gamma_2 \dots \gamma_n(y) = \gamma_1 \gamma_2 \dots \gamma_y(y) = \gamma_1 \gamma_2 \dots \gamma_{y-1}(\sigma(y)) = \gamma_1(\sigma(y)) = \sigma(y)$$

Ya que anteriormente vimos que:

$$\gamma_j(y) = \begin{cases} \sigma(y) & \text{si } y \in C_j \\ y & \text{si } y \notin C_j \end{cases} \quad \forall j \in X$$

Y se verifica que $y, \sigma(y) \in C_y$. Por tanto, tenemos que $\tau = \sigma$. Si ahora despreciamos de la expresión de τ los ciclos de longitud menor que 2, la permutación σ no cambia y tenemos que σ se expresa como producto de ciclos disjuntos (por el apartado 1) de longitud mayor o igual que 2. \square

Notación. A partir del Teorema 1.12, podemos introducir una nueva notación basada en los ciclos disjuntos. Dado $\sigma \in S_n$, como existe una única descomposición en ciclos disjuntos:

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_k$$

Teníamos una notación estandar para cada ciclo. Ahora podemos notar σ como el producto de todas esas notaciones.

Como acabamos de decir, a partir del Teorema 1.12, podremos notar a las permutaciones como su descomposición en ciclos disjuntos. Sin embargo, merece la pena preguntarse sobre el orden de los ciclos en esta descomposición, pregunta a la que contestamos con la siguiente proposición:

Proposición 1.13. *Se verifican:*

1. Si $\gamma_1, \gamma_2 \in S_n$ son dos ciclos disjuntos, entonces:

$$\gamma_1\gamma_2 = \gamma_2\gamma_1$$

Es decir, el producto de ciclos disjuntos es conmutativo.

2. Sea $\sigma \in S_n$ una permutación, si consideramos su descomposición en ciclos disjuntos:

$$\sigma = \gamma_1\gamma_2 \dots \gamma_k$$

Entonces, se tiene que:

$$\sigma^{-1} = \gamma_1^{-1}\gamma_2^{-1} \dots \gamma_k^{-1}$$

Demostración. Demostramos cada uno de los resultados:

1. Supongamos que:

$$\gamma_1 = (x_1 \ x_2 \ \dots \ x_n), \quad \gamma_2 = (y_1 \ y_2 \ \dots \ y_m)$$

$$x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m \in X \text{ todos ellos distintos}$$

Tenemos entonces que:

- Si $x \neq x_i, x \neq y_j$ para $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$:

$$\gamma_1(\gamma_2(x)) = \gamma_1(x) = x = \gamma_2(x) = \gamma_2(\gamma_1(x))$$

- Si consideramos $i \in \{1, \dots, n-1\}$:

$$\gamma_1(\gamma_2(x_i)) = \gamma_1(x_i) = x_{i+1} = \gamma_2(x_{i+1}) = \gamma_2(\gamma_1(x_i))$$

Donde hemos usado que $x_i \neq y_j$ para todo $j \in \{1, \dots, m\}$.

- Si consideramos ahora $j \in \{1, \dots, m-1\}$:

$$\gamma_1(\gamma_2(y_j)) = \gamma_1(y_{j+1}) = y_{j+1} = \gamma_2(y_j) = \gamma_2(\gamma_1(y_j))$$

Donde hemos usado que $y_j \neq x_i$ para todo $i \in \{1, \dots, n\}$.

- Faltan los casos de x_n y y_m , que son análogos:

$$\gamma_1(\gamma_2(x_n)) = \gamma_1(x_n) = x_1 = \gamma_2(x_1) = \gamma_2(\gamma_1(x_n))$$

$$\gamma_1(\gamma_2(y_m)) = \gamma_1(y_1) = y_1 = \gamma_2(y_m) = \gamma_2(\gamma_1(y_m))$$

Como hemos visto que $\gamma_1(\gamma_2(x)) = \gamma_2(\gamma_1(x))$ para todo $x \in X$, concluimos que $\gamma_1\gamma_2 = \gamma_2\gamma_1$.

2. Dado $\sigma = \gamma_1\gamma_2 \dots \gamma_k$, buscamos una permutación $\tau \in S_n$ que verifique que:

$$\sigma\tau = \gamma_1\gamma_2 \dots \gamma_{k-1}\gamma_k\tau = 1$$

Observamos que como τ podemos tomar:

$$\tau = \gamma_k^{-1}\gamma_{k-1}^{-1} \dots \gamma_2^{-1}\gamma_1^{-1}$$

sin embargo, como los γ_i con $i \in \{1, \dots, k\}$ eran ciclos disjuntos, por la Proposición 1.11, sabemos que los γ_i^{-1} también seguirán siendo ciclos disjuntos y por 1 sabemos que su producto es conmutativo, por lo que podemos escribir:

$$\tau = \gamma_1^{-1} \gamma_2^{-1} \dots \gamma_k^{-1}$$

Como $\sigma\tau = 1$, concluimos que $\tau = \sigma^{-1}$.

□

Ejemplo. En S_{13} , consideramos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$$

De forma por ciclos disjuntos, podemos notar:

$$\sigma = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9)$$

Dada una permutación en notación de ciclos disjuntos, sabemos que para calcular la permutación inversa basta calcular la inversa de cada uno de los ciclos:

$$\sigma^{-1} = (4 \ 10 \ 8 \ 12 \ 1)(2 \ 13)(7 \ 11 \ 5)(6 \ 9)$$

Del Teorema 1.12 deducimos el siguiente corolario:

Corolario 1.13.1. *El orden de una permutación $\sigma \in S_n$ es el mínimo común múltiplo de las longitudes de los ciclos disjuntos en los que se descompone.*

Demostración. Supongamos que σ se descompone de la forma:

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_k$$

como $\gamma_i \gamma_j = \gamma_j \gamma_i$ para $i, j \in \{1, \dots, k\}$, tenemos que $\forall m \in \mathbb{N}$:

$$\sigma^m = \gamma_1^m \gamma_2^m \dots \gamma_k^m$$

Si $m = O(\sigma)$, entonces:

$$\sigma^m = 1 \iff \gamma_i^m = 1 \xrightarrow{(*)} O(\gamma_i) | m \quad \forall i \in \{1, \dots, k\}$$

Donde en $(*)$ hemos usado la Proposición 1.8. Concluimos que m es el mínimo común múltiplo de los órdenes de los ciclos, que por la Proposición 1.11, coincide con el mínimo común múltiplo de las longitudes de los ciclos. □

Ejemplo. Para familiarizarnos con la notación de permutaciones por ciclos disjuntos, vamos a enumerar todos los elementos de S_n para $n = 2, 3, 4$:

1. Para $n = 2$, tenemos $X = \{1, 2\}$ y por tanto:

$$S_2 = \{id, (1 \ 2)\}$$

2. Para $n = 3$, tenemos $X = \{1, 2, 3\}$ y:

$$S_3 = \{id, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$$

3. Para $n = 4$, tenemos $X = \{1, 2, 3, 4\}$ y:

$$\begin{aligned} S_4 = \{ & id, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), \\ & (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4), (1\ 2\ 4\ 3), \\ & (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \} \end{aligned}$$

Definición 1.15 (Elementos conjugados). Sea G un grupo y $a, c \in G$, decimos que son conjugados si $\exists b \in G$ de forma que $a = bcb^{-1}$.

Proposición 1.14. Si $\gamma \in S_n$ es un ciclo de longitud m , también lo será cualquier conjugado suyo. Es decir, si $\tau \in S_n$ y γ es un ciclo, entonces $\tau\gamma\tau^{-1}$ es un ciclo de longitud m .

Demostración. Si $\gamma = (x_1\ x_2\ \dots\ x_m)$, sea $\tau \in S_n$, entonces veamos que:

$$\alpha = \tau\gamma\tau^{-1} = (\tau(x_1)\ \tau(x_2)\ \dots\ \tau(x_m))$$

Luego α será un ciclo de longitud m . Para ello, sea $y \in \{1, \dots, n\}$:

- Si $\tau^{-1}(y) = x_i \implies y = \tau(x_i)$ con $i \in \{1, \dots, m-1\}$:

$$y \xrightarrow{\tau^{-1}} x_i \xrightarrow{\gamma} x_{i+1} \xrightarrow{\tau} \tau(x_{i+1}) = \alpha(\tau(x_i))$$

- Si $\tau^{-1}(y) = x_m \implies y = \tau(x_m)$:

$$y \xrightarrow{\tau^{-1}} x_m \xrightarrow{\gamma} x_1 \xrightarrow{\tau} \tau(x_1) = \alpha(\tau(x_m))$$

- Si $\tau^{-1}(y) = x \implies y = \tau(x)$ con $x \neq x_i$ para todo $i \in \{1, \dots, m\}$:

$$y \xrightarrow{\tau^{-1}} x \xrightarrow{\gamma} x \xrightarrow{\tau} \tau(x) = \alpha(\tau(x))$$

Concluimos que $\alpha = (\tau(x_1)\ \tau(x_2)\ \dots\ \tau(x_m))$. □

Ejemplo. Veamos la última Proposición en un caso práctico. Si consideramos:

$$\tau = (1\ 3\ 4), \quad \gamma = (2\ 4\ 5\ 3), \quad \tau^{-1} = (4\ 3\ 1)$$

Y tratamos de estudiar la imagen de $X = \{1, 2, 3, 4, 5\}$ bajo $\alpha = \tau\gamma\tau^{-1}$:

$$\begin{aligned} 1 &\xrightarrow{\tau^{-1}} 4 \xrightarrow{\gamma} 5 \xrightarrow{\tau} 5 \\ 2 &\xrightarrow{\tau^{-1}} 2 \xrightarrow{\gamma} 4 \xrightarrow{\tau} 1 \\ 3 &\xrightarrow{\tau^{-1}} 1 \xrightarrow{\gamma} 1 \xrightarrow{\tau} 3 \\ 4 &\xrightarrow{\tau^{-1}} 3 \xrightarrow{\gamma} 2 \xrightarrow{\tau} 2 \\ 5 &\xrightarrow{\tau^{-1}} 5 \xrightarrow{\gamma} 3 \xrightarrow{\tau} 4 \end{aligned}$$

Tenemos entonces que α es también un ciclo de longitud 4:

$$\alpha = \tau\gamma\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} = (1\ 5\ 4\ 2)$$

Proposición 1.15. Sea $\sigma \in S_n$ una permutación de forma que se descompone en ciclos disjuntos de la forma:

$$\sigma = \gamma_1 \dots \gamma_k$$

Entonces, podemos calcular su conjugado mediante $\tau \in S_n$ componiendo el conjugado de cada uno de los ciclos disjuntos en los que se descompone:

$$\tau \sigma \tau^{-1} = \tau \gamma_1 \tau^{-1} \dots \tau \gamma_k \tau^{-1}$$

Demostración.

$$\tau \sigma \tau^{-1} = \tau \gamma_1 \dots \gamma_k \tau^{-1} = \tau \gamma_1 id \gamma_2 id \dots id \gamma_k \tau^{-1} = \tau \gamma_1 \tau^{-1} \tau \gamma_2 \tau^{-1} \dots \tau \gamma_k \tau^{-1}$$

□

Ejemplo. Para practicar la conjugación de ciclos aplicando las Proposiciones 1.14 y 1.15, se plantea dados:

$$\sigma = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9), \quad \tau = (4 \ 8 \ 12 \ 7 \ 5 \ 9)$$

calcular $\tau \sigma \tau^{-1}$. Para ello, sabemos por la Proposición 1.15 que si⁹ $\sigma = \gamma_1 \gamma_2 \gamma_3 \gamma_4$, entonces basta calcular:

$$\tau \gamma_1 \tau^{-1}, \quad \tau \gamma_2 \tau^{-1}, \quad \tau \gamma_3 \tau^{-1}, \quad \tau \gamma_4 \tau^{-1}$$

Por la Proposición 1.14, sabemos que:

$$\tau \gamma_1 \tau^{-1} = (\tau(1) \ \tau(12) \ \tau(8) \ \tau(10) \ \tau(4)) = (1 \ 7 \ 12 \ 10 \ 8)$$

$$\tau \gamma_2 \tau^{-1} = (\tau(2) \ \tau(13)) = (2 \ 13)$$

$$\tau \gamma_3 \tau^{-1} = (\tau(5) \ \tau(11) \ \tau(7)) = (9 \ 11 \ 5)$$

$$\tau \gamma_4 \tau^{-1} = (\tau(6) \ \tau(9)) = (6 \ 4)$$

Si lo escribimos todo junto:

$$\tau \sigma \tau^{-1} = (1 \ 7 \ 12 \ 10 \ 8)(2 \ 13)(9 \ 11 \ 5)(6 \ 4)$$

Proposición 1.16. Toda permutación es un producto de transposiciones.

Demostración. Dada $\sigma \in S_n$, esta tiene su descomposición en ciclos disjuntos:

$$\sigma = \gamma_1 \dots \gamma_k$$

Basta demostrar que todo ciclo es producto de transposiciones.

En efecto, sea $\gamma = (x_1 \ x_2 \ \dots \ x_m)$, podemos escribir:

$$(x_1 \ x_2 \ \dots \ x_m) = (x_1 \ x_m)(x_1 \ x_{m-1}) \dots (x_1 x_3)(x_1 x_2)$$

⁹Observar la descomposición hecha ya de σ .

Para verlo, observemos qué hace la aplicación de la derecha con cada elemento (léase la descomposición de derecha a izquierda):

$$\begin{aligned}
 x_1 &\longmapsto x_2 \\
 x_2 &\longmapsto x_1 \longmapsto x_3 \\
 x_3 &\longmapsto x_1 \longmapsto x_4 \\
 &\vdots \\
 x_i &\longmapsto x_1 \longmapsto x_{i+1} \\
 &\vdots \\
 x_m &\longmapsto x_1
 \end{aligned}$$

O también podemos escribir:

$$(x_1 \ x_2 \ \dots \ x_m) = (x_1 \ x_2)(x_2 \ x_3) \dots (x_{m-1} \ x_m)$$

Para verlo:

$$\begin{aligned}
 x_1 &\longmapsto x_2 \\
 x_2 &\longmapsto x_3 \\
 x_3 &\longmapsto x_4 \\
 &\vdots \\
 x_i &\longmapsto x_{i+1} \\
 &\vdots \\
 x_m &\longmapsto x_{m-1} \longmapsto x_{m-2} \longmapsto \dots \longmapsto x_3 \longmapsto x_2 \longmapsto x_1
 \end{aligned}$$

□

Ejemplo. Sea $\sigma = (1 \ 2 \ 3 \ 4 \ 5)$, veamos que σ se puede descomponer en transposiciones de la forma:

$$\sigma = t_1 t_2 t_3 t_4$$

Con $t_1 = (1 \ 5)$, $t_2 = (1 \ 4)$, $t_3 = (1 \ 3)$, $t_4 = (1 \ 2)$.

Para ello, escribamos la imagen de $X = \{1, 2, 3, 4, 5\}$ mediante la permutación resultante de componer las 4 transposiciones $\gamma = t_1 t_2 t_3 t_4$ y veamos que coincide con la de σ :

$$\left. \begin{aligned}
 1 &\xrightarrow{t_4} 2 \xrightarrow{t_3} 2 \xrightarrow{t_2} 2 \xrightarrow{t_1} 2 \\
 2 &\longmapsto 1 \longmapsto 3 \longmapsto 3 \longmapsto 3 \\
 3 &\longmapsto 3 \longmapsto 1 \longmapsto 4 \longmapsto 4 \\
 4 &\longmapsto 4 \longmapsto 4 \longmapsto 1 \longmapsto 5 \\
 5 &\longmapsto 5 \longmapsto 5 \longmapsto 5 \longmapsto 1
 \end{aligned} \right\} \implies \left\{ \begin{aligned}
 1 &\xrightarrow{\gamma} 2 \\
 2 &\longmapsto 3 \\
 3 &\longmapsto 4 \\
 4 &\longmapsto 5 \\
 5 &\longmapsto 1
 \end{aligned} \right.$$

De esta forma:

$$\gamma = t_1 t_2 t_3 t_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1 \ 2 \ 3 \ 4 \ 5) = \sigma$$

Si ahora consideramos la descomposición de la forma:

$$\sigma = r_1 r_2 r_3 r_4$$

Con $r_1 = (1\ 2)$, $r_2 = (2\ 3)$, $r_3 = (3\ 4)$, $r_4 = (4\ 5)$, escribimos ahora la imagen de X mediante la permutación $\tau = r_1 r_2 r_3 r_4$:

$$\left. \begin{array}{l} 1 \xrightarrow{r_4} 1 \xrightarrow{r_3} 1 \xrightarrow{r_2} 1 \xrightarrow{r_1} 2 \\ 2 \mapsto 2 \mapsto 2 \mapsto 3 \mapsto 3 \\ 3 \mapsto 3 \mapsto 4 \mapsto 4 \mapsto 4 \\ 4 \mapsto 5 \mapsto 5 \mapsto 5 \mapsto 5 \\ 5 \mapsto 4 \mapsto 3 \mapsto 2 \mapsto 1 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{l} 1 \xrightarrow{\gamma} 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ 4 \mapsto 5 \\ 5 \mapsto 1 \end{array} \right.$$

Vemos igual que antes que $\tau = \sigma$.

Proposición 1.17. *Una permutación admite varias descomposiciones en productos de transposiciones, pero todas ellas coinciden en la paridad del número de transposiciones.*

1.3.1. Signatura

Definición 1.16 (Signatura). Consideraremos el siguiente polinomio de n variables:

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \dots, x_n]$$

Y definimos para cada $\sigma \in S_n$:

$$\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

Podemos ahora definir la aplicación signatura $\varepsilon : S_n \longrightarrow \{-1, 1\}$ dada por:

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{si } \sigma(\Delta) = \Delta \\ -1 & \text{si } \sigma(\Delta) = -\Delta \end{cases}$$

- Si $\varepsilon(\sigma) = 1$, diremos que σ es una permutación par.
- Si $\varepsilon(\sigma) = -1$, diremos que σ es una permutación impar.

Observación. A partir de la definición anterior, tenemos que $\sigma(\Delta) = \varepsilon(\sigma)\Delta$.

Ejemplo. Sea $n = 4$, estaremos interesados en el polinomio:

$$\Delta = \prod_{1 \leq i < j \leq 4} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

Si consideramos $\sigma = (1\ 2\ 3\ 4)$, queremos comprobar cual es la signatura de σ . Como:

$$\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_4 - x_1) = -\Delta$$

Deducimos que $\varepsilon(\sigma) = -1$, es decir, σ es una permutación impar.

Proposición 1.18. *La aplicación signatura verifica que:*

$$\varepsilon \left(\prod_{i=1}^m \sigma_i \right) = \prod_{i=1}^m \varepsilon(\sigma_i)$$

Con $\sigma_1, \sigma_2, \dots, \sigma_m \in S_n$.

Demostración. Por inducción sobre m :

- Para $m = 2$: Queremos ver que dadas $\sigma, \tau \in S_n$, entonces:

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$$

Para ello, si vemos que $(\sigma\tau)(\Delta) = \sigma(\tau(\Delta))$ y que $\sigma(-\Delta) = -\sigma(\Delta)$, basta distinguir casos:

- Si σ es par:
 - Si τ es par, se tendrá $\sigma(\tau(\Delta)) = \sigma(\Delta) = \Delta$, con lo que $\sigma\tau$ es par.
 - Si τ es impar, se tendrá $\sigma(\tau(\Delta)) = \sigma(-\Delta) = -\sigma(\Delta) = -\Delta$, con lo que $\sigma\tau$ es impar.
- Si σ es impar:
 - Si τ es par, se tendrá $\sigma(\tau(\Delta)) = \sigma(\Delta) = -\Delta$, con lo que $\sigma\tau$ es impar.
 - Si τ es impar, se tendrá $\sigma(\tau(\Delta)) = \sigma(-\Delta) = -\sigma(\Delta) = \Delta$, con lo que $\sigma\tau$ es par.

- Supuesto para m :

$$\varepsilon\left(\prod_{i=1}^m \sigma_i\right) = \varepsilon\left(\left(\prod_{i=1}^{m-1} \sigma_i\right) \sigma_m\right) = \varepsilon\left(\prod_{i=1}^{m-1} \sigma_i\right) \varepsilon(\sigma_m) \stackrel{(*)}{=} \prod_{i=1}^{m-1} (\varepsilon(\sigma_i)) \varepsilon(\sigma_m) = \prod_{i=1}^m \varepsilon(\sigma_i)$$

Donde en $(*)$ hemos usado la hipótesis de inducción.

□

Proposición 1.19. *Se verifican los siguientes resultados:*

1. *Las transposiciones son permutaciones impares.*
2. *Una permutación es par si y solo si se descompone en el producto de un número par de transposiciones.*
3. *Un ciclo de longitud $m \geq 2$ es par si y solo si m es impar.*
4. *Una permutación es par si y solo si el número de ciclos de longitud par en su descomposición en ciclos disjuntos es par.*

Demostración. Demostramos cada uno de los resultados:

1. Sea $\sigma = (i \ j)$ una transposición (con $1 \leq i < j \leq n$), estudiemos qué sucede con $\sigma(\Delta)$:
 - Por una parte, está claro que hay un cambio de signo tras aplicar σ al factor $(x_i - x_j)$, ya que este pasa a ser $(x_j - x_i)$.
 - Está claro que los factores de la forma $(x_a - x_b)$ con $a, b \notin \{i, j\}$ se mantienen invariantes ante σ , por lo que no hay cambio de signo en estos.

- Además, los factores de la forma $(x_a - x_y)$ con $y \in \{i, j\}$ y $a < i$ tampoco alteran el signo de Δ , ya que al aplicar σ :

$$\begin{aligned}(x_a - x_i) &\xrightarrow{\sigma} (x_a - x_j) \\ (x_a - x_j) &\xrightarrow{\sigma} (x_a - x_i)\end{aligned}$$

Tenemos que un factor va al otro, por lo que no alteran el signo.

- De forma análoga, los factores de la forma $(x_y - x_b)$ con $y \in \{i, j\}$ y $b > j$ tampoco alteran el signo de Δ :

$$\begin{aligned}(x_i - x_b) &\xrightarrow{\sigma} (x_j - x_b) \\ (x_j - x_b) &\xrightarrow{\sigma} (x_i - x_b)\end{aligned}$$

- Finalmente, los únicos factores que nos quedan por considerar son los de la forma $(x_i - x_a)$ y $(x_a - x_j)$, con $i < a < j$. En este caso:

$$\begin{aligned}(x_i - x_a) &\xrightarrow{\sigma} (x_j - x_a) = -(x_a - x_j) \\ (x_a - x_j) &\xrightarrow{\sigma} (x_a - x_i) = -(x_i - x_a)\end{aligned}$$

Fijado a con $i < a < j$, tanto el factor $(x_i - x_a)$ como el $(x_a - x_j)$ cambian de signo, por lo que el doble cambio de signo se compensa, luego estos factores no alteran el signo de Δ al aplicar σ .

Concluimos que al aplicar $\sigma = (i \ j)$ sobre Δ , el signo obtenido es el mismo salvo por el factor $(x_i - x_j)$, que cambia de signo, por lo que:

$$\sigma(\Delta) = -\Delta$$

y llegamos a que σ es impar.

2. Sea $\sigma \in S_n$ una permutación, sabemos que puede descomponerse en k transposiciones:

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_k$$

Usando la Proposición 1.18, tenemos que:

$$\varepsilon(\sigma) = \prod_{i=1}^k \varepsilon(\gamma_i)$$

Por lo que:

- Si k es par, entonces $\varepsilon(\sigma) = 1$.
 - Si k es impar, entonces $\varepsilon(\sigma) = -1$.
3. Para $m = 2$, un ciclo de longitud m es una transposición, que ya sabemos que es impar. Sea τ un ciclo de longitud $m \geq 3$, en la Proposición 1.16 vimos que τ se podía descomponer como producto de $m - 1$ transposiciones:

$$\tau = \gamma_1 \gamma_2 \dots \gamma_{m-1}$$

Por tanto, y aplicando 2, tenemos que:

- Si m es par, entonces $m - 1$ es impar, con lo que τ es impar.
 - Si m es impar, entonces $m - 1$ es par, con lo que τ es par.
4. Sea $\sigma \in S_n$, esta se puede descomponer como producto de k ciclos disjuntos de longitud mayor o igual que 2:

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_k$$

Usando la Proposición 1.18, tenemos que:

$$\varepsilon(\sigma) = \prod_{i=1}^k \varepsilon(\gamma_i)$$

Si consideramos la siguiente partición de $\{1, \dots, k\}$:

$$\begin{aligned} A &= \{i \in \{1, \dots, k\} \mid \gamma_i \text{ tiene longitud impar}\} \\ B &= \{i \in \{1, \dots, k\} \mid \gamma_i \text{ tiene longitud par}\} \end{aligned}$$

Por 3 tenemos que $\varepsilon(\gamma_i) = 1$ para todo $i \in A$ y que $\varepsilon(\gamma_j) = -1$ para todo $j \in B$. De esta forma:

$$\varepsilon(\sigma) = \left(\prod_{i \in A} \varepsilon(\gamma_i) \right) \left(\prod_{i \in B} \varepsilon(\gamma_i) \right) = \left(\prod_{i \in A} 1 \right) \left(\prod_{i \in B} -1 \right) = \prod_{i \in B} -1$$

Por tanto:

- Si $|B|$ es par, tenemos que σ es par.
- Si $|B|$ es impar, tenemos que σ es impar.

□

Ejemplo. Ahora, es fácil determinar la signatura de cualquier permutación. Por ejemplo, si consideramos:

$$\sigma = (1 \ 12 \ 8 \ 10 \ 4)(2 \ 13)(5 \ 11 \ 7)(6 \ 9)$$

Como tiene 2 ciclos de longitud par (un número par), σ es una permutación par.

1.3.2. Grupos Alternados A_n

Definición 1.17 (Grupos Alternados A_n). En S_n consideramos el conjunto:

$$A_n = \{\sigma \in S_n \mid \sigma \text{ es par}\}$$

Se verifica que $(A_n, \circ, 1)$ es un grupo:

- La asociatividad de \circ es heredada de la de \circ en S_n .
- El producto de dos permutaciones pares es par, luego está bien definido el grupo.

- La identidad es una permutación par, que es el neutro de la operación binaria.
- Dado $\sigma \in A_n$, escribimos su descomposición en ciclos disjuntos e invertimos cada ciclo. La longitud de los ciclos no cambia, luego la paridad del ciclo inverso tampoco, por lo que σ^{-1} sigue siendo una permutación par.

Al grupo A_n lo llamamos el grupo alternado de grado n , que verifica:

$$|A_n| = \frac{n!}{2}$$

Observación. Notemos que si definimos $B_n = \{\sigma \in S_n \mid \sigma \text{ es impar}\}$, entonces sobre B_n no podemos tener una estructura de grupo con la operación \circ , ya que el neutro para \circ de S_n no está en B_n , sino en A_n .

Ejemplo. Listar todos los elementos de los grupos alternados es fácil si previamente listamos todos los elementos de su grupo simétrico correspondiente:

1. Para $n = 3$:

$$S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

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

2. Para $n = 4$:

$$S_4 = \{1, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4),$$

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

$$(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

$$A_4 = \{1, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),$$

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Proposición 1.20. *Se tiene que:*

$$(a) \ S_n = \langle (1\ 2), (2\ 3), \dots, (n-1\ n) \rangle$$

$$(b) \ S_n = \langle (1\ 2), (1\ 2 \dots n) \rangle$$

$$(c) \ S_n = \langle (1\ 2), (1\ 3), \dots, (1\ n) \rangle$$

$$(d) \ A_n = \langle (x_1\ x_2\ x_3) \rangle \text{ con } n \geq 3$$

$$(e) \ A_n = \langle (1\ x\ y) \rangle \text{ con } n \geq 3$$

Demostración. Veamos cada uno de los enunciados:

- (a) Sabemos que (por la Proposición 1.16):

$$S_n = \langle (i\ j) \mid i, j \in \{1, \dots, n\}, i < j \rangle$$

Supuesto que $i < j$, vemos que:

$$(i\ j) = (i\ i+1)(i+1\ i+2) \dots (j-2\ j-1)(j-1\ j)(j-1\ j-2) \dots (i+2\ i+1)(i+1\ i)$$

- (b) Por el apartado anterior, basta obtener cualquier transposición de la forma $(i \ i+1)$ con $i \in \{1, \dots, n-1\}$ a partir de $\sigma = (1 \ 2 \ \dots \ n)$ y $(1 \ 2)$. Para ello, como se tiene que:

$$\sigma^{i-1}(1) = i \quad \sigma^{i-1}(2) = i+1$$

Podemos considerar el conjugado de $(1 \ 2)$ mediante σ^{i-1} :

$$\sigma^{i-1}(1 \ 2)(\sigma^{i-1})^{-1} = \sigma^{i-1}(1 \ 2)\sigma^{1-i} = (\sigma^{i-1}(1) \ \sigma^{i-1}(2)) = (i \ i+1)$$

- (c) Basta ver que $(1 \ 2 \ \dots \ n)$ se puede obtener por composición de transposiciones de la forma $(1 \ j)$ con $j \in \{2, \dots, n\}$, lo que ya se hizo en la Proposición 1.16:

$$(1 \ 2 \ \dots \ n) = (1 \ n)(1 \ n-1) \dots (1 \ 3)(1 \ 2)$$

- (d) Podemos suponer que $x_1 < x_2 < x_3$, ya que:

$$(x_1 \ x_3 \ x_2) = (x_1 \ x_2 \ x_3)^2$$

Sabemos que si $\sigma \in A_n$, entonces será producto de un número par de transposiciones, por lo que basta expresar estos productos en función de ciclos de la forma $(x_1 \ x_2 \ x_3)$.

- Si hay elementos comunes, escribiremos:

$$(x_1 \ x_2)(x_2 \ x_3) = (x_1 \ x_2 \ x_3)$$

- Si no hay elementos comunes (tenemos dos transposiciones disjuntas), entonces:

$$(x_1 \ x_2)(x_3 \ x_4) = (x_1 \ x_2 \ x_3)(x_2 \ x_3 \ x_4)$$

- (e) Usando el apartado anterior, tenemos que cualquier terna ordenada $(x_1 \ x_2 \ x_3)$ podemos escribirla de la forma:

$$(x_1 \ x_2 \ x_3) = (1 \ x_3 \ x_2)(1 \ x_1 \ x_2)(1 \ x_1 \ x_3)$$

□

Ejemplo. Usando la Proposición 1.20, veamos distintos conjuntos generadores para varios grupos:

- (a) Destacamos:

- $S_3 = \langle (1 \ 2), (2 \ 3) \rangle$ y buscamos expresar la última transposición como producto de estas:

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

- En $S_4 = \langle (1 \ 2)(2 \ 3)(3 \ 4) \rangle$ mostramos por ejemplo que:

$$(1 \ 4) = (1 \ 2)(2 \ 3)(3 \ 4)(3 \ 2)(2 \ 1)$$

- (b) Ahora:

- En $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$:

$$(2\ 3) = (1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1}$$

- En $S_4 = \langle (1\ 2), (1\ 2\ 3\ 4) \rangle$:

$$(2\ 3) = (1\ 2\ 3\ 4)(1\ 2)(1\ 2\ 3\ 4)^{-1}$$

$$(3\ 4) = (1\ 2\ 3\ 4)^2(1\ 2)(1\ 2\ 3\ 4)^{-2}$$

(d) Recordamos los elementos de A_4 :

$$A_4 = \{1, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), \\ (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Tenemos que:

$$A_4 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4) \rangle$$

Por ejemplo, podemos escribir:

$$(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$$

(e) Tenemos:

$$A_4 = \langle (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4) \rangle$$

1.4. Grupos de matrices

Sea \mathbb{F} un cuerpo, las matrices cuadradas de orden n sobre \mathbb{F} las denotaremos por:

$$\mathcal{M}_n(\mathbb{F})$$

Sabemos que $(\mathcal{M}_n(\mathbb{F}), +, \cdot)$ es un anillo, aunque estaremos interesados en ver el conjunto $\mathcal{M}_n(\mathbb{F})$ como un grupo en su forma más interesante, es decir, como grupo con notación multiplicativa.

1.4.1. Grupo lineal $\text{GL}_n(\mathbb{F})$

Definición 1.18 (Grupo lineal $\text{GL}_n(\mathbb{F})$). Sea \mathbb{F} un cuerpo finito, en $\mathcal{M}_n(\mathbb{F})$ consideramos el conjunto:

$$\text{GL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) \neq 0\}$$

Se verifica que $(\text{GL}_n(\mathbb{F}), \cdot, I)$ es un grupo:

- La asociatividad de \cdot viene heredada de la de \cdot en $\mathcal{M}_n(\mathbb{F})$.
- $\det(I) = 1 \neq 0$ y se tiene que I es el elemento neutro para \cdot .
- Como consideramos las matrices con determinante no nulo, sabemos que todas estas tienen inversa.

A $\text{GL}_n(\mathbb{F})$ lo llamamos el grupo lineal de orden n .

Proposición 1.21. *Sea $n \in \mathbb{N}$, si $|\mathbb{F}| = q$, entonces se verifica que:*

$$|\text{GL}_n(\mathbb{F})| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) = \prod_{k=1}^n (q^n - q^{k-1})$$

Demostración. Como $A \in \text{GL}_n(\mathbb{F}) \iff A$ es regular \iff sus filas son vectores linealmente independientes, basta contar de cuántas formas podemos elegir n vectores linealmente independientes con n entradas en \mathbb{F} (que recordamos tenía q elementos). Para ello:

- Para elegir el primer vector $v_1 \in \mathbb{F}^n$, podemos elegir cualquiera, luego el problema es elegir n números de entre q posibilidades, q^n posibles elecciones.

Sin embargo, como queremos que v_1 sea linealmente independiente con el resto de vectores que forman las filas de una matriz, hemos de exigir $v_1 \neq 0$, con lo que tenemos $q^n - 1$ posibilidades para v_1 .

- Una vez elegido v_1 , para elegir v_2 no podemos elegir un vector de $\mathcal{L}(v_1) \cong \mathbb{F}$, por lo que tenemos q vectores que no podemos elegir; elegimos un vector de los $q^n - q$ restantes.
- Repitiendo el proceso, una vez elegido v_{k-1} , para elegir v_k (con $k \in \{2, \dots, n\}$), no podemos elegir ningún vector de $\mathcal{L}(v_1, \dots, v_{k-1}) \cong \mathbb{F}^{k-1}$, por lo que tenemos q^{k-1} vectores que no podemos elegir y elegimos entre los $q^n - q^{k-1}$ restantes.

Este proceso ilustra que las posibles elecciones totales de vectores para las filas de una matriz de $\text{GL}_n(\mathbb{F})$ son:

$$\prod_{k=1}^n (q^n - q^{k-1})$$

Por lo que este debe ser el cardinal de $|\text{GL}_n(\mathbb{F})|$. □

Ejemplo. Veamos:

- En $|\text{GL}_2(\mathbb{Z}_2)| = (2^2 - 1)(2^2 - 2) = 6$:

$$\text{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

Podemos escribirlos sin que se nos olvide ninguna pensando en que tenemos que escribir todas las matrices de forma que los vectores formados por las columnas sean linealmente independientes entre sí (para así conseguir un determinante no nulo).

- Tenemos $|\text{GL}_3(\mathbb{Z}_2)| = 168$. Se deja como ejercicio escribir todas las matrices.
- Tenemos $|\text{GL}_2(\mathbb{Z}_3)| = 48$.

1.4.2. Grupo lineal especial $\mathrm{SL}_n(\mathbb{F})$

Definición 1.19 (Grupo lineal especial $\mathrm{SL}_n(\mathbb{F})$). Sea \mathbb{F} un cuerpo finito, en $\mathcal{M}_n(\mathbb{F})$ consideramos el conjunto:

$$\mathrm{SL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) = 1\}$$

Se verifica que $(\mathrm{SL}_n(\mathbb{F}), \cdot, I)$ es un grupo:

- La asociatividad de \cdot viene heredada de la de \cdot en $\mathcal{M}_n(\mathbb{F})$.
- $\det(I) = 1$ y se tiene que I es el elemento neutro para \cdot .
- Como consideramos las matrices con determinante $1 \neq 0$, sabemos que todas estas tienen inversa.

A $\mathrm{SL}_n(\mathbb{F})$ lo llamamos el grupo lineal especial de orden n .

Proposición 1.22. Sea $n \in \mathbb{N}$, si $|\mathbb{F}| = q$, entonces se verifica que:

$$|\mathrm{SL}_n(\mathbb{F})| = \frac{|\mathrm{GL}_n(\mathbb{F})|}{q - 1}$$

Demostración. Sea $A \in \mathrm{GL}_n(\mathbb{F})$, observemos que $\det(A)$ puede¹⁰ tomar q valores distintos, uno por cada elemento de \mathbb{F} . De esta forma, si dado $k \in \mathbb{F}^* = \mathbb{F} \setminus \{0\}$ definimos:

$$D_k = \{A \in \mathrm{GL}_n(\mathbb{F}) : \det(A) = k\}$$

Es claro que estos conjuntos forman una partición de $\mathrm{GL}_n(\mathbb{F})$:

$$\mathrm{GL}_n(\mathbb{F}) = \bigsqcup_{k \in \mathbb{F}^*} D_k$$

Veamos que $|D_k| = |D_1|$ para todo $k \in \mathbb{F}^*$. Para ello, sea $k \in \mathbb{F}^*$, definimos la aplicación $\varphi_k : \mathrm{GL}_n(\mathbb{F}) \rightarrow \mathrm{GL}_n(\mathbb{F})$ dada por:

$$\varphi_k(A) = \varphi_k((a_{ij})_{i,j}) = (\overline{a_{ij}})_{i,j} \quad \forall A = (a_{ij})_{i,j} \in \mathrm{GL}_n(\mathbb{F})$$

Donde:

$$\overline{a_{ij}} = \begin{cases} ka_{ij} & \text{si } i = 1 \\ a_{ij} & \text{si } i \neq 1 \end{cases}$$

Es decir, φ_k multiplica la primera fila de una matriz por k . De esta forma, las propiedades de los determinantes nos dicen que si $A \in D_1$, entonces:

$$\det(\varphi_k(A)) = k \cdot \det(A) = k$$

Por lo que $\varphi_k(A) \in D_k$ para todo $k \in \mathbb{F}^*$. Por tanto, podemos definir la aplicación $\psi_k : D_1 \rightarrow D_k$ de forma que $\psi_k = \varphi_{k|_{D_1}}$. Veamos que ψ_k es biyectiva para terminar el razonamiento. Para ello, dada ψ_k para un cierto $k \in \mathbb{F}$, consideramos $\psi_{k^{-1}}$. Como:

$$kk^{-1}a_{ij} = k^{-1}ka_{ij} = a_{ij} \quad \forall a_{ij} \in \mathbb{F}$$

¹⁰De hecho los toma, es fácil comprobar que $\det : \mathrm{GL}_n(\mathbb{F}) \rightarrow \mathbb{F}$ es una aplicación sobreyectiva.

Concluimos que $\psi_k^{-1} = \psi_{k^{-1}}$ y además vemos que $\varphi_{k^{-1}}(D_k) \subseteq D_1$. Llegamos a que ψ_k es biyectiva, por lo que $|D_k| = |D_1|$ para todo $k \in \mathbb{F}^*$.

Sea ahora $\phi : \{1, \dots, q-1\} \rightarrow \mathbb{F}^*$ cualquier biyección de forma que $\phi(1) = 1$, como los D_k formaban una partición finita de $\text{GL}_n(\mathbb{F})$, tenemos que:

$$|\text{GL}_n(\mathbb{F})| = \sum_{k=1}^{q-1} |D_{\phi(k)}| = \sum_{k=1}^{q-1} |D_1| = (q-1)|D_1| = (q-1)|\text{SL}_n(\mathbb{F})|$$

De donde deducimos que:

$$|\text{SL}_n(\mathbb{F})| = \frac{|\text{GL}_n(\mathbb{F})|}{q-1}$$

□

Ejemplo. Tenemos:

- $|\text{SL}_3(\mathbb{Z}_3)| = 24$.
- $\text{SL}_n(\mathbb{Z}_2) = \text{GL}_n(\mathbb{Z}_2) \forall n \in \mathbb{N}$

1.5. Homomorfismos de grupos

Definición 1.20 (Homomorfismo). Dados dos grupos G y H , un homomorfismo de grupos de G en H es una aplicación $f : G \rightarrow H$ que verifica:

$$f(xy) = f(x)f(y) \quad \forall x, y \in G$$

Proposición 1.23. Si $f : G \rightarrow H$ es un homomorfismo de grupos, entonces:

1. $f(1) = 1$
2. $f(x^{-1}) = (f(x))^{-1}$
3. $f(x^n) = (f(x))^n \forall n \in \mathbb{N}$

Demostración. Veamos cada una:

1. $f(1) = f(1 \cdot 1) = f(1)f(1) \implies f(1) = 1$
2. $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}) \implies f(x^{-1}) = (f(x))^{-1}$
3. $f(x^n) = f(\underbrace{x \cdot \dots \cdot x}_{n \text{ veces}}) = \underbrace{f(x) \cdot \dots \cdot f(x)}_{n \text{ veces}} = (f(x))^n$

□

Definición 1.21. Sea $f : G \rightarrow H$ un homomorfismo de grupos, distinguimos:

- $\ker f = \{x \in G \mid f(x) = 1\}$
- $\text{Im} f = \{f(x) \mid x \in G\}$

Ejemplo. Ejemplos de homomorfismos de grupos son:

1. Dado G un grupo, $id : G \rightarrow G$.

2. Dados G, H grupos, consideramos el siguiente homomorfismo, denominado *homomorfismo trivial*:

$$\begin{aligned} f : G &\longrightarrow H \\ x &\longmapsto 1 \end{aligned}$$

3. La exponencial es también un homomorfismo:

$$\begin{aligned} \exp : (\mathbb{R}, +) &\longrightarrow (\mathbb{R}^+, \cdot) \\ x &\longmapsto e^x \end{aligned}$$

4. La aplicación determinante de matrices con determinante no nulo:

$$\begin{aligned} \det : \text{GL}_n(\mathbb{F}) &\longrightarrow \mathbb{F}^* \\ A &\longmapsto \det(A) \end{aligned}$$

5. La aplicación signatura:

$$\begin{aligned} \varepsilon : S_n &\longrightarrow \mathcal{U}(\mathbb{Z}) = \{-1, 1\} \\ \sigma &\longmapsto \varepsilon(\sigma) \end{aligned}$$

Proposición 1.24. Sean $f : G \rightarrow H$ y $g : H \rightarrow T$ dos homomorfismos de grupos, entonces la aplicación $g \circ f : G \rightarrow T$ es un homomorfismo de grupos.

Demostración. Sean $x, y \in G$, entonces:

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$$

□

Definición 1.22. Dado $f : G \rightarrow H$ un homomorfismo de grupos, decimos que:

- f es un monomorfismo si es inyectiva.
- f es un epimorfismo si es sobreyectiva.
- f es un isomorfismo si es biyectiva.
- Si $G = H$, diremos que f es un endomorfismo.
- Si f es un endomorfismo biyectivo, diremos que es un automorfismo.

Proposición 1.25. Sea $f : G \rightarrow H$ un homomorfismo de grupos, entonces:

- i) f es monomorfismo $\iff \ker(f) = \{1\}$
- ii) f es isomorfismo $\iff f^{-1}$ es un isomorfismo.

Demostración. Veamos los dos resultados:

- i) Para el primero, demostramos las dos implicaciones:

\implies) $x \in \ker(f) \implies f(x) = 1 = f(1)$, pero como f es inyectiva, tenemos que $x = 1$.

\impliedby) Sean $x, y \in G$ de forma que $f(x) = f(y)$, entonces:

$$f(x)(f(y))^{-1} = 1 \implies f(xy^{-1}) = 1 \implies xy^{-1} = 1 \implies x = y$$

Concluimos que f es inyectiva.

ii) Demostramos las dos implicaciones:

\implies) Si f es un isomorfismo, entonces es biyectiva, por lo que tendrá una aplicación inversa f^{-1} , que por lo pronto ya sabemos que es biyectiva. Basta ver que esta aplicación es un homomorfismo. Para ello, sean $y, y' \in H$, por ser f un biyectiva, existirán $x, x' \in G$ de forma que $f(x) = y$ y $f(x') = y'$, luego $x = f^{-1}(y)$ y $x' = f^{-1}(y')$. Por tanto:

$$f^{-1}(yy') = f^{-1}(f(x)f(x')) = f^{-1}(f(xx')) = xx' = f^{-1}(y)f^{-1}(y')$$

Lo que demuestra que f^{-1} es un homomorfismo biyectivo, luego isomorfismo.

\impliedby) Si f^{-1} es un isomorfismo, entonces por la implicación que acabamos de demostrar, $(f^{-1})^{-1} = f$ también es un isomorfismo. \square

Definición 1.23 (Grupos isomorfos). Sean G y H dos grupos, decimos que son isomorfos si existe un isomorfismo entre ellos, que se denotará por $G \cong H$.

Proposición 1.26. *La propiedad de ser isomorfo es una relación de equivalencia.*

Demostración. Demostramos cada una de las propiedades:

- Propiedad reflexiva. Sea G un grupo, como $id : G \rightarrow G$ es un homomorfismo, tenemos que $G \cong G$.
- Propiedad simétrica. Sean G y H dos grupos de forma que $G \cong H$, entonces existe un isomorfismo $f : G \rightarrow H$. Por la Proposición 1.25, $f^{-1} : H \rightarrow G$ también será un isomorfismo, por lo que $H \cong G$.
- Propiedad transitiva. Sean G, H y T tres grupos de forma que $G \cong H$ y $H \cong T$, entonces existen dos isomorfismos: $f : G \rightarrow H$ y $g : H \rightarrow T$. Si consideramos $g \circ f : G \rightarrow T$, tenemos por la Proposición 1.24 que $g \circ f$ es un isomorfismo de G en T , por lo que $G \cong T$.

\square

Proposición 1.27. *Se verifican:*

- i) Si $f : X \rightarrow Y$ es una aplicación biyectiva, se tiene que la aplicación siguiente es un isomorfismo de grupos:

$$\begin{aligned} \varphi : \text{Perm}(X) &\longrightarrow \text{Perm}(Y) \\ \sigma &\longmapsto f\sigma f^{-1} \end{aligned}$$

- ii) $\text{Aut}(G) = \{f : G \rightarrow G \mid f \text{ automorfismo}\}$ con la composición forman un grupo.
- iii) Si $f : G \rightarrow H$ es un isomorfismo, entonces $|G| = |H|$.
- iv) Si G y H son isomorfos, entonces G es abeliano $\iff H$ es abeliano.
- v) Si $f : G \rightarrow H$ es un isomorfismo, entonces se mantiene el orden:

$$O(x) = O(f(x)) \quad \forall x \in G$$

- vi) Si $f : G \rightarrow H$ es un epimorfismo y $S = \{s_1, \dots, s_n\} \subseteq G$ cumple que $G = \langle S \rangle$, entonces $H = \langle f(S) \rangle$.

Demostración. Veamos cada una:

- i) Hemos de ver que φ es un homomorfismo biyectivo:

- Sean $\sigma, \tau \in \text{Perm}(X)$, entonces:

$$\varphi(\sigma\tau) = f\sigma\tau f^{-1} \stackrel{(*)}{=} f\sigma f^{-1} f\tau f^{-1} = \varphi(\sigma)\varphi(\tau)$$

Donde podemos ver $(*)$ descomponiendo en ciclos disjuntos tanto σ como τ y aplicando la Proposición 1.15.

- Definimos la siguiente aplicación:

$$\begin{aligned} \psi : \text{Perm}(Y) &\longrightarrow \text{Perm}(X) \\ \tau &\longmapsto f^{-1}\tau f \end{aligned}$$

Veamos que ψ es la inversa de φ :

$$\begin{aligned} \psi(\varphi(\sigma)) &= \psi(f\sigma f^{-1}) = f^{-1}f\sigma f^{-1}f = \sigma \\ \varphi(\psi(\tau)) &= \varphi(f^{-1}\tau f) = f(f^{-1}\tau f)f^{-1} = \tau \end{aligned}$$

Por tanto, φ es biyectiva.

Como φ es un homomorfismo biyectivo, es un isomorfismo.

- ii) La asociatividad viene heredada de la asociatividad de funciones, el neutro del grupo es $\text{id} : G \rightarrow G$ y como son automorfismos, son aplicaciones biyectivas, con lo que cada una tiene inversa.
- iii) Por ser f biyectiva, se tiene $|G| = |H|$.
- iv) Veamos las dos implicaciones:

\implies) Sean $x, y \in H$:

$$xy = f(f^{-1}(xy)) = f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(y)f(f^{-1}(x))) = f(f^{-1}(yx)) = yx$$

\impliedby) Como $G \cong H \iff H \cong G$, por la propiedad simétrica se tiene la otra implicación.

v) Si $O(x) = n$, entonces:

$$(f(x))^n = f(x^n) = f(1) = 1$$

Por tanto, tenemos que $O(f(x)) \leq n$. Si suponemos ahora que $\exists m \in \mathbb{N}$ tal que $(f(x))^m = 1$, entonces $f(x^m) = 1 = f(1)$ y por inyectividad tenemos que $x^m = 1$, luego $n \leq m$. De todo esto deducimos que $O(f(x)) = n$.

Si $O(x) = +\infty$, basta observar que $f(x^n) = (f(x))^n$ para todo $n \in \mathbb{N} \setminus \{0\}$, para concluir que $O(f(x)) = +\infty$. Si $O(f(x)) = +\infty$, basta usar f^{-1} .

vi) Sea $y \in H$, buscamos una descomposición de y en función de los elementos $f(s_i)$. Para ello, como f es sobreyectiva, existirá $x \in G$ de forma que $y = f(x)$. Como $G = \langle S \rangle$, tendremos que existen $\gamma_1, \dots, \gamma_k \in \mathbb{Z}$ de forma que:

$$x = s_1^{\gamma_1} s_2^{\gamma_2} \dots s_k^{\gamma_k}$$

Luego:

$$y = f(x) = f(s_1^{\gamma_1} s_2^{\gamma_2} \dots s_k^{\gamma_k}) = f(s_1)^{\gamma_1} f(s_2)^{\gamma_2} \dots f(s_k)^{\gamma_k}$$

Por lo que $H = \langle f(s_1), f(s_2), \dots, f(s_n) \rangle = \langle f(S) \rangle$.

□

Teorema 1.28 (de Dyck). *Sea G un grupo finito con una presentación*

$$G = \langle S \mid R_1, R_2, \dots, R_k \rangle \quad S = \{s_1, \dots, s_m\}$$

Sea H otro grupo finito con $\{r_1, \dots, r_m\} \subseteq H$, y supongamos que cualquier relación satisfecha en G por los s_i con $i \in \{1, \dots, m\}$ es también satisfecha en H para los r_i con $i \in \{1, \dots, m\}$. Entonces existe un único homomorfismo de grupos $f : G \rightarrow H$ de forma que:

$$f(s_i) = r_i \quad i \in \{1, \dots, m\}$$

- Si además $\{r_1, \dots, r_m\}$ son un conjunto de generadores de H , entonces f es un epimorfismo.
- Más aún, si $|G| = |H|$, entonces f es un isomorfismo.

Ejemplo. Usando el Teorema 1.28, podemos dar muchos ejemplos de grupos isomorfos:

1. Si consideramos el grupo cíclico de orden n : $C_n = \langle x \mid x^n = 1 \rangle$.

Observamos que en \mathbb{Z}_n el elemento $\bar{1}$ también verifica la propiedad $x^n = 1$, ya que:

$$n \cdot \bar{1} = \underbrace{\bar{1} + \dots + \bar{1}}_{n \text{ veces}} = 0$$

De esta forma, por el Teorema 1.28, sabemos que existe un homomorfismo $f : C_n \rightarrow \mathbb{Z}_n$, de forma que $f(x) = \bar{1}$.

Más aún, como $\mathbb{Z}_n = \langle \bar{1} \rangle$ y $|C_n| = n = |\mathbb{Z}_n|$, tenemos que f es un isomorfismo de grupos, por lo que $C_n \cong \mathbb{Z}_n$.

2. Si ahora consideramos el grupo de Klein abstracto:

$$V^{\text{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx \rangle$$

Podemos intentar relacionarlo con el grupo directo $\mathbb{Z}_2 \times \mathbb{Z}_2$, ya que los elementos $(0, 1)$ y $(1, 0)$ cumplen las relaciones enunciadas:

$$\begin{aligned} 2 \cdot (0, 1) &= (0, 1) + (0, 1) = (0, 0) \\ 2 \cdot (1, 0) &= (1, 0) + (1, 0) = (0, 0) \\ (0, 1) + (1, 0) &= (1, 1) = (1, 0) + (0, 1) \end{aligned}$$

Por lo que existirá un homomorfismo $f : V^{\text{abs}} \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ de forma que $f(x) = (0, 1)$ y $f(y) = (1, 0)$.

Más aún, como $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (0, 1), (1, 0) \rangle$ y es claro que $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4 = |V^{\text{abs}}|$, tenemos que f es un isomorfismo, por lo que $V^{\text{abs}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

3. Si tratamos ahora de relacionar el grupo de Klein abstracto (visto en el ejemplo anterior) con el grupo de Klein:

$$V = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Como $(1\ 2)(3\ 4)$ y $(1\ 3)(2\ 4)$ verifican que:

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

Por el Teorema de Dyck, existe un homomorfismo $g : V^{\text{abs}} \rightarrow V$ de forma que $g(x) = (1\ 2)(3\ 4)$ y $g(y) = (1\ 3)(2\ 4)$.

Como hemos visto ya que $V = \langle g(x), g(y) \rangle$ y que $|V^{\text{abs}}| = 4 = |V|$, g es un isomorfismo. Tenemos que $V^{\text{abs}} \cong V$.

Como vimos que \cong es una relación de equivalencia, también tendremos que $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Consideramos ahora el grupo diédrico de orden 3:

$$D_3 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^2s \rangle$$

Que vamos a intentar relacionar con S_3 . Como $(1\ 2)$ y $(1\ 2\ 3)$ verifican que:

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

Tenemos que existe un homomorfismo $f : D_3 \rightarrow S_3$ de forma que $f(r) = (1\ 2\ 3)$ y $f(s) = (1\ 2)$. Como además tenemos que¹¹ $S_3 = \langle (1\ 2)(1\ 2\ 3) \rangle$ y que $|D_3| = 2 \cdot 3 = 6 = 3! = |S_3|$, concluimos que f es un isomorfismo, por lo que $D_3 \cong S_3$.

¹¹Esto se vio en la Proposición 1.20.

5. Si consideramos el grupo lineal de orden 2 sobre \mathbb{Z}_2 :

$$\mathrm{GL}_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

Y tratamos de relacionarlo con $S_3 = \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^2s \rangle$, como tenemos que:

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^3 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

Entonces, existe un homomorfismo $f : S_3 \rightarrow \mathrm{GL}_2(\mathbb{Z}_2)$ de forma que:

$$f(r) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad f(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Además, como (ver el Ejercicio 3.2.18):

$$\mathrm{GL}_2(\mathbb{Z}_2) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

Y ambos tienen el mismo número de elementos, f es un isomorfismo.

6. Fijado $n \in \mathbb{N} \setminus \{0, 3\}$, si ahora consideramos el grupo simétrico de orden n , S_n y el grupo diédrico de orden n , D_n , como $|D_n| = 2n \neq n! = |S_n|$ no vamos a tener un isomorfismo de grupos. Sin embargo, los elementos:

$$(1 \ 2 \ \dots \ n), \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix} \in S_n$$

Verifican todas las propiedades de la presentación de D_n , por lo que existirá un homomorfismo $f : D_n \rightarrow S_n$ de forma que

$$\begin{aligned} f(r) &= (1 \ 2 \ \dots \ n) \\ f(s) &= \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix} \end{aligned}$$

7. Si consideramos ahora:

$$Q_2^{\mathrm{abs}} = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$$

Y pensamos en relacionarlo con $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$, como tenemos que:

$$\begin{aligned} i^4 &= 1 \\ j^2 &= -1 = i^2 \\ ji(-j) &= j(-k) = -i \end{aligned}$$

Sabemos que existe un homomorfismo $f : Q_2^{\mathrm{abs}} \rightarrow Q_2$ de forma que $f(x) = i$ y $f(y) = j$. Además, como $Q_2 = \langle i, j \rangle$ y $|Q_2^{\mathrm{abs}}| = 4 = |Q_2|$, tenemos que f es un isomorfismo, por lo que $Q_2^{\mathrm{abs}} \cong Q_2$.

8. Como último ejemplo, si consideramos $k, n \in \mathbb{N}$, $k \geq 3$ con $k \mid n$ y consideramos los grupos diédricos:

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, sr = r^{-1}s \rangle$$

$$D_k = \langle r_1, s_1 \mid r_1^k = 1, s_1^2 = 1, s_1 r_1 = r_1^{-1} s_1 \rangle$$

Y tratamos de relacionarlos, como $k \mid n$, existirá $p \in \mathbb{N}$ de forma que $n = kp$.

Como $r_1, s_1 \in D_k$ verifican que:

$$r_1^n = r_1^{kp} = (r_1^k)^p = 1^p = 1$$

$$s_1^2 = 1$$

$$s_1 r_1 = r_1^{-1} s_1$$

Tenemos por el Teorema 1.28 que existe un homomorfismo $f : D_n \rightarrow D_k$ de forma que $f(r) = r_1$ y $f(s) = s_1$.

1.6. Resumen de grupos

Para finalizar este capítulo, haremos un breve repaso de los grupos vistos hasta el momento, ya que los usaremos de forma constante a lo largo de la asignatura, por lo que conviene tenerlos siempre presentes.

Grupo Trivial. $(\{e\}, *, e)$.

Grupos de los enteros módulo n . $(\mathbb{Z}_n, +)$, $(\mathcal{U}(\mathbb{Z}_n), \cdot)$.

Grupo de raíces n -ésimas de la unidad.

$$\mu_n = \left\{ 1, \xi, \xi^2, \dots, \xi^{n-1} \mid \xi = \cos\left(\frac{2\pi}{n}\right) + i \operatorname{sen}\left(\frac{2\pi}{n}\right) \right\} \subseteq \mathbb{C}$$

Grupo lineal de orden n . Sea \mathbb{F} un cuerpo:

$$\operatorname{GL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) \neq 0\}$$

Grupo lineal especial de orden n . Sea \mathbb{F} un cuerpo:

$$\operatorname{SL}_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid \det(A) = 1\}$$

Potencias de grupos. Sea G un grupo y X un conjunto:

$$G^X = \operatorname{Apl}(X, G) = \{f : X \rightarrow G \mid f \text{ aplicación}\}$$

n -ésimo grupo diédrico. Sea $n \in \mathbb{N}$:

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

n -ésimo grupo simétrico. Sea X un conjunto con $|X| = n \in \mathbb{N}$:

$$S_n = \operatorname{Perm}(X) = \{f : X \rightarrow X \mid f \text{ biyectiva}\}$$

n -ésimo grupo alternado. Sea $n \in \mathbb{N}$:

$$A_n = \{\sigma \in S_n \mid \sigma \text{ es par}\}$$

Grupo cíclico de orden n . Sea $n \in \mathbb{N}$:

$$C_n = \langle x \mid x^n = 1 \rangle = \{1, x, x^2, x^3, \dots, x^{n-1}\}$$

Grupo de los cuaternios.

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

Grupo abstracto Q_2^{abs} .

$$\begin{aligned} Q_2^{\text{abs}} &= \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle \\ &= \{1, x, x^2, x^3, y, yx, yx^2, yx^3\} \end{aligned}$$

Grupo de Klein. Sea $n \in \mathbb{N}$ con $n \geq 4$:

$$V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq S_n$$

Grupo de Klein abstracto.

$$V^{\text{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx \rangle = \{1, x, y, xy\}$$

2. Subgrupos, Generadores, Retículos y Grupos cíclicos

Definición 2.1 (Subgrupo). Dados dos grupos G y H , decimos que H es un subgrupo de G , denotado por $H < G$ si $H \subseteq G$ y la aplicación de inclusión¹ $i : H \rightarrow G$ es un homomorfismo de grupos.

Observación. Dado un grupo $(G, *, e)$, este tendrá siempre dos subgrupos:

- $(\{e\}, *, e)$, al que llamaremos subgrupo trivial.
- El propio $(G, *, e)$

Definición 2.2. Sea H un subgrupo de otro G , diremos que H es un subgrupo impropio de G si H es el grupo trivial o el propio G . En otro caso, diremos que H es un subgrupo propio de G .

Notación. Recordamos la notación que ya usábamos en Álgebra I para, fijado $n \in \mathbb{N} \setminus \{0\}$, denotar a todos los múltiplos de n en \mathbb{Z} :

$$n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$$

Ejemplo. Vemos claramente que:

1. $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$
2. $\{r^k \mid k \leq n, r \in D_n\} < D_n$
3. $n\mathbb{Z} < \mathbb{Z}$ para todo $n \in \mathbb{N}$.
4. $\text{SL}_n(\mathbb{F}) < \text{GL}_n(\mathbb{F})$
5. $(\mathbb{Q}^*, \cdot) \not< (\mathbb{R}, +)$ No es un subgrupo, ya que $i(1) = 1 \neq 0$.
6. $(\mathbb{Z}^+, +) \not< (\mathbb{Z}, +)$, ya que $(\mathbb{Z}^+, +)$ no es un grupo.
7. $D_6 \not< D_8$, ya que $D_6 \not\subseteq D_8$.

Observación. Si G , H y T son grupos de forma que $G < H < T$, entonces $G < T$.

Demostración. La transitividad de \subseteq nos da que $G \subseteq H \subseteq T$. Por otra parte, como las inclusiones $j : G \rightarrow H$ y $k : H \rightarrow T$ son homomorfismos, tendremos que $i = k \circ j : G \rightarrow T$ es un homomorfismo. \square

¹Viene dada por $i(x) = x$, para todo $x \in H$.

Proposición 2.1. Sea G un grupo y $\emptyset \neq H \subseteq G$, entonces son equivalentes:

- i) $H < G$
- ii) Se verifican:
 - (a) Si $x, y \in H$ entonces $xy \in H$.
 - (b) $1 \in H$.
 - (c) Si $x \in H$, entonces $x^{-1} \in H$.
- iii) Si $x, y \in H$, entonces $xy^{-1} \in H$.

Demostración. Veamos las implicaciones de forma cíclica:

$i) \implies ii)$ Como H es un grupo, por su definición se han de cumplir (a), (b) y (c).

$ii) \implies iii)$ Si $x, y \in H$, entonces $y^{-1} \in H$, por lo que tendremos que $xy^{-1} \in H$.

$iii) \implies i)$ Como $\emptyset \neq H$, existirá al menos un $x \in H$, por lo que $xx^{-1} = 1 \in H$. Además, si $x \in H$ también tendremos que $1x^{-1} = x^{-1} \in H$. Para ver que H es un grupo, tan solo nos falta ver que su operación interna está bien definida; es decir, que si $x, y \in H$, entonces $xy \in H$. Dados $x, y \in H$, tendremos que $y^{-1} \in H$, por lo que:

$$xy = x(y^{-1})^{-1} \in H$$

Con esto tenemos ya que H es un grupo. Al considerar en H la misma operación que en G , tenemos directamente que $i : H \rightarrow G$ es un homomorfismo, ya que $id : H \rightarrow H$ es un homomorfismo y al extender el codominio para considerar la aplicación inclusión i , seguirá siendo un homomorfismo².

□

Proposición 2.2. Sea G un grupo finito y $\emptyset \neq H \subseteq G$, entonces son equivalentes:

- i) $H < G$
- ii) Si $x, y \in H$, entonces $xy \in H$

Demostración. Veamos las dos implicaciones:

$i) \implies ii)$ Se verifica por ser H un grupo.

$ii) \implies i)$ Como G es finito, por la Proposición 1.9, para todo $x \in G$ existirá $n > 0$ de forma que $x^n = 1$, por lo que $x^{-1} = x^{n-1}$. De esto deducimos que $x^{-1} \in H$ y que $1 = xx^{-1} \in H$. Por la Proposición 2.1, $H < G$.

□

Ejemplo. Se deja como ejercicio comprobar que:

1. $A_n < S_n$

²Notemos que si en H tenemos una operación distinta que en G esto no siempre será cierto y habrá que comprobar que $i : H \rightarrow G$ es un homomorfismo.

2. Todo subgrupo de \mathbb{Z} es de la forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.
3. $V < S_4$
4. Si $n \mid m$, entonces $D_n < D_m$

Definición 2.3. Sea G un grupo, $f : G \rightarrow G'$ una aplicación, y $H \subseteq G$, $H' \subseteq G'$, definimos:

- El conjunto imagen directa de H por f como el conjunto:

$$f_*(H) = \{f(x) \mid x \in H\} \subseteq G'$$

- El conjunto imagen inversa de H' por f como el conjunto:

$$f^*(H') = \{x \in G \mid f(x) \in H'\} \subseteq G$$

Proposición 2.3. Sea $f : G \rightarrow G'$ un homomorfismo de grupos, entonces:

- i) Si $H < G$, entonces $f_*(H) < G'$
- ii) Si $H' < G'$, entonces $f^*(H') < G$

Demostración. Demostramos las dos implicaciones:

- i) Sean $x, y \in f_*(H)$, entonces $\exists a, b \in H$ de forma que $x = f(a), y = f(b)$. Como H es un subgrupo de G , tendremos que $ab^{-1} \in H$, por lo que:

$$f(ab^{-1}) = f(a)f(b)^{-1} = xy^{-1} \in f_*(H)$$

Concluimos que $f_*(H)$ es un subgrupo de G' .

- ii) Sean $x, y \in f^*(H')$, entonces $a = f(x), b = f(y) \in H'$. Por ser H' un subgrupo de G' , tendremos que

$$ab^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in H'$$

Por tanto, $xy^{-1} \in f^*(H')$. Concluimos que $f^*(H')$ es un subgrupo de G .

□

Proposición 2.4. Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de G , entonces la intersección de todo ellos sigue siendo un subgrupo de G :

$$\bigcap_{i \in I} H_i < G$$

Demostración. En primer lugar, como $H_i < G$ para todo $i \in I$, se ha de verificar que $1 \in H_i \forall i \in I$, por lo que $1 \in \bigcap_{i \in I} H_i \neq \emptyset$. Como la intersección es no vacía, podemos pensar en aplicar el tercer punto de la Proposición 2.1 para comprobar que es un subgrupo de G .

Para ello, sean $x, y \in \bigcap_{i \in I} H_i$, entonces $x, y \in H_i$ para todo $i \in I$, por lo que por ser $H_i < G$, tendremos que $xy^{-1} \in H_i \forall i \in I$, luego:

$$xy^{-1} \in \bigcap_{i \in I} H_i$$

Concluimos que $\bigcap_{i \in I} H_i$ es un subgrupo de G . □

Ejemplo. En general, la unión de subgrupos no es un subgrupo:

$$2\mathbb{Z} \cup 3\mathbb{Z} \not\subseteq \mathbb{Z}$$

Ya que $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ y $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

2.1. Generadores de subgrupos

Definición 2.4 (Subgrupo generado). Sea G un grupo y $S \subseteq G$, definimos el subgrupo generado por S como el menor subgrupo de G que contiene a S , es decir:

$$\langle S \rangle = \bigcap \{H < G \mid S \subseteq H\}$$

Observación. Notemos que, gracias a la Proposición 2.4, $\langle S \rangle$ efectivamente es un subgrupo de G .

Proposición 2.5. Sea (G, \cdot, e) un grupo, $S \subseteq G$, entonces:

- Si $S = \emptyset$, entonces $\langle S \rangle = \{e\}$, el grupo trivial.
- Si $S \neq \emptyset$, entonces $\langle S \rangle = \{x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \mid m \geq 1, x_i \in S, \gamma_i \in \mathbb{Z}\}$

Demostración. Distinguimos casos:

- Si $S = \emptyset$, entonces $\{e\} < G$ con $S \subseteq \{e\}$. Como $\{e\}$ solo tiene un elemento y todo subgrupo de G contiene a e , concluimos que:

$$\langle S \rangle = \bigcap \{H < G \mid S \subseteq H\} = \{e\}$$

- Si $S \neq \emptyset$, si notamos $\mathcal{S} = \bigcap \{H < G \mid S \subseteq H\}$, queremos ver que:

$$\mathcal{S} = \{x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \mid m \geq 1, x_i \in S, \gamma_i \in \mathbb{Z}\}$$

\supseteq) Como $S \subseteq \mathcal{S}$ y \mathcal{S} es un grupo, tendremos que:

$$x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \in \mathcal{S} \quad x_i \in S, \gamma_i \in \mathbb{Z} \quad \forall 1 \leq i \leq m$$

\subseteq) Si llamamos A al conjunto de la derecha, A es un grupo, ya que si tomamos $a, b \in A$, existirán x_1, \dots, x_p y y_1, \dots, y_q en S y $\gamma_1, \dots, \gamma_p, \alpha_1, \dots, \alpha_q \in \mathbb{Z}$ de forma que:

$$a = x_1^{\gamma_1} \dots x_p^{\gamma_p} \quad b = y_1^{\alpha_1} \dots y_q^{\alpha_q}$$

Por lo que

$$ab^{-1} = x_1^{\gamma_1} \dots x_p^{\gamma_p} y_q^{-\alpha_q} \dots y_1^{-\alpha_1} \in A$$

Lo que demuestra que A es un subgrupo de G . Además, como es claro que $S \subseteq A$, tenemos un grupo del que S es subconjunto, por lo que por ser \mathcal{S} el menor subgrupo que contiene a S , está claro que $\mathcal{S} \subseteq A$. □

Corolario 2.5.1. Si $S \subseteq G$ de forma que $\langle S \rangle = G$, entonces S es un conjunto de generadores de G .

Demostración. Por la Proposición 2.5, sabemos que si $\langle S \rangle = G$, entonces cualquier elemento $x \in G$ se puede expresar de la forma:

$$x = x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \quad x_i \in S, \gamma_i \in \mathbb{Z}, \quad \forall 1 \leq i \leq m$$

Por lo que S es un conjunto de generadores de G . □

Ejemplo. Ejemplos interesantes de subgrupos generados por ciertos conjuntos son:

1. Si $S = \{r\} \subseteq D_n$, entonces $\langle S \rangle = \{1, r, r^2, \dots, r^{n-1}\}$
2. Si $S = \{s\} \subseteq D_n$, entonces $\langle S \rangle = \{1, s\}$
3. Si $S = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4)\} \subseteq S_4$, entonces $\langle S \rangle = V$
4. Si $S = \{(x_1\ x_2\ x_3) \mid x_1 < x_2 < x_3\} \subseteq S_n$, entonces $\langle S \rangle = A_n$
5. Si $S = \left\{ \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \subseteq \text{GL}_2(\mathbb{C})$, entonces $\langle S \rangle < \text{GL}_2(\mathbb{C})$.

En la Proposición 2.4 vimos que la intersección de una familia arbitraria de subgrupos era un subgrupo, mientras que con el ejemplo de $2\mathbb{Z} \cup 3\mathbb{Z} \subseteq \mathbb{Z}$, vimos que, en general, la unión de dos subgrupos no es un subgrupo. Sin embargo, cabe preguntarse de qué forma podemos hacer una operación parecida con subgrupos para sí obtener un subgrupo. De esto nace la siguiente definición.

Definición 2.5 (Compuesto). Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de un grupo G , llamamos compuesto de los subgrupos H_i , denotado por $\bigvee_{i \in I} H_i$, al subgrupo:

$$\bigvee_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i \right\rangle$$

Cuando tengamos un número finito de subgrupos $\{H_1, H_2, \dots, H_n\}$, notaremos:

$$H_1 \vee H_2 \vee \dots \vee H_n$$

Notemos que es natural la definición, ya que como la unión de subgrupos no es en general un subgrupo, buscamos el menor subgrupo que contenga a la unión de subgrupos, que por definición es el compuesto de la familia de subgrupos que queríamos unir.

2.2. Retículo de subgrupos de un grupo

Introduciremos ahora el concepto de retículo³, estructura algebraica de gran interés que usaremos brevemente para trabajar de forma cómoda con el conjunto de todos los subgrupos de un grupo.

³Que en el contexto de teoría de conjuntos o del orden puede tener otra definición.

Definición 2.6 (Retículo). Un retículo es una tripleta (L, \vee, \wedge) donde:

- L es un conjunto no vacío.
- \wedge y \vee son dos operaciones⁴ binarias en L que verifican las leyes:

i) Conmutativa:

$$a \vee b = b \vee a \quad a \wedge b = b \wedge a$$

ii) Asociativa:

$$a \vee (b \vee c) = (a \vee b) \vee c \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

iii) de Absorción:

$$a \vee (a \wedge b) = a \quad a \wedge (a \vee b) = a$$

iv) de Idempotencia:

$$a \vee a = a \quad a \wedge a = a$$

En el caso de que (L, \vee, \wedge) sea un retículo, es común definir una relación binaria notada por “ \leq ” y definida por:

$$a \leq b \iff a \vee b = b \iff a \wedge b = a$$

donde para la segunda equivalencia hemos empleado la conmutatividad y la propiedad de absorción.

Proposición 2.6. *Todo retículo (L, \vee, \wedge) junto con la relación de orden \leq que se define a partir de sus operaciones es un conjunto parcialmente ordenado.*

Demostración. Hemos de probar las propiedades:

- Reflexiva. Por la propiedad de idempotencia, dado $a \in L$, tenemos que:

$$a \vee a = a \implies a \leq a$$

- Antisimétrica. Sean $a, b \in L$ de forma que $a \leq b$ y $b \leq a$. Por definición de \leq , tenemos que:

$$a \vee b = b \quad b \vee a = a$$

Y aplicando la conmutatividad de \vee llegamos a que:

$$a = a \vee b = b \vee a = b$$

- Transitiva. Sean $a, b, c \in L$ de forma que $a \leq b$ y $b \leq c$, es decir, $a \vee b = b$ y $b \vee c = c$, entonces:

$$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$$

De donde deducimos que $a \leq c$.

□

⁴Es común referirse a \vee por “supremo” y a \wedge por “ínfimo”.

Ejemplo. Ejemplos de retículos son:

1. El retículo endoplasmático rugoso.
2. Dado un número $n \in \mathbb{N}$, el conjunto de divisores de n :

$$D(n) = \{m \in \mathbb{N} : m \text{ divide a } n\}$$

Junto con las operaciones de:

$$a \vee b = \text{mcm}(a, b)$$

$$a \wedge b = \text{mcd}(a, b)$$

forma un retículo⁵. En este, la relación de orden que obtenemos es la de “ser divisor de”; es decir, si $a, b \in D(n)$, entonces:

$$a \leq b \iff a \mid b$$

3. En la asignatura LMD vimos que los álgebras de Boole eran retículos.

Lema 2.7. Sea G un grupo y $T, U < G$, entonces:

$$\langle \langle T \rangle \cup U \rangle = \langle T \cup U \rangle$$

Demostración. Hagámoslo por doble inclusión:

\supseteq) Basta ver que:

$$T \subseteq \langle T \rangle \implies T \cup U \subseteq \langle T \rangle \cup U \implies \langle T \cup U \rangle \subseteq \langle \langle T \rangle \cup U \rangle$$

\subseteq) Sea $x \in \langle \langle T \rangle \cup U \rangle$, entonces existirán $\alpha_1, \dots, \alpha_n \in \langle T \rangle$, $u_1, \dots, u_m \in U$ y $\gamma_1, \dots, \gamma_{n+m} \in \mathbb{Z}$ de forma que:

$$x = \alpha_1^{\gamma_1} \dots \alpha_n^{\gamma_n} u_1^{\gamma_{n+1}} \dots u_m^{\gamma_{n+m}}$$

Pero por ser $\alpha_1, \dots, \alpha_n \in \langle T \rangle$, podemos encontrar $t_{ij} \in T$ y $\delta_{ij} \in \mathbb{Z}$ de forma que:

$$\alpha_1 = t_{11}^{\delta_{11}} \dots t_{1n_1}^{\delta_{1n_1}}$$

$$\vdots$$

$$\alpha_n = t_{n1}^{\delta_{n1}} \dots t_{nn_n}^{\delta_{nn_n}}$$

Por lo que:

$$x = t_{11}^{\delta_{11}} \dots t_{1n_1}^{\delta_{1n_1}} \dots t_{nn_n}^{\delta_{nn_n}} u_1^{\gamma_{n+1}} \dots u_m^{\gamma_{n+m}} \in \langle T \cup U \rangle$$

□

⁵Es un buen ejercicio comprobarlo.

Proposición 2.8. Sea G un grupo, si definimos el conjunto de subgrupos de G :

$$\Lambda = \{H \subseteq G \mid H < G\}$$

Se verifica que Λ es un retículo, junto con las operaciones:

$$T \vee U = \langle T \cup U \rangle$$

$$T \wedge U = T \cap U$$

Demostración. De Álgebra I ya sabemos que la intersección de conjuntos es conmutativa, asociativa y que tiene la propiedad de idempotencia. Veamos estas para el compuesto de dos subgrupos, que se deducen a partir de las propiedades conmutativa, asociativa y de idempotencia para la unión de dos conjuntos:

- Conmutativa. Sean $T, U \in \Lambda$:

$$T \vee U = \langle T \cup U \rangle = \langle U \cup T \rangle = U \vee T$$

- Asociativa. Sean $T, U, V \in \Lambda$:

$$\begin{aligned} T \vee (U \vee V) &= T \vee \langle U \cup V \rangle = \langle T \cup \langle U \cup V \rangle \rangle \stackrel{(*)}{=} \langle T \cup U \cup V \rangle \\ &\stackrel{(*)}{=} \langle \langle T \cup U \rangle \cup V \rangle = \langle T \cup U \rangle \vee V = (T \vee U) \vee V \end{aligned}$$

Donde en $(*)$ hemos aplicado el Lema anterior.

- Idempotencia. Sea $T \in \Lambda$:

$$T \vee T = \langle T \cup T \rangle = \langle T \rangle \stackrel{(*)}{=} T$$

Donde en $(*)$ hemos usado que T es un grupo, por ser subgrupo de G .

Finalmente, nos queda comprobar las propiedades de absorción. Para ello, sean $T, U \in \Lambda$:

$$\begin{aligned} T \vee (T \cap U) &= \langle T \cup (T \cap U) \rangle = \langle (T \cup T) \cap (T \cup U) \rangle = \langle T \cap (T \cup U) \rangle = \langle T \rangle = T \\ T \cap (T \vee U) &= T \cap \langle T \cup U \rangle = T \end{aligned}$$

□

Al trabajar con retículos, una estructura que surge de forma natural son los diagramas de Hasse, que nos permiten comprender mucho mejor la estructura de un retículo concreto.

Definición 2.7 (Diagrama de Hasse). Sea (L, \leq) un conjunto finito parcialmente ordenado, definimos su diagrama de Hasse como el grafo dirigido (V, E) donde:

- Los vértices son cada uno de los elementos de L , es decir: $V = L$.

- Dados dos vértices $a, b \in V$ con $a \neq b$, tendremos una arista de a a b ($a \rightarrow b$) si $a \leq b$ y no existe ningún elemento $c \in V$ con $a \neq c \neq b$ de forma que $a \leq c \leq b$.

Es decir, escribiremos $a \rightarrow b$ en el caso en el que $a \leq b$, obviando los ciclos (ya que \leq es una relación simétrica) y las relaciones que puedan deducirse de la transitividad de \leq : si $a \leq b$ y $b \leq c$, no consideraremos la arista $a \rightarrow c$.

Notación. Por comodidad y claridad a la hora de dibujar los diagramas de Hasse, no dibujaremos grafos dirigidos, sino que lo que haremos será ordenar los vértices por “niveles”: colocaremos abajo del todo los vértices que son menores o iguales que todos los demás (colocando en un mismo nivel aquellos elementos que no son comparables entre sí⁶). En el nivel inmediatamente superior a este, colocaremos los elementos que son menores o iguales a todos los demás salvo a estos últimos. Repetiremos el proceso de forma sucesiva, hasta colocar en el último nivel aquellos elementos que son mayores o iguales que todos los demás.

De esta forma, tendremos el diagrama de Hasse ordenado por niveles, donde podremos ver “qué tan grande” es cada elemento. Además, no necesitaremos dibujar las aristas dirigidas, ya que dibujaremos aristas no dirigidas pensando que todas las aristas están dirigidas hacia arriba.

2.2.1. Ejemplos

Ejemplo. Diagramas de Hasse para ciertos retículos⁷ son:

1. Para $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$:

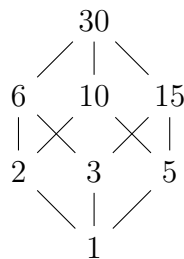


Figura 2.1: Diagrama de Hasse para $D(30)$.

2. Para \mathcal{B}^3 , el álgebra de Boole con 3 elementos, tenemos:

⁶Ya que no tenemos por qué tener un orden total.

⁷Notemos que cualquier retículo es un conjunto parcialmente ordenado.

Figura 2.2: Diagrama de Hasse para \mathcal{B}^3 .

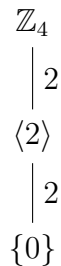
Centrándonos ya en los retículos que nos interesan, daremos a continuación varios ejemplos de retículos de los retículos formados por los subgrupos de un grupo dado, que representaremos mediante sus diagramas de Hasse (en estos aparecerán las aristas etiquetadas con números, que por ahora ignoraremos, pero que luego señalaremos lo que significan).

Ejemplo. Veamos varios ejemplos con grupos de la forma \mathbb{Z}_n :

1. Para calcular el retículo de subgrupos de \mathbb{Z}_4 , hemos de pensar primero en todos los subgrupos posibles de \mathbb{Z}_4 . Para ello, vemos que:

$$\begin{aligned}
 \langle 0 \rangle &= \{0\} \\
 \langle 1 \rangle &= \mathbb{Z}_4 \\
 \langle 2 \rangle &= \{0, 2\} \\
 \langle 3 \rangle &= \mathbb{Z}_4
 \end{aligned}$$

Concluimos que $\Lambda_{\mathbb{Z}_4} = \{\{0\}, \{0, 2\}, \mathbb{Z}_4\}$. Pasamos ahora a ver cómo se relacionan mediante su diagrama de Hasse.

Figura 2.3: Diagrama de Hasse para los subgrupos de \mathbb{Z}_4 .

2. En \mathbb{Z}_6 tenemos que⁸:

$$\begin{aligned}
 \langle 1 \rangle &= \langle 5 \rangle = \mathbb{Z}_6 \\
 \langle 2 \rangle &= \langle 4 \rangle = \{0, 2, 4\} \\
 \langle 3 \rangle &= \{0, 3\}
 \end{aligned}$$

⁸Hemos escrito directamente los subgrupos de \mathbb{Z}_6 , pero lo que hemos hecho para buscarlos todos es pensar en todos los posibles conjuntos de generadores.

Y podemos dibujar su diagrama de Hasse:

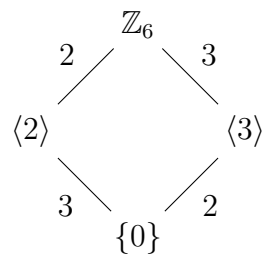


Figura 2.4: Diagrama de Hasse para los subgrupos de \mathbb{Z}_6 .

3. En \mathbb{Z}_8 , tenemos que:

$$\begin{aligned}\langle 1 \rangle &= \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_8 \\ \langle 2 \rangle &= \langle 6 \rangle = \{0, 2, 4, 6\} \\ \langle 4 \rangle &= \{0, 4\}\end{aligned}$$

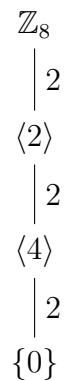
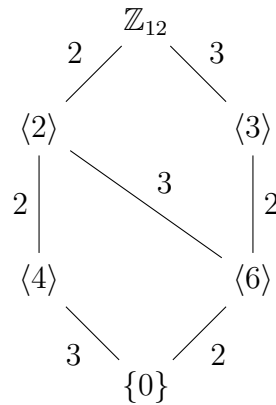


Figura 2.5: Diagrama de Hasse para los subgrupos de \mathbb{Z}_8 .

4. En \mathbb{Z}_{12} , tenemos:

$$\begin{aligned}\langle 1 \rangle &= \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \mathbb{Z}_{12} \\ \langle 2 \rangle &= \langle 10 \rangle = \{0, 2, 4, 6, 8, 10\} \\ \langle 3 \rangle &= \langle 9 \rangle = \{0, 3, 6, 9\} \\ \langle 4 \rangle &= \langle 8 \rangle = \{0, 4, 8\} \\ \langle 6 \rangle &= \{0, 6\}\end{aligned}$$

Figura 2.6: Diagrama de Hasse para los subgrupos de \mathbb{Z}_{12} .

Ejemplo. Si trabajamos ahora con otro tipo de grupos:

1. Si consideramos el grupo de Klein:

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

Todos sus subgrupos posibles son:

$$V, \langle (1\ 2)(3\ 4) \rangle, \langle (1\ 3)(2\ 4) \rangle, \langle (1\ 4)(2\ 3) \rangle, \{1\}$$

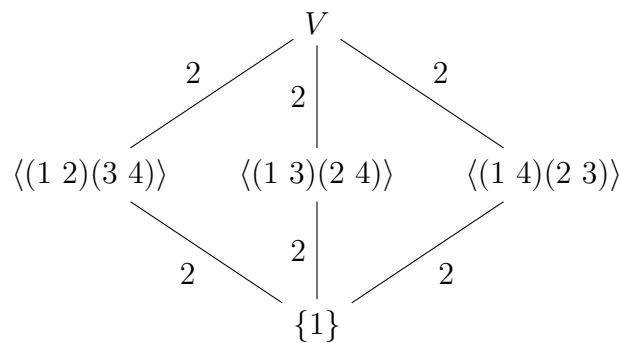


Figura 2.7: Diagrama de Hasse para los subgrupos del grupo de Klein.

2. En el grupo de los cuaternios:

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

Los subgrupos posibles son:

$$Q_2, \langle i \rangle, \langle j \rangle, \langle k \rangle, \langle -1 \rangle, \{1\}$$



Figura 2.8: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

3. En $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, los posibles subgrupos son:

$$S_3, \langle (1\ 2\ 3) \rangle, \langle (1\ 2) \rangle, \langle (1\ 3) \rangle, \langle (2\ 3) \rangle, \{1\}$$

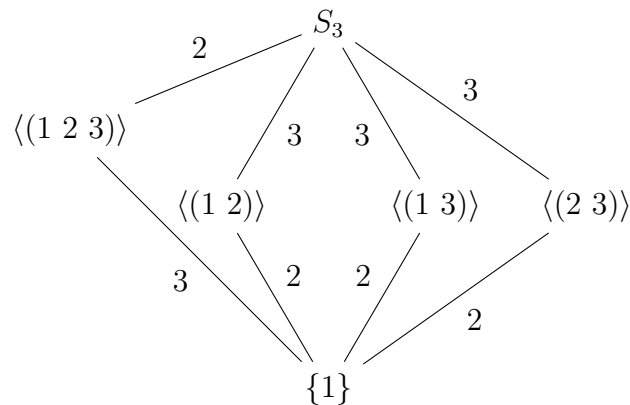


Figura 2.9: Diagrama de Hasse para los subgrupos de S_3 .

4. En $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, los posibles subgrupos son:

$$\begin{aligned}
 \langle r \rangle &= \langle r^3 \rangle = \{1, r, r^2, r^3\} \\
 \langle r^2 \rangle &= \{1, r^2\} \\
 \langle s \rangle &= \{1, s\} \\
 \langle sr \rangle &= \{1, sr\} \\
 \langle sr^2 \rangle &= \{1, sr^2\} \\
 \langle sr^3 \rangle &= \{1, sr^3\} \\
 \langle r^2, s \rangle &= \{1, r^2, s, sr^2\} \\
 \langle r^2, sr \rangle &= \{1, r^2, sr, sr^3\}
 \end{aligned}$$

Figura 2.10: Diagrama de Hasse para los subgrupos de D_4 .

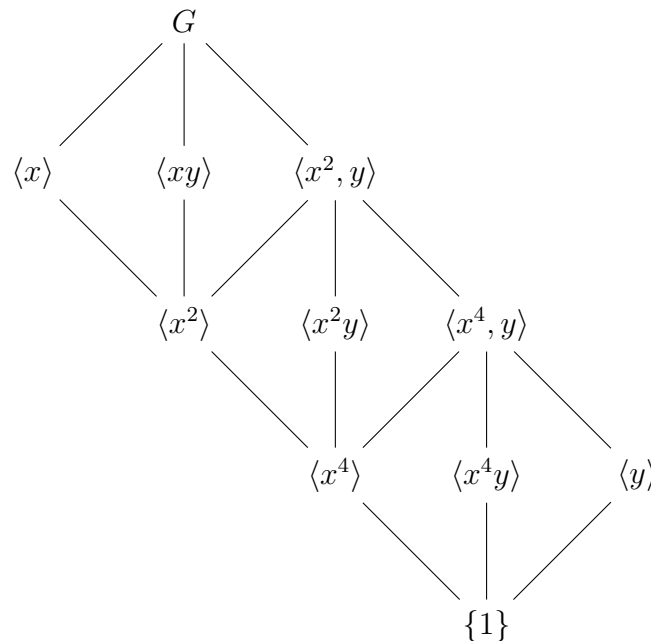
Ejemplo. Obtenemos un ejemplo interesante al considerar los grupos:

$$G = \langle x, y \mid x^8 = y^2 = 1, xy = yx \rangle$$

$$H = \langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$$

Donde H recibe el nombre de “grupo modular de orden 16”, notemos que ambos grupos tienen orden 16. Además, como G es conmutativo y H no, sabemos que no pueden ser isomorfos. Sin embargo, sucede algo particular cuando consideramos sus diagramas de Hasse. Antes de ello, debemos calcular todos los subgrupos de cada uno, cosa que no vamos a detallar pero sí daremos aquellos subgrupos más grandes:

- G tiene 3 subgrupos de orden 8: $\langle x^2, y \rangle$, $\langle x \rangle$, $\langle xy \rangle$.
- H tiene 3 subgrupos de orden 8: $\langle u, v^2 \rangle$, $\langle u \rangle$, $\langle uv \rangle$.

Figura 2.11: Diagrama de Hasse para los subgrupos de G .

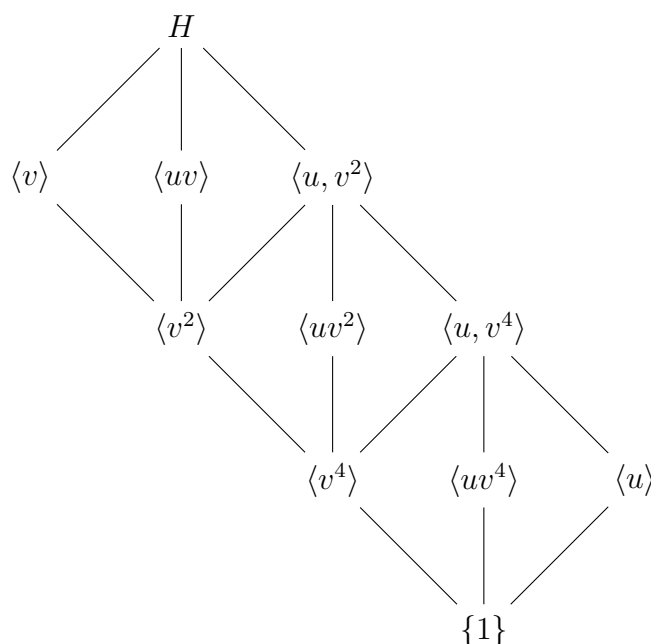


Figura 2.12: Diagrama de Hasse para los subgrupos de H .

A lo largo de todos estos ejemplos hemos debido darnos cuenta de una particularidad, que se pone de manifiesto especialmente en el ejemplo de los \mathbb{Z}_n . Resulta que los órdenes de los subgrupos que hemos ido obteniendo dividían al orden del grupo, resultado que luego demostraremos en general. Sin embargo, estamos ya en condiciones de demostrar que el contrarrecíproco no es cierto en general, es decir, no todos los divisores del orden de un grupo se corresponden con el orden de algún subgrupo suyo.

Proposición 2.9. *El orden del subgrupo divide al orden del grupo, pero no todos los divisores del orden del grupo se corresponden con el orden de algún subgrupo suyo.*

Veremos que el orden de todo subgrupo divide al orden del grupo (en caso de ser el grupo finito) en el Teorema de Lagrange (Teorema 2.13).

Ejemplo. Para ver que el recíproco no se cumple, consideramos:

$$A_4 = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3)\}$$

Que recordamos tiene de orden:

$$|A_4| = \frac{4!}{2} = 4 \cdot 3 = 12$$

Y todos los posibles divisores de 12 son:

$$D(12) = \{1, 2, 3, 4, 6, 12\}$$

Sin embargo, A_4 tiene:

- Un subgrupo de orden 1, $\{1\}$.

- Cuatro subgrupos de orden 3.
- Un subgrupo de orden 4, $V < A_4$.
- Tres subgrupos de orden 2.
- Un subgrupo de orden 12, A_4 .

Más aún, veamos que es imposible que tenga un subgrupo de orden 6.

Demostración. Supongamos que existe $H < A_4$ de forma que $|H| = 6$. En dicho caso, viendo todos los elementos de A_4 , concluimos que H debe contener al menos un 3-ciclo:

$$(x_1 \ x_2 \ x_3) \in H$$

En dicho caso, por ser H un subgrupo de A_4 , también debe estar su elemento inverso:

$$(x_1 \ x_3 \ x_2) \in H$$

Ahora, distingamos casos:

- Si H no tiene más 3-ciclos, la única posibilidad (observando nuevamente todos los elementos de A_4) es que H sea de la forma:

$$H = \{1, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3), (x_1 \ x_2 \ x_3), (x_1 \ x_3 \ x_2)\}$$

En cuyo caso, observemos que $V < H$. Sin embargo, $|V| = 4 \nmid 6 = |H|$, contradicción.

- Si H tiene otro 3-ciclo, por ejemplo $(x_1 \ x_2 \ x_4)$, también ha de contener a su inverso, por lo que:

$$\{(x_1 \ x_2 \ x_3), (x_1 \ x_3 \ x_2), (x_1 \ x_2 \ x_4), (x_1 \ x_4 \ x_2)\} \subseteq H$$

Sin embargo, como:

$$(x_1 \ x_2 \ x_3)(x_1 \ x_4 \ x_2) = (x_1 \ x_4 \ x_3)$$

Concluimos que también $(x_1 \ x_4 \ x_3)$ y su inverso: $(x_1 \ x_3 \ x_4)$ deben estar en H , luego H es un subgrupo formado por 6 3-ciclos, contradicción, ya que H debe también contener al 1.

Concluimos que no puede existir un subgrupo de A_4 con 6 elementos. □

2.3. Índice y Teorema de Lagrange

Definición 2.8. Sea G un grupo, $H, K < G$, definimos:

$$HK = \{hk \mid h \in H, k \in K\}$$

Proposición 2.10. Sea G un grupo, $H, K < G$, tenemos que HK es un subgrupo de G si y solo si $HK = KH$. En cuyo caso, tendremos que:

$$HK = H \vee K$$

Demostración. Por doble implicación:

\implies) Veamos que $KH = HK$ por doble inclusión:

\subseteq) Sean $k \in K, h \in H$, tenemos que:

$$kh = (h^{-1}k^{-1})^{-1} \in HK \implies KH \subseteq HK$$

\supseteq) Observemos que la única hipótesis que tenemos es que HK es un subgrupo de G (nada tenemos sobre KH). Sean $h \in H, k \in K$:

$$hk = (k^{-1}h^{-1})^{-1} \in HK$$

Por lo que $k^{-1}h^{-1} \in HK$, luego existirán $h_1 \in H, k_1 \in K$ de forma que:

$$k^{-1}h^{-1} = h_1k_1$$

Finalmente:

$$hk = (k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

\Leftarrow) Sean $hk, h_1k_1 \in HK$, queremos ver qué pasa con $hk(h_1k_1)^{-1}$:

$$hk(h_1k_1)^{-1} = hkk_1^{-1}h_1^{-1} \stackrel{(*)}{=} hk_2h_2 \stackrel{(**)}{=} hh_3k_3 \in HK$$

Donde:

- En $(*)$ hemos aplicado que K es un grupo, ya que si $k, k_1 \in K$, entonces $kk_1^{-1} \in K$, por lo que existirá $k_2 = kk_1^{-1} \in K$.
De forma análoga, como $h_1 \in H$, tenemos que $h_1^{-1} \in H$, por lo que existirá $h_2 = h_1^{-1} \in H$.
- En $(**)$ hemos aplicado que $k_2h_2 \in KH = HK$, por lo que existirán $h_3 \in H, k_3 \in K$ de forma que $k_2h_2 = h_3k_3$.

Falta ver que si $HK < G$ con $HK = KH$ (que ya sabemos que son equivalentes), entonces:

$$HK = H \vee K$$

\subseteq) Sea $x \in HK$, entonces $\exists h \in H, k \in K$ de forma que $x = hk \in \langle H \cup K \rangle = H \vee K$.

\supseteq) Sea $x \in H \vee K$, entonces sabemos que existen $\alpha_1, \dots, \alpha_n \in H \cup K$ y $\gamma_1, \dots, \gamma_n \in \mathbb{Z}$ de forma que:

$$x = \alpha_1^{\gamma_1} \dots \alpha_n^{\gamma_n}$$

Como $HK = KH$, tras varias conmutaciones de términos, existirán $h_1, \dots, h_p \in H, k_{p+1}, \dots, k_n \in K$ y $\delta_1, \dots, \delta_n \in \mathbb{Z}$ de forma que:

$$x = h_1^{\delta_1} \dots h_p^{\delta_p} k_{p+1}^{\delta_{p+1}} \dots k_n^{\delta_n}$$

Y por ser H y K grupos, tendremos que existen $h \in H$ y $k \in K$ de forma que:

$$\begin{aligned} h &= h_1^{\delta_1} \dots h_p^{\delta_p} \\ k &= k_{p+1}^{\delta_{p+1}} \dots k_n^{\delta_n} \end{aligned}$$

Por lo que $x = hk \in HK$. □

Definición 2.9. Sea G un grupo y $H < G$, definimos dos relaciones binarias en G :

- La relación ${}_H\sim$ definida por:

$$y {}_H\sim x \iff x^{-1}y \in H$$

- La relación \sim_H definida por:

$$y \sim_H x \iff yx^{-1} \in H$$

Proposición 2.11. Sea G un grupo y $H < G$, se verifica que ${}_H\sim$ y \sim_H son relaciones de equivalencia en G . Además, dado $x \in G$, se tiene que sus clases de equivalencia⁹ son de la forma:

$$\begin{aligned} {}_H[x] &= \{xh \mid h \in H\} \\ [x]_H &= \{hx \mid h \in H\} \end{aligned}$$

Demostración. Comprobemos primero que ${}_H\sim$ y \sim_H son relaciones de equivalencia:

- Propiedad reflexiva. Como H es un grupo, $1 \in H$, por lo que dado $x \in G$:

$$xx^{-1} = x^{-1}x = 1 \in H$$

De donde deducimos que $x {}_H\sim x$ y $x \sim_H x$, de forma respectiva.

- Propiedad simétrica. Sean $x, y \in G$:

- Si $x {}_H\sim y$, entonces $y^{-1}x \in H$, pero por ser H un grupo, también tendremos:

$$(y^{-1}x)^{-1} = x^{-1}y \in H$$

De donde deducimos que $y {}_H\sim x$.

- Si $x \sim_H y$, entonces $xy^{-1} \in H$, y por ser H un grupo:

$$(xy^{-1})^{-1} = yx^{-1} \in H$$

De donde deducimos que $y \sim_H x$.

- Propiedad transitiva. Sean $x, y, z \in G$:

- Si $x {}_H\sim y$ y $y {}_H\sim z$, entonces: $y^{-1}x, z^{-1}y \in H$ y por ser H un grupo, deducimos que:

$$(z^{-1}y)(y^{-1}x) = z^{-1}x \in H$$

De donde $x {}_H\sim z$.

- Si $x \sim_H y$ y $y \sim_H z$, entonces $xy^{-1}, yz^{-1} \in H$ y por ser H un grupo:

$$(xy^{-1})(yz^{-1}) = xz^{-1} \in H$$

De donde $x \sim_H z$.

⁹Que denotaremos por ${}_H[x]$ y por $[x]_H$ respectivamente.

Concluimos que $_H\sim$ y \sim_H son relaciones de equivalencia en G . Falta comprobar las igualdades:

$$_H[x] \stackrel{(1)}{=} \{xh \mid h \in H\}$$

$$[x]_H \stackrel{(2)}{=} \{hx \mid h \in H\}$$

1. Sean $x, y \in G$, tenemos que:

$$\begin{aligned} x \sim_H y &\iff y^{-1}x \in H \iff \exists h \in H \text{ con } y^{-1}x = h \iff \exists h \in H \text{ con } y^{-1} = hx^{-1} \\ &\iff \exists h \in H \text{ con } y = xh^{-1} \iff \exists h' \in H \text{ con } y = xh' \end{aligned}$$

Concluimos que se cumple (1).

2. Sean $x, y \in G$:

$$\begin{aligned} x \sim_H y &\iff xy^{-1} \in H \iff \exists h \in H \text{ con } xy^{-1} = h \iff \exists h \in H \text{ con } y = h^{-1}x \\ &\iff \exists h' \in H \text{ con } y = hx \end{aligned}$$

Concluimos que también se cumple (2).

□

Definición 2.10. Sea G un grupo y $H < G$:

- Si consideramos la relación $_H\sim$, dado $x \in G$, definimos la clase lateral por la izquierda de G en H definida por x a la clase de equivalencia de x por la relación de equivalencia $_H\sim$, que denotamos por:

$$xH = \{xh \mid h \in H\}$$

De esta forma, tendremos que el conjunto cociente dado por la relación es de la forma:

$$G/_H\sim = \{xH \mid x \in G\}$$

- Si consideramos ahora la relación \sim_H , dado $x \in G$, definimos la clase lateral por la derecha de G en H definida por x a la clase de equivalencia de x por la relación de equivalencia \sim_H , denotada por:

$$Hx = \{hx \mid h \in H\}$$

Y consideraremos el conjunto cociente:

$$G/\sim_H = \{Hx \mid x \in G\}$$

Ejemplo. En $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, si consideramos como H :

$$H = \langle (1\ 2) \rangle = \{1, (1\ 2)\}$$

Podemos calcular todas las clases laterales por la izquierda de G en H si consideramos la relación $_H\sim$:

$$\begin{aligned} 1H &= \{1 \cdot 1, 1(1\ 2)\} = \{1, (1\ 2)\} = H \\ (1\ 2)H &= \{(1\ 2)1, (1\ 2)(1\ 2)\} = \{(1\ 2), 1\} = H \\ (1\ 3)H &= \{(1\ 3)1, (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\} \\ (2\ 3)H &= \{(2\ 3)1, (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\} \\ (1\ 2\ 3)H &= \{(1\ 2\ 3)1, (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\} = (1\ 3)H \\ (1\ 3\ 2)H &= \{(1\ 3\ 2)1, (1\ 3\ 2)(1\ 2)\} = \{(1\ 3\ 2), (2\ 3)\} = (2\ 3)H \end{aligned}$$

Por lo que el conjunto cociente $G/_H\sim$ vendrá dado por:

$$G/_H\sim = \{H, (1\ 3)H, (2\ 3)H\}$$

Si ahora calculamos todas las clases laterales por la derecha de G en H , considerando la relación \sim_H , entonces:

$$\begin{aligned} H1 &= \{1 \cdot 1, (1\ 2)1\} = \{1, (1\ 2)\} = H \\ H(1\ 2) &= \{1(1\ 2), (1\ 2)(1\ 2)\} = \{(1\ 2), 1\} = H \\ H(1\ 3) &= \{1(1\ 3), (1\ 2)(1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\} \\ H(2\ 3) &= \{1(2\ 3), (1\ 2)(2\ 3)\} = \{(2\ 3), (1\ 2\ 3)\} \\ H(1\ 2\ 3) &= \{1(1\ 2\ 3), (1\ 2)(1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 3)\} = H(2\ 3) \\ H(1\ 3\ 2) &= \{1(1\ 3\ 2), (1\ 2)(1\ 3\ 2)\} = \{(1\ 3\ 2), (1\ 3)\} = H(1\ 3) \end{aligned}$$

Por lo que el conjunto cociente G/\sim_H vendrá dado por:

$$G/\sim_H = \{H, H(1\ 3), H(2\ 3)\}$$

Proposición 2.12. Sea G un grupo, $H < G$ y $x \in G$, entonces:

- i) $x \in xH$ y $x \in Hx$.
- ii) Los conjuntos H , xH y Hx son biyectivos.
- iii) Los conjuntos cocientes $G/_H\sim$ y G/\sim_H son biyectivos.

Demostración. Veamos cada una de ellas:

- i) Como H es un grupo, tendremos que $1 \in H$, por lo que:

$$x = x \cdot 1 \in xH \quad x = 1 \cdot x \in Hx$$

- ii) Sean $f : xH \longrightarrow H$, $g : H \longrightarrow Hx$ dadas por:

$$\begin{aligned} f(xh) &= h & \forall xh \in xH \\ g(h) &= hx & \forall h \in H \end{aligned}$$

Es fácil comprobar que f y g son biyectivas, por lo que xH es biyectivo con H y H es biyectivo con Hx . Basta considerar $g \circ f$ para obtener una biyección de xH con Hx .

iii) Sea $f : G/_H \sim \longrightarrow G/ \sim_H$ dada por:

$$f(xH) = Hx^{-1} \quad \forall xH \in G/_H \sim$$

En primer lugar, hemos de ver que f está bien definida. Para ello, sean $x, y \in G$ de forma que $xH = yH$, entonces $x_H \sim y$, luego $y^{-1}x \in H$, pero por ser H un grupo:

$$(y^{-1}x)^{-1} = x^{-1}y \in H \implies x^{-1} \sim_H y^{-1}$$

Por lo que $Hx^{-1} = Hy^{-1}$, luego f está bien definida. Finalmente, es fácil ver que f es biyectiva. \square

Definición 2.11 (Índice de un grupo en un subgrupo). Sea G un grupo y $H < G$, en la Proposición 2.12, vimos que:

$$|G/_H \sim| = |G/ \sim_H|$$

Los cardinales de estos conjuntos recibirán el nombre de índice de G en H , y los denotaremos por $[G : H]$.

Ejemplo. En los diagramas de Hasse de las Figuras 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9 y 2.10, los números que dibujábamos en las aristas de los diagramas de Hasse eran los índices de los grupos en los respectivos subgrupos marcados por la arista. Por ejemplo, en la Figura 2.9, observamos que $[S_3 : \langle (1\ 2) \rangle] = 3$.

Otro ejemplo puede ser el anterior, donde considerábamos en S_3 el conjunto:

$$H = \langle (1\ 2) \rangle = \{1, (1\ 2)\}$$

En esta situación, teníamos que $[S_3 : H] = |G/ \sim_H| = |G/_H \sim| = 3$.

Teorema 2.13 (de Lagrange). Sea G un grupo finito y $H < G$, entonces:

$$|G| = [G : H]|H|$$

Observemos que a partir de esta igualdad deducimos que $|H|$ divide a $|G|$.

Demostración. Como $_H \sim$ es una relación de equivalencia, tenemos una partición de G a partir de las clases de equivalencia dadas por esta relación:

$$G = \bigcup_{x \in G} xH$$

Como G es finito, habrá un número finito de clases de equivalencia, si elegimos un elemento en cada una de estas, tendremos un conjunto con cada uno de los representantes de las clases $\{x_1, x_2, \dots, x_n\}$, con lo que:

$$|G| = |x_1H| + |x_2H| + \dots + |x_nH| \stackrel{(*)}{=} n|H|$$

Donde en $(*)$ hemos usado la Proposición 2.12, ya que como xH es biyectivo con H para cualquier $x \in G$, concluimos que $|x_iH| = |x_1H|$ para todo $i \in \{1, \dots, n\}$. Sin embargo, n es el número de clases de equivalencia distintas del conjunto cociente, es decir, $n = [G : H]$, con lo que:

$$|G| = [G : H]|H|$$

\square

Observación. Notemos que a partir del Teorema de Lagrange podemos deducir resultados ya vistos y demostrados, como por ejemplo, la Proposición 1.22, donde deducíamos el orden de los grupos $|\mathrm{SL}_n(\mathbb{F})|$, pero resulta que $[\mathrm{GL}_n(\mathbb{F}) : \mathrm{SL}_n(\mathbb{F})] = q - 1$ si $|\mathbb{F}| = q$, por lo que:

$$|\mathrm{GL}_n(\mathbb{F})| = (q - 1)|\mathrm{SL}_n(\mathbb{F})|$$

Corolario 2.13.1. *Sea G un grupo finito, el orden de cualquier elemento de G divide a $|G|$.*

Demostración. Sea $x \in G$, basta ver que $O(x) = |\langle x \rangle|$. Sin embargo, por la Proposición 1.9, ya vimos que por ser G un grupo finito, entonces $\exists n \in \mathbb{N} \setminus \{0\}$ de forma que $O(x) = n$. En esta misma Proposición vimos que entonces x tenía n potencias distintas, por lo que:

$$\langle x \rangle = \{1, x, x^2, \dots, x^{n-1}\} \implies |\langle x \rangle| = n$$

Basta aplicar el Teorema de Lagrange, puesto que $\langle x \rangle < G$. □

Corolario 2.13.2. *Sea G un grupo finito y $K < H < G$, entonces:*

$$[G : K] = [G : H][H : K]$$

Demostración. Por el Teorema de Lagrange, sabemos que:

$$\left. \begin{aligned} |G| &= [G : K]|K| \\ |G| &= [G : H]|H| = [G : H][H : K]|K| \end{aligned} \right\} \implies [G : K] = [G : H][H : K]$$

□

2.4. Propiedades de grupos cíclicos

Terminaremos este capítulo repasando varias propiedades de los grupos cíclicos que debemos conocer, no sin antes recordar la definición de un grupo cíclico. Decimos que un grupo G es cíclico si $\exists a \in G$ de forma que $G = \langle a \rangle$. En cuyo caso, todos los elementos de G serán potencias de a : si $x \in G$, existirá $n \in \mathbb{N}$ de forma que $x = a^n$.

Antes de continuar, recordamos una propiedad de los grupos cíclicos: sea $G = \langle a \rangle$ un grupo cíclico, entonces:

$$|G| = O(a)$$

Proposición 2.14. *Si G es un grupo con $|G| = p$ primo, entonces G es cíclico.*

Demostración. Sea $a \in G$, $a \neq 1$ (como p es primo, $p \geq 2$), observamos que:

$$\{1\} \neq \langle a \rangle < G$$

Por el Teorema de Lagrange, $1 \neq |\langle a \rangle|$ divide a $|G|$, pero p es primo, por lo que $|\langle a \rangle| = p$ y ha de ser $\langle a \rangle = G$. □

Lema 2.15. Sea G un grupo, $a \in G$, existe un homomorfismo de grupos

$$\varphi_a : \mathbb{Z} \rightarrow G$$

De forma que $\varphi_a(1) = a$ y $\text{Im}(\varphi_a) = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$.

Demostración. Definimos φ_a como la aplicación:

$$\varphi_a(n) = a^n \quad \forall n \in \mathbb{Z}$$

Es claro que $\varphi_a(1) = a$ y que $\text{Im}(\varphi_a) = \{a^n \mid n \in \mathbb{Z}\} = \langle a \rangle$. Falta ver que φ_a es un homomorfismo. Para ello:

$$\varphi_a(n+m) = a^{n+m} = a^n a^m = \varphi_a(n) \varphi_a(m) \quad \forall n, m \in \mathbb{Z}$$

□

Teorema 2.16. Sea G un grupo cíclico, entonces:

- Si G es infinito, $G \cong \mathbb{Z}$.
- Si $|G| = n$, $G \cong \mathbb{Z}_n$.

Demostración. Como G es cíclico, existirá $a \in G$ de forma que $\langle a \rangle = G$. El Lema anterior nos da una aplicación $\varphi_a : \mathbb{Z} \rightarrow G$ sobreyectiva, veamos cómo conseguir la inyectividad:

- Si G es infinito, entonces ha de ser $O(a) = +\infty$, por lo que $\nexists n \in \mathbb{N} \setminus \{0\}$ de forma que $\varphi_a(n) = a^n = 1$, por lo que:

$$\ker(\varphi_a) = \{0\} \implies \varphi_a \text{ inyectiva}$$

Concluimos que $G \cong \mathbb{Z}$.

- Si G es finito y tiene cardinal $n \in \mathbb{N} \setminus \{0\}$, entonces tendremos que $O(a) = n$, por lo que $\varphi_a(n) = a^n = 1$ y φ_a no será inyectiva por ser $\{0, n\} \subseteq \ker(\varphi_a)$. Sin embargo, podemos definir la aplicación $\psi_a : \mathbb{Z}_n \rightarrow G$ dada por $\psi_a(\bar{r}) = a^r$ para todo $\bar{r} \in \mathbb{Z}_n$:

- ψ_a está bien definida, ya que si $\bar{r}, \bar{s} \in \mathbb{Z}_n$ de forma que $\bar{r} = \bar{s}$, entonces:

$$r - s \in n\mathbb{Z} \implies \exists t \in \mathbb{Z} \text{ con } a^{r-s} = a^{nt} = (a^n)^t = 1 \implies a^r = a^s$$

- ψ_a es un homomorfismo:

$$\psi_a(\bar{r} + \bar{s}) = a^{r+s} = a^r a^s = \psi_a(\bar{r}) \psi_a(\bar{s}) \quad \forall \bar{r}, \bar{s} \in \mathbb{Z}_n$$

- ψ_a es inyectiva, ya que si $\bar{r} \in \mathbb{Z}_n$ con $\psi_a(\bar{r}) = a^r = 1$, entonces $n \mid r$, luego $\bar{r} = \bar{0}$ y se tiene que:

$$\ker(\psi_a) = \{\bar{0}\}$$

- Como $\langle a \rangle = G$ y $|G| = n = O(a)$, está claro que ψ_a es sobreyectiva.

Por todo esto, concluimos que ψ_a es un isomorfismo, luego $G \cong \mathbb{Z}_n$.

□

Proposición 2.17. Sea $G = \langle a \rangle$ un grupo cíclico con $O(a) = n$, entonces para cada divisor m de n , existe un único subgrupo de G de orden m , el subgrupo cíclico $\langle a^{\frac{n}{m}} \rangle$. Además, estos son los únicos subgrupos de G .

Demostración. Sea m un divisor de n , veamos que $\langle a^{\frac{n}{m}} \rangle$ es un grupo cíclico de orden m . Para ello, veamos que $O(a^{\frac{n}{m}}) = m$:

- En primer lugar, tenemos que:

$$(a^{\frac{n}{m}})^m = a^n = 1$$

- Sea $t \in \mathbb{N} \setminus \{0\}$ de forma que:

$$(a^{\frac{n}{m}})^t = 1 \implies n \mid \frac{nt}{m}$$

En cuyo caso, existe $r \in \mathbb{N}$ de forma que:

$$\frac{nt}{m} = rn \implies t = rm \implies m \mid t$$

Concluimos que $O(a^{\frac{n}{m}}) = m$. Ahora, si $H < G$, nos gustaría probar que si $|H| = m$, entonces:

$$H = \langle a^{\frac{n}{m}} \rangle$$

En primer lugar, observemos que si $H < G$, por el Teorema de Lagrange tenemos que $m \mid n$. Para ver la igualdad, sea:

$$k = \min\{t \in \mathbb{N} \setminus \{0\} \mid a^t \in H\}$$

Veamos que $H = \langle a^k \rangle$:

⊇) Se tiene por la definición de k .

⊆) Sea $b \in H < G = \langle a \rangle$, entonces $\exists s \in \mathbb{N}$ de forma que $b = a^s$. Si dividimos s entre k , tenemos que $\exists q, r \in \mathbb{N}$ de forma que:

$$s = kq + r \quad 0 \leq r < k$$

Y por ser $a^s, a^k \in H$, vemos que:

$$a^r = a^s a^{-kq} \in H$$

Por esto, concluimos que $r = 0$, ya que k era el menor que cumplía esta propiedad, por lo que $s = kq$ y:

$$b = (a^k)^q \in \langle a^k \rangle$$

Falta ahora ver que $k = n/m$. Como H es un grupo, tenemos que $a^n = 1 \in H$, por lo que $k \mid n$ por la Proposición 1.8. De aquí deducimos que:

$$m = |H| = O(a^k) = \frac{n}{k} \implies k = \frac{n}{m}$$

□

Observación. De la Proposición anterior, deducimos que dado G un grupo cíclico con $|G| = n$, entonces la aplicación $\phi : Div(n) \rightarrow \Lambda_G$ con:

$$\Lambda_G = \{H \subseteq G \mid H < G\}$$

dada por:

$$\phi(m) = \langle a^{\frac{n}{m}} \rangle \quad \forall m \in Div(n)$$

Es una biyección.

Ejemplo. A partir de esta última observación, es muy fácil calcular todos los subgrupos de cualquier grupo cíclico, ya que el problema se reduce a estudiar todos los divisores del orden del grupo. Ilustramos el procedimiento con el grupo cíclico de orden 12:

$$C_{12} = \langle x \mid x^{12} = 1 \rangle$$

Tenemos que:

$$Div(12) = \{1, 2, 3, 4, 6, 12\}$$

Y usando nuestra aplicación ϕ , podemos listar todos los subgrupos de C_{12} :

$$\begin{aligned} 1 &\xrightarrow{\phi} \langle x^{\frac{12}{1}} \rangle = \langle x^{12} \rangle = \langle 1 \rangle = \{1\} \\ 2 &\xrightarrow{\phi} \langle x^{\frac{12}{2}} \rangle = \langle x^6 \rangle = \{1, x^6\} \\ 3 &\xrightarrow{\phi} \langle x^{\frac{12}{3}} \rangle = \langle x^4 \rangle = \{1, x^4, x^8\} \\ 4 &\xrightarrow{\phi} \langle x^{\frac{12}{4}} \rangle = \langle x^3 \rangle = \{1, x^3, x^6, x^9\} \\ 6 &\xrightarrow{\phi} \langle x^{\frac{12}{6}} \rangle = \langle x^2 \rangle = \{1, x^2, x^4, x^6, x^8, x^{10}\} \\ 12 &\xrightarrow{\phi} \langle x^{\frac{12}{12}} \rangle = \langle x \rangle = C_{12} \end{aligned}$$

Por lo que su diagrama de Hasse será de la forma:

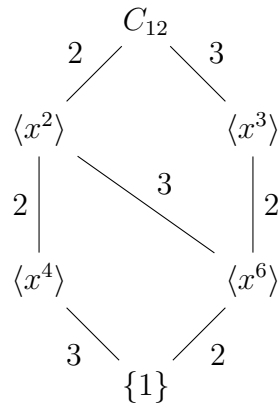


Figura 2.13: Diagrama de Hasse para los subgrupos de C_{12} .

Corolario 2.17.1. Si tenemos un grupo cíclico de orden p^n con p primo, entonces todos sus subgrupos serán cíclicos y de orden p^r , con $0 \leq r \leq n$.

Proposición 2.18. Sea G un grupo, $a \in G$ con $O(a) = n$ y $k \in \mathbb{N} \setminus \{0\}$, entonces:

$$\langle a^k \rangle = \langle a^d \rangle \quad \text{siendo } d = \text{mcd}(n, k)$$

En cuyo caso, $O(a^k) = \frac{n}{d}$.

Demostración. Por doble inclusión:

\subseteq) Como $d \mid k$, tenemos que $k = dt$ para cierto t , luego $a^k = a^{dt} \in \langle a^d \rangle$.

\supseteq) Como $d = \text{mcd}(n, k)$, entonces la ecuación:

$$nX + kY = d$$

tiene solución (se vió en Álgebra I), por lo que existen $u, v \in \mathbb{N}$ de forma que $nu + kv = d$, luego:

$$a^d = a^{nu} a^{kv} = (a^n)^u (a^k)^v \in \langle a^k \rangle$$

Para ver que $O(a^k) = \frac{n}{d}$, como $\langle a^k \rangle = \langle a^d \rangle$, tenemos que $O(a^k) = O(a^d)$ y como:

■ Tenemos que:

$$(a^d)^{\frac{n}{d}} = a^n = 1$$

■ Si $t \in \mathbb{N}$ de forma que:

$$(a^d)^t = 1 \implies n \mid dt \implies \frac{n}{d} \mid t$$

Concluimos que $O(a^k) = O(a^d) = \frac{n}{d}$. □

Ejemplo. Por ejemplo, ¿por qué en \mathbb{Z}_{12} la clase del 8 coincide con la del 4?, porque $4 = \text{mcd}(8, 12)$.

Corolario 2.18.1. Sea G un grupo y $a \in G$ con $O(a) = n$, entonces:

$$\langle a^p \rangle = \langle a^q \rangle \iff \text{mcd}(n, p) = \text{mcd}(n, q)$$

Corolario 2.18.2. Sea $G = \langle a \rangle$ un grupo cíclico con $O(a) = n$, entonces:

$$G = \langle a^k \rangle \iff \text{mcd}(k, n) = 1$$

Es decir, el número de generadores de G es $\varphi(n)$, siendo φ la función de Euler:

$$\varphi(n) = \{k \in \mathbb{N} \mid \text{mcd}(k, n) = 1\}$$

Ejemplo. En \mathbb{Z}_{12} :

$$\mathbb{Z}_{12} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$$

3. Relaciones de Ejercicios

3.1. Combinatoria y Teoría de Grafos

Ejercicio 3.1.1. Diez personas están sentadas alrededor de una mesa circular. Cada persona estrecha la mano a todos los demás excepto a la persona sentada directamente enfrente de la mesa. Dibuja un grafo que modele la situación.

La situación se puede modelar con el grafo de la Figura 3.1.
Su matriz de adyacencia es:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Ejercicio 3.1.2. Seis hermanos (Alonso, Bernardo, Carlos, Daniel, Enrique y Fernando) tienen que emparejarse para compartir habitación en el próximo curso escolar. Cada uno de ellos ha elaborado una lista con los nombres de aquellos con los que quiere emparejarse:

- Lista de Alonso: Daniel.
- Lista de Bernardo: Alonso, Enrique.
- Lista de Carlos: Daniel, Enrique.
- Lista de Daniel: Carlos.
- Lista de Enrique: Daniel, Bernardo, Fernando.
- Lista de Fernando: Alonso, Bernardo.

Dibuja el grafo dirigido que modela esta situación.

La situación se puede modelar con el grafo de la Figura 3.2, donde cada persona viene representada con un vértice con su inicial.

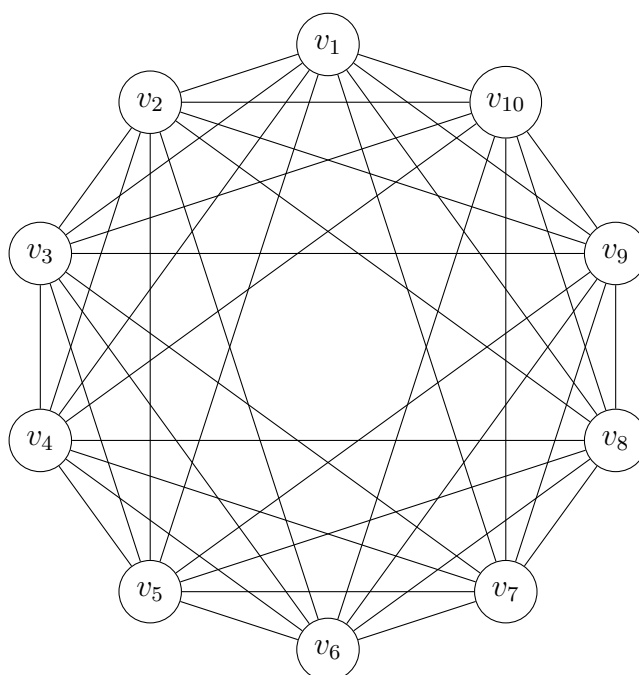


Figura 3.1: Situación del Ejercicio 3.1.1.

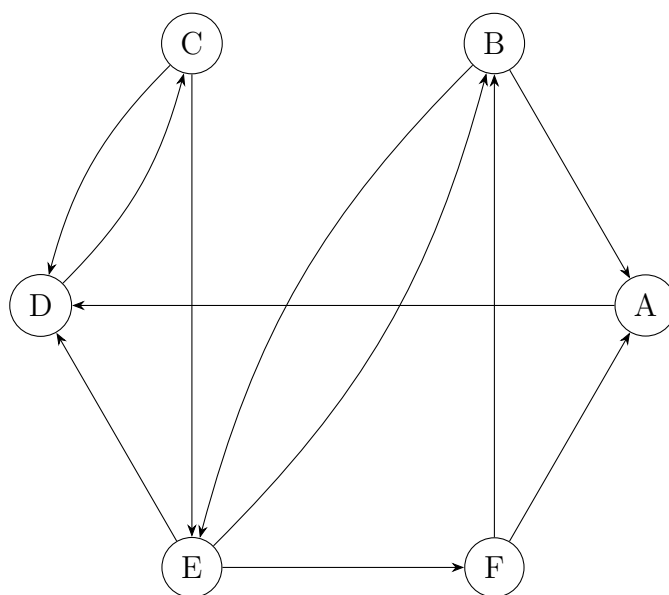


Figura 3.2: Situación del Ejercicio 3.1.2.

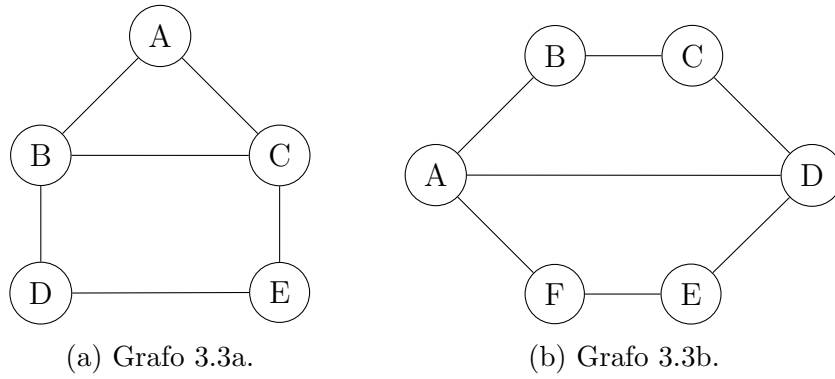


Figura 3.3: Grafos para el ejercicio 3.1.3.

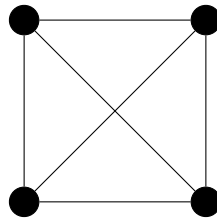


Figura 3.4: Grafo K_4 .

Ejercicio 3.1.3. Expresa en forma matricial los grafos de la Figura 3.3.

La matriz de adyacencia del grafo 3.3a es:

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

La matriz de adyacencia del grafo 3.3b es:

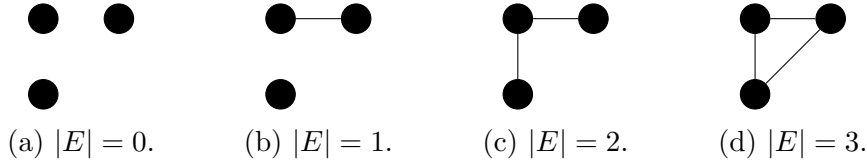
$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Ejercicio 3.1.4. Sea G un grafo completo con cuatro vértices. Construye todos sus subgrafos salvo isomorfismo.

El grafo completo con cuatro vértices es K_4 , representado en la Figura 3.4.

Para evitar pérdida de subgrafos, sabiendo que K_4 tiene 4 vértices, se pueden construir los siguientes subgrafos:

- No consideramos los subgrafos con 0 vértices.
- Tan solo hay un subgrafo con un vértice.

Figura 3.5: Subgrafos de K_4 con 2 vértices, $|V| = 2$.Figura 3.6: Subgrafos de K_4 con 3 vértices, $|V| = 3$.

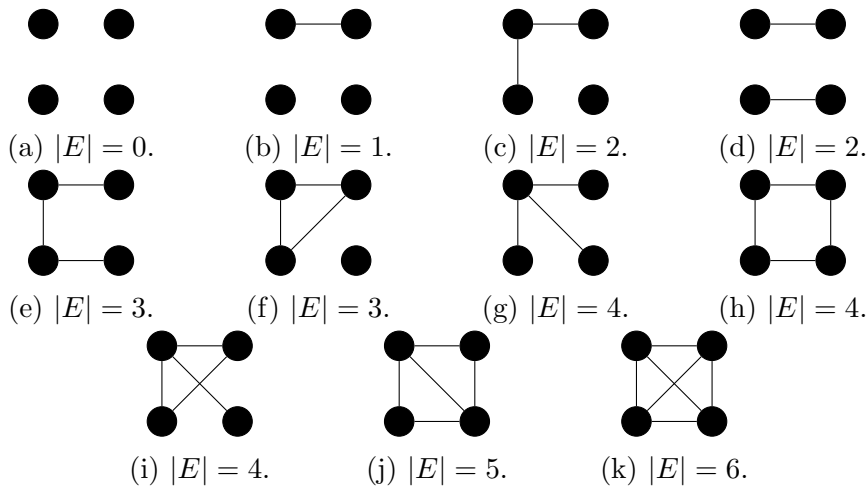
- Los subgrafos con dos vértices se encuentran en la Figura 3.5.
- Los subgrafos con tres vértices se encuentran en la Figura 3.6.
- Los subgrafos con cuatro vértices se encuentran en la Figura 3.7.

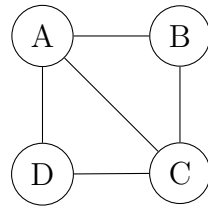
Ejercicio 3.1.5. ¿Son isomorfos los grafos de la Figura 3.8? ¿Y los de la Figura 3.9? ¿Y los de la Figura 3.10?

Veamos que los grafos de la Figura 3.8 son isomorfos. Sea $G(V, E)$ el grafo 3.8a y $G'(V', E')$ el grafo 3.8b. Las biyecciones $h_E : E \rightarrow E'$ y $h_V : V \rightarrow V'$ vienen dadas por:

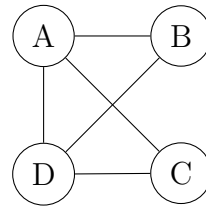
$$\begin{aligned}
 h_V : V &\rightarrow V' \\
 A &\mapsto A \\
 B &\mapsto B \\
 C &\mapsto D \\
 D &\mapsto C \\
 E &\mapsto E
 \end{aligned}$$

$$\begin{aligned}
 h_E : E &\rightarrow E' \\
 e = \{u, v\} &\mapsto e' = \{h_V(u), h_V(v)\}
 \end{aligned}$$

Figura 3.7: Subgrafos de K_4 con 4 vértices, $|V| = 4$.

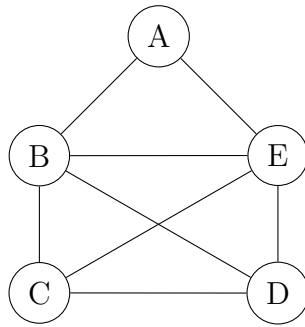


(a) Grafo 3.8a.

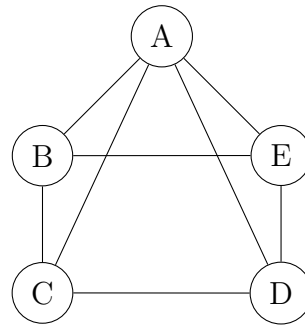


(b) Grafo 3.8b.

Figura 3.8: Primer par de grafos para el ejercicio 3.1.5.



(a) Grafo 3.9a.



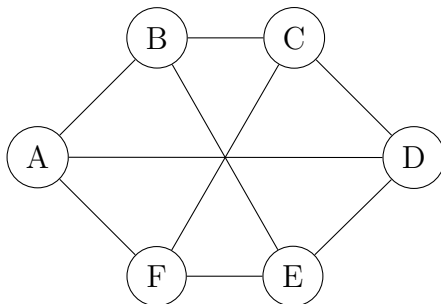
(b) Grafo 3.9b.

Figura 3.9: Segundo par de grafos para el ejercicio 3.1.5.

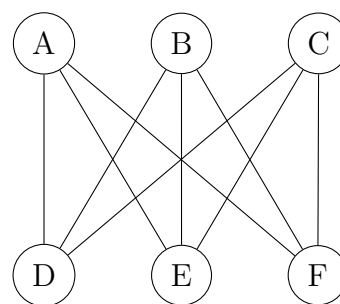
Respecto al par de grafos de la Figura 3.9, sabemos que no son isomorfos puesto que no tienen la misma sucesión de grafos; pues notando por $G(E, V)$ al grafo 3.9a y $G'(E', V')$ al grafo 3.9b, se tiene que:

$$D_4(G) = 0 \neq 1 = D_4(G')$$

Por último, veamos que los grafos de la Figura 3.10 son isomorfos. Sea $G(V, E)$ el grafo 3.10a y $G'(V', E')$ el grafo 3.10b. Las biyecciones $h_E : E \rightarrow E'$ y $h_V : V \rightarrow V'$



(a) Grafo 3.10a.



(b) Grafo 3.10b.

Figura 3.10: Tercer par de grafos para el ejercicio 3.1.5.

vienen dadas por:

$$\begin{aligned}
 h_V : V &\rightarrow V' \\
 A &\mapsto A \\
 B &\mapsto D \\
 C &\mapsto C \\
 D &\mapsto B \\
 E &\mapsto E \\
 F &\mapsto F \\
 \\
 h_E : E &\longrightarrow E' \\
 e = \{u, v\} &\longmapsto e' = \{h_V(u), h_V(v)\}
 \end{aligned}$$

Ejercicio 3.1.6. Demostrar que, en cualquier grafo, el número de vértices de grado impar es par. (Así, en un grupo de personas, el número total de personas que estrechan la mano de un número impar de otras personas es siempre par).

Sea el grafo $G(V, E)$ con V el conjunto de vértices y E el conjunto de aristas. Sea I el conjunto de vértices de grado impar:

$$I = \{v \in V \mid \deg(v) \text{ es impar}\}.$$

Usamos ahora el Lema de Apretón de Manos, descomponiendo V en dos conjuntos disjuntos, I y su complemento \bar{I} :

$$\sum_{v \in V} \deg(v) = \sum_{v \in I} \deg(v) + \sum_{v \notin I} \deg(v) = 2|E| \implies \sum_{v \in I} \deg(v) = 2|E| - \sum_{v \notin I} \deg(v).$$

Por tanto, como $2|E|$ es par, y la suma y resta de números pares es par, tenemos que:

$$\sum_{v \in I} \deg(v) \text{ es par}$$

Por la definición de I , sabemos que dicha sumatoria es una suma de números impares cuya suma es par. Por tanto, como la suma de dos números impares es par, y la suma de un número par y un número impar es impar, tenemos que la cantidad de elementos en I ha de ser par.

$$|I| \text{ es par}$$

Ejercicio 3.1.7. Demostrar que si cada vértice de un grafo G es de grado 2, cada componente conexa de G es un ciclo.

Fijada una componente conexa del grafo G , seleccionamos un vértice suyo fijo, sea este v_0 . Como $\deg v_0 = 2$, este tendrá dos vértices adyacentes, por lo que seleccionamos uno de ellos; sea este v_1 . Como $\deg v_1 = 2$, entonces también tendrá dos vecinos, pero uno de ellos ya lo hemos visitado (v_0), por lo que seleccionamos el otro vecino; sea este v_2 .

Repetiendo dicho algoritmo seleccionando vértices que no hayamos seleccionado, eventualmente llegaremos a v_0 (ya que en caso contrario V no sería finito). Por tanto, habríamos construido un ciclo. Además, como la elección está fijada y se trata de una componente conexa, habremos recorrido todos los vértices de la componente conexa luego, efectivamente, la componente conexa es un ciclo.

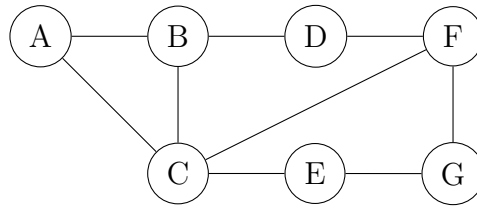


Figura 3.11: Grafo para el ejercicio 3.1.8.

Ejercicio 3.1.8. Los siguientes hechos se conocen de las personas A, B, C, D, E, F, G:

- A habla inglés.
- B habla inglés y español.
- C habla inglés, italiano y ruso.
- D habla japonés y español.
- E habla alemán e italiano.
- F habla francés, japonés y ruso.
- G habla francés y alemán.

Demostrar que cada par de personas entre estas siete puede comunicarse (con la ayuda de intérpretes, si es necesario, tomados de los cinco restantes).

Construiremos un grafo, en el que dos personas están conectadas por una arista si hablan el mismo idioma. Dicho grafo es el de la Figura 3.11. Como se trata de un grafo conexo, dada una persona p , podemos llegar a cualquier otra persona q mediante un camino simple (que representan los intérpretes). Por tanto, cada par de personas puede comunicarse.

Ejercicio 3.1.9. Demuestra que en todo grafo con más de un vértice existen dos vértices con el mismo grado.

Supongamos un grafo $G(V, E)$ con $|V| > 1$. Como hay $|V|$ vértices, el grado máximo posible es $|V| - 1$ (que representaría que dicho vértice está conectado con todos los demás). Por tanto, los posibles grados son:

$$0, 1, 2, \dots, |V| - 1.$$

No obstante, veamos que no todos son posibles; ya que si hay un vértice de grado 0, entonces no puede haber vértices de grado $|V| - 1$ (pues dichos vértices no podrían estar conectados con el vértice de grado 0). Por tanto, hay $|V|$ vértices y el número de grados posibles es menor que $|V|$; por lo que, por el principio del palomar, hay al menos dos vértices con el mismo grado.

Ejercicio 3.1.10. Prueba que si un grafo G contiene solo dos vértices de grado impar entonces ambos han de encontrarse en la misma componente conexa.

Por reducción al absurdo, supongamos que los dos vértices de grado impar se encuentran en componentes conexas distintas; y consideramos $G'(V', E')$ la componente conexa que contiene a uno de ellos (sin pérdida de generalidad, sea v_1) y $G''(V'', E'')$ la componente conexa que contiene al otro (sea v_2). Como componentes conexas que son, podemos considerarlos como subgrafos de G , por lo que G' (se podría trabajar análogamente con G'') cumple el Lema del Apretón de Manos:

$$\sum_{v \in V'} \deg(v) = 2|E'| \implies \left(\sum_{\substack{v \in V' \\ v \neq v_1}} \deg(v) \right) + \deg(v_1) = 2|E'|$$

No obstante, la sumatoria sabemos que es una suma de grados pares (pues todos los vértices de G' son de grado par, salvo v_1), por lo que es par; y la suma de un número par y un número impar es impar; por lo que no es posible que su suma valga $2|E'|$ (que es par). Por tanto, por reducción al absurdo, los dos vértices de grado impar han de encontrarse en la misma componente conexa.

Ejercicio 3.1.11. ¿Existe algún grafo regular de grado 5 con 25 vértices?

No, por el Ejercicio 3.1.6 (25 es impar).

Ejercicio 3.1.12. ¿Existe un grafo completo con 595 lados?

En un grafo completo, sabemos que:

$$|E| = \frac{|V|(|V| - 1)}{2}.$$

Suponiendo que fuese posible, como $|E| = 595$, tendríamos que:

$$595 = \frac{|V|(|V| - 1)}{2} \implies |V|^2 - |V| - 1190 = 0 \implies |V| = \frac{1 \pm \sqrt{1 + 4 \cdot 1190}}{2} = \frac{1 \pm 69}{2} \implies |V| = 35$$

Por tanto, sí es posible, y este es el grafo K_{35} .

Ejercicio 3.1.13. ¿Existe un grafo con 6 vértices cuyos grados sean 1, 2, 2, 3, 4 y 4 respectivamente?

Buscamos saber si dicha sucesión es gráfica. Para ello, aplicamos el Algoritmo de Havel-Hakimi:

| | | | | | | |
|---|---|---|---|---|---|--|
| 4 | 4 | 3 | 2 | 2 | 1 | Eliminamos el 4 y restamos uno a los 4 términos siguientes |
| | 3 | 2 | 1 | 1 | 1 | Eliminamos el 3 y restamos uno a los 3 términos siguientes |
| | | 1 | 0 | 0 | 1 | Reordenamos los términos |
| | | 1 | 1 | 0 | 0 | Eliminamos el 1 y restamos uno al término siguiente |
| | | | 0 | 0 | 0 | |



Figura 3.12: Grafo con sucesión de grados 0, 0, 0.



Figura 3.13: Grafo con sucesión de grados 1, 1, 0, 0.

Llegados a este punto, como la sucesión 0, 0, 0 es gráfica, entonces la sucesión 1, 2, 2, 3, 4, 4 también lo es. Reconstruimos para ello el grafo; partiendo de la sucesión 0, 0, 0, cuyo grafo es el de la Figura 3.12.

La siguiente sucesión es 1, 1, 0, 0, que resultó en la sucesión **0**, 0, 0; por lo que hemos de añadir un vértice de grado 1 que se conecte con uno de los vértices de grado 0; obteniendo el grafo de la Figura 3.13.

La siguiente sucesión es 3, 2, 1, 1, 1, que resultó en la sucesión **1**, **0**, **0**, 1; por lo que hemos de añadir un vértice de grado 3 que se conecte con un vértice de grado 1 y dos de grado 0; obteniendo el grafo de la Figura 3.14.

La siguiente sucesión es 4, 4, 3, 2, 2, 1, que resultó en la sucesión **3**, **2**, **1**, **1**, 1; por lo que hemos de añadir un vértice de grado 4 que se conecte con un vértice de grado 3, uno de grado 2 y dos de grado 1; obteniendo el grafo de la Figura 3.15.

Ejercicio 3.1.14. En cada uno de los siguientes casos, dibuja un grafo de Euler que verifique las condiciones, o prueba que tal grafo no existe:

1. Con un número par de vértices y un número par de lados.
Además de $K_{n,m}$ con m, n pares; el grafo de la Figura 3.16 cumple con las condiciones.
2. Con un número par de vértices y un número impar de lados.
El grafo de la Figura 3.17 cumple con las condiciones.
3. Con un número impar de vértices y un número par de lados.
Además de K_5 , el grafo de la Figura 3.18 cumple con las condiciones.
4. Con un número impar de vértices y un número impar de lados.
Además de K_3 , el grafo de la Figura 3.19 cumple con las condiciones.

Ejercicio 3.1.15. Encuentra un circuito de Euler para los grafos de la Figura 3.20.

Para el grafo de la Figura 3.20a, un circuito de Euler es:

$$A \rightarrow B \rightarrow D \rightarrow G \rightarrow H \rightarrow D \rightarrow E \rightarrow B \rightarrow C \rightarrow E \rightarrow H \rightarrow I \rightarrow E \rightarrow F \rightarrow I \rightarrow J \rightarrow F \rightarrow C \rightarrow A$$

Para el grafo de la Figura 3.20b, un circuito de Euler es:

$$B \rightarrow A \rightarrow C \rightarrow B \rightarrow E \rightarrow C \rightarrow D \rightarrow F \rightarrow E \rightarrow D \rightarrow B$$

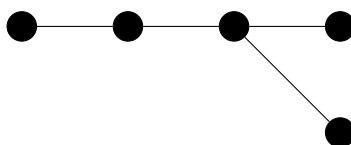


Figura 3.14: Grafo con sucesión de grados 3, 2, 1, 1, 1.

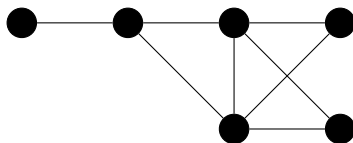


Figura 3.15: Grafo con sucesión de grados 4, 4, 3, 2, 2, 1.

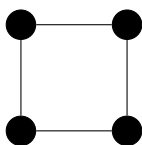


Figura 3.16: Grafo para el Ejercicio 3.1.14.1.

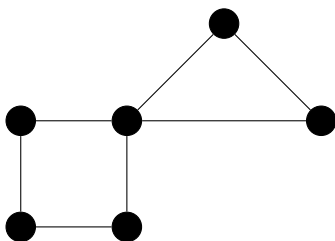


Figura 3.17: Grafo para el Ejercicio 3.1.14.2.

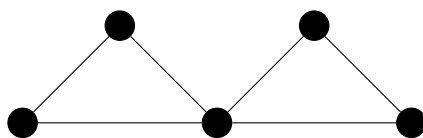


Figura 3.18: Grafo para el Ejercicio 3.1.14.3.

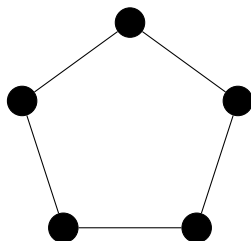


Figura 3.19: Grafo para el Ejercicio 3.1.14.4.

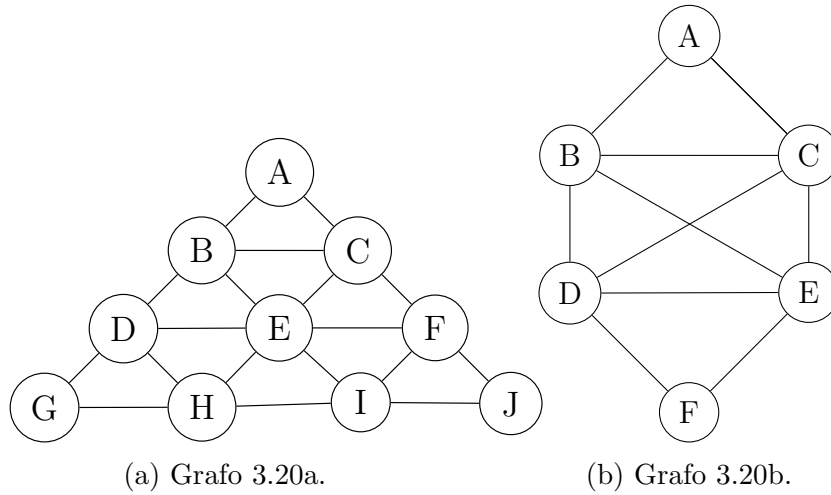


Figura 3.20: Grafos para el ejercicio 3.1.15.

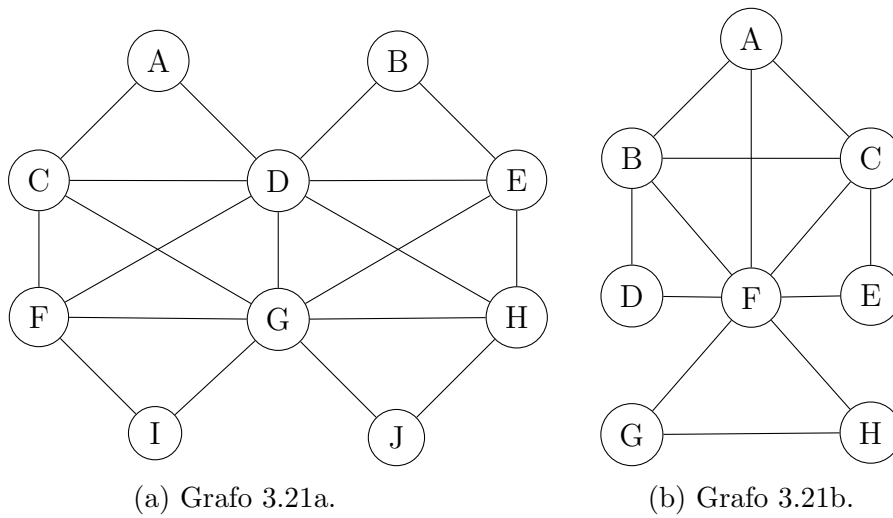


Figura 3.21: Grafos para el ejercicio 3.1.16.

Ejercicio 3.1.16. Encuentra un camino de Euler para los grafos de la Figura 3.21.

Para el grafo de la Figura 3.21a, un circuito de Euler es:

$$D \rightarrow C \rightarrow G \rightarrow D \rightarrow F \rightarrow I \rightarrow G \rightarrow F \rightarrow C \rightarrow A \rightarrow D \rightarrow E \rightarrow B \rightarrow D \rightarrow H \rightarrow E \rightarrow G \rightarrow J \rightarrow H \rightarrow G$$

Para el grafo de la Figura 3.21b, un circuito de Euler es:

$$A \rightarrow B \rightarrow C \rightarrow A \rightarrow F \rightarrow D \rightarrow B \rightarrow F \rightarrow C \rightarrow E \rightarrow F \rightarrow G \rightarrow H \rightarrow F$$

Ejercicio 3.1.17. Encontrar un circuito de Euler en el grafo de la Figura 3.22 y un camino de Euler en el grafo de la Figura 3.23.

Para el grafo de la Figura 3.22, un circuito de Euler es:

$$A \rightarrow G \rightarrow B \rightarrow C \rightarrow E \rightarrow F \rightarrow L \rightarrow K \rightarrow J \rightarrow L \rightarrow I \rightarrow H \rightarrow B \rightarrow I \rightarrow J \rightarrow E \rightarrow D \rightarrow C \rightarrow J \rightarrow B \rightarrow A$$

Para el grafo de la Figura 3.23, un camino de Euler es:

$$E \rightarrow B \rightarrow F \rightarrow E \rightarrow A \rightarrow B \rightarrow C \rightarrow D \rightarrow G \rightarrow C \rightarrow H \rightarrow G \rightarrow F \rightarrow A$$

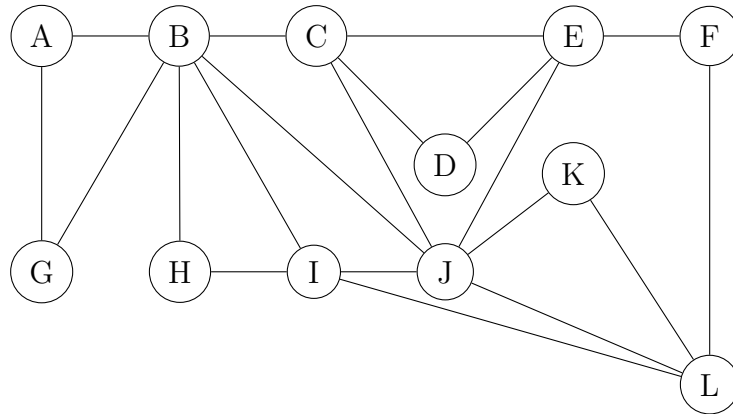


Figura 3.22: Primer grafo para el ejercicio 3.1.17.

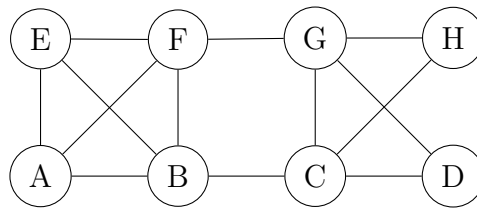


Figura 3.23: Segundo grafo para el ejercicio 3.1.17.

Ejercicio 3.1.18. ¿Para qué valores de n el grafo K_n es un circuito de Euler?

El grafo K_n sabemos que es conexo y, al ser completo, todos los vértices tienen grado $n - 1$. Además, para que un grafo conexo sea de Euler, todos sus vértices han de tener grado par. Por tanto, $n - 1$ ha de ser par, es decir, n ha de ser impar. Por tanto, el grafo K_n es un circuito de Euler si y solo si n es impar.

Ejercicio 3.1.19. Un viajante vive en la ciudad A y se supone que visita las ciudades B, C y D antes de volver a A. Encontrar la ruta más corta que consuma este viaje si las distancias entre las cuatro ciudades son, en Km:

- 120 entre A y B.
- 70 entre B y C.
- 140 entre A y C.
- 180 entre A y D.
- 100 entre B y D.
- 110 entre C y D.

Representamos el problema mediante el grafo de la Figura 3.24, que es K_4 con las distancias entre las ciudades. Para revolver el problema, podríamos usar algoritmos vistos en la Asignatura de Algorítmica, como el algoritmo de Kruskal. No se verá en esta asignatura, puesto que no se considerarán grafos ponderados.

Ejercicio 3.1.20. El grafo línea $L(G)$ de un un grafo G se define como sigue: Los vértices de $L(G)$ son los lados de G , $V(L(G)) = E(G)$; y dos vértices en $L(G)$

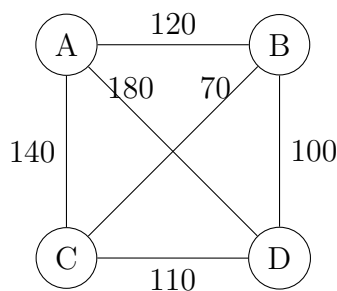


Figura 3.24: Grafo para el ejercicio 3.1.19.

son adyacentes si y solo si los lados correspondientes en G comparten un vértice. Demostrar:

1. Si G es un grafo conexo regular de grado r , entonces $L(G)$ es un grafo de Euler.

Por ser G un grafo conexo, tenemos que todos los vértices están conectados; y por tanto lo están también los lados de G . Es decir, dados dos lados cualesquiera de G , siempre podemos encontrar una sucesión de vértices adyacentes que los conecten; por lo que $L(G)$ es conexo.

Veamos ahora que el grado de cada vértice de $L(G)$ es par. Dado un vértice e de $L(G)$, este representa un lado de G que conecta dos vértices de G , sea $\gamma_G(e) = \{v_1, v_2\}$. Por cada lado de G incidente a v_1 o v_2 (excepto e), hay un vértice adyacente a e en $L(G)$; por lo que:

$$\deg_{L(G)}(e) = \deg_G(v_1) + \deg_G(v_2) - 2$$

donde se resta 2 por el lado e que comparten v_1 y v_2 . Por ser G regular de grado r , tenemos que:

$$\deg_{L(G)}(e) = r + r - 2 = 2r - 2 = 2(r - 1)$$

Por tanto, como e es un vértice arbitrario de $L(G)$, tenemos de hecho que $L(G)$ es regular de grado $2(r - 1)$, es decir, todos los vértices de $L(G)$ tienen grado par. Por tanto, $L(G)$ es un grafo de Euler.

2. Si G es un grafo de Euler entonces $L(G)$ es Hamiltoniano.

Supongamos que G es un grafo de Euler, por lo que podemos encontrar una sucesión de lados e_1, e_2, \dots, e_n que recorren todos los lados de G una vez sin repetir ninguno. Por la definición de $L(G)$, cada vértice de $L(G)$ representa un lado de G ; por lo que la sucesión de lados de G se convierte en una sucesión de vértices de $L(G)$ que recorre todos los vértices de $L(G)$ una vez sin repetir ninguno. Además, esto es posible porque dos lados adyacentes en G comparten un vértice, por lo que serán vértices adyacentes en $L(G)$. Por tanto, $L(G)$ es Hamiltoniano.

Ejercicio 3.1.21. De entre los grafos de la Figura 3.25 y la Figura 3.26, ¿cuáles contienen un circuito de Hamilton?

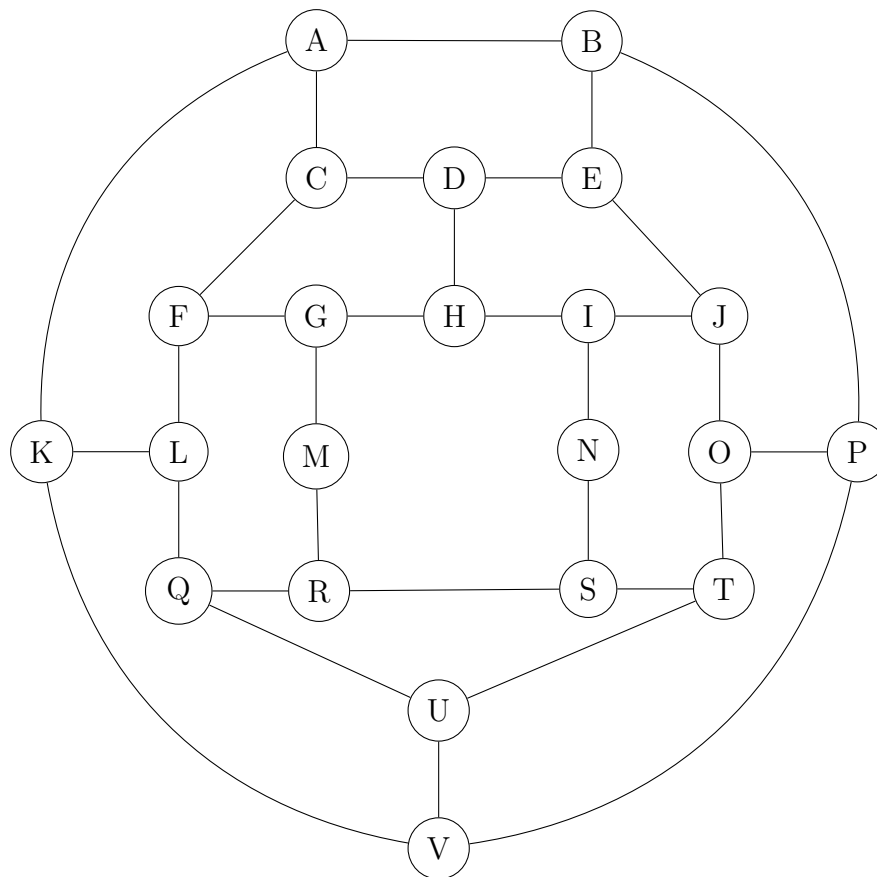


Figura 3.25: Primer grafo para el ejercicio 3.1.21.

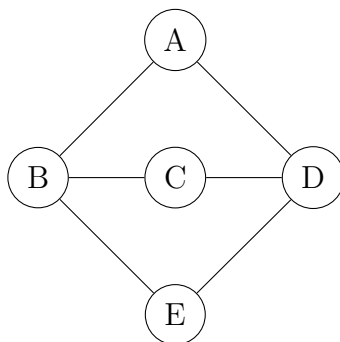


Figura 3.26: Segundo grafo para el ejercicio 3.1.21.

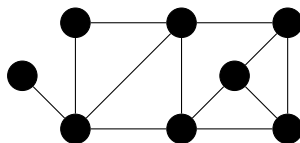


Figura 3.27: Grafo para el ejercicio 3.1.22.1.

Respecto al grafo de la Figura 3.25, se comprueba que no cumple ninguna de las condiciones suficientes para ser Hamiltoniano; aunque sí cumple todas las condiciones necesarias. Por tanto, hemos de buscar el circuito de Hamilton a ciegas. Este es:

$$A \rightarrow K \rightarrow V \rightarrow P \rightarrow H \rightarrow E \rightarrow J \rightarrow O \rightarrow T \rightarrow U \rightarrow Q \rightarrow L \rightarrow F \rightarrow G \rightarrow M \rightarrow R \rightarrow S \rightarrow N \rightarrow I \rightarrow H \rightarrow D \rightarrow C \rightarrow A$$

Respecto al grafo de la Figura 3.26, este no es Hamiltoniano.

Ejercicio 3.1.22.

1. Prueba, utilizando el algoritmo explicado en clase, que la sucesión $4 \geq 4 \geq 4 \geq 3 \geq 3 \geq 3 \geq 2 \geq 1$ es gráfica y, utilizando dicho algoritmo, encuentra un grafo que tenga como sucesión de grados la correspondiente.

Aplicamos el Algoritmo de Havel-Hakimi, y posteriormente construimos el grafo correspondiente, que se muestra en la Figura 3.27.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|--|
| 4 | 4 | 4 | 3 | 3 | 3 | 2 | 1 | Eliminamos el 4 y restamos uno a los 4 términos siguientes |
| | 3 | 3 | 2 | 2 | 3 | 2 | 1 | Reordenamos los términos |
| | 3 | 3 | 3 | 2 | 2 | 2 | 1 | Eliminamos el 3 y restamos uno a los 3 términos siguientes |
| | | 2 | 2 | 1 | 2 | 2 | 1 | Reordenamos los términos |
| | | 2 | 2 | 2 | 2 | 1 | 1 | Eliminamos el 2 y restamos uno a los 2 términos siguientes |
| | | | 1 | 1 | 2 | 1 | 1 | Reordenamos los términos |
| | | | 2 | 1 | 1 | 1 | 1 | Eliminamos el 2 y restamos uno a los 2 términos siguientes |
| | | | | 0 | 0 | 1 | 1 | |

2. El grafo con matriz de adyacencia M dada por:

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

es de Euler o en él hay un camino de Euler entre dos vértices. Razona cuál es la situación y encuentra, en su caso, el circuito o el camino de Euler que existe.

Sabemos que el grado del vértice v_i es la suma de los elementos de la fila i de la matriz de adyacencia. Calculando los grados de los vértices, obtenemos que todos son pares a excepción de los vértices v_1 y v_8 , por lo que hay un camino de Euler entre ellos. Este lo construimos con el algoritmo de Fleury, obteniendo el camino:

$$\begin{aligned} v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_6 \rightarrow v_7 \rightarrow v_8 \rightarrow v_5 \rightarrow v_2 \rightarrow v_7 \rightarrow v_1 \rightarrow v_6 \rightarrow \\ \rightarrow v_3 \rightarrow v_1 \rightarrow v_4 \rightarrow v_7 \rightarrow v_5 \rightarrow v_6 \rightarrow v_2 \rightarrow v_4 \rightarrow v_8 \end{aligned}$$

Ejercicio 3.1.23.

1. En el grafo G cuya matriz de adyacencia es

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

determina el número de aristas y la sucesión de grados de los vértices y, caso de que G sea de Euler, describe un circuito de Euler en él usando el algoritmo apropiado.

Tenemos que:

$$\begin{array}{llll} \deg v_1 = 4 & \deg v_2 = 2 & \deg v_3 = 4 & \deg v_4 = 4 \\ \deg v_5 = 2 & \deg v_6 = 4 & \deg v_7 = 2 & \deg v_8 = 4 \end{array}$$

Por tanto, usando el Lema del Apretón de Manos, tenemos que:

$$\sum_{v \in V} \deg v = 4 + 2 + 4 + 4 + 2 + 4 + 2 + 4 = 26 = 2|E| \implies |E| = 13$$

La sucesión de grados por tanto es:

$$0, 0, 3, 0, 5$$

Realizando un recorrido del grafo, vemos que el grafo es conexo; y como todos sus vértices tienen grado par, es de Euler. Por tanto, aplicamos el algoritmo de Fleury para encontrar un circuito de Euler, obteniendo el circuito:

$$v_1 \rightarrow v_2 \rightarrow v_8 \rightarrow v_6 \rightarrow v_1 \rightarrow v_4 \rightarrow v_3 \rightarrow v_6 \rightarrow v_4 \rightarrow v_8 \rightarrow v_7 \rightarrow v_3 \rightarrow v_5 \rightarrow v_1$$

2. Calcula el número de vértices de un grafo plano, conexo y regular de grado 5 con 20 caras.

Por ser plano y conexo, tenemos que:

$$|V| + 20 = |E| + 2$$

Por el Lema del Apretón de Manos, tenemos que:

$$\sum_{v \in V} \deg v = 2|E| \implies 5|V| = 2|E|$$

Resolvemos por tanto el siguiente sistema:

$$\begin{aligned} |V| + 20 &= |E| + 2 \\ 5|V| &= 2|E| \implies |E| = \frac{5}{2} \cdot |V| \end{aligned}$$

Por tanto, tenemos que:

$$|V| + 20 = \frac{5}{2} \cdot |V| + 2 \implies |V| = \frac{18 \cdot 2}{3} = 12$$

Ejercicio 3.1.24.

1. La siguiente matriz es la matriz de incidencia o adyacencia de un grafo. Razona qué caso es y dibuja el correspondiente grafo.

$$M = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

¿Es el grafo anterior de Euler o Hamilton? Razona la respuesta y da un circuito de Euler o Hamilton en caso de que los haya.

Como no se trata de una matriz cuadrada, no puede ser de adyacencia, por lo que se trata de una matriz de incidencia. El grafo correspondiente es el de la Figura 3.28.

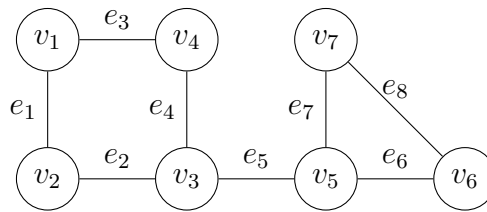


Figura 3.28: Grafo para el ejercicio 3.1.24.1.

Los grados de los vértices son la suma de las filas de la matriz de incidencia, obteniendo:

$$\begin{array}{llll} \deg v_1 = 2 & \deg v_2 = 2 & \deg v_3 = 3 & \deg v_4 = 2 \\ \deg v_5 = 3 & \deg v_6 = 2 & \deg v_7 = 2 & \end{array}$$

Por tanto, no se trata de un grafo de Euler (pues hay vértices de grado impar), pero sí tiene un camino de Euler entre los vértices v_3 y v_5 , que es:

$$v_3 \xrightarrow{e_4} v_4 \xrightarrow{e_3} v_1 \xrightarrow{e_1} v_2 \xrightarrow{e_2} v_3 \xrightarrow{e_5} v_5 \xrightarrow{e_6} v_6 \xrightarrow{e_8} v_7 \xrightarrow{e_7} v_5$$

Además, no es un grafo de Hamilton, pues contiene una arista puente. Esto implica que no se podrá construir un circuito (aunque no sabemos nada sobre camino) de Hamilton en él.

2. Aplica el algoritmo para comprobar si la siguiente sucesión

$$6 \geq 4 \geq 4 \geq 3 \geq 3 \geq 3 \geq 3 \geq 3$$

es, o no es, una sucesión gráfica y, en caso de serlo, también aplica el algoritmo para encontrar un grafo que la tenga como sucesión de grados.

No se trata de una sucesión gráfica, pues la suma de los grados es impar, lo que contradice el Lema del Apretón de Manos:

$$\sum_{v \in V} \deg v = 6 + 4 + 4 + 3 + 3 + 3 + 3 + 3 = 29$$

Ejercicio 3.1.25. Razona cuál es la respuesta correcta en cada una de las siguientes cuestiones (todos los grafos a los que se hace referencia son simples, no tienen lazos ni lados paralelos):

1. El grafo completo K_n :

- a) Es siempre de Euler.
- b) Es siempre de Hamilton.
- c) Dependiendo de n puede ser, o no, de Hamilton o de Euler.

Sabemos que K_n es conexo y que todos sus vértices tienen grado $n - 1$. Por tanto, en primer lugar vemos que:

$$K_n \text{ es de Euler} \iff n \text{ es impar}$$

Por otro lado, sabemos que, para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = n - 1 + n - 1 = 2n - 2 \geq n \iff n \geq 2$$

Por tanto, sabemos que K_n con $n \geq 2$ es de Hamilton. Además, como K_1 y K_2 son trivialmente de Hamilton, tenemos que:

$$K_n \text{ es de Hamilton} \quad \forall n \in \mathbb{N}$$

Por tanto, la respuesta correcta es la **b**).

2. He encontrado un grafo plano y conexo con 200 vértices y:

- a) Un número par de caras y un número impar de lados.
- b) Un número par de lados y un número impar de caras.
- c) Un número par de lados y caras.

Por ser plano y conexo, sabemos que:

$$200 + |C| = |E| + 2$$

Por tanto, o bien $|E|$ y $|C|$ son ambos pares, o ambos impares. Por tanto, la respuesta correcta es la **c**).

3. Tengo un grafo con un solo vértice de grado impar v :

- a) Puedo encontrar un camino que empiece en ese vértice v , recorra todos los lados del grafo solo una vez y vuelva a él.
- b) Si añado un lado que conecte ese vértice con otro cualquiera del grafo, pongamos w , puedo encontrar un camino que empiece en v , recorra todos los lados del grafo (incluido el que he añadido) solo una vez y termine en w .
- c) Es imposible tener un grafo como ese.

Por el Ejercicio 3.1.6, sabemos que el número de vértices de grado impar en un grafo es par. Por tanto, la respuesta correcta es la **c**).

4. En un grafo plano con cinco componentes conexas y 24 lados:

- a) El número de vértices y el número de caras son opuestos módulo 30.
- b) El número de vértices y el número de caras son congruentes módulo 30.
- c) Ninguna de las anteriores es cierta.

Por ser plano, tenemos que:

$$|V| + |C| = 24 + 1 + 5 = 30$$

Por tanto, la respuesta correcta es la **a**).

5. Dado un grafo regular de grado 1, entonces:

- a) El grafo no puede ser conexo.
- b) El grafo tiene tantas componentes conexas como vértices.
- c) El grafo tiene tantas componentes conexas como lados.

La respuesta correcta es la **c**).

6. Un grafo regular conexo de grado 11 con veinte vértices:

- a) Es siempre de Euler.
- b) Es siempre de Hamilton.
- c) Ninguna de las dos respuestas anteriores es cierta.

Como es regular de grafo 11 (impar), sabemos que no es de Euler. Por otro lado, sabemos que, para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 11 + 11 = 22 \geq 20$$

Por tanto, sabemos que es de Hamilton. Por tanto, la respuesta correcta es la **b**).

7. Elija la respuesta correcta:

- a) Sólo hay dos grafos con cuatro vértices y cuatro lados no isomorfos.
- b) Todos los grafos con cuatro vértices y cuatro lados son isomorfos.
- c) Sólo hay tres grafos con cuatro vértices y cuatro lados no isomorfos.

En el Ejercicio 3.1.4 vimos que la respuesta correcta es la **a**).

8. Un grafo cuya matriz de adyacencia es

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

- a) Es de Euler.
- b) No es de Euler pero hay un camino de Euler entre dos vértices.
- c) No es de Euler pero sus componentes conexas sí lo son.

No es de Euler, pues no es conexo. Sus componentes conexas, formadas por los vértices $\{v_1, v_2, v_3\}$ y $\{v_4, v_5, v_6, v_7\}$ respectivamente, sí son de Euler por ser conexas y tener todos los grados pares. Por tanto, la respuesta correcta es la **c**).

9. Un grafo cuya matriz de incidencia es

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- a) Es de Hamilton.
- b) No es de Hamilton pero sus componente conexas sí lo son.
- c) No es de Hamilton y tampoco lo son sus componentes conexas.

Este grafo es conexo (el vértice v_3 está conectado con todos los demás). Además, como $\deg v_5 = 1$, sabemos que no es de Hamilton. Por tanto, la respuesta correcta es la **c**).

10. La siguiente matriz

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

- a) Puede ser la matriz de adyacencia de un grafo pero no la de incidencia.
- b) Puede ser la matriz de incidencia de un grafo pero no la de adyacencia.
- c) No puede ser la matriz de adyacencia ni la de incidencia de un grafo.

Como $a_{13} = 0 \neq 1 = a_{31}$, la matriz no es simétrica y por tanto no puede ser la matriz de adyacencia de un grafo. Por otro lado, como la suma de la tercera columna es 3, si se tratase de la matriz de incidencia, tendríamos una arista que conecta tres vértices, lo que no es posible en un grafo simple. Por tanto, la respuesta correcta es la **c**).

Ejercicio 3.1.26.

1. Prueba, utilizando el algoritmo explicado en clase, que la sucesión dada por $3 \geq 3 \geq 2 \geq 2 \geq 2 \geq 2 \geq 2$ es gráfica y, utilizando dicho algoritmo, encuentra un grafo en que los grados de sus vértices sean los términos de esa sucesión. Prueba que el grafo es plano y que satisface el teorema de la característica de Euler.

Aplicamos el Algoritmo de Havel-Hakimi, y posteriormente construimos el grafo correspondiente, que se muestra en la Figura 3.29.

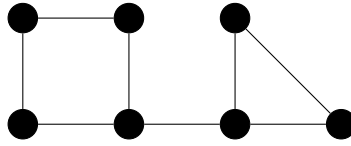


Figura 3.29: Grafo para el ejercicio 3.1.26.1.

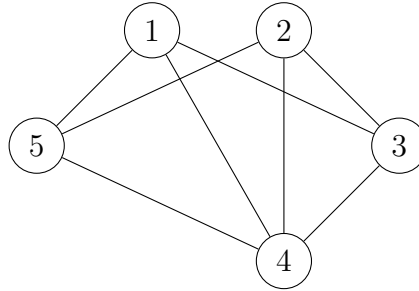


Figura 3.30: Grafo G_1 para el ejercicio 3.1.26.2.

| | | | | | | | |
|---|---|---|---|---|---|---|--|
| 3 | 3 | 2 | 2 | 2 | 2 | 2 | Eliminamos el 3 y restamos uno a los 3 términos siguientes |
| | 2 | 1 | 1 | 2 | 2 | 2 | Reordenamos los términos |
| | 2 | 2 | 2 | 2 | 1 | 1 | Eliminamos el 2 y restamos uno a los 2 términos siguientes |
| | | 1 | 1 | 2 | 1 | 1 | Reordenamos los términos |
| | | 2 | 1 | 1 | 1 | 1 | Eliminamos el 2 y restamos uno a los 2 términos siguientes |
| | | | 0 | 0 | 1 | 1 | |

2. Considera los grafos G_1 dado por el diagrama de la Figura 3.30 y G_2 con matriz de incidencia

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Estudia si son o no isomorfos, si son o no planos, si son o no de Euler o si hay un camino de Euler (en caso afirmativo aplica el algoritmo para calcular un circuito o un camino de Euler) y si son o no de Hamilton (encontrando el camino en caso afirmativo).

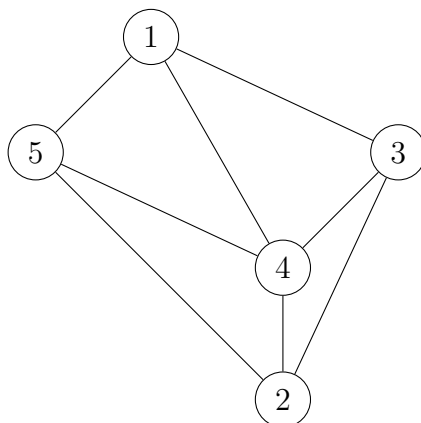
Estudiamos cada aspecto:

- No son isomorfos, puesto que G_1 no tiene vértices de grado 2 y G_2 sí (v_5).
- En ambos casos, tanto para G_1 como para G_2 , tenemos que:

$$|V| = 5 \quad |E| = 8$$

Además, tenemos que:

- Para K_5 : $|V| = 5$, $|E| = 10$.
- Para $K_{3,3}$: $|V| = 6$, $|E| = 9$.

Figura 3.31: Representación plana de G_1 (Figura 3.30).

Como $|E| = 8 < 9, 10$, y toda contracción de un grafo reduce el número de aristas, sabemos que ningún subgrafo de ninguno de los dos podrá contraerse a K_5 o a $K_{3,3}$. Por tanto, por el Teorema de Kuratowski, sabemos que ambos son planos. De hecho, en la Figura 3.31 se muestra la representación plana de G_1 (Figura 3.30).

- Ninguno de ellos es de Euler, puesto que tienen vértices de grado impar.
- G_1 no tiene ningún camino de Euler, puesto que hay más de dos vértices de grado impar. G_1 , no obstante, sí tiene un camino de Euler de v_1 a v_4 :

$$v_1 \xrightarrow{e_1} v_2 \xrightarrow{e_3} v_4 \xrightarrow{e_2} v_1 \xrightarrow{e_8} v_3 \xrightarrow{e_4} v_2 \xrightarrow{e_5} v_5 \xrightarrow{e_7} v_3 \xrightarrow{e_6} v_4$$

- Respecto al circuito de Hamilton, estudiamos en primer lugar G_1 . Sus grados son:

$$\deg v_1 = 3 \quad \deg v_2 = 3 \quad \deg v_3 = 3 \quad \deg v_4 = 4 \quad \deg v_5 = 3$$

Por tanto, dados dos vértices cualesquiera no adyacentes, se verifica que:

$$\deg v_i + \deg v_j \geq 6 \geq 5 \implies G_1 \text{ es de Hamilton}$$

Un posible recorrido de Hamilton para G_1 es:

$$1 \rightarrow 3 \rightarrow 2 \rightarrow 5 \rightarrow 4 \rightarrow 1$$

Por otro lado, estudiamos G_2 . Sus grados son:

$$\deg v_1 = 3 \quad \deg v_2 = 4 \quad \deg v_3 = 4 \quad \deg v_4 = 3 \quad \deg v_5 = 2$$

Por tanto, dados dos vértices cualesquiera no adyacentes, se verifica que:

$$\deg v_i + \deg v_j \geq 5 \geq 5 \implies G_2 \text{ es de Hamilton}$$

Un posible recorrido de Hamilton para G_2 es:

$$v_1 \xrightarrow{e_1} v_2 \xrightarrow{e_5} v_5 \xrightarrow{e_7} v_3 \xrightarrow{e_6} v_4 \xrightarrow{e_2} v_1$$



Figura 3.32: Grafos para el ejercicio 3.1.27.2.

Ejercicio 3.1.27.

1. Si G es un grafo completo con 6 vértices entonces:

- a) G es regular de grado 5.
- b) G tiene 20 aristas.
- c) G es de Euler y de Hamilton.

Sabemos que K_6 es regular de grado 5 y:

$$|E| = \frac{6 \cdot 5}{2} = 15$$

Además, aunque sí es de Hamilton, no es de Euler, por lo que la respuesta correcta es la **a**).

2. Sea G' un subgrafo completo (pleno) de un grafo G . Entonces:

- a) Si G es de Euler también G' es de Euler.
- b) Si G es de Hamilton también G' es de Hamilton.
- c) Ninguna de las anteriores.

Consideramos el contraejemplo de la Figura 3.32. El grafo G de la Figura 3.32a es de Euler y de Hamilton, pero su subgrafo completo G' de la Figura 3.32b no es ni de Euler ni de Hamilton. Por tanto, la respuesta correcta es la **c**).

3. Seleccione la respuesta correcta:

- a) Sólo hay dos grafos con cuatro vértices y 5 lados no isomorfos.
- b) Todos los grafos con cuatro vértices y 5 lados son isomorfos.
- c) Todos los grafos con cuatro vértices y cinco lados son de Euler.

En el Ejercicio 3.1.4 vimos que la respuesta correcta es la **b**).

4. Sea G un grafo plano conexo regular de grado 6 con 15 caras. Entonces:

- a) G tiene 13 vértices.
- b) El número de vértices es el triple del de aristas.
- c) No existe un tal grafo.

Por ser plano y conexo, sabemos que:

$$|V| + 15 = |E| + 2$$

Por ser regular de grado 6, sabemos que:

$$2|E| = 6|V| \implies |E| = 3|V|$$

Por tanto, sustituyendo en la primera ecuación, obtenemos:

$$|V| + 15 = 3|V| + 2 \implies |V| = \frac{13}{2}$$

Por tanto, la respuesta correcta es la **c**).

5. Salvo isomorfismos, grafos con 50 vértices y 1225 aristas:

- a) Solo hay 1.
- b) Hay 2.
- c) No existen grafos en esas condiciones.

Tan solo hay uno, y se trata de K_{50} , por lo que la respuesta correcta es la **a**).

Ejercicio 3.1.28.

1. Considera la sucesión 4, 4, 4, 4, 4.

- a) Utiliza el algoritmo dado en clase para probar que la sucesión es una sucesión gráfica y para dibujar un grafo G que la tenga como sucesión gráfica.

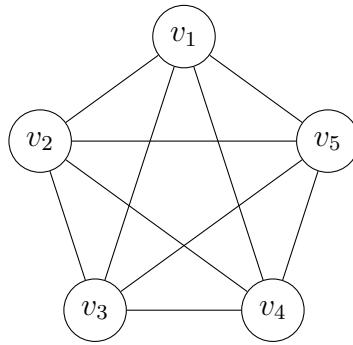
Aplicamos el Algoritmo de Havel-Hakimi, y posteriormente construimos el grafo correspondiente, que se muestra en la Figura 3.33 y se observa que $G = K_5$.

| | | | | | |
|---|---|---|---|---|--|
| 4 | 4 | 4 | 4 | 4 | Eliminamos el 4 y restamos uno a los 4 términos siguientes |
| 3 | 3 | 3 | 3 | | Eliminamos el 3 y restamos uno a los 3 términos siguientes |
| 2 | 2 | 2 | | | Eliminamos el 2 y restamos uno a los 2 términos siguientes |
| 1 | 1 | | | | Eliminamos el 1 y restamos uno al término siguiente |
| 0 | | | | | |

- b) Calcula las matrices incidencia y adyacencia del grafo G obtenido en el apartado anterior.

La matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Figura 3.33: Grafo G del ejercicio 3.1.28.1.

La matriz de incidencia es:

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

- c) ¿Es G de Euler o tiene un camino de Euler? En caso afirmativo, utiliza el algoritmo dado en clase para calcular el circuito o el camino de Euler. Sí es de Euler, puesto que todos los vértices son de grado par. Un posible circuito de Euler es:

$$v_1 \rightarrow v_3 \rightarrow v_5 \rightarrow v_2 \rightarrow v_4 \rightarrow v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_1$$

- d) ¿Es G de Hamilton? En caso afirmativo calcula el circuito de Hamilton. Sí, puesto que para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 4 + 4 = 8 \geq 5$$

Un posible circuito de Hamilton es:

$$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_1$$

- e) ¿Es G plano? En caso afirmativo comprueba la fórmula de la característica de Euler.

No, ya se ha demostrado que $G = K_5$ no es plano; ya que $|V| = 5$, $|E| = 10$ pero:

$$|E| \not\leq 3|V| - 6$$

2. Demuestra que si G es un grafo de Euler con n vértices que solo tiene 2 vértices de grado 2 entonces $|E| \geq 2n - 2$.

Sean $v_1, v_2 \in V$ los vértices de grado 2. Por ser de Euler, tenemos que $\deg v$ es par para todo $v \in V$. Por tanto, como v_1 y v_2 son los únicos vértices de grado 2, tenemos que:

$$\deg v \geq 4 \quad \forall v \in V \setminus \{v_1, v_2\}$$

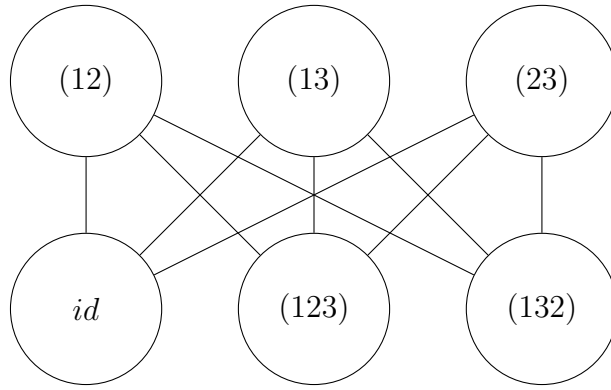


Figura 3.34: Grafo para el ejercicio 3.1.29.

Por tanto, tenemos que:

$$\begin{aligned}
 |E| &= \frac{1}{2} \sum_{v \in V} \deg v = \frac{1}{2} \left(2 + 2 + \sum_{v \in V \setminus \{v_1, v_2\}} \deg v \right) \\
 &\geq \frac{1}{2} (2 + 2 + 4(n - 2)) = 2n - 2
 \end{aligned}$$

Ejercicio 3.1.29.

1. Considera el subconjunto $X = \{(12), (13), (23)\} \subset S_3$ y el siguiente grafo G : Los vértices de G son los elementos de S_3 y hay un lado entre dos vértices x e y si $xy^{-1} \in X$.

a) Dibuja el grafo.

Calculemos en primer lugar los lados. Dados $x, y \in S_3$, tenemos que:

$$\varepsilon(xy^{-1}) = \varepsilon(x)\varepsilon(y^{-1}) = \varepsilon(x)\varepsilon(y)$$

Veamos ahora que hay un lado entre dos vértices $x, y \in S_3$ si y solo si $\varepsilon(x) \neq \varepsilon(y)$.

\Rightarrow) Supongamos que hay un lado entre $x, y \in S_3$; por lo que $xy^{-1} \in X$.

Por tanto:

$$\varepsilon(xy^{-1}) = \varepsilon(x)\varepsilon(y) \in \varepsilon(X) = \{-1\} \implies \varepsilon(x) \neq \varepsilon(y)$$

\Leftarrow) Supongamos que $\varepsilon(x) \neq \varepsilon(y)$. Por tanto, $\varepsilon(xy^{-1}) = \varepsilon(x)\varepsilon(y) = -1$. Como las únicas permutaciones de S_3 impares son las transposiciones, tenemos que $xy^{-1} \in X$.

Por tanto, el grafo es el de la Figura 3.34. Tenemos efectivamente que se trata de $K_{3,3}$, siendo las dos particiones de S_3 los conjuntos de permutaciones con signatura par e impar, respectivamente.

- b) Calcula sus matrices de incidencia y adyacencia.

Numeramos los vértices de G como sigue:

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

La matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

La matriz de incidencia es:

$$B = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

- c) ¿Es de Euler o tiene un camino de Euler? En caso afirmativo aplica el algoritmo dado en clase para calcular un ciclo o un camino de Euler.

No es de Euler ni hay un camino de Euler, puesto que hay más de dos vértices de grado impar.

- d) ¿Es de Hamilton? En caso afirmativo calcula el ciclo de Hamilton.

Sí es de Hamilton, puesto que para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 3 + 3 = 6 \geq 6 = |V|$$

Un posible ciclo de Hamilton es:

$$(id) \rightarrow (12) \rightarrow (123) \rightarrow (23) \rightarrow (132) \rightarrow (13) \rightarrow (id)$$

- e) ¿Es plano? En caso afirmativo comprueba la fórmula de Euler.

No es plano, puesto que es el mismo $K_{3,3}$.

2. Si G es un grafo con n vértices y m lados. Prueba que $m \leq \frac{n(n-1)}{2}$ y que se da la igualdad si y solo si $G = K_n$ es el grafo completo.

Por el Lema del Apretón de Manos, sabemos que:

$$\sum_{v \in V} \deg v = 2|E| \implies m = |E| = \frac{\sum_{v \in V} \deg v}{2}$$

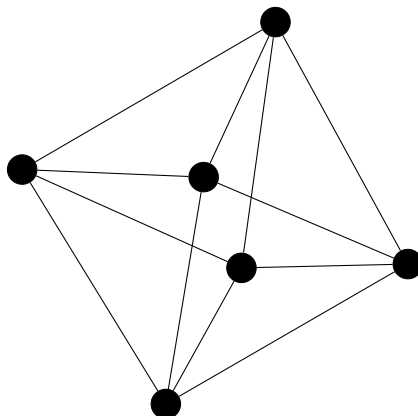


Figura 3.35: Octaedro para el ejercicio 3.1.30.

Por otro lado, sabemos que el grado máximo de un vértice en un grafo con n vértices es $n - 1$ (ya que en caso contrario sería necesario que hubiese lados paralelos o lazos, algo que no consideramos). Por tanto, tenemos que:

$$m \leq \frac{\sum_{v \in V} (n - 1)}{2} = \frac{\sum_{i=1}^n (n - 1)}{2} = \frac{n(n - 1)}{2}$$

Además, se da la igualdad si y solo si G es el grafo regular de n vértices y grado $n - 1$, es decir, K_n .

Ejercicio 3.1.30. Demuestra, utilizando el algoritmo explicado en clase, que la sucesión gráfica asociada a un octaedro (poliedro regular con 6 vértices, 8 caras y 12 aristas) es gráfica y, utilizando dicho algoritmo, encuentra un grafo G en que los grados de sus vértices sean los términos de esa sucesión. Encuentra las matrices de adyacencia e incidencia de G .

Comprueba que el grafo G es plano y estudia si es de Euler y, en caso afirmativo, determina por algún algoritmo explicado en clase un circuito de Euler para G . ¿Es G un grafo de Hamilton? Razona la respuesta.

En primer lugar, dibujamos el octaedro, que se muestra en la Figura 3.35, para poder así obtener la sucesión gráfica asociada, que es:

$$4, 4, 4, 4, 4, 4$$

Aplicamos el Algoritmo de Havel-Hakimi, y obtenemos el grafo de la Figura 3.36.

| | | | | | | |
|---|---|---|---|---|---|--|
| 4 | 4 | 4 | 4 | 4 | 4 | Eliminamos el 4 y restamos uno a los 4 términos siguientes |
| 3 | 3 | 3 | 3 | 4 | | Reordenamos los términos |
| 4 | 3 | 3 | 3 | 3 | | Eliminamos el 4 y restamos uno a los 4 términos siguientes |
| 2 | 2 | 2 | 2 | | | Eliminamos el 2 y restamos uno a los 2 términos siguientes |
| 1 | 1 | 2 | | | | Reordenamos los términos |
| 2 | 1 | 1 | | | | Eliminamos el 2 y restamos uno a los 2 términos siguientes |
| 0 | 0 | | | | | |

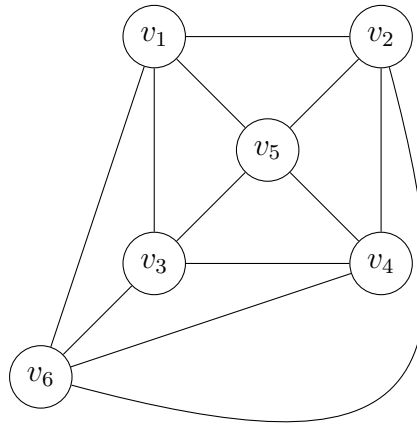


Figura 3.36: Grafo para el ejercicio 3.1.30.

La matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

La matriz de incidencia es:

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

El grafo es plano, puesto que se da una representación en la que no se cruzan aristas. Además, es de Euler, puesto que todos los vértices son de grado par. Un posible circuito de Euler es:

$$v_1 \rightarrow v_3 \rightarrow v_6 \rightarrow v_4 \rightarrow v_3 \rightarrow v_5 \rightarrow v_4 \rightarrow v_2 \rightarrow v_5 \rightarrow v_1 \rightarrow v_2 \rightarrow v_6 \rightarrow v_1$$

Además, el grafo también es de Hamilton, puesto que para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 4 + 4 = 8 \geq 6 = |V|$$

De hecho, un posible circuito de Hamilton es:

$$v_1 \rightarrow v_5 \rightarrow v_2 \rightarrow v_4 \rightarrow v_3 \rightarrow v_6 \rightarrow v_1$$

Ejercicio 3.1.31. Razona cuál es la respuesta correcta en cada una de las siguientes cuestiones (todos los grafos a los que se hace referencia son simples, no tienen lazos ni lados paralelos):

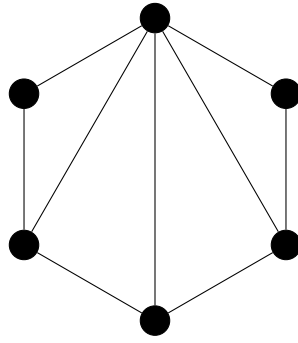


Figura 3.37: Grafo plano para el ejercicio 3.1.31.2.

1. La sucesión $70, 69, 68, \dots, 3, 2, 1$.

- a) Es una sucesión gráfica y su grafo asociado es el completo K_{70} .
- b) Es una sucesión gráfica pero su grafo asociado no es K_{70} .
- c) No es una sucesión gráfica.

Supongamos que es gráfica. Entonces, tenemos que:

$$\sum_{v \in V} \deg v = \sum_{i=1}^{70} i = \frac{70 \cdot 71}{2} = 35 \cdot 71 \text{ impar}$$

Por tanto, no puede ser gráfica, ya que la suma de los grados de los vértices debe ser par. Por tanto, la respuesta correcta es la **c**).

2. Tengo un grafo conexo con 6 vértices y 9 lados:

- a) Puedo asegurar que es plano.
- b) Puedo asegurar que no es plano.
- c) Puede ser plano o no serlo.

Tenemos que $|E| = 9 \leq 12 = 3|V| - 6$, por lo que puede ser plano. De hecho, el grafo de la Figura 3.37 es plano y $K_{3,3}$ no lo es, mientras que ambos son conexos con 6 vértices y 9 lados. Por tanto, la respuesta correcta es la **c**).

3. La sucesión $4, 4, 4, 4$:

- a) No es una sucesión gráfica pero si le añadimos al final un 2 sí lo es.
- b) No es una sucesión gráfica pero si le añadimos al final un 3 sí lo es.
- c) No es una sucesión gráfica pero si le añadimos al final un 4 sí lo es.

No es gráfica, puesto que si hay 4 vértices el mayor grado posible es 3. No obstante, si le añadimos un 4 al final, sí es gráfica, ya que es la sucesión correspondiente a K_5 . Por tanto, la respuesta correcta es la **c**).

4. Puedo encontrar un grafo plano conexo con:

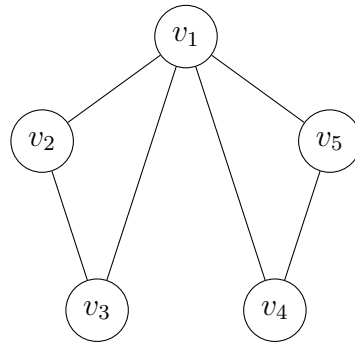


Figura 3.38: Grafo G del ejercicio 3.1.31.5.

- a) Un número impar de vértices, un número impar de lados y un número impar de caras.
- b) Un número par de vértices, un número par de lados y un número impar de caras.
- c) Un número impar de vértices, un número par de lados y un número impar de caras.

Sabemos que:

$$|V| + |F| = 2 + |E|$$

Por tanto, de entre las tres opciones, la única que puede cumplir la fórmula de Euler es la **c**).

5. La sucesión 4, 2, 2, 2, 2:

- a) Es la sucesión de grados de un grafo de Euler y de Hamilton.
- b) Es la sucesión de grados de un grafo de Hamilton y no de Euler.
- c) Es la sucesión de grados de un grafo de Euler y no de Hamilton.

El grafo de la Figura 3.38 tiene la sucesión de grados dada. Este es de Euler, con el circuito:

$$v_1 \rightarrow v_3 \rightarrow v_2 \rightarrow v_1 \rightarrow v_4 \rightarrow v_5 \rightarrow v_1$$

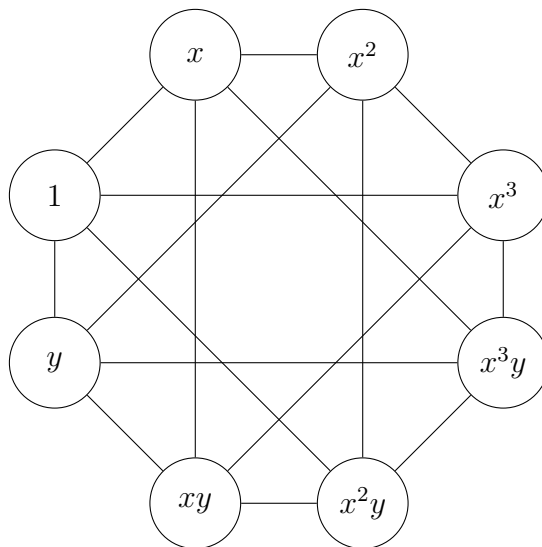
No obstante, no es de Hamilton. Por tanto, la respuesta correcta es la **c**).

6. Un grafo regular de grado 7:

- a) Tiene que tener al menos 8 vértices y un número impar de lados.
- b) Tiene que tener al menos 8 vértices pero puede tener un número impar o par de lados.
- c) Lo único que puedo afirmar sobre él es que tiene un número par de vértices.

Efectivamente, tiene que tener al menos 8 vértices. Respecto del número de lados, por el Lema del Apretón de Manos tenemos que:

$$2|E| = 7|V|$$

Figura 3.39: Grafo G del ejercicio 3.1.33.

Por tanto, podemos afirmar que ha de tener un número par de vértices. El grafo K_8 es regular de grado 7 y tiene 28 lados. El grafo regular de grado 7 con 10 vértices tiene 35 aristas, por lo que la respuesta correcta es la **b**).

Ejercicio 3.1.32. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle (123) \rangle$.

1. Construye el conjunto cociente S_4/H de clases laterales por la izquierda xH .
2. Para cada clase xH denotamos $m(xH)$ al máximo común divisor de los órdenes de los elementos en xH . Considera el grafo G con vértices las clases xH y en el que hay un lado entre xH e yH si $m(xH)$ divide a $m(yH)$ o $m(yH)$ divide a $m(xH)$. Identifica el grafo G dando la sucesión de grados de sus vértices y su matriz de adyacencia. ¿Es G de Euler, de Hamilton o plano?
3. Considera el subgrafo G' obtenido a partir de G eliminando la clase $1H$, ¿es G' de Euler? En caso afirmativo aplica el algoritmo dado en clase para calcular un circuito de Euler.

Ejercicio 3.1.33. Se considera el grupo $Q_2^{\text{abs}} = \langle x, y \mid x^4 = 1, x^2 = y^2, yx = x^{-1}y \rangle$ y el grafo G cuyos vértices son los elementos de Q_2^{abs} y en el que, para cualquier $a \in Q_2^{\text{abs}}$, hay un lado entre a y ax y también un lado entre a y ay .

1. Comprueba que G es un grafo regular dando la sucesión de grados de sus vértices y calcula su matriz de adyacencia.

Calculamos los elementos de Q_2^{abs} :

$$Q_2 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$$

El grafo es el de la Figura 3.39.

La matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Por tanto, su sucesión de grados es:

$$0, 0, 0, 0, 8, 0, 0, 0$$

Se trata por tanto de un grafo regular de grado 4 y 8 vértices. En particular, vemos que se trata de $K_{4,4}$, con la descomposición:

$$Q_2^{\text{abs}} = \{1, x^2, x^3y, xy\} \cup \{x, x^3, x^2y, y\}$$

2. Razona si G es un grafo de Hamilton o plano.

Para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 4 + 4 = 8 \geq 8 = |V|$$

Por tanto, G es de Hamilton, con un posible circuito:

$$1 \rightarrow x \rightarrow x^2 \rightarrow x^3 \rightarrow x^3y \rightarrow x^2y \rightarrow xy \rightarrow y \rightarrow 1$$

No obstante, no es plano, ya que $K_{4,4}$ puede contraerse a $K_{3,3}$.

3. Razona si G es un grafo de Euler y, en caso afirmativo, aplica el algoritmo dado en clase para calcular un circuito de Euler.

Sí es de Euler, puesto que todos los vértices son de grado par. Un posible circuito de Euler es:

$$1 \rightarrow x \rightarrow x^2 \rightarrow x^3 \rightarrow x^3y \rightarrow x^2y \rightarrow xy \rightarrow y \rightarrow 1 \rightarrow x^3 \rightarrow xy \rightarrow x \rightarrow \\ \rightarrow x^3y \rightarrow y \rightarrow x^2 \rightarrow x^2y \rightarrow 1$$

Ejercicio 3.1.34. Se considera el grupo $D_4 = \langle r, s \mid r^4 = 1, s^2 = 1, sr = r^{-1}s \rangle$ y el grafo G cuyos vértices son los elementos de D_4 y en el que, para cualquier $a \in D_4$, hay un lado entre a y ar y también un lado entre a y as .

1. Comprueba que G es un grafo regular dando la sucesión de grados de sus vértices y calcula su matriz de adyacencia.

Calculamos los elementos de D_4 :

$$D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$$

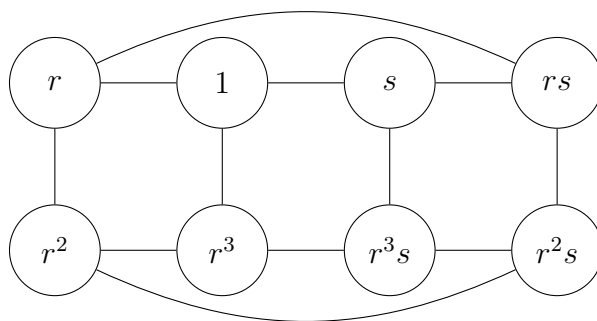


Figura 3.40: Grafo G del ejercicio 3.1.34.

El grafo es el de la Figura 3.40.

Su matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Por tanto, su sucesión de grados es:

$$0, 0, 0, 8, 0, 0, 0, 0$$

Se trata por tanto de un grafo regular de grado 3 y 8 vértices.

2. Razona si G es un grafo de Hamilton o plano.

Sí es de Hamilton, con un posible circuito:

$$1 \rightarrow r \rightarrow r^2 \rightarrow r^3 \rightarrow r^3s \rightarrow r^2s \rightarrow rs \rightarrow s \rightarrow 1$$

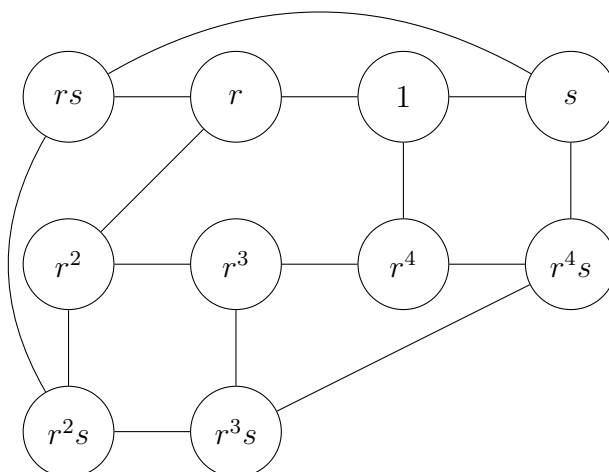
Además, en la Figura 3.40 se puede ver que G es plano.

3. Razona si G es un grafo de Euler y, en caso afirmativo, aplica el algoritmo dado en clase para calcular un circuito de Euler.

No es de Euler, puesto que hay más de dos vértices de grado impar.

Ejercicio 3.1.35. Se considera el grupo $D_5 = \langle r, s \mid r^5 = 1, s^2 = 1, sr = r^{-1}s \rangle$ y el grafo G cuyos vértices son los elementos de D_5 y en el que, para cualquier $a \in D_5$, hay un lado entre a y ar y también un lado entre a y as .

1. Calcula la sucesión de grados de G y razona si G es un grafo de Euler, de Hamilton o plano.

Figura 3.41: Grafo G del ejercicio 3.1.35.

Calculamos los elementos de D_5 :

$$D_5 = \{1, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$$

El grafo es el de la Figura 3.41.

Tenemos que la sucesión de grados es:

$$0, 0, 0, 10, 0, 0, 0, 0, 0, 0$$

Por tanto, se trata de un grafo regular de grado 3 y 10 vértices. Como hay más de dos vértices de grado impar, no es de Euler ni hay un camino de Euler. Además, en la Figura 3.41 se puede ver que G es plano. También es de Hamilton, con un posible circuito:

$$rs \rightarrow r^2s \rightarrow r^3s \rightarrow r^4s \rightarrow r^4 \rightarrow r^3 \rightarrow r^2 \rightarrow r \rightarrow 1 \rightarrow s \rightarrow rs$$

2. Considera un nuevo grafo G' obtenido añadiendo a G un nuevo vértice adyacente a todos los de G . Razona si G' es un grafo de Euler y, en caso afirmativo, aplica algún algoritmo dado en clase para calcular un circuito de Euler.

El grafo G' tampoco es de Euler, ya que hay más de dos vértices de grado impar.

Ejercicio 3.1.36. Razona cuál es la respuesta correcta en cada una de las siguientes cuestiones. Todos los grafos a los que se hace referencia son simples (es decir, no tienen lazos ni lados paralelos).

1. La matriz

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

es la de adyacencia de un grafo que:

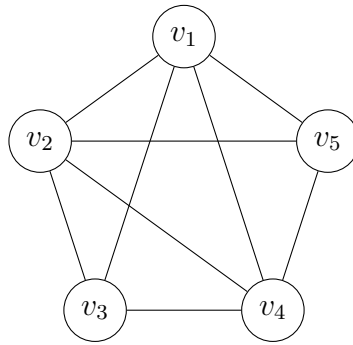


Figura 3.42: Grafo del ejercicio 3.1.36.1.

- a) Es de Euler.
- b) No es de Hamilton.
- c) Es plano.

El grafo en cuestión se encuentra en la Figura 3.42. Sabemos que no es de Euler por tener vértices de grado impar. No obstante, sí es de Hamilton, con el circuito:

$$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_1 \rightarrow v_3 \rightarrow v_5 \rightarrow v_4 \rightarrow v_2 \rightarrow v_1$$

Por último, veamos si es plano sabiendo que $|E| = 9$ y $|V| = 5$. Como $|V| = 5 < 6$, ningún subgrafo suyo se puede contraer a $K_{3,3}$; y como $|E| = 9 < 10$, no se puede contraer a K_5 ; y por tanto es plano. Por tanto, la respuesta correcta es la **c**).

2. Un grafo plano conexo regular de grado 8 con 23 caras:

- a) No existe.
- b) Tiene 12 aristas.
- c) Tiene 9 vértices.

Por ser un grafo plano conexo, sabemos que:

$$|V| + 23 = 2 + |E|$$

Por ser regular de grado 8, sabemos que:

$$2|E| = 8|V| \implies |E| = 4|V|$$

Por tanto, sustituyendo en la primera ecuación, obtenemos:

$$|V| + 23 = 2 + 4|V| \implies 3|V| = 21$$

Por tanto, $|V| = 7$; pero esto no es posible si es regular de grado 8. Por tanto, la respuesta correcta es la **a**).

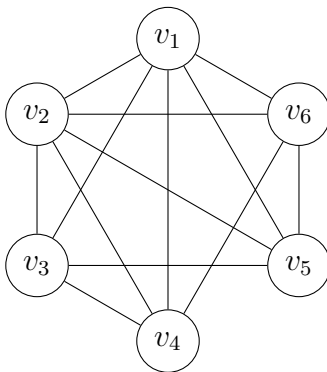


Figura 3.43: Grafo del ejercicio 3.1.36.4.

3. Se tiene que:

- a) Un grafo que es de Euler y de Hamilton siempre es plano.
- b) Un grafo que es plano y de Euler siempre es de Hamilton.
- c) Ninguna de las respuestas anteriores es cierta.

La opción a) es falsa, y como contraejemplo podemos emplear K_5 , que es de Euler y de Hamilton, pero no es plano. La opción b) es falsa, y como contraejemplo podemos emplear el grafo de la Figura 3.26, que es plano y de Euler, pero no es de Hamilton. Por tanto, la respuesta correcta es la **c**).

4. Se tiene que:

- a) La sucesión 5, 5, 4, 2, 2, 2 es la sucesión gráfica de un grafo plano.
- b) La sucesión 5, 5, 4, 4, 4, 4 es la sucesión gráfica de un grafo de Hamilton.
- c) La sucesión 5, 4, 4, 3, 3, 3 es la sucesión gráfica de un grafo de Euler.

En primer lugar, la sucesión de la opción a) no es gráfica, por lo que esta opción no es correcta. La sucesión de la opción c) tampoco es gráfica (puesto que el número de vértices de grado impar debe ser par), por lo que tampoco es correcta. Para comprobar que la sucesión de la opción b) es la asociada a un grafo de Hamilton, lo vemos representado en la Figura 3.43, y el circuito de Hamilton es:

$$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_6 \rightarrow v_5 \rightarrow v_1$$

Ejercicio 3.1.37. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle (123) \rangle$.

1. Construye el conjunto cociente S_4 / \sim_H de clases laterales por la derecha Hx , $x \in S_4$.
2. Para cada clase Hx denotamos $n(Hx)$ al mínimo común múltiplo de los órdenes de los elementos en Hx . Considera el grafo G con vértices las clases Hx y en el que hay un lado entre Hx e Hy si $n(Hx)$ divide a $n(Hy)$ o $n(Hy)$ divide a $n(Hx)$. Identifica el grafo G dando la sucesión de grados de sus vértices y su matriz de adyacencia. ¿Es G de Euler, de Hamilton o plano?

3. Considera, si es posible, un subgrafo G' de G obtenido al suprimir una arista entre dos vértices de G de grado impar. ¿Es G' de Euler? ¿Hay un camino de Euler entre dos vértices de G' ? En caso afirmativo aplica algún algoritmo dado en clase para calcular un circuito o camino de Euler en G' .

Ejercicio 3.1.38. Se considera el grupo A_4 y su subgrupo $H = \langle (12)(34) \rangle$. Se considera el grafo G con vértices las clases laterales por la izquierda de H en A_4 , xH , y en el que hay un lado entre xH e yH si $m(xH)$ divide a $m(yH)$ o $m(yH)$ divide a $m(xH)$, donde $m(Hx)$ denota el máximo común divisor de los órdenes de los elementos en xH . Razone cuál de las siguientes es la respuesta correcta:

1. G es plano pero no es de Hamilton.
2. G no es plano y tiene dos vértices conectados por un camino de Euler.
3. G es de Hamilton pero no es de Euler.

Ejercicio 3.1.39. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle (1234) \rangle$.

1. Construye el conjunto cociente S_4/H de clases laterales por la izquierda xH . ¿Es $H \triangleleft S_4$?
2. Para cada clase xH denotamos $m(xH)$ al máximo común divisor de los órdenes de los elementos en xH . Considera el grafo G con vértices las clases xH y en el que hay un lado entre dos clases xH e yH si $m(xH) = m(yH)$. Identifica el grafo G dando la sucesión de grados de sus vértices y su matriz de adyacencia. ¿Es G de Euler, de Hamilton o plano?
3. Considera el subgrafo G' obtenido a partir de G eliminando la clase $(13)H$. ¿Es G' de Euler? En caso afirmativo aplica algún algoritmo dado en clase para calcular un circuito o camino de Euler en G' .

Ejercicio 3.1.40. Razona cuál es la respuesta correcta en cada una de las siguientes cuestiones. Todos los grafos a los que se hace referencia son simples (es decir, no tienen lazos ni lados paralelos).

1. Se tiene que:

a) Hay un grafo conexo regular de grado 6 con 22 caras y 24 aristas.

Como menciona caras, suponemos que es plano. Por tanto, tenemos que:

$$|V| + 22 = 2 + 24 \implies |V| = 4$$

Comprobemos ahora que se cumple el Lema del Apretón de Manos:

$$\sum_{v \in V} \deg v = 6 \cdot |V| = 24 \neq 48 = 2 \cdot |E|$$

Por tanto, esta opción no es correcta.

- b) La sucesión 4, 4, 4, 3, 3 es la sucesión gráfica de un grafo plano que tiene un camino de Euler entre dos vértices.

Esta opción es correcta; ya que se trata de K_5 quitándole una arista. Como K_5 es de Euler, el camino buscado será el ciclo de Euler de K_5 sin cerrarlo.

- c) Un grafo conexo y plano es de Euler si y solo si es de Hamilton.

Esta opción es incorrecta, puesto que K_4 es conexo, plano y de Hamilton, pero no es de Euler.

2. La matriz

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

es la de adyacencia de un grafo:

- a) Con 11 aristas y que es de Euler y de Hamilton.
 b) Que es conexo y plano pero no de Hamilton.
 c) Que no es de Hamilton ni plano ni de Euler.

El grafo descrito es K_5 al que le hemos añadido un vértice adicional conectado mediante una única arista a uno de los vértices de K_5 . Como dicho vértice tiene grado 1, entonces el grafo no es de Euler ni de Hamilton. Además, como un subgrafo suyo es K_5 , en particular dicho subgrafo se puede contraer a K_5 , por lo que tampoco es plano. Por tanto, la opción correcta es la c).

Ejercicio 3.1.41. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle (134) \rangle$.

1. Construye el conjunto cociente S_4 / \sim_H de clases laterales por la derecha Hx , $x \in S_4$.
2. Para cada clase Hx denotamos $n(Hx)$ al mínimo común múltiplo de los órdenes de los elementos en Hx . Considera el grafo G con vértices las clases Hx y en el que hay un lado entre Hx y Hy si $n(Hx)$ divide a $n(Hy)$ o $n(Hy)$ divide a $n(Hx)$. Identifica el grafo G dando la sucesión de grados de sus vértices y su matriz de adyacencia.
3. ¿Hay alguna condición suficiente que asegure que G es de Hamilton? ¿Y necesaria para ser plano? ¿Es G de Euler, de Hamilton o plano?
4. Considera el subgrafo G' de G obtenido al suprimir la arista entre las clases $H(23)$ y $H(24)$. ¿Es G' de Hamilton, plano o de Euler? ¿Hay un camino de Euler entre dos vértices de G' ? En caso afirmativo aplica algún algoritmo dado en clase para calcular un circuito o camino de Euler en G' .

3.2. Grupos: generalidades y ejemplos

Ejercicio 3.2.1. Describir explícitamente la tabla de multiplicar de los grupos \mathbb{Z}_n^\times para $n = 4$, $n = 6$ y $n = 8$, donde por \mathbb{Z}_n^\times denotamos al grupo de las unidades del anillo \mathbb{Z}_n .

Sabemos que, fijado $n \in \mathbb{N}$, las unidades del anillo \mathbb{Z}_n son:

$$\mathcal{U}(\mathbb{Z}_n) = \mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid \text{mcd}(a, n) = 1\}$$

Describimos entonces a continuación las tablas de multiplicar de los grupos \mathbb{Z}_4^\times , \mathbb{Z}_6^\times y \mathbb{Z}_8^\times .

- Para $n = 4$:

| \cdot | 1 | 3 |
|---------|---|---|
| 1 | 1 | 3 |
| 3 | 3 | 1 |

- Para $n = 6$:

| \cdot | 1 | 5 |
|---------|---|---|
| 1 | 1 | 5 |
| 5 | 5 | 1 |

- Para $n = 8$:

| \cdot | 1 | 3 | 5 | 7 |
|---------|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

Ejercicio 3.2.2. Describir explícitamente la tabla de multiplicar de los grupos \mathbb{Z}_p^\times para $p = 2$, $p = 3$, $p = 5$ y $p = 7$.

- Para $p = 2$:

| \cdot | 1 |
|---------|---|
| 1 | 1 |

- Para $p = 3$:

| \cdot | 1 | 2 |
|---------|---|---|
| 1 | 1 | 2 |
| 2 | 2 | 1 |

- Para $p = 5$:

| \cdot | 1 | 2 | 3 | 4 |
|---------|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

- Para $p = 7$:

| \cdot | 1 | 2 | 3 | 4 | 5 | 6 |
|---------|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

Ejercicio 3.2.3. Calcular el inverso de 7 en los grupos \mathbb{Z}_{11}^\times y \mathbb{Z}_{37}^\times .

Para calcular el inverso de un elemento a en un grupo \mathbb{Z}_n^\times , basta con encontrar un elemento b tal que $ab = 1$ en \mathbb{Z}_n .

- Para \mathbb{Z}_{11}^\times :

$$7 \cdot 8 = 56 = 1 \implies 7^{-1} = 8$$

- Para \mathbb{Z}_{37}^\times :

$$7 \cdot 16 = 112 = 1 \implies 7^{-1} = 16$$

Ejercicio 3.2.4. Describir explícitamente los grupos μ_n (de raíces n -ésimas de la unidad) para $n = 3$, $n = 4$ y $n = 8$, dando su tabla de multiplicar.

- Para $n = 3$:

$$\begin{aligned} \mu_3 &= \left\{ 1, \xi_3, \xi_3^2 \mid \xi_3 = \cos\left(\frac{2\pi}{3}\right) + i \operatorname{sen}\left(\frac{2\pi}{3}\right) \right\} = \\ &= \left\{ 1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2} \right\} \end{aligned}$$

| \cdot | 1 | ξ_3 | ξ_3^2 |
|-----------|-----------|-----------|-----------|
| 1 | 1 | ξ_3 | ξ_3^2 |
| ξ_3 | ξ_3 | ξ_3^2 | 1 |
| ξ_3^2 | ξ_3^2 | 1 | ξ_3 |

- Para $n = 4$:

$$\begin{aligned} \mu_4 &= \left\{ 1, \xi_4, \xi_4^2, \xi_4^3 \mid \xi_4 = \cos\left(\frac{\pi}{2}\right) + i \operatorname{sen}\left(\frac{\pi}{2}\right) \right\} = \\ &= \{1, \xi_4, \xi_4^2, \xi_4^3 \mid \xi_4 = i\} = \{1, i, -1, -i\} \end{aligned}$$

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

■ Para $n = 8$:

$$\begin{aligned}\mu_8 &= \left\{ 1, \xi_8, \xi_8^2, \xi_8^3, \xi_8^4, \xi_8^5, \xi_8^6, \xi_8^7 \mid \xi_8 = \cos\left(\frac{\pi}{4}\right) + i \operatorname{sen}\left(\frac{\pi}{4}\right) \right\} = \\ &= \left\{ 1, \xi_8, \xi_8^2, \xi_8^3, \xi_8^4, \xi_8^5, \xi_8^6, \xi_8^7 \mid \xi_8 = \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} \right\} = \\ &= \left\{ 1, \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}, i, -\frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}, -1, -\frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}}, -i, \frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}} \right\}\end{aligned}$$

| \cdot | 1 | ξ_8 | ξ_8^2 | ξ_8^3 | ξ_8^4 | ξ_8^5 | ξ_8^6 | ξ_8^7 |
|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| 1 | 1 | ξ_8 | i | ξ_8^3 | -1 | ξ_8^5 | -i | ξ_8^7 |
| ξ_8 | ξ_8 | i | ξ_8^3 | -1 | ξ_8^5 | -i | ξ_8^7 | 1 |
| ξ_8^2 | i | ξ_8^3 | -1 | ξ_8^5 | -i | ξ_8^7 | 1 | ξ_8 |
| ξ_8^3 | ξ_8^3 | -1 | ξ_8^5 | -i | ξ_8^7 | 1 | ξ_8 | i |
| ξ_8^4 | -1 | ξ_8^5 | -i | ξ_8^7 | 1 | ξ_8 | i | ξ_8^3 |
| ξ_8^5 | ξ_8^5 | -i | ξ_8^7 | 1 | ξ_8 | i | ξ_8^3 | -1 |
| ξ_8^6 | -i | ξ_8^7 | 1 | ξ_8 | i | ξ_8^3 | -1 | ξ_8^5 |
| ξ_8^7 | ξ_8^7 | 1 | ξ_8 | i | ξ_8^3 | -1 | ξ_8^5 | -i |

Ejercicio 3.2.5. En el conjunto $\mathbb{Q}^\times := \{q \in \mathbb{Q} \mid q \neq 0\}$ de los números racionales no nulos, se considera la operación de división, dada por $(x, y) \mapsto x/y = xy^{-1}$. ¿Nos da esta operación una estructura de grupo en \mathbb{Q}^\times ?

Veamos qué condiciones han de cumplirse para que se tenga la propiedad asociativa. Sean $a, b, c \in \mathbb{Q}^\times$, entonces:

$$\frac{a/b}{c} = \frac{a}{b/c} \iff \frac{a}{bc} = \frac{ac}{b} \iff ab = abc^2 \iff 1 = c^2$$

Por tanto, tomando por ejemplo $2, 3, 4 \in \mathbb{Q}^\times$ no se tiene la propiedad asociativa, por lo que no se tiene un grupo.

Ejercicio 3.2.6. Sea G un grupo en el que $x^2 = 1$ para todo $x \in G$. Demostrar que el grupo G es abeliano.

Dados $x, y \in G$, se tiene que:

$$\begin{aligned}(xy)(xy) &= (xy)^2 = 1 \implies (xy)^{-1} = xy \\ xy &= (xy)^{-1} = y^{-1}x^{-1} = yx\end{aligned}$$

Por tanto, $xy = yx$ para todo $x, y \in G$, por lo que G es abeliano.

Ejercicio 3.2.7. Sea G un grupo. Demostrar que son equivalentes:

1. G es abeliano.
2. $\forall x, y \in G$ se verifica que $(xy)^2 = x^2y^2$.
3. $\forall x, y \in G$ se verifica que $(xy)^{-1} = x^{-1}y^{-1}$.

Demostración.

$1 \implies 2$) Dados $x, y \in G$, se tiene que:

$$(xy)^2 = xyxy \stackrel{(*)}{=} x^2y^2$$

donde en $(*)$ se ha usado que G es abeliano.

$2 \implies 1$) Dados $x, y \in G$, se tiene que:

$$\begin{aligned} (xy)^2 &= (xy)(xy) = xyxy \\ &\stackrel{(*)}{=} x^2y^2 \end{aligned}$$

donde en $(*)$ se ha usado la hipótesis. Por la propiedad cancelativa, se tiene que:

$$xyxy = x^2y^2 \implies xy = yx$$

Como se tiene para todo $x, y \in G$, entonces G es abeliano.

$1 \implies 3$) Dados $x, y \in G$, se tiene que:

$$(xy)^{-1} = y^{-1}x^{-1} \stackrel{(*)}{=} x^{-1}y^{-1}$$

donde en $(*)$ se ha usado que G es abeliano.

$3 \implies 1$) Dados $x, y \in G$, tenemos que:

$$(xy)^{-1} \stackrel{(*)}{=} x^{-1}y^{-1} = (yx)^{-1} \implies ((xy)^{-1})^{-1} = ((yx)^{-1})^{-1} \implies xy = yx$$

donde en $(*)$ se ha usado la hipótesis. Por tanto, como se tiene para todo $x, y \in G$, entonces G es abeliano.

□

Ejercicio 3.2.8. Demostrar que si en un grupo G , $x, y \in G$ verifican que $xy = yx$ entonces, para todo $n \in \mathbb{N} \setminus \{0\}$, se tiene que $(xy)^n = x^n y^n$.

Demostramos por inducción sobre n .

■ Caso base: $n = 1$.

$$(xy)^1 = xy = yx = x^1 y^1$$

■ Paso inductivo: Supuesto cierto para n , veamos que se cumple para $n + 1$.

$$\begin{aligned} (xy)^{n+1} &= (xy)^n(xy) = x^n y^n xy \\ &= x^n xy^n x = x^{n+1} y^{n+1} \end{aligned}$$

Por tanto, por inducción, se tiene que $(xy)^n = x^n y^n$ para todo $n \in \mathbb{N} \setminus \{0\}$.

Ejercicio 3.2.9. Demostrar que el conjunto de las aplicaciones $f : \mathbb{R} \rightarrow \mathbb{R}$, tales que $f(x) = ax + b$ para algún $a, b \in \mathbb{R}$, $a \neq 0$, es un grupo con la composición como ley de composición.

Definimos el conjunto siguiente:

$$G = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid \exists a, b \in \mathbb{R}, a \neq 0 \text{ tales que } f(x) = ax + b \forall x \in \mathbb{R}\}$$

En primer lugar, hemos de comprobar que G es cerrado bajo la composición de funciones, algo que tendremos gracias a ser \mathbb{R} cerrado para el producto y la suma. Dados $f, g \in G$, entonces existen $a, b, c, d \in \mathbb{R}$, $a, c \neq 0$ tales que:

$$f(x) = ax + b, \quad g(x) = cx + d$$

Entonces, se tiene que:

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) = a(cx + d) + b = acx + ad + b \in G \\ (g \circ f)(x) &= g(f(x)) = c(ax + b) + d = acx + cb + d \in G \end{aligned}$$

Por tanto, G es cerrado bajo la composición de funciones. Ahora, tomando $a = 1$ y $b = 0$, se tiene que $\text{Id}_{\mathbb{R}} \in G$. Veamos que $(G, \circ, \text{Id}_{\mathbb{R}})$ es un grupo.

- Asociatividad: Se tiene de forma directa por serlo la composición de funciones.
- Elemento neutro: Se tiene de forma directa.
- Elemento inverso: Dado $f \in G$, entonces existen $a, b \in \mathbb{R}$, $a \neq 0$ tales que $f(x) = ax + b$. Entonces, definimos su elemento inverso como:

$$f^{-1}(z) = a^{-1}(z - b) \in G$$

Comprobémoslo (notemos que tan solo hace falta comprobar que $f \circ f^{-1} = \text{Id}_{\mathbb{R}}$, puesto que en la definición no se impone $f^{-1} \circ f = \text{Id}_{\mathbb{R}}$):

$$(f \circ f^{-1})(z) = a(a^{-1}(z - b)) + b = z \quad \forall z \in \mathbb{R}$$

Por tanto, para todo $f \in G$, existe $f^{-1} \in G$ tal que $f \circ f^{-1} = \text{Id}_{\mathbb{R}}$.

Ejercicio 3.2.10.

1. Demostrar que $|\text{GL}_2(\mathbb{Z}_2)| = 6$, describiendo explícitamente todos los elementos que forman este grupo.

Sea $A \in \text{GL}_2(\mathbb{Z}_2)$:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies |A| = ad - bc \neq 0 \implies ad \neq bc$$

Por tanto, los elementos de $\text{GL}_2(\mathbb{Z}_2)$ son:

$$\begin{aligned} A_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & A_2 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, & A_3 &= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \\ A_4 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & A_5 &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, & A_6 &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

2. Sea $\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ y $\beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Demostrar que

$$\text{GL}_2(\mathbb{Z}_2) = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}.$$

Tenemos que:

$$1 = A_1, \quad \alpha = A_5, \quad \alpha^2 = A_6, \quad \beta = A_4, \quad \alpha\beta = A_3, \quad \alpha^2\beta = A_2$$

3. Escribir, utilizando la representación anterior, la tabla de multiplicar de $\text{GL}_2(\mathbb{Z}_2)$.

| \cdot | 1 | α | α^2 | β | $\alpha\beta$ | $\alpha^2\beta$ |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| 1 | 1 | α | α^2 | β | $\alpha\beta$ | $\alpha^2\beta$ |
| α | α | α^2 | 1 | $\alpha\beta$ | $\alpha^2\beta$ | β |
| α^2 | α^2 | 1 | α | $\alpha^2\beta$ | β | $\alpha\beta$ |
| β | β | $\alpha^2\beta$ | $\alpha\beta$ | 1 | α^2 | α |
| $\alpha\beta$ | $\alpha\beta$ | β | $\alpha^2\beta$ | α | 1 | α^2 |
| $\alpha^2\beta$ | $\alpha^2\beta$ | $\alpha\beta$ | β | α^2 | α | 1 |

Ejercicio 3.2.11. Dar las tablas de grupo para los grupos D_3 , D_4 , D_5 y D_6 .

Recordamos que:

$$D_n = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

■ Para D_3 :

| \cdot | 1 | r | r^2 | s | sr | sr^2 |
|---------|--------|--------|--------|--------|--------|--------|
| 1 | 1 | r | r^2 | s | sr | sr^2 |
| r | r | r^2 | 1 | sr^2 | s | sr |
| r^2 | r^2 | 1 | r | sr | sr^2 | s |
| s | s | sr | sr^2 | 1 | r | r^2 |
| sr | sr | sr^2 | s | r^2 | 1 | r |
| sr^2 | sr^2 | s | sr | r | r^2 | 1 |

■ Para D_4 :

| \cdot | 1 | r | r^2 | r^3 | s | sr | sr^2 | sr^3 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|
| 1 | 1 | r | r^2 | r^3 | s | sr | sr^2 | sr^3 |
| r | r | r^2 | r^3 | 1 | sr^3 | s | sr | sr^2 |
| r^2 | r^2 | r^3 | 1 | r | sr^2 | sr^3 | s | sr |
| r^3 | r^3 | 1 | r | r^2 | sr | sr^2 | sr^3 | s |
| s | s | sr | sr^2 | sr^3 | 1 | r | r^2 | r^3 |
| sr | sr | sr^2 | sr^3 | s | r^3 | 1 | r | r^2 |
| sr^2 | sr^2 | sr^3 | s | sr | r^2 | r^3 | 1 | r |
| sr^3 | sr^3 | s | sr | sr^2 | r | r^2 | r^3 | 1 |

■ Para D_5 :

| \cdot | 1 | r | r^2 | r^3 | r^4 | s | sr | sr^2 | sr^3 | sr^4 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 1 | 1 | r | r^2 | r^3 | r^4 | s | sr | sr^2 | sr^3 | sr^4 |
| r | r | r^2 | r^3 | r^4 | 1 | sr^4 | s | sr | sr^2 | sr^3 |
| r^2 | r^2 | r^3 | r^4 | 1 | r | sr^3 | sr^4 | s | sr | sr^2 |
| r^3 | r^3 | r^4 | 1 | r | r^2 | sr^2 | sr^3 | sr^4 | s | sr |
| r^4 | r^4 | 1 | r | r^2 | r^3 | sr | sr^2 | sr^3 | sr^4 | s |
| s | s | sr | sr^2 | sr^3 | sr^4 | 1 | r | r^2 | r^3 | r^4 |
| sr | sr | sr^2 | sr^3 | sr^4 | s | r^4 | 1 | r | r^2 | r^3 |
| sr^2 | sr^2 | sr^3 | sr^4 | s | sr | r^3 | r^4 | 1 | r | r^2 |
| sr^3 | sr^3 | sr^4 | s | sr | sr^2 | r^2 | r^3 | r^4 | 1 | r |
| sr^4 | sr^4 | s | sr | sr^2 | sr^3 | r | r^2 | r^3 | r^4 | 1 |

■ Para D_6 :

| \cdot | 1 | r | r^2 | r^3 | r^4 | r^5 | s | sr | sr^2 | sr^3 | sr^4 | sr^5 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 1 | 1 | r | r^2 | r^3 | r^4 | r^5 | s | sr | sr^2 | sr^3 | sr^4 | sr^5 |
| r | r | r^2 | r^3 | r^4 | r^5 | 1 | sr^5 | s | sr | sr^2 | sr^3 | sr^4 |
| r^2 | r^2 | r^3 | r^4 | r^5 | 1 | r | sr^4 | sr^5 | s | sr | sr^2 | sr^3 |
| r^3 | r^3 | r^4 | r^5 | 1 | r | r^2 | sr^3 | sr^4 | sr^5 | s | sr | sr^2 |
| r^4 | r^4 | r^5 | 1 | r | r^2 | r^3 | sr^2 | sr^3 | sr^4 | sr^5 | s | sr |
| r^5 | r^5 | 1 | r | r^2 | r^3 | r^4 | sr | sr^2 | sr^3 | sr^4 | sr^5 | s |
| s | s | sr | sr^2 | sr^3 | sr^4 | sr^5 | 1 | r | r^2 | r^3 | r^4 | r^5 |
| sr | sr | sr^2 | sr^3 | sr^4 | sr^5 | s | r^5 | 1 | r | r^2 | r^3 | r^4 |
| sr^2 | sr^2 | sr^3 | sr^4 | sr^5 | s | sr | r^4 | r^5 | 1 | r | r^2 | r^3 |
| sr^3 | sr^3 | sr^4 | sr^5 | s | sr | sr^2 | r^3 | r^4 | r^5 | 1 | r | r^2 |
| sr^4 | sr^4 | sr^5 | s | sr | sr^2 | sr^3 | r^2 | r^3 | r^4 | r^5 | 1 | r |
| sr^5 | sr^5 | s | sr | sr^2 | sr^3 | sr^4 | r | r^2 | r^3 | r^4 | r^5 | 1 |

Ejercicio 3.2.12. Demostrar que el conjunto de rotaciones respecto al origen del plano euclídeo junto con el conjunto de simetrías respecto a las rectas que pasan por el origen, es un grupo.

Denotamos por G al conjunto de rotaciones respecto al origen del plano euclídeo junto con el conjunto de simetrías respecto a las rectas que pasan por el origen. Notemos que no se trata de ningún grupo diédrico:

$$D_n \subsetneq G \quad \forall n \in \mathbb{N}$$

En primer lugar, sería necesario demostrar que es cerrado por la composición, algo que dejamos como ejercicio al lector por ser competencia de Geometría II.

Además, $\text{Id}_{\mathbb{R}^2} \in G$. Veamos que $(G, \circ, \text{Id}_{\mathbb{R}^2})$ es un grupo.

- Asociatividad: Se tiene de forma directa por serlo la composición de funciones.
- Elemento neutro: Se tiene de forma directa.
- Elemento inverso: Dado $f \in G$, veamos que existe $f^{-1} \in G$ tal que se tiene $f \circ f^{-1} = \text{Id}_{\mathbb{R}^2}$.

- Si f es una rotación de ángulo θ respecto al origen, entonces f^{-1} es la rotación de ángulo $-\theta$ respecto al origen.
- Si f es una simetría respecto a una recta que pasa por el origen, entonces f^{-1} es la misma simetría.

En ambos casos, se tiene que $f \circ f^{-1} = \text{Id}_{\mathbb{R}^2}$.

Por tanto, $(G, \circ, \text{Id}_{\mathbb{R}^2})$ es un grupo.

Ejercicio 3.2.13. Sea G un grupo y sean $a, b \in G$ tales que $ba = ab^k$, $a^n = 1 = b^m$ con $n, m > 0$.

1. Demostrar que para todo $i = 0, \dots, m-1$ se verifica $b^i a = ab^{ik}$.

Demostramos para todo $i \in \mathbb{N}$ por inducción sobre i .

- Caso base: $i = 0$.

$$b^0 a = a = ab^0$$

- Caso base: $i = 1$.

$$b^1 a = ba = ab^k = ab^{1 \cdot k}$$

- Paso inductivo: Supuesto cierto para i , veamos que se cumple para $i+1$.

$$b^{i+1} a = b b^i a = b a b^{ik} = a b^k b^{ik} = a b^{k(i+1)}$$

2. Demostrar que para todo $j = 0, \dots, n-1$ se verifica $ba^j = a^j b^{k^j}$.

Demostramos para todo $j \in \mathbb{N}$ por inducción sobre j .

- Caso base: $j = 0$.

$$ba^0 = b = a^0 b^{k^0}$$

- Caso base: $j = 1$.

$$ba = ab^k = a^1 b^{k^1}$$

- Paso inductivo: Supuesto cierto para j , veamos que se cumple para $j+1$.

$$ba^{j+1} = ba^j a = a^j b^{k^j} a \stackrel{(*)}{=} a^j a b^{k^j k} = a^{j+1} b^{k^{j+1}}$$

donde en $(*)$ se ha usado el apartado anterior.

3. Demostrar que para todo $i = 0, \dots, m-1$ y todo $j = 0, \dots, n-1$ se verifica $b^i a^j = a^j b^{ik^j}$.

Fijado $i \in \mathbb{N}$, demostramos por inducción sobre j .

- Caso base: $j = 0$.

$$b^i a^0 = b^i = a^0 b^{ik^0}$$

- Caso base: $j = 1$.

$$b^i a = ab^{ik} = a^1 b^{ik^1}$$

- Paso inductivo: Supuesto cierto para j , veamos que se cumple para $j+1$.

$$b^i a^{j+1} = b^i a^j a = a^j b^{ik^j} a \stackrel{(*)}{=} a^j a b^{ik^j k} = a^{j+1} b^{ik^{j+1}}$$

donde en $(*)$ se ha usado el apartado anterior.

Por tanto, se tiene para todo $i, j \in \mathbb{N}$.

4. Demostrar que todo elemento de $\langle a, b \rangle$ puede escribirse como $a^r b^s$ cumpliendo $0 \leq r < n$, $0 \leq s < m$.

Dado $x \in \langle a, b \rangle$, entonces x es producto de elementos de $\{a, b, a^{-1}, b^{-1}\}$. Como $a^n = 1 = b^m$, entonces $a^{-1} = a^{n-1}$ y $b^{-1} = b^{m-1}$. Por tanto, se tiene que x es producto de elementos de $\{a, b\}$. Usando el apartado anterior, podemos “llevar” los a ’s a la izquierda y los b ’s a la derecha, obteniendo lo siguiente:

$$x = a^{r'} b^{s'} \quad r', s' \in \mathbb{N} \cup \{0\}$$

Supuesto $r' \geq n$, sea $r = r' \text{ mód } n$ ($r' = nk + r$) y se tiene que:

$$a^{r'} = a^{nk+r} = (a^n)^k \cdot a^r = a^r$$

Además, se cumple que $0 \leq r < n$. Análogamente, supuesto $s' \geq m$, sea $s = s' \text{ mód } m$ ($s' = mk + s$) y se tiene que:

$$b^{s'} = b^{mk+s} = (b^m)^k \cdot b^s = b^s$$

Además, se cumple que $0 \leq s < m$. Por tanto:

$$x = a^{r'} b^{s'} = a^r b^s \quad 0 \leq r < n, \quad 0 \leq s < m$$

Observación. Notemos que D_n es un caso particular de este grupo, donde:

$$a = r, \quad b = s, \quad k = n - 1, \quad m = 2, \quad n = n$$

Ejercicio 3.2.14. Sean $s_1, s_2 \in S_7$ las permutaciones dadas por

$$s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 4 & 3 \end{pmatrix}, \quad s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 1 & 7 & 6 \end{pmatrix}.$$

Calcular los productos $s_1 s_2$, $s_2 s_1$ y s_2^2 , y su representación como producto de ciclos disjuntos.

En notación matricial, se tiene que:

$$\begin{aligned} s_1 s_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 2 & 3 & 5 & 4 \end{pmatrix} \\ s_2 s_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 1 & 5 & 3 & 4 \end{pmatrix} \\ s_2^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 7 & 5 & 2 & 6 \end{pmatrix} \end{aligned}$$

Descomponiendo en ciclos disjuntos, se tiene que:

$$\begin{aligned}s_2 &= (1\ 5)(2\ 7\ 3\ 6\ 4) \\ s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ s_1 s_2 &= (2\ 6\ 5\ 3\ 7\ 4) \\ s_2 s_1 &= (1\ 6\ 3\ 2\ 7\ 4) \\ s_2^2 &= (2\ 3\ 4\ 7\ 6)\end{aligned}$$

Ejercicio 3.2.15. Dadas las permutaciones

$$p_1 = (1\ 3\ 2\ 8\ 5\ 9)(2\ 6\ 3), \quad p_2 = (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5),$$

hallar la descomposición de la permutación producto $p_1 p_2$ como producto de ciclos disjuntos.

Usando la notación matricial, se tiene que:

$$p_1 p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 6 & 4 & 8 & 3 & 7 & 2 & 9 \end{pmatrix}$$

Descomponiendo en ciclos disjuntos, se tiene que:

$$p_1 p_2 = (2\ 5\ 8)(3\ 6)$$

Ejercicio 3.2.16. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas en los ejercicios anteriores.

Observación. Aquí tratamos a S_7 como un subgrupo de S_9 , donde consideramos cada permutación del conjunto $\{1, 2, 3, 4, 5, 6, 7\}$ como una permutación del conjunto $\{1, \dots, 9\}$ que deja fijos a los elementos 8 y 9.

1. Descomponer la permutación $s_1 s_2 s_1 s_2$ como producto de ciclos disjuntos.

$$\begin{aligned}s_1 s_2 s_1 s_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 6 & 7 & 3 & 2 & 8 & 9 \end{pmatrix} \\ &= (2\ 5\ 7)(3\ 4\ 6)\end{aligned}$$

2. Expresar matricialmente la permutación $p_3 = p_2 p_1 p_2$ y obtener su descomposición como ciclos disjuntos.

$$\begin{aligned}p_3 = p_2 p_1 p_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 1 & 4 & 6 & 2 & 7 & 8 & 5 \end{pmatrix} \\ &= (1\ 9\ 5\ 6\ 2\ 3)\end{aligned}$$

3. Descomponer la permutación $s_2 p_2$ como producto de ciclos disjuntos y expresarla matricialmente.

$$\begin{aligned}s_2 p_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 2 & 6 & 5 & 3 & 4 & 1 \end{pmatrix} \\ &= (1\ 9)(2\ 8\ 4)(3\ 7)(5\ 6)\end{aligned}$$

Ejercicio 3.2.17. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas en los ejercicios anteriores.

1. Calcular el orden de la permutación producto $s_1 s_2$. ¿Coincide dicho orden con el producto de los órdenes de s_1 y s_2 ?

$$\begin{aligned}s_1 s_2 &= (2\ 6\ 5\ 3\ 7\ 4) \\ s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ s_2 &= (1\ 5)(2\ 7\ 3\ 6\ 4)\end{aligned}$$

Por el Corolario 1.13.1, se tiene que:

$$\begin{aligned}O(s_1 s_2) &= 6 \\ O(s_1) &= \text{mcm}(4, 2) = 4 \\ O(s_2) &= \text{mcm}(2, 5) = 10\end{aligned}$$

Por tanto, $O(s_1 s_2) \neq O(s_1)O(s_2)$.

2. Calcular el orden de $s_1(s_2)^{-1}(s_1)^{-1}$.

$$\begin{aligned}s_1(s_2)^{-1}(s_1)^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 2 & 4 \end{pmatrix} = \\ &= (1\ 3)(2\ 5\ 7\ 4\ 6)O(s_1(s_2)^{-1}(s_1)^{-1}) = \text{mcm}(2, 5) = 10\end{aligned}$$

3. Calcular la permutación $(s_1)^{-1}$, y expresarla como producto de ciclos disjuntos.

$$\begin{aligned}s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ (s_1)^{-1} &= (5\ 4\ 3\ 1)(7\ 6)\end{aligned}$$

4. Calcular la permutación $(p_1)^{-1}$ y expresarla matricialmente.

$$\begin{aligned}p_1^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 1 & 4 & 8 & 2 & 7 & 3 & 5 \end{pmatrix} = \\ &= (1\ 9\ 5\ 8\ 3)(2\ 6)\end{aligned}$$

5. Calcular la permutación $p_2(s_2)^2(p_1)^{-1}$. ¿Cuál es su orden?

$$\begin{aligned}p_2 &= (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5) \\ (s_2)^2 &= (2\ 3\ 4\ 7\ 6) \\ (p_1)^{-1} &= (1\ 9\ 5\ 8\ 3)(2\ 6) \\ p_2(s_2)^2(p_1)^{-1} &= (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5)(2\ 3\ 4\ 7\ 6)(1\ 9\ 5\ 8\ 3)(2\ 6) \\ &= (1\ 5\ 6\ 2\ 8\ 4\ 7)(3\ 9) \\ O(p_2(s_2)^2(p_1)^{-1}) &= \text{mcm}(7, 2) = 14\end{aligned}$$

Ejercicio 3.2.18. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas anteriormente. Sean también $s_3 = (2\ 4\ 6)$ y $s_4 = (1\ 2\ 7)(2\ 4\ 6\ 1)(5\ 3)$. ¿Cuál es la paridad de las permutaciones $s_1, s_4p_1p_2$ y p_2s_3 ?

$$\begin{aligned}s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ s_4p_1p_2 &= (1\ 7)(2\ 3)(4\ 6\ 5\ 8) \\ p_2s_3 &= (1\ 9\ 5\ 3\ 2\ 4)(6\ 8)\end{aligned}$$

Por tanto:

$$\begin{aligned}\varepsilon(s_1) &= 1 \\ \varepsilon(s_4p_1p_2) &= -1 \\ \varepsilon(p_2s_3) &= 1\end{aligned}$$

Ejercicio 3.2.19. En el grupo S_3 , se consideran las permutaciones $\sigma = (1\ 2\ 3)$ y $\tau = (1\ 2)$.

1. Demostrar que

$$S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Sabemos que $|S_3| = 3! = 6$. Dividimos S_3 en dos conjuntos, uno con las permutaciones pares (P) y otro con las impares (I).

$$\begin{aligned}P &= \{1, \sigma, \sigma^2\} \\ I &= \{\tau, \sigma\tau, \sigma^2\tau\}\end{aligned}$$

Como $O(\sigma) = 3$, tenemos que las tres permutaciones pares son distintas. Supongamos ahora que dos permutaciones impares son iguales. Entonces, componiendo por la derecha con τ^{-1} , obtenemos que dos permutaciones pares serían iguales, algo que hemos descartado. Por tanto, las tres permutaciones impares son distintas.

$$|P| = |I| = 3$$

Como una permutación par no puede ser igual a una impar, tenemos que $P \cap I = \emptyset$. Por tanto:

$$\left. \begin{array}{l} |P \cup I| = |P| + |I| = 6 = |S_3| \\ \wedge \\ P \cup I \subset S_3 \end{array} \right\} \Rightarrow S_3 = P \cup I$$

Por tanto, $S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.

2. Reescribir la tabla de multiplicar de S_3 empleando la anterior expresión de los elementos de S_3 .

| \cdot | 1 | σ | σ^2 | τ | $\sigma\tau$ | $\sigma^2\tau$ |
|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| 1 | 1 | σ | σ^2 | τ | $\sigma\tau$ | $\sigma^2\tau$ |
| σ | σ | σ^2 | 1 | $\sigma\tau$ | $\sigma^2\tau$ | τ |
| σ^2 | σ^2 | 1 | σ | $\sigma^2\tau$ | τ | $\sigma\tau$ |
| τ | τ | $\sigma^2\tau$ | $\sigma\tau$ | 1 | σ^2 | σ |
| $\sigma\tau$ | $\sigma\tau$ | τ | $\sigma^2\tau$ | σ | 1 | σ^2 |
| $\sigma^2\tau$ | $\sigma^2\tau$ | $\sigma\tau$ | τ | σ^2 | σ | 1 |

3. Probar que

$$\sigma^3 = 1, \quad \tau^2 = 1, \quad \tau\sigma = \sigma^2\tau.$$

Como $O(\sigma) = 3$, tenemos que $\sigma^3 = 1$. Por otro lado, como $O(\tau) = 2$, tenemos que $\tau^2 = 1$. El último caso hay que calcularlo, y se ha visto ya en la tabla de multiplicar.

4. Observar que es posible escribir toda la tabla de multiplicar de S_3 usando simplemente la descripción anterior y las relaciones anteriores.

Ejercicio 3.2.20. Describir los diferentes ciclos del grupo S_4 . Expresar todos los elementos de S_4 como producto de ciclos disjuntos.

Veamos cuántos ciclos de longitud m hay en un S_n . Cada una de las elecciones es una variación de n elementos tomados de m en m . Como además un mismo ciclo de longitud m puede empezar en m posiciones distintas, tenemos que el número de ciclos de longitud m es:

$$\frac{V_n^m}{m} = \frac{n!}{m(n-m)!}$$

Por tanto, los ciclos son:

| l | Nº | Ciclos |
|---|----|--|
| 1 | 1 | id |
| 2 | 6 | $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$ |
| 3 | 8 | $(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$ |
| 4 | 6 | $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$ |

Tenemos ahora que $|S_4| = 4! = 24$. Como ya hemos dado 21 elementos, nos faltan 3. Estos son los elementos que no son ciclos, y son los siguientes:

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

Ejercicio 3.2.21. Demostrar que el conjunto de transposiciones

$$\{(1, 2), (2, 3), \dots, (n-1, n)\}$$

genera al grupo simétrico S_n .

Demostramos por doble inclusión que:

$$\langle (1, 2), (2, 3), \dots, (n-1, n) \rangle = S_n$$

⊂) Dado $\sigma \in \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$, entonces como S_n es cerrado por producto, se tiene que $\sigma \in S_n$.

⊃) Dado $\sigma \in S_n$, veamos que $\sigma \in \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$. Por ser una permutación, tenemos que σ es producto de transposiciones. Por tanto, basta con demostrar que cualquier transposición se puede escribir como producto de elementos de $\{(1, 2), (2, 3), \dots, (n-1, n)\}$.

Sea una transposición (i, j) , y sin pérdida de generalidad, supongamos que $i < j$. Entonces, se tiene que:

$$(i, j) = (i, i+1)(i+1, i+2) \cdots (j-2, j-1)(j-1, j)(j-2, j-1) \cdots (i+1, i+2)(i, i+1)$$

Por tanto, $\sigma \in \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$.

Ejercicio 3.2.22. Demostrar que el conjunto $\{(1, 2, \dots, n), (1, 2)\}$ genera al grupo simétrico S_n .

Demostramos por doble inclusión que:

$$\langle (1, 2, \dots, n), (1, 2) \rangle = S_n$$

⊂) Dado $\sigma \in \langle (1, 2, \dots, n), (1, 2) \rangle$, entonces como S_n es cerrado por producto, se tiene que $\sigma \in S_n$.

⊃) Dado $\sigma \in S_n$, veamos que $\sigma \in \langle (1, 2, \dots, n), (1, 2) \rangle$. En primer lugar, definimos $\tau = (1, 2, \dots, n)$. Entonces, se tiene que:

$$\tau^k(j) = j + k \quad \forall k, j \in \{1, \dots, n\}, \quad k + j \leq n$$

Además, por las propiedades de los conjugados, tenemos que:

$$\tau^{(k-1)}(1, 2)\tau^{-(k-1)} = (\tau^{k-1}(1), \tau^{k-1}(2)) = (k, k+1) \quad \forall k \in \mathbb{N}, \quad k < n$$

Entonces, tenemos que:

$$\{(1, 2), (2, 3), \dots, (n-1, n)\} \subset \langle (1, 2, \dots, n), (1, 2) \rangle$$

Por tanto:

$$\sigma \in S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle \subset \langle (1, 2, \dots, n), (1, 2) \rangle$$

Ejercicio 3.2.23. Demostrar que para cualquier permutación $\alpha \in S_n$ se verifica que $\varepsilon(\alpha) = \varepsilon(\alpha^{-1})$, donde ε denota la signatura, o paridad, de una permutación.

Sabemos que la paridad depende del número de ciclos de longitud par que tiene una permutación en su descomposición en ciclos disjuntos. Como este valor es el mismo para una permutación y su inversa, se tiene que $\varepsilon(\alpha) = \varepsilon(\alpha^{-1})$.

Ejercicio 3.2.24. Demostrar que si $(x_1 \ x_2 \ \cdots \ x_r) \in S_n$ es un ciclo de longitud r , entonces

$$\varepsilon(x_1 x_2 \cdots x_r) = (-1)^{r-1}.$$

- Si r es par, entonces hay un solo ciclo de longitud par, y por tanto $\varepsilon(x_1 x_2 \cdots x_r) = -1$. Como además $r-1$ es impar, se tiene que $(-1)^{r-1} = -1$.
- Si r es impar, entonces hay un solo ciclo de longitud impar, y 0 ciclos de longitud par. Por tanto, $\varepsilon(x_1 x_2 \cdots x_r) = 1$. Como además $r-1$ es par, se tiene que $(-1)^{r-1} = 1$.

Ejercicio 3.2.25. Encontrar un isomorfismo $\mu_2 \cong \mathbb{Z}_3^\times$.

Definimos la aplicación $f : \mu_2 \rightarrow \mathbb{Z}_3^\times$ dada por:

$$\begin{aligned} 1 &\mapsto 1 \\ -1 &\mapsto 2 \end{aligned}$$

Vemos de forma directa que es biyectiva. Veamos además que se trata de un homomorfismo. Para ello, a priori deberíamos de comprobar que, para todas las parejas $x, y \in \mu_2$, se cumple que $f(xy) = f(x)f(y)$. Sin embargo, por tratarse de grupos conmutativos, podemos ahorrarnos la comprobación de algunas de ellas. Además, en todas las parejas en las que aparezca el elemento neutro, puesto que $f(1) = 1$, se tiene que:

$$f(x) = f(1 \cdot x) = f(1) \cdot f(x) = 1 \cdot f(x) = f(x) \quad \forall x \in \mu_2$$

Por tanto, todas estas también se tienen ya comprobadas (idea que repetiremos en ejercicios posteriores). Comprobamos las restantes:

$$1 = f(1) = f((-1) \cdot (-1)) = f(-1) \cdot f(-1) = 2 \cdot 2 = 4 = 1$$

Por tanto, f es un isomorfismo entre ambos grupos.

Ejercicio 3.2.26.

1. Demostrar que la aplicación $f : \mu_4 \rightarrow \mathbb{Z}_5^\times$ dada por:

$$1 \mapsto 1, \quad -1 \mapsto 4, \quad i \mapsto 2, \quad -i \mapsto 3,$$

da un isomorfismo entre el grupo μ_4 de las raíces cuárticas de la unidad y el grupo \mathbb{Z}_5^\times de las unidades en \mathbb{Z}_5 .

De forma directa, vemos que es biyectiva. Para ver que es un homomorfismo, tendremos que comprobar que se da la condición para las 16 posibles parejas. Por tratarse de grupos conmutativos, podremos ahorrarnos la comprobación de algunas de ellas.

$$\begin{aligned} 1 &= f(1) = f((-1) \cdot (-1)) = f(-1) \cdot f(-1) = 4 \cdot 4 = 16 = 1 \\ 4 &= f(-1) = f(i \cdot i) = f(i) \cdot f(i) = 2 \cdot 2 = 4 \\ 4 &= f(-1) = f((-i) \cdot (-i)) = f(-i) \cdot f(-i) = 3 \cdot 3 = 9 = 4 \\ 3 &= f(-i) = f((-1) \cdot i) = f(-1) \cdot f(i) = 4 \cdot 2 = 8 = 3 \\ 2 &= f(i) = f((-1) \cdot (-i)) = f(-1) \cdot f(-i) = 4 \cdot 3 = 12 = 2 \\ 1 &= f(1) = f(i \cdot (-i)) = f(i) \cdot f(-i) = 2 \cdot 3 = 6 = 1 \end{aligned}$$

Por tanto, f es un isomorfismo entre ambos grupos.

2. Encontrar otro isomorfismo entre estos dos grupos que sea distinto del anterior.

Sea $g : \mu_4 \rightarrow \mathbb{Z}_5^\times$ otra aplicación que a continuación definiremos de forma que sea un isomorfismo. En primer lugar, hemos de imponer que $g(1) = 1$, por ser este el elemento neutro en ambos grupos. Por otro lado, en \mathbb{Z}_5^\times tenemos que:

$$O(2) = O(3) = 4 \quad O(4) = 2$$

Como en μ_2 tenemos que $O(-1) = 2$ y sabemos que el orden se conserva en un isomorfismo, tenemos que ha de ser $g(-1) = 4$. Por tanto, solo nos quedan dos opciones para i y $-i$ de forma que g sea biyectiva. Una de ellas opciones nos daría f , por lo que consideramos la otra alternativa. Definimos g entonces como sigue:

$$1 \mapsto 1, \quad -1 \mapsto 4, \quad i \mapsto 3, \quad -i \mapsto 2,$$

La biyección la tenemos de forma directa, y hemos de comprobar que se trata de un homomorfismo. Comprobamos tan solo los pares en los que intervienen los elementos i o $-i$:

$$\begin{aligned} 4 &= g(-1) = g(i \cdot i) = g(i) \cdot g(i) = 3 \cdot 3 = 9 = 4 \\ 4 &= g(-1) = g((-i) \cdot (-i)) = g(-i) \cdot g(-i) = 2 \cdot 2 = 4 \\ 3 &= g(i) = g((-1) \cdot (-i)) = g(-1) \cdot g(-i) = 4 \cdot 2 = 8 = 3 \\ 2 &= g(-i) = g((-1) \cdot i) = g(-1) \cdot g(i) = 4 \cdot 3 = 12 = 2 \\ 1 &= g(1) = g(i \cdot (-i)) = g(i) \cdot g(-i) = 3 \cdot 2 = 6 = 1 \end{aligned}$$

Ejercicio 3.2.27. Encontrar un isomorfismo $\mu_2 \times \mu_2 \cong \mathbb{Z}_8^\times$.

Sea $f : \mu_2 \times \mu_2 \rightarrow \mathbb{Z}_8^\times$ la aplicación definida por:

$$\begin{aligned} (1, 1) &\mapsto 1 \\ (1, -1) &\mapsto 3 \\ (-1, 1) &\mapsto 5 \\ (-1, -1) &\mapsto 7 \end{aligned}$$

Comprobamos que es biyectiva de forma directa. Veamos ahora que es un homomorfismo:

$$\begin{aligned} 1 &= f(1, 1) = f[(1, -1)(1, -1)] = f(1, -1)f(1, -1) = 3 \cdot 3 = 9 = 1 \\ 1 &= f(1, 1) = f[(-1, 1)(-1, 1)] = f(-1, 1)f(-1, 1) = 5 \cdot 5 = 25 = 1 \\ 1 &= f(1, 1) = f[(-1, -1)(-1, -1)] = f(-1, -1)f(-1, -1) = 7 \cdot 7 = 49 = 1 \\ 7 &= f(-1, -1) = f[(1, -1)(-1, 1)] = f(1, -1)f(-1, 1) = 3 \cdot 5 = 15 = 7 \\ 5 &= f(-1, 1) = f[(1, -1)(-1, -1)] = f(1, -1)f(-1, -1) = 3 \cdot 7 = 21 = 5 \\ 3 &= f(1, -1) = f[(-1, 1)(-1, -1)] = f(-1, 1)f(-1, -1) = 5 \cdot 7 = 35 = 3 \end{aligned}$$

Por tanto, f es un isomorfismo entre ambos grupos.

Ejercicio 3.2.28. Demostrar, haciendo uso de las representaciones conocidas, que $D_3 \cong S_3 \cong \text{GL}_2(\mathbb{Z}_2)$.

En primer lugar, tenemos que:

$$\begin{aligned} |D_3| &= 2 \cdot 3 = 6 \\ |S_3| &= 3! = 6 \\ |\text{GL}_2(\mathbb{Z}_2)| &= (2^2 - 1)(2^2 - 2) = 6 \end{aligned}$$

Ahora, damos generadores para cada grupo. El generador de S_3 se ha visto en el Ejercicio 3.2.22, mientras que el generador de $\text{GL}_2(\mathbb{Z}_2)$ se ha visto en el Ejercicio 3.2.10.

$$\begin{aligned} D_3 &= \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^{-1}s \rangle \\ S_3 &= \langle (1\ 2\ 3), (1\ 2) \rangle \\ \text{GL}_2(\mathbb{Z}_2) &= \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \end{aligned}$$

Comprobemos en primer lugar que el generador de S_3 cumple las relaciones de D_3 .

- Como $O((1\ 2\ 3)) = 3$, se tiene que $(1\ 2\ 3)^3 = 1$.
- Como $O((1\ 2)) = 2$, se tiene que $(1\ 2)^2 = 1$.
- Comprobemos que $(1\ 2)(1\ 2\ 3) = (3\ 2\ 1)(1\ 2)$.

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

Por tanto, por el Teorema de Dyck (Teorema 1.28), se tiene que existe un único homomorfismo f de D_3 en S_3 dado por:

$$\begin{aligned} r &\mapsto (1\ 2\ 3) \\ s &\mapsto (1\ 2) \end{aligned}$$

Como además $\{f(r), f(s)\}$ son un generador de S_3 , tenemos que se trata de un epimorfismo, y como además $|D_3| = |S_3|$, se trata de un isomorfismo. Por tanto, $D_3 \cong S_3$.

Comprobemos ahora que el generador de $\text{GL}_2(\mathbb{Z}_2)$ cumple las relaciones de D_3 .

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^3 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

Entonces, existe un único homomorfismo $g : S_3 \rightarrow \text{GL}_2(\mathbb{Z}_2)$ de forma que:

$$g(r) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad g(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Como además $\{g(r), g(s)\}$ son un generador de $\text{GL}_2(\mathbb{Z}_2)$, tenemos que se trata de un epimorfismo, y como además $|S_3| = |\text{GL}_2(\mathbb{Z}_2)|$, se trata de un isomorfismo. Por tanto, $S_3 \cong \text{GL}_2(\mathbb{Z}_2)$.

Por ser \cong una relación de equivalencia, tenemos que:

$$D_3 \cong S_3 \cong \text{GL}_2(\mathbb{Z}_2)$$

Ejercicio 3.2.29. Sea \mathbb{K} un cuerpo y considérese la operación binaria

$$\begin{aligned}\otimes : \mathbb{K} \times \mathbb{K} &\longrightarrow \mathbb{K} \\ (a, b) &\longmapsto a \otimes b = a + b - ab.\end{aligned}$$

Demostrar que $(\mathbb{K} \setminus \{1\}, \otimes)$ es un grupo isomorfo al grupo multiplicativo \mathbb{K}^* .

En primer lugar, hemos de ver que es cerrado para el producto así definido. Dados $a, b \in \mathbb{K} \setminus \{1\}$, veamos que $a \otimes b \neq 1$. Tenemos que:

$$a \otimes b = 1 \iff a + b - ab = 1 \iff a(1 - b) = 1 - b \iff a = 1$$

donde, en la última implicación, hemos usado que \mathbb{K} es un cuerpo y $b \neq 1$, por lo que $1 - b \neq 0$ y por tanto tiene inverso. Por tanto, se tiene que $a \otimes b \neq 1$ y por tanto es cerrado para dicho producto. Veamos ahora que se trata de un grupo (donde hemos de tener en cuenta que no tenemos garantizada la conmutatividad de la suma):

1. **Asociatividad:** Dados $a, b, c \in \mathbb{K} \setminus \{1\}$, hemos de comprobar que se da la igualdad $(a \otimes b) \otimes c = a \otimes (b \otimes c)$. Tenemos que:

$$\begin{aligned}(a \otimes b) \otimes c &= (a + b - ab) \otimes c = a + b - ab + c - (a + b - ab)c \\ a \otimes (b \otimes c) &= a \otimes (b + c - bc) = a + b + c - bc - a(b + c - bc)\end{aligned}$$

Por tanto, tenemos que:

$$(a \otimes b) \otimes c = a \otimes (b \otimes c) \iff -ab - ac - bc - abc = -bc - ab - ac - abc$$

Por tanto, se tiene que la asociatividad se cumple.

2. **Elemento neutro:** Hemos de encontrar un elemento neutro $e \in \mathbb{K} \setminus \{1\}$ tal que $a \otimes e = a$ para todo $a \in \mathbb{K} \setminus \{1\}$. Tenemos que:

$$a \otimes e = a \iff a + e - ae = a \iff e = ae \iff e = 0$$

Por tanto, el elemento neutro es el elemento neutro para la suma en \mathbb{K} , $e = 0$.

3. **Elemento inverso:** Dado $a \in \mathbb{K} \setminus \{1\}$, hemos de encontrar un elemento inverso $a^{-1} \in \mathbb{K} \setminus \{1\}$ tal que $a \otimes a^{-1} = e$. Tenemos que:

$$a \otimes a^{-1} = 0 \iff a + a^{-1} - aa^{-1} = 0 \iff a = a^{-1}(-1 + a) \iff a^{-1} = a(-1 + a)^{-1}$$

donde hemos usado que $a \neq 1$ y por tanto $-1 + a \neq 0$, por lo que podemos considerar su inverso en \mathbb{K} .

Veamos ahora que son isomorfos. Como necesitamos que la imagen del 0 sera el 1, definimos la siguiente aplicación:

$$\begin{aligned}f : \mathbb{K} \setminus \{1\} &\longrightarrow \mathbb{K}^* \\ x &\longmapsto 1 - x\end{aligned}$$

Veamos en primer lugar que está bien definida.

$$f(x) = 1 - x = 0 \iff x = 1 \notin \mathbb{K} \setminus \{1\}$$

Veamos ahora que es un homomorfismo. Dados $x, y \in \mathbb{K} \setminus \{1\}$, tenemos que:

$$f(x \otimes y) = 1 - (x \otimes y) = 1 - (x + y - xy) = 1 - x - y + xy = f(x)f(y) = (1 - x)(1 - y) = 1 - x - y + xy$$

Por tanto, f es un homomorfismo entre ambos grupos. Además, es biyectiva, ya que su inversa es $f^{-1}(x) = 1 - x$. Por tanto, f es un isomorfismo entre ambos grupos.

Ejercicio 3.2.30.

1. Probar que si $f : G \rightarrow G'$ es un isomorfismo de grupos, entonces se mantiene el orden; es decir, $O(a) = O(f(a))$ para todo elemento $a \in G$.

Probado en la Proposición 1.27.

2. Listar los órdenes de los diferentes elementos del grupo Q_2 y del grupo D_4 y concluir que D_4 y Q_2 no son isomorfos.

En primer lugar, tenemos que:

$$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

Calculamos los órdenes de D_4 :

$$O(1) = 1 \quad O(r) = O(r^3) = 4$$

$$O(r^2) = O(s) = O(sr) = O(sr^2) = O(sr^3) = 2$$

Por otro lado, calculamos los órdenes de Q_2 :

$$O(1) = 1 \quad O(-1) = 2$$

$$O(\pm i) = O(\pm j) = O(\pm k) = 4$$

Por tanto no es posible establecer un isomorfismo $f : D_4 \rightarrow Q_2$ de forma que cumpla

$$O(x) = O(f(x)) \quad \forall x \in D_4$$

Por tanto, D_4 y Q_2 no son isomorfos.

Ejercicio 3.2.31. Calcular el orden de:

1. La permutación $\sigma = (1 \ 8 \ 10 \ 4)(2 \ 8)(5 \ 1 \ 4 \ 8) \in S_{15}$.

$$\sigma = (2 \ 10 \ 4)(5 \ 8)$$

$$O(\sigma) = \text{mcm}(3, 2) = 6$$

2. Cada elemento del grupo \mathbb{Z}_{11}^\times .

$$O(1) = 1$$

$$O(3) = O(4) = O(5) = O(9) = 5$$

$$O(2) = O(6) = O(7) = O(8) = 10$$

$$O(10) = 2$$

Ejercicio 3.2.32. Demostrar que un grupo generado por dos elementos distintos de orden dos, que conmutan entre sí, consiste del 1, de esos elementos y de su producto y es isomorfo al grupo de Klein.

Sea $G = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$. Entonces, por el Ejercicio 3.2.13 tenemos:

$$G = \{1, a, b, ab\}$$

Sea ahora el grupo de Klein el siguiente:

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

Por tanto, hemos de encontrar un isomorfismo entre ambos grupos. Comprémos que los elementos generadores de V cumplen las relaciones de G :

$$\begin{aligned} O((1\ 2)(3\ 4)) &= \text{mcm}(2, 2) = 2 \implies [(1\ 2)(3\ 4)]^2 = 1 \\ O((1\ 3)(2\ 4)) &= \text{mcm}(2, 2) = 2 \implies [(1\ 3)(2\ 4)]^2 = 1 \\ (1\ 2)(3\ 4) (1\ 3)(2\ 4) &= (1\ 4)(2\ 3) \\ (1\ 3)(2\ 4) (1\ 2)(3\ 4) &= (1\ 4)(2\ 3) \end{aligned}$$

Por tanto, por el Teorema de Dyck (Teorema 1.28), se tiene que existe un único homomorfismo $f : G \rightarrow V$ cumpliendo:

$$\begin{aligned} a &\mapsto (1\ 2)(3\ 4) \\ b &\mapsto (1\ 3)(2\ 4) \end{aligned}$$

Como además $\{f(a), f(b)\}$ son un generador de V , tenemos que se trata de un epimorfismo, y como además $|G| = |V|$, se trata de un isomorfismo. Por tanto, $G \cong V$.

Ejercicio 3.2.33. Sea G un grupo y sean $a, b \in G$.

1. Demostrar que $O(b) = O(aba^{-1})$ (un elemento y su conjugado tienen el mismo orden).

Para todo $n \in \mathbb{N}$, se tiene que:

$$1 = (aba^{-1})^n = ab^n a^{-1} \iff a^{-1} = b^n a^{-1} \iff 1 = b^n$$

Comprémos ahora que $O(b) = O(aba^{-1})$:

- Si $O(b) = \infty$, supongamos por reducción al absurdo que $\exists n \in \mathbb{N}$ tal que $(aba^{-1})^n = 1$. Entonces, se tiene que $b^n = 1$, lo que contradice que $O(b) = \infty$.
- Si $O(b) = n$, entonces se tiene que $b^n = 1$, por lo que $(aba^{-1})^n = 1$ y por tanto $O(aba^{-1}) \leq n$. Por otro lado, supongamos que $\exists m \in \mathbb{N}$, con $m < n$, tal que $(aba^{-1})^m = 1$. Entonces, se tiene que $b^m = 1$, lo que contradice que $O(b) = n$. Por tanto, $O(aba^{-1}) = n$.

En cualquier caso, se tiene que $O(b) = O(aba^{-1})$.

2. Demostrar que $O(ba) = O(ab)$.

Por el apartado anterior, considerando ahora $ba \in G$, se tiene:

$$O(ba) = O(a \, ba \, a^{-1}) = O(ab)$$

Ejercicio 3.2.34. Sea G un grupo y sean $a, b \in G$, $a \neq 1 \neq b$, tales que $a^2 = 1$ y $ab^2 = b^3a$. Demostrar que $O(a) = 2$ y que $O(b) = 5$.

Comprobemos en primer lugar que $O(a) = 2$. Por hipótesis, tenemos que $a^2 = 1$, por lo que $O(a) \mid 2$. Por tanto, $O(a) = 1$ o $O(a) = 2$. Como $a \neq 1$, se tiene que $O(a) = 2$. Veamos ahora que $O(b) = 5$. Tenemos que:

$$\begin{aligned} ab^2 = b^3a &\implies b^2 = ab^3a \implies \\ &\implies b^4 = (ab^3a)(ab^3a) = ab^6a = a(ab^3a)(ab^3a)a = b^9 \implies 1 = b^5 \end{aligned}$$

Por tanto, $O(b) \mid 5$. Por tanto, $O(b) = 1$ o $O(b) = 5$. Como $b \neq 1$, se tiene que $O(b) = 5$.

Ejercicio 3.2.35. Sea $f : G \rightarrow H$ un homomorfismo de grupos.

1. $f(x^n) = f(x)^n \, \forall n \in \mathbb{Z}$.

Por inducción, se tiene que:

- Caso base: $n = 1$.

$$f(x^1) = f(x) = f(x)^1$$

- Paso inductivo: Supongamos que se cumple para n , y veamos que se cumple para $n + 1$.

$$f(x^{n+1}) = f(x^n x) = f(x^n) f(x) = f(x)^n f(x) = f(x)^{n+1}$$

Por tanto, se tiene que $f(x^n) = f(x)^n \, \forall n \in \mathbb{Z}$.

2. Si f es un isomorfismo entonces G y H tienen el mismo número de elementos de orden n . ¿Es cierto el resultado si f es sólo un homomorfismo?

Consideramos la aplicación inclusión dada por:

$$\begin{aligned} i : \mathbb{R}^* &\longrightarrow \mathbb{C}^* \\ x &\longmapsto x \end{aligned}$$

Comprobemos que se trata de un homomorfismo:

$$i(x \cdot y) = x \cdot y = i(x) \cdot i(y) \quad \forall x, y \in \mathbb{R}^*$$

No obstante, tenemos que en \mathbb{C}^* hay elementos de orden 4 ($O(i) = 4$), mientras que en \mathbb{R}^* no los hay. Por tanto, no se cumple el resultado si f es solo un homomorfismo.

3. Si f es un isomorfismo entonces G es abeliano $\Leftrightarrow H$ es abeliano.

Probado en la Proposición 1.27.

Ejercicio 3.2.36.

1. Demostrar que los grupos multiplicativos \mathbb{R}^* (de los reales no nulos) y \mathbb{C}^* (de los complejos no nulos) no son isomorfos.

En \mathbb{C}^* , tenemos que $O(i) = 4$. Busquemos $x \in \mathbb{R}^*$ tal que $O(x) = 4$.

$$x^4 = 1 \iff x = \pm 1$$

No obstante, $O(1) = 1$ y $O(-1) = 2$. Por tanto, no pueden ser isomorfos.

2. Demostrar que los grupos aditivos \mathbb{Z} y \mathbb{Q} no son isomorfos.

Por reducción al absurdo, supongamos que existe un isomorfismo $f : \mathbb{Q} \rightarrow \mathbb{Z}$. Entonces, consideramos $f^{-1}(1) = q \in \mathbb{Q}$, que sabemos que existe por ser f biyectiva. Entonces, se tiene que:

$$1 = f(q) = f\left(\frac{q}{2} + \frac{q}{2}\right) = f\left(\frac{q}{2}\right) + f\left(\frac{q}{2}\right) = 2f\left(\frac{q}{2}\right) \implies f\left(\frac{q}{2}\right) = \frac{1}{2} \notin \mathbb{Z}$$

Por tanto, hemos llegado a una contradicción y, por tanto, hemos probado que no puede existir tal isomorfismo.

Ejercicio 3.2.37. Sea G un grupo. Demostrar:

1. G es abeliano \iff La aplicación $f : G \rightarrow G$ dada por $f(x) = x^{-1}$ es un homomorfismo de grupos.

\implies) Supongamos que G es abeliano. Entonces, para todo $x, y \in G$, se tiene que:

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1} \stackrel{(*)}{=} x^{-1}y^{-1} = f(x)f(y)$$

donde en $(*)$ hemos usado que G es abeliano. Por tanto, f es un homomorfismo.

\impliedby) Supongamos que f es un homomorfismo. Entonces, para todo $x, y \in G$, se tiene que:

$$xy = (y^{-1}x^{-1})^{-1} = f(y^{-1}x^{-1}) = f(y^{-1})f(x^{-1}) = yx$$

Por tanto, G es abeliano.

2. G es abeliano \iff La aplicación $f : G \rightarrow G$ dada por $f(x) = x^2$ es un homomorfismo de grupos.

\implies) Supongamos que G es abeliano. Entonces, para todo $x, y \in G$, se tiene que:

$$f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$$

Por tanto, f es un homomorfismo.

\Longleftrightarrow) Supongamos que f es un homomorfismo. Entonces, para todo $x, y \in G$, se tiene que:

$$xyxy = f(xy) = f(x)f(y) = x^2y^2 \implies xy = yx$$

Por tanto, G es abeliano.

Ejercicio 3.2.38. Si G es un grupo cíclico demostrar que cualquier homomorfismo de grupos $f : G \rightarrow H$ está determinado por la imagen del generador.

Sea $G = \langle a \rangle$. Entonces, para todo $x \in G$, se tiene que $x = a^n$ para algún $n \in \mathbb{Z}$. Por tanto, se tiene que:

$$f(x) = f(a^n) = f(a)^n$$

Por tanto, f está determinado por la imagen de a .

Ejercicio 3.2.39. Demostrar que no existe ningún cuerpo \mathbb{K} tal que sus grupos aditivo $(\mathbb{K}, +)$ y (\mathbb{K}^*, \cdot) sean isomorfos.

Si \mathbb{K} es finito, entonces:

$$|\mathbb{K}^*| = |\mathbb{K}| - 1 \neq |\mathbb{K}|$$

Por tanto, no pueden ser isomorfos. Si \mathbb{K} es infinito, entonces supongamos por reducción al absurdo que existe un isomorfismo $f : \mathbb{K} \rightarrow \mathbb{K}^*$. Como \mathbb{K} es un cuerpo, podemos considerar su característica, que es el orden del 1 en el grupo aditivo.

1. Si \mathbb{K} tiene característica 2, entonces $1 + 1 = 0$, por lo que $1 = -1$. Por tanto, para cada $x \in \mathbb{K}$, se tiene que:

$$x + x = x + 1 \cdot x = x + (-1) \cdot x = x - x = 0$$

Por tanto, en \mathbb{K} vemos que $O(x) = 2$ para todo $x \neq 0$. Como el orden se conserva en un isomorfismo, en \mathbb{K}^* también se tendría que $O(x) = 2$ para todo $x \neq 0, 1$; o equivalentemente, $x^2 = 1$ para todo $x \neq 0, 1$. Es decir:

$$(x - 1)(x + 1) = 0 \quad \forall x \in \mathbb{K}^* \setminus \{1\}$$

Por ser \mathbb{K} un cuerpo, en particular es un DI, y por tanto o bien $x - 1 = 0$ o bien $x + 1 = 0$; por lo que $x = 1$ o $x = -1$. Por tanto, tenemos que $\mathbb{K}^* = \{1, -1\}$, y de hecho es $\mathbb{K}^* = \{1\}$; es decir, el cuerpo trivial. Esto contradice que \mathbb{K} sea infinito.

2. Si \mathbb{K} tiene característica distinta de 2, entonces $1 + 1 \neq 0$. Por ser f un isomorfismo, consideramos f^{-1} . En \mathbb{K}^* , se tiene que:

$$(-1)(-1) = 1 \implies O(-1) = 2$$

Por ser el orden conservado en un isomorfismo, tenemos que:

$$O(f^{-1}(-1)) = 2 \implies f^{-1}(-1) + f^{-1}(-1) = 0 \implies f^{-1}(-1)(1 + 1) = 0$$

Por ser \mathbb{K} un cuerpo, en particular es un DI, y por tanto o bien $f^{-1}(-1) = 0$ o bien $1 + 1 = 0$. Como la característica de \mathbb{K} es distinta de 2, se tiene que $1 + 1 \neq 0$, por lo que:

$$f^{-1}(-1) = 0 \implies f(0) = -1$$

No obstante, $f(0) = 1$. Además, $1 \neq -1$ (pues la característica de \mathbb{K} es distinta de 2), por lo que hemos llegado a que f no es inyectiva, lo que contradice que sea un isomorfismo.

En cualquier caso, no puede existir un cuerpo \mathbb{K} tal que sus grupos aditivo y multiplicativo sean isomorfos.

3.3. Subgrupos, Generadores, Retículos y Grupos cíclicos

Ejercicio 3.3.1. Describir todos los elementos de los grupos alternados A_n , consistentes en las permutaciones pares del S_n correspondiente, para:

1. $n = 2$.

$$S_2 = \{1, (1\ 2)\}$$

$$A_2 = \{1\}$$

2. $n = 3$.

$$S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

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

3. $n = 4$.

$$S_4 = \{1, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4),$$

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

$$(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

$$A_4 = \{1, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),$$

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Ejercicio 3.3.2. Sea D_n el grupo diédrico. Demostrar que el subgrupo de D_n generado por los elementos $\{r^j s, r^k s\}$ es todo el grupo D_n siempre que $0 \leq j < k < n$ y $\text{mcd}(k - j, n) = 1$.

Haciendo uso de que $D_n = \langle r, s \rangle$, veamos que:

$$\langle r^j s, r^k s \rangle = D_n$$

\subseteq) Como $r, s \in D_n$, entonces $r^j s, r^k s \in D_n$. Por ser D_n un grupo, en particular es cerrado para el producto y para inversos, por lo que $\langle r^j s, r^k s \rangle \subseteq D_n$.

\supseteq) Veamos en primer lugar que $r \in \langle r^j s, r^k s \rangle$. Sabemos que:

$$(r^j s)^{-1} = s r^{-j} \in \langle r^j s, r^k s \rangle$$

Por tanto, como $r^k s \in \langle r^j s, r^k s \rangle$, entonces:

$$r^k s (r^j s)^{-1} = r^k s s r^{-j} = r^{k-j} \in \langle r^j s, r^k s \rangle$$

Como $\text{mcd}(k - j, n) = 1$, entonces existe $m \in \mathbb{Z}$, con $0 \leq m < n$, tal que $m(k - j) = qn + 1$ para algún $q \in \mathbb{Z}$. Por tanto:

$$(r^{k-j})^m = r^{m(k-j)} = r^{qn+1} = r \in \langle r^j s, r^k s \rangle$$

Por último, veamos que $s \in \langle r^j s, r^k s \rangle$. Como $r \in \langle r^j s, r^k s \rangle$, entonces:

$$r^{n-j} r^j s = r^{n-j+j} s = s \in \langle r^j s, r^k s \rangle$$

Por tanto, $r, s \in \langle r^j s, r^k s \rangle$, y por ser $D_n = \langle r, s \rangle$, entonces $D_n \subset \langle r^j s, r^k s \rangle$.

Ejercicio 3.3.3.

1. Demostrar que el subgrupo de $\text{SL}_2(\mathbb{Z}_3)$ generado por los elementos

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

es isomorfo al grupo cuaternio Q_2 .

Por la propiedad transitiva de la isomorfia, basta con encontrar un isomorfismo entre $\text{SL}_2(\mathbb{Z}_3)$ y:

$$Q_2^{abs} = \langle x, y \mid x^4 = 1, y^2 = x^2, yx = x^{-1}y \rangle$$

Comprobamos que i, j cumplen las relaciones de Q_2^{abs} :

$$\begin{aligned} i^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ j^2 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ ji &= \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \\ i^3j &= \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \end{aligned}$$

Por tanto, i, j cumplen las relaciones de Q_2^{abs} . Por el Teorema de Teorema de Dyck, existe un único homomorfismo $f : Q_2^{abs} \rightarrow \langle i, j \rangle$ tal que $f(x) = i$ y $f(y) = j$.

- Como $i, j \in \langle i, j \rangle$ son un generador de $\langle i, j \rangle$, entonces se trata de un epimorfismo.
- Para terminar de ver que es un isomorfismo, basta con comprobar que $|Q_2^{abs}| = |\langle i, j \rangle|$. Sabemos que:

$$\begin{aligned} \langle i, j \rangle &= \{1, i, i^2, i^3, j, ij, i^2j, i^3j\} \\ |Q_2^{abs}| &= 8 = |\langle i, j \rangle| \end{aligned}$$

Por tanto, f es un isomorfismo.

Por tanto, $\langle i, j \rangle \cong Q_2^{abs} \cong Q_2$.

2. Demostrar que $\text{SL}_2(\mathbb{Z}_3)$ y S_4 son dos grupos de orden 24 que no son isomorfos.

Observación. Demostrar que S_4 no puede contener a ningún subgrupo isomorfo a Q_2 .

Ejercicio 3.3.4. Razonar que un subconjunto no vacío $X \subseteq G$ de un grupo G es un subgrupo de G si, y sólo si, $X = \langle X \rangle$.

\implies) Supongamos que X es un subgrupo de G , y veamos que $X = \langle X \rangle$.

\subseteq) Por definición de subgrupo generado por un conjunto, $X \subseteq \langle X \rangle$.

\supseteq) Veamos que $\langle X \rangle \subseteq X$. Dado $x \in \langle X \rangle$, entonces x es una combinación de elementos de X mediante el producto y el inverso. Por ser X un subgrupo, en particular es un grupo, por lo que es cerrado para el producto y para inversos. Por tanto, $x \in X$.

Por tanto, $X = \langle X \rangle$.

\impliedby) Supongamos que $X = \langle X \rangle$, y veamos que X es un subgrupo de G . Por definición, $\langle X \rangle$ es el menor subgrupo de G que contiene a X . Por tanto, X es un subgrupo de G .

Ejercicio 3.3.5. Sean $a, b \in G$ dos elementos de un grupo que conmutan entre sí, esto es, para los que $ab = ba$, y de manera que sus órdenes son primos relativos, esto es, $\text{mcd}(O(a), O(b)) = 1$.

1. Razonar que $\langle a \rangle \cap \langle b \rangle = \{1\}$.

Puesto que la intersección de dos subgrupos es un subgrupo, sabemos que $\langle a \rangle \cap \langle b \rangle$ es un subgrupo de G , y por tanto $1 \in \langle a \rangle \cap \langle b \rangle \neq \emptyset$. Por tanto, podemos considerar $x \in \langle a \rangle \cap \langle b \rangle$.

Como menciona el $\text{mcd}(O(a), O(b))$, podemos considerar que ambos órdenes son finitos. Por tanto, como el orden de todo elemento de un grupo finito divide al orden del grupo, entonces:

$$\begin{aligned} O(x) \mid |\langle a \rangle| &= O(a) \\ O(x) \mid |\langle b \rangle| &= O(b) \end{aligned}$$

Por tanto, $O(x)$ es divisor común de $O(a)$ y $O(b)$, y por ser $\text{mcd}(O(a), O(b)) = 1$, entonces $O(x) = 1$. Por tanto, $x = 1$, y por tanto $\langle a \rangle \cap \langle b \rangle = \{1\}$.

2. Demostrar que $O(ab) = O(a)O(b)$.

Puesto que conmutan, tenemos que:

$$(ab)^k = a^k b^k \quad \forall k \in \mathbb{Z}$$

Como $\text{mcd}(O(a), O(b)) = 1$ y $O(x) = O(x^{-1})$, suponiendo que $a, b \neq 1$ (puesto que en ese caso el resultado es trivial), entonces tenemos que:

$$(ab)^k = 1 \iff a^k b^k = 1 \iff a^k = b^k = 1 \iff \begin{cases} O(a) \mid k \\ O(b) \mid k \end{cases}$$

Por tanto, k debe ser múltiplo común de $O(a)$ y $O(b)$. Por tanto, por definición de orden:

$$O(ab) = \text{mcm}(O(a), O(b)) \stackrel{(*)}{=} O(a)O(b)$$

donde en $(*)$ hemos usado que $O(a)$ y $O(b)$ son primos relativos.

Ejercicio 3.3.6. Encontrar un grupo G y elementos $a, b \in G$ tales que sus órdenes sean primos relativos, pero para los que no se verifique la igualdad $O(ab) = O(a)O(b)$ del ejercicio anterior.

En primer lugar, hemos de tener que no conmuten. Por tanto, consideremos el grupo S_3 y los elementos:

$$\begin{aligned}a &= (1\ 2) \\ b &= (1\ 2\ 3)\end{aligned}$$

Tenemos que $O(a) = 2$ y $O(b) = 3$, y por tanto $\text{mcd}(O(a), O(b)) = 1$. Además, $O(a)O(b) = 6$. Supongamos que $\exists \sigma \in S_3$ tal que $O(\sigma) = 6$. Por tanto, el mínimo común múltiplo de los ciclos disjuntos que la descomponen debe ser 6. Sin embargo, esto no es posible, porque en S_3 tan solo hay elementos de orden 1, 2 y 3. Por tanto, $O(ab) \neq O(a)O(b)$.

Ejercicio 3.3.7. Sea G un grupo y $a, b \in G$ dos elementos de orden finito. ¿Es ab necesariamente de orden finito?

Observación. Considerar el grupo $\text{GL}_2(\mathbb{Q})$ y los elementos

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

Calculemos el orden de a y b :

$$\begin{aligned}a^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 \implies O(a) = 4 \\ b^2 &= \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \\ b^3 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 \implies O(b) = 6\end{aligned}$$

Calculamos ahora el orden de ab . Por inducción, demostraremos que:

$$(ab)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

■ Caso base: $n = 1$.

$$(ab)^1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

■ Supuesto cierto para n , demostramos para $n + 1$:

$$(ab)^{n+1} = (ab)^n(ab) = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -(n+1) \\ 0 & 1 \end{pmatrix}$$

Por tanto, como en $(ab)^n \neq I_2$ para todo $n \in \mathbb{N}$, entonces $O(ab) = \infty$.

Ejercicio 3.3.8. En el grupo S_3 se considera el conjunto

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

1. Demostrar que H es un subgrupo de S_3 .
2. Describir las diferentes clases de S_3 módulo H .

Ejercicio 3.3.9. Sea G un grupo finito.

1. Demostrar que si $H \leq G$ es un subgrupo, entonces $[G : H] = |G|$ si, y sólo si, $H = \{1\}$, mientras que $[G : H] = 1$ si, y sólo si, $H = G$.
2. Demostrar que si se tienen subgrupos $G_2 \leq G_1 \leq G$, entonces

$$[G : G_2] = [G : G_1][G_1 : G_2],$$

3. Demostrar que si se tiene una cadena descendente de subgrupos de la forma

$$G = G_0 \geq G_1 \geq \cdots \geq G_{r-1} \geq G_r,$$

entonces

$$[G : G_r] = \prod_{i=0}^{r-1} [G_i : G_{i+1}].$$

4. Demostrar que si se tiene una cadena descendente de subgrupos de la forma

$$G = G_0 \geq G_1 \geq \cdots \geq G_{r-1} \geq G_r = \{1\},$$

entonces

$$|G| = \prod_{i=0}^{r-1} [G_i : G_{i+1}].$$

Ejercicio 3.3.10.

1. Demostrar que si G es un grupo de orden 4, entonces se tiene que o bien G es cíclico, o bien es isomorfo al grupo de Klein.
2. Demostrar que si G es un grupo de orden 6, entonces se tiene que o bien G es cíclico, o bien es isomorfo al grupo diédrico D_3 .

Ejercicio 3.3.11. Describir los retículos de subgrupos de los siguientes grupos:

1. El grupo V de Klein.
2. El grupo simétrico S_3 .
3. El grupo diédrico D_4 .
4. El grupo cuaternio Q_2 .
5. El grupo alternado A_4 .

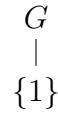


Figura 3.44: Retículo de subgrupos de para el Ejercicio 3.3.13.

Ejercicio 3.3.12. Fijado un número primo p , describe el retículo de subgrupos del grupo cíclico C_{p^n} . En particular, describe el retículo de subgrupos del grupo cíclico C_8 .

Ejercicio 3.3.13. Demostrar que un grupo finito $G \neq \{1\}$ carece de subgrupos propios, esto es, que su retículo de subgrupos es el de la Figura 3.44 si, y sólo si, $G = C_p$ es un grupo cíclico de orden primo.

Ejercicio 3.3.14. Describir los retículos de subgrupos de los grupos cíclicos siguientes:

1. C_6 .
2. C_{12} .

Ejercicio 3.3.15. Se considera el grupo cíclico C_{136} de orden 136, con generador t . ¿Qué relación hay entre los subgrupos $H_1 = \langle t^{48}, t^{72} \rangle$ y $H_2 = \langle t^{46} \rangle$?

Ejercicio 3.3.16. Demostrar que el grupo de unidades \mathbb{Z}_7^\times es un grupo cíclico.

Ejercicio 3.3.17. Sea G un grupo y sea C_n el grupo cíclico de orden n generado por x . Demostrar que:

1. Si $\theta : C_n \rightarrow G$ es un homomorfismo de grupos, entonces:

$$O(\theta(x)) \mid n, \quad \text{y} \quad \theta(x^k) = \theta(x)^k \quad \forall k \in \{0, \dots, n-1\}.$$

2. Para cada $g \in G$ tal que $O(g) \mid n$, existe un único homomorfismo de grupos $\theta_g : C_n \rightarrow G$ tal que $\theta_g(x) = g$.
3. Si $g \in G$ es tal que $O(g) \mid n$, entonces el morfismo θ_g es monomorfismo si, y sólo si, $O(g) = n$.
4. Existe un isomorfismo de grupos

$$U(\mathbb{Z}_n) \cong \text{Aut}(C_n),$$

dado por $r \mapsto f_r$ para cada $r = 1, \dots, n$ con $\text{mcd}(r, n) = 1$, donde el automorfismo f_r se define mediante $f_r(x) = x^r$.

En particular, $\text{Aut}(C_n)$ es un grupo abeliano de orden $\varphi(n)$.

Ejercicio 3.3.18.

1. Describir explícitamente el grupo de automorfismos $\text{Aut}(C_8)$.
2. Demostrar que $\text{Aut}(C_8)$ es isomorfo al grupo de Klein.