

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	7
1.1. Grupos diédricos D_n	19
1.1.1. Motivación	20
1.1.2. Definición y primeras propiedades	25
1.2. Generadores de un grupo	26
1.3. Grupos Simétricos S_n	29
1.3.1. Signatura	39
1.3.2. Grupos Alternados A_n	43
1.4. Grupos de matrices	45
1.4.1. Grupo lineal $GL_n(\mathbb{F})$	46
1.4.2. Grupo lineal especial $SL_n(\mathbb{F})$	47
1.5. Homomorfismos de grupos	48
1.5.1. Ejemplos	52
1.6. Resumen de grupos	55
2. Subgrupos, Generadores, Retículos y Grupos cíclicos	57
2.1. Generadores de subgrupos	60
2.2. Retículo de subgrupos de un grupo	62
2.2.1. Ejemplos	65
2.3. Índice y Teorema de Lagrange	73
2.4. Propiedades de grupos cíclicos	79
3. Grupos cocientes y Teoremas de isomorfía	85
3.1. Subgrupos normales	85
3.2. Grupo cociente	91
3.3. Teoremas de isomorfía	95
3.4. Producto directo	105
3.4.1. Caracterización del grupo directo por isomorfismo	108
3.4.2. Producto directo de una familia de grupos	112
3.4.3. Producto directo de una familia finita de subgrupos	113
3.5. Producto directo interno	113
3.5.1. Producto directo interno de una familia de subgrupos	120
3.5.2. Producto directo interno de una familia finita de subgrupos	120
3.6. Producto directo de grupos cíclicos	121

4. Grupos resolubles	123
4.1. Series de un grupo	123
4.1.1. Series de composición	125
4.2. Grupos resolubles	137
4.2.1. Preliminares	137
4.2.2. Definición	139
5. G-conjuntos y p-grupos	145
5.1. Órbitas de un elemento	149
5.1.1. Acción por traslación	153
5.1.2. Acción por conjugación	154
5.1.3. Acción por conjugación sobre subgrupos	157
5.2. p -grupos	157
5.2.1. p -subgrupos de Sylow	161
6. Clasificación de grupos abelianos finitos	169
7. Relaciones de Ejercicios	173
7.1. Combinatoria y Teoría de Grafos	173
7.2. Grupos: generalidades y ejemplos	219
7.3. Subgrupos, Generadores, Retículos y Grupos cíclicos	243
7.4. Grupos cociente. Teoremas de isomorfismo. Productos	266

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:*

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

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

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 forma 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 nulo 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 $O(x) \in \mathbb{N} \setminus \{0\}$ 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 equilátero (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 .

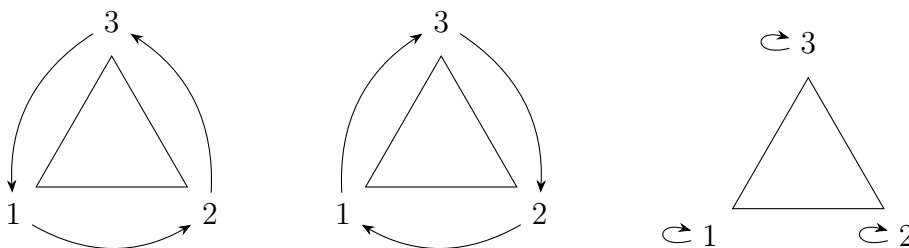


Figura 1.2: Todos los giros que dejan invariante al triángulo.

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. 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 .
- La simetría respecto a la recta l_3 es sr .

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

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.

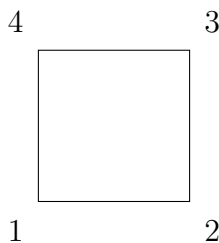


Figura 1.4: Cuadrado con centro en el origen de coordenadas.

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 $(1\ 4\ 3\ 2)$.
- El giro de ángulo 2π es la identidad, (1) .



Figura 1.5: Giros y simetrías que dejan invariante al cuadrado

- 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. $s^2 = 1$. En particular, $O(s) = 2$.
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 $x = 0$, entonces: $x = 1 - 1$.

2. $D_n = \langle r, s \rangle$, ya que $D_n = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$.

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 $D_1 = \{1, s\}$.

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:

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

Ejemplo. Las similitudes que hemos encontrado entre distintos grupos como entre V^{abs} y D_2 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 identidad), 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:

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

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):

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

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:

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

□

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 :

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

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 $\tau = r_1 r_2 r_3 r_4$:

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

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 . Como¹⁰:

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

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

¹⁰Marcamos en rojo los factores que se invierten.

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 $m - 1$:

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

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 y 1, tenemos que:

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

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:

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

Por tanto:

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

□

Con esta Proposición, la demostración de la Proposición 1.17 se hace ya evidente.

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 $n = 3$:

$$\begin{aligned} S_3 &= \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} \\ A_3 &= \{1, (1\ 2\ 3), (1\ 3\ 2)\} \end{aligned}$$

2. Para $n = 4$:

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

$$\begin{aligned} A_4 &= \{1, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), \\ &\quad (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \end{aligned}$$

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 $\mathcal{M}_n(\mathbb{F})$.
- Como el determinante del producto es el producto de los determinantes, \cdot es una operación cerrada para $\text{GL}_n(\mathbb{F})$.
- $\det(I) = 1 \neq 0$ 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 $|\mathrm{GL}_2(\mathbb{Z}_2)| = (2^2 - 1)(2^2 - 2) = 6$:

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

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

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 $\mathcal{M}_n(\mathbb{F})$.
- Como el determinante del producto es el producto de los determinantes, \cdot es una operación cerrada para $\mathrm{SL}_n(\mathbb{F})$.
- $\det(I) = 1$ 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 $\det(A)$ puede¹¹ tomar $q - 1$ valores distintos, uno por cada elemento de \mathbb{F}^* . De esta forma, si dado $k \in \mathbb{F}^*$ definimos:

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

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

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

¹¹De hecho los toma, es fácil comprobar que $\det : \mathrm{GL}_n(\mathbb{F}) \rightarrow \mathbb{F}^*$ es una aplicación sobreyectiva.

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

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

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:

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

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:

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

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. $f(1) = 1$

$$2. f(x^{-1}) = (f(x))^{-1}$$

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

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:

$$\blacksquare \ker f = \{x \in G \mid f(x) = 1\}$$

$$\blacksquare \operatorname{Im} f = \{f(x) \mid x \in G\}$$

Ejemplo. Ejemplos de homomorfismos de grupos son:

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

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:

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

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 $G \cong T$.

□

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 $S \subseteq G$ 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:

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

- 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 $id : G \rightarrow G$ 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 $x, y \in H$, existirá un isomorfismo $f : G \rightarrow H$, luego:

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

\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 $s_1, \dots, s_k \in S$ y $\gamma_1, \dots, \gamma_k \in \mathbb{Z}$ 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 $H = \langle f(S) \rangle$.

□

1.5.1. Ejemplos

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:

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

$$(1\ 2)^2 = (1\ 2)(1\ 2) = 1$$

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

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 que¹² $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$ y que $|D_3| = 2 \cdot 3 = 6 = 3! = |S_3|$, concluimos que f es un isomorfismo, por lo que $D_3 \cong S_3$.

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

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

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 $f : S_3 \rightarrow \text{GL}_2(\mathbb{Z}_2)$ 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 7.2.10):

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

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:

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

¹²Esto se vio en la Proposición 1.20.

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

$$f(r) = (1 \ 2 \ \dots \ n)$$

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

7. Si consideramos ahora:

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

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

$$i^4 = 1$$

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

$$ji(-j) = j(-k) = -i$$

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

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.

Esta observación la usaremos con frecuencia en toda la asignatura: cada vez que tengamos G un grupo y $H \subseteq G$, como casi siempre consideraremos en H la misma operación que en G , bastará simplemente demostrar también que H es un grupo, para así concluir que $H < G$.

□

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, $H < G$.

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.

□

Ejemplo. Se deja como ejercicio comprobar que:

1. $A_n < S_n$
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 todos 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:

$$2\mathbb{Z} \cup 3\mathbb{Z} \not< \mathbb{Z}$$

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 $S \neq \emptyset$, por doble inclusión:

\supseteq) Como $S \subseteq \langle S \rangle$ y $\langle S \rangle$ es un grupo, tendremos que:

$$x_1^{\gamma_1} x_2^{\gamma_2} \dots x_m^{\gamma_m} \in \langle S \rangle \quad x_i \in S, \gamma_i \in \mathbb{Z} \quad \forall 1 \leq i \leq m$$

\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 $\langle S \rangle$ el menor subgrupo que contiene a S , está claro que $\langle S \rangle \subseteq A$. \square

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 . \square

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.

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:

$$a = a \vee b = b \vee a = b$$

³Que en el contexto de teoría de conjuntos o del orden puede tener otra definición.

⁴Es común referirse a \vee por “supremo” y a \wedge por “ínfimo”.

- 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 $a \leq c$.

□

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:

⊇) Basta ver que:

$$T \subseteq \langle T \rangle \implies T \cup U \subseteq \langle T \rangle \cup U \implies \langle T \cup U \rangle \subseteq \langle \langle T \rangle \cup U \rangle$$

⊆) 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 :

$$\Lambda_G = \{H \subseteq G \mid H < G\}$$

Se verifica que Λ_G es un retículo, junto con las operaciones:

$$T \vee U = \langle T \cup U \rangle$$

$$T \wedge U = T \cap U$$

Además, la relación de orden en Λ_G es \subseteq .

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 $T, U \in \Lambda_G$:

$$T \vee U = \langle T \cup U \rangle = \langle U \cup T \rangle = U \vee T$$

- Asociativa. Sean $T, U, V \in \Lambda_G$:

$$\begin{aligned} T \vee (U \vee V) &= T \vee \langle U \cup V \rangle = \langle T \cup \langle U \cup V \rangle \rangle \stackrel{(*)}{=} \langle T \cup U \cup V \rangle \\ &\stackrel{(*)}{=} \langle \langle T \cup U \rangle \cup V \rangle = \langle T \cup U \rangle \vee V = (T \vee U) \vee V \end{aligned}$$

Donde en $(*)$ hemos aplicado el Lema anterior.

- Idempotencia. Sea $T \in \Lambda_G$:

$$T \vee T = \langle T \cup T \rangle = \langle T \rangle \stackrel{(*)}{=} T$$

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 $T, U \in \Lambda_G$:

$$\begin{aligned} T \vee (T \cap U) &= \langle T \cup (T \cap U) \rangle = \langle (T \cup T) \cap (T \cup U) \rangle = \langle T \cap (T \cup U) \rangle = \langle T \rangle = T \\ T \cap (T \vee U) &= T \cap \langle T \cup U \rangle = T \end{aligned}$$

Para ver que la relación de orden es \subseteq , notemos que si $T, U \in \Lambda_G$, entonces:

$$A \subseteq B \iff A \cap B = A$$

Que es como se define la relación de orden para los retículos. □

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 reflexiva) 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 lo que haremos será primero ordenar los vértices por “niveles” en función de la cardinalidad de los subgrupos: colocaremos en el nivel más bajo el menor subgrupo del grupo que consideremos (notemos que siempre será el subgrupo trivial $\{e\}$) e iremos subiendo en niveles por la cardinalidad del subgrupo, hasta llegar al nivel superior, donde colocaremos al grupo de mayor cardinal (que coincidirá con el grupo que consideramos inicialmente).

En segundo lugar, uniremos aquellos nodos que han de estar unidos mediante aristas no dirigidas (entendiendo que en realidad son aristas dirigidas, todas ellas apuntando hacia arriba, que es donde están los conjuntos más grandes).

De esta forma, tendremos el diagrama de Hasse ordenado por niveles, donde podremos ver “qué tan grande” es cada subgrupo, así como las relaciones de inclusión entre ellos gracias a las aristas.

2.2.1. Ejemplos

Ejemplo. Diagramas de Hasse para ciertos retículos⁶ son:

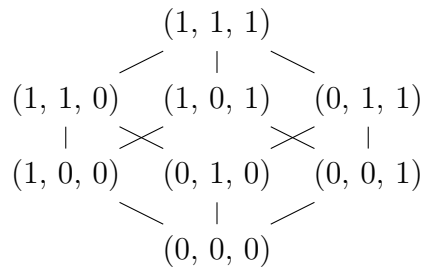
1. Para $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$:



Figura 2.1: Diagrama de Hasse para $D(30)$.

2. Para \mathcal{B}^3 , el álgebra de Boole con 3 elementos, tenemos:

⁶Notemos que cualquier retículo es un conjunto parcialmente ordenado.

Figura 2.2: Diagrama de Hasse para \mathcal{B}^3 .

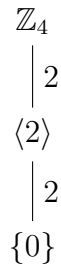
Centrándonos ya en los retículos que nos interesan, daremos a continuación varios ejemplos de retículos formados por los subgrupos de un grupo dado, que representaremos mediante sus diagramas de Hasse (en estos aparecerán las aristas etiquetadas con números, que por ahora ignoraremos, pero que luego 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 ello⁷, 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:

$$\begin{aligned}\langle 1 \rangle &= \langle 5 \rangle = \mathbb{Z}_6 \\ \langle 2 \rangle &= \langle 4 \rangle = \{0, 2, 4\} \\ \langle 3 \rangle &= \{0, 3\}\end{aligned}$$

⁷Al final del tema se entenderá por qué es suficiente con esto.

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:

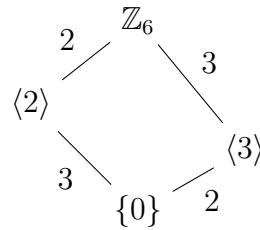


Figura 2.4: Diagrama de Hasse para los subgrupos de \mathbb{Z}_6 .

3. En \mathbb{Z}_8 , tenemos que:

$$\begin{aligned}\langle 1 \rangle &= \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_8 \\ \langle 2 \rangle &= \langle 6 \rangle = \{0, 2, 4, 6\} \\ \langle 4 \rangle &= \{0, 4\}\end{aligned}$$

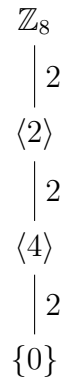


Figura 2.5: Diagrama de Hasse para los subgrupos de \mathbb{Z}_8 .

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:

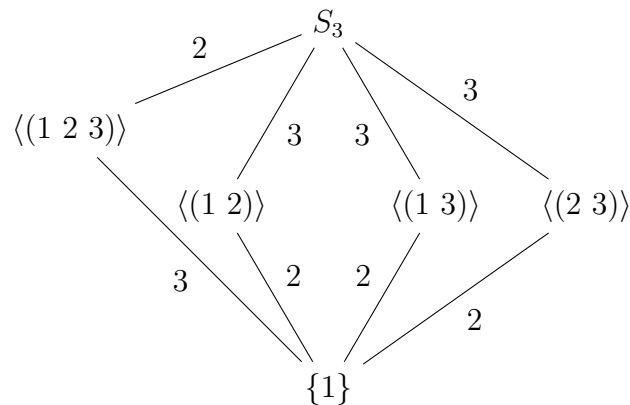
$$Q_2, \langle i \rangle, \langle j \rangle, \langle k \rangle, \langle -1 \rangle, \{1\}$$



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. En general, si consideramos dos grupos isomorfos, obtendremos dos diagramas de Hasse que serán grafos isomorfos entre sí. Sin embargo, el recíproco no es cierto, si tenemos dos diagramas de Hasse que sean grafos isomorfos, los grupos de los que partían no tienen por qué ser isomorfos. En este ejemplo se pone de manifiesto, ya que G y H no son isomorfos (basta con observar que G es conmutativo y H no), pero veremos que tienen diagramas de Hasse isomorfos. 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. \square

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:

$$hk = (k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

\Longleftarrow) 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:

$$HK = H \vee K$$

- ⊆) Sea $x \in HK$, entonces $\exists h \in H, k \in K$ de forma que $x = hk \in \langle H \cup K \rangle = H \vee K$.
- ⊇) 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:

$$\begin{aligned} h &= h_1^{\delta_1} \dots h_p^{\delta_p} \in H \\ k &= k_{p+1}^{\delta_{p+1}} \dots k_n^{\delta_n} \in K \end{aligned}$$

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:

⁹Que denotaremos por ${}_H[x]$ y por $[x]_H$ respectivamente.

- 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 $x \sim_H x$ y $x_H \sim x$, 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 $x \sim_H z$.

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:

$$\begin{aligned} x_H \sim y &\iff y^{-1}x \in H \iff \exists h \in H \text{ con } y^{-1}x = h \iff \exists h \in H \text{ con } y^{-1} = hx^{-1} \\ &\iff \exists h \in H \text{ con } y = xh^{-1} \iff \exists h' \in H \text{ con } y = xh' \end{aligned}$$

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 $f : xH \rightarrow H$, $g : H \rightarrow Hx$ 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 $f : G/_H\sim \rightarrow G/\sim_H$ 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 $[S_3 : \langle(1\ 2)\rangle] = 3$, algo que comprobamos en el último ejemplo, donde tomábamos:

$$H = \langle(1\ 2)\rangle = \{1, (1\ 2)\}$$

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 \sim_H 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:

$$|G| = [G : H]|H|$$

□

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:

$$|G| = [G : H]|H| = [G : H][H : K]|K| \quad \left. \begin{array}{l} |G| = [G : K]|K| \\ |G| = [G : H]|H| \end{array} \right\} \implies [G : K] = [G : H][H : K]$$

□

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 $\langle a \rangle = G$. \square

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:

$$\varphi_a(n+m) = a^{n+m} = a^n a^m = \varphi_a(n) \varphi_a(m) \quad \forall n, m \in \mathbb{Z}$$

\square

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:

$$m \in \text{Div}(n) \quad \text{y} \quad H = \langle a^{\frac{n}{m}} \rangle$$

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 natural no nulo que cumplía esta propiedad (y $r < k$), por lo que $s = kq$ y:

$$b = (a^k)^q \in \langle a^k \rangle$$

Falta finalmente ver que $k = n/m$. Para ello, como $a^n = 1 \in H$ por ser H un grupo, tenemos que $k \leq n$ y si dividimos n entre k , $\exists q, r \in \mathbb{N}$ de forma que:

$$n = qk + r \quad 0 \leq r < k$$

De donde: $1 = a^n = a^{qk} a^r$, pero por ser $1 \in H$ y $a^{qk} \in H$, deducimos que $a^r \in H$ con $r < k$, luego ha de ser $r = 0$ (ya que si no entraría en contradicción con la definición de k), por lo que $k \mid n$. De aquí deducimos que:

$$m = |H| = O(a^k) \stackrel{(*)}{=} \frac{n}{k} \implies k = \frac{n}{m}$$

Donde en $(*)$ hemos usado que $O(a^k) = \frac{n}{k}$, ya que:

■ En primer lugar:

$$(a^k)^{\frac{n}{k}} = a^n = 1$$

■ Si $t \in \mathbb{N}$ de forma que:

$$(a^k)^t = 1 = a^n$$

Como $O(a) = n$, por la Proposición 1.8, tenemos que $n \mid kt$, luego existe s de forma que:

$$ns = kt \implies \frac{n}{k}s = t$$

Por lo que $\frac{n}{k} \mid t$.

Lo que nos dice que $O(a^k) = \frac{n}{k}$. □

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:

$$\text{Div}(12) = \{1, 2, 3, 4, 6, 12\}$$

Y usando nuestra aplicación ϕ , podemos listar todos los subgrupos de C_{12} :

$$\begin{aligned} 1 &\xrightarrow{\phi} \langle x^{\frac{12}{1}} \rangle = \langle x^{12} \rangle = \langle 1 \rangle = \{1\} \\ 2 &\mapsto \langle x^{\frac{12}{2}} \rangle = \langle x^6 \rangle = \{1, x^6\} \\ 3 &\mapsto \langle x^{\frac{12}{3}} \rangle = \langle x^4 \rangle = \{1, x^4, x^8\} \\ 4 &\mapsto \langle x^{\frac{12}{4}} \rangle = \langle x^3 \rangle = \{1, x^3, x^6, x^9\} \\ 6 &\mapsto \langle x^{\frac{12}{6}} \rangle = \langle x^2 \rangle = \{1, x^2, x^4, x^6, x^8, x^{10}\} \\ 12 &\mapsto \langle x^{\frac{12}{12}} \rangle = \langle x \rangle = C_{12} \end{aligned}$$

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 $a^k = a^{dt} \in \langle a^d \rangle$.

⊇) Como $d = \text{mcd}(n, k)$, entonces la ecuación:

$$nX + kY = d$$

tiene solución¹⁰, por lo que existen $u, v \in \mathbb{N}$ de forma que $nu + kv = d$, luego:

$$a^d = a^{nu} a^{kv} = \cancel{(a^n)^u}^1 (a^k)^v \in \langle a^k \rangle$$

Para ver que $O(a^k) = n/d$, 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 $O(a^k) = O(a^d) = n/d$. □

Ejemplo. Por ejemplo, ¿por qué en \mathbb{Z}_{12} el subgrupo generado por el 8 coincide con el generado por el 4? Porque $4 = \text{mcd}(8, 12)$.

Corolario 2.18.1. Sea G un grupo y $a \in G$ con $O(a) = n$, entonces:

$$\langle a^p \rangle = \langle a^q \rangle \iff \text{mcd}(n, p) = \text{mcd}(n, q)$$

Demostración. Veamos la doble implicación:

\Leftarrow) Si $\text{mcd}(n, p) = d = \text{mcd}(n, q)$, entonces (por la Proposición anterior):

$$\langle a^p \rangle = \langle a^d \rangle = \langle a^q \rangle$$

\Rightarrow) Si $\langle a^p \rangle = \langle a^q \rangle$, entonces (por la Proposición anterior):

$$\frac{n}{\text{mcd}(n, p)} = O(a^p) = O(a^q) = \frac{n}{\text{mcd}(n, q)} \implies \text{mcd}(n, p) = \text{mcd}(n, q)$$

□

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:

$$\varphi(n) = |\{m \in \mathbb{N} \mid 1 \leq m \leq n \wedge \text{mcd}(n, m) = 1\}|$$

Demostración. Basta usar el Corolario anterior:

$$G = \langle a \rangle = \langle a^k \rangle \iff 1 = \text{mcd}(n, 1) = \text{mcd}(n, k)$$

□

Ejemplo. En \mathbb{Z}_{12} :

$$\mathbb{Z}_{12} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$$

¹⁰Se vió en Álgebra I, se trata de la Identidad de Bezout.

3. Grupos cocientes y Teoremas de isomorfía

Este tema se centrará en las relaciones de equivalencia $_H\sim$ y \sim_H definidas en el capítulo anterior, donde ya vimos propiedades de estas relaciones (recordamos la Proposición 2.12), como que $G/_H\sim$ y G/\sim_H eran biyectivos o el Teorema de Lagrange. Estaremos especialmente interesados en el caso en el que los conjuntos cocientes de estas dos relaciones de equivalencia coincidan, propiedad que nos dará los Teoremas de Isomorfía, que son el principal objeto de estudio de este tema.

3.1. Subgrupos normales

Definición 3.1 (Subgrupos normales). Sea G un grupo y $H < G$, diremos que H es un subgrupo normal de G , denotado por $H \triangleleft G$, si las clases laterales de cada elemento coinciden, es decir, si:

$$xH = Hx \quad \forall x \in G$$

En cuyo caso, tendremos que $G/_H\sim = G/\sim_H$, y notaremos a este conjunto como G/H , al que llamaremos conjunto de las clases laterales de H en G .

Definición 3.2 (Conjugado). Sea G un grupo, $H \subseteq G$ y $x \in G$, definimos el conjugado de H por x como el conjunto:

$$xHx^{-1} = \{xhx^{-1} \mid h \in H\}$$

Proposición 3.1. Sea G un grupo, $H < G$ y $x \in G$, entonces $xHx^{-1} < G$.

Demostración. Para ello, sean $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$, entonces:

$$xh_1x^{-1}(xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2^{-1}x^{-1} = xh_1h_2^{-1}x^{-1} \in xHx^{-1}$$

Ya que como H es un subgrupo de G , entonces $h_1h_2^{-1} \in H$. □

Buscamos ahora formas cómodas de detectar cuándo un subgrupo de un grupo es normal o no, ya que es tedioso comprobar la igualdad $xH = Hx$ para todo elemento x del grupo que estemos considerando en cada caso.

Proposición 3.2 (Caracterización de subgrupos normales).

Sea G un grupo y $H < G$, son equivalentes:

$$i) \ H \triangleleft G.$$

$$ii) \ xhx^{-1} \in H \ \forall x \in G, \forall h \in H.$$

$$iii) \ xHx^{-1} \subseteq H \ \forall x \in G.$$

$$iv) \ xHx^{-1} = H \ \forall x \in G.$$

Demostración. Veamos todas las implicaciones:

$i) \implies ii)$ Sean $x \in G$ y $h \in H$, entonces $xh \in xH = Hx$ por ser $H \triangleleft G$, lo que nos dice que $\exists h' \in H$ de forma que $xh = h'x$ y multiplicando por x^{-1} a la derecha, llegamos a que:

$$xhx^{-1} = h' \in H$$

$ii) \iff iii)$ Es claro.

$iii) \implies iv)$ Sea $h \in H$ y dado $x \in G$, en particular tendremos que $x^{-1} \in G$, por lo que usando la hipótesis, tenemos que $x^{-1}hx \in x^{-1}Hx \subseteq H$, por lo que $x^{-1}hx \in H$ y tendremos que:

$$xx^{-1}hxx^{-1} = h \in xHx^{-1}$$

$iv) \implies i)$ Fijado $x \in G$, veamos que $xH = Hx$:

\subseteq) Si $xh \in xH$, entonces tendremos que:

$$xhx^{-1} \in xHx^{-1} = H$$

Con lo que existirá $h' \in H$ de forma que $xhx^{-1} = h'$. Si multiplicamos por x a la derecha, obtenemos que:

$$xh = h'x \in Hx$$

\supseteq) Para la otra inclusión, si $hx \in Hx$, tendremos que:

$$x^{-1}hx \in x^{-1}Hx = H$$

Por lo que existirá $h' \in H$ de forma que $x^{-1}hx = h'$. Si multiplicamos por x a la izquierda:

$$hx = xh' \in xH$$

□

Comprobar que $xhx^{-1} \in H$ para todo $x \in G$ y para todo $h \in H$ puede ser una labor tediosa, por lo que presentamos la siguiente Proposición, que puede resultar de utilidad a la hora de comprobar si un subgrupo H de un grupo G es normal o no.

Proposición 3.3. Sea G un grupo, $H < G$ y $S \subseteq G$ de forma que $G = \langle S \rangle$, entonces:

$$xhx^{-1} \in H \ \forall x \in G, \forall h \in H \iff shs^{-1} \in H \ \forall s \in S \cup S^{-1}, \forall h \in H$$

Donde $S^{-1} = \{x \in G \mid x^{-1} \in S\}$. Es decir, basta comprobar la condición con los generadores de G y con los inversos de los generadores de G .

Demostración. Veamos las dos implicaciones:

\implies) En particular, tenemos que $x \in S \cup S^{-1} \subseteq G$.

\impliedby) Sea $x \in G = \langle S \rangle$, entonces existirán $s_1, \dots, s_n \in S$ y $\gamma_1, \dots, \gamma_n \in \{\pm 1\}$ de forma que:

$$x = s_1^{\gamma_1} \dots s_n^{\gamma_n}$$

Por inducción sobre n :

■ Si $n = 1$: Entonces $x = s^\gamma$ con $s \in S$ y $\gamma \in \{\pm 1\}$. Distinguiamos casos:

• Si $\gamma = 1$, entonces:

$$xhx^{-1} = shs^{-1} \in H \quad \forall h \in H$$

• Si $\gamma = -1$, entonces:

$$xhx^{-1} = s^{-1}hs \in H \quad \forall h \in H$$

■ Supuesto para $m < n$, veámoslo para n :

$$xhx^{-1} = s_1^{\gamma_1} s_2^{\gamma_2} \dots s_n^{\gamma_n} h s_n^{-\gamma_n} \dots s_2^{-\gamma_2} s_1^{-\gamma_1}$$

Si cogemos $y = s_2^{\gamma_2} \dots s_n^{\gamma_n}$, por hipótesis de inducción tendremos que:

$$yhy^{-1} = s_2^{\gamma_2} \dots s_n^{\gamma_n} h s_n^{-\gamma_n} \dots s_2^{-\gamma_2} \in H$$

Por lo que:

$$xhx^{-1} = s_1^{\gamma_1} yhy^{-1} s_1^{-\gamma_1} \in H$$

□

Ejemplo. Hemos caracterizado ya a los grupos normales, pero veamos ejemplos de ellos:

1. Dado un grupo G , los dos subgrupos impropios de G siempre son subgrupos normales del mismo:

■ Para el caso $H = \{e\}$:

$$xex^{-1} = xx^{-1} = e \in \{e\} \quad \forall x \in G$$

Y por la Proposición anterior, tenemos que $\{e\} \triangleleft G$.

■ Para el caso $H = G$:

$$xhx^{-1} \in G \quad \forall x \in G, \forall h \in G$$

Y por la misma razón, también tenemos que $G \triangleleft G$.

2. En un grupo abeliano G , todos sus subgrupos son normales (sea $H < G$):

$$xH = \{xh \mid h \in H\} = \{hx \mid h \in H\} = Hx \quad \forall x \in G$$

3. Todo subgrupo de índice 2 es normal, es decir, si $H < G$ con $[G : H] = 2$, entonces $H \triangleleft G$.

Para verlo, si tomamos $x \in G \setminus H$, como $[G : H] = 2$, tenemos que:

$$H \cup xH = G = H \cup Hx$$

En ambos casos, como son particiones disjuntas, tenemos que $xH = Hx$ para todo $x \in G \setminus H$ (y si $x \in H$, entonces $xH = H = Hx$), con lo que $H \triangleleft G$.

4. En S_3 , si consideramos $H = \langle (1\ 2) \rangle$, H no es un subgrupo normal de S_3 , como se vio en el correspondiente ejemplo del tema anterior, y podemos volverlo a comprobar con la caracterización, ya que $(2\ 3) \in S_3$ y:

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

Igual les pasa a los subgrupos $\langle (2\ 3) \rangle$ y $\langle (1\ 3) \rangle$. Sea ahora $A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$, como $[S_3 : A_3] = 2$, tenemos que $A_3 \triangleleft S_3$:

$$S_3/A_3 = \{A_3, A_3(1\ 2)\} = \{A_3, (1\ 2)A_3\}$$

5. La relación de “ser un subgrupo normal de” no es transitiva, es decir, si G es un grupo con $\bar{K} < H < G$, $K \triangleleft H$ y $H \triangleleft G$, entonces no necesariamente se tiene que $K \triangleleft G$. La situación es la descrita en la Figura 3.1

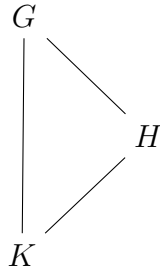
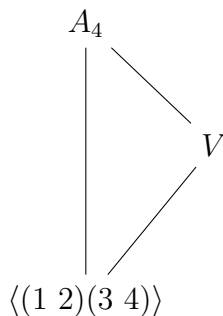


Figura 3.1: Situación descrita.

Por ejemplo, en A_4 consideramos el grupo de Klein V y $\langle (1\ 2)(3\ 4) \rangle$. Vamos a ver que $\langle (1\ 2)(3\ 4) \rangle \triangleleft V$ y que $V \triangleleft A_4$ pero no se cumple que $\langle (1\ 2)(3\ 4) \rangle \triangleleft A_4$:



- En primer lugar, $\langle (1\ 2)(3\ 4) \rangle \triangleleft V$, por ser $[V : \langle (1\ 2)(3\ 4) \rangle] = 2$.

- Veamos ahora que $V \triangleleft A_4$. Para ello, consideramos:

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

Por la Proposición 3.3, basta comprobar la caracterización para todos los generadores de $A_4 = \langle (1\ 2\ 3), (1\ 2\ 4) \rangle$:

$$\begin{aligned} (1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} &\in V \\ (1\ 2\ 3)(1\ 3)(2\ 4)(1\ 2\ 3)^{-1} &\in V \\ (1\ 2\ 3)(1\ 4)(2\ 3)(1\ 2\ 3)^{-1} &\in V \\ (1\ 2\ 3)1(1\ 2\ 3)^{-1} &\in V \\ (1\ 2\ 4)(1\ 2)(3\ 4)(1\ 2\ 4)^{-1} &\in V \\ (1\ 2\ 4)(1\ 3)(2\ 4)(1\ 2\ 4)^{-1} &\in V \\ (1\ 2\ 4)(1\ 4)(2\ 3)(1\ 2\ 4)^{-1} &\in V \\ (1\ 2\ 4)1(1\ 2\ 4)^{-1} &\in V \end{aligned}$$

- Veremos ahora que no se tiene que $\langle (1\ 2)(3\ 4) \rangle \triangleleft A_4$, ya que:

$$(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} = (1\ 4)(2\ 3) \notin A_4$$

Hemos visto ya que la relación \triangleleft no es en general transitiva. Sin embargo, de ella podemos deducir ciertas relaciones, como se pone de manifiesto en este Corolario:

Corolario 3.3.1. *Como corolario de la Proposición 3.2, si G es un grupo de forma que $A \subseteq B \subseteq G$ con $A \triangleleft G$ y $B < G$, entonces $A \triangleleft B$.*

Demostración. Por la Proposición 3.2, tendremos que $axa^{-1} \in A$ para todo $x \in G$ y $a \in A$. Sea $b \in B$, como en particular $b \in G$, también se cumplirá:

$$bab^{-1} \in A \quad \forall b \in B, a \in A$$

Concluimos que $A \triangleleft B$. □

Definición 3.3 (Centro). Sea G un grupo, definimos el centro de G como el conjunto de los elementos de G que conmutan con todos los demás, es decir, el conjunto:

$$Z(G) = \{a \in G \mid ax = xa, \forall x \in G\}$$

Podemos entender $Z(G)$ como “la parte abeliana del grupo” G .

Proposición 3.4. *Sea G un grupo, se verifica:*

- i) $Z(G) < G$.
- ii) $Z(G) \triangleleft G$.
- iii) Si G es abeliano, entonces $Z(G) = G$.

Demostración. Demostramos las propiedades:

i) Sean $a, b \in Z(G)$ y dado $x \in G$, entonces:

$$(ab^{-1})x = a(b^{-1}x) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1}) = (ax)b = (xa)b = x(ab^{-1})$$

Por lo que $ab^{-1} \in Z(G)$, lo que nos dice que $Z(G)$ es un subgrupo de G .

ii) Sea $x \in G$, entonces:

$$xZ(G) = \{xz \mid z \in Z(G)\} = \{zx \mid z \in Z(G)\} = Z(G)x$$

iii) Es evidente. □

Ejemplo. Ejemplos interesantes:

- Veamos que $Z(S_n) = 1$ cuando $n \geq 3$. Para ello, supongamos que $n \geq 3$ y consideremos $1 \neq \sigma \in S_n$, con lo que existirán $i, j \in \{1, \dots, n\}$ con $i \neq j$ de forma que $\sigma(i) = j$.

En dicho caso, $\exists k \in \{1, \dots, n\} \setminus \{i, j\}$ ($n \geq 3$). Si consideramos $\tau = (j \ k)$:

$$\left. \begin{array}{l} \sigma\tau(i) = \sigma(i) = j \\ \tau\sigma(i) = \tau(j) = k \end{array} \right\} \implies \sigma\tau \neq \tau\sigma$$

Por tanto, $\sigma \notin Z(S_n)$, para todo $\sigma \in S_n \setminus \{1\}$.

- Veamos que que $Z(A_n) = 1$ cuando $n \geq 4$. Para $n \geq 4$, $\exists i, j \in \{1, \dots, n\}$ con $i \neq j$ de forma que $\sigma(i) = j$, con lo que podemos encontrar $k, l \in \{1, \dots, n\}$, distintos entre sí y distintos de i y j . Consideramos:

$$\tau = (j \ k \ l) \in A_4$$

Y tenemos de la misma forma que:

$$\left. \begin{array}{l} \sigma\tau(i) = k \\ \tau\sigma(i) = j \end{array} \right\} \implies Z(A_n) = \{1\}$$

Proposición 3.5. Sea G un grupo, $H < G$, entonces, equivalen:

i) $H \triangleleft G$.

ii) $\forall x, y \in G$ con $xy \in H$, entonces $yx \in H$

Demostración. Veamos las dos implicaciones:

$i) \implies ii)$ Sean $x, y \in G$ con $xy \in H$, entonces $\exists h \in H$ de forma que $xy = h$, de donde $y = x^{-1}h \in x^{-1}H = Hx^{-1}$, por lo que $\exists h' \in H$ con $y = h'x^{-1}$ y multiplicando a la derecha por x , llegamos a que $yx = h' \in H$.

$ii) \implies i)$ Sean $x \in G$ y $h \in H$, tenemos que:

$$h = x^{-1}(xh) \in H$$

De donde deducimos por hipótesis que $(xh)x^{-1} \in H$, lo que nos dice que $H \triangleleft G$. □

3.2. Grupo cociente

Mostraremos ahora la propiedad que más nos interesa de los grupos normales: dotan al conjunto cociente de estructura de grupo.

Teorema 3.6. *Sea G un grupo y $H \triangleleft G$, entonces en el conjunto G/H podemos definir una operación binaria $G/H \times G/H \rightarrow G/H$ que dota a G/H de estructura de grupo, de modo que la proyección canónica $p : G \rightarrow G/H$ sea un homomorfismo de grupos. De esta forma, llamaremos a G/H grupo cociente.*

Demostración. Definimos la operación binaria $\cdot : G/H \times G/H \rightarrow G/H$ dada por:

$$xH \cdot yH = xyH \quad \forall xH, yH \in G/H$$

A esta operación la denotaremos a partir de ahora por yuxtaposición.

- En primer lugar, comprobemos que está bien definida, es decir, si $xH = x'H$ y $yH = y'H$, entonces $xyH = x'y'H$. Para ello:

$$\left. \begin{array}{l} xH = x'H \\ yH = y'H \end{array} \right\} \implies \left\{ \begin{array}{l} \exists h_1, h_2 \in H \\ x' = xh_1 \\ y' = yh_2 \end{array} \right.$$

Vemos ahora que dado $h \in H$:

\supseteq)

$$x'y'h = xh_1yh_2h \stackrel{(*)}{=} xyh'_1h_2h \in xyH$$

Donde en $(*)$ hemos usado que $H \triangleleft G$, por lo que $Hy = yH$ y podemos encontrar un h'_1 de forma que $h_1y = yh'_1$. Tenemos $x'y'H \subseteq xyH$.

\subseteq)

$$xyh = x'h_1^{-1}y'h_2^{-1}h \stackrel{(*)}{=} x'y'h''_1h_2^{-1}h \in x'y'H$$

Donde en $(*)$ hemos usado una idea similar a la anterior, lo que nos da la otra inclusión.

- Que la operación es asociativa es claro, ya que la operación de G era asociativa.
- El elemento neutro de la operación es $1H = H$.
- Fijado un elemento $xH \in G/H$, tendremos que $(xH)^{-1} = x^{-1}H$.

Concluimos que G/H es un grupo.

Ahora, consideramos la proyección canónica $p : G \rightarrow G/H$, que viene definida por $p(x) = xH$ para todo $x \in G$. Gracias a la definición de la operación de G/H , tenemos que:

$$p(xy) = xyH = xHyH = p(x)p(y) \quad \forall x, y \in G$$

Lo que demuestra que p es un homomorfismo de grupos. \square

Notemos la importancia de considerar en el teorema anterior H como subgrupo normal de G , ya que es lo que nos ha permitido comprobar que la operación de G/H estaba bien definida. Como propiedades a destacar del grupo cociente G/H :

- Sabemos por el capítulo anterior que el orden del grupo G/H es (si G es finito):

$$|G/H| = [G : H] = \frac{|G|}{|H|}$$

- Además, si $p : G \rightarrow G/H$ es la proyección al cociente, tenemos que:

$$\ker(p) = \{x \in G \mid p(x) = H\} = \{x \in G \mid xH = H\} = \{x \in H\} = H$$

Ejemplo. Algunas consecuencias de que G/H sea un grupo:

1. En S_3 , si consideramos $A_3 = \{1, (1\ 2\ 3), (1\ 3\ 2)\} \triangleleft S_3$, tenemos que:

$$S_3/A_3 = \{A_3, (1\ 2)A_3\}$$

Que por ser un grupo de orden 2, ya sabemos por el capítulo anterior que ha de ser $S_3/A_3 \cong \mathbb{Z}_2$.

2. Si consideramos $H < \mathbb{Z}$, entonces $H \triangleleft \mathbb{Z}$, ya que \mathbb{Z} es abeliano. Además, sabemos que $\exists n \in \mathbb{Z}$ de forma que $H = n\mathbb{Z}$. De esta forma, tendremos que:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

Por lo que el grupo cociente de \mathbb{Z} bajo cualquier subgrupo normal suyo ya era conocido para nosotros, puesto que todos ellos son de la forma \mathbb{Z}_n , para cierto $n \in \mathbb{N}$.

3. Veamos otra vez que A_4 no tiene subgrupos de orden 6. Si $H < A_4$ con $|H| = 6$, entonces:

$$[A_4 : H] = \frac{|A_4|}{|H|} = 2$$

Por tanto, $H \triangleleft A_4$. De esta forma, $A_4/H \cong \mathbb{Z}_2$, por ser el único grupo de orden 2. Si el cociente es isomorfo con \mathbb{Z}_2 y consideramos $xH \in A_4/H$, entonces:

$$(xH)^2 = x^2H = H \quad \forall x \in A_4$$

Por tanto, los cuadrados de los 8 3-ciclos de A_4 pertenecerían a H , de donde $|H| \geq 8$, contradicción.

Proposición 3.7. Sea G un grupo y $H < G$, entonces: $H \triangleleft G$ si y solo si existe un homomorfismo de grupos $f : G \rightarrow G'$ de forma que $\ker(f) = H$.

Demostración. Veamos las dos implicaciones:

\implies) Si $H \triangleleft G$, entonces la proyección canónica $p : G \rightarrow G/H$ es un homomorfismo de grupos de forma que $\ker(p) = H$, gracias al Teorema 3.6.

\impliedby) Supongamos ahora que existe un homomorfismo $f : G \rightarrow G'$ de grupos de forma que $\ker(f) = H$, sabemos ya que $H < G$ por ser $H = f^*(\{1\})$. Sean $x \in G$ y $h \in H$, tenemos que:

$$f(xhx^{-1}) = f(x)f(h)(f(x))^{-1} = f(x)(f(x))^{-1} = 1$$

De donde deducimos que $xhx^{-1} \in \ker(f) = H$, lo que nos dice que $H \triangleleft G$. \square

Observación. De esta forma, dado un homomorfismo de grupos $f : G \rightarrow G'$, tendremos siempre que $\ker(f) \triangleleft G$, ya que por ser $\{1\} < G'$ un subgrupo, tendremos que $\ker(f) = f^*(\{1\}) < G$ y por la Proposición 3.7, automáticamente tenemos que $\ker(f) \triangleleft G$.

Teorema 3.8 (Propiedad universal del grupo cociente). *Sea G un grupo, $H \triangleleft G$, $p : G \rightarrow G/H$ la proyección canónica al cociente, entonces para cualquier homomorfismo $f : G \rightarrow G'$ tal que $H \subseteq \ker(f)$, existe un único homomorfismo de grupos $\varphi : G/H \rightarrow G'$ de forma que $\varphi \circ p = f$.*

Más aún, tendremos que:

$$\begin{aligned} f \text{ sobreyectiva} &\iff \varphi \text{ sobreyectiva} \\ H = \ker(f) &\iff \varphi \text{ inyectiva} \end{aligned}$$

La situación descrita podemos observarla en la Figura 3.2. Este resultado nos dice que el diagrama conmuta.

Demostración. Definimos $\varphi : G/H \rightarrow G'$ de la forma más natural posible:

$$\varphi(xH) = f(x) \quad \forall xH \in G/H$$

- En primer lugar, veamos que está bien definida. Para ello, sean $x, y \in G$ de forma que $xH = yH$, entonces $y^{-1}x \in H \subseteq \ker(f)$, de donde:

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

- Veamos ahora que φ es un homomorfismo:

$$\varphi(xHyH) = \varphi(xyH) = f(xy) = f(x)f(y) = \varphi(xH)\varphi(yH) \quad \forall x, y \in G$$

- Veamos que $\varphi \circ p = f$:

$$(\varphi \circ p)(x) = \varphi(p(x)) = \varphi(xH) = f(x) \quad \forall x \in G$$

- Para la unicidad, supongamos que existe otra función $\psi : G/H \rightarrow G'$ de forma que $\psi \circ p = f$. En cuyo caso:

$$\psi(xH) = \psi(p(x)) = (\psi \circ p)(x) = f(x) = \varphi(xH) \quad \forall xH \in G/H$$

Por lo que $\psi = \varphi$.

Veamos la relación entre la sobreyectividad de f y φ :

$$f \text{ sobreyectiva} \iff \varphi \text{ sobreyectiva}$$

\Leftarrow) Como $f = \varphi \circ p$ y la composición de aplicaciones sobreyectivas es sobreyectiva, concluimos que f será sobreyectiva.

\implies) Supongamos que f es sobreyectiva y sea $y \in G'$, por lo que $\exists x \in G$ de forma que $f(x) = y$, pero:

$$y = f(x) = \varphi(p(x)) = \varphi(xH)$$

Concluimos que φ es sobreyectiva.

Veamos ahora la relación de inyectividad:

$$H = \ker(f) \iff \varphi \text{ inyectiva}$$

\implies) Si $H = \ker(f)$ y $\varphi(xH) = 1$, entonces:

$$1 = \varphi(xH) = f(x) \implies x \in \ker(f) = H$$

Con lo que $xH = H$, lo que nos dice que φ es inyectiva¹ ($\ker(\varphi) = \{H\}$).

\Leftarrow) Vamos a ver que $\ker(f) \subseteq H$, ya que conocemos $H \subseteq \ker(f)$ por hipótesis. Para ello, sea $x \in \ker(f)$, entonces:

$$1 = f(x) = \varphi(p(x)) = \varphi(xH) \implies xH \in \ker(\varphi)$$

Pero como φ es inyectiva, tenemos que $\ker(\varphi) = \{H\}$, con lo que $xH = H$, de donde $x \in H$.

□

La idea que subyace y que debemos entender de la propiedad universal del grupo cociente es la siguiente: G/H es la mejor forma de “colapsar H al elemento neutro sin perder las propiedades de grupo”. Como ya vimos en el Teorema 3.6, en el que definimos al grupo cociente y donde vimos que la proyección canónica era un homomorfismo, resulta que en el grupo cociente, H es el elemento neutro de la operación, por lo que hemos conseguido colapsar H al elemento neutro.

Ahora, la propiedad universal del grupo cociente nos dice que si tenemos cualquier homomorfismo de grupos que “mata a H ” (es decir, lo envía al núcleo del homomorfismo), entonces necesariamente ese homomorfismo ha de pasar por G/H , es decir, que existirá un único homomorfismo $\varphi : G/H \rightarrow G'$ que haga que el diagrama siguiente conmute. Cualquier homomorfismo que “mate a H ” podremos factorizarlo pasando por el grupo cociente, luego este grupo ha de ser el que mejor colapsa a H .

$$\begin{array}{ccc} G & \xrightarrow{p} & G/H \\ & \searrow f & \downarrow \varphi \\ & & G' \end{array}$$

Figura 3.2: Situación del Teorema 3.8.

¹Ya que H es el elemento neutro en G/H .

3.3. Teoremas de isomorfía

Teorema 3.9 (Primer Teorema de Isomorfía para grupos). *Sea $f : G \rightarrow G'$ un homomorfismo de grupos, entonces existe un isomorfismo de grupos de forma que*

$$G/\ker(f) \cong \text{Im}f$$

Y vendrá definido por $x\ker(f) \mapsto f(x)$.

Demostración. En primer lugar, por un resultado de la Proposición 3.7, tenemos que $\ker(f) \triangleleft G$. De esta forma, podemos considerar la proyección canónica al cociente $p : G \rightarrow G/\ker(f)$. Consideramos ahora la restricción del codominio de f a su imagen, lo que nos da un epimorfismo. Por la propiedad universal del grupo cociente, tenemos que existe un único homomorfismo $\varphi : G/\ker(f) \rightarrow \text{Im}(f)$ que hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} G & \xrightarrow{p} & G/\ker(f) \\ & \searrow f & \downarrow \varphi \\ & & \text{Im}(f) \end{array}$$

Finalmente, aplicando el Teorema 3.8:

- φ es sobreyectiva debido a que la restricción de f en codominio a su imagen es sobreyectiva.
- φ es inyectiva ya que el grupo normal que consideramos para hacer el cociente es $\ker(f)$. □

Ejemplo. Como consecuencia del primer teorema de isomorfía: consideramos \mathbb{K} , un cuerpo finito con $|\mathbb{K}| = q$ elementos. La aplicación $\det : \text{GL}_n(\mathbb{K}) \rightarrow \mathbb{K}^*$ es un homomorfismo de grupos y tenemos que:

$$\ker(\det) = \text{SL}_n(\mathbb{K})$$

Con lo que $\text{GL}_n(\mathbb{K})/\text{SL}_n(\mathbb{K}) \cong \text{Im}(\det) = \mathbb{K}^*$. Usémoslo para calcular $|\text{SL}_n(\mathbb{K})|$, ya que la isomorfía recién encontrada nos dice que:

$$|\mathbb{K}^*| = |\text{GL}_n(\mathbb{K})/\text{SL}_n(\mathbb{K})| = \frac{|\text{GL}_n(\mathbb{K})|}{|\text{SL}_n(\mathbb{K})|} \implies |\text{SL}_n(\mathbb{K})| = \frac{|\text{GL}_n(\mathbb{K})|}{|\mathbb{K}^*|} = \frac{|\text{GL}_n(\mathbb{K})|}{q-1}$$

Teorema 3.10 (Segundo Teorema de Isomorfía para grupos). *Sea G un grupo, $H, K < G$ de forma que $K \triangleleft G$, entonces:*

$$H \cap K \triangleleft H$$

Y existe un isomorfismo de grupos de forma que

$$H/H \cap K \cong HK/K$$

La situación descrita podemos observarla en la Figura 3.3.

Demostración. En primer lugar, justifiquemos de forma breve que el grupo de la derecha del isomorfismo tiene todo el sentido, es decir, que HK es efectivamente un grupo (no lo sabemos a priori) y que $K \triangleleft HK$. Para ello:

- Para ver que HK es un grupo (un subgrupo de G), como vimos en la Proposición 2.10, hemos de ver que $HK = KH$. Para ello, como $K \triangleleft G$, tenemos que:

$$xK = Kx \quad \forall x \in G$$

En particular, para $x \in H$, por lo que $HK = KH$.

- Como tenemos que $K < HK < G$ con $K \triangleleft G$, tendremos que $K \triangleleft HK$.

Consideramos ahora el homomorfismo resultante de componer la inclusión de H en G con la proyección al cociente G/K :

$$\begin{aligned} H &\xrightarrow{i} G \xrightarrow{p} G/K \\ x &\longmapsto x \longmapsto xK \end{aligned}$$

Si calculamos ahora la imagen y el núcleo de este homomorfismo:

$$\begin{aligned} \text{Im}(p \circ i) &= \{(p \circ i)(h) \mid h \in H\} = \{p(h) \mid h \in H\} = \{hK \mid h \in H\} \stackrel{(*)}{=} HK/K \\ \ker(p \circ i) &= \{h \in H \mid hK = (p \circ i)(h) = K\} = \{h \in H \mid h \in K\} = H \cap K \end{aligned}$$

Como $H \cap K = \ker(p \circ i)$, tenemos por la Proposición 3.7 que $H \cap K \triangleleft H$. Si aplicamos el Primer Teorema de Isomorfía al homomorfismo $p \circ i$, llegamos a que:

$$\frac{H}{H \cap K} = \frac{H}{\ker(p \circ i)} \cong \text{Im}(p \circ i) = HK/K$$

La igualdad $(*)$ anterior puede parecer rara, pero es muy natural, veamos que:

$$\{hK \mid h \in H\} = HK/K$$

\subseteq) Dado $h \in H$, en particular tendremos que $h = h \cdot 1 \in HK$, con lo que $hK \in HK/K$.

\supseteq) Sea $hkK \in HK/K$ para ciertos $h \in H$, $k \in K$, por la definición del producto en el grupo cociente tenemos:

$$hkK = (hK)(kK) = (hK)K = hK \in \{hK \mid h \in H\}$$

□

El Segundo Teorema de Isomorfía para grupos puede recordarse fácilmente observando la siguiente figura, donde pensamos en que $HK/K \cong H/H \cap K$ bajo las hipótesis del Teorema, que podemos recordar observando las diagonales del paralelogramo:



Figura 3.3: Situación del Teorema 3.10.

Ejemplo. Sea $H < S_n$ un subgrupo conteniendo una permutación impar, entonces $[H : H \cap A_n] = 2$. Es decir, H tiene el mismo número de permutaciones pares que de impares.

Para verlo, sabemos que $[S_n : A_n] = 2$, luego $A_n \triangleleft S_n$ y además, como H tiene una permutación impar, tenemos que $H \not\subseteq A_n$, por lo que tenemos:

$$HA_n = S_n$$

Que se puede deducir observando el retículo de subgrupos de S_n . Por el Segundo Teorema de Isomorfía, tenemos que:

$$H/H \cap A_n \cong S_n/A_n \cong \mathbb{Z}_2$$

Teorema 3.11 (Tercer Teorema de Isomorfía para grupos, o del doble cociente). Sea G un grupo, $N \triangleleft G$, entonces existe una biyección entre los subgrupos de G que contienen a N y los subgrupos de G/N , dada por $H \mapsto H/N$.

Además, $H \triangleleft G \iff H/N \triangleleft G/N$. En este caso:

$$\frac{G/N}{H/N} \cong G/H$$

Demostración. Si consideramos la proyección al cociente $p : G \rightarrow G/N$ dada por $p(x) = xN$ para todo $x \in G$, consideramos las aplicaciones imagen directa e imagen inversa por p , dadas por:

$$\begin{aligned} p_* : \mathcal{P}(G) &\rightarrow \mathcal{P}(G/N) \\ p^* : \mathcal{P}(G/N) &\rightarrow \mathcal{P}(G) \\ p_*(H) &= \{p(h) \mid h \in H\} \subseteq G/N \\ p^*(J) &= \{x \in G \mid p(x) \in J\} \subseteq G \end{aligned}$$

Que podemos restringirlas en dominio y codominio a los conjuntos:

$$\begin{aligned} \mathcal{A} &= \{H < G \mid N \subseteq H\} \\ \mathcal{B} &= \{J < G/N\} \end{aligned}$$

Obteniendo aplicaciones (que nombramos igual ya que nos olvidamos de las otras):

$$\begin{aligned} p_* : \mathcal{A} &\rightarrow \mathcal{B} \\ p^* : \mathcal{B} &\rightarrow \mathcal{A} \end{aligned}$$

Veamos que estas aplicaciones están bien definidas (es decir, que podemos poner \mathcal{B} como codominio de p_* y \mathcal{A} como codominio de p^*):

- Para p_* , hemos de observar primero que si cogemos $H \in \mathcal{A}$, entonces tendremos por el Corolario 3.3.1 que $N \triangleleft H$. En segundo lugar, ya vimos en la Proposición 2.3 que si $H < G$ entonces $p_*(H) < G/N$, por lo que la aplicación p_* está bien definida. Vemos lo que pasa cuando la aplicamos a un elemento de \mathcal{A} :

$$p_*(H) = \{p(h) \mid h \in H\} = \{hN \mid h \in H\} = H/N < G/N$$

- Para p^* , vimos también en la Proposición 2.3 que si $J < G/N$ (es decir, $J \in \mathcal{B}$), entonces $p^*(J) < G$. Veamos que $N \subseteq p^*(J)$. Para ello, vemos que:

$$p(n) = nN = N \in J \quad \forall n \in N$$

Donde $N \in J$ por ser N el elemento neutro para el grupo G/N y ser $J < G/N$. En conclusión, $n \in p^*(J) \forall n \in N$, y concluimos que p^* está bien definida.

Veamos ahora qué sucede con la composición de las aplicaciones:

- Por una parte, dado $J \in \mathcal{B}$:

$$(p_* \circ p^*)(J) = p_*(\{x \in G \mid p(x) \in J\}) \stackrel{(*)}{=} J$$

Donde en $(*)$ hemos aplicado que p es sobreyectiva, por lo que si tenemos $yN \in J$, existirá un $x \in G$ de forma que $p(x) = yN$, luego todos los valores de J se alcanzan.

- Dado $H \in \mathcal{A}$, veamos si $H = (p^* \circ p_*)(H)$:

\subseteq) Sea $h \in H$, tenemos que:

$$\{h\} = p^*(\{p(h)\}) = p^*(p_*(\{h\})) \subseteq p^*(p_*(H))$$

\supseteq) Sea $x \in p^*(p_*(H))$, entonces:

$$xN = p(x) \in p_*(H) = H/N = \{hN \mid h \in H\}$$

Por lo que $x \in H$.

Concluimos que $(p_*)^{-1} = p^*$, por lo que p_* es biyectiva y \mathcal{A} es biyectivo con \mathcal{B} .

Veamos ahora que:

$$H \triangleleft G \iff H/N \triangleleft G/N$$

\implies) Sean $xN \in G/N$, $hN \in H/N$:

$$xNhN(xN)^{-1} = xNhNx^{-1}N \stackrel{(*)}{=} xhx^{-1}N \stackrel{(**)}{\in} H/N$$

Donde en $(*)$ hemos aplicado la definición del producto en el cociente y en $(**)$ hemos aplicado que $H \triangleleft G$, con lo que $xhx^{-1} \in H$.

\impliedby) Ahora, sean $x \in G$ y $h \in H$:

$$xhx^{-1}N = xNhN(xN)^{-1} \in H/N$$

De donde concluimos que $xhx^{-1} \in H$, con lo que $H \triangleleft G$.

Finalmente, en este caso veamos que $\frac{G/N}{H/N} \cong G/H$. Para ello, consideramos las proyecciones $p_N : G \rightarrow G/N$ y $p_H : G \rightarrow G/H$. Como $N \subseteq H = \ker(p_H)$, sabemos por la Propiedad Universal del grupo cociente (Teorema 3.8) que existe un único homomorfismo $\varphi : G/N \rightarrow G/H$ que hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} G & \xrightarrow{p_N} & G/N \\ & \searrow p_H & \downarrow \varphi \\ & & G/H \end{array}$$

Es decir, φ cumplirá que:

$$\varphi p_N = p_H$$

Si aplicamos ahora el Primer Teorema de Isomorfía sobre φ :

$$\frac{G/N}{\ker(\varphi)} \cong \text{Im}(\varphi)$$

Y basta observar que:

- Por ser p_H sobreyectiva (es una proyección), φ también será sobreyectiva, por lo que $\text{Im}(\varphi) = G/H$.
- Veamos que $\ker(\varphi) = H/N$:

\subseteq) Sea $xN \in \ker(\varphi)$, entonces:

$$H = \varphi(xN) = \varphi(p_N(x)) = p_H(x) = xH \implies x \in H$$

\supseteq) Sea $hN \in H/N$, entonces:

$$\varphi(hN) = \varphi(p_N(h)) = p_H(h) = hH = H$$

Por lo que $hN \in \ker(\varphi)$.

En definitiva, hemos probado que:

$$\frac{G/N}{H/N} \cong G/H$$

□

Ejemplo. Recordando el retículo de subgrupos de D_4 :

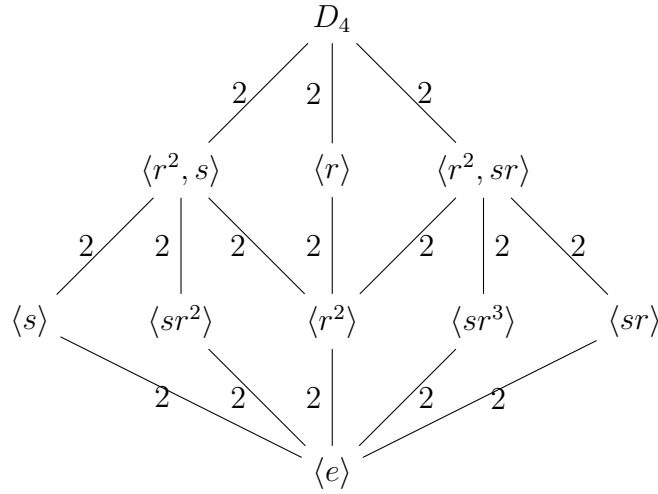


Figura 3.4: Diagrama de Hasse para los subgrupos de D_4 .

Si consideramos los 5 grupos del centro del diagrama y los dividimos entre $\langle r^2 \rangle$, llegamos a que el conjunto que contiene a estos es isomorfo al grupo de Klein:



Cuarto Teorema de Isomorfía

Antes de ver el Cuarto Teorema de Isomorfía, hemos de ver dos Lemas previos que nos ayudarán en su demostración:

Lema 3.12 (Ley modular o regla de Dedekind). *Sea G un grupo y $A, B, C < G$ con $A < C$, entonces:*

$$A(B \cap C) = AB \cap C$$

Demostración. Por doble implicación:

\subseteq) Sea $z \in A(B \cap C)$, entonces existen $a \in A$ y $x \in B \cap C$ de forma que $z = ax$, con lo que $ax \in AB$ y $ax \in AC = C$ por ser $A < C$, de donde deducimos que $z = ax \in AB \cap C$.

\supseteq) Sea $z \in AB \cap C$, entonces:

- Por una parte, como $z \in AB$, tenemos que $\exists a \in A$ y $b \in B$ de forma que $z = ab$.
- Además, como $z \in C$, tenemos que $z = ab \in C$

Por ser $A < C$, tenemos que $a \in C$, por lo que $a^{-1} \in C$, de donde:

$$b = a^{-1}z \in C$$

Como además teníamos $b \in B$, llegamos a que $z = ab \in A(B \cap C)$.

□

Observación. La hipótesis $A < C$ no es necesaria, basta con tener $A \subseteq C$.

Lema 3.13. Sea G un grupo y $A, B, C < G$ con $B \triangleleft A$, entonces:

- $B \cap C \triangleleft A \cap C$ y $A \cap C / B \cap C \cong B(A \cap C) / B$.
- Si además $C \triangleleft G$, entonces: $BC \triangleleft AC$ y $AC / BC \cong A / B(A \cap C)$



Demostración. Veamos los dos apartados:

- Aplicando el Segundo Teorema de Isomorfía sobre el diagrama (observamos el paralelogramo), tenemos el resultado de forma directa:

$$A \cap C / B \cap C \cong B(A \cap C) / B$$

- Ahora, si $C \triangleleft G$ (los elementos de G conmutan con los de C), tendremos que $BC = CB$ y $AC = CA$, por lo que $BC, AC < G$. Además, como $B < A$, también tendremos que $BC < AC$. Veamos que esta última relación es normal. Para ello, sean $bc \in BC$, $ax \in AC$:

$$axbc(ax)^{-1} = axbcx^{-1}a^{-1} = axa^{-1}aba^{-1}acx^{-1}a^{-1} = (axa^{-1})(aba^{-1})(acx^{-1}a^{-1})$$

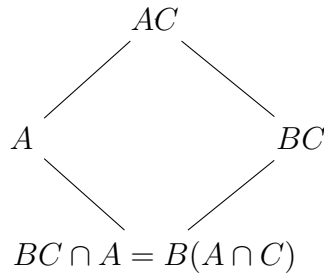
Para ver dónde está este último elemento:

- Como $x \in C$ y $C \triangleleft G$, $axa^{-1} \in C$.
- Como $b \in B$ y $B \triangleleft A$, $aba^{-1} \in B$.
- Como $c, x \in C$, tendremos $cx^{-1} \in C$ y por ser $C \triangleleft G$, $acx^{-1}a^{-1} \in C$.

En definitiva:

$$axbc(ax)^{-1} \in CBC = BCC = BC$$

De donde deducimos que $BC \triangleleft AC$. Ahora, si tenemos en mente el siguiente diagrama, podemos aplicar el Segundo Teorema de Isomorfía, ya que tenemos $A, BC < AC$ y $BC \triangleleft AC$.



El Segundo Teorema de Isomorfía nos dice que $B(C \cap A) \triangleleft A$, y que:

$$A/B(A \cap C) \cong AC/BC$$

□

Observación. Sin embargo, el Lema anterior se podría hacer también suponiendo solo que $A, B \subseteq G$ para A y B , solo es necesario suponer que $C < G$.

A continuación, veremos el Cuarto Teorema de Isomorfía, o Teorema de Zassenhaus, para el cual conviene pensar en la Figura 3.6 (aunque en esta figura el retículo de subgrupos está al revés de a lo que estamos acostumbrados: arriba los conjuntos de menor tamaño y debajo los conjuntos mayores).

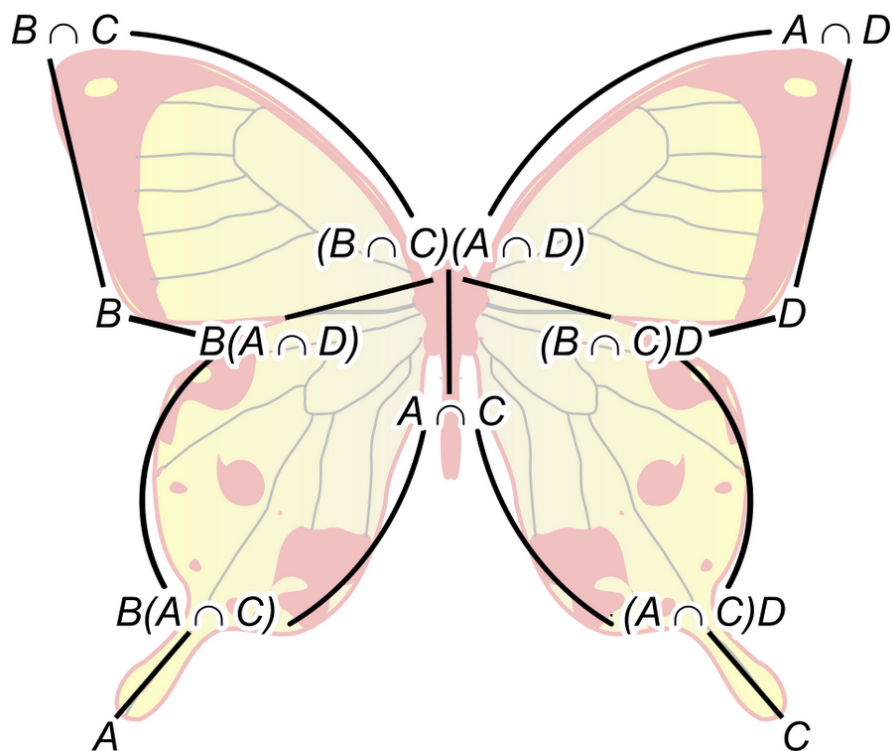


Figura 3.6: Situación del Teorema 3.14

Teorema 3.14 (Cuarto Teorema de Isomorfía para grupos). *Sea G un grupo y $A_1, C_1, A_2, C_2 < G$ y $C_1 \triangleleft A_1$, $C_2 \triangleleft A_2$, entonces:*

- i) $(A_1 \cap C_2)C_1 \triangleleft (A_1 \cap A_2)C_1$.
- ii) $(A_2 \cap C_1)C_2 \triangleleft (A_1 \cap A_2)C_2$.
- iii) $(A_1 \cap A_2)C_1 / (A_1 \cap C_2)C_1 \cong A_1 \cap A_2 / (A_1 \cap C_2)(A_2 \cap C_1) \cong (A_1 \cap A_2)C_2 / (A_2 \cap C_1)C_2$

Demostración. Veamos cada apartado:

- i) En primer lugar², como $C_1 \triangleleft A_1$, entonces los elementos de C_1 conmutarán con los de A_1 , luego:

$$\begin{aligned} (A_1 \cap C_2)C_1 &= C_1(A_1 \cap C_2) \\ (A_1 \cap A_2)C_1 &= C_1(A_1 \cap A_2) \end{aligned}$$

Por lo que ambos serán subgrupos de G . Además, como $C_2 < A_2$, tenemos ya que:

$$(A_1 \cap C_2)C_1 < (A_1 \cap A_2)C_1$$

Para ver la normalidad, sean $x \in (A_1 \cap A_2)C_1, y \in (A_1 \cap C_2)C_1$, entonces existirán elementos $a \in A_1 \cap A_2, b \in A_1 \cap C_2, c, c' \in C_1$ de forma que:

$$x = ac \quad y = bc'$$

²Esta demostración se hizo en clase de otra forma usando resultados previos. Si alguien hace esta demostración de forma más sencilla que se ponga en contacto con nosotros.

Si calculamos:

$$xyx^{-1} = acbc'c^{-1}a^{-1} = (aca^{-1})(aba^{-1})(ac'a^{-1})(ac^{-1}a^{-1})$$

Veamos dónde está este elemento:

- Como $c \in C_1$, $a \in A_1 \cap A_2$ y $C_1 \triangleleft A_1$, $aca^{-1} \in C_1$.
- Como $b \in A_1 \cap C_2 \subseteq C_2$ y $a \in A_1 \cap A_2 \subseteq A_2$ con $C_2 \triangleleft A_2$, entonces $aba^{-1} \in A_1 \cap C_2$.
- Como $c', c \in C_1$, $a \in A_1 \cap A_2$ y $C_1 \triangleleft A_1$, $ac'a^{-1}, ac^{-1}a^{-1} \in C_1$.

En definitiva:

$$xyx^{-1} \in C_1(A_1 \cap C_2)C_1C_1 = (A_1 \cap C_2)C_1C_1C_1 = (A_1 \cap C_2)C_1$$

Y concluimos que $(A_1 \cap C_2)C_1 \triangleleft (A_1 \cap A_2)C_1$.

ii) Es análogo, cambiando los papeles de C_1 y C_2 .

iii) Para el primer isomorfismo, si tomamos:

$$\begin{aligned} G_1 &= A_1 \\ A &= A_1 \cap A_2 \\ B &= A_1 \cap C_2 \\ C &= C_1 \end{aligned}$$

Nos encontramos en las Hipótesis del Lema 3.13, ya que $A, B, C < G_1$ y $B \triangleleft A$, por ser $C_2 \triangleleft A_2$. Como además $C \triangleleft G_1$ por hipótesis, concluimos que:

$$AC/BC \cong A/B(A \cap C)$$

Que en nuestro caso significa:

$$(A_1 \cap A_2)C_1 / (A_1 \cap C_2)C_1 \cong A_1 \cap A_2 / (A_1 \cap C_2)(A_1 \cap A_2 \cap C_1) = A_1 \cap A_2 / (A_1 \cap C_2)(A_2 \cap C_1)$$

Para el segundo, hemos de tomar:

$$\begin{aligned} G_2 &= A_2 \\ A &= A_1 \cap A_2 \\ B &= A_1 \cap C_2 \\ C &= C_2 \end{aligned}$$

□

3.4. Producto directo

En un ejemplo del Capítulo 1 vimos que dados dos grupos H y G podíamos definir de forma sencilla una operación en $H \times G$ en función de las operaciones de H y G , que nos dotaba a $H \times G$ de estructura de grupo. A este grupo lo llamábamos grupo directo de G y H , grupo que volveremos a definir a partir de ahora y en el que nos centraremos durante esta sección.

Definición 3.4 (Producto directo). Sean H y G dos grupos, definimos en el producto cartesiano $H \times G$ la operación

$$\begin{aligned} \cdot : (H \times G) \times (H \times G) &\longrightarrow H \times G \\ (h, k)(h', k') &\longmapsto (hh', kk') \end{aligned}$$

Se verifica que $H \times G$ junto con esta operación es un grupo:

- Es claro que la operación es asociativa, por ser las respectivas operaciones de H y G asociativas.
- El elemento $(1, 1) \in H \times G$ es el elemento neutro para la operación.
- Dado un elemento $(h, k) \in H \times G$, tenemos que:

$$(h, k)(h^{-1}, k^{-1}) = (hh^{-1}, kk^{-1}) = (1, 1)$$

Este grupo que hemos definido en $H \times G$ recibirá el nombre de producto directo de H y G .

Algunos autores llaman al producto directo que hemos definido producto directo externo, para diferenciarlo del producto directo interno, que luego definiremos. Sin embargo, nosotros lo llamaremos simplemente producto directo.

Proposición 3.15. Si H y K son dos grupos finitos, entonces:

- i) $|H \times K| = |H||K|$.
- ii) $O(h, k) = \text{mcm}(O(h), O(k)) \forall (h, k) \in H \times K$.

Demostración. Veamos las dos propiedades:

- i) Se vió en Álgebra I.
- ii) Como H y K son finitos, también lo será $H \times K$ y como ya vimos en la Proposición 1.9, los órdenes de los elementos son finitos, por lo que el enunciado tiene todo el sentido.

Llamando $m(h, k) = \text{mcm}(O(h), O(k))$, en primer lugar vemos que:

$$(h, k)^{m(h, k)} = (h^{m(h, k)}, k^{m(h, k)}) = (1, 1)$$

Donde en la primera igualdad hemos usado la definición del producto directo de H y K y en la segunda hemos usado que $O(h) \mid m(h, k)$ y que $O(k) \mid m(h, k)$.

Ahora, sea $t \in \mathbb{N} \setminus \{0\}$ de forma que $(h, k)^t = (1, 1)$, tenemos entonces que $h^t = 1$ y $k^t = 1$, con lo que $O(h) \mid t$ y $O(k) \mid t$, de donde deducimos que (por definición de mínimo común múltiplo) $m(h, k) \mid t$. \square

Definición 3.5 (Proyecciones e inyecciones). Dados H y G dos grupos, en el producto directo de H y G podemos definir 4 aplicaciones que nos serán útiles:

1. La proyección en la primera coordenada, $p_1 : H \times G \rightarrow H$, dada por:

$$p_1(h, k) = h \quad \forall (h, k) \in H \times G$$

2. La proyección en la segunda coordenada, $p_2 : H \times G \rightarrow G$, dada por:

$$p_2(h, k) = k \quad \forall (h, k) \in H \times G$$

3. La inyección en la primera coordenada, $i_1 : H \rightarrow H \times G$, dada por:

$$i_1(h) = (h, 1) \quad \forall h \in H$$

4. La inyección en la segunda coordenada, $i_2 : G \rightarrow H \times G$, dada por:

$$i_2(k) = (1, k) \quad \forall k \in G$$

Aplicaciones que podremos recordar fácilmente observando la Figura 3.7.

$$H \begin{array}{c} \xrightarrow{i_1} \\ \xleftarrow{p_1} \end{array} H \times G \begin{array}{c} \xleftarrow{i_2} \\ \xrightarrow{p_2} \end{array} G$$

Figura 3.7: Diagrama de las proyecciones y las inyecciones.

Proposición 3.16. *Se verifica que:*

1. Las proyecciones y las inyecciones son homomorfismos de grupos.
2. $p_1 i_1 = id = p_2 i_2$ y las aplicaciones $p_1 i_2$ y $p_2 i_1$ son la aplicación constantemente igual a 1.
3. Las proyecciones son sobreyectivas y las inyecciones son inyectivas.
4. Si tomamos $H' = \{(h, 1) \mid h \in H\}$, tenemos que:

$$Im(i_1) = \ker(p_2) = H' \triangleleft H \times G$$

Además, $H' \cong H$.

5. De la misma forma, si tomamos $G' = \{(1, k) \mid k \in G\}$, tenemos:

$$Im(i_2) = \ker(p_1) = G' \triangleleft H \times G$$

Además, $G' \cong G$.

6. $H' \cap G' = \{1\}$.

7. $xy = yx$ para todo $x \in H'$, $y \in G'$.

Demostración. Veamos cada apartado:

1. Tenemos 4 casos:

- Para p_1 , vemos que:

$$p_1((h, k)(h', k')) = p_1(hh', kk') = hh' = p_1(h, k)p_1(h', k') \quad \forall (h, k), (h', k') \in H \times G$$

Y la demostración para p_2 es análoga.

- Para i_1 , vemos que:

$$i_1(hh') = (hh', 1) = (h, 1)(h', 1) = i_1(h)i_1(h') \quad \forall h, h' \in H$$

Y la demostración es análoga para i_2 .

2. Si los índices coinciden, tenemos que:

$$\begin{aligned} (p_1 \circ i_1)(h) &= p_1(i_1(h)) = p_1(h, 1) = h & \forall h \in H \\ (p_2 \circ i_2)(k) &= p_2(i_2(k)) = p_2(1, k) = k & \forall k \in G \end{aligned}$$

Y si no coinciden, tenemos:

$$\begin{aligned} (p_1 \circ i_2)(k) &= p_1(i_2(k)) = p_1(1, k) = 1 & \forall k \in G \\ (p_2 \circ i_1)(h) &= p_2(i_1(h)) = p_2(h, 1) = 1 & \forall h \in H \end{aligned}$$

3. Para comprobar que p_1 es sobreyectiva, vemos que dada $h \in H$, tenemos que $p_1(h, 1) = h$ y para ver que p_2 es sobreyectiva, dado $k \in G$, tenemos que $p_2(1, k) = k$.

Para ver la inyectividad de i_1 , si dados $h, h' \in H$ de forma que:

$$(h, 1) = i_1(h) = i_1(h') = (h', 1)$$

De donde deducimos que $h = h'$, por lo que i_1 es inyectiva. La demostración para i_2 es análoga.

4. En primer lugar:

$$\begin{aligned} \text{Im}(i_1) &= \{i_1(h) \mid h \in H\} = \{(h, 1) \mid h \in H\} \\ \ker(p_2) &= \{(h, k) \in H \times G \mid p_2(h, k) = 1\} = \{(h, k) \in H \times G \mid k = 1\} \\ &= \{(h, 1) \in H \times G\} = \{(h, 1) \mid h \in H\} \end{aligned}$$

Además, la igualdad $H' = \ker(p_2)$ nos dice que $H' \triangleleft H \times G$, gracias a la Proposición 3.7.

Para ver que $H' \cong H$, en el apartado 1 vimos que i_1 era un homomorfismo y aplicando 3 tenemos que, de hecho, es un monomorfismo. Como $\text{Im}(i_1) = H'$, la restricción al codominio de i_1 a su imagen nos da un isomorfismo entre H y H' , con lo que $H' \cong H$.

5. Vemos que:

$$\begin{aligned} \text{Im}(i_2) &= \{i_2(k) \mid k \in G\} = \{(1, k) \mid k \in G\} \\ \ker(p_1) &= \{(h, k) \in H \times G \mid p_1(h, k) = 1\} = \{(h, k) \in H \times G \mid h = 1\} \\ &= \{(1, k) \in H \times G\} = \{(1, k) \mid k \in G\} \end{aligned}$$

La igualdad $G' = \ker(p_1)$ nos vuelve a decir que $G' \triangleleft H \times G$.

Y finalmente, para ver que $G' \cong G$, tenemos que i_2 es un monomorfismo, por lo que la restricción en codominio a su imagen, $\text{Im}(i_2) = G'$ nos da un isomorfismo entre G y G' .

6. La igualdad se tiene porque:

$$H' \cap G' = \{(h, k) \in H \times G \mid k = 1 \wedge h = 1\} = \{(1, 1)\} = \{1\}$$

7. Sean $x \in H'$ y $y \in G'$, entonces $\exists h \in H$ y $k \in G$ de forma que $x = (h, 1)$ y $y = (1, k)$, de donde:

$$xy = (h, 1)(1, k) = (h, k) = (1, k)(h, 1) = yx$$

□

3.4.1. Caracterización del grupo directo por isomorfismo

Teorema 3.17 (Propiedad universal del producto directo). *Sea G un grupo y sean $f_1 : G \rightarrow H$, $f_2 : G \rightarrow K$ dos homomorfismos de grupos, entonces existe un único homomorfismo de grupos $f : G \rightarrow H \times K$ tal que $p_1 f = f_1$ y $p_2 f = f_2$.*

Es decir, existe un único homomorfismo f que hace conmutar el siguiente diagrama:

$$\begin{array}{ccccc} & & G & & \\ & \swarrow f_1 & \downarrow f & \searrow f_2 & \\ H & \xleftarrow{p_1} & H \times K & \xrightarrow{p_2} & K \end{array}$$

Demostración. Definimos $f : G \rightarrow H \times K$ dada por:

$$f(x) = (f_1(x), f_2(x)) \quad \forall x \in G$$

■ Vemos las dos igualdades:

$$\begin{aligned} (p_1 \circ f)(x) &= p_1(f(x)) = p_1(f_1(x), f_2(x)) = f_1(x) & \forall x \in G \\ (p_2 \circ f)(x) &= p_2(f(x)) = p_2(f_1(x), f_2(x)) = f_2(x) & \forall x \in G \end{aligned}$$

■ Para ver que f es un homomorfismo:

$$\begin{aligned} f(xy) &= (f_1(xy), f_2(xy)) = (f_1(x)f_1(y), f_2(x)f_2(y)) \\ &= (f_1(x), f_2(x))(f_1(y), f_2(y)) = f(x)f(y) & \forall x, y \in G \end{aligned}$$

- $$g(x) = (p_1(g(x)), p_2(g(x))) = (f_1(x), f_2(x)) = f(x) \quad \forall x \in G$$

☐

Teorema 3.18. *Sea L un grupo y sean $l_1 : L \rightarrow H$, $l_2 : L \rightarrow K$ dos homomorfismos de grupos de forma que si G es un grupo y $f_1 : G \rightarrow H$ y $f_2 : G \rightarrow K$ son otros dos homomorfismos que cumplen la tesis de la propiedad universal del producto directo para L (es decir, que existe un único homomorfismo $f : G \rightarrow L$ de forma que $l_1 f = f_1$ y $l_2 f = f_2$). Entonces, tendremos que:*

$$L \cong H \times K$$

$$\begin{array}{ccc}
& L & \\
l_1 \swarrow & \uparrow f & \searrow l_2 \\
H & & K \\
f_1 \swarrow & & \searrow f_2 \\
& G &
\end{array}$$
$$\begin{aligned} p_1 l &= l_1 \\ p_2 l &= l_2 \end{aligned}$$

$$\begin{array}{ccccc} & & L & & \\ & \swarrow l_1 & \downarrow l & \searrow l_2 & \\ H & \xleftarrow{p_1} & H \times K & \xrightarrow{p_2} & K \end{array}$$

$$\begin{aligned} l_1 p &= p_1 \\ l_2 p &= p_2 \end{aligned}$$

$$\begin{array}{ccccc}
& & L & & \\
& \swarrow l_1 & & \searrow l_2 & \\
H & \xleftarrow{p_1} & H \times K & \xrightarrow{p_2} & K
\end{array}$$

$p \nearrow$ $\downarrow l$

Para terminar la demostración, basta ver que p y l son inversos el uno del otro. Para ello, observamos que:

$$\begin{aligned}
l_1 = p_1 l = l_1 p l &\implies p l = id_L \\
p_1 = l_1 p = p_1 l p &\implies l p = id_{H \times K}
\end{aligned}$$

Concluimos que $p^{-1} = l$, con lo que p y l son isomorfismos y $L \cong H \times K$. \square

Notemos que tanto en la propiedad universal del producto directo como en su unicidad por isomorfismo solo hemos usado las proyecciones p_1 y p_2 . Si consideramos resultados análogos para las inyecciones i_1 y i_2 , estos seguirán siendo ciertos, teniendo que añadir una hipótesis extra:

Teorema 3.19 (Propiedad universal del producto directo 2). *Sea G un grupo y $f_1 : H \rightarrow G$, $f_2 : K \rightarrow G$ dos homomorfismos de grupos verificando que:*

$$f_1(h)f_2(k) = f_2(k)f_1(h) \quad \forall h \in H, k \in K$$

Entonces, existe un único homomorfismo de grupos $f : H \times K \rightarrow G$ tal que $f i_1 = f_1$, $f i_2 = f_2$.

$$\begin{array}{ccccc}
& & G & & \\
& \nearrow f_1 & \uparrow f & \nwarrow f_2 & \\
H & \xrightarrow{i_1} & H \times K & \xleftarrow{i_2} & K
\end{array}$$

Demostración. Definimos $f : H \times K \rightarrow G$ dada por:

$$f(h, k) = f_1(h)f_2(k) \quad \forall (h, k) \in H \times K$$

- Vemos que verifica las dos igualdades:

$$\begin{aligned}
(f \circ i_1)(h) &= f(i_1(h)) = f(h, 1) = f_1(h)f_2(1) = f_1(h) & \forall h \in H \\
(f \circ i_2)(k) &= f(i_2(k)) = f(1, k) = f_1(1)f_2(k) = f_2(k) & \forall k \in K
\end{aligned}$$

- Vemos que f es un homomorfismo, ya que dados $(h, k), (h', k') \in H \times K$:

$$\begin{aligned}
f((h, k)(h', k')) &= f(hh', kk') = f_1(hh')f_2(kk') = f_1(h)f_1(h')f_2(k)f_2(k') \\
&= f_1(h)f_2(k)f_1(h')f_2(k') = f(h, k)f(h', k')
\end{aligned}$$

- Sea $g : H \times K \rightarrow G$ otro homomorfismo de grupos de forma que $g i_1 = f_1$ y $g i_2 = f_2$, entonces dado $(h, k) \in H \times K$:

$$g(h, k) = g((h, 1)(1, k)) = g(h, 1)g(1, k) = g(i_1(h))g(i_2(k)) = f_1(h)f_2(k) = f(h, k)$$

\square

Teorema 3.20. Sea L un grupo y $l_1 : H \rightarrow L$, $l_2 : K \rightarrow L$ dos homomorfismos de grupos que verifican que

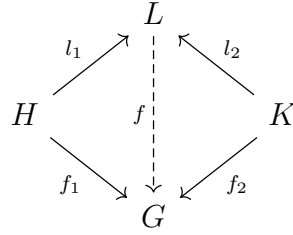
$$l_1(h)l_2(k) = l_2(k)l_1(h) \quad \forall h \in H, k \in K$$

y que para todo grupo G y para todo par de homomorfismos $f_1 : H \rightarrow G$ y $f_2 : K \rightarrow G$ tales que

$$f_1(h)f_2(k) = f_2(k)f_1(h) \quad \forall h \in H, k \in K$$

existe un único homomorfismo $f : L \rightarrow G$ tal que $fl_1 = f_1$ y $fl_2 = f_2$, entonces:

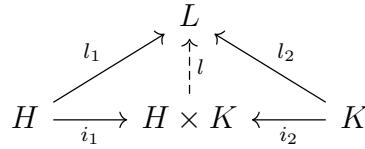
$$L \cong H \times K$$



Demostración. En primer lugar, por ser $l_1 : H \rightarrow L$ y $l_2 : K \rightarrow L$ dos homomorfismos de forma que $l_1(h)l_2(k) = l_2(k)l_1(h) \quad \forall h \in H, k \in K$, tenemos que existe un único homomorfismo $l : H \times K \rightarrow L$ de forma que:

$$li_1 = l_1$$

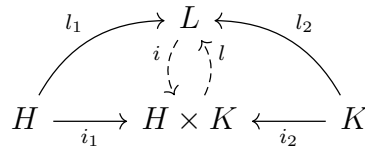
$$li_2 = l_2$$



Ahora, si tomamos $G = H \times K$ y consideramos $i_1 : H \rightarrow H \times K$ y $i_2 : K \rightarrow H \times K$, tenemos por la Proposición 3.16 que $i_1(h)i_2(k) = i_2(k)i_1(h)$ para todo $h \in H$ y para todo $k \in K$, por lo que por hipótesis tenemos que existe un único homomorfismo $i : L \rightarrow H \times K$ de forma que:

$$il_1 = i_1$$

$$il_2 = i_2$$



Basta ver que i y l son inversos el uno del otro. Para ello, observamos que:

$$l_1 = li_1 = lli_1 \implies li = id_{H \times K}$$

$$i_2 = il_2 = ili_2 \implies il = id_L$$

Concluimos que $i^{-1} = l$, con lo que i y l son isomorfismos y $L \cong H \times K$. □

3.4.2. Producto directo de una familia de grupos

Los resultados vistos para el producto directo de dos grupos G y H puede generalizarse para el conjunto cartesiano obtenido de multiplicar una familia arbitraria de grupos. Para estudiar este caso, fijaremos la notación en un inicio: sea Λ un conjunto arbitrariamente grande, si tenemos una familia de tantos grupos como elementos hay en Λ :

$$\{G_\lambda \mid \lambda \in \Lambda\}$$

Podemos considerar el producto cartesiano de todos ellos, que denotaremos por G :

$$G = \prod_{\lambda \in \Lambda} \{G_\lambda \mid \lambda \in \Lambda\} = \prod_{\lambda \in \Lambda} G_\lambda$$

Proposición 3.21. Si $\{G_\lambda \mid \lambda \in \Lambda\}$ es una familia de grupos, definimos en su producto cartesiano $G = \prod_{\lambda \in \Lambda} G_\lambda$ la operación $\cdot : G \times G \rightarrow G$ dada por:

$$x \cdot y = z$$

De forma que la λ -ésima coordenada de z es el producto de la λ -ésima coordenadas de x por la λ -ésima coordenada de y . Se verifica que G con esta operación es un grupo.

Notación. Si $\Lambda = \{1, \dots, n\}$, notaremos:

$$G = \prod_{\lambda \in \Lambda} G_\lambda = G_1 \times G_2 \times \dots \times G_n$$

Si por otra parte se tiene que $G_\lambda = H$ para todo $\lambda \in \Lambda$, entonces notaremos:

$$G = \prod_{\lambda \in \Lambda} G_\lambda = H^\Lambda$$

En el caso de que Λ sea finito y tenga n elementos, notaremos H^n .

Definición 3.6 (Proyecciones e inyecciones). Fijado $\lambda \in \Lambda$, definimos:

- La proyección en la λ -ésima coordenada, $p_\lambda : G \rightarrow G_\lambda$ dada por:

$$p_\lambda(g) = g_\lambda \quad \forall g \in G$$

Siendo g_λ la λ -ésima coordenada de g .

- La inyección en la λ -ésima coordenada, $i_\lambda : G_\lambda \rightarrow G$ dada por:

$$i_\lambda(x) = g \quad \forall x \in G_\lambda$$

Donde $g_\mu = 1 \ \forall \mu \in \Lambda \setminus \{\lambda\}$ y $g_\lambda = x$.

Proposición 3.22. Sea $\{G_\lambda \mid \lambda \in \Lambda\}$ una familia de grupos y sea $G = \prod_{\lambda \in \Lambda} G_\lambda$, se verifica:

1. p_λ y i_λ son homomorfismos de grupos, $\forall \lambda \in \Lambda$.

2. Las proyecciones son epimorfismos y las inyecciones son monomorfismos.
3. $p_\lambda i_\lambda = id_{G_\lambda}$ y $(p_\lambda i_\mu)(x) = 1$ para todo $x \in G_\mu$, $\forall \lambda \in \Lambda, \mu \in \Lambda \setminus \{\lambda\}$.
4. $G'_\lambda = Im(i_\lambda) \cong G_\lambda$ y es un subgrupo normal de G .

Teorema 3.23 (Propiedad universal del producto directo). Sea $\{G_\lambda \mid \lambda \in \Lambda\} \cup \{H\}$ una familia de grupos y $G = \prod_{\lambda \in \Lambda} G_\lambda$, si tenemos una familia de homomorfismos para cada coordenada $\{f_\lambda : H \rightarrow G_\lambda \mid \lambda \in \Lambda\}$, entonces existe un único homomorfismo $f : H \rightarrow G$ de forma que $f_\lambda = p_\lambda f$, $\forall \lambda \in \Lambda$. Además, cualquier otro grupo que verifique esta propiedad será isomorfo a G .

$$\begin{array}{ccc} H & & \\ \downarrow f & \searrow f_\lambda & \\ G & \xrightarrow{p_\lambda} & G_\lambda \end{array}$$

3.4.3. Producto directo de una familia finita de subgrupos

Teorema 3.24 (Ley asociativa general). Tenemos que:

1. Si G_1, G_2, G_3 son tres grupos, entonces:

$$(G_1 \times G_2) \times G_3 \cong G_1 \times G_2 \times G_3 \cong G_1 \times (G_2 \times G_3)$$

2. Si G_1, G_2, \dots, G_n son n grupos, entonces si $k \in \{1, \dots, n-1\}$, se tiene:

$$\left(\prod_{j=1}^k G_j \right) \times \left(\prod_{j=k+1}^n G_j \right) \cong \prod_{j=1}^n G_j$$

Teorema 3.25. Sean G_1, G_2, \dots, G_n n grupos y $G = G_1 \times G_2 \times \dots \times G_n$:

1. $|G| = |G_1| |G_2| \dots |G_n|$. En particular, G es finito si y solo si G_k es finito, para todo $k \in \{1, \dots, n\}$.
2. $O(g_1, \dots, g_n) = \text{mcm}(O(g_1), \dots, O(g_n))$, $\forall (g_1, \dots, g_n) \in G$.

3.5. Producto directo interno

El caso que nos interesará ahora será fijado un grupo G , consideramos dos subgrupos suyos, $H, K < G$ y trataremos de caracterizar cuándo $H \times K \cong G$. En cuyo caso, diremos que G es producto directo interno de H y de K .

Definición 3.7 (Conmutador). Sea G un grupo, definimos sobre G la operación conmutador $[\cdot, \cdot] : G \times G \rightarrow G$ dada por:

$$[h, k] = hk(kh)^{-1} = hkh^{-1}k^{-1} \quad \forall h, k \in G$$

Esta operación viene a decirnos cómo de abelianos son los elementos h y k que estemos considerando.

Proposición 3.26. Sea G un grupo y $h, k \in G$:

$$hk = kh \iff [h, k] = 1$$

Demostración. Basta observar que:

$$hk = kh \iff (hk)^{-1} = (kh)^{-1} \iff [h, k] = hk(kh)^{-1} = 1$$

□

Aunque el siguiente Teorema no nos caracteriza el hecho de que el producto de dos subgrupos de un grupo sea producto directo interno, es el resultado al que comúnmente se le conoce como caracterización del producto directo interno, puesto que viene a decirnos cuándo $H \times K \cong G$ bajo un isomorfismo que se obtiene de una forma muy natural.

Por tanto, diremos que $H \times K$ con $H, K < G$ es producto directo interno de G cuando $H \times K \cong G$ bajo el isomorfismo del siguiente Teorema:

Teorema 3.27 (Caracterización del producto directo interno). Sea G un grupo, $H, K < G$, equivalen:

- i) La aplicación $\phi : H \times K \rightarrow G$ dada por $\phi(h, k) = hk$ es un isomorfismo.
- ii) $H, K \triangleleft G$, $HK = G$ y $H \cap K = \{1\}$.
- iii) $hk = kh \quad \forall h \in H, k \in K$, $H \vee K = G$ y $H \cap K = \{1\}$.
- iv) $hk = kh \quad \forall h \in H, k \in K$ y para todo $g \in G$, $\exists_1 h \in H, \exists_1 k \in K$ de forma que $g = hk$.

Demostración. Veamos las implicaciones:

i) \implies ii) Veamos las tres propiedades:

- Primero que $HK = G$:
 \subseteq) $HK \subseteq G$ por definición de HK .
 \supseteq) Como ϕ es sobreyectiva, dado $g \in G$, existen $h \in H, k \in K$ de forma que $g = \phi(h, k) = hk$, lo que nos dice que $G \subseteq HK$.
- Sea $g \in H \cap K$, entonces $g = \phi(g, 1) = \phi(1, g) = g$, pero por ser ϕ inyectiva, tenemos que $(g, 1) = (1, g)$, de donde $g = 1$.
- Finalmente, para ver que $H, K \triangleleft G$, basta observar que:

$$\begin{array}{ccccc} & & G & & \\ & \nearrow \phi & & \searrow \phi^{-1} & \\ H & \xleftarrow{p_1} & H \times K & \xrightarrow{p_2} & K \end{array}$$

Para deducir:

$$\ker(p_2\phi^{-1}) = \{hk \in G \mid k = 1\} = H$$

$$\ker(p_1\phi^{-1}) = \{hk \in G \mid h = 1\} = K$$

De donde tenemos que $H, K \triangleleft G$ (ya que $p_2\phi^{-1}$ y $p_1\phi^{-1}$ son homomorfismos y H y K conciden con sus respectivos núcleos, ver la Proposición 3.7).

$ii) \implies iii)$ Dados $h \in H$ y $k \in K$, veamos que $[h, k] = 1$, de donde deducimos que $hk = kh$:

$$[h, k] = hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$$

- Por un lado, como K es normal, tendremos que $hkh^{-1} \in K$, de donde $[h, k] = (hkh^{-1})k^{-1} \in K$.
- Por otro lado, como H es normal, tendremos también que $kh^{-1}k^{-1} \in H$, de donde $[h, k] = h(kh^{-1}k^{-1}) \in H$.

En definitiva:

$$[h, k] \in H \cap K = \{1\} \implies hk = kh$$

Para la segunda propiedad, basta ver que:

$$G = HK \subseteq H \vee K \subseteq G$$

$iii) \implies iv)$ Sea $g \in G$, veamos que se expresa como producto de un elemento de H por otro elemento de K . Para ello, como $G = H \vee K$, existirán elementos $\alpha_1, \dots, \alpha_n \in H \cup K$ de forma que:

$$g = \alpha_1 \dots \alpha_n$$

Pero como $hk = kh$ para todo $k \in K$ y $h \in H$, podremos conmutar los elementos de forma que lleguemos a:

$$g = (h_1 \dots h_m)(k_{m+1} \dots k_n) = hk \in HK$$

Para ciertos $h \in H$, $k \in K$. Para la unicidad, si $g = h_1k_1 = h_2k_2$, tenemos que:

$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\} \implies h_2 = h_1 \wedge k_1 = k_2$$

$iv) \implies i)$ Tenemos para $(h_1, k_1), (h_2, k_2) \in H \times K$ arbitrarios que:

$$\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2)$$

De donde ϕ es un homomorfismo. La biyectividad de ϕ se debe a que dado $g \in G$, existen unos únicos $h \in H$, $k \in K$ de forma que $g = hk = \phi(h, k)$. \square

Ejemplo. Veamos si los siguientes ejemplos son o no un producto interno directo, bajo el isomorfismo natural del Teorema anterior:

1. En $G = \mathbb{R}^*$, consideramos $H = \{\pm 1\}$ y $K = \{x \in \mathbb{R} \mid x > 0\}$.

Sí es producto interno directo, ya que se verifican:

- $G = HK$.
- G es abeliano, luego $H, K \triangleleft G$.
- $H \cap K = \{1\}$.

Y podemos aplicar el Teorema 3.27.

2. Sean:

$$\begin{aligned} G &= \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \text{GL}_2(\mathbb{R}) \right\} \\ H &= \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in \text{GL}_2(\mathbb{R}) \right\} \\ K &= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R}) \right\} \end{aligned}$$

Dado un elemento de G , podemos escribirlo como un elemento de HK :

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ab \\ 0 & c \end{pmatrix}$$

Luego $G = HK$. Sin embargo, $hk \neq kh$ para $h \in H$ y $k \in K$, ya que:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & bc \\ 0 & c \end{pmatrix} \neq \begin{pmatrix} a & ab \\ 0 & c \end{pmatrix}$$

Por lo que G no es producto directo interno de H y de K .

3. Sea $G = \mathbb{C}^*$, consideramos $H = \{z \in \mathbb{C} \mid |z| = 1\}$ y $K = \mathbb{R}^+$. Por la forma polar de los números complejos, tenemos que $G = HK$:

$$z = \frac{z}{|z|} |z| \in HK$$

Y como G es abeliano, tenemos que $H, K \triangleleft G$. Además:

$$H \cap K = \{1\}$$

Veamos ahora cómo se comportan los subgrupos con el producto directo:

Proposición 3.28. *Sea G un grupo, $H, K < G$, si $H_1 < H$ y $K_1 < K$, entonces:*

1. $H_1 \times K_1 < H \times K$.
2. Existe un monomorfismo $\text{Aut}(H) \times \text{Aut}(K) \rightarrow \text{Aut}(H \times K)$.

Demostración. Veamos que los dos se cumplen:

1. $H_1 \times K_1 \subseteq H \times K$. Además, como $H_1 < H$ y $K_1 < K$, $H_1 \times K_1$ va a ser cerrado para el producto, el producto será asociativo, tendrá al elemento $(1, 1)$ como neutro y fijado un elemento $(x, y) \in H_1 \times K_1$, tendremos que $(x, y)^{-1} = (x^{-1}, y^{-1}) \in H_1 \times K_1$, de donde concluimos que $H_1 \times K_1 < H \times K$.
2. Consideramos:

$$\begin{aligned} \psi : \text{Aut}(H) \times \text{Aut}(K) &\longrightarrow \text{Aut}(H \times K) \\ (\alpha, \beta) &\longmapsto \psi(\alpha, \beta) \end{aligned}$$

Donde $\psi(\alpha, \beta) : H \times K \rightarrow H \times K$ viene dada por:

$$\psi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)) \quad \forall (h, k) \in H \times K$$

Veamos en primer lugar que la aplicación ψ está bien definida, es decir, que $\psi(\alpha, \beta)$ es un automorfismo siempre que $\alpha \in \text{Aut}(H)$ y $\beta \in \text{Aut}(K)$:

- Para ver que $\psi(\alpha, \beta)$ es un homomorfismo, dados $(h, k), (h', k') \in H \times K$:

$$\begin{aligned}\psi(\alpha, \beta)((h, k)(h', k')) &= \psi(\alpha, \beta)(hh', kk') = (\alpha(hh'), \beta(kk')) \\ &= (\alpha(h)\alpha(h'), \beta(k)\beta(k')) = (\alpha(h), \beta(k))(\alpha(h'), \beta(k')) = \psi(\alpha, \beta)(h, k)\psi(\alpha, \beta)(h', k')\end{aligned}$$

- Para la sobreyectividad, dado $(h, k) \in H \times K$, como $\alpha \in \text{Aut}(H)$ y $\beta \in \text{Aut}(K)$ son sobreyectivas, existirán $h' \in H, k' \in K$ de forma que:

$$\alpha(h') = h \quad \beta(k') = k$$

Por lo que:

$$\psi(\alpha, \beta)(h', k') = (\alpha(h'), \beta(k')) = (h, k)$$

- Para la inyectividad, sean $(h, k), (h', k') \in H \times K$ de forma que:

$$(\alpha(h), \beta(k)) = \psi(\alpha, \beta)(h, k) = \psi(\alpha, \beta)(h', k') = (\alpha(h'), \beta(k'))$$

De donde deducimos que:

$$\alpha(h) = \alpha(h') \quad \beta(k) = \beta(k')$$

Pero como α y β son inyectivas, tenemos que $h = h'$ y $k = k'$, de donde $(h, k) = (h', k')$.

Finalmente, veamos que ψ es un monomorfismo:

- Para ver que es un homomorfismo, dadas $(\alpha, \beta), (\alpha', \beta') \in \text{Aut}(H) \times \text{Aut}(K)$:

$$\psi((\alpha, \beta)(\alpha', \beta')) = \psi(\alpha\alpha', \beta\beta') \stackrel{(*)}{=} \psi(\alpha, \beta)\psi(\alpha', \beta')$$

Donde en $(*)$ se da la igualdad funcional, ya que para $(h, k) \in H \times K$:

$$\begin{aligned}\psi(\alpha\alpha', \beta\beta')(h, k) &= ((\alpha \circ \alpha')(h), (\beta \circ \beta')(k)) = (\alpha(\alpha'(h)), \beta(\beta'(k))) \\ (\psi(\alpha, \beta)\psi(\alpha', \beta'))(h, k) &= \psi(\alpha, \beta)(\alpha'(h), \beta'(k)) = (\alpha(\alpha'(h)), \beta(\beta'(k)))\end{aligned}$$

- Para ver que ψ es inyectiva, sean $(\alpha, \beta), (\alpha', \beta') \in \text{Aut}(H) \times \text{Aut}(K)$ de forma que:

$$\psi(\alpha, \beta) = \psi(\alpha', \beta')$$

Entonces:

$$\psi(\alpha, \beta)(h, k) = (\alpha(h), \beta(k)) = (\alpha'(h), \beta'(k)) = \psi(\alpha', \beta')(h, k) \quad \forall (h, k) \in H \times K$$

De donde deducimos que $\alpha = \alpha'$ y que $\beta = \beta'$, por lo que ψ es inyectiva.

□

Teorema 3.29. Sean H, K dos grupos finitos tales que $\text{mcd}(|H|, |K|) = 1$, entonces:

1. $\forall L < H \times K, \exists_1 H_1 < H, K_1 < K$ de forma que:

$$L = H_1 \times K_1$$

Es decir, todo subgrupo de $H \times K$ se descompone de forma única como un subgrupo de H por un subgrupo de K .

2. La aplicación $\psi : \text{Aut}(H) \times \text{Aut}(K) \rightarrow \text{Aut}(H \times K)$ de la Proposición 3.28 es un isomorfismo.

Demostración. Veamos los dos resultados:

1. Sea $L < H \times K$, consideramos:

$$H_1 = p_1(L) < H \quad K_1 = p_2(L) < K$$

Por la Proposición 3.28, tenemos que $H_1 \times K_1 < H \times K$, y por la definición de L que $L < H_1 \times K_1$, ya que si $(h, k) \in L$:

$$h = p_1(h, k) \in H_1$$

$$k = p_2(h, k) \in K_1$$

Basta ver que $H_1 \times K_1 < L$.

$$\begin{array}{ccccc} H & \xleftarrow{p_1} & H \times K & \xrightarrow{p_2} & K \\ | & & | & & | \\ H_1 & & L & & K_1 \end{array}$$

Para ello, si notamos $n = |H|$ y $m = |K|$, por el Teorema de Bezout $\exists r, s \in \mathbb{Z}$ de forma que:

$$nr + ms = 1$$

- En primer lugar, si $h \in H_1$, por su definición y la sobreyectividad de p_1 , existirá $(h, k) \in L$ de forma que $p_1(h, k) = h$, de donde:

$$L \ni (h, k)^{ms} = (h^{ms}, k^{ms}) = (h^{1-nr}, 1) = (h, 1)$$

Por lo que: $\{(h, 1) \mid h \in H_1\} \subseteq L$.

- Ahora, si $k \in K_1$, por su definición y la sobreyectividad de p_2 , existirán $(h, k) \in L$ de forma que $p_2(h, k) = k$, de donde:

$$L \ni (h, k)^{nr} = (h^{nr}, k^{nr}) = (1, k^{1-ms}) = (1, k)$$

Por lo que: $\{(1, k) \mid k \in K_1\} \subseteq L$.

Sea ahora $(h, k) \in H_1 \times K_1$, tenemos que:

$$(h, k) = (h, 1)(1, k) \in L$$

De donde $H_1 \times K_1 < L$. Finalmente, la construcción que hemos realizado nos da la unicidad, pues si existen otros subconjuntos $H_2 < H$ y $K_2 < K$ de forma que $L = H_2 \times K_2$, tendríamos que:

$$H_2 = p_1(L) = H_1 \quad K_2 = p_2(L) = K_1$$

2. Basta ver que $\psi : \text{Aut}(H) \times \text{Aut}(K) \rightarrow \text{Aut}(H \times K)$ es sobreyectiva, es decir, que dada $\varphi \in \text{Aut}(H \times K)$, podemos encontrar $\alpha \in \text{Aut}(H)$ y $\beta \in \text{Aut}(K)$ de forma que $\varphi = \psi(\alpha, \beta)$. Para ello, mostraremos el proceso para encontrar α y el proceso para encontrar β es análogo.

En primer lugar, lo que hacemos es estudiar la imagen por φ del conjunto $H \times \{1\} < H \times K$. Como φ es un homomorfismo, sabemos que la imagen de $H \times \{1\}$ por φ será un subgrupo de $H \times K$, a quien llamaremos G_1 :

$$G_1 = \varphi(H \times \{1\}) < H \times K$$

Por el apartado 1, sabemos que podemos encontrar únicos $H_1 < H$ y $K_1 < K$ de forma que $G_1 = H_1 \times K_1$. Además, por ser φ biyectiva, tendremos que:

$$|H| = |H \times \{1\}| = |H_1 \times K_1| = |H_1||K_1|$$

Veamos que $|K_1| = 1$. Para ello, si $m = |K_1| \in \mathbb{N}$:

- De la igualdad $|H| = |H_1|m$ deducimos que m divide a $|H|$.
- Como $m = |K_1|$ y $K_1 < K$, por el Teorema de Lagrange tenemos también que m divide a $|K|$.

Por la definición del máximo común divisor, concluimos que m divide a $\text{mcd}(|H|, |K|) = 1$, de donde $m = 1$ y $K_1 = \{1\}$.

Finalmente, de la igualdad $|H| = |H_1|$ concluimos que $H = H_1$. Hemos probado que:

$$\varphi(H \times \{1\}) = H \times \{1\}$$

Definimos ahora $\alpha : H \rightarrow H$ dada por:

$$\alpha(h) = p_1(\varphi(i_1(h))) \quad \forall h \in H$$

Está claro que α es un homomorfismo, como composición de homomorfismos.

- Para la sobreyectividad de α , como $\varphi(H \times \{1\}) = H \times \{1\}$, tenemos que:

$$\alpha(H) = p_1(\varphi(i_1(H))) = p_1(\varphi(H \times \{1\})) = p_1(H \times \{1\}) = H$$

- Para la inyectividad, sean $h_1, h_2 \in H$ de forma que:

$$p_1(\varphi(h_1, 1)) = \alpha(h_1) = \alpha(h_2) = p_2(\varphi(h_2, 1))$$

Como $\varphi(H \times \{1\}) = H \times \{1\}$, sabemos que existirán $h'_1, h'_2 \in H$ de forma que:

$$\varphi(h_1, 1) = (h'_1, 1) \quad \varphi(h_2, 1) = (h'_2, 1)$$

Por lo que:

$$h'_1 = p_1(h'_1, 1) = p_1(\varphi(h_1, 1)) = p_1(\varphi(h_2, 1)) = p_1(h'_2, 1) = h'_2$$

De donde concluimos que α es inyectiva.

De forma análoga a lo que hicimos anteriormente, puede probarse que:

$$\varphi(\{1\} \times K) = \{1\} \times K$$

Y definiendo $\beta : H \times K \rightarrow H \times K$ dada por:

$$\beta(k) = p_2(\varphi(i_2(k))) \quad \forall k \in K$$

Tenemos que $\beta \in \text{Aut}(K)$.

Con estos dos automorfismos, veamos que $\psi(\alpha, \beta) = \varphi$:

$$\begin{aligned} \psi(\alpha, \beta)(h, k) &= (\alpha(h), \beta(k)) = (p_1(\varphi(h, 1)), p_2(\varphi(1, k))) \stackrel{(*)}{=} \varphi(h, k) \\ &\quad \forall (h, k) \in H \times K \end{aligned}$$

Donde en $(*)$ hemos usado que existirán $h' \in H$ y $k' \in K$ de forma que:

$$\varphi(h, 1) = (h', 1) \quad \varphi(1, k) = (1, k')$$

Por lo que:

$$\begin{aligned} (p_1(\varphi(h, 1)), p_2(\varphi(1, k))) &= (p_1(h', 1), p_2(1, k')) = (h', k') \\ &= (h', 1)(1, k') = \varphi(h, 1)\varphi(1, k) = \varphi(h, k) \end{aligned}$$

□

El punto 2 de este último Teorema será un resultado que usemos en numerosos ejercicios, sin considerar de forma explícita la aplicación ψ pero usando el isomorfismo $\text{Aut}(H) \times \text{Aut}(K) \cong \text{Aut}(H \times K)$ bajo las hipótesis apropiadas.

3.5.1. Producto directo interno de una familia de subgrupos

Teorema 3.30. Sea $\{G_\lambda \mid \lambda \in \Lambda\}$ una familia de grupos de forma que para cada $\lambda \in \Lambda$ tenemos $H_\lambda < G_\lambda$, entonces:

$$\prod_{\lambda \in \Lambda} H_\lambda < \prod_{\lambda \in \Lambda} G_\lambda$$

Teorema 3.31. Sea $\{G_\lambda \mid \lambda \in \Lambda\}$, entonces existe un monomorfismo

$$\prod_{\lambda \in \Lambda} \text{Aut}(G_\lambda) \longrightarrow \text{Aut}\left(\prod_{\lambda \in \Lambda} G_\lambda\right)$$

3.5.2. Producto directo interno de una familia finita de subgrupos

Teorema 3.32. Sea G un grupo y $G_1, \dots, G_n < G$ n subgrupos de G , definimos la aplicación $\phi : G_1 \times \dots \times G_n \rightarrow G$ dada por:

$$\phi(g_1, \dots, g_n) = g_1 \cdot \dots \cdot g_n \quad \forall (g_1, \dots, g_n) \in G_1 \times \dots \times G_n$$

Son equivalentes:

- i) ϕ es un isomorfismo.
- ii) $G_k \triangleleft G \forall k \in \{1, \dots, n\}$, $G_1 \dots G_n = G$ y $(G_1 \dots G_{k-1}) \cap G_k = \{1\}$ para todo $k \in \{2, \dots, n\}$.
- iii) $g_k g_h = g_h g_k$ para todo $g_h \in G_h$, $g_k \in G_k$ con $k \neq h$, $G = G_1 \vee \dots \vee G_n$ y $(G_1 \dots G_{k-1}) \cap G_k = \{1\}$ para todo $k \in \{2, \dots, n\}$.
- iv) $g_k g_h = g_h g_k$ para todo $g_h \in G_h$, $g_k \in G_k$ con $k \neq h$, y todo elemento $g \in G$ se expresa de manera única como $g = g_1 \dots g_n$ con $g_k \in G_k$ para todo $k \in \{1, \dots, n\}$.

Teorema 3.33. Sean G_1, \dots, G_n n grupos de forma que sus órdenes son primos relativos dos a dos, si $G = G_1 \times \dots \times G_n$, entonces:

1. $\exists_1 H_k < G_k$ tal que $L = H_1 \times \dots \times H_k$ para todo $L < G$.
2. $\text{Aut}(G_1) \times \dots \times \text{Aut}(G_n) \cong \text{Aut}(G)$.

3.6. Producto directo de grupos cíclicos

Notación. Cuando hablemos del producto directo de dos grupos cíclicos, en vez de usar \times , usaremos como notación \oplus , ya que normalmente usamos la notación aditiva al trabajar con grupos cíclicos.

Ejemplo. En primer lugar, hemos de tener en cuenta que el producto directo de dos grupos cíclicos no tiene por qué ser en general un grupo cíclico. Veamos varios ejemplos de que no se cumple:

1. Supongamos que $\mathbb{Z} \oplus \mathbb{Z}$ es cíclico. En cuyo caso, tenemos que $\exists(r, s) \in \mathbb{Z} \oplus \mathbb{Z}$ de forma que:

$$\mathbb{Z} \oplus \mathbb{Z} = \langle (r, s) \rangle$$

De donde para $(1, 0) \in \mathbb{Z} \oplus \mathbb{Z} \exists n \in \mathbb{Z}$ de forma que:

$$(1, 0) = n(r, s) \implies \begin{cases} nr = 1 \\ ns = 0 \end{cases} \implies \begin{cases} n, r \in \{\pm 1\} \\ s = 0 \end{cases} \implies (r, s) = \begin{cases} (-1, 0) \\ (1, 0) \end{cases}$$

Sin embargo, $(0, 1) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$, por lo que $\exists m \in \mathbb{Z}$ de forma que:

$$(0, 1) = m(1, 0) \implies \begin{cases} m = 0 \\ 1 = 0 \end{cases}$$

Contradicción, por lo que $\mathbb{Z} \oplus \mathbb{Z}$ no es cíclico.

2. Ahora, supongamos que $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ es cíclico, con lo que de la misma forma, $\exists(r, s) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ de modo que:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \langle (\bar{r}, \bar{s}) \rangle$$

Sin embargo:

$$O(\bar{r}, \bar{s}) = \text{mcm}(O(\bar{r}), O(\bar{s})) = \begin{cases} 1 \iff \bar{r} = \bar{s} = 0 \\ 2 \iff \bar{r} \neq 0 \vee \bar{s} \neq 0 \end{cases}$$

En $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ no hay elementos de orden 4, pero:

$$|\mathbb{Z}_2 \oplus \mathbb{Z}_2| = 4$$

Un grupo de orden 4 que no tiene elementos de orden 4 nunca puede ser cíclico. De hecho, tendremos que $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong V$.

3. Un ejemplo de dos grupos cíclicos cuyo producto directo es cíclico es:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3$$

Que tiene orden $|\mathbb{Z}_2 \oplus \mathbb{Z}_3| = |\mathbb{Z}_2||\mathbb{Z}_3| = 6$. Si consideramos $(\bar{1}, \bar{1})$, tenemos que:

$$O(\bar{1}, \bar{1}) = \text{mcm}(O(\bar{1}_2), O(\bar{1}_3)) = \text{mcm}(2, 3) = 6$$

Por lo que $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (\bar{1}, \bar{1}) \rangle$. Notemos que el motivo de que esto haya sucedido es porque 2 y 3 son primos relativos.

Proposición 3.34. Si G y H son grupos cíclicos finitos, entonces:

$$G \oplus H \text{ es cíclico} \iff \text{mcd}(|G|, |H|) = 1$$

Demostración. Veamos las dos implicaciones. Para ello, supongamos que:

$$G = \langle x \rangle, \quad O(x) = n, \quad H = \langle y \rangle, \quad O(y) = m$$

Para ciertos $x \in G$ y $y \in H$.

\Leftarrow) Si $\text{mcd}(n, m) = 1$, entonces $\text{mcm}(n, m) = nm$, de donde:

$$O(x, y) = \text{mcm}(O(x), O(y)) = nm = |G||H| = |G \times H|$$

Tenemos un grupo de orden nm que contiene a un elemento de orden nm , luego $G \times H = \langle (x, y) \rangle$.

\Rightarrow) Si $G \oplus H = \langle (a, b) \rangle$, entonces:

$$O(a, b) = \text{mcm}(O(a), O(b)) = nm = |G||H| = |G \times H|$$

Como $O(a) \mid n$ y $O(b) \mid m$, llegamos a que $O(a) = n$ y $O(b) = m$. Finalmente:

$$\text{mcd}(n, m) = \frac{nm}{\text{mcm}(n, m)} = \frac{nm}{nm} = 1$$

□

Corolario 3.34.1. Si G_1, G_2, \dots, G_n son n grupos cíclicos finitos, entonces:

$$\bigoplus_{k=1}^n G_k \text{ cíclico} \iff \text{mcd}(|G_i|, |G_j|) = 1 \quad \forall i, j \in \{1, \dots, n\}, i \neq j$$

Ejemplo. Aplicando esta última proposición:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30}$.
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ no es cíclico.

Ejemplo. Podemos demostrar que S_3 no es producto directo interno de subgrupos propios. Por reducción al absurdo, si fuera producto directo, como $|S_3| = 6$, tendría un subgrupo de orden 2 y otro de orden 3, ambos isomorfos a C_2 y C_3 . Si tuviera dos subgrupos propios cuyo producto propio fuera él mismo, tendríamos:

$$S_3 \cong C_2 \oplus C_3 \cong C_6$$

Pero S_3 no es cíclico, hemos llegado a una contradicción.

4. Grupos resolubles

Este Capítulo trata sobre los grupos resolubles, propiedad interesante de un grupo que tendrá numerosas aplicaciones, como por ejemplo en la solución de ecuaciones con radicales. Sin embargo, la definición de grupo resoluble ha de esperar, pues primero tenemos que hacer un estudio de las “series de un grupo”.

4.1. Series de un grupo

Definición 4.1 (Serie de un grupo). Sea G un grupo, una serie de G es una cadena de subgrupos G_0, G_1, \dots, G_r de forma que:

$$G = G_0 > G_1 > G_2 > \dots > G_r = \{1\}$$

En dicho caso, diremos que la serie tiene longitud r .

Ejemplo. En S_3 , podemos considerar la serie:

$$S_3 > A_3 > \{1\}$$

Definición 4.2 (Refinamiento). Sea G un grupo, si consideramos sobre él dos series:

$$G = H_0 > H_1 > \dots > H_s = \{1\} \quad (4.1)$$

$$G = G_0 > G_1 > G_2 > \dots > G_r = \{1\} \quad (4.2)$$

Diremos que (4.2) es un refinamiento de (4.1) si todo grupo que aparece en (4.1) también aparece en (4.2). Ha de ser por tanto $r \geq s$.

Decimos que (4.2) es un refinamiento propio de (4.1) si en (4.1) hay grupos que no aparecen en (4.2). En dicho caso, ha de ser $r > s$.

Ejemplo. En A_4 , podemos considerar la serie:

$$A_4 > V > \{1\}$$

Un refinamiento propio de la misma es:

$$A_4 > V > \langle (1\ 2)(3\ 4) \rangle > \{1\}$$

Definición 4.3 (Series propia y normal). Sea G un grupo, si consideramos una serie de G :

$$G = G_0 > G_1 > \dots > G_r = \{1\}$$

- Decimos que es una serie propia si todas las inclusiones entre los subgrupos son propias, es decir, si $G_{k+1} \subsetneq G_k$, para todo $k \in \{0, \dots, r-1\}$.
- Decimos que es una serie normal si todas las relaciones de subgrupo que aparecen son de subgrupo normal, es decir, si $G_k \triangleright G_{k+1}$, para todo $k \in \{0, \dots, r-1\}$.

En dicho caso, lo notaremos como:

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\}$$

Ejemplo. Todas las series anteriores eran series normales propias:

$$\begin{aligned} S_3 &\triangleright A_3 \triangleright \{1\} \\ A_4 &\triangleright V \triangleright \{1\} \\ A_4 &\triangleright V \triangleright \langle (1\ 2)(3\ 4) \rangle \triangleright \{1\} \end{aligned}$$

Definición 4.4 (Índices y factores de una serie).

Dada una serie normal de un grupo G :

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\}$$

- Llamamos factores de la serie a los grupos cocientes:

$$G_{k-1}/G_k \quad \forall k \in \{1, \dots, r\}$$

- Llamamos índices de la serie a los correspondientes órdenes de los factores.

Si $i_k = [G_{k-1} : G_k]$ para todo $k \in \{1, \dots, r\}$, entonces notaremos:

$$G = G_0 \overset{i_1}{\triangleright} G_1 \overset{i_2}{\triangleright} \dots \overset{i_r}{\triangleright} G_r = \{1\}$$

Ejemplo. Por ejemplo, en la serie:

$$S_3 \triangleright A_3 \triangleright \{1\}$$

Tenemos los factores:

$$S_3/A_3 \cong C_2 \quad A_3/\{1\} \cong A_3$$

Y los índices:

$$S_3 \overset{2}{\triangleright} A_3 \overset{3}{\triangleright} \{1\}$$

Si consideramos ahora la serie:

$$A_4 \overset{3}{\triangleright} V \overset{2}{\triangleright} \langle (1\ 2)(3\ 4) \rangle \overset{2}{\triangleright} \{1\}$$

Los factores que obtenemos son:

$$A_4/V \quad V/\langle (1\ 2)(3\ 4) \rangle \quad \langle (1\ 2)(3\ 4) \rangle/\{1\}$$

Definición 4.5. Sea G un grupo, si tenemos dos series normales de G :

$$\begin{aligned} G &= G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\} \\ G &= H_0 \triangleright H_1 \triangleright \dots \triangleright H_s = \{1\} \end{aligned}$$

Se dice que son isomorfas si $r = s$ y existe $\sigma \in S_r$ de forma que:

$$G_{k-1}/G_k \cong H_{\sigma(k)-1}/H_{\sigma(k)} \quad \forall k \in \{1, \dots, r\}$$

Ejemplo. En $\mathbb{Z}/24\mathbb{Z}$ consideramos las series:

$$\begin{aligned} \mathbb{Z}/24\mathbb{Z} &\triangleright 2\mathbb{Z}/24\mathbb{Z} \triangleright 4\mathbb{Z}/24\mathbb{Z} \triangleright 8\mathbb{Z}/24\mathbb{Z} \triangleright 24\mathbb{Z}/24\mathbb{Z} = \{0\} \\ \mathbb{Z}/24\mathbb{Z} &\triangleright 3\mathbb{Z}/24\mathbb{Z} \triangleright 6\mathbb{Z}/24\mathbb{Z} \triangleright 12\mathbb{Z}/24\mathbb{Z} \triangleright 24\mathbb{Z}/24\mathbb{Z} = \{0\} \end{aligned}$$

Que son dos series isomorfas, para la permutación $\sigma = (1 \ 2 \ 3 \ 4)$, ya que:

$$\begin{aligned} \mathbb{Z}/24\mathbb{Z} &\stackrel{2}{\triangleright} 2\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 4\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 8\mathbb{Z}/24\mathbb{Z} \stackrel{3}{\triangleright} 24\mathbb{Z}/24\mathbb{Z} = \{0\} \\ \mathbb{Z}/24\mathbb{Z} &\stackrel{3}{\triangleright} 3\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 6\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 12\mathbb{Z}/24\mathbb{Z} \stackrel{2}{\triangleright} 24\mathbb{Z}/24\mathbb{Z} = \{0\} \end{aligned}$$

4.1.1. Series de composición

Pasamos ya al estudio de las series que nos interesarán, que son las series de composición.

Definición 4.6 (Serie de composición). Una serie de G se dice que es una serie de composición de G si es una serie normal sin refinamientos normales propios.

En una serie de composición, será usual referirnos a los factores como factores de composición, y a los índices como índices de composición.

Ejemplo. Ejemplos de series de composición son:

- Las dos series anteriores sobre $\mathbb{Z}/24\mathbb{Z}$ son series de composición, ya que los índices no permiten introducir más subgrupos a la serie.
- Anteriormente vimos que la serie $A_4 \triangleright V \triangleright \{1\}$ no era de composición, ya que podíamos refinarla más: $A_4 \triangleright V \triangleright \langle (1 \ 2)(3 \ 4) \rangle \triangleright \{1\}$, aunque ya esta última sí que es de composición.

Por ahora, para estudiar si una serie es o no de composición, no nos queda otra que realizar un análisis exhaustivo del retículo de subgrupos del grupo que consideremos, analizando solo las inclusiones de subgrupos que sean normales, algo que mostraremos en los siguientes ejemplos.

Ejemplo. Sea \mathbb{K} un cuerpo, sobre $\text{GL}_2(\mathbb{K})$ consideramos las matrices triangulares superiores:

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{K}^*, b \in \mathbb{K} \right\}$$

Que tiene infinitos elementos y no es un grupo abeliano, ya que:

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$$

Si consideramos ahora:

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{K} \right\}$$

Tenemos que $T \triangleright U \triangleright \{1\}$ es una serie de composición.

Notemos que:

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

Si ahora para $n > 2$ cogemos como T el conjunto de las matrices triangulares superiores y luego cogemos:

$$N = \{\text{matrices triangulares superiores con diagonal de ceros}\}$$

$$U_r = I + N^r$$

Tomando potencias los elementos van subiendo en la diagonal. Podemos considerar:

$$T \triangleright U_1 \triangleright U_2 \triangleright \dots \triangleright U_n = I$$

Ejemplo. Tratamos de buscar cuántas series de composición hay en los siguientes grupos:

- En S_3 , recordamos que el retículo de subgrupos que teníamos era:

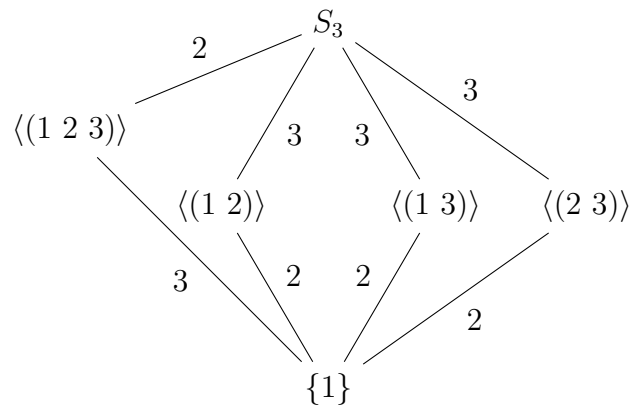
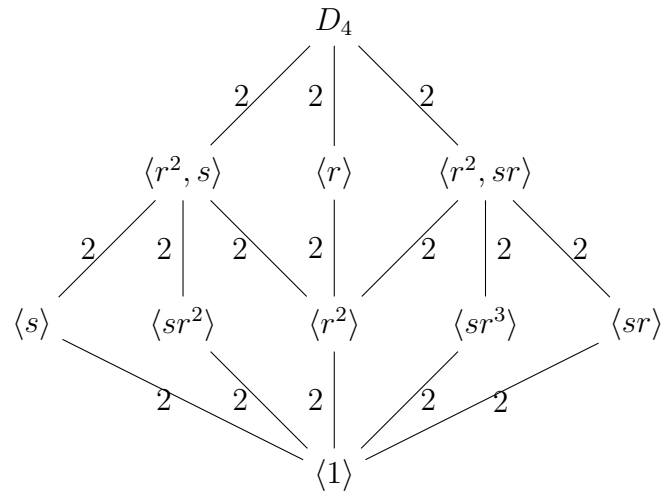


Figura 4.1: Diagrama de Hasse para los subgrupos de S_3 .

Como $A_3 = \langle (1\ 2\ 3) \rangle \triangleleft S_3$ (por tener índice 2) y ningún otro subgrupo de S_3 es normal salvo el trivial, la única serie de composición de S_3 es:

$$S_3 \triangleright A_3 \triangleright \{1\}$$

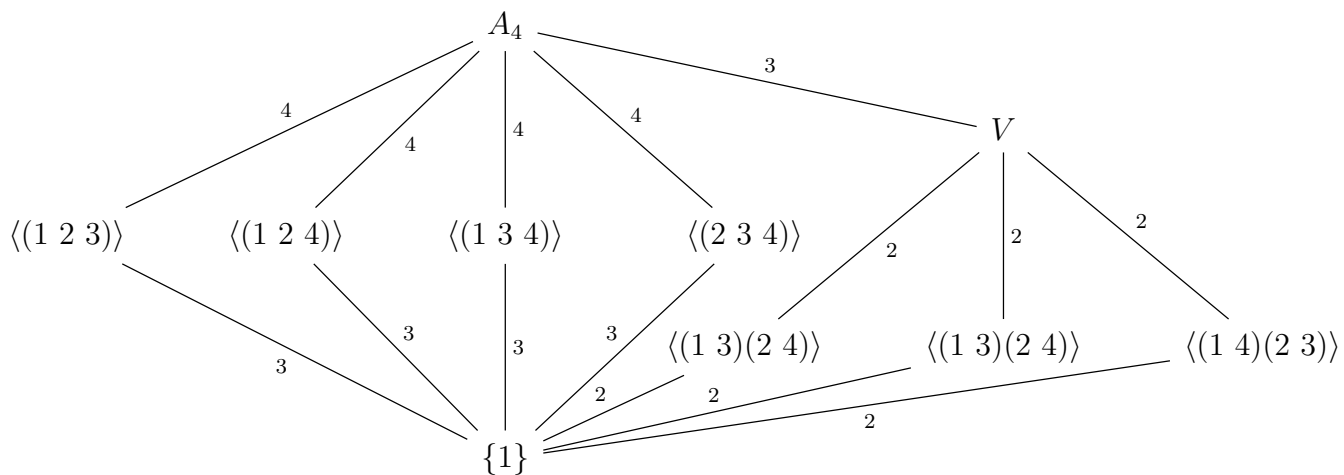
- En D_4 :

Figura 4.2: Diagrama de Hasse para los subgrupos de D_4 .

Como todos los índices del grafo son 2, todas las relaciones de inclusión mostradas en el grafo en realidad son relaciones de normalidad (\triangleleft), por lo que tenemos 7 series de composición distintas (una por cada forma que tengamos de llegar desde D_4 hasta $\{1\}$ en el grafo mediante caminos descendientes):

$$\begin{aligned}
 D_4 &\triangleright \langle r^2, s \rangle \triangleright \langle s \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, s \rangle \triangleright \langle sr^2 \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, s \rangle \triangleright \langle r^2 \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, sr \rangle \triangleright \langle r^2 \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, sr \rangle \triangleright \langle sr \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r^2, sr \rangle \triangleright \langle sr^3 \rangle \triangleright \{1\} \\
 D_4 &\triangleright \langle r \rangle \triangleright \langle r^2 \rangle \triangleright \{1\}
 \end{aligned}$$

■ Para A_4 :



Como $V \triangleleft A_4$, tenemos como series de composición:

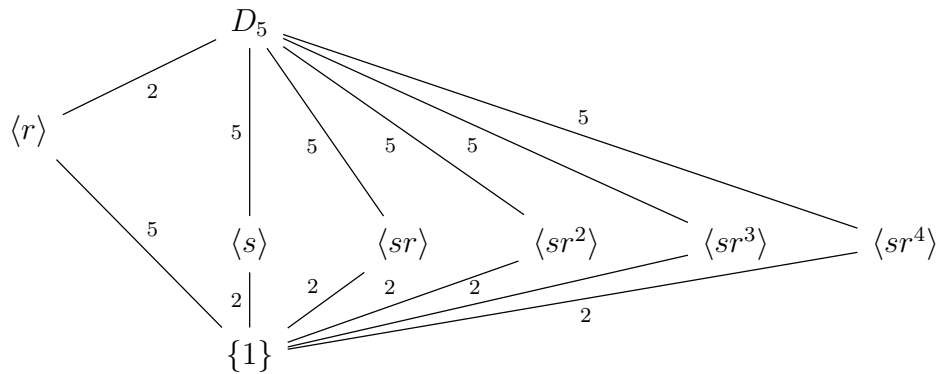
$$A_4 \triangleright V \triangleright \langle (1\ 2)(3\ 4) \rangle \triangleright \{1\}$$

$$A_4 \triangleright V \triangleright \langle (1\ 3)(2\ 4) \rangle \triangleright \{1\}$$

$$A_4 \triangleright V \triangleright \langle (2\ 3)(2\ 3) \rangle \triangleright \{1\}$$

Además, como ninguna de las relaciones $\langle (i\ j\ k) \rangle < A_4$ es normal, no tenemos más series de composición.

- En $D_5 = \langle r, s \mid r^5 = s^2 = 1, sr = r^4s \rangle$ tenemos:



Solo tenemos la serie de composición:

$$D_5 \triangleright \langle r \rangle \triangleright \{1\}$$

Ya que D_5 no tiene más subgrupos normales, a parte del trivial.

- En el grupo de los cuaternios:

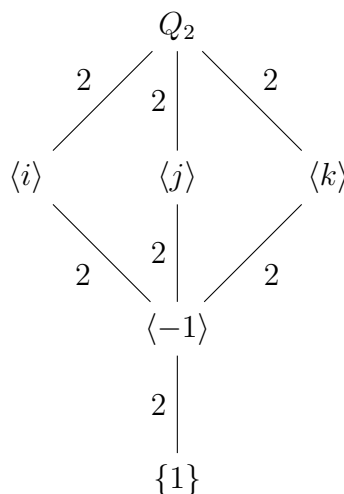


Figura 4.3: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

Como todas las aristas del grafo están numeradas con índice 2, todas las relaciones de subgrupo son normales, por lo que tenemos 3 series de composición,

una por cada camino posible:

$$Q_2 \triangleright \langle i \rangle \triangleright \langle -1 \rangle \triangleright \{1\}$$

$$Q_2 \triangleright \langle j \rangle \triangleright \langle -1 \rangle \triangleright \{1\}$$

$$Q_2 \triangleright \langle k \rangle \triangleright \langle -1 \rangle \triangleright \{1\}$$

- En $S_3 \times \mathbb{Z}_2$: Por una parte, en S_3 teníamos una única serie de composición:

$$S_3 \triangleright A_3 \triangleright \{1\}$$

Y en \mathbb{Z}_2 la única opción a considerar es $\mathbb{Z}_2 \triangleright \{0\}$. Podemos considerar ahora las series de composición resultantes de considerar todas las combinaciones:

$$S_3 \times \mathbb{Z}_2 \triangleright S_3 \times \{0\} \triangleright A_3 \times \{0\} \triangleright \{(1, 0)\}$$

$$S_3 \times \mathbb{Z}_2 \triangleright A_3 \times \mathbb{Z}_2 \triangleright A_3 \times \{0\} \triangleright \{(1, 0)\}$$

$$S_3 \times \mathbb{Z}_2 \triangleright A_3 \times \mathbb{Z}_2 \triangleright \{1\} \times \mathbb{Z}_2 \triangleright \{(1, 0)\}$$

Que obtenemos primero variando algunos y luego otras. Esto es posible ya que el producto de subgrupos es subgrupo del producto, como vimos en la Proposición 3.28.

Sin embargo, como $\text{mcd}(6, 2) = 2 \neq 1$, el Teorema 3.29 no puede asegurarnos que todos los subgrupos de $S_3 \times \mathbb{Z}_2$ sean producto de subgrupos, y de hecho vamos a tener que hay subgrupos del producto que no son producto de subgrupos de cada coordenada, por lo que tendremos otra serie de composición, que tendrá la forma:

$$S_3 \times \mathbb{Z}_2 \overset{2}{\triangleright} H_1 \overset{2}{\triangleright} H_2 \overset{3}{\triangleright} \{1\}$$

Con $H_1, H_2 < S_3 \times \mathbb{Z}_2$ que no especificaremos pero diremos que $H_1 \cong S_3$ y $H_2 \cong A_3$.

Definición 4.7 (Grupo simple). Un grupo G se dice simple si no es trivial y no tiene subgrupos normales propios

Ejemplo. \mathbb{Z}_3 es un grupo simple, ya que su retículo de subgrupos es:

$$\begin{array}{c} \mathbb{Z}_3 \\ | \\ \{0\} \end{array}$$

Un resultado que veremos luego (el Teorema de Abel) nos dirá que los grupos A_n para $n \geq 5$ son grupos simples.

Resultados sobre series de composición

Proposición 4.1. *Un grupo abeliano finito es simple si y solo si es un grupo cíclico de orden primo.*

Demostración. Por doble implicación:

\Leftarrow) Si G es cíclico de orden primo, no va a tener subgrupos propios, por lo que será simple.

\Rightarrow) Si G es abeliano, entonces todos sus subgrupos serán normales. Si es simple, no tendrá subgrupos propios (ya que si no serían normales, luego no sería simple). Sea $1 \neq x \in G$, sabemos que $\langle x \rangle < G$, de donde $\{1\} \neq \langle x \rangle$ y G no tiene subgrupos propios) $G = \langle x \rangle$, por lo que G es cíclico.

Si $|G| = nm$, entonces $1 \neq \langle x^m \rangle < G$, por lo que G tendría subgrupos propios, luego no sería simple. Por tanto, $|G|$ ha de ser primo.

□

Ejemplo. Estudiando un poco el caso de grupos cíclicos infinitos, \mathbb{Z} no es simple, ya que tiene subgrupos propios (que además son normales, por ser \mathbb{Z} abeliano).

Proposición 4.2 (Caracterización de series de composición). *Sea G un grupo, una serie normal es de composición si y solo si sus factores son grupos simples.*

Demostración. Consideramos una serie normal de longitud r :

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\}$$

Y demostraremos que la serie no es de composición si y solo si tiene un factor que no es un grupo simple:

\Rightarrow) Si la serie no es de composición, podemos encontrar $H < G$ de forma que la serie:

$$G = G_0 \triangleright \dots \triangleright G_{k-1} \triangleright H \triangleright G_k \triangleright \dots \triangleright G_r = \{1\}$$

Sea un refinamiento normal propio de la serie de partida. Si consideramos la proyección al cociente de los grupos:

$$G_{k-1} \triangleright H \triangleright G_k$$

Llegamos a que:

$$p_*(G_{k-1}) = G_{k-1}/G_k \triangleright p_*(H) = H/G_k \triangleright p_*(G_k) = \{G_k\}$$

Y ninguna de estas inclusiones es una igualdad, ya que:

- Si $G_{k-1}/G_k = H/G_k$, entonces $G_{k-1} = H$ y el refinamiento anterior no era propio.
- Si $H/G_k = \{G_k\}$, entonces $H = G_k$ y el refinamiento anterior no era propio.

En definitiva, hemos encontrado un subgrupo normal propio de G_{k-1}/G_k , por lo que este factor no es un grupo simple.

\Leftarrow) Si existe $k \in \{1, \dots, r\}$ de forma que G_{k-1}/G_k no es un grupo simple, entonces dicho grupo tendrá un subgrupo propio normal suyo:

$$\{G_k\} = \{1\} \neq H \triangleleft G_{k-1}/G_k$$

Si usamos el Tercer Teorema de Isomorfía considerando la proyección al cociente $p_k : G_{k-1} \rightarrow G_{k-1}/G_k$, tenemos que:

$$p_k^*(H) \triangleleft G_{k-1}$$

Además, como $H < G_{k-1}/G_k$, tendremos que $G_k \in H$, luego:

$$G_k = \ker(p_k) = p_k^*(\{G_k\}) \subseteq p_k^*(H) \triangleleft G_{k-1}$$

Y por ser $G_k \triangleleft G_{k-1}$, deducimos que también $G_k \triangleleft p_k^*(H)$. Hemos encontrado un subgrupo normal de G que estaría entre G_k y G_{k-1} :

$$G = G_0 \triangleright \dots \triangleright G_{k-1} \triangleright p_k^*(H) \triangleright G_k \triangleright \dots \triangleright G_r = \{1\}$$

Además, este refinamiento de la serie normal es propio, ya que:

- Si fuese $p_k^*(H) = G_k$, tendríamos que $H = \{G_k\}$.
- Si fuese $p_k^*(H) = G_{k-1}$, tendríamos que $H = G_{k-1}/G_k$.

Ambos casos son imposibles, puesto que H era un subgrupo propio de G_{k-1}/G_k . Hemos encontrado un refinamiento normal propio de la serie de partida, por lo que esta no era de composición.

□

Proposición 4.3. *Todo grupo finito tiene una serie de composición.*

Demostración. Sea G un grupo finito, distinguimos casos:

- Si G es el grupo trivial, es fácil hayar la serie de composición.
- Si G es simple, entonces no tiene subgrupos normales propios, por lo que tiene una única serie de composición:

$$G \triangleright \{1\}$$

- Si $|G| = p$ primo, vimos en la Proposición 2.14 que entonces G es cíclico, y la Proposición 4.1 nos dice que G es simple, por lo que estamos en el caso anterior.
- Si $|G|$ no es primo y G no es simple, por inducción sobre $n = |G|$, suponemos que es cierto para todo grupo H con $|H| < |G|$ (observemos que el punto anterior nos sirve como caso base).

Como G es finito, tiene un número finito de subgrupos, entre los que podemos encontrar (por ser G no simple) G_1 , un subgrupo normal propio maximal¹ de G . Como $|G_1| < |G|$ (G_1 es subgrupo propio), por hipótesis de inducción tenemos una serie de composición para G_1 :

$$G_1 \triangleright G_2 \triangleright \dots \triangleright G_r = \{1\}$$

Además, como G_1 era el subgrupo normal maximal de G , sabemos que no existe $H \triangleleft G$ con $G_1 \triangleleft H \triangleleft G$, por lo que la serie:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_r = \{1\}$$

Es de composición.

□

¹Es decir, que no existe $K \triangleleft G$ con $G_1 \triangleleft K$.

Teorema 4.4 (de Refinamiento de Schreier). *Sea G un grupo, dos series normales de G tienen refinamientos isomorfos.*

Demostración. Consideramos dos series normales de G :

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{i-1} \triangleright G_i \triangleright \dots \triangleright G_r = \{1\} \quad (4.3)$$

$$G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_{j-1} \triangleright H_j \triangleright \dots \triangleright H_s = \{1\} \quad (4.4)$$

Fijado $i \in \{1, \dots, r\}$, tenemos $G_i \triangleleft G_{i-1} < G$, y para todo $j \in \{1, \dots, s\}$ tenemos $H_j \triangleleft H_{j-1} < G$, donde podemos aplicar el primer apartado del Cuarto Teorema de Isomorfía, obteniendo la siguiente relación entre los grupos:

$$G_{ij} = G_i(H_j \cap G_{i-1}) \triangleleft G_i(H_{j-1} \cap G_{i-1}) = G_{ij-1} \quad \forall j \in \{1, \dots, s\}$$

En los casos extremos (es decir, en $j = 0$ y $j = s$), tendremos:

$$\begin{aligned} G_{i0} &= G_i(H_0 \cap G_{i-1}) = G_i G_{i-1} = G_{i-1} \\ G_{is} &= G_i(H_s \cap G_{i-1}) = G_i \{1\} = G_i \end{aligned}$$

De esta forma, tenemos para todo $i \in \{1, \dots, r\}$ que:

$$G_{i-1} = G_{i0} \triangleright G_{i1} \triangleright \dots \triangleright G_{is-1} \triangleright G_{is} = G_i$$

Que podemos meter en todos los eslabones de la serie (4.3):

$$\begin{aligned} G = G_0 = G_{10} \triangleright G_{11} \triangleright \dots \triangleright G_{1s} = G_1 = G_{20} \triangleright G_{21} \triangleright \dots \triangleright G_{2s} = G_2 = G_{30} \triangleright \dots \\ \dots \triangleright G_{r-1s} = G_{r-1} = G_{r0} \triangleright \dots \triangleright G_{rs} = G_r = \{1\} \end{aligned}$$

Obteniendo un refinamiento de longitud $r(s+1) - (r-1) = rs+1$:

En cada eslabón (teníamos r) hemos metido $s+1$ eslabones, de los que se repetían ($G_{is} = G_{i+1,0}$, para $i \in \{0, \dots, r-1\}$) $r-1$ eslabones.

Si repetimos el procedimiento para la serie (4.4), fijado $j \in \{1, \dots, s\}$, para todo $i \in \{0, \dots, r\}$ podemos aplicar el primer apartado del Cuarto Teorema de Isomorfía, obteniendo que:

$$H_{ij} = H_j(G_i \cap H_{j-1}) \triangleleft H_j(G_{i-1} \cap H_{j-1}) = H_{i-1j} \quad \forall i \in \{1, \dots, r\}$$

En los casos extremos tendremos:

$$\begin{aligned} H_{0j} &= H_{j-1} \\ H_{rj} &= H_j \end{aligned}$$

Por lo que para todo $j \in \{1, \dots, s\}$, tenemos:

$$H_{j-1} = H_{0j} \triangleright H_{1j} \triangleright \dots \triangleright H_{r-1j} \triangleright H_{rj} = H_j$$

Y podemos obtener un refinamiento de (4.4) al igual que hicimos antes, metiendo la cadena superior entre cada uno de los eslabones de la serie original:

$$G = H_0 = H_{01} \triangleright H_{11} \triangleright \dots \triangleright H_{r1} = H_1 = H_{02} \triangleright H_{12} \triangleright \dots \triangleright H_{r2} = G_2 = H_{03} \triangleright \dots \\ \dots \triangleright H_{rs-1} = H_{s-1} = H_{0s} \triangleright H_{1s} \triangleright \dots \triangleright H_{rs} = H_s = \{1\}$$

Que tiene longitud $s(r+1) - (s-1) = rs+1$, al igual que antes.

Ahora, por la segunda parte del Cuarto Teorema de Isomorfía, tenemos que:

$$\frac{G_{ij-1}}{G_{ij}} = \frac{G_i(H_j \cap G_{i-1})}{G_i(H_j \cap G_{i-1})} \cong \frac{H_j(G_{i-1} \cap H_{j-1})}{H_j(G_i \cap H_{j-1})} = \frac{H_{i-1j}}{H_{ij}}$$

Por lo que los dos refinamientos encontrados son isomorfos. \square

Ejercicio. Se pide calcular un refinamiento isomorfo aplicando el método de Schreier a las dos siguientes series normales:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 = \{1\} \\ G = H_0 \triangleright H_1 \triangleright H_2 = \{1\}$$

Teorema 4.5 (Jordan-Holder). *Si un grupo G admite una serie de composición, cualquier serie normal puede refinarse a una serie de composición.*

Además, dos series de composición de un mismo grupo son isomorfas siempre.

Demostración. Tomamos una serie de composición de G :

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\}$$

Y también una serie normal de G :

$$G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_s = \{1\}$$

Por el Teorema de Schreier (la serie de composición es normal), existe un refinamiento de ambos isomorfo. Sin embargo, como la primera serie es de composición, su refinamiento coincide con ella misma. Para la segunda serie, obtendremos un refinamiento isomorfo a la primera:

$$G = \overline{G_0} \triangleright \overline{G_1} \triangleright \dots \triangleright \overline{G_r} = \{1\}$$

\square

Con este último Teorema de Jordan-Holder se tiene claro ya el interés en las series de composición, ya que cada grupo admite una única (salvo isomorfismos) serie de composición.

Podemos pensar en calcular series de composición de un grupo conocida una serie de composición en un grupo isomorfo, resultado que podemos esperar que sea cierto (y que de hecho vamos a probar a continuación); sin embargo, el recíproco no es cierto en general: si tenemos dos series de composición, una de un grupo G y otra de otro grupo K que son isomorfas, en general G y K no van a ser isomorfos.

Ejemplo. Por ejemplo, anteriormente vimos en un ejemplo que la única serie de composición que podemos considerar en S_3 es:

$$S_3 \triangleright A_3 \triangleright \{1\}$$

En \mathbb{Z}_6 , que no es isomorfo a S_3 por ser abeliano, si observamos su retículo:

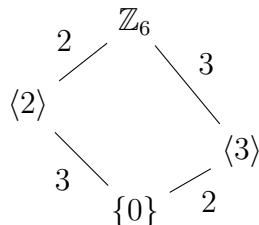


Figura 4.4: Diagrama de Hasse para los subgrupos de \mathbb{Z}_6 .

Vemos que una serie de composición de \mathbb{Z}_6 es:

$$\mathbb{Z}_6 \triangleright \langle 2 \rangle \triangleright \{0\}$$

Además, sabemos ahora por el Teorema de Jordan-Holder que \mathbb{Z}_6 no tiene más series de composición, ya que la otra posibilidad sería la serie:

$$\mathbb{Z}_6 \triangleright \langle 3 \rangle \triangleright \{0\}$$

Pero como esta no es isomorfa a la primera y sabemos que todas las series de composición de un mismo grupo son isomorfas, sabemos que esta segunda no es de composición. Veamos que las series:

$$S_3 \stackrel{2}{\triangleright} A_3 \stackrel{3}{\triangleright} \{1\}$$

$$\mathbb{Z}_6 \stackrel{2}{\triangleright} \langle 2 \rangle \stackrel{3}{\triangleright} \{0\}$$

Son isomorfas. Para ello, basta ver que:

$$\begin{aligned} S_3/A_3 &\cong \mathbb{Z}_2 \cong \mathbb{Z}_6/\langle 2 \rangle \\ A_3/\{0\} &\cong A_3 \cong \mathbb{Z}_3 \cong \langle 2 \rangle \cong \langle 2 \rangle/\{0\} \end{aligned}$$

Proposición 4.6. Sean G y K dos grupos isomorfos, entonces todas las series de composición de G son isomorfas a todas las series de composición de K .

El objetivo principal de esta asignatura es clasificar los grupos finitos. Como estos grupos van a tener series de composición cuyos factores serán grupos simples, nos centraremos en clasificar los grupos simples, para luego clasificar los grupos finitos.

La teoría de clasificación de grupos simples comenzó en 1960 y fue completada en 2004, con una demostración de 15000 páginas en lo que se conoce como el “Teorema enorme”. En la demostración intervinieron matemáticos como Gorestein (1923 - 1992). Esta clasificación de los grupos simples se hizo en:

- 18 familias infinitas de grupos simples.
- 26 grupos simples, llamados grupos esporádicos.

Como curiosidad, el grupo esporádico más pequeño tiene orden 7920 y el más grande, 10^{54} .

Cualquier grupo finito simple pertenece a una de estas 18 familias, o es isomorfo a alguno de los 26 grupos esporádicos.

Entre las 18 familias de grupos simples destacamos 2, que son las que nos interesan por ahora:

- Los grupos cíclicos de orden primo, que ya hemos demostrado que se tratan de grupos simples.
- Los grupos alternados A_n con $n \geq 5$.

Veremos ahora este segundo resultado, en el ya prometido Teorema de Abel.

Teorema 4.7 (de Abel). A_n es simple, para $n \geq 5$.

Demostración. Sea $\{1\} \neq N \triangleleft A_n$, veamos que ha de ser $N = A_n$. En la Proposición 1.20 vimos que dado² $j \in X_n \setminus \{1, 2\}$, teníamos que:

$$A_n = \langle (1 \ 2 \ j) \rangle$$

Y la demostración terminará viendo que N contiene a un elemento de esta forma. Bajo estas hipótesis, sabemos que va a existir (por ser N finito) $1 \neq \sigma \in N$, la permutación de N que mueve menos elementos. Por ser σ par (estamos en A_n), ha de mover más de dos elementos. Veamos que mueve exactamente 3:

1. Si σ es producto de ciclos disjuntos de longitud 2: supongamos que σ mueve, al menos, los elementos x_1, x_2, x_3 (distintos entre sí), con lo que podemos escribir:

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

Sea $\tau = (x_3 \ x_4 \ x_5)$ para ciertos $x_4, x_5 \in X_n$ distintos de x_1, x_2, x_3 y distintos entre sí, definimos:

$$\sigma_1 = (x_3 \ x_4 \ x_5)\sigma(x_3 \ x_4 \ x_5)^{-1} \in N$$

σ_1 está en N por ser $N \triangleleft A_n$. Si consideramos:

$$[\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} = \sigma_1\sigma^{-1} \in N$$

- Supongamos que σ mueve a x_5 , en cuyo caso:

$$\begin{aligned} \sigma &= (x_1 \ x_2)(x_3 \ x_4)(x_5 \ \sigma(x_5)) \dots \\ \sigma_1 &= (x_1 \ x_2)(x_3 \ \sigma(x_5))(x_4 \ x_5) \dots \end{aligned}$$

²Donde $X_n = \{1, 2, \dots, n\}$.

Con lo que:

$$[\tau, \sigma] = (x_3 \sigma(x_5))(x_4 x_5)(x_3 x_4)(x_5 \sigma(x_5))$$

Luego $[\tau, \sigma]$ deja fijos a x_1 y x_2 y mueve a los mismos que movía σ . Por ello, $[\tau, \sigma] \in N$ y $[\tau, \sigma]$ mueve menos elementos que σ , contradicción, que viene de suponer que σ mueve a x_5 .

- Si suponemos que σ no mueve a x_5 :

$$\sigma_1 = (x_1 x_2)(x_4 x_5)$$

Tenemos:

$$[\tau, \sigma] = (x_3 x_5 x_4)$$

Que mueve menos elementos que σ , contradicción.

Por tanto, σ no puede ser producto de transposiciones, ya que llegamos a contradicciones.

2. Si σ tiene un ciclo de longitud mayor o igual que 3 en el que mueve a x_1, x_2 y x_3 :

$$\begin{aligned}\tau &= (x_3 x_4 x_5) \\ \sigma_1 &= \tau \sigma \tau^{-1} \in N\end{aligned}$$

Supongamos que σ mueve más de 3 elementos, por lo que mueve al menos (por ser una permutación par) 5. En dicho caso:

$$\sigma_1 = (x_1 x_2 x_4 \dots) \neq \sigma$$

Por lo que:

$$[\tau, \sigma] = \sigma_1 \sigma^{-1} \in N$$

Y $[\tau, \sigma]$ deja fijos a los mismos que σ y a x_2 . En dicho caso, tenemos que $[\tau, \sigma]$ mueve menos que σ .

En definitiva, concluimos que σ contiene a un ciclo de longitud 3, a saber: $(i j k)$, todos ellos elementos distintos.

- Si $i, j, k, 1, 2$ son todos distintos:

$$(1 i)(2 j)(i j k)(1 i)(2 j) = (1 2 k) \in N$$

- Si $i = 1$ y $j, k, 2$ fueran distintos, $\exists h$ distinto de los anteriores de forma que:

$$(2 j)(k h)(1 j k)(2 j)(k h) = (1 2 h) \in N$$

- Si $i = 2$ y $j, k, 1$ fueran distintos, $\exists h$ distintos de los anteriores de forma que:

$$\dots = (1 2 h) \in N$$

En definitiva, N contiene al generador de A_n , de donde:

$$N = \langle (1 2 j) \rangle = A_n$$

□

4.2. Grupos resolubles

Antes de pasar con la definición de grupos resolubles, hemos de repasar ciertos conceptos relacionados con la operación de conmutador que ya definimos sobre los elementos de G , recordamos que era la aplicación $[\cdot, \cdot] : G \times G \rightarrow G$ dada por:

$$[x, y] = xy(yx)^{-1} = xyx^{-1}y^{-1} \quad \forall x, y \in G$$

4.2.1. Preliminares

Sobre el conmutador solo vimos la Proposición 3.26, que nos decía que dados dos elementos h, k de un grupo G :

$$hk = kh \iff [h, k] = 1$$

Proposición 4.8. Sea G un grupo y $x, y \in G$, se verifican:

$$i) [x, y]^{-1} = [y, x].$$

$$ii) z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}], \quad \forall z \in G.$$

Demostración. Veamos cada apartado:

i) Basta con ver:

$$[x, y][y, x] = xy(yx)^{-1}yx(xy)^{-1} = xy(xy)^{-1} = 1$$

ii) Sea $z \in G$, basta aplicar la definición del conmutador:

$$\begin{aligned} z[x, y]z^{-1} &= zxy(yx)^{-1}z^{-1} = zxy(x^{-1}y^{-1}z^{-1}) \\ [zxz^{-1}, zyz^{-1}] &= zxz^{-1}zyz^{-1}(zyz^{-1}zxz^{-1})^{-1} = zxyz^{-1}(zx^{-1}y^{-1}z^{-1}) \\ &= zxy(x^{-1}y^{-1}z^{-1}) \end{aligned}$$

□

Proposición 4.9. Sea G un grupo, el conjunto:

$$\langle [x, y] \mid x, y \in G \rangle$$

es un subgrupo normal de G .

Demostración. Llamando Λ a dicho conjunto, para ver que es un subgrupo, si $a, b \in \Lambda$, entonces $\exists n, m \in \mathbb{Z}$ de forma que:

$$a = ([x, y])^n \quad b = ([x, y])^m$$

En dicho caso:

$$ab^{-1} = ([x, y])^n ([x, y])^{-m} = ([x, y])^{n-m}$$

Con $n - m \in \mathbb{Z}$, por lo que $ab^{-1} \in \Lambda$, de donde $\Lambda < G$.

Ahora, para ver que $\Lambda \triangleleft G$, sea $a \in \Lambda$, existirán $n \in \mathbb{Z}$, $x, y \in G$ de forma que $a = ([x, y])^n$. Sea $z \in G$:

- Si $n = 1$:

$$z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}] \in \Lambda$$

- Si $n = -1$:

$$z([x, y])^{-1}z^{-1} = z[y, x]z^{-1} = [zyz^{-1}, zxz^{-1}] \in \Lambda$$

- Supuesto para $n - 1$, para n :

$$z([x, y])^n z^{-1} = z[x, y]z^{-1}z([x, y])^{n-1}z^{-1} = (z[x, y]z^{-1})(z([x, y])^{n-1}z^{-1})$$

Con $z[x, y]z^{-1} \in \Lambda$ por ser $[x, y] \in \Lambda$ y $z([x, y])^{n-1}z^{-1} \in \Lambda$ por hipótesis de inducción. Como $\Lambda < G$, concluimos que $z([x, y])^n z^{-1} \in \Lambda$. Escribiendo $m = -n$:

$$(z([x, y])^m z^{-1})^{-1} = z^{-1}([x, y])^{-m}z \in \Lambda$$

Por ser $\Lambda < G$, concluimos que $z([x, y])^m z^{-1} \in \Lambda$.

En definitiva, $\Lambda \triangleleft G$. □

Definición 4.8 (Subgrupo conmutador). Sea G un grupo, llamamos subgrupo conmutador de G al subgrupo:

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle$$

Observemos que como $hk = kh \iff [h, k] = 1$, este grupo está generado por los conmutadores de los elementos que no conmutan entre sí:

$$[G, G] = \langle [x, y] \mid xy \neq yx \rangle$$

Proposición 4.10. Sea G un grupo, $G/[G, G]$ es abeliano. Más aún, es el menor subgrupo normal de G que hace que el cociente sea abeliano. Es decir, si $N \triangleleft G$:

$$G/N \text{ es abeliano} \iff [G, G] < N$$

$G/[G, G]$ recibe el nombre de grupo abelianizado de G .

Demostración. Si demostramos la doble implicación, como $[G, G] < [G, G]$, tendremos que $G/[G, G]$ es abeliano, por lo que solo tenemos que probar esto:

\implies) Si consideramos la proyección al cociente $p : G \rightarrow G/N$, sea $a \in [G, G]$, entonces existirán $n \in \mathbb{Z}$ y $x, y \in G$ de forma que:

$$a = ([x, y])^n$$

Si calculamos la imagen de a por p (que recordamos que es un homomorfismo):

$$\begin{aligned} p(a) &= (p([x, y]))^n = (p(xy(yx)^{-1}))^{-1} = (p(xy))^n (p(yx))^{-n} \\ &\stackrel{(*)}{=} (p(x))^n (p(y))^n (p(y))^{-n} (p(x))^{-n} = 1 \end{aligned}$$

Donde en $(*)$ hemos usado que G/N es abeliano. Tenemos que $a \in \ker(p) = N$.

\Longleftarrow) Sean $x, y \in G$, entonces:

$$xy(yx)^{-1} = [x, y] \in [G, G] < N$$

Pero:

$$(xN)(yN) = xyN = yxN = (yN)(xN) \Longleftrightarrow xy(yx)^{-1}N = N$$

Por lo que $(xN)(yN) = (yN)(xN)$, para todos $x, y \in G$.

□

Corolario 4.10.1. Si G es un grupo:

$$G \text{ abeliano} \Longleftrightarrow [G, G] = \{1\}$$

Demostración. Como $G \cong G/\{1\}$:

$$G \text{ abeliano} \Longleftrightarrow G/\{1\} \text{ abeliano} \Longleftrightarrow [G, G] < \{1\} \Longleftrightarrow [G, G] = \{1\}$$

□

Ejercicio. Se pide comprobar que:

$$[A_3, A_3] = \{1\}$$

$$[S_3, S_3] = A_3$$

$$[A_4, A_4] = V$$

4.2.2. Definición

Definición 4.9 (Serie derivada). La serie derivada de un grupo G es la cadena de subgrupos normales:

$$G = G^0 \triangleright G' \triangleright G'' \triangleright \dots \triangleright G^{(k)} \triangleright \dots$$

Donde:

$$G^{(k+1)} = [G^{(k)}, G^{(k)}]$$

De esta forma, el subgrupo $G' = [G, G]$ recibe el nombre de subgrupo derivado de G , o primer derivado de G .

Un grupo G se dice resoluble si existe un índice k de forma que $G^{(k)} = \{1\}$. Es decir, la serie derivada de G alcanza el $\{1\}$.

Ejemplo. Veamos que:

- Si G es abeliano, entonces G es resoluble:

$$G' = [G, G] = \{1\}$$

Por lo que la serie derivada es:

$$G \triangleright G' = \{1\}$$

- S_3 es resoluble:

$$\begin{aligned} S'_3 &= [S_3, S_3] = A_3 \\ S''_3 &= A'_3 = [A_3, A_3] = \{1\} \end{aligned}$$

Y la serie derivada es:

$$S_3 \triangleright A_3 \triangleright \{1\}$$

- A_4 es resoluble:

$$\begin{aligned} A'_4 &= [A_4, A_4] = V \\ A''_4 &= V' = [V, V] = \{1\} \end{aligned}$$

Y la serie derivada es:

$$A_4 \triangleright V \triangleright \{1\}$$

- S_4 es resoluble, ya que $S'_4 = [S_4, S_4] = A_4$ y ya tenemos la serie de A_4 :

$$S_4 \triangleright A_4 \triangleright V \triangleright \{1\}$$

En general, si G es un grupo cuyo grupo derivado es resoluble, entonces G será resoluble.

- A_5 no es resoluble:

$$A'_5 = [A_5, A_5] \neq \{1\}$$

Ya que A_5 no es abeliano, pero como A_5 es simple, no tiene subgrupos normales propios, con lo que $A'_5 = A_5$. La serie derivada será:

$$A_5 \triangleright A_5 \triangleright A_5 \triangleright \dots$$

En general, ningún grupo no abeliano y simple es resoluble.

- S_n no es resoluble para $n \geq 5$, ya que:

$$[S_n, S_n] = A_n \quad \forall n \geq 3$$

Y como ya vimos lo que le pasa a A_n para $n \geq 5$, la serie derivada de S_n será:

$$S_n \triangleright A_n \triangleright A_n \triangleright \dots$$

Teorema 4.11 (Caracterización de grupos resolubles para grupos finitos).

Si G es un grupo finito, son equivalentes:

- i) G es resoluble.
- ii) G tiene una serie normal con factores abelianos.
- iii) Los factores de composición de G son cíclicos de orden primo.
- iv) G tiene una serie normal con factores cíclicos.

Demostración. Veamos todas las implicaciones:

$i) \implies ii)$ Si G es resoluble, la serie derivada será de la forma:

$$G = G^0 \triangleright G' \triangleright \dots \triangleright G^{(r)} = \{1\}$$

Que es una serie normal con factores abelianos, ya que los factores son de la forma:

$$G^{(k-1)}/G^{(k)} = G^{(k-1)} / [G^{(k-1)}, G^{(k-1)}]$$

Que ya vimos en la Proposición 4.10 que siempre era un grupo abeliano.

$ii) \implies iii)$ Si tenemos una serie normal con factores abelianos:

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_s = \{1\}$$

Por el Teorema de Jordan-Holder, podemos refinarla a una serie de composición, donde nos fijaremos ahora en lo que pasa entre dos eslabones de la serie original:

$$\dots \triangleright G_r \triangleright H_{r1} \triangleright H_{r2} \triangleright \dots \triangleright H_{rs} \triangleright G_{r+1} \triangleright \dots$$

Por hipótesis los factores son abelianos, es decir, los grupos:

$$G_{k-1}/G_k \quad \forall k \in \{1, \dots, s\}$$

son abelianos. Por consiguiente, como todo subgrupo de un grupo abeliano también es abeliano, tenemos que los siguientes cocientes también son abelianos:

$$H_{r1}/G_{r+1} \quad H_{r2}/G_{r+1} \quad \dots \quad H_{rs}/G_{r+1} \quad < \quad G_r/G_{r+1}$$

Por tanto, los factores:

$$\begin{aligned} G_r/H_{r1} &\cong \frac{G_r/G_{r+1}}{H_{r1}/G_{r+1}} \\ H_{r1}/H_{r2} &\cong \frac{H_{r1}/G_{r+1}}{H_{r2}/G_{r+1}} \\ &\vdots \\ H_{rs-1}/H_{rs} &\cong \frac{H_{rs-1}/G_{r+1}}{H_{rs}/G_{r+1}} \end{aligned}$$

Son abelianos, por ser isomorfos a un cociente de un grupo abeliano. En definitiva, todos los factores de composición son abelianos, finitos y simples (por ser factores de composición), luego son cíclicos de orden primo, por la Proposición 4.1.

$iii) \implies iv)$ Como las series de composición son, en particular, series normales, cualquier³ serie de composición de G será normal con factores cíclicos.

³Gracias al Teorema de Jordan-Holder.

$iv) \implies i)$ Consideramos una serie normal con factores cíclicos (luego abelianos):

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_r = \{1\}$$

Veamos que $G^{(k)} < G_k$, para todo $k \in \{1, \dots, r\}$: como G_{k-1}/G_k es abeliano por ser un factor, entonces por la Proposición 4.10:

$$[G_{k-1}, G_{k-1}] = G^{(k)} < G_k$$

En particular:

$$G^{(r)} < G_r = \{1\}$$

Y tenemos ya que la serie derivada alcanza el mínimo:

$$G = G^0 \triangleright G' \triangleright \dots \triangleright G^{(r)} = \{1\}$$

Por lo que G es resoluble. □

Ejemplo. Aplicaciones del Teorema son:

- Vimos ya que S_4 era resoluble, veámoslo de otra forma:

$$S_4 \triangleright A_4 \triangleright V \triangleright \{1\}$$

Es una serie normal con factores cíclicos abelianos:

$$S_4/A_4 \quad A_4/V \quad V/\{1\}$$

- En D_n :

$$D_n \triangleright \langle r \rangle \triangleright \{1\}$$

Es una serie normal con factores cíclicos abelianos, luego D_n es resoluble.

Una estrategia muy usada a la hora de comprobar si un grupo es resoluble o no es buscar si nuestro grupo tiene un subgrupo normal resoluble que haga que el cociente sea resoluble, con lo que podemos aplicar el tercer apartado de la siguiente Proposición:

Proposición 4.12. *Se verifica que:*

- i) Todo subgrupo de un grupo resoluble es resoluble.*
- ii) Todo cociente de un grupo resoluble es resoluble.*
- iii) Si $N \triangleleft G$ y N y G/N son resolubles, entonces G es resoluble.*

Demostración. Veamos cada una:

- i)* Supongamos que la serie derivada de G es:

$$G = G^0 \triangleright G' \triangleright G'' \triangleright \dots \triangleright G^{(r)} = \{1\}$$

Si $H < G$, entonces $H^{(k)} < G^{(k)}$ para todo $k \in \{1, \dots, r\}$. Como tenemos que $G^{(r)} = \{1\}$, tendremos que $H^{(r)} = \{1\}$, por lo que H es resoluble.

ii) Supuesto que G es resoluble con la serie anterior, consideramos $N \triangleleft G$. Por inducción, tendremos que:

$$(G/N)^{(k)} = G^{(k)}N/N$$

Y como $G^{(r)} = \{1\}$, entonces:

$$(G/N)^{(r)} = \{1\} \implies G/N \text{ resoluble}$$

iii) Si $N \triangleleft G$ y G/N son resolubles: por ser G/N resoluble, entonces $\exists s$ de forma que:

$$G^{(s)}N/N = (G/N)^{(s)} = \{1\}$$

En dicho caso:

$$G^{(s)} < N$$

Y como N es resoluble, $\exists t$ de forma que $N^{(t)} = \{1\}$. En dicho caso:

$$G^{(s+t)} < N^{(t)} = \{1\}$$

□

Para concluir los resultados sobre grupos resolubles, veamos qué pasa con el producto de grupos resolubles:

Corolario 4.12.1. *Cualquier producto finito de grupos resolubles es resoluble.*

Demostración. Suponiendo que G_1 y G_2 son resolubles, cada uno tendrá su serie derivada. Tenemos:

$$G_2 \cong \{1\} \times G_2 < G_1 \times G_2$$

Con $\{1\} \times G_2$ resoluble por ser isomorfo a G_2 . Además, $\{1\} \times G_2 \triangleleft G_1 \times G_2$. Busquemos el cociente:

$$G_1 \times G_2 / \{1\} \times G_2 \cong G_1$$

Que es resoluble, por lo que usando el apartado 3 de la Proposición superior, concluimos que $G_1 \times G_2$ es resoluble.

Por hipótesis de inducción, fijada una coordenada, movemos todas las demás. □

5. G –conjuntos y p -grupos

Definición 5.1. Sea G un grupo y X un conjunto no vacío, una acción¹ de G sobre X es una aplicación:

$$\begin{aligned} ac : G \times X &\longrightarrow X \\ (g, x) &\longmapsto ac(g, x) \end{aligned}$$

Que verifica:

$$i) \quad ac(1, x) = x \quad \forall x \in X.$$

$$ii) \quad ac(g, ac(h, x)) = ac(gh, x) \quad \forall x \in X, \quad \forall g, h \in G.$$

En dicho caso, diremos que G actúa² (o que opera) sobre X .

Si G actúa sobre X , diremos que este conjunto X es el G –conjunto a izquierda. A la aplicación ac se le llama aplicación de la G –estructura.

Notación. Si $ac : G \times X \rightarrow X$ es una acción de G sobre X , es común denotar:

$$ac(g, x) = {}^g x = g \cdot x = g * x$$

En este documento, usaremos la notación $ac(g, x) = {}^g x$.

Con esta notación, las propiedades que ha de cumplir una aplicación $ac : G \times X \rightarrow X$ para ser una acción son:

$$i) \quad {}^1 x = x \quad \forall x \in X.$$

$$ii) \quad {}^g ({}^h x) = {}^{gh} x \quad \forall x \in X, \quad \forall g \in G.$$

Ejemplo. Si G es un grupo y X es un conjunto no vacío, ejemplos de acciones de G sobre X son:

1. La acción trivial:

$$\begin{aligned} ac : G \times X &\longrightarrow X \\ (g, x) &\longmapsto x \end{aligned}$$

2. Si tenemos una acción $ac : G \times X \rightarrow X$ y $H < G$, podemos considerar la acción por restricción $ac : H \times X \rightarrow X$, dada por:

$$ac(h, x) = ac(i(h), x) \quad \forall h \in H, x \in X$$

Donde consideramos la aplicación inclusión $i : H \rightarrow G$ dada por $i(h) = h$, para todo $h \in H$.

¹En realidad esta es la definición de acción por la izquierda, pero no vamos a trabajar con las acciones por la derecha, por lo que hablaremos simplemente de acciones.

²En realidad deberíamos decir que “ G actúa por la izquierda sobre X ”.

3. Dado $n \in \mathbb{N}$, si $X = \{1, \dots, n\}$ y $G = S_n$, la acción natural de S_n sobre X será la acción $ac : S_n \times X \rightarrow X$ dada por:

$$ac(\sigma, k) = {}^\sigma k = \sigma(k) \quad \forall \sigma \in S_n, k \in X$$

Proposición 5.1. *Sea G un grupo y X un conjunto no vacío, dar una acción de G sobre X equivale a dar un homomorfismo de grupos de G en $\text{Perm}(X)$.*

Demostración. Veamos que es posible:

- Por una parte, dada una acción de G sobre X , $ac : G \times X \rightarrow X$, podemos definir la aplicación:

$$\begin{aligned} \phi : G &\longrightarrow \text{Perm}(X) \\ g &\longmapsto \phi(g) \end{aligned}$$

Donde $\phi(g)$ es una aplicación $\phi(g) : X \rightarrow X$ dada por:

$$\phi(g)(x) = {}^g x \quad \forall x \in X$$

Veamos en primer lugar que ϕ está bien definida, es decir, que $\phi(g) \in \text{Perm}(X)$ para cada $g \in G$. Para ello, veamos antes que ϕ cumple:

- $\phi(1) = id_X$, ya que la aplicación $x \mapsto ac(1, x)$ es la aplicación identidad en X , por ser ac una acción de G sobre X .
- $\phi(g)\phi(h) = \phi(gh)$, ya que al evaluar en cualquier $x \in G$:

$$(\phi(g)\phi(h))(x) = \phi(g)(\phi(h)(x)) = \phi(g)({}^h x) = {}^g({}^h x) \stackrel{(*)}{=} {}^{gh} x = \phi(gh)(x)$$

Donde en $(*)$ hemos usado que ac es una acción de G sobre X .

Ahora, veamos que dado $g \in G$, la aplicación $\phi(g)$ es biyectiva (es decir, está en $\text{Perm}(X)$), ya que su aplicación inversa es $\phi(g^{-1})$:

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(1) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

Y anteriormente vimos que $\phi(1) = id_X$, por lo que $\phi(g) \in \text{Perm}(X)$, para todo $g \in G$ y la aplicación ϕ está bien definida.

Además, por las dos propiedades anteriores, tenemos que ϕ es un homomorfismo de grupos.

- Sea $\phi : G \rightarrow \text{Perm}(X)$ un homomorfismo de grupos, definimos la aplicación $ac : G \times X \rightarrow X$ dada por:

$$ac(g, x) = \phi(g)(x) \quad \forall g \in G, x \in X$$

Veamos que es una acción:

$$\begin{aligned} ac(1, x) &= \phi(1)(x) = x \quad \forall x \in X \\ ac(g, ac(h, x)) &= \phi(g)(\phi(h)(x)) = \phi(gh)(x) = ac(gh, x) \quad \forall x \in X, \quad \forall g, h \in G \end{aligned}$$

□

Definición 5.2 (Representación por permutaciones). Sea G un grupo y X un conjunto no vacío, si tenemos una acción de G sobre X , el homomorfismo ϕ dado por esta acción según la Proposición 5.1 recibirá el nombre de representación de G por permutaciones.

Además, llamaremos a $\ker(\phi)$ núcleo de la acción, ya que:

$$\ker(\phi) = \{g \in G \mid \phi(g) = id_X\} = \{g \in G \mid {}^g x = x \quad \forall x \in X\}$$

En el caso de que $\ker(\phi) = \{1\}$, diremos que la acción es fiel.

Ejemplo. A continuación, damos varios ejemplos de acciones, consideraremos en cada caso su representación por permutaciones:

1. La representación por permutaciones de la acción trivial es el homomorfismo $\phi : G \rightarrow Perm(X)$ dado por:

$$\phi(g) = id_X \quad \forall g \in G$$

2. Si tenemos una acción $ac : G \times X \rightarrow X$ sobre un grupo G y un conjunto no vacío X que tiene asociada una representación por permutaciones ϕ , entonces la acción por restricción $ac : H \times X \rightarrow X$ tendrá asociada como representación por permutaciones el homomorfismo $\phi_H : H \rightarrow Perm(X)$ dado por:

$$\phi_H = \phi \circ i$$

Siendo $i : H \rightarrow G$ la aplicación inclusión.

3. En el caso de la acción natural de S_n sobre $X = \{1, \dots, n\}$, tenemos que la representación por permutaciones es el homomorfismo $\phi : S_n \rightarrow Perm(X)$ dado por:

$$\phi(\sigma) = \sigma \quad \forall \sigma \in S_n$$

Es decir, $\phi = id_{S_n}$.

4. Sea G un grupo, podemos definir la acción por traslación como:

$$\begin{aligned} ac : G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh \end{aligned}$$

Y el homomorfismo asociado a la acción como representación por permutaciones será $\phi : G \rightarrow Perm(G)$ dado por:

$$\phi(g)(h) = gh \quad \forall g, h \in G$$

Como además:

$$\ker(\phi) = \{g \in G \mid gh = h \quad \forall h \in G\} = \{1\}$$

Tenemos que es una acción fiel.

Teorema 5.2 (Cayley). *Todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones.*

Demostración. Sea G un grupo finito, consideramos la acción por traslación:

$$\begin{aligned} ac : G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh \end{aligned}$$

Y su representación por permutaciones, $\phi : G \rightarrow \text{Perm}(G)$ dado por:

$$\phi(g)(h) = gh \quad \forall g \in G, \forall h \in G$$

Como la acción por traslación es una acción fiel, tendremos que $\ker(\phi) = \{1\}$ y aplicando el Primer Teorema de Isomorfía sobre ϕ , obtenemos que:

$$G \cong G/\{1\} \cong \text{Im}(\phi)$$

Donde $\text{Im}(\phi) = \phi_*(G)$, que en la Proposición 2.3 vimos que es un subgrupo de $\text{Perm}(G)$. \square

Ejemplo. Podemos considerar las traslaciones de G sobre conjuntos especiales:

- La acción por traslación de G sobre $\mathcal{P}(G)$ será $ac : G \times \mathcal{P}(G) \rightarrow \mathcal{P}(G)$ dada por:

$$ac(g, A) = gA = \{ga \mid a \in A\} \subseteq G \quad \forall A \in \mathcal{P}(G)$$

- Podemos también considerar la acción por traslación en el cociente por las clases laterales por la izquierda³: si $H < G$, consideramos el cociente de G sobre H por la izquierda y la acción $ac : G \times G/H \rightarrow G/H$ dada por:

$$ac(g, xH) = {}^g(xH) = gxH = \{gxh \mid h \in H\}$$

6. La acción por conjugación se define como $ac : G \times G \rightarrow G$ dada por:

$$ac(g, h) = {}^g h = ghg^{-1}$$

Que es una acción, ya que:

$$\begin{aligned} {}^1 h &= 1h1^{-1} = h \quad \forall h \in G \\ {}^g({}^h l) &= g {}^h l g^{-1} = gh l h^{-1} g^{-1} gh l (gh)^{-1} = {}^{gh} l \quad \forall g, h, l \in G \end{aligned}$$

El homomorfismo asociado es:

$$\begin{aligned} \phi : G &\rightarrow \text{Perm}(X) \\ \phi(g)(h) &= ghg^{-1} \quad \forall g, h \in G \end{aligned}$$

Y a $\phi(g)$ lo llamábamos (en el ej 14 de la relación 4, φ_g) automorfismo interior definido por G , con imagen:

$$\text{Im}(\phi) = \text{Int}(G)$$

El núcleo en este caso es:

$$\ker(\phi) = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg \quad \forall h \in G\} = Z(G)$$

³No es necesario considerar $H \triangleleft G$, ya que solo consideramos conjuntos no vacíos, por lo que no es necesario que el cociente tenga estructura de grupo.

7. La acción por conjugación en partes de G se define como la aplicación $ac : G \times \mathcal{P}(G) \rightarrow \mathcal{P}(G)$ dada por:

$$ac(g, A) = {}^g A = gAg^{-1} = \{gag^{-1} \mid a \in A\} \subseteq G \quad \forall A \in \mathcal{P}(G)$$

8. Podemos definir la acción por conjugación de G también sobre $Subg(G)$:

$$Subg(G) = \{H \subseteq G \mid H < G\}$$

Como la aplicación $ac : G \times Subg(G) \rightarrow Subg(G)$ dada por:

$$ac(g, H) = {}^g H = gHg^{-1} < G$$

Ya que en la Proposición 3.1 vimos que gHg^{-1} era un subgrupo de G , al que llamaremos subgrupos conjugado de G .

5.1. Órbitas de un elemento

Definición 5.3 (Órbita). Sea G un grupo y X un G -conjunto, definimos en X una relación de equivalencia \sim dada por:

$$y \sim x \iff \exists g \in G \mid y = {}^g x$$

La clase de equivalencia de cada $x \in X$ se llama órbita de x , denotada por:

$$Orb(x) = \{y \in X \mid y = {}^g x, g \in G\}$$

Tenemos de esta forma que el conjunto cociente X/\sim es el conjunto de las órbitas.

Ejemplo. Sobre $X = \{1, 2, 3, 4\}$: En S_4 consideramos $ac : S_4 \times X \rightarrow X$, la acción natural de S_4 sobre X :

$$ac(\sigma, k) = {}^\sigma k = \sigma(k)$$

- Si tenemos $H = \langle (1\ 2\ 3) \rangle$. Queremos calcular las órbitas de los elementos del H :

$$Orb(1) = \{k \in X \mid \exists \sigma \in H \text{ con } \sigma(k) = 1\} = \{1, 2, 3\}$$

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

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

$$Orb(4) = \{4\}$$

Donde pensamos en $Orb(k)$ como en los elementos de X desde los que podemos llegar a k con una permutación de H .

- En A_4 :

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

Como tenemos todos los 3-ciclos:

$$Orb(1) = X$$

Y también tendremos que $Orb(k) = X$, para $k \in X$.

- En V , que contiene a todos los 2-ciclos, la situación será la misma:

$$\text{Orb}(k) = X \quad \forall k \in X$$

- En $H = \langle (1\ 2\ 3\ 4) \rangle$ sucede lo mismo:

$$\text{Orb}(k) = X \quad \forall k \in X$$

Definición 5.4. Si el conjunto de órbitas X/\sim es unitario, decimos que la acción es transitiva.

Este nombre se debe a que dados $x, y \in X$, siempre $\exists g \in G$ de forma que:

$$y = {}^g x$$

Definición 5.5 (Estabilizador). Sea G un grupo y X un G -conjunto, definimos el grupo de estabilizadores de $x \in X$ en G como:

$$\text{Stab}_G(x) = \{g \in G \mid {}^g x = x\}$$

También se le llama grupo de isotropía.

Proposición 5.3. Sea G un grupo y X un G -conjunto:

$$\text{Stab}_G(x) < G \quad \forall x \in X$$

Demostración. Fijado $x \in X$, es claro que $\text{Stab}_G(x) \subseteq G$. Vemos que:

- $1 \in \text{Stab}_G(x)$, ya que ${}^1 x = x$ por definición de acción.
- Si $g \in \text{Stab}_G(x)$, supongamos que $g^{-1} \notin \text{Stab}_G(x)$, con lo que ${}^{g^{-1}} x = y \in X$ con $y \neq x$. En dicho caso:

$$x = {}^1 x = {}^{g^{-1}g} x = {}^{g^{-1}} ({}^g x) = {}^{g^{-1}} x = y$$

Llegamos a una contradicción, luego $g^{-1} \in \text{Stab}_G(x)$ para todo $g \in \text{Stab}_G(x)$.

- Finalmente, si $g, h \in \text{Stab}_G(x)$, entonces:

$${}^{gh} x = {}^g ({}^h x) = {}^g x = x$$

Por lo que $gh \in \text{Stab}_G(x)$.

□

Ejemplo. Si nuevamente sobre $X = \{1, 2, 3, 4\}$ volvemos a considerar la acción natural de S_4 sobre X :

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

$$\text{Stab}_H(1) = \{\sigma \in H \mid \sigma(1) = 1\} = \{1\}$$

$$\text{Stab}_H(2) = \{1\}$$

$$\text{Stab}_H(3) = \{1\}$$

$$\text{Stab}_H(4) = H$$

- En A_4 :

$$\text{Stab}_{A_4}(1) = \{1, (2\ 3\ 4), (2\ 4\ 3)\} = \langle (2\ 3\ 4) \rangle$$

$$\text{Stab}_{A_4}(2) = \langle (1\ 3\ 4) \rangle$$

$$\text{Stab}_{A_4}(3) = \langle (1\ 2\ 4) \rangle$$

$$\text{Stab}_{A_4}(4) = \langle (1\ 2\ 3) \rangle$$

- En V :

$$\text{Stab}_V(k) = \{1\} \quad \forall k \in X$$

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

$$\text{Stab}_H(k) = \{1\} \quad \forall k \in X$$

Vamos a poder establecer una relación entre el orden de las órbitas y del conjunto cociente.

Proposición 5.4. *Sea G un grupo finito que actúa sobre X , entonces para cada $x \in X$, $\text{Orb}(x)$ es un conjunto finito y:*

$$|\text{Orb}(x)| = [G : \text{Stab}_G(x)]$$

En particular, el cardinal de la órbita es un divisor del orden de G .

Demostración. Fijado $x \in X$, si consideramos $\text{Stab}_G(x) < G$ y las clases laterales por la izquierda, $G/\text{Stab}_G(x) \sim$. Podemos considerar la aplicación $\phi : G/\text{Stab}_G(x) \rightarrow \text{Orb}(x)$ dada por:

$$\phi(g\text{Stab}_G(x)) = {}^g x \quad \forall g \in G$$

- Veamos que está bien definida. Para ello, sean $g, g' \in G$ de forma que:

$$g\text{Stab}_G(x) = g'\text{Stab}_G(x)$$

Entonces, existirá $h \in \text{Stab}_G(x)$ de forma que $g = g'h$. En dicho caso:

$${}^g x = {}^{g'h} x = {}^{g'} ({}^h x) = {}^{g'} x$$

Por lo que $\phi(g\text{Stab}_G(x)) = \phi(g'\text{Stab}_G(x))$.

- Veamos que es sobreyectiva: sea $y \in \text{Orb}(x)$, vemos que $\exists g \in G$ de forma que:

$$y = {}^g x$$

Por lo que $y = \phi(g\text{Stab}_G(x))$.

- Para la inyectividad, sean $g, g' \in G$ de forma que:

$${}^g x = \phi(g\text{Stab}_G(x)) = \phi(g'\text{Stab}_G(x)) = {}^{g'} x$$

Entonces, podemos escribir:

$$x = {}^{g^{-1}} ({}^g x) = {}^{g^{-1}} ({}^{g'} x) = {}^{g^{-1}g'} x$$

De donde concluimos que $g^{-1}g' \in \text{Stab}_G(x)$, por lo que $g\text{Stab}_G(x) = g'\text{Stab}_G(x)$. \square

Observación. La demostración es cierta sin suponer que G sea un grupo finito, salvo para concluir que $|Orb(x)|$ es un divisor de $|G|$.

Ejemplo. En el ejemplo de antes:

■ Tenemos:

$$|Orb(1)| = \{1, 2, 3\}$$

Y también que:

$$[H : Stab_H(1)] = \frac{|H|}{|Stab_H(1)|} \implies |Stab_H(1)| = 1$$

Proposición 5.5. Sea G un grupo que actúa sobre X , si $x, y \in X$ están en la misma órbita, entonces $Stab_G(x)$ y $Stab_G(y)$ son subgrupos conjugados.

Demostración. Si x e y están en la misma órbita, entonces $Orb(x) = Orb(y)$, por lo que $\exists g \in G$ de forma que $y = {}^g x$. En dicho caso, también tenemos que: $x = {}^{g^{-1}} y$. Veamos que:

$$Stab_G(y) = gStab_G(x)g^{-1}$$

Para ello:

\subseteq) Sea $h \in Stab_G(x)$:

$$ghg^{-1}y = {}^{gh}({}^{g^{-1}}y) = {}^{gh}x = {}^g({}^h x) = {}^g x = y$$

Entonces, $ghg^{-1} \in Stab_G(y)$, por lo que $gStab_G(x)g^{-1} \subseteq Stab_G(y)$.

\supseteq) Sea ahora $h \in Stab_G(y)$:

$$g^{-1}hg x = x \implies g^{-1}Stab_G(y)g \subseteq Stab_G(x)$$

Y multiplicando por g y g^{-1} tenemos la otra inclusión:

$$Stab_G(y) \subseteq gStab_G(x)g^{-1}$$

□

Definición 5.6. Sea G un grupo y X un G -conjunto, un elemento $x \in X$ se dice que es fijo por la acción si ${}^g x = x$, $\forall g \in G$.

Consideramos el conjunto de todos los elementos que se quedan fijos por todos los elementos de G :

$$Fix(X) = \{x \in X \mid {}^g x = x, \quad \forall g \in G\}$$

Proposición 5.6. Sea G un grupo y X un G -conjunto, si $x \in X$, entonces:

$$x \in Fix(X) \iff Orb(x) = \{x\} \iff Stab_G(x) = G$$

Demostración. Si recordamos las definiciones de estos tres conjuntos:

$$\begin{aligned} Orb(x) &= \{y \in X \mid \exists g \in G \text{ con } {}^g y = x\} \\ Stab_G(x) &= \{g \in G \mid {}^g x = x\} \\ Fix(X) &= \{x \in X \mid {}^g x = x \quad \forall g \in G\} \end{aligned}$$

Veamos todas las implicaciones:

$$x \in Fix(X) \implies Orb(x) = \{x\}$$

Si $y \in Orb(x)$, entonces $\exists g \in G$ con ${}^g y = x$, por lo que:

$$y = g^{-1} {}^g y = g^{-1} ({}^g y) = g^{-1} x \stackrel{(*)}{=} x$$

Donde en $(*)$ usamos que $x \in Fix(X)$. Concluimos que $Orb(x) = \{x\}$.

$$Orb(x) = \{x\} \implies Stab_G(x) = G$$

Sea $g \in G$, notamos $y = {}^g x$, pero entonces tenemos que:

$$x = g^{-1} {}^g x = g^{-1} ({}^g x) = g^{-1} y$$

Por lo que $y \in Orb(x) = \{x\}$, de donde $y = x$ y $g \in Stab_G(x)$.

$$Stab_G(x) = G \implies x \in Fix(x)$$

$${}^g x = x \quad \forall g \in G$$

De donde deducimos que $x \in Fix(X)$.

□

Observemos que si X es finito, $X/\sim = \{Orb(x_1), \dots, Orb(x_n)\}$:

$$\begin{aligned} |X| &= \sum_{k=1}^n |Orb(x_k)| = |Fix(X)| + \sum_{x_k \notin Fix(X)} |Orb(x_k)| \\ &= |Fix(X)| + \sum_{x_k \notin Fix(X)} [G : Stab_G(x_k)] \end{aligned}$$

A continuación, lo que haremos será estudiar los conjuntos $Orb(\cdot)$, $Stab_G(\cdot)$ y $Fix(X)$ para ciertos ejemplos comunes de acciones.

5.1.1. Acción por traslación

Sea G un grupo no trivial, la acción por traslación se define como $ac : G \times G \rightarrow G$ dada por:

$$ac(g, h) = {}^g h = gh \quad \forall g, h \in G$$

De esta forma, tenemos que:

$$Orb(h) = \{k \in G \mid \exists g \in G \text{ con } k = {}^g h = gh\} = G \quad \forall h \in G$$

Ya que fijado $k \in G$ y dado $h \in G$, siempre podemos tomar $g = kh^{-1} \in G$ para tener que ${}^g h = gh = k$.

$$\begin{aligned} Stab_G(h) &= \{g \in G \mid gh = {}^g h = h\} = \{1\} \quad \forall h \in G \\ Fix(G) &= \{h \in G \mid gh = {}^g h = h \quad \forall g \in G\} = \emptyset \end{aligned}$$

5.1.2. Acción por conjugación

Sea G un grupo, la acción por conjugación se define como $ac : G \times G \rightarrow G$ dada por:

$$ac(g, h) = {}^g h = ghg^{-1} \quad \forall g, h \in G$$

Preliminares

Antes de estudiar los subconjuntos notables de esta acción, definimos ciertos conjuntos y vemos propiedades de estos que nos ayudarán a entender la acción.

Definición 5.7 (Centralizador). Sea G un grupo y $S \subseteq G$, llamamos centralizador de S en G al conjunto:

$$C_G(S) = \{x \in G \mid xs = sx \quad \forall s \in S\}$$

Definición 5.8 (Normalizador). Sea G un grupo y $S \subseteq G$, llamamos normalizador de S en G al conjunto:

$$N_G(S) = \{x \in G \mid xS = Sx\}$$

Proposición 5.7. Sea G un grupo y $S \subseteq G$, se verifica:

- i) $N_G(S) < G$.
- ii) $C_G(S) \triangleleft N_G(S)$.
- iii) Si $S < G$, entonces $S \triangleleft N_G(S)$.

Demostración. Demostramos cada apartado:

i) Sean $x, y \in N_G(S)$, entonces tendremos que:

$$\begin{aligned} xS = Sx &\implies xSx^{-1} = S \\ yS = Sy &\implies S = y^{-1}Sy \end{aligned}$$

En dicho caso:

$$(xy^{-1})S(xy^{-1})^{-1} = (xy^{-1})S(yx^{-1}) = x(y^{-1}Sy)x^{-1} = xSx^{-1} = S$$

De donde deducimos que $(xy^{-1})S = S(xy^{-1})$, por lo que $xy^{-1} \in N_G(S)$ y $N_G(S) < G$.

ii) Hemos de ver primero que $C_G(S) < N_G(S)$:

■ En primer lugar, si $x \in C_G(S)$:

$$xS = \{xs \mid s \in S\} = \{sx \mid s \in S\} = Sx$$

Por lo que $x \in N_G(S)$ y se tiene que $C_G(S) \subseteq N_G(S)$.

■ Ahora, si $x, y \in C_G(S)$, entonces:

$$\begin{aligned} xs &= sx \implies xsx^{-1} = s \\ ys &= sy \implies s = y^{-1}sy \quad \forall s \in S \end{aligned}$$

Lo que nos permite escribir:

$$(xy^{-1})s(xy^{-1})^{-1} = x(y^{-1}sy)x^{-1} = xsx^{-1} = s \quad \forall s \in S$$

De donde deducimos que $xy^{-1} \in C_G(S)$, por lo que $C_G(S) < N_G(S)$.

Para la normalidad, dado $x \in C_G(S)$ y $g \in N_G(S)$, queremos ver que se cumple $y = gxg^{-1} \in C_G(S)$. Para ello, dado $s \in S$, vemos que:

$$ys = (gxg^{-1})s \stackrel{(*)}{=} gxs'g^{-1} = gs'xg^{-1} \stackrel{(**)}{=} s(gxg^{-1}) = sy$$

Donde en $(*)$ usamos que como $g \in N_G(S)$, también tenemos que $g^{-1} \in N_G(S)$, con lo que $\exists s' \in S$ de forma que:

$$g^{-1}s = s'g^{-1}$$

Y en $(**)$ deshacemos este proceso, ya que multiplicando la igualdad superior por derecha e izquierda por g , llegamos a que:

$$g^{-1}s = s'g^{-1} \implies gg^{-1}sg = gs'g^{-1}g \implies sg = gs'$$

En definitiva, de $ys = sy$ deducimos que $y = gxg^{-1} \in C_G(S)$, para todo $x \in C_G(S)$ y todo $g \in N_G(S)$, de donde $C_G(S) \triangleleft N_G(S)$.

iii) Si suponemos además que $S < G$, por una parte tenemos que:

$$sS = S = Ss \quad \forall s \in S$$

De donde deducimos que $S \subseteq N_G(S)$ y por ser $S < G$, tenemos que $S < N_G(S)$. Para la normalidad, si $g \in N_G(S)$, tendremos entonces que:

$$gS = Sg \implies gSg^{-1} = S$$

De donde deducimos que $S \triangleleft N_G(S)$.

□

Proposición 5.8. Sea G un grupo, $H, K < G$ con $H \subseteq K$, entonces:

$$H \triangleleft K \iff K < N_G(H)$$

De esta forma, el normalizador $N_G(H)$ se caracteriza como el mayor subgrupo de G en el que H es normal.

Demostración. Por ser $H, K < G$ con $H \subseteq K$, tenemos ya que $H < K$. Por una caracterización que vimos de los subgrupos normales:

$$H \triangleleft K \iff kHk^{-1} = H \quad \forall k \in K \iff kH = Hk \quad \forall k \in K \iff K \subseteq N_G(H)$$

Y por ser $K < G$, $K \subseteq N_G(H) \iff K < N_G(H)$.

□

Subconjuntos notables

Estudiadas ya las propiedades del centralizador y del normalizador, estamos ya en condiciones de estudiar los conjuntos notables de la acción por conjugación:

$$\text{Orb}(h) = \{k \in G \mid \exists g \in G \text{ con } k = {}^g h = ghg^{-1}\} = \{ghg^{-1} \mid g \in G\} = Cl_G(h) \quad \forall h \in G$$

Es la clase de conjugación de h en G (relación 4, ejercicio 30).

$$\text{Stab}_G(h) = \{g \in G \mid {}^g h = ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = C_G(h)$$

Centralizador de G en h (mismo ejercicio).

$$|Cl_G(h)| = [G : C_G(h)]$$

Y en el caso finito:

$$[G : C_G(h)] = \frac{|G|}{|C_G(h)|}$$

Por lo que $|Cl_G(h)|$ será un divisor de $|G|$.

$$\text{Fix}(X) = \{h \in G \mid ghg^{-1} = {}^g h = h \quad \forall g \in G\} = \{h \in G \mid gh = hg \quad \forall g \in G\} = Z(G)$$

Ejemplo. Calcular las clases de conjugación de D_4 :

$$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} = \{s^i r^j \mid i = 0, 1 \ j = 0, 1, 2, 3\}$$

$$Cl_{D_4}(1) = \{s^i r^j 1 (s^i r^j)^{-1}\} = \{1\}$$

$$Cl_{D_4}(r) = \{s^i r^j r (s^i r^j)^{-1}\} = \{s^i r^j r r^{-j} s^{-i}\} = \{s^i r s^i\} = \{r, sr s\} = \{r, r^3\}$$

$$Cl_{D_4}(r^2) = \{s^i r^2 s^i\} = \{r^2\}$$

$$Cl_{D_4}(s) = \{s, sr^2\}$$

$$Cl_{D_4}(sr) = \{sr, sr^3\}$$

$$|G| = |Z(G)| + \sum_{h \notin Z(G), h \in \Gamma} |Cl_G(h)| = |Z(G)| + \sum_{h \notin Z(G), h \in \Gamma} [G : C_G(h)]$$

(Γ indica que cogemos un elemento de cada clase) Es la fórmula de las clases de conjugación de G . Esta fórmula podemos generalizarla para cualquier subgrupo normal $H \triangleleft G$, en la fórmula de clases generalizada:

$$|H| = |H \cap Z(G)| + \sum_{h \in \Gamma} [H : C_H(h)]$$

Donde Γ son las órbitas con más de un elemento (C_G es el centralizador de G).

5.1.3. Acción por conjugación sobre subgrupos

Sea G un grupo, la acción por conjugación sobre sus subgrupos viene definida⁴ por $ac : G \times Subg(G) \rightarrow Subg(G)$ dada por:

$$ac(g, H) = {}^gH = gHg^{-1} \quad \forall g \in G, \quad \forall H \in Subg(G)$$

Veamos que:

$$Orb(H) = \{K \in Subg(G) \mid \exists g \in G \text{ con } gHg^{-1} = {}^gH = K\} = \{gHg^{-1} \mid g \in G\}$$

Es decir, la órbita de un subgrupo está formado por todos sus conjugados.

Observación. Sea G un grupo, $H \in Subg(G)$, si consideramos la acción por conjugación sobre subgrupos, tenemos que:

$$Orb(H) = \{H\} \iff H \triangleleft G$$

Esto se debe a que:

$$Orb(H) = \{H\} \iff \{gHg^{-1} \mid g \in G\} = \{H\} \iff H \triangleleft G$$

Donde la última equivalencia se tiene gracias a la Proposición 3.2, donde vimos una caracterización de los subgrupos normales.

El estabilizador:

$$Stab_G(H) = \{g \in G \mid {}^gH = H\} = \{g \in G \mid gH = Hg\} = N_G(H)$$

Vemos finalmente los subgrupos que quedan fijos mediante la acción:

$$Fix(Subg(G)) = \{H < G \mid gHg^{-1} = {}^gH = H \quad \forall g \in G\} = \{H < G \mid H \triangleleft G\}$$

Coincide con el conjunto de subgrupos normales de G .

Si G es finito:

$$|Orb(H)| = [G : N_G(H)]$$

El número de grupos conjugados es un divisor de $|G|$.

5.2. p -grupos

Definición 5.9 (p -grupo). Si p es un número primo, un grupo G se dice que es un p -grupo si todo elemento tiene orden una potencia de p .

Si G es un grupo, diremos que $H < G$ es un p -subgrupo de G si H es un p -grupo.

Ejemplo. \mathbb{Z}_8 es un ejemplo de 2-grupo.

Teorema 5.9 (de Cauchy). Si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p , y por tanto tendrá un subgrupo de orden p que será un p -subgrupo.

⁴está bien definida gracias a la Proposición 3.1

Demostración. Si consideramos:

$$X = \{(a_1, a_2, \dots, a_p) \in G^p \mid a_1 a_2 \dots a_p = 1\}$$

Si $|G| = n$, entonces $|X| = n^{p-1}$, ya que elegimos libremente las $p - 1$ primeras coordenadas (variación con repetición) y la última viene condicionada.

Sea $\sigma = (1 \ 2 \ \dots \ p) \subseteq S_p$ y:

$$H = \langle \sigma \rangle = \{1, \sigma, \dots, \sigma^{p-1}\} \subseteq S_p$$

Consideramos también la acción natural $ac : H \times X \rightarrow X$ dada por:

$$ac(\sigma^k, (a_1, a_2, \dots, a_p)) = (a_{\sigma^k(1)}, a_{\sigma^k(2)}, \dots, a_{\sigma^k(p)}) \quad \forall k \in \{0, \dots, p-1\}$$

Veamos que:

$$|Orb(a_1, \dots, a_p)| = [H : Stab_H(a_1, \dots, a_p)] = \frac{|H|}{|Stab_H(a_1, \dots, a_p)|}$$

De donde tenemos que $|Orb(a_1, \dots, a_p)|$ es un divisor de $|H|$. En dicho caso, $|Orb(a_1, \dots, a_p)|$ será 1 o p , por ser $|H| = p$.

Sean r el número de órbitas con un elemento y s el número de órbitas con p elementos, entonces:

$$|X| = r + sp = n^{p-1}$$

Veamos ahora cómo son los elementos de $Orb(a_1, \dots, a_p)$:

$$Orb(a_1, \dots, a_p) = \{(a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots, (a_p, a_1, \dots, a_{p-1})\}$$

La órbita será unitaria si y solo si $a_1 = a_2 = \dots = a_p$. Además, sabemos de la existencia de órbitas con un elemento ($r \geq 1$), como $Orb(1, 1, \dots, 1)$. Busquemos más: por hipótesis, $p \mid n$ y además $r = n^{p-1} - sp$, de donde $p \mid r$, por lo que $r \geq 2$ (ya que lo divide un primo).

En conclusión, $\exists a \in G \setminus \{1\}$ de forma que $Orb(a, a, \dots, a)$ es unitaria, de donde $a^p = 1$, por lo que $O(a) = p$. Tenemos que $\langle a \rangle$ es un p -subgrupo de orden p . \square

Corolario 5.9.1. Sea G un grupo finito y p un número primo:

$$G \text{ es un } p\text{-grupo} \iff \exists n \in \mathbb{N} \text{ con } |G| = p^n$$

Demostración. Veamos la doble implicación.

\Leftarrow) Si $|G| = p^n$ para cierto $n \in \mathbb{N}$, entonces tendremos que $O(x) \mid p^n$ para todo $x \in G$, de donde $O(x) = p^k$ para cierto $k \in \mathbb{N}$, luego G es un p -grupo.

\Rightarrow) Suponemos que q es un primo que divida al orden de $|G|$, luego por el Teorema de Cauchy debe existir $x \in G$ de forma que $O(x) = q$. En dicho caso, como G es un p -grupo, $q = p^r$ para cierto $r \in \mathbb{N}$, de donde $r = 1$ y $q = p$.

De esta forma, el único primo que divide a $|G|$ es p , luego $|G| = p^n$, para algún $n \in \mathbb{N}$. \square

Si consideramos el centro de un p -grupo:

Teorema 5.10 (de Burnside). *Si G es un p -grupo finito no trivial, entonces $|Z(G)| \geq p$, y en particular, $|Z(G)| \neq \{1\}$.*

Demostración. Distinguimos casos:

- Si G es abeliano, $Z(G) = G$ y tenemos que $|Z(G)| = |G| = p^n$ para cierto $n \in \mathbb{N}$, por lo que $|Z(G)| \geq p$. En particular, G no es trivial.
- Si G es no abeliano, entonces $Z(G) < G$ y por la fórmula anterior de las clases:

$$p^n = |G| = |Z(G)| + \sum_{h \notin Z(G), h \in \Gamma} [G : C_G(h)]$$

Como G es finito, $[G : C_G(h)]$ divide a $|G| = p^n$ para cualquier $h \in \Gamma$ y para cierto $n \in \mathbb{N}$. Es decir:

$$[G : C_G(h)] = p^k \quad \text{para algún } k \in \mathbb{N}, \quad \forall h \in \Gamma$$

En ningún caso puede ser $k = 0$, ya que diríamos que $C_G(h) = G$ y:

$$C_G(h) = \{g \in G \mid gh = hg\}$$

De donde $h \in Z(G)$, por lo que h no estaría en Γ .

En dicho caso, $p \mid [G : C_G(h)]$ para todo $h \in \Gamma$, $p \mid |Z(G)|$ (despejar $|Z(G)|$ de la anterior igualdad), de donde $|Z(G)| \geq p$.

□

Corolario 5.10.1. *Si G es un grupo y p es un número primo, si $|G| = p^n$, entonces:*

$$|Z(G)| \neq p^{n-1}$$

En particular, todos los grupos de orden p^2 son abelianos.

Demostración. Supongamos que $|G| = p^n$ y que $|Z(G)| = p^{n-1}$. De esta forma:

$$|G/Z(G)| = p$$

En dicho caso, $G/Z(G)$ es cíclico, luego G es abeliano (relación 4 ejercicio 4). En dicho caso, G coincide con su centro, $G = Z(G)$, luego $p^n = p^{n-1}$, contradicción.

En particular, si G es un grupo con $|G| = p^2$ con p primo, como $Z(G) < G$, $|Z(G)|$ a de dividir a p^2 , luego:

- Si $|Z(G)| = 1$, entonces $Z(G) = 1$, que contradice a Burnside.
- Si $|Z(G)| = p$, no puede ser.
- Falta que $|Z(G)| = p^2$, luego $Z(G) = G$.

□

Este corolario nos dice que todos los grupos de orden p^2 son resolubles, por ser abelianos.

Teorema 5.11. *Sea G un grupo finito con $|G| = n$ y sea p un número primo, entonces para toda potencia p^k que divida a n , existe un subgrupo $H < G$ con orden $|H| = p^k$.*

Demostración. Por inducción sobre k :

- Si $k = 1$: tenemos el Teorema de Cauchy.
- Primera hipótesis de inducción: el resultado es cierto para todo $l < k$: si $p^l \mid |G|$, entonces $\exists H < G$ con $|H| = p^l$.
Veamos qué ocurre con k , es decir, si $|G| = p^k r = n$ para cierto $r \in \mathbb{N}$.

Por inducción sobre r :

- Si $r = 1$: tomamos $H = G$.
- Segunda hipótesis de inducción: si $r > 1$, suponemos el resultado cierto para todo grupo de orden divisible por p^k que sea de la forma $p^k m$ con $m < r$, es decir, $\exists H < G$ con $|H| = p^k$, veamos qué ocurre con G :

Para ello, distinguimos casos:

- Si existe $K < G$, $K \neq G$ de forma que $p \nmid [G : K]$. En dicho caso: $|G| = [G : K]|K|$ y $p^k \mid |G|$, entonces p^k dividirá a $|K|$. Usando la Segunda Hipótesis de inducción, tendremos $H < K < G$ de forma que $|H| = p^k$.
- Si para cualquier $K < G$, $K \neq G$ se tiene que $p \mid [G : K]$, entonces usando la fórmula de las clases:

$$|Z(G)| = G - \sum_{h \notin Z(G), h \in \Gamma} [G : C_G(h)]$$

Y como p divide a todos los $[G : C_G(h)]$, concluimos que $p \mid |Z(G)|$. Por el Teorema de Cauchy, podemos encontrar $K < Z(G)$ de forma que $|K| = p$.

Por ser $K \subseteq Z(G)$, entonces $K \triangleleft G$ y podemos considerar el conjunto cociente G/K , con orden:

$$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{p}$$

De donde $p^{k-1} \mid |G/K|$.

Por la Primera Hipótesis de inducción, existe otro $L < G/K$ con $|L| = p^{k-1}$. Por el Tercer Teorema de Isomorfía, sabemos que $\exists K' \triangleleft H < G$ de forma que:

$$L = H/K$$

De donde:

$$|H| = |H/K||K| = p^{k-1}p = p^k$$

□

Ejemplo. Por ejemplo, si G es un grupo de la forma $|G| = 24 = 2^3 \cdot 3$, tendremos un subgrupo de orden 2, otro de orden 4 y otro de orden 8.

5.2.1. p -subgrupos de Sylow

En 1872, un noruego llamado Peter LM Sylow (1832-1918) definió unos grupos y llegó a unos resultados sobre ellos.

Definición 5.10 (p -subgrupos de Sylow). Si G es un grupo finito y p un número primo que divide a $|G|$, un p -subgrupo de Sylow de G es un p -subgrupo de G cuyo orden es la máxima potencia de p que divide a $|G|$.

Es decir, si $|G| = p^k m$ con $\text{mcd}(p, m) = 1$ y p primo, un p -subgrupo $H < G$ es de Sylow si $|H| = p^k$.

Ejemplo. Si tenemos un grupo G con $|G| = 24 = 2^3 \cdot 3$, vamos a tener:

- $P < G$ un 2-subgrupo de Sylow, con $|P| = 8$.
- $Q < G$ un 3-subgrupo de Sylow, con $|Q| = 3$.

Corolario 5.11.1 (Primer Teorema de Sylow). *Para todo grupo finito G y todo divisor primo p de su orden, existe al menos un p -subgrupo de Sylow.*

Demostración. Es evidente a partir del Teorema 5.11. □

Observación. Si G es un grupo y p es un número primo con:

$$|G| = p^k m \quad \text{mcd}(p, m) = 1$$

Y P es un p -grupo de Sylow con $P < H < G$, entonces usando la fórmula de los índices:

$$[G : P] = [G : H][H : P]$$

En dicho caso, $[H : P] \mid [G : P] = m$, por lo que p no dividirá a $[H : P]$. Además:

$$[G : H] \mid [G : P] \implies p \nmid [G : H]$$

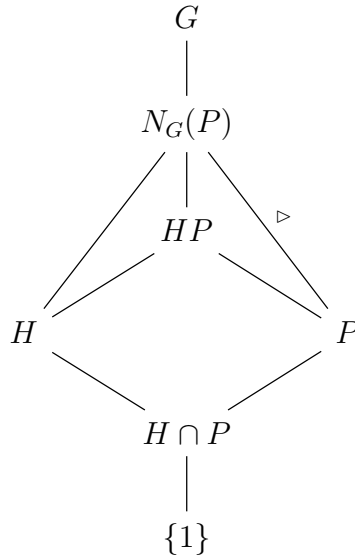
Es decir, si encontramos un grupo que contiene a P como subgrupo, p no dividirá a dichos índices.

Al siguiente Lema también le llaman Segundo Teorema de Sylow, aunque nos reservamos este nombre para el resultado que se demuestra a partir del Lema.

Lema 5.12. *Si P es un p -subgrupo de Sylow de un grupo finito G y H es un p -subgrupo de $N_G(P)$, entonces H está contenido en P .*

Es decir, los p -subgrupos del normalizador de un p -subgrupo de Sylow están contenidos en dicho subgrupo.

Demostración. Como $P \triangleleft N_G(P)$ y $H < N_G(P)$, tenemos que $HP < N_G(P)$ y $H \cap P < H$. Estamos en la situación:



Por el Segundo Teorema de Isomorfía:

$$HP/P \cong H/H \cap P$$

Ahora, si $r = [HP : P] = [H : H \cap P]$, entonces $p \nmid r$. Ahora, como $r = [H : H \cap P]$ y como H es un p -subgrupo, $p^k \mid r$ para cierto $k \in \mathbb{N}$ (como es un p -grupo, tendremos $k > 0$). Como $p \nmid r$ (por la observación anterior) y $p^k \mid r$, entonces $r = 1$, de donde $HP = P$ y $H < P$. \square

Teorema 5.13 (Segundo Teorema de Sylow). *Sea G un grupo finito, p un número primo, supongamos que $|G| = p^k m$ con $\text{mcd}(p, m) = 1$ y n_p denota el número de p -subgrupos de Sylow de G , entonces:*

- i) *Todo p -subgrupo de G está contenido (como subgrupo) en un p -subgrupo de Sylow de G .*
- ii) *Cualesquiera dos p -subgrupos de Sylow de G son conjugados.*
- iii) *$n_p \mid m$ y $n_p \equiv 1 \pmod{p}$.*

Demostración. Demostramos cada apartado:

- i) Si llamamos $S = \text{Syl}_p(G) = \{P \mid P \text{ es un } p\text{-subgrupo de Sylow de } G\}$, consideramos la acción por conjugación $G \times S \rightarrow S$ dada por:

$$ac(g, P) = {}^gP = gPg^{-1} \in S$$

Sea $P_1 \in S$, estudiemos su órbita y su estabilizador:

$$\begin{aligned} \text{Orb}(P_1) &= \{gP_1g^{-1} \mid g \in G\} \\ \text{Stab}_G(P_1) &= \{g \in G \mid gP_1g^{-1} = P_1\} = N_G(P_1) \end{aligned}$$

Tenemos:

$$\begin{aligned} |Orb(P_1)| &= [G : N_G(P_1)] \\ P_1 &< N_G(P_1) < G_1 \\ [G : P_1] &= [G : N_G(P_1)][N_G(P_1) : P_1] \end{aligned}$$

Por lo que $|Orb(P_1)|$ divide a $[G : P_1] = m$. En definitiva:

$$\text{mcd}(|Orb(P_1)|, p) = 1$$

Ahora, veamos que todo p -subgrupo está contenido en un p -subgrupo de Sylow. Para ello, sea H un p -subgrupo de G , consideramos la acción sobre la órbita de $P_1 \in S$, $H \times Orb(P_1) \rightarrow Orb(P_1)$, dada por:

$$ac(h, P) = {}^hP = hPh^{-1} \in Orb(P_1)$$

Tendremos:

$$Stab_H(P) = \{h \in H \mid hPh^{-1} = P\} = H \cap N_G(P) < H$$

Además, también tendremos que $H \cap N_G(P) < P$, ya que si H es un p -subgrupo de $N_G(P)$, entonces $H < P$. En definitiva:

$$Stab_H(P) = H \cap N_G(P) < H \cap P < H \cap N_G(P)$$

De donde tenemos que $N_G(P) = H \cap P$. Usando la fórmula de la órbita:

$$|Orb(P_1)| = \sum_P [H : Stab_H(P)] = \sum_P [H : H \cap P]$$

De donde cada sumando divide a $|H|$ con H un p -subgrupo de P , por lo que $|H|$ es una potencia de p . Sin embargo, como $p \nmid |Orb(P_1)|$ (su máximo común divisor era 1), ha de existir un grupo $P \in Orb(P_1)$ (notemos que P es un p -subgrupo de Sylow. De hecho, P es un conjugado de P_1) de forma que:

$$[H : H \cap P] = 1$$

Por lo que $H \cap P = H$ y $H < P$.

- ii) Veamos ahora que cualesquiera dos p -subgrupos de Sylow de G son conjugados. Para ello, sean P_1, P_2 dos p -subgrupos de Sylow de G , antes vimos (el lema) que si $H = P_2 < G$, entonces H está contenido en un subgrupo de Sylow, por lo que $\exists P$, un p -subgrupo de Sylow, conjugado de P_1 (por i)) de forma que $P_2 < P$, pero $|P| = |P_2|$, luego $P_2 = P$.
- iii) Veamos ahora que $n_p \mid m$ y que $n_p \equiv 1 \pmod{p}$.

En el apartado ii) hemos visto que $Orb(P_1) = S$, luego:

$$n_p = |S| = |Orb(P_1)| = [G : N_G(P_1)]$$

Por lo que $n_p \mid m$.

Si en el apartado i) tomamos $H = P_1$ (el de la demostración anterior):

$$n_p = |\text{Orb}(P_1)| = \sum_P [P_1 : P_1 \cap P]$$

Por lo que $[P_1 : P_1 \cap P] = 1$ y los demás eran múltiplos de p , deducimos que $n_p \equiv 1 \pmod{p}$.

□

Ejemplo. Vamos a calcular grupos de Sylow:

- En $C_n = \langle x \mid x^n = 1 \rangle$ para cierto $n \in \mathbb{N}$, por el Primer Teorema de Sylow tendremos grupos de Sylow de las potencias máximas de los primos que aparecen en la factorización de n . Es decir, si n se descompone como:

$$n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$$

Para cada $k \in \{1, 2, \dots, m\}$, existe un p_k -subgrupo de Sylow, que será cíclico y tendrá orden $p_k^{t_k}$, luego los subgrupos de Sylow serán de la forma: $C_{p_k^{t_k}}$.

- En S_3 , como $|S_3| = 6 = 2 \cdot 3$, tendremos 2-subgrupos de Sylow y 3-subgrupos de Sylow. Veamos cuántos tenemos:
 - 2-subgrupos de Sylow, es decir, subgrupos de orden 2 de S_3 . Como $n_2 \mid 3$ y ha de ser $n_2 \equiv 1 \pmod{2}$, tendremos que n_2 valdrá 1 o 3.

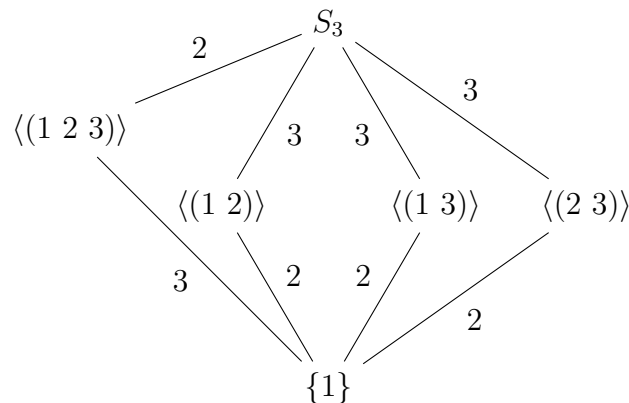


Figura 5.1: Diagrama de Hasse para los subgrupos de S_3 .

como los 3 subgrupos de la derecha son conjugados entre sí (compruébe-se), tendremos que $n_2 = 3$.

- Los 3-subgrupos de Sylow será un subgrupo de orden 3 de S_3 , que será el único que hay: $\langle (1 2 3) \rangle = A_3 \triangleleft S_3$.

Si queremos verlo por el Segundo Teorema de Sylow:

$$n_3 \equiv 1 \pmod{3} \quad \left. \begin{array}{l} n_3 \mid 2 \end{array} \right\} \implies n_3 = 1$$

- En A_4 , tenemos $|A_4| = 12 = 2^3 \cdot 3$. Tendremos:
 - 2-subgrupo de Sylow de orden 4. Busquemos por el Segundo Teorema de Sylow:

$$\left. \begin{array}{l} n_2 \mid 3 \\ n_2 \equiv 1 \pmod{2} \end{array} \right\} \implies n_2 \in \{1, 3\}$$

Concluimos que $n_2 = 1$, de donde el 2-subgrupo de Sylow es V , que era normal en A_4 .

- 3-subgrupo de Sylow de orden 3:

$$\left. \begin{array}{l} n_3 \mid 4 \\ n_3 \equiv 1 \pmod{3} \end{array} \right\} \implies n_3 \in \{1, 4\}$$

Y serán los subgrupos de A_4 generados por los 3-ciclos.

- En S_4 , $|S_4| = 24 = 2^3 \cdot 3$:
 - Para los 2-subgrupos:

$$\left. \begin{array}{l} n_2 \mid 3 \\ n_2 \equiv 1 \pmod{2} \end{array} \right\} \implies n_2 \in \{1, 3\}$$

Si suponemos que $n_2 = 1$, sea Q un grupo con $|Q| = 8$ que sea el 2-subgrupo de Sylow. En dicho caso, todas las trasposiciones deben estar contenidas en Q (por ser de orden 2), pero todas las trasposiciones generan a S_4 , luego $Q = S_4$, contradicción.

Por tanto, tenemos $n_2 = 3$, tenemos 3 2-subgrupos de Sylow: Q_1, Q_2 y Q_3 . El grupo de Klein V es un 2-subgrupo, y es normal en S_4 . Por tanto, va a estar contenido en algún Q_k ($k \in \{1, 2, 3\}$). Supongamos que $V < Q_1$. Como todos ellos son conjugados, $\exists \alpha, \beta \in S_4$ de forma que:

$$\begin{aligned} Q_2 &= \alpha Q_1 \alpha^{-1} \\ Q_3 &= \beta Q_1 \beta^{-1} \end{aligned}$$

Y si multiplicamos (como $V \triangleleft S_4$):

$$\begin{aligned} V &= \alpha V \alpha^{-1} < \alpha Q_1 \alpha^{-1} = Q_2 \\ V &= \beta V \beta^{-1} < \beta Q_1 \beta^{-1} = Q_3 \end{aligned}$$

De donde deducimos que $V < Q_k$ para todo $k \in \{1, 2, 3\}$. Los Q_k contendrán a V y a alguna transposición:

$$\begin{aligned} Q_1 &= V \langle (1 \ 2) \rangle \\ Q_2 &= V \langle (1 \ 3) \rangle \\ Q_3 &= V \langle (1 \ 4) \rangle \end{aligned}$$

- Para los 3-subgrupos de Sylow:

$$\left. \begin{array}{l} n_3 \mid 8 \\ n_3 \equiv 1 \pmod{3} \end{array} \right\} \implies n_3 \in \{1, 4\}$$

Los subgrupos de orden 4 de S_4 son:

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

Que son los 3-subgrupos de Sylow.

Corolario 5.13.1. *Sea P un p -subgrupo de Sylow de un grupo finito G . Entonces:*

$$P \text{ es el } \text{único } p\text{-subgrupo de Sylow} \iff P \triangleleft G$$

Demostración. Por doble implicación:

\implies) Si P es el único, como todos los conjugados de P son subgrupos de Sylow, tendremos que:

$$gPg^{-1} = P \quad \forall g \in G$$

Que era la caracterización de subgrupo normal de G .

\impliedby) Supuesto que $P \triangleleft G$, sea Q otro p -subgrupo de Sylow, como P y Q han de ser conjugados, sabemos que $\exists g \in G$ de forma que $gPg^{-1} = Q$, pero por ser $P \triangleleft G$, tenemos también que $P = gPg^{-1}$, luego:

$$P = gPg^{-1} = Q$$

□

Ejemplo. Todo grupo de orden 35 es resoluble.

Demostración. Sea G un grupo con $|G| = 35 = 5 \cdot 7$, vemos que:

$$\left. \begin{array}{l} n_7 \mid 5 \\ n_7 \equiv 1 \pmod{5} \end{array} \right\} \implies n_7 = 1$$

En dicho caso, tenemos un único 7-subgrupo de Sylow $H < G$, que además es normal y tendrá orden 7. En dicho caso, sabemos que será isomorfo a \mathbb{Z}_7 . Como los grupos abelianos son resolubles, tenemos que H es resoluble. Si consideramos el cociente:

$$|G/H| = 5$$

Por lo que $G/H \cong \mathbb{Z}_5$ y G/H será resoluble por ser isomorfo a un grupo abeliano. Deducimos que G es resoluble, por existir $H \triangleleft G$ y ser H y G/H resolubles. □

Se puede demostrar de forma análoga que ciertos grupos de cierto orden son siempre resolubles.

Teorema 5.14. *Sea G un grupo finito en el que todos sus subgrupos de Sylow son normales, entonces G es el producto directo interno de sus subgrupos de Sylow:*

$$G = \prod_{H \in \text{Syl}(G)} H$$

Demostración. En la caracterización de producto directo interno para una cantidad finita de subgrupos (Teorema 3.32), vimos que G era producto directo interno de todos ellos (los llamaremos H_i con $i \in \{1, \dots, n\}$) si y solo si:

- $H_i \triangleleft G$ para todo $i \in \{1, \dots, n\}$.
- $H_1 H_2 \dots H_n = G$.
- $(H_1 \dots H_{i-1}) \cap H_i = \{1\}$ para todo $i \in \{2, \dots, k\}$

Basta pues, demostrar estos 3 puntos. Supuesto que $|G| = p_1^{n_1} \dots p_k^{n_k}$, llamamos P_i al único p_i -subgrupo de Sylow, para todo $i \in \{1, \dots, k\}$.

- Por hipótesis, tendremos que $P_i \triangleleft G$ para todo $i \in \{1, \dots, k\}$.
- También:

$$|P_1 P_2 \dots P_k| = |P_1| |P_2| \dots |P_k| = |G|$$

De donde concluimos que $P_1 P_2 \dots P_k = G$.

- Fijado $i \in \{2, \dots, k\}$, veamos que $(P_1 \dots P_{i-1}) \cap P_i = \{1\}$. Para ello, sea $x \in (P_1 \dots P_{i-1}) \cap P_i$, tenemos:

$$\left. \begin{array}{l} O(x) \mid |P_1 \dots P_{i-1}| = p_1^{n_1} \dots p_{i-1}^{n_{i-1}} \\ O(x) \mid |P_i| = p_i^{n_i} \end{array} \right\} \implies O(x) = 1 \implies x = 1$$

□

Observación. Notemos que cualquier grupo abeliano finito es producto directo interno de sus subgrupos de Sylow, ya que en cualquier grupo abeliano los subgrupos son normales.

6. Clasificación de grupos abelianos finitos

El objetivo final del tema es demostrar los teoremas de estructura de los grupos abelianos finitos, que permiten clasificar todos estos grupos según su orden (para cada orden tendremos una clasificación), salvo isomorfismos.

Serán de especial relevancia varios resultados que ya hemos visto:

- $C_n \times C_m \cong C_{nm} \iff \text{mcd}(n, m) = 1$, en la Proposición 3.34.
- Si $|G| = p_1^{n_1} \dots p_k^{n_k}$ y G tenía un único P_i p_i -subgrupo de Sylow para cada $i \in \{1, \dots, k\}$, entonces $G \cong P_1 \times P_2 \times \dots \times P_k$.

Como trabajaremos con subgrupos abelianos, recordamos que la notación que usábamos para el producto directo de grupos abelianos era \oplus .

Teorema 6.1 (Estructura de los p -grupos abelianos finitos).

Sea A un p -grupo abeliano finito con orden $|A| = p^n$ para $n \geq 1$, entonces existen enteros $\beta_1 \geq \beta_2 \geq \dots \geq \beta_t \geq 1$ de forma que:

$$\beta_1 + \beta_2 + \dots + \beta_t = n$$

$$A \cong C_{p^{\beta_1}} \oplus C_{p^{\beta_2}} \oplus \dots \oplus C_{p^{\beta_t}}.$$

Además, esta expresión es única, es decir, si existen $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_s \geq 1$ de forma que:

$$\alpha_1 + \alpha_2 + \dots + \alpha_s = n$$

$$A \cong C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \dots \oplus C_{p^{\alpha_s}}, \text{ entonces } s = t \text{ y } \alpha_i = \beta_i \text{ para todo } i \in \{1, \dots, t\}.$$

Observación. Notemos que lo que estamos haciendo es tomar particiones de n de la forma β_i , y este Teorema nos dice que el p -grupo puede escribirse de forma única salvo isomorfismos como producto de ciertos subgrupos cíclicos.

Es decir, existen tantos p -grupos abelianos de orden p^n como particiones tengamos del número n .

Ejemplo. Por ejemplo:

- Grupos abelianos finitos de orden $8 = 2^3$, tenemos como particiones:

$$3 \implies A \cong C_8$$

$$1, 2 \implies A \cong C_4 \oplus C_2$$

$$1, 1, 1 \implies A \cong C_2 \oplus C_2 \oplus C_2$$

- Los grupos abelianos finitos de orden $81 = 3^4$, tenemos como particiones:

$$\begin{aligned} A &\cong C_{81} \\ A &\cong C_{27} \oplus C_3 \\ A &\cong C_9 \oplus C_9 \\ A &\cong C_9 \oplus C_3 \oplus C_3 \\ A &\cong C_3 \oplus C_3 \oplus C_3 \oplus C_3 \end{aligned}$$

Teorema 6.2 (Estructura de los grupos abelianos finitos).

Sea A un grupo abeliano finito con $|A| = p_1^{\gamma_1} \dots p_k^{\gamma_k}$ siendo p_i primo para todo $i \in \{1, \dots, k\}$, entonces:

$$A \cong \bigoplus_{i=1}^k \left(\bigoplus_{j=1}^{t_i} C_{p_i}^{n_{ij}} \right)$$

Donde para cada $i \in \{1, \dots, k\}$ tenemos:

$$\begin{aligned} n_{i1} &\geq n_{i2} \geq \dots \geq n_{it_i} \geq 1 \\ n_{i1} + n_{i2} + \dots + n_{it_i} &= r_i \end{aligned}$$

Y la descomposición es única salvo el orden.

Esta última recibe el nombre de descomposición cíclica primaria, y a los $p_i^{n_{ij}}$ con $i \in \{1, \dots, k\}$ y $j \in \{1, \dots, t_i\}$ se les llama divisores elementales de A .

Demostración. Si A es abeliano y finito, entonces todos sus p -subgrupos de Sylow son normales, luego podemos escribir:

$$A = P_1 \oplus P_2 \oplus \dots \oplus P_k$$

Siendo P_1, P_2, \dots, P_k el conjunto de todos sus p -subgrupos de Sylow, de forma que $|P_i| = p_i^{r_i}$, para todo $i \in \{1, \dots, k\}$. Como cada P_i es un p_i -subgrupo abeliano finito, aplicando el Teorema 6.1, podemos escribir:

$$P_i = \bigoplus_{j=1}^{t_i} C_{p_i}^{n_{ij}} \quad \forall i \in \{1, \dots, k\}$$

De donde tenemos la expresión de la tesis.

A cada P_i con $i \in \{1, \dots, k\}$ lo llamaremos componente p_i -primaria de A . □

Ejemplo. Si tenemos un subgrupo finito abeliano A con $|A| = 360 = 2^3 \cdot 3^2 \cdot 5$, veamos los divisores elementales:

Div. elementales	Descomp. cíclica primaria
$2^3 \ 3^2 \ 5$	$C_8 \oplus C_9 \oplus C_5$
$2^2 \ 2 \ 3^2 \ 5$	$C_4 \oplus C_2 \oplus C_9 \oplus C_5$
$2 \ 2 \ 2 \ 3^2 \ 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$
$2^3 \ 3 \ 3 \ 5$	$C_8 \oplus C_3 \oplus C_3 \oplus C_5 \oplus C_8$
$2 \ 2^2 \ 3 \ 3 \ 5$	$C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5$
$2 \ 2 \ 2 \ 3 \ 3 \ 5$	$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$

Serían todas las descomposiciones cíclicas primarias de A . Es decir, A será isomorfo a cualquiera de esos.

Sin embargo, si recordamos la Proposición 3.34, esto nos llevará a la descomposición cíclica, donde observaremos por ejemplo que:

$$\begin{aligned}
 C_8 \oplus C_9 \oplus C_5 &\cong C_{360} \\
 C_4 \oplus C_2 \oplus C_9 \oplus C_5 &\cong C_{180} \oplus C_2 \\
 C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5 &\cong C_{90} \oplus C_2 \oplus C_2 \\
 C_8 \oplus C_3 \oplus C_3 \oplus C_5 \oplus C_8 &\cong C_{120} \oplus C_3 \\
 C_2 \oplus C_4 \oplus C_3 \oplus C_3 \oplus C_5 &\cong C_{60} \oplus C_6 \\
 C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5 &\cong C_{30} \oplus C_6 \oplus C_7
 \end{aligned}$$

7. Relaciones de Ejercicios

7.1. Combinatoria y Teoría de Grafos

Ejercicio 7.1.1. 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 7.1.
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 7.1.2. 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 7.2, donde cada persona viene representada con un vértice con su inicial.



Figura 7.1: Situación del Ejercicio 7.1.1.



Figura 7.2: Situación del Ejercicio 7.1.2.

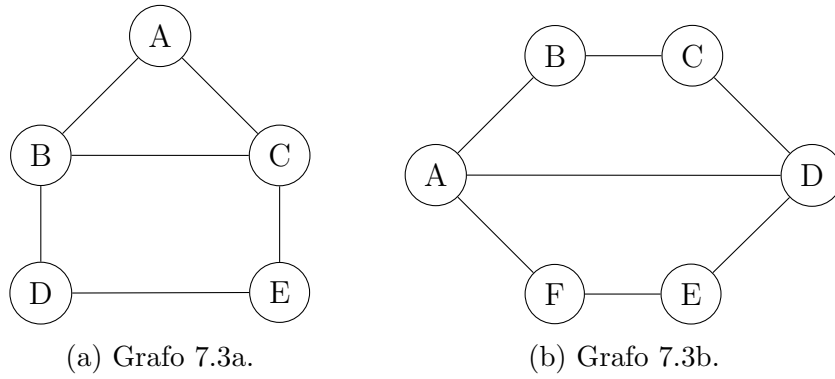


Figura 7.3: Grafos para el ejercicio 7.1.3.

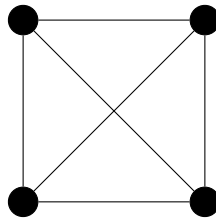


Figura 7.4: Grafo K_4 .

Ejercicio 7.1.3. Expresa en forma matricial los grafos de la Figura 7.3.

La matriz de adyacencia del grafo 7.3a 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 7.3b 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 7.1.4. 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 7.4.

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 7.5: Subgrafos de K_4 con 2 vértices, $|V| = 2$.



Figura 7.6: Subgrafos de K_4 con 3 vértices, $|V| = 3$.

- Los subgrafos con dos vértices se encuentran en la Figura 7.5.
- Los subgrafos con tres vértices se encuentran en la Figura 7.6.
- Los subgrafos con cuatro vértices se encuentran en la Figura 7.7.

Ejercicio 7.1.5. ¿Son isomorfos los grafos de la Figura 7.8? ¿Y los de la Figura 7.9? ¿Y los de la Figura 7.10?

Veamos que los grafos de la Figura 7.8 son isomorfos. Sea $G(V, E)$ el grafo 7.8a y $G'(V', E')$ el grafo 7.8b. Las biyecciones $h_E : E \rightarrow E'$ y $h_V : V \rightarrow V'$ vienen dadas por:

$$\begin{aligned}
 h_V : V &\rightarrow V' \\
 A &\mapsto A \\
 B &\mapsto B \\
 C &\mapsto D \\
 D &\mapsto C \\
 E &\mapsto E
 \end{aligned}$$

$$\begin{aligned}
 h_E : E &\rightarrow E' \\
 e = \{u, v\} &\mapsto e' = \{h_V(u), h_V(v)\}
 \end{aligned}$$

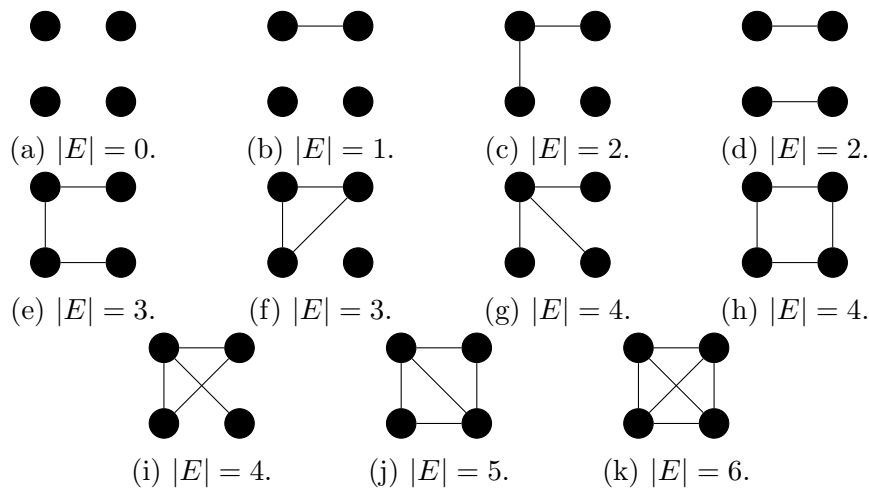


Figura 7.7: Subgrafos de K_4 con 4 vértices, $|V| = 4$.



(a) Grafo 7.8a.



(b) Grafo 7.8b.

Figura 7.8: Primer par de grafos para el ejercicio 7.1.5.



(a) Grafo 7.9a.



(b) Grafo 7.9b.

Figura 7.9: Segundo par de grafos para el ejercicio 7.1.5.

Respecto al par de grafos de la Figura 7.9, sabemos que no son isomorfos puesto que no tienen la misma sucesión de grafos; pues notando por $G(E, V)$ al grafo 7.9a y $G'(E', V')$ al grafo 7.9b, se tiene que:

$$D_4(G) = 2 \neq 1 = D_4(G')$$

Por último, veamos que los grafos de la Figura 7.10 son isomorfos. Sea $G(V, E)$ el grafo 7.10a y $G'(V', E')$ el grafo 7.10b. Las biyecciones $h_E : E \rightarrow E'$ y $h_V : V \rightarrow V'$



(a) Grafo 7.10a.



(b) Grafo 7.10b.

Figura 7.10: Tercer par de grafos para el ejercicio 7.1.5.

vienen dadas por:

$$\begin{aligned}
 h_V : V &\rightarrow V' \\
 A &\mapsto A \\
 B &\mapsto D \\
 C &\mapsto C \\
 D &\mapsto B \\
 E &\mapsto E \\
 F &\mapsto F
 \end{aligned}$$

$$\begin{aligned}
 h_E : E &\longrightarrow E' \\
 e = \{u, v\} &\longmapsto e' = \{h_V(u), h_V(v)\}
 \end{aligned}$$

Ejercicio 7.1.6. 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 7.1.7. 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.

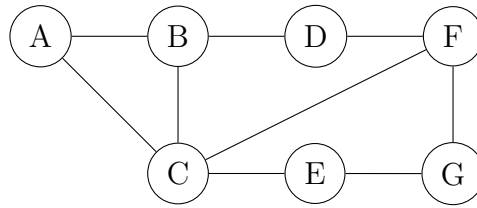


Figura 7.11: Grafo para el ejercicio 7.1.8.

Ejercicio 7.1.8. 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 7.11. 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 7.1.9. 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 7.1.10. 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 7.1.11. ¿Existe algún grafo regular de grado 5 con 25 vértices?

No, por el Ejercicio 7.1.6 (25 es impar).

Ejercicio 7.1.12. ¿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 7.1.13. ¿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 7.12: Grafo con sucesión de grados 0, 0, 0.



Figura 7.13: 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 7.12.

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 7.13.

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 7.14.

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 7.15.

Ejercicio 7.1.14. 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 7.16 cumple con las condiciones.
2. Con un número par de vértices y un número impar de lados.
El grafo de la Figura 7.17 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 7.18 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 7.19 cumple con las condiciones.

Ejercicio 7.1.15. Encuentra un circuito de Euler para los grafos de la Figura 7.20.

Para el grafo de la Figura 7.20a, 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 7.20b, un circuito de Euler es:

$$B \rightarrow A \rightarrow C \rightarrow B \rightarrow E \rightarrow C \rightarrow D \rightarrow F \rightarrow E \rightarrow D \rightarrow B$$

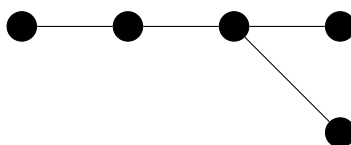


Figura 7.14: Grafo con sucesión de grados 3, 2, 1, 1, 1.

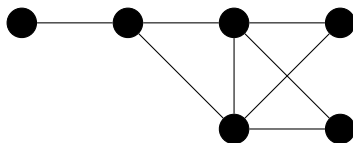


Figura 7.15: Grafo con sucesión de grados 4, 4, 3, 2, 2, 1.

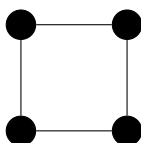


Figura 7.16: Grafo para el Ejercicio 7.1.14.1.

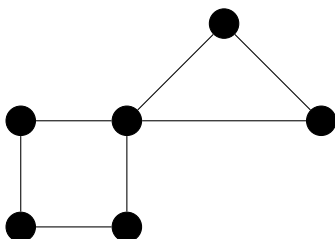


Figura 7.17: Grafo para el Ejercicio 7.1.14.2.

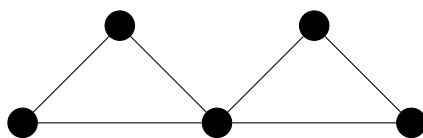


Figura 7.18: Grafo para el Ejercicio 7.1.14.3.

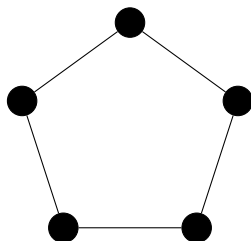


Figura 7.19: Grafo para el Ejercicio 7.1.14.4.

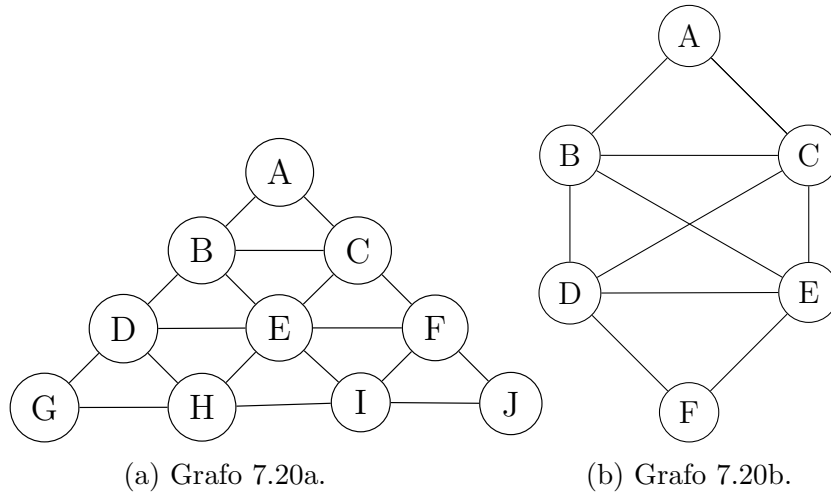


Figura 7.20: Grafos para el ejercicio 7.1.15.

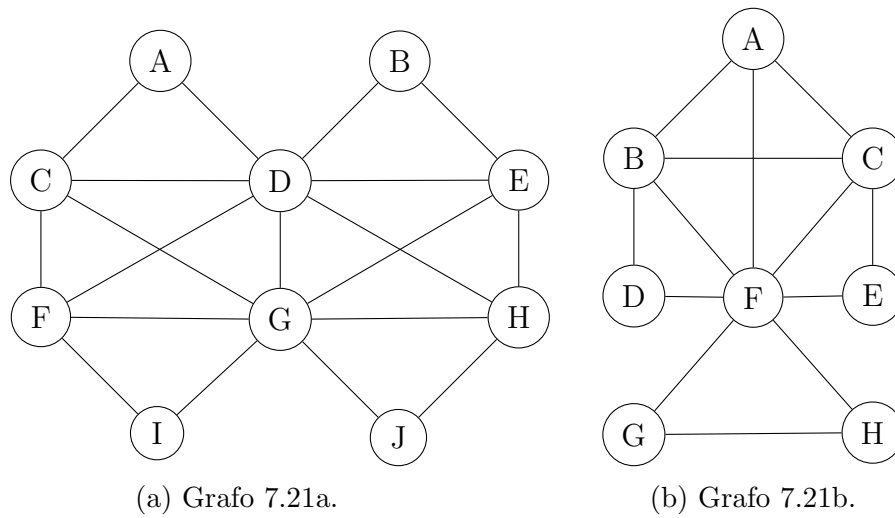


Figura 7.21: Grafos para el ejercicio 7.1.16.

Ejercicio 7.1.16. Encuentra un camino de Euler para los grafos de la Figura 7.21.

Para el grafo de la Figura 7.21a, 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 7.21b, 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 7.1.17. Encontrar un circuito de Euler en el grafo de la Figura 7.22 y un camino de Euler en el grafo de la Figura 7.23.

Para el grafo de la Figura 7.22, 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 7.23, 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 7.22: Primer grafo para el ejercicio 7.1.17.



Figura 7.23: Segundo grafo para el ejercicio 7.1.17.

Ejercicio 7.1.18. ¿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 7.1.19. 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 7.24, que es K_4 con las distancias entre las ciudades. Se trata del problema del Viajante del comercio, un problema NP-completo para el que no se conoce una solución y que ya fue estudiado en Algorítmica. Sin embargo, el trabajar solo con 4 nodos, podemos aplicar fuerza bruta para estudiar todos los caminos, sin mucha dificultad. Observemos que elegir un camino que salga de A, pase por todos los nodos y vuelva a A es equivalente

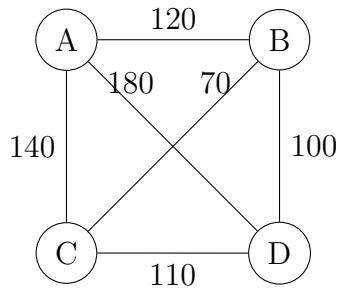


Figura 7.24: Grafo para el ejercicio 7.1.19.

a elegir 3 nodos de un conjunto de 3 nodos, por lo que tenemos $V_3^3 = P_3 = 3!$ posibilidades:

1. $B - C - D$
2. $B - D - C$
3. $C - B - D$
4. $C - D - B$
5. $D - B - C$
6. $D - C - B$

Sin embargo, observemos que nos da igual el orden (si recorremos el camino uvw o el wvu , es el mismo coste) en el que los visitamos, por lo que nos quedamos con 3 posibilidades (al ser los caminos 1 y 6, 2 y 4; y 3 y 5 iguales):

1. $B - C - D = 120 + 70 + 110 + 180 = 480$
2. $B - D - C = 120 + 100 + 110 + 140 = 470$
3. $C - B - D = 180 + 100 + 70 + 140 = 490$

Concluimos que el camino óptimo es: $A - B - D - C$, con un coste de 470.

Ejercicio 7.1.20. 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 $L(G)$ 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:

$$\deg_{L(G)}(e) = \deg_G(v_1) + \deg_G(v_2) - 2$$

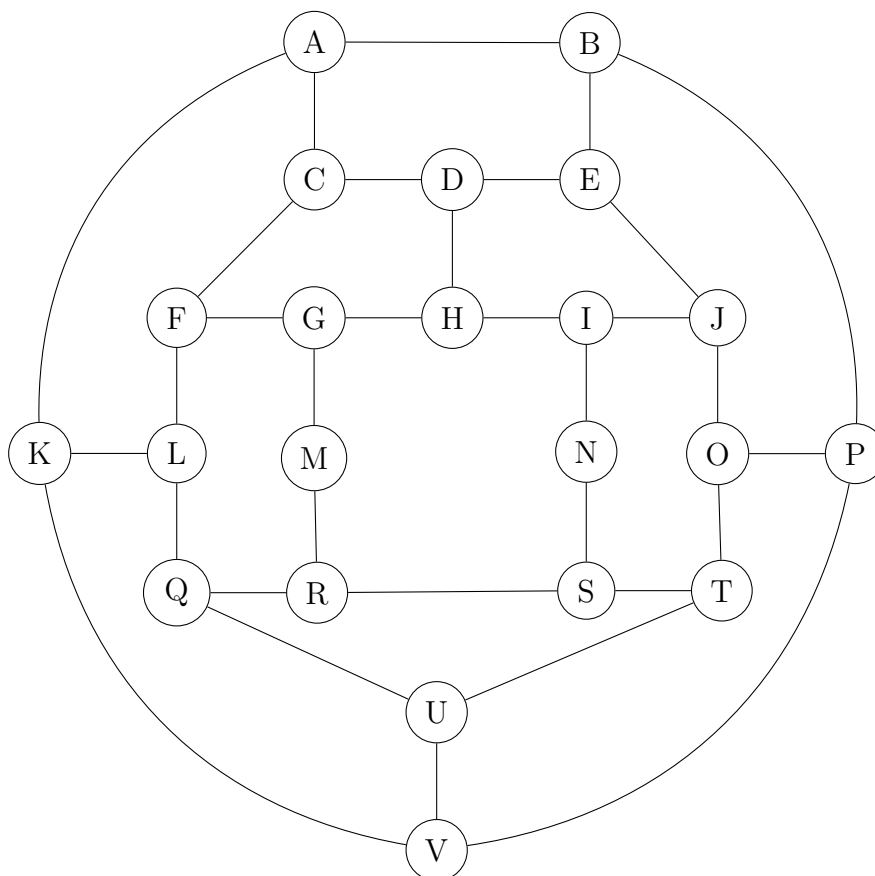


Figura 7.25: Primer grafo para el ejercicio 7.1.21.

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 7.1.21. De entre los grafos de la Figura 7.25 y la Figura 7.26, ¿cuáles contienen un circuito de Hamilton?

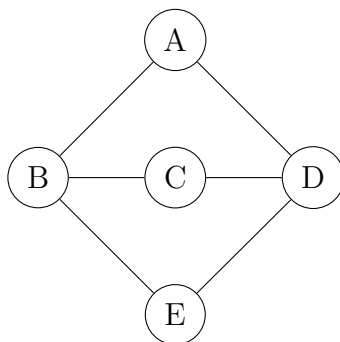


Figura 7.26: Segundo grafo para el ejercicio 7.1.21.

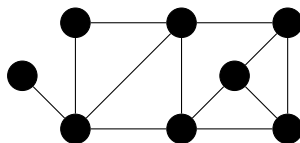


Figura 7.27: Grafo para el ejercicio 7.1.22.1.

Respecto al grafo de la Figura 7.25, 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 7.26, este no es Hamiltoniano.

Ejercicio 7.1.22.

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 7.27.

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 7.1.23.

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 7.1.24.

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 7.28.

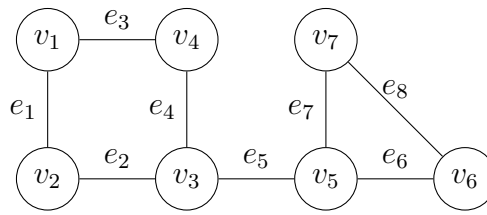


Figura 7.28: Grafo para el ejercicio 7.1.24.1.

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 7.1.25. 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. Aunque K_1 sí es de Hamilton, K_2 no lo es. Por tanto, tenemos que:

$$K_n \text{ es de Hamilton} \quad \forall n \in \mathbb{N} \setminus \{2\}$$

Por tanto, la respuesta correcta es la **c**).

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 7.1.6, 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 7.1.4 vimos que la respuesta correcta es la **a**).

8. Un grafo cuya matriz de adyacencia es

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

- 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 7.1.26.

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 7.29.

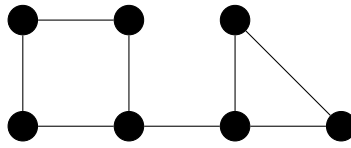


Figura 7.29: Grafo para el ejercicio 7.1.26.1.



Figura 7.30: Grafo G_1 para el ejercicio 7.1.26.2.

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 7.30 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 7.31: Representación plana de G_1 (Figura 7.30).

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 7.31 se muestra la representación plana de G_1 (Figura 7.30).

- 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 7.32: Grafos para el ejercicio 7.1.27.2.

Ejercicio 7.1.27.

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 7.32. El grafo G de la Figura 7.32a es de Euler y de Hamilton, pero su subgrafo completo G' de la Figura 7.32b 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 7.1.4 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 7.1.28.

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.

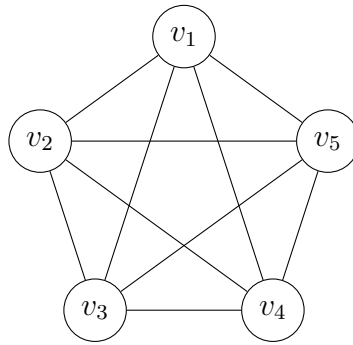
Aplicamos el Algoritmo de Havel-Hakimi, y posteriormente construimos el grafo correspondiente, que se muestra en la Figura 7.33 y se observa que $G = K_5$.

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 7.33: Grafo G del ejercicio 7.1.28.1.

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:

$$\deg v \geq 4 \quad \forall v \in V \setminus \{v_1, v_2\}$$

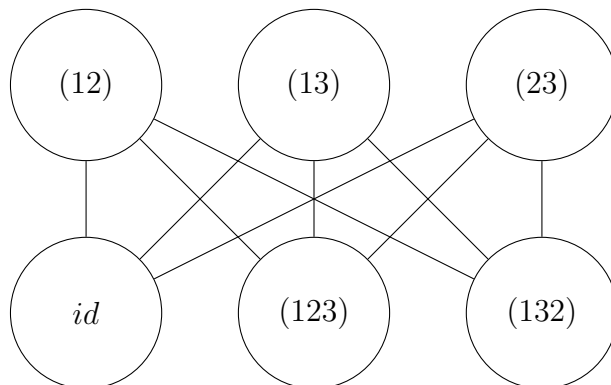


Figura 7.34: Grafo para el ejercicio 7.1.29.

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 7.1.29.

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 7.34. 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 7.35: Octaedro para el ejercicio 7.1.30.

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 7.1.30. 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 7.35, 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 7.36.

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 7.36: Grafo para el ejercicio 7.1.30.

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 7.1.31. 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):

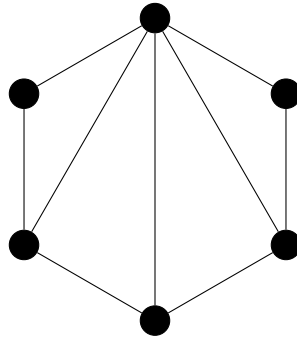


Figura 7.37: Grafo plano para el ejercicio 7.1.31.2.

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 7.37 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 7.38: Grafo G del ejercicio 7.1.31.5.

- 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 7.38 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:

$$2|E| = 7|V|$$

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 7.1.32. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle (1\ 2\ 3) \rangle$.

1. Construye el conjunto cociente $S_4/H \sim$ de clases laterales por la izquierda xH .

Por el Teorema de Lagrange, sabemos que:

$$[S_4 : H] = \frac{|S_4|}{|H|} = \frac{4!}{3} = 8$$

Por tanto, hemos de encontrar 8 clases laterales por la izquierda distintas:

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

Por tanto, el conjunto cociente es:

$$S_4/H \sim = \{1H, (1\ 2)H, (1\ 4)H, (2\ 4)H, (3\ 4)H, (1\ 2\ 4)H, (1\ 4\ 2)H, (1\ 4\ 3)H\}$$

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?

Calculamos $m(xH)$ para cada clase:

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

Por tanto el grafo resultante es el grafo completo de 8 vértices; es decir, K_8 . La sucesión de grados de sus vértices es:

$$\{D_0(K_8), D_1(K_8), \dots, D_7(K_8)\} = \{0, \dots, 0, 8\}$$

Su matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Figura 7.39: Grafo G del ejercicio 7.1.33.

No es de Euler, puesto que tiene vértices de grado impar. Tampoco es plano, puesto que puede contraerse a K_5 . No obstante, sí es de Hamilton, puesto que para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 8 + 8 = 16 \geq 8 = |V|$$

De hecho, un posible ciclo de Hamilton es:

$$1H \rightarrow (1\ 2)H \rightarrow (1\ 4)H \rightarrow (2\ 4)H \rightarrow (3\ 4)H \rightarrow (1\ 2\ 4)H \rightarrow (1\ 4\ 2)H \rightarrow (1\ 4\ 3)H \rightarrow 1H$$

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.

Tras eliminar la clase $1H$, obtenemos el grafo completo K_7 , que es de Euler puesto que todos sus vértices tienen grado 6 (par).

Ejercicio 7.1.33. 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 7.39.

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:

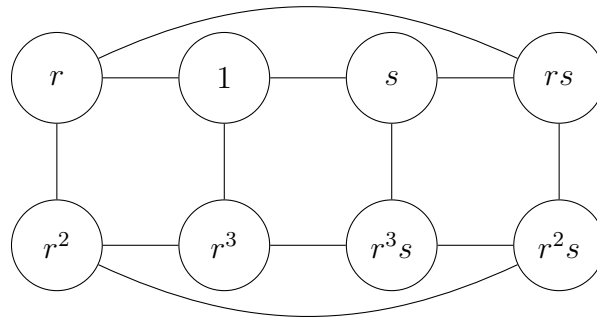
$$1 \rightarrow x \rightarrow x^2 \rightarrow x^3 \rightarrow x^3y \rightarrow x^2y \rightarrow xy \rightarrow y \rightarrow 1 \rightarrow x^3 \rightarrow xy \rightarrow x \rightarrow \\ \rightarrow x^3y \rightarrow y \rightarrow x^2 \rightarrow x^2y \rightarrow 1$$

Ejercicio 7.1.34. 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 7.40: Grafo G del ejercicio 7.1.34.

El grafo es el de la Figura 7.40.

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:

$$1 \rightarrow r \rightarrow r^2 \rightarrow r^3 \rightarrow r^3s \rightarrow r^2s \rightarrow rs \rightarrow s \rightarrow 1$$

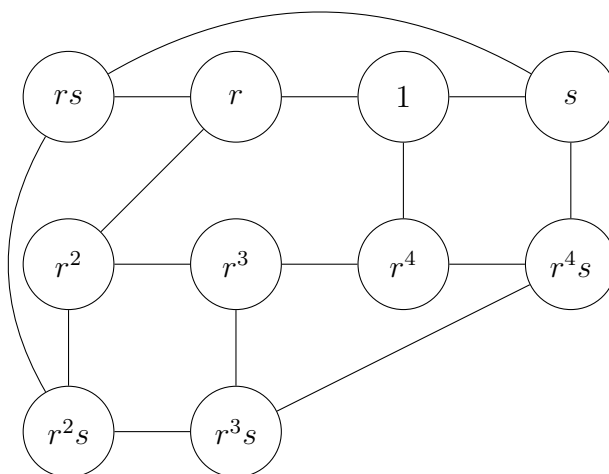
Además, en la Figura 7.40 se puede ver que G es plano.

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 7.1.35. 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 7.41: Grafo G del ejercicio 7.1.35.

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 7.41.

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 7.41 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' sí será de Euler, puesto que todos los vértices anteriores tendrán grado 4 y el nuevo vértice tendrá grado 10. Por tanto, será de Euler.

Ejercicio 7.1.36. 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 7.42: Grafo del ejercicio 7.1.36.1.

- a) Es de Euler.
- b) No es de Hamilton.
- c) Es plano.

El grafo en cuestión se encuentra en la Figura 7.42. 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**).

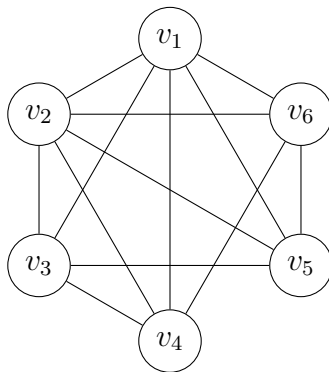


Figura 7.43: Grafo del ejercicio 7.1.36.4.

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 7.38, 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 7.43, 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 7.1.37. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle (1\ 2\ 3) \rangle$.

1. Construye el conjunto cociente S_4 / \sim_H de clases laterales por la derecha Hx , $x \in S_4$.

Por el Teorema de Lagrange, sabemos que:

$$[S_4 : H] = |S_4 / \sim_H| = \frac{|S_4|}{|H|} = \frac{4!}{3} = 8$$

Figura 7.44: Grafo G del ejercicio 7.1.37.

Por tanto, hemos de encontrar 8 clases laterales por la derecha distintas:

$$\begin{aligned}
 H1 &= \langle (1\ 2\ 3) \rangle = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H(1\ 2\ 3) = H(1\ 3\ 2) \\
 H(1\ 2) &= \{(1\ 2), (1\ 3), (2\ 3)\} = H(1\ 3) = H(2\ 3) \\
 H(1\ 4) &= \{(1\ 4), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\} = H(1\ 4\ 2\ 3) = H(1\ 4\ 3\ 2) \\
 H(2\ 4) &= \{(2\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4)\} = H(1\ 2\ 4\ 3) = H(1\ 3\ 2\ 4) \\
 H(3\ 4) &= \{(3\ 4), (1\ 2\ 3\ 4), (1\ 3\ 4\ 2)\} = H(1\ 2\ 3\ 4) = H(1\ 3\ 4\ 2) \\
 H(1\ 2\ 4) &= \{(1\ 2\ 4), (1\ 3)(2\ 4), (2\ 4\ 3)\} = H(1\ 3)(2\ 4) = H(2\ 4\ 3) \\
 H(1\ 3\ 4) &= \{(1\ 3\ 4), (2\ 3\ 4), (1\ 2)(3\ 4)\} = H(2\ 3\ 4) = H(1\ 2)(3\ 4) \\
 H(1\ 4\ 2) &= \{(1\ 4\ 2), (1\ 4\ 3), (1\ 4)(2\ 3)\} = H(1\ 4\ 3) = H(1\ 4)(2\ 3)
 \end{aligned}$$

Por tanto, el conjunto cociente es:

$$S_4 / \sim_H = \{H1, H(1\ 2), H(1\ 4), H(2\ 4), H(3\ 4), H(1\ 2\ 4), H(1\ 3\ 4), H(1\ 4\ 2)\}$$

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?

Tenemos que:

$$\begin{aligned}
 n(H1) &= 3 & n(H(1\ 2)) &= 2 \\
 n(H(1\ 4)) &= n(H(2\ 4)) = n(H(3\ 4)) &= 4 \\
 n(H(1\ 2\ 4)) &= n(H(1\ 3\ 4)) = n(H(1\ 4\ 2)) &= 6
 \end{aligned}$$

El grafo es el de la Figura 7.44.

La sucesión de grados de dicho grafo G es:

$$\{D_0(G), D_1(G), D_2(G), D_3(G), D_4(G), D_5(G), D_6(G), D_7(G)\} = \{0, 0, 0, 4, 3, 0, 1, 0\}$$

Su matriz de Adyacencia, considerando la numeración

$$H1, H(1\ 2), H(1\ 4), H(2\ 4), H(3\ 4), H(1\ 2\ 4), H(1\ 3\ 4), H(1\ 4\ 2)$$

es la siguiente:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Como vemos, este grafo sí es plano. Además, como tiene vértices de grado impar, no es de Euler. Por último, tampoco es de Hamilton, pues el vértice $H(1\ 2)$ divide al grafo en dos componentes conexas, por lo que habría que pasar por él dos veces para hacer un circuito de Hamilton.

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' .

Supongamos que quitamos la arista entre $H(2\ 4)$ y $H(1\ 4)$. Entonces, todos los vértices de G' tendrán grado par a excepción de dos de ellos, $H(3\ 4)$ y $H1$. Por tanto, G' no es de Euler pero sí admite un camino de Euler entre esos dos nodos. Este por ejemplo sería:

$$H(3\ 4) \rightarrow H(1\ 2) \rightarrow H(1\ 4) \rightarrow H(3\ 4) \rightarrow H(2\ 4) \rightarrow H(1\ 2) \rightarrow H(1\ 4\ 2) \rightarrow H1 \rightarrow \\ \rightarrow H(1\ 3\ 4) \rightarrow H(1\ 4\ 2) \rightarrow H(1\ 2\ 4) \rightarrow H(1\ 3\ 4) \rightarrow H(1\ 2) \rightarrow H(1\ 2\ 4) \rightarrow H1$$

Ejercicio 7.1.38. Se considera el grupo A_4 y su subgrupo $H = \langle (1\ 2)(3\ 4) \rangle$. 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:

- a) G es plano pero no es de Hamilton.
- b) G no es plano y tiene dos vértices conectados por un camino de Euler.
- c) G es de Hamilton pero no es de Euler.

Por el Teorema de Lagrange, sabemos que:

$$[A_4 : H] = |A_4 / H \sim| = \frac{|A_4|}{|H|} = \frac{12}{2} = 6$$

Figura 7.45: Grafo G del ejercicio 7.1.38.

Por tanto, hemos de encontrar 6 clases laterales por la izquierda distintas:

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

Por tanto, el conjunto cociente es:

$$A_4 / {}_H \sim = \{1H, (1\ 3)(2\ 4)H, (1\ 2\ 3)H, (1\ 2\ 4)H, (1\ 3\ 2)H, (1\ 4\ 2)H\}$$

Tenemos que:

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

El grafo es el de la Figura 7.45. Sabemos que no es de Hamilton por tener un vértice de grado 1. Además, no es plano, pues un subgrafo suyo es K_5 . Aunque no es de Euler por tener vértices de grado impar, sí tiene un camino de Euler entre $(1\ 3)(2\ 4)H$ y $1H$, puesto que son los únicos vértices de grado impar. Por tanto, la respuesta correcta es la **b**).

Ejercicio 7.1.39. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle (1\ 2\ 3\ 4) \rangle$.

1. Construye el conjunto cociente $S_4 / {}_H \sim$ de clases laterales por la izquierda xH . ¿Es $H < S_4$?

Por el Teorema de Lagrange, sabemos que:

$$[S_4 : H] = |S_4 /_H \sim| = \frac{|S_4|}{|H|} = \frac{4!}{4} = 6$$

Por tanto, hemos de encontrar 6 clases laterales por la izquierda distintas:

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

Por tanto, el conjunto cociente es:

$$S_4 /_H \sim = \{1H, (1\ 2)H, (1\ 3)H, (1\ 4)H, (2\ 3)H, (3\ 4)H\}$$

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?

Calculamos $m(xH)$ para cada clase:

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

Por tanto, el grafo consiste de K_5 con un vértice adicional $((1\ 3)H)$ aislado. Por tanto, el grafo no es plano, ni de Euler ni de Hamilton. La sucesión de grados de dicho grafo G es:

$$\{D_0(G), D_1(G), D_2(G), D_3(G), D_4(G), D_5(G)\} = \{1, 0, 0, 0, 5, 0\}$$

Su matriz de Adyacencia, considerando la numeración

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

es la siguiente:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

3. Considera el subgrafo G' obtenido a partir de G eliminando la clase $(1\ 3)H$. ¿Es G' de Euler?

El grafo resultante es K_5 , que sabemos que sí es de Euler.

Ejercicio 7.1.40. 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 7.1.41 (Parcial DGIIM 2024/24). Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle (1\ 3\ 4) \rangle$.

1. Construye el conjunto cociente S_4 / \sim_H de clases laterales por la derecha Hx , $x \in S_4$.

Por el Teorema de Lagrange, sabemos que:

$$[S_4 : H] = |S_4 / \sim_H| = \frac{|S_4|}{|H|} = \frac{4!}{3} = 8$$

Por tanto, hemos de encontrar 8 clases laterales por la derecha distintas:

$$\begin{aligned} H1 &= \{1, (1\ 3\ 4), (1\ 4\ 3)\} = H(1\ 3\ 4) = H(1\ 4\ 3) \\ H(1\ 2) &= \{(1\ 2), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3)\} = H(1\ 2\ 3\ 4) = H(1\ 2\ 4\ 3) \\ H(1\ 3) &= \{(1\ 3), (1\ 4), (3\ 4)\} = H(1\ 4) = H(3\ 4) \\ H(2\ 3) &= \{(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 3\ 2)\} = H(1\ 3\ 2\ 4) = H(1\ 4\ 3\ 2) \\ H(2\ 4) &= \{(2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3)\} = H(1\ 3\ 4\ 2) = H(1\ 4\ 2\ 3) \\ H(1\ 2\ 3) &= \{(1\ 2\ 3), (1\ 2\ 4), (1\ 2)(3\ 4)\} = H(1\ 2\ 4) = H(1\ 2)(3\ 4) \\ H(1\ 3\ 2) &= \{(1\ 3\ 2), (1\ 4)(2\ 3), (2\ 4\ 3)\} = H(1\ 4)(2\ 3) = H(2\ 4\ 3) \\ H(1\ 4\ 2) &= \{(1\ 4\ 2), (2\ 3\ 4), (1\ 3)(2\ 4)\} = H(2\ 3\ 4) = H(1\ 3)(2\ 4) \end{aligned}$$

Por tanto, el conjunto cociente es:

$$S_4 / \sim_H = \{H1, H(1\ 2), H(1\ 3), H(2\ 3), H(2\ 4), H(1\ 2\ 3), H(1\ 3\ 2), H(1\ 4\ 2)\}$$

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.

Calculamos $n(Hx)$ para cada clase:

$$\begin{aligned} n(H1) &= 3 & n(H(1\ 3)) &= 2 \\ n(H(1\ 2)) &= n(H(2\ 3)) = n(H(2\ 4)) &= 4 \\ n(H(1\ 2\ 3)) &= n(H(1\ 3\ 2)) = n(H(1\ 4\ 2)) &= 6 \end{aligned}$$

El grafo es el de la Figura 7.46.

La sucesión de grados de dicho grafo G es:

$$\{D_0(G), D_1(G), D_2(G), D_3(G), D_4(G), D_5(G), D_6(G), D_7(G)\} = \{0, 0, 0, 4, 3, 0, 1, 0\}$$

Su matriz de Adyacencia, considerando la numeración

$$H1, H(1\ 3), H(2\ 4), H(1\ 2), H(2\ 3), H(1\ 2\ 3), H(1\ 3\ 2), H(1\ 4\ 2)$$

es la siguiente:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Figura 7.46: Grafo G del ejercicio 7.1.41.

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?

No, no verifica ninguna de las dos, puesto que G no es de Hamilton. No obstante, sí es plano, por lo que verifica las condiciones necesarias para ser plano. Por último, puesto que tiene vértices de grado impar, no es de Euler.

4. Considera el subgrafo G' de G obtenido al suprimir la arista entre las clases $H(2 3)$ y $H(2 4)$. ¿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' .

Sigue sin ser de Euler ni de Hamilton, aunque sí es plano. De nuevo, sí hay un camino de Euler entre $H(1 2)$ y $H1$. Este sería:

$$H(1 2) \rightarrow H(2 4) \rightarrow H(1 3) \rightarrow H(1 2) \rightarrow H(2 3) \rightarrow H(1 3) \rightarrow H(1 4 2) \rightarrow H1 \rightarrow \\ \rightarrow H(1 3 2) \rightarrow H(1 4 2) \rightarrow H(1 2 3) \rightarrow H(1 3) \rightarrow H(1 3 2) \rightarrow H(1 2 3) \rightarrow H1$$

7.2. Grupos: generalidades y ejemplos

Ejercicio 7.2.1. 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 7.2.2. 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 7.2.3. 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 7.2.4. 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 7.2.5. 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 7.2.6. 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 7.2.7. 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 7.2.8. 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 7.2.9. 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 7.2.10.

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 7.2.11. 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 7.2.12. 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 7.2.13. 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 7.2.14. 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 7.2.15. 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 7.2.16. 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 7.2.17. 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 $s_1(s_2)^{-1}(s_1)^{-1}$.

$$\begin{aligned}s_1(s_2)^{-1}(s_1)^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 2 & 4 \end{pmatrix} = \\ &= (1\ 3)(2\ 5\ 7\ 4\ 6) \implies O(s_1(s_2)^{-1}(s_1)^{-1}) = \text{mcm}(2, 5) = 10\end{aligned}$$

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 7.2.18. 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 7.2.19. 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 7.2.20. 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 7.2.21. 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 7.2.22. 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 7.2.23. 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 7.2.24. 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 7.2.25. 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 7.2.26.

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 7.2.27. 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 7.2.28. 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 7.2.22, mientras que el generador de $\text{GL}_2(\mathbb{Z}_2)$ se ha visto en el Ejercicio 7.2.10.

$$\begin{aligned} D_3 &= \langle r, s \mid r^3 = 1, s^2 = 1, sr = r^{-1}s \rangle \\ S_3 &= \langle (1\ 2\ 3), (1\ 2) \rangle \\ \text{GL}_2(\mathbb{Z}_2) &= \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \end{aligned}$$

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 7.2.29. 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:

$$\begin{aligned} f(x \otimes y) &= 1 - (x \otimes y) = 1 - (x + y - xy) = 1 - x - y + xy \\ f(x)f(y) &= (1 - x)(1 - y) = 1 - x - (1 - x)y = 1 - x - y + xy \end{aligned}$$

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 7.2.30.

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:

$$\begin{aligned} Q_2 &= \{\pm 1, \pm i, \pm j, \pm k\} \\ D_4 &= \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \end{aligned}$$

Calculamos los órdenes de D_4 :

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

Por otro lado, calculamos los órdenes de Q_2 :

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

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 7.2.31. Calcular el orden de:

1. La permutación $\sigma = (1 \ 8 \ 10 \ 4)(2 \ 8)(5 \ 1 \ 4 \ 8) \in S_{15}$.

$$\begin{aligned} \sigma &= (2 \ 10 \ 4)(5 \ 8) \\ O(\sigma) &= \text{mcm}(3, 2) = 6 \end{aligned}$$

2. Cada elemento del grupo \mathbb{Z}_{11}^\times .

$$\begin{aligned} O(1) &= 1 \\ O(3) &= O(4) = O(5) = O(9) = 5 \\ O(2) &= O(6) = O(7) = O(8) = 10 \\ O(10) &= 2 \end{aligned}$$

Ejercicio 7.2.32. 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 7.2.13 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, $G \cong V$. Como G es abeliano, V también lo es.

Ejercicio 7.2.33. 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:

$$1 = (aba^{-1})^n = ab^n a^{-1} \iff a^{-1} = b^n a^{-1} \iff 1 = b^n$$

Comprobemos 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 $O(ba) = O(ab)$.

Considerando ahora $ba \in G$, se tiene que:

$$O(ba) \stackrel{(*)}{=} O(a \, ba \, a^{-1}) = O(a \, b \cdot 1) = O(ab)$$

donde en $(*)$ hemos usado el apartado anterior.

Ejercicio 7.2.34. 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 7.2.35. Sea $f : G \rightarrow H$ un homomorfismo de grupos.

1. $f(x^n) = f(x)^n \, \forall n \in \mathbb{Z}$.

Lo demostraremos en primer lugar para todo $n \in \mathbb{N}$. Por inducción, se tiene que:

- Caso base: $n = 0$.

$$f(x^0) = f(1) = 1 = f(x)^0$$

- Paso inductivo: Supongamos que se cumple para n , y veamos que se cumple para $n + 1$.

$$f(x^{n+1}) = f(x^n x) = f(x^n) f(x) = f(x)^n f(x) = f(x)^{n+1}$$

Veamos ahora qué ocurre con $n \in \mathbb{Z}$, $n < 0$.

$$f(x^n) = f((x^{-1})^{-n}) \stackrel{(*)}{=} f(x^{-1})^{-n} = ((f(x))^{-1})^{-n} = f(x)^n$$

donde en $(*)$ hemos usado que $-n \in \mathbb{N}$. 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 7.2.36.

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.

Opción 1 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.

Opción 2 (Notemos que usaremos conceptos del Tema 3)

Por reducción al absurdo, supongamos que existe un isomorfismo dado por $f : \mathbb{Z} \rightarrow \mathbb{Q}$. Como $\mathbb{Z} = \langle 1 \rangle$ y f es un epimorfismo, entonces tendremos $\mathbb{Q} = \langle f(1) \rangle$. Supongamos que $f(1) = \frac{a}{b}$ con $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. Entonces, se tiene que:

$$\mathbb{Q} = \left\langle \frac{a}{b} \right\rangle = \left\{ \frac{ka}{b} \mid k \in \mathbb{Z} \right\}$$

Sabemos que $a/2b \in \mathbb{Q}$, por lo que $\exists k \in \mathbb{Z}$ tal que:

$$\frac{ka}{b} = \frac{a}{2b} \implies 2kab = ab \implies 2ka = a \implies \begin{cases} a = 0 \\ k = 1/2 \notin \mathbb{Z} \end{cases}$$

Por tanto, $a = 0$. Entonces:

$$f(1) = \frac{0}{b} = 0 \stackrel{(*)}{=} f(0)$$

donde en $(*)$ hemos usado que f es un homomorfismo entre grupos aditivos. Por tanto, f no es inyectiva, lo que contradice que sea un isomorfismo.

Ejercicio 7.2.37. 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.

\impliedby) 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.

Observación. Notemos que este ejercicio es consecuencia directa del Ejercicio 7.2.7, pero lo hacemos por motivos didácticos.

Ejercicio 7.2.38. 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 7.2.39. 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.

7.3. Subgrupos, Generadores, Retículos y Grupos cíclicos

Ejercicio 7.3.1. 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 7.3.2. 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 7.3.3.

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 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 .

Tenemos que:

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

Los órdenes de los elementos de Q_2 son:

$$O(\pm i) = O(\pm j) = O(\pm k) = 4 \quad O(-1) = 2$$

Supongamos ahora $\exists H \leq S_4$ tal que $H \cong Q_2$. Por lo pronto, sabemos que $1 \in H$ y $|H| = 8$. Además, como los isomorfismos mantienen los órdenes, sabemos que en H habrá 6 elementos distintos de orden 4 y 1 de orden 2. Como en S_4 tan solo hay 6 elementos de orden 4, entonces H ha de contener a todos los elementos de orden 4 de S_4 ; es decir:

$$\{1, (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\} \subseteq H$$

Por tanto, ya tenemos 7 elementos de H , y sabemos que el restante es de orden 2 (no sabemos si es una transposición o un producto de dos transposición disjuntas). Por ser H un grupo, tenemos que es cerrado para productos, por lo que:

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

No obstante, hemos encontrado un elemento de orden 3 perteneciente a H , lo cual es una contradicción. Por tanto, no puede existir un subgrupo de S_4 isomorfo a Q_2 .

Para demostrar lo pedido, supongamos que $\exists f : \text{SL}_2(\mathbb{Z}_3) \rightarrow S_4$ un isomorfismo, y consideramos la restricción a $Q = \langle i, j \rangle \cong Q_2$. Sabemos que la siguiente aplicación es un isomorfismo:

$$\begin{aligned} f|_Q : Q &\longrightarrow f_*(Q) \\ x &\longmapsto f(M) \end{aligned}$$

Por tanto, $Q_2 \cong Q \cong f_*(Q)$. Además, como f_* es un homomorfismo y se tiene $Q < \text{SL}_2(\mathbb{Z}_3)$, entonces $f_*(Q) < S_4$. Por tanto, hemos encontrado un subgrupo de S_4 isomorfo a Q_2 , lo cual es una contradicción por lo que hemos demostrado anteriormente. Por tanto, $\text{SL}_2(\mathbb{Z}_3) \not\cong S_4$.

Ejercicio 7.3.4. Razonar que un subconjunto no vacío $X \subseteq G$ de un grupo G es un subgrupo de G si, y sólo si, $X = \langle X \rangle$.

\Rightarrow) 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, $X = \langle X \rangle$.

\Leftarrow) 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 7.3.5. 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 $\langle a \rangle \cap \langle b \rangle = \{1\}$.

Opición 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 el Teorema de Lagrange, sabemos que:

$$\begin{aligned} |\langle a \rangle \cap \langle b \rangle| & \mid |\langle a \rangle| = O(a) \\ |\langle a \rangle \cap \langle b \rangle| & \mid |\langle b \rangle| = O(b) \end{aligned}$$

Por tanto, $|\langle a \rangle \cap \langle b \rangle|$ es divisor común de $O(a)$ y $O(b)$, y por ser $\text{mcd}(O(a), O(b)) = 1$, entonces $|\langle a \rangle \cap \langle b \rangle| = 1$. Por tanto, $\langle a \rangle \cap \langle b \rangle = \{1\}$.

Opición 2 Demostremoslo por doble inclusión.

\supseteq) Como $\langle a \rangle$ y $\langle b \rangle$ son subgrupos de G , entonces $\langle a \rangle \cap \langle b \rangle$ es un subgrupo de G , y en particular es un grupo. Por tanto, $1 \in \langle a \rangle \cap \langle b \rangle$.

\subseteq) Sea $x \in \langle a \rangle \cap \langle b \rangle$.

- Como $x \in \langle a \rangle$, entonces $x = a^s$ para algún $s \in \mathbb{Z}$.
- Como $x \in \langle b \rangle$, entonces $x = b^t$ para algún $t \in \mathbb{Z}$.

Por tanto:

$$1 = (a^{O(a)})^s = (a^s)^{O(a)} = x^{O(a)} = (b^t)^{O(a)} = b^{tO(a)} \implies O(b) \mid tO(a)$$

Como $\text{mcd}(O(a), O(b)) = 1$, entonces $O(b) \mid t$, por lo que $\exists k \in \mathbb{Z}$ tal que $t = kO(b)$. Por tanto:

$$x = b^t = b^{kO(b)} = (b^{O(b)})^k = 1^k = 1$$

Por tanto, $\langle a \rangle \cap \langle b \rangle \subset \{1\}$.

2. Demostrar que $O(ab) = O(a)O(b)$.

Puesto que conmutan, tenemos que:

$$(ab)^k = a^k b^k \quad \forall k \in \mathbb{Z}$$

Por comodidad, sean $O(a) = n$ y $O(b) = m$.

$$(ab)^{nm} = a^{nm} b^{nm} = (a^n)^m (b^m)^n = 1$$

Supongamos ahora $t \in \mathbb{N}$ tal que $(ab)^t = 1$.

$$1 = (ab)^t = a^t b^t \implies a^t = b^{-t} \in \langle a \rangle \cap \langle b \rangle = \{1\} \implies \left\{ \begin{array}{l} a^t = 1 \implies n \mid t \\ a^t = 1 \implies m \mid t \end{array} \right\} \xRightarrow{(*)} nm \mid t$$

donde en $(*)$ hemos usado que $\text{mcd}(n, m) = 1$. Por tanto:

$$O(ab) = nm = O(a)O(b)$$

Ejercicio 7.3.6. 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 7.3.7. 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 7.3.8. 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 .

Opción 1. Por ser S_3 finito, tan solo hemos de comprobar que H es cerrado para el producto. Como vimos, no es necesario comprobar si uno de los elementos es el neutro.

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

Por tanto, $H < S_3$.

Opción 2. Demostremos que $H = \langle (1\ 2\ 3) \rangle$.

- \subseteq) Tan solo será necesario ver que $(1\ 2\ 3)^2 = (1\ 3\ 2)$, y se tendría de manera inmediata que $H \subseteq \langle (1\ 2\ 3) \rangle$.
- \supseteq) Sea $x \in \langle (1\ 2\ 3) \rangle$. Entonces $x = (1\ 2\ 3)^n$ para algún $n \in \mathbb{Z}$. Como $O((1\ 2\ 3)) = 3$, entonces $n \in \{0, 1, 2\}$. Por tanto:

$$x \in \{(1\ 2\ 3)^0, (1\ 2\ 3)^1, (1\ 2\ 3)^2\} = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H$$

2. Describir las diferentes clases de S_3 módulo H .

Por el Teorema de Lagrange, sabemos que:

$$|S_3| = [S_3 : H] \cdot |H| \implies [S_3 : H] = \frac{6}{3} = 2 \implies |S_3 /_H \sim| = |S_3 / \sim_H| = 2$$

Calculamos ahora las clases de equivalencia de $S_3 /_H \sim$:

$$\begin{aligned}1H &= \{1x \mid x \in H\} = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H \\ (1\ 2)H &= \{(1\ 2)x \mid x \in H\} = \{(1\ 2), (1\ 2)(1\ 2\ 3), (1\ 2)(1\ 3\ 2)\} = \{(1\ 2), (2\ 3), (1\ 3)\} \neq H\end{aligned}$$

Como ya hemos encontrado dos clases de equivalencia distintas, entonces hemos encontrado todas las posibles.

$$S_3 /_H \sim = \{H, (1\ 2)H\}$$

Calculamos ahora las clases de equivalencia de S_3 / \sim_H :

$$\begin{aligned}H1 &= \{x1 \mid x \in H\} = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H \\ H(1\ 2) &= \{x(1\ 2) \mid x \in H\} = \{(1\ 2), (1\ 2\ 3)(1\ 2), (1\ 3\ 2)(1\ 2)\} = \{(1\ 2), (1\ 3), (2\ 3)\} \neq H\end{aligned}$$

Por tanto, hemos encontrado todas las clases de equivalencia de S_3 / \sim_H .

$$S_3 / \sim_H = \{H, H(1\ 2)\}$$

Ejercicio 7.3.9. 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, $H = G$.

Demostremos en primer lugar que $[G : H] = |G| \iff H = \{1\}$. Por el Teorema de Lagrange, sabemos que $|G| = [G : H] \cdot |H|$. Por tanto:

$$[G : H] = \frac{|G|}{|H|} = |G| \iff |G| = |G| |H| \iff |H| = 1 \iff H = \{1\}$$

donde, desde el inicio, hemos usado que $|G|, |H| \neq 0$.

De nuevo, por el Teorema de Lagrange, sabemos que $|G| = [G : H] \cdot |H|$. Por tanto:

$$[G : H] = \frac{|G|}{|H|} = 1 \iff |G| = |H|$$

Como además $H \subset G$ por ser subgrupo, tenemos que $[G : H] = 1$ si y solo si $H = G$.

2. Demostrar que si se tienen subgrupos $G_2 \leq G_1 \leq G$, entonces

$$[G : G_2] = [G : G_1][G_1 : G_2],$$

Por un lado, como $G_2 \leq G$, entonces:

$$|G| = [G : G_2] \cdot |G_2|$$

Por otro lado, como $G_1 \leq G$, y $G_2 \leq G_1$, entonces:

$$|G| = [G : G_1] \cdot |G_1| = [G : G_1][G_1 : G_2] \cdot |G_2|$$

Uniendo ambos resultados, tenemos que:

$$[G : G_2] = [G : G_1][G_1 : G_2]$$

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

$$[G : G_r] = \prod_{i=0}^{r-1} [G_i : G_{i+1}].$$

Demotrsamos por inducción sobre r :

- $r = 2$: $G = G_0 \geq G_1 \geq G_2$. Por el apartado anterior, sabemos que:

$$[G : G_2] = [G : G_1][G_1 : G_2]$$

- Supuesto cierto para r , demostramos para $r + 1$: Por hipótesis de inducción, sabemos que:

$$[G : G_r] = \prod_{i=0}^{r-1} [G_i : G_{i+1}]$$

Por otro lado, como $G_{r+1} \leq G_r \leq G$, aplicando el apartado anterior, tenemos que:

$$[G : G_{r+1}] = [G : G_r][G_r : G_{r+1}]$$

Uniendo ambos resultados, tenemos que:

$$[G : G_{r+1}] = \prod_{i=0}^{r-1} [G_i : G_{i+1}] \cdot [G_r : G_{r+1}] = \prod_{i=0}^r [G_i : G_{i+1}]$$

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

$$|G| = \prod_{i=0}^{r-1} [G_i : G_{i+1}].$$

Por el primer apartado, como $G_r = \{1\}$, entonces $[G : G_r] = |G|$. Por tanto, aplicando el apartado anterior, tenemos que:

$$|G| = \prod_{i=0}^{r-1} [G_i : G_{i+1}]$$

Ejercicio 7.3.10.

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.

Como $|G| = 4$, entonces $O(x) \mid 4$ para todo $x \in G$. Por tanto, $O(x) \in \{1, 2, 4\}$. Consideramos los siguientes casos:

- Supongamos $\exists x \in G \mid O(x) = 4$:

En este caso, como x tiene 4 potencias distintas, entonces:

$$\langle x \rangle = \{1, x, x^2, x^3\} \subset G$$

Como además $|\langle x \rangle| = 4 = |G|$, entonces $G = \langle x \rangle$. Por tanto, G es cíclico, $G = C_4$.

- Supongamos $\nexists x \in G \mid O(x) = 4$:

En este caso, $\forall x \in G$, $O(x) \in \{1, 2\}$. Como $O(x) = 1 \iff x = 1$, entonces G tiene 3 elementos de orden 2. Sea $x \in G$ tal que $O(x) = 2$.

En este caso, $\langle x \rangle = \{1, x\} \subset G$. Como $|G| = 4$, ha de existir un elemento $y \in G$ tal que $y \notin \langle x \rangle$ y $O(y) = 2$.

Veamos que G cumple las relaciones del grupo de Klein abstracto:

$$V^{\text{abs}} = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$$

Sabemos que $x^2 = y^2 = 1$. Ahora, nos falta ver que $xy = yx$. Como $xy \in G$, entonces $O(xy) \in \{1, 2\}$. En cualquier caso, $(xy)^2 = 1$, por lo que:

$$xyxy = 1 \implies yxy = x \implies xy = yx$$

Por tanto, por el Teorema de Dyck, $G \cong V^{\text{abs}} \cong V$.

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 .

Seguiremos la misma estrategia que en el apartado anterior. Como $|G| = 6$, entonces $O(x) \mid 6$ para todo $x \in G$. Por tanto, $O(x) \in \{1, 2, 3, 6\}$. Consideramos los siguientes casos:

- Supongamos $\exists x \in G \mid O(x) = 6$:

En este caso, como x tiene 6 potencias distintas, entonces:

$$\langle x \rangle = \{1, x, x^2, x^3, x^4, x^5\} \subset G$$

Como además $|\langle x \rangle| = 6 = |G|$, entonces $G = \langle x \rangle$. Por tanto, G es cíclico, $G = C_6$.

- Supongamos $\nexists x \in G \mid O(x) = 6$:

En este caso, $\forall x \in G$, $O(x) \in \{1, 2, 3\}$. Como $O(x) = 1 \iff x = 1$, entonces G tiene 5 elementos cuyo orden es 2 o 3.

- Supongamos $\nexists x \in G \mid O(x) = 3$:

Entonces, G tiene 5 elementos de orden 2. Sea $x \in G$ tal que $O(x) = 2$.

$$\langle x \rangle = \{1, x\} \subset G$$

Como $|G| = 6$, ha de existir un elemento $y \in G$ tal que $y \notin \langle x \rangle$ y $O(y) = 2$. Veamos que $xy \notin \{1, x, y\}$.

- Si $xy = 1$, entonces $y = x^{-1} = x$, lo cual es una contradicción.
- Si $xy = x$, entonces $y = 1$, lo cual es una contradicción.
- Si $xy = y$, entonces $x = 1$, lo cual es una contradicción.

Por tanto, tenemos que:

$$\langle x, y \rangle = \{1, x, y, xy\} \subset G$$

Por tanto, hemos encontrado un subgrupo de G de orden 4, pero esto es una contradicción, porque por el Teorema de Lagrange, el orden de un subgrupo ha de dividir al orden del grupo.

- Supongamos $\nexists x \in G \mid O(x) = 2$:

En este caso, G tiene 5 elementos de orden 3. Sea $x \in G$ tal que $O(x) = 3$.

$$\langle x \rangle = \{1, x, x^2\} \subset G$$

Como $|G| = 6$, ha de existir un elemento $y \in G$ tal que $y \notin \langle x \rangle$ y $O(y) = 3$. Veamos que $xy \notin \{1, x, x^2, y, y^2\}$.

- Si $xy = 1$, entonces $y = x^{-1} = x^2$, lo cual es una contradicción.
- Si $xy = x$, entonces $y = 1$, lo cual es una contradicción.
- Si $xy = x^2$, entonces $y = x$, lo cual es una contradicción.
- Si $xy = y$, entonces $x = 1$, lo cual es una contradicción.
- Si $xy = y^2$, entonces $x = y$, lo cual es una contradicción.

Por tanto, tenemos que $\{1, x, x^2, y, y^2, xy\} \subset G$. Como $|G| = 6$, entonces $G = \{1, x, x^2, y, y^2, xy\}$. Veamos que $x^2y \notin G$:

- Si $x^2y = 1$, entonces $y = x$, lo cual es una contradicción.
- Si $x^2y = x$, entonces $y = x^2$, lo cual es una contradicción.
- Si $x^2y = x^2$, entonces $y = 1$, lo cual es una contradicción.
- Si $x^2y = y$, entonces $x^2 = 1$, lo cual es una contradicción.
- Si $x^2y = y^2$, entonces $x^2 = y$, lo cual es una contradicción.
- Si $x^2y = xy$, entonces $x = 1$, lo cual es una contradicción.

Por tanto, G no es cerrado para el producto, lo cual es una contradicción.

- Por tanto, $\exists x \in G \mid O(x) = 3$ y $\exists y \in G \mid O(y) = 2$. Comprobemos que G cumple las relaciones del grupo diédrico D_3 :

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

Veamos en primer lugar los elementos de G . Sabemos que $\{1, x, x^2\} \subset G$. Veamos ahora que y no puede ser uno de estos elementos:

$$y = x^2 \implies 1 = y^2 = x^4 = x \implies x = 1$$

Por tanto, $y \notin \{1, x, x^2\}$, y tenemos $\{1, x, x^2, y\} \subset G$. Veamos ahora que $xy \notin \{1, x, x^2, y\}$:

- Si $xy = 1$, entonces $y = x$, lo cual es una contradicción.
- Si $xy = x$, entonces $y = 1$, lo cual es una contradicción.
- Si $xy = x^2$, entonces $y = x$, lo cual es una contradicción.
- Si $xy = y$, entonces $x = 1$, lo cual es una contradicción.

Por tanto, $\{1, x, x^2, y, xy\} \subset G$. Veamos ahora que $x^2y \notin \{1, x, x^2, y, xy\}$:

- Si $x^2y = 1$, entonces $y = x$, lo cual es una contradicción.
- Si $x^2y = x$, entonces $y = x^2$, lo cual es una contradicción.
- Si $x^2y = x^2$, entonces $y = 1$, lo cual es una contradicción.
- Si $x^2y = y$, entonces $x^2 = 1$, lo cual es una contradicción.
- Si $x^2y = xy$, entonces $x = 1$, lo cual es una contradicción.

Por tanto, $\{1, x, x^2, y, xy, x^2y\} \subset G$. Como $|G| = 6$, entonces:

$$G = \{1, x, x^2, y, xy, x^2y\}$$

Como G es un grupo, $yx \in G$. Veamos el valor de yx :

- Si $yx = 1$, entonces $y = x$, lo cual es una contradicción.
- Si $yx = x$, entonces $y = 1$, lo cual es una contradicción.

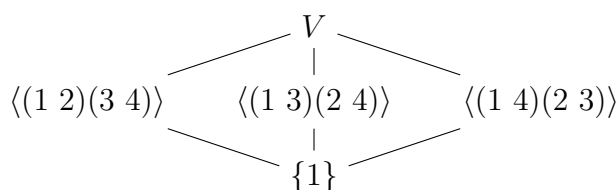


Figura 7.47: Diagrama de Hasse para los subgrupos del grupo de Klein.

- Si $yx = x^2$, entonces $y = x$, lo cual es una contradicción.
- Si $yx = y$, entonces $x = 1$, lo cual es una contradicción.
- Si $yx = xy$, entonces G es abeliano. En este caso, veamos que $O(xy) = 6$:

$$(xy)^2 = x^2 \quad (xy)^3 = y \quad (xy)^4 = x \quad (xy)^5 = x^2y \quad (xy)^6 = 1$$

Por tanto, $O(xy) = 6$, pero habíamos supuesto que $\nexists x \in G$ tal que $O(x) = 6$. Por tanto, hemos llegado a una contradicción.

Por tanto, como $yx \in G$, tan solo queda la opción de que $yx = x^2y$. Por tanto, G cumple las relaciones del grupo diédrico D_3 . Como además $\langle x, y \rangle$ es un grupo de generadores de G y $|G| = |D_3| = 6$, por el Teorema de Dyck, $G \cong D_3$.

Ejercicio 7.3.11. Describir los retículos de subgrupos de los siguientes grupos:

1. El grupo V de Klein.

La complejidad en todo este ejercicio será hallar todos los subgrupos de un cierto grupo. Una vez hallados, dibujar los Diagramas de Hasse no será complicado.

Sabemos que $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Por el Teorema de Lagrange, sabemos que los subgrupos de V han de tener orden 1, 2 o 4. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 4 es V . Veamos ahora los subgrupos de orden 2. Como 2 es primo, entonces los subgrupos de orden 2 han de ser cíclicos. Por tanto, los subgrupos de orden 2 son:

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

Por tanto, el retículo de subgrupos de V es el de la Figura 7.47.

2. El grupo simétrico S_3 .

Sabemos que $|S_3| = 6$. Por el Teorema de Lagrange, sabemos que los subgrupos de S_3 han de tener orden 1, 2, 3 o 6. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 6 es S_3 . Veamos ahora los subgrupos de orden 2 y 3. Como 2 y 3 son primos, entonces los subgrupos de orden 2 y 3 han de ser cíclicos. Sabemos que:

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

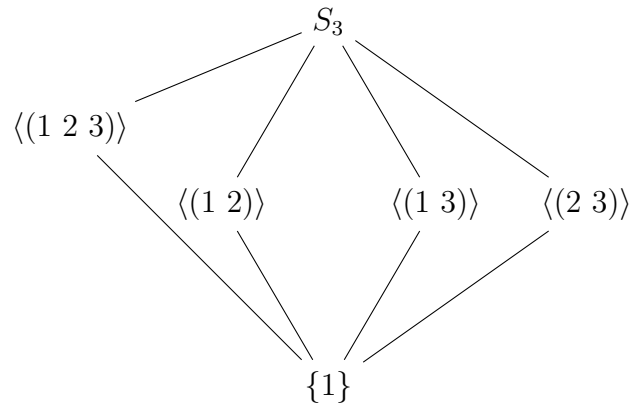


Figura 7.48: Diagrama de Hasse para los subgrupos de S_3 .

Por tanto, los subgrupos de orden 2 son:

$$\begin{aligned}\langle(1\ 2)\rangle &= \{1, (1\ 2)\} \\ \langle(1\ 3)\rangle &= \{1, (1\ 3)\} \\ \langle(2\ 3)\rangle &= \{1, (2\ 3)\}\end{aligned}$$

Por otro lado, los subgrupos de orden 3 son:

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

Notemos que no ha hecho falta calcular $\langle(1\ 3\ 2)\rangle$ puesto que, $\langle x \rangle = \langle x^{-1} \rangle$. Por tanto, el retículo de subgrupos de S_3 es el de la Figura 7.48.

3. El grupo diédrico D_4 .

Sabemos que $|D_4| = 8$. Por el Teorema de Lagrange, sabemos que los subgrupos de D_4 han de tener orden 1, 2, 4 u 8. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 8 es D_4 . Veamos ahora los subgrupos de orden 2 y 4. Como 2 es primo, entonces los subgrupos de orden 2 han de ser cíclicos. Sabemos que:

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

Calculemos el orden de los elementos de D_4 :

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

Por tanto, los subgrupos de orden 2 son:

$$\begin{aligned}\langle r^2 \rangle &= \{1, r^2\} \\ \langle s \rangle &= \{1, s\} \\ \langle sr \rangle &= \{1, sr\} \\ \langle sr^2 \rangle &= \{1, sr^2\} \\ \langle sr^3 \rangle &= \{1, sr^3\}\end{aligned}$$

Calculamos ahora los subgrupos de orden 4. Sabemos que:

$$\langle r \rangle = \{1, r, r^2, r^3\} = \langle r^3 \rangle$$

No obstante, busquemos más grupos de orden 4, algo que no será sencillo. Dado un subgrupo H , como $H = \langle H \rangle$, entonces siempre podemos encontrar un conjunto de generadores suyo. Buscaremos por tanto conjuntos de generadores con 1, 2, 3 y 4 elementos.

■ Con un elemento:

Los subgrupos generados por un único elemento sabemos que son cíclicos y el orden del elemento ha de ser el orden del grupo. Por tanto, el único subgrupo de D_4 de orden 4 es:

$$\langle r \rangle = \{1, r, r^2, r^3\} = \langle r^3 \rangle$$

■ Con dos elementos:

A partir de aquí, es más complejo. Sabemos que los generadores no han de ser ni r ni r^3 , pues estos generarían un grupo de orden mayor que 4. Además, incluir a 1 como generador no tiene sentido. Por último, notemos que x y x^{-1} generan el mismo grupo. Las posibles combinaciones son:

$$\begin{aligned} \langle s, r^2 \rangle &= \{1, s, r^2, sr^2\} \\ \langle s, sr \rangle &= D_4 \text{ pues } r = s \cdot sr \\ \langle s, sr^2 \rangle &= \langle s, r^2 \rangle \text{ pues } s \cdot sr^2 = r^2 \\ \langle s, sr^3 \rangle &\supset \langle r^3 \rangle \text{ pues } s \cdot sr^3 = r^3 \\ \langle sr, r^2 \rangle &= \{1, sr, sr^3, r^2\} \\ \langle sr, sr^2 \rangle &\supset \langle r \rangle \text{ pues } sr \cdot sr^2 = ssr^3r^2 = r \\ \langle sr, sr^3 \rangle &= \langle sr, r^2 \rangle \text{ pues } sr \cdot sr^3 = r^2 \\ \langle r^2, sr^2 \rangle &= \langle s, r^2 \rangle \text{ pues } sr^2 \cdot r^2 = s \\ \langle r^2, sr^3 \rangle &= \langle sr, r^2 \rangle \text{ pues } sr^3 \cdot r^2 = sr \\ \langle sr^2, sr^3 \rangle &= D_4 \text{ pues } r = sr^2 \cdot sr^3 \text{ y } sr^3 \cdot r = s \end{aligned}$$

Por tanto, y en resumen, los únicos subgrupos de D_4 de orden 4 generados por dos elementos son:

$$\begin{aligned} \langle s, r^2 \rangle &= \{1, s, r^2, sr^2\} \\ \langle sr, r^2 \rangle &= \{1, sr, sr^3, r^2\} \end{aligned}$$

■ Con tres elementos:

Supongamos (pues en otro caso ya se habría estudiado) que todos los elementos generadores son de orden 2 y distintos. Sean estos x , y y z . Como $\langle x, y \rangle$ nos proporciona un subgrupo de orden 4 o mayor, caben dos posibilidades:

- Al añadir z como generador, no se generen más elementos. En este caso, $\langle x, y, z \rangle = \langle x, y \rangle$, caso ya estudiado.

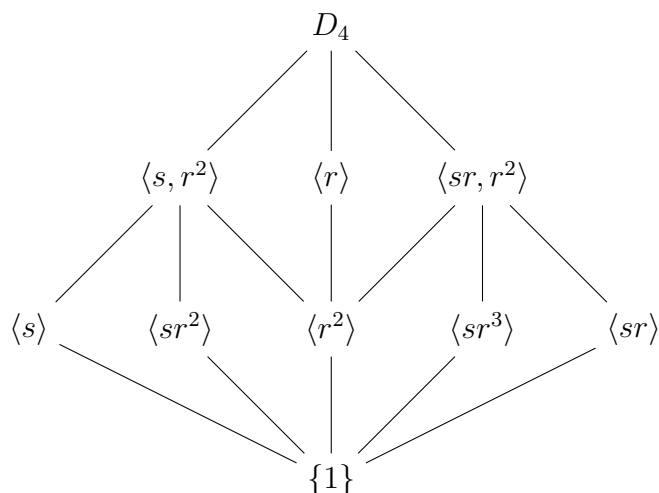


Figura 7.49: Diagrama de Hasse para los subgrupos de D_4 .

- Al añadir z como generador, se generen más elementos. En este caso, $\langle x, y, z \rangle = D_4$.
- Con cuatro elementos:
Supongamos (pues en otro caso ya se habría estudiado) que todos los elementos generadores son de orden 2 y distintos. Entonces, como también el 1 pertenecerá a dicho subgrupo, tenemos que este grupo será D_4 .

Por tanto, los únicos subgrupos de D_4 de orden 4 son:

$$\begin{aligned}\langle r \rangle &= \{1, r, r^2, r^3\} = \langle r^3 \rangle \\ \langle s, r^2 \rangle &= \{1, s, r^2, sr^2\} \\ \langle sr, r^2 \rangle &= \{1, sr, sr^3, r^2\}\end{aligned}$$

Por tanto, el retículo de subgrupos de D_4 es el de la Figura 7.49.

4. El grupo cuaternio Q_2 .

Sabemos que $|Q_2| = 8$. Por el Teorema de Lagrange, sabemos que los subgrupos de Q_2 han de tener orden 1, 2, 4 u 8. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 8 es Q_2 . Veamos en primer lugar el orden de los elementos de Q_2 :

$$O(1) = 1 \quad O(-1) = 2 \quad O(\pm i) = O(\pm j) = O(\pm k) = 4$$

Como 2 es primo, los subgrupos de orden 2 han de ser cíclicos y generados por un elemento de orden 2. Por tanto, el único subgrupo de orden 2 es:

$$\langle -1 \rangle = \{1, -1\}$$

Respecto a los subgrupos de orden 4, buscaremos conjuntos de generadores de 1, 2, 3 y 4 elementos.

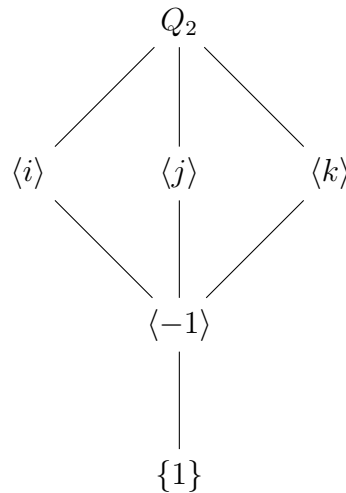


Figura 7.50: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

■ Con un elemento:

Los subgrupos generados por un único elemento sabemos que son cíclicos y el orden del elemento ha de ser el orden del grupo. Por tanto, estos son:

$$\langle i \rangle = \{1, i, -1, -i\}$$

$$\langle j \rangle = \{1, j, -1, -j\}$$

$$\langle k \rangle = \{1, k, -1, -k\}$$

■ Con dos elementos:

Supongamos (pues en otro caso ya se habría estudiado) que los generadores no son de orden 4. Entonces tan solo puede ser el 1 y el -1 , caso ya estudiado. Por tanto, no consideramos ni este caso ni los generados por más elementos.

Por tanto, el retículo de subgrupos de Q_2 es el de la Figura 7.50.

5. El grupo alternado A_4 .

Sabemos que $|A_4| = 12$. Por el Teorema de Lagrange, sabemos que los subgrupos de A_4 han de tener orden 1, 2, 3, 4, 6 o 12. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 12 es A_4 . Veamos ahora los subgrupos de orden 2, 3, 4 y 6. Para ello, antes de nada, mostremos los elementos de A_4 :

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

Como $V < A_4$, entonces los subgrupos de V son subgrupos de A_4 . Estos son:

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

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

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

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

Veamos si hay más subgrupos de orden 2. Como 2 es primo, estos han de ser cíclicos generados por un elemento de orden 2; pero no hay más elementos de orden 2 en A_4 . Por tanto, los subgrupos de orden 2 son los anteriormente mencionados.

Veamos ahora los subgrupos de orden 3. Como 3 es primo, estos han de ser cíclicos generados por un elemento de orden 3. Además, hemos de tener en cuenta que $\langle x \rangle = \langle x^{-1} \rangle$. Por tanto, los subgrupos de orden 3 son:

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

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

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

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

Veamos ahora los subgrupos de orden 4. Como 4 no es primo, no es tan sencillo. Buscaremos que estén generados por 1, 2, 3 y 4 elementos.

■ Con un elemento:

Los subgrupos generados por un único elemento sabemos que son cíclicos y el orden del elemento ha de ser el orden del grupo. Como no hay elementos de orden 4, no hay subgrupos de orden 4 generados por un único elemento.

■ Con dos elementos:

Supongamos (pues en otro caso ya se habría estudiado) que los dos elementos son distintos y de orden 2 (pues el orden de todo elemento debe dividir al orden del subgrupo al que pertenece). Entonces, llegamos al grupo de Klein, caso ya estudiado. Por tanto, no consideramos generadores de más elementos.

Respecto a los subgrupos de orden 6, en el ejemplo de la página 72 se vió que no existen subgrupos de orden 6 en A_4 . Por tanto, el retículo de subgrupos de A_4 es el de la Figura 7.51.

Ejercicio 7.3.12. 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 .

Sabemos que, para cada divisor de p^n , existe un subgrupo de C_{p^n} de ese orden. En concreto, los únicos subgrupos de C_{p^n} son los de la forma $\langle x^{p^k} \rangle$ con $k \in \{0, \dots, n\}$. Además:

$$O(\langle x^{p^k} \rangle) = \frac{O(x)}{\text{mcd}(O(x), p^k)} = \frac{p^n}{\text{mcd}(p^n, p^k)} = \frac{p^n}{p^k} = p^{n-k}$$

Por tanto, $\langle x^{p^k} \rangle = C_{p^{n-k}}$. Además, fijado $k \in \{0, \dots, n\}$, tenemos que $\langle x^{p^{k+1}} \rangle \subset \langle x^{p^k} \rangle$, puesto que $x^{p^{k+1}} = (x^{p^k})^p$. Por tanto, el retículo de subgrupos de C_{p^n} es el de la Figura 7.52.

En particular, para C_8 , tenemos que $p = 2$ y $n = 3$. Por tanto, el retículo de subgrupos de C_8 es el de la Figura 7.53.

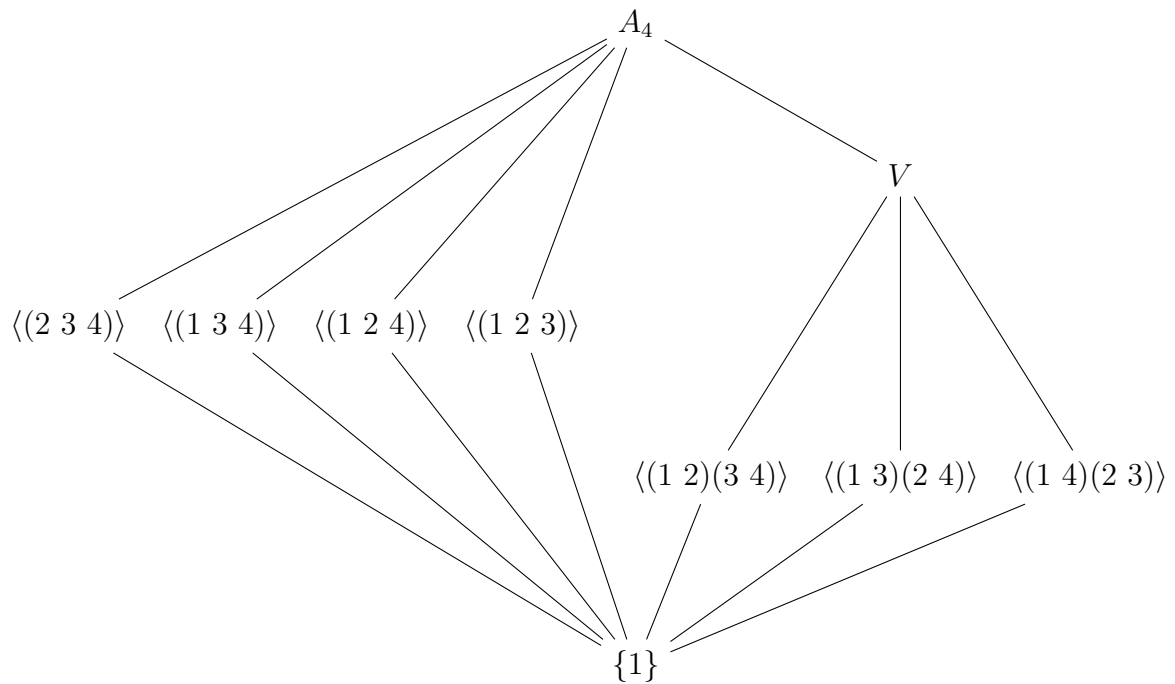


Figura 7.51: Diagrama de Hasse para los subgrupos del grupo alternado A_4 .

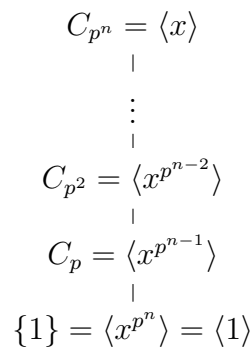


Figura 7.52: Retículo de subgrupos de C_{p^n} para el Ejercicio 7.3.12.

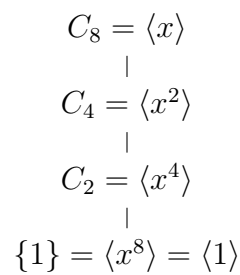
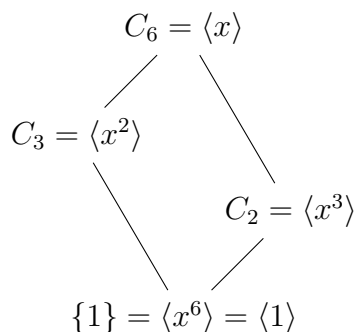


Figura 7.53: Retículo de subgrupos de C_8 para el Ejercicio 7.3.12.



Figura 7.54: Retículo de subgrupos de para el Ejercicio 7.3.13.

Figura 7.55: Retículo de subgrupos de C_6 para el Ejercicio 7.3.14.

Ejercicio 7.3.13. Demostrar que un grupo finito $G \neq \{1\}$ carece de subgrupos propios, esto es, que su retículo de subgrupos es el de la Figura 7.54 si, y sólo si, $G = C_p$ es un grupo cíclico de orden primo.

\Rightarrow) Supongamos que G es un grupo finito que carece de subgrupos propios. Como $G \neq \{1\}$, sea $x \in G \setminus \{1\}$. Entonces, $\langle x \rangle \neq \{1\}$ es un subgrupo de G ; y como este no es propio, entonces $\langle x \rangle = G$. Por tanto, G es cíclico.

Por último, por ser G cíclico sabemos que, por cada divisor de $|G|$, existe un subgrupo de G de ese orden. Como G no tiene subgrupos propios, entonces los únicos divisores de $|G|$ son 1 y $|G|$. Por tanto, $|G|$ es primo.

\Leftarrow) Supongamos que $G = C_p$ es un grupo cíclico de orden primo. Sabemos que, por cada divisor de $|G|$, existe un subgrupo de G de ese orden. Como $|G| = p$ es primo, entonces los únicos divisores de $|G|$ son 1 y $|G|$. Por tanto, G carece de subgrupos propios.

Ejercicio 7.3.14. Describir los retículos de subgrupos de los grupos cíclicos siguientes:

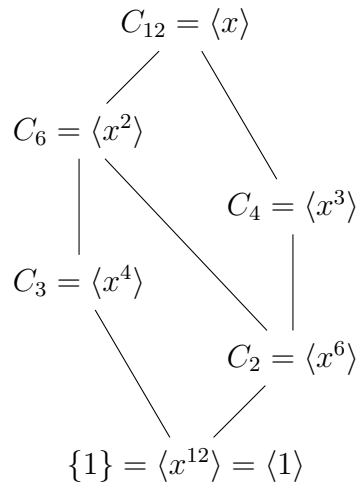
1. C_6 .

Sabemos que los subgrupos propios de C_6 son de la forma $\langle x^k \rangle$ con $k \in \{2, 3\}$. Además, $O(x^k) = \frac{6}{\gcd(6,k)} = \frac{6}{k}$. Por tanto, estos son:

$$\begin{aligned} \langle x^2 \rangle &= \{1, x^2, x^4\} \\ \langle x^3 \rangle &= \{1, x^3\} \end{aligned}$$

Por tanto, el retículo de subgrupos de C_6 es el de la Figura 7.55.

2. C_{12} .

Figura 7.56: Retículo de subgrupos de C_{12} para el Ejercicio 7.3.14.

Sabemos que los subgrupos propios de C_{12} son de la forma $\langle x^k \rangle$ con $k \in \{2, 3, 4, 6\}$. Además, $O(x^k) = \frac{12}{\gcd(12,k)} = \frac{12}{k}$. Por tanto, estos son:

$$\langle x^2 \rangle = \{1, x^2, x^4, x^6, x^8, x^{10}\}$$

$$\langle x^3 \rangle = \{1, x^3, x^6, x^9\}$$

$$\langle x^4 \rangle = \{1, x^4, x^8\}$$

$$\langle x^6 \rangle = \{1, x^6\}$$

Por tanto, el retículo de subgrupos de C_{12} es el de la Figura 7.56.

Ejercicio 7.3.15. 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 $H_2 = \langle t^{46} \rangle$?

Estudiamos en primer lugar el grupo H_2 . Como $O(t) = 136$, entonces:

$$H_2 = \langle t^{46} \rangle = \langle t^{\gcd(136,46)} \rangle = \langle t^2 \rangle$$

Por otro lado:

$$\begin{aligned} H_1 &= \langle t^{48}, t^{72} \rangle = \langle t^{48} \rangle \vee \langle t^{72} \rangle = \langle t^{\gcd(136,48)} \rangle \vee \langle t^{\gcd(136,72)} \rangle \\ &= \langle t^8 \rangle \vee \langle t^8 \rangle = \langle t^8 \rangle \end{aligned}$$

Por tanto, se nos pide estudiar la relación entre los subgrupos $\langle t^2 \rangle$ y $\langle t^8 \rangle$. Puesto que $t_8 \in \langle t^2 \rangle$, entonces:

$$H_1 = \langle t^8 \rangle < \langle t^2 \rangle = H_2$$

Ejercicio 7.3.16. Demostrar que el grupo de unidades \mathbb{Z}_7^\times es un grupo cíclico.

Opción 1. Veamos que $O(5) = 6$:

$$5^2 = 4$$

$$5^3 = 6$$

$$5^4 = 2$$

$$5^5 = 3$$

$$5^6 = 1$$

Por tanto, $\mathbb{Z}_7^\times = \langle 5 \rangle$ es un grupo cíclico.

Opción 2. Sabemos que $|\mathbb{Z}_7^\times| = 6$. Por el Ejercicio 7.3.10, sabemos que hay dos posibilidades, o bien \mathbb{Z}_7^\times es cíclico, o bien $\mathbb{Z}_7^\times \cong D_3$. No obstante, no puede ser isomorfo a D_3 , puesto que D_3 no es abeliano y \mathbb{Z}_7^\times sí lo es. Por tanto, \mathbb{Z}_7^\times es cíclico.

Ejercicio 7.3.17. 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:

$$O(\theta(x)) \mid n, \quad \text{y} \quad \theta(x^k) = \theta(x)^k \quad \forall k \in \{0, \dots, n-1\}.$$

Para la primera parte, queremos ver que $(\theta(x))^n = 1$. Sabemos que:

$$1 = \theta(1) = \theta(x^n) = \theta(x)^n \implies O(\theta(x)) \mid n$$

Para ver el segundo resultado, es suficiente ver que, por ser un homomorfismo, de hecho se tiene para todo $k \in \mathbb{Z}$.

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 $\theta_g(x) = g$.

Veamos que $g^n = 1$. Como $O(g) \mid n$, existe $m \in \mathbb{Z}$ tal que $n = m \cdot O(g)$. Por tanto:

$$g^n = g^{m \cdot O(g)} = (g^{O(g)})^m = 1^m = 1$$

Por tanto, por el Teorema de Dyck, 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, $O(g) = n$.

Partimos de:

$$\theta_g \text{ es monomorfismo} \iff \ker(\theta_g) = \{1\}$$

Calculemos el núcleo de θ_g :

$$\begin{aligned} \ker(\theta_g) &= \{x \in C_n \mid \theta_g(x) = 1\} = \{x^k \mid k \in \{0, \dots, n-1\}, \theta_g(x^k) = 1\} \\ &= \{x^k \mid k \in \{0, \dots, n-1\}, g^k = 1\} \end{aligned}$$

Como $O(x) = n$, sabemos que $x^k \neq 1$ para $k \in \{1, \dots, n-1\}$. Por tanto:

$$\ker(\theta_g) = \{1\} \iff g^k \neq 1 \quad \forall k \in \{1, \dots, n-1\} \iff O(g) \geq n$$

Como partimos de que $O(g) \mid n$, entonces:

$$\theta_g \text{ es monomorfismo} \iff O(g) = n$$

4. Existe un isomorfismo de grupos

$$\mathcal{U}(\mathbb{Z}_n) \cong \text{Aut}(C_n),$$

dado por $r \mapsto f_r$ para cada $r = 1, \dots, n-1$ 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 $\varphi(n)$.

Para cada $r \in \{1, \dots, n-1\}$ con $\text{mcd}(r, n) = 1$ (es decir, $r \in \mathcal{U}(\mathbb{Z}_n)$), definimos el siguiente automorfismo de C_n :

$$\begin{aligned} f_r : C_n &\longrightarrow C_n \\ x &\longmapsto x^r \end{aligned}$$

Comprobemos en primer lugar que se trata de un automorfismo. Puesto que $C_n \cong \mathbb{Z}_n$, entonces C_n es abeliano y, de ahí, se tiene de forma directa que f_r es un homomorfismo. Veamos que es inyectivo:

- Inyectividad: Supongamos $k, l \in \{0, \dots, n-1\}$ tales que $f_r(x^k) = f_r(x^l)$. Entonces, $x^{rk} = x^{rl} \implies x^{r(k-l)} = 1$. Como $O(x) = n$, se tiene que $n \mid r(k-l)$. Como además $\text{mcd}(r, n) = 1$, entonces $n \mid k-l$, tenemos que $k, l \in \{0, \dots, n-1\}$, entonces $k-l = 0$. Por tanto, $k = l$.

Por tanto, por ser inyectivo y ser C_r finito, entonces f_r biyectivo. Por tanto, f_r es un automorfismo. Esto nos permite definir la siguiente función:

$$\begin{aligned} \Phi : \mathcal{U}(\mathbb{Z}_n) &\longrightarrow \text{Aut}(C_n) \\ r &\longmapsto f_r \end{aligned}$$

Dividimos la demostración en varios aspectos:

Bien definida: Veamos en primer lugar que Φ está bien definida. Para ello, consideramos $r, s \in \mathbb{Z}$ tales que $[r] = [s]$. Entonces, $s = r + tn$ para algún $t \in \mathbb{Z}$. Veamos que $f_r = f_s$. Supongamos $\langle x \rangle = C_n$. Entonces, para cada $k \in \{0, \dots, n-1\}$, se tiene que:

$$\begin{aligned} f_r(x^k) &= x^{rk} \\ f_s(x^k) &= x^{sk} = (x^{r+tn})^k = x^{rk} x^{tnk} = x^{rk} \cdot (x^n)^{tk} = x^{rk} \cdot 1 = x^{rk} \end{aligned}$$

Por tanto, $f_r = f_s$, y por tanto Φ está bien definida.

Homomorfismo: Veamos ahora que Φ es un homomorfismo. Para ello, consideramos $r, s \in \mathcal{U}(\mathbb{Z}_n)$:

$$\Phi(rs) = f_{rs} \quad \Phi(r) \circ \Phi(s) = f_r \circ f_s$$

Comprobamos que se trata del mismo automorfismo:

$$f_{rs}(x) = x^{rs} = (x^s)^r = f_r(f_s(x)) = (f_r \circ f_s)(x) \quad \forall x \in C_n$$

Por tanto, Φ es un homomorfismo.

Inyectividad: Veamos ahora que $\ker(\Phi) = \{1\}$. Para ello, supongamos que $\exists k \in \mathcal{U}(\mathbb{Z}_n) \setminus \{1\}$ tal que $\Phi(k) = f_k = id$. Entonces, para $x \in C_n$ con $O(x) = n$, se tiene que:

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

Como además $k \in \mathcal{U}(\mathbb{Z}_n)$, entonces $k < n$, luego $k-1 = 0$ y por tanto $k = 1$. Por tanto, $\ker(\Phi) = \{1\}$, y por tanto Φ es monomorfismo.

Sobreyectividad: Veamos ahora que Φ es sobreyectivo. Para ello, consideramos $f \in \text{Aut}(C_n)$. Consideramos $x \in C_n$ tal que $\text{mcd}(x, n) = 1$, de forma que $C_n = \langle x \rangle$. Entonces, $f(x) \in C_n$, por lo que $f(x) = x^r$ para algún $r \in \{0, \dots, n-1\}$. Además, como f es un epimorfismo, entonces $C_n = \langle f(x) \rangle = \langle x^r \rangle$. Por tanto, $\text{mcd}(r, n) = 1$, y por tanto $r \in \mathcal{U}(\mathbb{Z}_n)$. Veamos que $f = f_r$:

$$f(x^k) = f(x)^k = (x^r)^k = x^{rk} = f_r(x^k) \quad \forall k \in \{0, \dots, n-1\}$$

Por tanto, Φ es sobreyectivo. Por tanto, Φ es un isomorfismo.

Una vez demostrado eso, como $\mathcal{U}(\mathbb{Z}_n)$ es finito, entonces $\text{Aut}(C_n)$ es finito, con:

$$|\text{Aut}(C_n)| = |\mathcal{U}(\mathbb{Z}_n)| = \varphi(n)$$

Además, como $\mathcal{U}(\mathbb{Z}_n)$ es abeliano, entonces $\text{Aut}(C_n)$ es abeliano.

Ejercicio 7.3.18.

1. Describir explícitamente el grupo de automorfismos $\text{Aut}(C_8)$.

Por el Ejercicio 7.3.17, sabemos que $\text{Aut}(C_8) \cong \mathcal{U}(\mathbb{Z}_8)$. Calculemos $\mathcal{U}(\mathbb{Z}_8)$:

$$\mathcal{U}(\mathbb{Z}_8) = \{1, 3, 5, 7\}$$

Por tanto, hay cuatro automorfismos en $\text{Aut}(C_8)$, que son $f_1 = id$, f_3 , f_5 y f_7 (tal y como definíamos en el Ejercicio 7.3.17). Veámoslo explícitamente en la siguiente tabla:

x	$f_1(x)$	$f_3(x)$	$f_5(x)$	$f_7(x)$
1	1	1	1	1
x	x	x^3	x^5	x^7
x^2	x^2	x^6	x^2	x^6
x^3	x^3	x	x^7	x^5
x^4	x^4	x^4	x^4	x^4
x^5	x^5	x^7	x	x^3
x^6	x^6	x^2	x^6	x^2
x^7	x^7	x^5	x^3	x

2. Demostrar que $\text{Aut}(C_8)$ es isomorfo al grupo de Klein.

Por el apartado anterior, sabemos que $|\text{Aut}(C_8)| = 4$. Por el Ejercicio 7.3.10, sabemos que hay dos posibilidades, o bien $\text{Aut}(C_8)$ es cíclico, o bien $\text{Aut}(C_8) \cong V$.

Supongamos que $\text{Aut}(C_8)$ es cíclico. Entonces, $\exists f \in \text{Aut}(C_8) \mid O(f) = 4$. Para cada $x \in C_8$, tenemos que:

$$\begin{aligned}(f_3 \circ f_3)(x) &= f_3(x^3) = x^9 = x \\(f_5 \circ f_5)(x) &= f_5(x^5) = x^{25} = x \\(f_7 \circ f_7)(x) &= f_7(x^7) = x^{49} = x\end{aligned}$$

Por tanto, $O(f_3) = O(f_5) = O(f_7) = 2$, lo cual es una contradicción. Por tanto, $\text{Aut}(C_8)$ no es cíclico, y por tanto $\text{Aut}(C_8) \cong V$.

7.4. Grupos cociente. Teoremas de isomorfismo. Productos

Ejercicio 7.4.1. Demostrar que si $G \leq S_n$, entonces $G \subseteq A_n$ o bien se tiene que $[G : G \cap A_n] = 2$. Concluir que un subgrupo de S_n consiste sólo en permutaciones pares, o bien contiene el mismo número de permutaciones pares que de impares.

Sea $G \leq S_n$ un subgrupo de S_n . O bien $G \subseteq A_n$ (en cuyo caso consiste sólo de permutaciones pares); o bien $\exists \sigma \in G$ tal que $\sigma \notin A_n$, es decir, $\varepsilon(\sigma) = -1$. Para ver que $[G : G \cap A_n] = 2$, hay varias posibilidades.

Opción 1: Consideramos el homomorfismo $\varepsilon : G \rightarrow \{-1, 1\}$ dado por la aplicación signatura. Calculemos su núcleo y su imagen:

$$\ker(\varepsilon) = \{\sigma \in G \mid \varepsilon(\sigma) = 1\} = A_n \cap G,$$

$$\text{Im}(\varepsilon) = \{\varepsilon(\sigma) \mid \sigma \in G\} \stackrel{(*)}{=} \{-1, 1\}$$

donde vamos a razonar el por qué de $(*)$. Como $1 \in G$ por ser este un grupo, entonces $1 \in \text{Im}(\varepsilon)$, y como $\exists \sigma \in G$ tal que $\varepsilon(\sigma) = -1$, entonces $-1 \in \text{Im}(\varepsilon)$. Por lo tanto, $\text{Im}(\varepsilon) = \{-1, 1\}$. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{\ker(\varepsilon)} \cong \text{Im}(\varepsilon) \implies \frac{G}{A_n \cap G} \cong \{-1, 1\} \cong \mathbb{Z}_2.$$

Por definición de índice, se tiene que:

$$[G : A_n \cap G] = \left| \frac{G}{A_n \cap G} \right| = |\mathbb{Z}_2| = 2$$

Opción 2: Por el Teorema de Lagrange, sabemos que:

$$[S_n : A_n] = \frac{|S_n|}{|A_n|} = 2 \implies A_n \triangleleft S_n$$

Aplicando el Segundo Teorema de Isomorfía a G y A_n , tenemos que:

$$\frac{G}{G \cap A_n} \cong \frac{GA_n}{A_n}$$

Veamos qué grupo es GA_n . En primer lugar, para $1 \in G$ vemos que $A_n \subset GA_n$. No obstante, como $\exists \sigma \in G$ con $\varepsilon(\sigma) = -1$, entonces $A_n \neq GA_n$, por lo que $|GA_n| > |A_n| = |S_n|/2$. Como $|GA_n| \mid |S_n|$, ha de ser $|GA_n| = |S_n|$, por lo que $GA_n = S_n$. Por tanto:

$$\frac{G}{G \cap A_n} \cong \frac{S_n}{A_n}$$

Por definición de índice, se tiene que:

$$[G : A_n \cap G] = \left| \frac{G}{A_n \cap G} \right| = \left| \frac{S_n}{A_n} \right| = \frac{|S_n|}{|A_n|} = 2$$

En cualquier caso, hemos visto que $[G : A_n \cap G] = 2$. Por el Teorema de Lagrange, se tiene que $|G| = 2 \cdot |G \cap A_n|$, por lo que la mitad de las permutaciones de G son pares. Como una permutación o bien es par o es impar, entonces la otra mitad ha de tener signatura impar. Por tanto, contiene el mismo número de permutaciones pares que de impares.

Ejercicio 7.4.2. Sea \mathbb{K} un cuerpo.

1. Se considera la siguiente aplicación:

$$\begin{aligned} \det : \text{GL}_n(\mathbb{K}) &\longrightarrow \mathbb{K}^\times \\ G &\longmapsto \det(G) \end{aligned}$$

Demostrar que dicha aplicación es un epimorfismo de grupos. ¿Cuál es el núcleo de este homomorfismo?

Para comprobar que se trata de un homomorfismo, tomamos $A, B \in \text{GL}_n(\mathbb{K})$ y por las propiedades de la determinante, se tiene que:

$$\det(AB) = \det(A) \cdot \det(B)$$

Por otro lado, para cada $a \in \mathbb{K}^\times$, se considera la siguiente matriz:

$$A_a = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Como $\det(A_a) = a \neq 0$, entonces $A_a \in \text{GL}_n(\mathbb{K})$. Como $\det(A_a) = a$, se tiene que \det es sobreyectiva. Por lo tanto, \det es un epimorfismo de grupos. Su núcleo es:

$$\ker(\det) = \{A \in \text{GL}_n(\mathbb{K}) \mid \det(A) = 1\} = \text{SL}_n(\mathbb{K})$$

2. Si \mathbb{K} es un cuerpo finito con q elementos, determinar el orden del grupo $\text{SL}_n(\mathbb{K})$.

Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{\text{GL}_n(\mathbb{K})}{\text{SL}_n(\mathbb{K})} \cong \mathbb{K}^\times$$

Por el Teorema de Lagrange, se tiene que:

$$|\text{SL}_n(\mathbb{K})| = \frac{|\text{GL}_n(\mathbb{K})|}{|\mathbb{K}^\times|} = \frac{|\text{GL}_n(\mathbb{K})|}{q-1} = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{q-1}$$

Ejercicio 7.4.3. Sea $n \in \mathbb{N} \setminus \{0\}$, y sea G un grupo verificando que para todo par de elementos $x, y \in G$ se tiene que $(xy)^n = x^n y^n$. Se definen:

$$\begin{aligned} H &= \{x \in G \mid x^n = 1\}, \\ K &= \{x^n \mid x \in G\}. \end{aligned}$$

Demostrar que $H, K \triangleleft G$, y que $|K| = [G : H]$.

Definimos en primer lugar la siguiente aplicación:

$$\begin{aligned} f : G &\longrightarrow G \\ x &\longmapsto x^n \end{aligned}$$

Para demostrar que se trata de un homomorfismo emplearemos la propiedad dada en el enunciado (*):

$$f(xy) = (xy)^n \stackrel{(*)}{=} x^n y^n = f(x)f(y) \quad \forall x, y \in G$$

Por tanto, f es un homomorfismo. Como $\{1\}, G < G$, entonces los siguientes grupos son subgrupos de G :

$$\begin{aligned} f^*(\{1\}) &= \{x \in G \mid f(x) = 1\} = \{x \in G \mid x^n = 1\} = H = \ker(f), \\ f_*(G) &= \{f(x) \mid x \in G\} = \{x^n \mid x \in G\} = K = \text{Im}(f). \end{aligned}$$

Por tanto, tenemos que $H, K < G$. Probamos ahora que son grupos normales en G . En primer lugar, para H tomamos $x \in G$ y $h \in H$ (por lo que $h^n = 1$). Entonces:

$$(xhx^{-1})^n = xh^n x^{-1} = x \cdot 1 \cdot x^{-1} = 1 \implies xhx^{-1} \in H$$

Por tanto, $H \triangleleft G$. Ahora probamos que K es normal en G . Tomamos $x \in G$ y $k \in K$ (por lo que $\exists y \in G$ tal que $k = y^n$). Entonces, consideramos $xyx^{-1} \in G$ y calculamos:

$$xkx^{-1} = x(y^n)x^{-1} = (xyx^{-1})^n \in K$$

Por tanto, $K \triangleleft G$. Para probar que $|K| = [G : H]$, tomamos el homomorfismo f anteriormente descrito. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{H} \cong K \implies |K| = \left| \frac{G}{H} \right| = [G : H]$$

Ejercicio 7.4.4. Para un grupo G se define su *centro* como

$$Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}.$$

1. Demostrar que $Z(G) < G$.

Como $Z(G) \subset G$, hay dos principales posibilidades, ambas equivalentes:

Opción 1: Comprobamos las tres condiciones que caracterizan a los subgrupos:

- $1 \in Z(G)$: Para todo $x \in G$, se tiene que $1x = x1 = x$.
- $a, b \in Z(G) \implies ab \in Z(G)$: Para todo $x \in G$, se tiene que:

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

- $a \in Z(G) \implies a^{-1} \in Z(G)$: Para todo $x \in G$, se tiene que:

$$a^{-1}x = (x^{-1}a)^{-1} = (ax^{-1})^{-1} = xa^{-1}.$$

Opción 2: Dados $a, b \in Z(G)$, comprobemos que $ab^{-1} \in Z(G)$:

$$(ab^{-1})x = a(b^{-1}x) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}).$$

En cualquier caso, $Z(G)$ es un subgrupo de G .

2. Demostrar que $Z(G) \triangleleft G$.

De nuevo, hay dos posibilidades:

Opción 1: Para $x \in G$. Entonces:

$$xZ(G) = \{xz \mid z \in Z(G)\} = \{zx \mid z \in Z(G)\} = Z(G)x.$$

Opción 2: Empleamos la caracterización de subgrupo normal. Para $x \in G$ y $z \in Z(G)$, busquemos ver que $xzx^{-1} \in Z(G)$:

$$xzx^{-1}y = zxx^{-1}y = zy = yz = yzxx^{-1} = yxzx^{-1} \quad \forall y \in G.$$

En ambos casos, se tiene que $Z(G) \triangleleft G$.

3. Demostrar que G es abeliano si, y sólo si, $G = Z(G)$.

$$G = Z(G) \iff G = \{a \in G \mid ax = xa \forall x \in G\} \iff ax = xa \forall a, x \in G \iff G \text{ es abeliano.}$$

4. Demostrar que $G/Z(G)$ es abeliano si, y sólo si, G es abeliano. Demostrar que si $G/Z(G)$ es cíclico, entonces G es abeliano.

Como $G/Z(G)$ es cíclico, entonces existe $x \in G$ tal que $G/Z(G) = \langle xZ(G) \rangle$. Como las clases de equivalencia forman una partición disjunta de G , para cada $x \in G$ existe $k \in \mathbb{Z}$ tal que $x \in x^k Z(G)$. Buscamos ahora demostrar que G es abeliano. Dados $a, b \in G$, entonces existen $p, q \in \mathbb{Z}$ tales que $a \in x^p Z(G)$ y $b \in x^q Z(G)$. Entonces, existen $z_a, z_b \in Z(G)$ tales que $a = x^p z_a$ y $b = x^q z_b$. Por tanto:

$$ab = (x^p z_a)(x^q z_b) = x^{p+q} z_a z_b = x^q z_b x^p z_a = (x^q z_b)(x^p z_a) = ba$$

Por tanto, $ab = ba$ para todo $a, b \in G$, por lo que G es abeliano.

Ejercicio 7.4.5. Determinar el centro del grupo diédrico D_4 . Observar que el cociente $D_4/Z(D_4)$ es abeliano, aunque D_4 no lo sea (compárese este hecho con el tercer apartado del ejercicio anterior).

El grupo D_4 está formado por las siguientes rotaciones y reflexiones:

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

Sabemos que $Z(D_4)$ es un subgrupo normal de D_4 . En primer lugar, sabemos que $1 \in Z(D_4)$. Veamos que $r^2 \in Z(D_4)$. En primer lugar, vemos que conmuta con todas las potencias de r . Veamos ahora que conmuta con el resto de elementos:

$$\begin{aligned} r^2 s &= r s r^3 = s r^6 = s r^2 \\ r^2 sr &= sr^2 r = sr r^2 \\ r^2 sr^2 &= s r r^2 r = s = sr^4 = sr^2 r^2 \\ r^2 sr^3 &= sr = sr^5 = sr^3 r^2 \end{aligned}$$

Por tanto, $\{1, r^2\} \subset Z(D_4)$. Además, tenemos que:

$$\begin{aligned} sr = r^3s \neq rs &\implies s, r \notin Z(D_4) \\ sr^3 = r^9s = rs \neq r^3s &\implies r^3 \notin Z(D_4) \\ sr^2s = r^3 \neq r &\implies sr \notin Z(D_4) \\ sr^3s = r \neq r^3 &\implies sr^3 \notin Z(D_4) \end{aligned}$$

Como $|Z(D_4)|$ divide a $|D_4| = 8$ y $2 \leq |Z(D_4)| \leq 3$, se tiene que $|Z(D_4)| = 2$. Por tanto,

$$Z(D_4) = \{1, r^2\}$$

Veamos que $D_4/Z(D_4)$ es abeliano. Sabemos que:

$$|D_4/Z(D_4)| = \frac{|D_4|}{|Z(D_4)|} = \frac{8}{2} = 4$$

Por tanto, $D_4/Z(D_4)$ es isomorfo a V o a C_4 . Por el último apartado del ejercicio anterior, si fuese $D_4/Z(D_4)$ isomorfo a C_4 , entonces D_4 sería abeliano. Como no lo es, se tiene que $D_4/Z(D_4) \cong V$. Como V es abeliano, se tiene que $D_4/Z(D_4)$ también lo es.

Ejercicio 7.4.6. Determinar el centro de los grupos S_n y A_n para $n \geq 2$.

Para $n = 2$, tenemos que:

$$\begin{aligned} S_2 = \{1, (1\ 2)\} &\implies Z(S_2) = S_2 \\ A_2 = \{1\} &\implies Z(A_2) = A_2 \end{aligned}$$

Calculamos ahora $Z(S_n)$ para $n \geq 3$. Sea $\sigma \neq 1 \in S_n$. Entonces, $\exists i, j \in \{1, \dots, n\}$ tales que $i \neq j$ y $\sigma(i) = j$. Consideramos ahora $k \in \{1, \dots, n\}$ tal que $k \neq i, j$, y sea la permutación $\tau = (j\ k)$. Entonces:

$$\begin{aligned} \sigma\tau(i) &= \sigma(i) = j \\ \tau\sigma(i) &= \tau(j) = k \end{aligned}$$

Por tanto, $\sigma\tau \neq \tau\sigma$. Como σ es arbitrario, se tiene que $Z(S_n) = \{1\}$ para $n \geq 3$.

Trabajamos ahora con A_n . En primer lugar, para $n = 3$ tenemos que $|A_3| = 3$ primo, por lo que A_3 es cíclico y en particular abeliano. Por tanto, $Z(A_3) = A_3$.

Para $n \geq 4$, sea $\sigma \in A_n$ tal que $\sigma \neq 1$. Entonces, $\exists i, j \in \{1, \dots, n\}$ tales que $i \neq j$ y $\sigma(i) = j$. Consideramos ahora $k, l \in \{1, \dots, n\} \setminus \{i, j\}$, tal que $k \neq l$. Consideramos ahora $\tau = (j\ k\ l) \in A_n$. Entonces:

$$\begin{aligned} \sigma\tau(i) &= \sigma(i) = j \\ \tau\sigma(i) &= \tau(j) = k \end{aligned}$$

Por tanto, $\sigma\tau \neq \tau\sigma$. Como σ es arbitrario, se tiene que $Z(A_n) = \{1\}$ para $n \geq 4$. Notemos que hemos tenido que imponer que $n \geq 4$ para que podamos elegir 4 elementos distintos.

Ejercicio 7.4.7. Determinar el centro del grupo D_n para $n \geq 3$.

Dado $z \in D_n$, como $D_n = \langle r, s \rangle$ entonces $z \in Z(D_n)$ si y sólo si z conmuta con r y con s . Distinguimos según los elementos de D_n :

- $1 \in Z(D_n)$ para todo $n \geq 3$.
- Fijado $m \in \{1, \dots, n-1\}$, veamos si $r^m \in Z(D_n)$.

$$r^m r = r^{m+1} = r r^m$$

$$r^m s = sr^{m(n-1)} = sr^{-m} = sr^{n-m} = s r^m \iff r^{n-m} = r^m \xLeftrightarrow{(*)} n-m=m \iff n=2m$$

donde en $(*)$ hemos usado que $n-m, m \in \{1, \dots, n-1\}$. Por tanto, hay que distinguir según la paridad de n :

- Si n es impar, entonces $r^m \notin Z(D_n)$ para todo $m \in \{1, \dots, n-1\}$.
- Si n es par, entonces $r^{n/2} \in Z(D_n)$, y $r^m \notin Z(D_n)$ para todo $m \in \{1, \dots, n-1\} \setminus \{n/2\}$.
- Fijado $m \in \{0, \dots, n-1\}$, veamos si $sr^m \in Z(D_n)$.

$$sr^m r = sr^{m+1} = r^{(m+1)(n-1)} s = r^{mn-m+n-1} s = r^{n-m-1} s$$

$$r sr^m = r r^{n-m} s = r^{n-m+1} s$$

Por tanto, se necesita que $r^{n-m-1} = r^{n-m+1}$, y equivalentemente se necesita que $r^{-1} = r$, es decir, que $r^2 = 1$. Esto es cierto para $n = 2$, pero no para $n \geq 3$. Por tanto, $sr^m \notin Z(D_n)$ para todo $m \in \{0, \dots, n-1\}$.

En resumen, tenemos que:

- Si n es impar, entonces $Z(D_n) = \{1\}$.
- Si n es par, entonces $Z(D_n) = \{1, r^{n/2}\}$.

Ejercicio 7.4.8. Sean H y K dos subgrupos finitos de un grupo G , uno de ellos normal. Demostrar que

$$|H||K| = |HK||H \cap K|.$$

Sean $H, K < G$, y $K \triangleleft G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

Tomando índices y usando el Teorema de Lagrange, se tiene que:

$$\left| \frac{HK}{K} \right| = \frac{|HK|}{|K|} = \left| \frac{H}{H \cap K} \right| = \frac{|H|}{|H \cap K|} \implies |H||K| = |HK||H \cap K|.$$

Si por el contrario $H \triangleleft G$, entonces:

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

y de igual forma se llega a la misma conclusión.

Ejercicio 7.4.9. Sea G finito y $N \triangleleft G$. Probar que $G/N \cong G$ si, y sólo si, $N = \{1\}$, y que $G/N \cong \{1\}$ si, y sólo si, $N = G$.

Veamos que $G/N \cong G$ si, y sólo si, $N = \{1\}$.

\Rightarrow) Supongamos que $G/N \cong G$. Entonces, por el Teorema de Lagrange, se tiene que:

$$|G| = |G/N| = \frac{|G|}{|N|} \implies |N| = 1 \implies N = \{1\}.$$

\Leftarrow) Supongamos que $N = \{1\}$. Definimos ahora el homomorfismo siguiente:

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

Tenemos que:

$$\begin{aligned} \ker(f) &= \{x \in G \mid f(x) = 1\} = \{x \in G \mid x = 1\} = \{1\} = N, \\ \text{Im}(f) &= \{f(x) \mid x \in G\} = \{x \mid x \in G\} = G \end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{N} \cong G$$

Veamos ahora que $G/N \cong \{1\}$ si, y sólo si, $N = G$.

\Rightarrow) Supongamos que $G/N \cong \{1\}$. Entonces, por el Teorema de Lagrange, se tiene que:

$$1 = |G/N| = \frac{|G|}{|N|} \implies |G| = |N|$$

Como $N \leq G$, se tiene que $N \subset G$, y por tanto $N = G$.

\Leftarrow) Supongamos que $N = G$. Entonces, definimos el homomorfismo siguiente:

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

Entonces, tenemos que:

$$\begin{aligned} \ker(f) &= \{x \in G \mid f(x) = 1\} = \{x \in G \mid 1 = 1\} = G = N, \\ \text{Im}(f) &= \{f(x) \mid x \in G\} = \{1 \mid x \in G\} = \{1\} \end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{N} \cong \{1\}$$

Observación. Notemos que en las implicaciones hacia la izquierda no es necesario suponer que G es finito. Lo usaremos por tanto sin esta restricción.

Ejercicio 7.4.10. Sean G y H dos grupos cuyos órdenes sean primos relativos. Probar que si $f : G \rightarrow H$ es un homomorfismo, entonces necesariamente $f(x) = 1$ para todo $x \in G$, es decir, que el único homomorfismo entre ellos es el trivial.

Como $|G|$ y $|H|$ son primos relativos, en particular son grupos finitos. Por ser f un homomorfismo, se tiene que $f(G) < H$, luego $|f(G)| \mid |H|$. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{\ker(f)} \cong f(G) \implies |G| = |\ker(f)| \cdot |f(G)| \implies |f(G)| \mid |G|$$

Como $\text{mcd}(|G|, |H|) = 1$, se tiene que $|f(G)| = 1$. Como además $f(G)$ es un grupo, se tiene que $f(G) = \{1\}$. Por tanto, f es el homomorfismo trivial.

Ejercicio 7.4.11. Sean $H, K \leq G$, y sea $N \triangleleft G$ un subgrupo normal de G tal que $HN = KN$. Demostrar que

$$\frac{H}{H \cap N} \cong \frac{K}{K \cap N}.$$

Aplicamos dos veces el Segundo Teorema de Isomorfía:

- Consideramos $H, N \leq G$, con $N \triangleleft G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

- Consideramos $K, N \leq G$, con $N \triangleleft G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{KN}{N} \cong \frac{K}{K \cap N}$$

Como $KN = HN$ y ser congruente es una relación de equivalencia, se tiene que:

$$\frac{H}{H \cap N} \cong \frac{HN}{N} = \frac{KN}{N} \cong \frac{K}{K \cap N}$$

Ejercicio 7.4.12. Sea $N \triangleleft G$ tal que N y G/N son abelianos. Sea H un subgrupo cualquiera de G . Demostrar que existe un subgrupo normal $K \triangleleft H$ tal que K y H/K son abelianos.

Por el Segundo Teorema de Isomorfía, se tiene que $K = H \cap N \triangleleft H$. Como $K \subset N$ y K es un grupo, entonces $K \leq N$. Como N es abeliano, se tiene que K también lo es. Nos falta por ver que H/K es abeliano. Por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{H}{K} \cong \frac{HN}{N}$$

Veamos ahora que $HN/N \leq G/N$. Como $HN \subset G$, por definición de conjunto cociente se tiene que $HN/N \subset G/N$. Como HN/N es un grupo, se tiene que $HN/N \leq G/N$. Como G/N es abeliano, se tiene que HN/N también lo es. Por tanto, por el Segundo Teorema de Isomorfía, se tiene que H/K es abeliano.

Ejercicio 7.4.13. Sea G un grupo finito, y sean $H, K \leq G$, con $K \triangleleft G$ y tales que $|H|$ y $[G : K]$ son primos relativos. Demostrar que $H \subseteq K$.

Por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{H}{H \cap K} \cong \frac{HK}{K}$$

Como $HK \leq G$, entonces $HK/K \leq G/K$. Por tanto $|\frac{H}{H \cap K}| = |\frac{HK}{K}|$ divide a $|\frac{G}{K}| = [G : K]$. Por otro lado:

$$\left| \frac{H}{H \cap K} \right| = \frac{|H|}{|H \cap K|} \implies |H| = |H \cap K| \cdot \left| \frac{H}{H \cap K} \right| \implies \left| \frac{H}{H \cap K} \right| \mid |H|$$

Como $\text{mcd}(|H|, [G : K]) = 1$, se tiene que $|\frac{H}{H \cap K}| = 1$. Por tanto, $|H| = |H \cap K|$, y como $H \cap K \subset H$, se tiene que $H \cap K = H$. Por tanto, $H \subset K$.

Ejercicio 7.4.14. Sea G un grupo.

1. Demostrar que para cada $a \in G$ la aplicación $\varphi_a : G \rightarrow G$ definida por $\varphi_a(x) = axa^{-1}$, es un automorfismo de G . φ_a se llama automorfismo interno o de conjugación de G definido por a .

Vemos en primer lugar que está bien definida, puesto que un grupo es cerrado para inversos y productos. Por tanto, $\varphi_a(x) \in G$ para todo $x \in G$. Veamos ahora que es un isomorfismo:

- Para ver que es un homomorfismo:

$$\varphi_a(xy) = a(xy)a^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y) \quad \forall x, y \in G$$

- Para ver que es inyectiva, sean $x, y \in G$ de forma que:

$$\varphi_a(x) = axa^{-1} = aya^{-1} = \varphi_a(y)$$

Entonces, aplicando dos veces la propiedad cancelativa, tenemos que:

$$axa^{-1} = aya^{-1} \implies ax = ay \implies x = y$$

- Para ver que es sobreyectiva, sea $y \in G$, tomamos $x = a^{-1}ya$. Entonces:

$$\varphi_a(x) = \varphi_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = aa^{-1}yaa^{-1} = y$$

Concluimos que φ_a es un automorfismo de G .

2. Demostrar que la siguiente aplicación es un homomorfismo:

$$\begin{aligned} \varphi : G &\longrightarrow \text{Aut}(G) \\ a &\longmapsto \varphi_a \end{aligned}$$

Para esto, es necesario probar que, fijados $a, b \in G$, se tiene que:

$$\varphi_{ab} = \varphi_a \circ \varphi_b$$

Tenemos que:

$$\varphi_{ab}(x) = (ab)x(ab)^{-1} = (ab)x(b^{-1}a^{-1}) = a(bxb^{-1})a^{-1} = a\varphi_b(x)a^{-1} = \varphi_a(\varphi_b(x)) \quad \forall x \in G$$

Por tanto, $\varphi_{ab} = \varphi_a \circ \varphi_b$. Por tanto, φ es un homomorfismo de grupos.

3. Demostrar que el conjunto de automorfismos internos de G , que se denota $\text{Int}(G)$, es un subgrupo normal de $\text{Aut}(G)$.

Para ello, en primer lugar es necesario ver que $\text{Int}(G) < \text{Aut}(G)$. Considerados $a, b \in G$, tenemos que:

$$\begin{aligned} (\varphi_a \circ \varphi_b^{-1})(x) &= \varphi_a(b^{-1}xb) = a(b^{-1}xb)a^{-1} = ab^{-1}xba^{-1} = \\ &= (ab^{-1})x(ab^{-1})^{-1} = \varphi_{ab^{-1}}(x) \quad \forall x \in G \end{aligned}$$

Veamos ahora que $\text{Int}(G) \triangleleft \text{Aut}(G)$. Para ello es necesario ver que se tiene $f \circ \varphi \circ f^{-1} \in \text{Int}(G)$ para todo $f \in \text{Aut}(G)$ y $\varphi \in \text{Int}(G)$. Sea $f \in \text{Aut}(G)$ y $\varphi_a \in \text{Int}(G)$. Entonces, tenemos que:

$$\begin{aligned} (f \circ \varphi_a \circ f^{-1})(x) &= f(\varphi_a(f^{-1}(x))) = f(a(f^{-1}(x))a^{-1}) \\ &= f(a)f(f^{-1}(x))f(a^{-1}) = f(a)xf(a^{-1}) = \varphi_{f(a)}(x) \in \text{Int}(G) \end{aligned}$$

Por tanto, $f \circ \varphi_a \circ f^{-1} \in \text{Int}(G)$, y por tanto $\text{Int}(G) \triangleleft \text{Aut}(G)$.

4. Demostrar que $G/Z(G) \cong \text{Int}(G)$.

Buscamos aplicar el Primer Teorema de Isomorfía al homomorfismo φ del apartado 2. Tenemos que:

$$\begin{aligned} \ker(\varphi) &= \{a \in G \mid \varphi_a = \text{Id}_G\} = \{a \in G \mid \varphi_a(x) = x \quad \forall x \in G\} \\ &= \{a \in G \mid axa^{-1} = x \quad \forall x \in G\} = \{a \in G \mid ax = xa \quad \forall x \in G\} = Z(G) \\ \text{Im}(\varphi) &= \{\varphi_a \mid a \in G\} = \{f \in \text{Aut}(G) \mid f(x) = axa^{-1} \quad \forall x \in G\} = \text{Int}(G) \end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{Z(G)} \cong \text{Int}(G)$$

5. Demostrar que $\text{Int}(G) = \{\text{Id}_G\}$ si y sólo si G es abeliano.

\implies) Supongamos que $\text{Int}(G) = \{\text{Id}_G\}$. Entonces, para todo $a \in G$, se tiene que:

$$\varphi_a = \text{Id}_G \implies axa^{-1} = x \quad \forall x \in G$$

Por tanto, $ax = xa \quad \forall x \in G$. Como a es arbitrario, se tiene que G es abeliano.

\impliedby) Supongamos que G es abeliano. Entonces, para todo $a \in G$, se tiene que:

$$\varphi_a(x) = axa^{-1} = aa^{-1}x = x \quad \forall x \in G$$

Por tanto, $\varphi_a = \text{Id}_G$. Como a es arbitrario, se tiene que $\text{Int}(G) = \{\text{Id}_G\}$.

Ejercicio 7.4.15. Demostrar que el grupo de automorfismos de un grupo no abeliano no puede ser cíclico.

Sea G un grupo no abeliano. Por el recíproco del Ejercicio 7.4.4.4, sabemos que $G/Z(G)$ no es cíclico. Como $G/Z(G) \cong \text{Int}(G)$, se tiene que $\text{Int}(G)$ no es cíclico. Como $\text{Int}(G) < \text{Aut}(G)$ y todo subgrupo de un grupo cíclico es cíclico, se tiene que $\text{Aut}(G)$ no es cíclico.

Ejercicio 7.4.16. Demostrar que $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

Sabemos que:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V^{\text{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx \rangle$$

Construimos ahora automorfismos de $\mathbb{Z}_2 \times \mathbb{Z}_2$. Sabemos que todos los elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ (a excepción del neutro) son de orden 2, y además este grupo es conmutativo. Por tanto, con el Teorema de Dyck podemos construir automorfismos de forma sencilla. Haciendo uso de que $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (1, 0), (0, 1) \rangle$, tenemos los siguientes automorfismos:

	f_1	f_2	f_3	f_4	f_5	f_6
$f_i(1, 0)$	$(1, 0)$	$(1, 0)$	$(0, 1)$	$(0, 1)$	$(1, 1)$	$(1, 1)$
$f_i(0, 1)$	$(0, 1)$	$(1, 1)$	$(1, 0)$	$(1, 1)$	$(0, 1)$	$(1, 0)$

Además, no puede haber más automorfismos, puesto que fijada la imagen de un elemento generador, la imagen del otro elemento generador tan solo tiene dos posibilidades, puesto que no puede ser el neutro. Por tanto, tenemos que:

$$|\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 6$$

Por tanto, $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ es un grupo de orden 6, por lo que es cíclico o es isomorfo a $D_3 \cong S_3$. Tenemos que:

$$\begin{aligned} (f_2 \circ f_3)(1, 0) &= f_2(f_3(1, 0)) = f_2(0, 1) = (1, 1) \\ (f_3 \circ f_2)(1, 0) &= f_3(f_2(1, 0)) = f_3(1, 0) = (0, 1) \end{aligned}$$

Por tanto, $f_2 \circ f_3 \neq f_3 \circ f_2$, por lo que $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ no es abeliano y por tanto no es cíclico. Por tanto, $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

Ejercicio 7.4.17. Demostrar que los grupos S_3 , \mathbb{Z}_{p^n} (con p primo) y \mathbb{Z} no son producto directo internos de subgrupos propios.

1. S_3 .

Como $|S_3| = 6$, entonces sus subgrupos propios son de orden 2 y 3. Por reducción al absurdo, supongamos que $S_3 \cong K \times H$ con $K, H < S_3$. Entonces, $|S_3| = |K||H|$, y como $|K|$ y $|H|$ son divisores de 6, se tiene que $|K| = 2$ y $|H| = 3$. Por tanto, $K \cong C_2$ y $H \cong C_3$. Por tanto, $S_3 = K \times H \cong C_2 \times C_3$. Como C_2 y C_3 son cíclicos con $\text{mcd}(|C_2|, |C_3|) = 1$, se tiene que $C_2 \times C_3$ es cíclico. Por tanto, S_3 es cíclico, lo cual es una contradicción.

2. \mathbb{Z}_{p^n} .

Por ser \mathbb{Z}_{p^n} un grupo cíclico de orden p^n , todos sus subgrupos propios son cíclicos de orden p^k con $k \in \{1, \dots, n-1\}$. Por tanto, por reducción al absurdo, supongamos que $\exists p, q \in \{1, \dots, n-1\}$ tales que $\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^k} \times \mathbb{Z}_{p^q}$. Por ser \mathbb{Z}_{p^k} y \mathbb{Z}_{p^q} cíclicos, se tiene que $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^q}$ es cíclico si y solo si $\text{mcd}(p^k, p^q) = 1$. Como p^k y p^q son potencias de un mismo primo, se tiene que $\text{mcd}(p^k, p^q) \geq p$. Por tanto, $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^q}$ no es cíclico. Por tanto, \mathbb{Z}_{p^n} no es producto directo interno de subgrupos propios.

3. \mathbb{Z} .

Sabemos que todos los subgrupos de \mathbb{Z} son de la forma $k\mathbb{Z}$, con $k \in \mathbb{N}$. Por tanto, por reducción al absurdo, supongamos que $\exists p, q \in \mathbb{N}$ tales que se tiene $\mathbb{Z} \cong p\mathbb{Z} \times q\mathbb{Z} \stackrel{(*)}{\cong} \mathbb{Z} \times \mathbb{Z}$. No obstante, $\mathbb{Z} \times \mathbb{Z}$ no es cíclico, y por tanto no es isomorfo a \mathbb{Z} . Por tanto, \mathbb{Z} no es producto directo interno de subgrupos propios.

En (*), el isomorfismo es el siguiente (que se prueba fácilmente es un isomorfismo):

$$\begin{aligned} f: n\mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto x/n \end{aligned}$$

Ejercicio 7.4.18. En cada uno de los siguientes casos, decidir si el grupo G es o no producto directo interno de los subgrupos H y K .

1. $G = \mathbb{R}^\times$, $H = \{\pm 1\}$, $K = \{x \in \mathbb{R} \mid x > 0\}$.

Es directo que $G = HK$ y $H \cap K = \{1\}$. Como $H, K < G$ y G es abeliano, se tiene que $H, K \triangleleft G$. Por tanto, $G \cong H \times K$.

2. $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \text{GL}_2(\mathbb{R}) \right\}$, $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in \text{GL}_2(\mathbb{R}) \right\}$, $K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R}) \right\}$.

3. $G = \mathbb{C}^\times$, $H = \{z \in \mathbb{C} \mid |z| = 1\}$, $K = \{x \in \mathbb{R} \mid x > 0\}$.

Dado $z \in G$, podemos escribir:

$$z = \frac{z}{|z|} \cdot |z| \quad \frac{z}{|z|} \in H, |z| \in K$$

Por tanto, $G = HK$. Además, $H \cap K = \{1\}$, y como $H, K < G$ y G es abeliano, se tiene que $H, K \triangleleft G$. Por tanto, $G \cong H \times K$.

Ejercicio 7.4.19. Sean G, H y K grupos. Demostrar que:

1. $H \times K \cong K \times H$.

Definimos el isomorfismo:

$$\begin{aligned} f: H \times K &\longrightarrow K \times H \\ (h, k) &\longmapsto (k, h) \end{aligned}$$

Vemos que f es un isomorfismo:

- f es un homomorfismo:

$$\begin{aligned} f((h_1, k_1)(h_2, k_2)) &= f(h_1 h_2, k_1 k_2) = (k_1 k_2, h_1 h_2) \\ &= (k_1, h_1)(k_2, h_2) = f(h_1, k_1)f(h_2, k_2) \end{aligned}$$

- f es inyectiva:

$$\begin{aligned} \ker(f) &= \{(h, k) \in H \times K \mid f(h, k) = (1, 1)\} \\ &= \{(h, k) \in H \times K \mid (k, h) = (1, 1)\} = \{(1, 1)\} \end{aligned}$$

- f es sobreyectiva:

Dado $(k, h) \in K \times H$, tomamos $(h, k) \in H \times K$. Entonces:

$$f(h, k) = (k, h) \quad \forall (h, k) \in H \times K$$

Por tanto, f es un isomorfismo.

2. $G \times (H \times K) \cong (G \times H) \times K$.

Definimos el isomorfismo:

$$\begin{aligned} f : G \times (H \times K) &\longrightarrow (G \times H) \times K \\ (g, (h, k)) &\longmapsto ((g, h), k) \end{aligned}$$

Vemos que f es un isomorfismo:

- f es un homomorfismo:

$$\begin{aligned} f((g_1, (h_1, k_1))(g_2, (h_2, k_2))) &= f(g_1 g_2, (h_1 h_2, k_1 k_2)) \\ &= ((g_1 g_2, h_1 h_2), k_1 k_2) = \\ &= ((g_1, h_1), k_1)((g_2, h_2), k_2) = \\ &= f(g_1, (h_1, k_1))f(g_2, (h_2, k_2)) \end{aligned}$$

- f es inyectiva:

$$\begin{aligned} \ker(f) &= \{(g, (h, k)) \in G \times (H \times K) \mid f(g, (h, k)) = ((1, 1), 1)\} \\ &= \{(g, (h, k)) \in G \times (H \times K) \mid ((g, h), k) = ((1, 1), 1)\} = \{(1, (1, 1))\} \end{aligned}$$

- f es sobreyectiva:

Dado $((g, h), k) \in (G \times H) \times K$, tomamos $(g, (h, k)) \in G \times (H \times K)$. Entonces:

$$f(g, (h, k)) = ((g, h), k) \quad \forall (g, (h, k)) \in G \times (H \times K)$$

Por tanto, f es un isomorfismo.

Ejercicio 7.4.20. Dados isomorfismos de grupos $A \cong K$ y $B \cong H$, demostrar que $A \times B \cong K \times H$.

Sea $f : A \rightarrow K$ y $g : B \rightarrow H$ los isomorfismos. Definimos la siguiente aplicación:

$$\begin{aligned} h : A \times B &\longrightarrow K \times H \\ (a, b) &\longmapsto (f(a), g(b)) \end{aligned}$$

Veamos que h es un homomorfismo. Fijados $(a_1, b_1), (a_2, b_2) \in A \times B$, tenemos que:

$$\begin{aligned} h((a_1, b_1)(a_2, b_2)) &= h(a_1a_2, b_1b_2) = (f(a_1a_2), g(b_1b_2)) \\ &= (f(a_1)f(a_2), g(b_1)g(b_2)) = (f(a_1), g(b_1))(f(a_2), g(b_2)) \\ &= h(a_1, b_1)h(a_2, b_2) \quad \forall (a_1, b_1), (a_2, b_2) \in A \times B \end{aligned}$$

Por tanto, h es un homomorfismo. Veamos ahora que es inyectiva. Para ello, tenemos que:

$$\begin{aligned} \ker(h) &= \{(a, b) \in A \times B \mid h(a, b) = (1, 1)\} \\ &= \{(a, b) \in A \times B \mid (f(a), g(b)) = (1, 1)\} = \\ &= \{(a, b) \in A \times B \mid f(a) = 1 \wedge g(b) = 1\} = \\ &= \{(1, 1)\} \end{aligned}$$

Por tanto, h es inyectiva. Veamos ahora que es sobreyectiva. Dado $(k, h) \in K \times H$, tomamos $(a, b) \in A \times B$ tales que $f(a) = k$ y $g(b) = h$ (que existe por ser f, g biyectivas). Entonces:

$$h(a, b) = (f(a), g(b)) = (k, h) \quad \forall (a, b) \in A \times B$$

Por tanto, h es sobreyectiva. Concluimos que h es un isomorfismo.

Ejercicio 7.4.21. Sean H, K, L y M grupos tales que $H \times K \cong L \times M$. ¿Se verifica necesariamente que $H \cong L$ y $K \cong M$?

Sabemos que $C_2 \times C_3$ es cíclico de orden 6, luego $C_2 \times C_3 \cong C_6$. Además, sabemos que para todo grupo G , se tiene que $G \cong G \times \{1\}$ usando como isomorfismo la aplicación:

$$\begin{aligned} f : G &\longrightarrow G \times \{1\} \\ x &\longmapsto (x, 1) \end{aligned}$$

Por tanto, $C_2 \times C_3 \cong C_6 \cong C_6 \times \{1\}$.

No obstante, $|C_2| \neq |C_6|$ y $|C_3| \neq |1|$. Por tanto, tomando $H = C_2$, $K = C_3$, $L = C_6$ y $M = \{1\}$, se tiene que $H \times K \cong L \times M$. Sin embargo, no se verifica que $H \cong L$ y $K \cong M$.

Ejercicio 7.4.22. Demostrar que no todo subgrupo de un producto directo $H \times K$ es de la forma $H_1 \times K_1$, con $H_1 \leq H$ y $K_1 \leq K$.

Trabajamos con el grupo directo $\mathbb{Z}_2 \times \mathbb{Z}_2$. El grupo \mathbb{Z}_2 no tiene subgrupos propios, y por tanto los subgrupos suyos son $\{0\}$ y \mathbb{Z}_2 . Por tanto, los subgrupos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ que se descomponen como producto directo de subgrupos de \mathbb{Z}_2 son:

$$\blacksquare \{0\} \times \{0\} = \{(0, 0)\}$$

- $\{0\} \times \mathbb{Z}_2 = \{(0, 0), (0, 1)\}$
- $\mathbb{Z}_2 \times \{0\} = \{(0, 0), (1, 0)\}$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$

No obstante, consideramos el subgrupo de $\mathbb{Z}_2 \times \mathbb{Z}_2$ dado por:

$$\langle (1, 1) \rangle = \{(0, 0), (1, 1)\} \quad O((1, 1)) = \text{mcm}(2, 2) = 2$$

Este subgrupo no es de la forma $H_1 \times K_1$, con $H_1 \leq H$ y $K_1 \leq K$. Por tanto, no todo subgrupo de un producto directo $H \times K$ es de la forma $H_1 \times K_1$, con $H_1 \leq H$ y $K_1 \leq K$.

Ejercicio 7.4.23. Sean H, K dos grupos y sean $H_1 \triangleleft H$, $K_1 \triangleleft K$. Demostrar que $H_1 \times K_1 \triangleleft H \times K$ y que

$$\frac{H \times K}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}.$$

Como $H_1 < H$ y $K_1 < K$, se tiene que $H_1 \times K_1 < H \times K$. Veamos ahora que $H_1 \times K_1 \triangleleft H \times K$. Para cada $(h, k) \in H \times K$ y $(h_1, k_1) \in H_1 \times K_1$, tenemos que:

$$(h, k)(h_1, k_1)(h, k)^{-1} = (hh_1h^{-1}, kk_1k^{-1}) \in H_1 \times K_1$$

por ser $H_1 \triangleleft H$ y $K_1 \triangleleft K$. Por tanto, $H_1 \times K_1 \triangleleft H \times K$. Para ver el isomorfismo, consideramos la siguiente aplicación:

$$\begin{aligned} f : H \times K &\longrightarrow \frac{H}{H_1} \times \frac{K}{K_1} \\ (h, k) &\longmapsto (hH_1, kK_1) \end{aligned}$$

Vemos que f es un homomorfismo:

$$\begin{aligned} f((h_1, k_1)(h_2, k_2)) &= f(h_1h_2, k_1k_2) = (h_1h_2H_1, k_1k_2K_1) \\ &= (h_1H_1 \cdot h_2H_1, k_1K_1 \cdot k_2K_1) = (h_1H_1, k_1K_1)(h_2H_1, k_2K_1) \\ &= f(h_1, k_1)f(h_2, k_2) \quad \forall (h_1, k_1), (h_2, k_2) \in H \times K \end{aligned}$$

Calculamos ahora su núcleo e imagen:

$$\begin{aligned} \ker(f) &= \{(h, k) \in H \times K \mid f(h, k) = (H_1, K_1)\} \\ &= \{(h, k) \in H \times K \mid (hH_1, kK_1) = (H_1, K_1)\} = \\ &= \{(h, k) \in H \times K \mid hH_1 = H_1 \wedge kK_1 = K_1\} = H_1 \times K_1 \\ \text{Im}(f) &= \left\{ (hH_1, kK_1) \in \frac{H}{H_1} \times \frac{K}{K_1} \mid (h, k) \in H \times K \right\} = \\ &= \left\{ (hH_1, kK_1) \in \frac{H}{H_1} \times \frac{K}{K_1} \mid h \in H \wedge k \in K \right\} = \frac{H}{H_1} \times \frac{K}{K_1} \end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{H \times K}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}$$

Ejercicio 7.4.24. Sean $H, K \triangleleft G$ tales que $H \cap K = \{1\}$. Demostrar que G es isomorfo a un subgrupo de $G/H \times G/K$.

Definimos la aplicación:

$$\begin{aligned} f: G &\longrightarrow G/H \times G/K \\ g &\longmapsto (gH, gK) \end{aligned}$$

Vemos que f es un homomorfismo:

$$\begin{aligned} f(gh) &= (ghH, ghK) = (gH, gK)(hH, hK) = \\ &= f(g)f(h) \quad \forall g, h \in G \end{aligned}$$

Calculamos su núcleo:

$$\begin{aligned} \ker(f) &= \{g \in G \mid f(g) = (H, K)\} \\ &= \{g \in G \mid (gH, gK) = (H, K)\} = \\ &= \{g \in G \mid gH = H \wedge gK = K\} = H \cap K = \{1\} \end{aligned}$$

Por tanto, tenemos que:

$$\frac{G}{\ker(f)} = \frac{G}{\{1\}} \cong G$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$G \cong \frac{G}{\ker(f)} \cong \text{Im}(f)$$

Como $G < G$ y f es un homomorfismo, se tiene que $\text{Im}(f) < G/H \times G/K$. Por tanto, G es isomorfo a $\text{Im}(f)$, que es un subgrupo de $G/H \times G/K$.

Ejercicio 7.4.25. Sean $H, K \triangleleft G$ tales que $HK = G$. Demostrar que

$$\frac{G}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{H} \times \frac{G}{K}.$$

La demostración no es directa, y la dividiremos en dos partes. Por un lado, demostraremos la primera relación de isomofía, y posteriormente veremos la segunda.

Por el Segundo Teorema de Isomorfía aplicado dos veces, tenemos que $H \cap K \triangleleft H, K$. Veamos ahora que $H \cap K \triangleleft G$. Para ello, tomamos $g \in G$ y $x \in H \cap K$. Como $G = HK$, tenemos que $g = hk$ con $h \in H$ y $k \in K$. Entonces:

$$\begin{aligned} gxg^{-1} &= (hk)x(hk)^{-1} = (hk)x(k^{-1}h^{-1}) = \\ &= h(kxk^{-1})h^{-1} \stackrel{(*)}{=} h\tilde{k}h^{-1} \stackrel{(**)}{\in} H \cap K \end{aligned}$$

donde $(*)$ se cumple porque $H \cap K \triangleleft K$, por lo que $kxk^{-1} = \tilde{k} \in K$ y $(**)$ se cumple porque $H \cap K \triangleleft H$, por lo que $h\tilde{k}h^{-1} \in H$. Por tanto, $H \cap K \triangleleft G$, y el primer cociente tiene sentido.

Definimos la aplicación:

$$\begin{aligned} f : G &\longrightarrow \frac{H}{H \cap K} \times \frac{K}{H \cap K} \\ g &\longmapsto (h(H \cap K), k(H \cap K)) \end{aligned}$$

Veamos que está bien definida, puesto que la descomposición no tiene por qué ser única. Sean $k_1, k_2 \in K$ y $h_1, h_2 \in H$ tales que $g = k_1 h_1 = k_2 h_2$. Entonces, en primer lugar vemos que $h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$. Por tanto:

- $h_1 = k_1^{-1} k_2 h_2$, con $k_1^{-1} k_2 \in K \cap K$ y $h_2 \in H$, por lo que $h_1(H \cap K) = h_2(H \cap K)$.
- $k_1 = k_2 h_1^{-1} h_2$, con $h_1^{-1} h_2 \in H \cap H$ y $k_2 \in K$, por lo que $k_1(H \cap K) = k_2(H \cap K)$.

Por tanto, f está bien definida. Veamos que es un homomorfismo. Dados $g_1, g_2 \in G$, $\exists h_1, h_2 \in H$ y $k_1, k_2 \in K$ tales que $g_1 = h_1 k_1$ y $g_2 = h_2 k_2$. Entonces:

$$\begin{aligned} f(g_1 g_2) &= f(h_1 k_1 h_2 k_2) = \\ &= (h_1 h_2(H \cap K), k_1 k_2(H \cap K)) = \\ &= (h_1(H \cap K), k_1(H \cap K))(h_2(H \cap K), k_2(H \cap K)) \\ &= f(g_1) f(g_2) \quad \forall g_1, g_2 \in G \end{aligned}$$

Calculamos su núcleo:

$$\begin{aligned} \ker(f) &= \{g \in G \mid f(g) = (H \cap K, H \cap K)\} \\ &= \{g = hk \in G \mid (h(H \cap K), k(H \cap K)) = (H \cap K, H \cap K)\} = \\ &= \{g = hk \in G \mid h(H \cap K) = H \cap K \wedge k(H \cap K) = H \cap K\} = \\ &= \{g = hk \in G \mid h, k \in H \cap K\} \stackrel{(*)}{=} H \cap K \end{aligned}$$

donde $(*)$ se cumple porque la inclusión $\ker f \subseteq H \cap K$ se cumple por ser $H \cap K$ cerrado para el producto; mientras que la inclusión $H \cap K \subseteq \ker f$ se cumple tomando $g = g \cdot 1$.

Veamos ahora que es sobreyectiva. Dado $(h(H \cap K), k(H \cap K)) \in \frac{H}{H \cap K} \times \frac{K}{H \cap K}$, tomamos $g = hk \in G$. Entonces:

$$f(g) = f(hk) = (h(H \cap K), k(H \cap K)) \quad \forall g \in G$$

Por tanto, f es sobreyectiva. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K}$$

Llegamos a este punto, tan solo nos falta probar que:

$$\frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{H} \times \frac{G}{K}$$

Para ello, aplicamos en primer lugar dos veces el Segundo Teorema de Isomorfía.

- $H, K < G$ y $K \triangleleft G$:

$$\frac{G}{K} \cong \frac{H}{H \cap K}$$

- $H, K < G$ y $H \triangleleft G$:

$$\frac{G}{H} \cong \frac{K}{H \cap K}$$

Por tanto, tenemos que:

$$\frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{K} \times \frac{G}{H}$$

Como $G/H \times G/K \cong G/K \times G/H$, tenemos que:

$$\frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{K} \times \frac{G}{H} \cong \frac{G}{H} \times \frac{G}{K}$$

Por tanto, se cumple la segunda relación de isomorfía. Concluimos que:

$$\frac{G}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{H} \times \frac{G}{K}$$

Ejercicio 7.4.26. Demostrar que si G es un grupo que es producto directo interno de subgrupos H y K , y $N \triangleleft G$ tal que $N \cap H = \{1\} = N \cap K$, entonces N es abeliano.

Ejercicio 7.4.27. Dar un ejemplo de un grupo G que sea producto directo interno de dos subgrupos propios H y K , y que contenga a un subgrupo normal no trivial N tal que $N \cap H = \{1\} = N \cap K$. Concluir que para $N \triangleleft H \times K$ es posible que se tenga

$$N \neq (N \cap (H \times \{1\})) \times (N \cap (\{1\} \times K)).$$

Ejercicio 7.4.28. Sea G un grupo finito que sea producto directo interno de dos subgrupos H y K tales que $\text{mcd}(|H|, |K|) = 1$. Demostrar que para todo subgrupo $N \leq G$ se verifica que $N = (N \cap H) \times (N \cap K)$.

Ejercicio 7.4.29. Sea G un grupo y sea $f : G \rightarrow G$ un endomorfismo idempotente (esto es, verificando que $f^2 = f$) y tal que $\text{Im}(f) \triangleleft G$. Demostrar que

$$G \cong \text{Im}(f) \times \ker(f).$$

Opción 1. Método Directo

Sea la siguiente aplicación:

$$\begin{aligned} \varphi : \text{Im}(f) \times \ker(f) &\longrightarrow G \\ (x, y) &\longmapsto xy \end{aligned}$$

Veamos que φ es un isomorfismo. Para ello, previamente veremos que para todo $x \in \text{Im}(f)$, se tiene que $f(x) = x$. Dado $x \in \text{Im}(f)$, existe $y \in G$ tal que $f(y) = x$. Entonces:

$$f(x) = f(f(y)) = f^2(y) \stackrel{(*)}{=} f(y) = x$$

donde en $(*)$ se cumple porque f es idempotente.

Homomorfismo

Veamos que φ es homomorfismo. Para cada $(x_1, y_1), (x_2, y_2) \in \text{Im}(f) \times \ker(f)$, tenemos que:

$$\begin{aligned}\varphi((x_1, y_1)(x_2, y_2)) &= \varphi(x_1x_2, y_1y_2) = x_1x_2y_1y_2 \\ \varphi(x_1, y_1)\varphi(x_2, y_2) &= (x_1y_1)(x_2y_2) = x_1y_1x_2y_2\end{aligned}$$

Veamos que $x_2y_1 = y_1x_2$. Es decir, que dados $x \in \text{Im}(f)$ y $y \in \ker(f)$, tenemos que $xy = yx$. Como $\text{Im}(f) \triangleleft G$, y $\ker f \subset G$, tenemos que $xyx^{-1} \in \text{Im}(f)$. Por lo visto anteriormente, $f(yxx^{-1}) = yxx^{-1}$. Aplicando que f es un homomorfismo (estamos demostrando que φ lo es, pero sabemos que f lo es), tenemos que:

$$yxx^{-1} = f(yxx^{-1}) = f(y)f(x)f(x^{-1}) = f(y)xf(y)^{-1} \stackrel{(*)}{=} 1x1 = x \implies yx = xy$$

donde en $(*)$ se cumple porque $y \in \ker(f)$ y $x \in \text{Im}(f)$.

Por tanto, φ es un homomorfismo.

Inyectividad

Veamos que φ es inyectiva. Para ello, sean $(x_1, y_1), (x_2, y_2) \in \text{Im}(f) \times \ker(f)$ tales que $\varphi(x_1, y_1) = \varphi(x_2, y_2)$. Entonces:

$$x_1y_1 = x_2y_2 \implies x_2^{-1}x_1 = y_2y_1^{-1} \in \ker(f) \cap \text{Im}(f)$$

Veamos ahora que $\ker(f) \cap \text{Im}(f) = \{1\}$. Sea $x \in \ker(f) \cap \text{Im}(f)$. Como $x \in \ker(f)$, tenemos que $f(x) = 1$, y como $x \in \text{Im}(f)$, $f(x) = x$. Entonces $1 = f(x) = x$, por lo que $x = 1$. Por tanto, $\ker(f) \cap \text{Im}(f) = \{1\}$, por lo que:

$$\begin{aligned}x_2^{-1}x_1 = 1 &\implies x_1 = x_2 \\ y_2y_1^{-1} = 1 &\implies y_1 = y_2\end{aligned}$$

Por tanto, φ es inyectiva.

Sobreyectividad

Veamos que es sobreyectiva. Dado $g \in G$, tomamos $x = f(g) \in \text{Im}(f)$ e $y = f(g^{-1})g$. Veamos en primer lugar que $y \in \ker(f)$:

$$f(y) = f(f(g^{-1})g) = f(f(g^{-1}))f(g) = f^2(g^{-1})f(g) = f(g^{-1})f(g) = f(g^{-1}g) = f(1) = 1$$

Por tanto, $y \in \ker(f)$. Veamos ahora que $\varphi(x, y) = g$. Entonces:

$$\varphi(x, y) = \varphi(f(g), f(g^{-1})g) = f(g)f(g^{-1})g = f(gg^{-1})g = f(1)g = 1g = g$$

Por tanto, φ es sobreyectiva.

Concluimos que φ es un isomorfismo. Por tanto, $G \cong \text{Im}(f) \times \ker(f)$.

Opción 2.

En primer lugar, sabemos que $\ker f \triangleleft G$, y por hipótesis $\operatorname{Im}(f) \triangleleft G$. Veamos ahora que $\ker(f) \cap \operatorname{Im}(f) = \{1\}$. Previamente veremos que para todo $x \in \operatorname{Im}(f)$, se tiene que $f(x) = x$. Dado $x \in \operatorname{Im}(f)$, existe $y \in G$ tal que $f(y) = x$. Entonces:

$$f(x) = f(f(y)) = f^2(y) \stackrel{(*)}{=} f(y) = x$$

donde en $(*)$ se cumple porque f es idempotente. Sea ahora $x \in \ker(f) \cap \operatorname{Im}(f)$. Como $x \in \ker(f)$, tenemos que $f(x) = 1$, y como $x \in \operatorname{Im}(f)$, $f(x) = x$. Entonces $1 = f(x) = x$, por lo que $x = 1$. Por tanto, $\ker(f) \cap \operatorname{Im}(f) = \{1\}$. Veamos ahora que $G = \ker(f)\operatorname{Im}(f)$:

\supseteq) Como $\ker(f), \operatorname{Im}(f) < G$, y G es un grupo, tenemos que $\ker(f)\operatorname{Im}(f) \subset G$.

\subseteq) Sea $g \in G$. Consideramos ahora $x = f(g) \in \operatorname{Im}(f)$ e $y = f(g^{-1})g$. Veamos en primer lugar que $y \in \ker(f)$:

$$f(y) = f(f(g^{-1})g) = f(f(g^{-1}))f(g) = f^2(g^{-1})f(g) = f(g^{-1})f(g) = f(g^{-1}g) = f(1) = 1$$

Por tanto, $y \in \ker(f)$. Veamos ahora que $g = xy$. Entonces:

$$xy = f(g)f(g^{-1})g = f(gg^{-1})g = f(1)g = 1g = g$$

Por tanto, $g = xy \in \ker(f)\operatorname{Im}(f)$.

Por tanto, $G = \ker(f)\operatorname{Im}(f)$. Por la condición suficiente de producto directo interno, tenemos que $G \cong \ker(f) \times \operatorname{Im}(f)$.

Ejercicio 7.4.30. Sea S un subconjunto de un grupo G . Se llama *centralizador* de S en G al conjunto

$$C_G(S) = \{x \in G \mid xs = sx \ \forall s \in S\}$$

y se llama *normalizador* de S en G al conjunto

$$N_G(S) = \{x \in G \mid xS = Sx\}.$$

1. Demostrar que $N_G(S) \leq G$.

Comprobamos las tres condiciones:

- $1 \in N_G(S)$, ya que $1S = S1 = S$.
- Sea $x, y \in N_G(S)$. Entonces $xS = Sx$ y $yS = Sy$. Entonces:

$$(xy)S = x(yS) = x(Sy) = (xS)y = (Sx)y = S(xy)$$

Por tanto, es cerrado para el producto.

- Sea $x \in N_G(S)$, $xS = Sx$. Entonces:

$$xS = Sx \implies S = x^{-1}Sx \implies Sx^{-1} = x^{-1}S \implies x^{-1} \in N_G(S)$$

Por tanto, es cerrado para inversos.

2. Demostrar que $C_G(S) \triangleleft N_G(S)$.

Veamos en primer lugar que $C_G(S) \leq N_G(S)$. Para ello, vemos en primer lugar que $C_G(S) \subseteq N_G(S)$. Fijado $x \in C_G(S)$, tenemos que $xs = sx$ para todo $s \in S$, por lo que:

$$xS = \{xs \mid s \in S\} = \{sx \mid s \in S\} = Sx$$

Comprobamos ahora las tres condiciones para ser subgrupo:

- $1 \in C_G(S)$, ya que $1s = s = s1$.
- Sea $x, y \in C_G(S)$. Entonces $xs = sx$ y $ys = sy$ para todo $s \in S$. Entonces:

$$(xy)s = x(ys) = x(sy) = (xs)y = (sx)y = s(xy)$$

Por tanto, es cerrado para el producto.

- Sea $x \in C_G(S)$, $xs = sx$. Entonces:

$$xs = sx \implies s = x^{-1}sx \implies sx^{-1} = x^{-1}s \implies x^{-1} \in C_G(S)$$

Por tanto, es cerrado para inversos.

Comprobamos ahora que $C_G(S) \triangleleft N_G(S)$. Para ello, tomamos $x \in N_G(S)$ y $y \in C_G(S)$, y veamos que $xyx^{-1} \in C_G(S)$. Para ello, tomamos $s \in S$, y como $x \in N_G(S)$, tenemos que $xS = Sx$, por lo que $sx = xs'$ con $s' \in S$ y por tanto $x^{-1}sx \in S$. Entonces:

$$yx^{-1}sx = x^{-1}sxy \implies xyx^{-1}s = sxyx^{-1} \implies xyx^{-1} \in C_G(S)$$

3. Demostrar que si $S \leq G$ entonces $S \triangleleft N_G(S)$.

Sea $s \in S$. Veamos que $s \in N_G(S)$, es decir que $sS = Ss$.

- ⊂) Sea $x \in sS$. Entonces, $\exists s' \in S$ tal que $x = ss'$. Entonces, como $ss'(s^{-1}) \in S$, tenemos que:

$$x = ss' = ss'(s^{-1})s \in Ss$$

- ⊃) Sea $x \in Ss$. Entonces, $\exists s' \in S$ tal que $x = s's$. Entonces, como $(s^{-1})s's \in S$, tenemos que:

$$x = s's = ss^{-1}s's \in sS$$

Por tanto, $S \subset N_G(S)$. Como $S \subset N_G(S)$ y $S, N_G(S) < G$, tenemos que $S < N_G(S)$. Veamos ahora que $S \triangleleft N_G(S)$. Para ello, tomamos $x \in N_G(S)$ y $s \in S$, y veamos que $xsx^{-1} \in S$. Entonces:

$$xsx^{-1} \stackrel{(*)}{=} s'xx^{-1} = s' \in S$$

donde en $(*)$ hemos empleado que $x \in N_G(S)$, por lo que $xS = Sx$.

Ejercicio 7.4.31. Sea G un grupo y H y K subgrupos suyos con $H \subseteq K$. Entonces demostrar que H es normal en K si y sólo si $K < N_G(H)$. (Así, el normalizador $N_G(H)$ queda caracterizado como el mayor subgrupo de G en el que H es normal.)

\implies) Sea $H \triangleleft K$, y veamos que $K \subset N_G(H)$. Como $H \triangleleft K$, tenemos que $kH = Hk$ para todo $k \in K$, luego $K \subset N_G(H)$. Como además $K, N_G(H) < G$, tenemos que $K < N_G(H)$.

\impliedby) Sea $K < N_G(H)$, luego $K \subset N_G(H)$. Entonces, para todo $k \in K$, tenemos que $kH = Hk$. Por tanto, $H \triangleleft K$.

Ejercicio 7.4.32. Sea G un grupo.

1. Demostrar que $C_G(Z(G)) = G$ y que $N_G(Z(G)) = G$.

Veamos en primer lugar que $C_G(Z(G)) = G$.

\subset) Sea $x \in C_G(Z(G))$, luego trivialmente $x \in G$.

\supset) Sea $x \in G$, luego $xz = zx$ para todo $z \in Z(G)$. Por tanto, $x \in C_G(Z(G))$.

Veamos ahora que $N_G(Z(G)) = G$.

\subset) Sea $x \in N_G(Z(G))$, luego trivialmente $x \in G$.

\supset) Sea $x \in G$, luego $xz = zx$ para todo $z \in Z(G)$. Por tanto, $xZ(G) = Z(G)x$, luego $x \in N_G(Z(G))$.

Análogamente, también podríamos haber usando que $G = C_G(Z(G))$ y $C_G(Z(G)) \triangleleft N_G(Z(G))$.

2. Si G es un grupo y $H < G$ ¿Cuándo es $G = N_G(H)$? ¿Y cuándo es $G = C_G(H)$?

Por el ejercicio anterior, que nos caracteriza el normalizador, sabemos que:

$$G = N_G(H) \iff H \triangleleft G$$

Por otro lado, sabemos que $C_G(H) = G$ si y sólo si $H \subset Z(G)$.

3. Si $H \leq G$ con $|H| = 2$, demostrar que $N_G(H) = C_G(H)$. Deducir que $H \triangleleft G$ si y sólo si $H \subset Z(G)$.

Si $|H| = 2$, entonces $H = \{1, h\}$ con $h \in G \setminus \{1\}$, luego $h = h^{-1}$. Veamos que $N_G(H) = C_G(H)$.

\subset) Sea $x \in N_G(H)$, luego $xH = Hx$. Como $xh \in Hx$, entonces hay dos opciones:

- $xh = 1$, luego $x = h^{-1}$. Por tanto, $xh = h^{-1}h = 1 = hh^{-1} = hx$.
- $xh = h$, luego $x = 1$. Por tanto, $xh = 1h = h = h1 = hx$.

En cual caso, $xh = hx$, luego $x \in C_G(H)$.

\supset) Como $C_G(H) \triangleleft N_G(H)$, se tiene.

Demostramos ahora que $H \triangleleft G$ si y sólo si $H \subset Z(G)$.

\implies) Como $H \triangleleft G$, por el apartado anterior tenemos que $G = N_G(H)$. Como acababa de ver que $N_G(H) = C_G(H)$, tenemos que $G = C_G(H)$. Por tanto, para todo $x \in G$, tenemos que $xh = hx$ para todo $h \in H$. Por tanto, $H \subset Z(G)$.

\Longleftarrow) Como $H \subset Z(G)$, tenemos que $C_G(H) = G$. Por tanto, se tiene que $N_G(H) = C_G(H) = G$, luego $H \triangleleft G$.

Ejercicio 7.4.33. Sea G un grupo arbitrario. Para dos elementos $x, y \in G$ se define su *conmutador* como el elemento

$$[x, y] = xyx^{-1}y^{-1}.$$

Observación. (El conmutador recibe tal nombre porque $[x, y]yx = xy$.)

Como $[x, y]^{-1} = [y, x]$, el inverso de un conmutador es un conmutador. Sin embargo el producto de dos conmutadores no tiene porqué ser un conmutador. Entonces se define el *subgrupo conmutador* o (primer) *subgrupo derivado* de G , denotado $[G, G]$, como el subgrupo generado por todos los conmutadores de G .

1. Demostrar que, $\forall a, x, y \in G$, se tiene que $a[x, y]a^{-1} = [axa^{-1}, aya^{-1}]$.

$$[axa^{-1}, aya^{-1}] = axa^{-1}aya^{-1}ax^{-1}a^{-1}ay^{-1}a^{-1} = axyx^{-1}y^{-1}a^{-1} = a[x, y]a^{-1}$$

2. Demostrar que $[G, G] \triangleleft G$.

Tenemos que:

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle$$

Como $[x, y] \in G$ para todo $x, y \in G$ y $[G, G]$ es un grupo, tenemos que $[G, G] \leq G$. Veamos que $[G, G] \triangleleft G$. Para ello, tomamos $g \in G$ y $z \in [G, G]$. Entonces, como $z \in [G, G]$, tenemos que:

$$z = [x_1, y_1] \cdots [x_n, y_n] \quad x_i, y_i \in G \quad \forall i = 1, \dots, n$$

Entonces:

$$\begin{aligned} gzg^{-1} &= g[x_1, y_1] \cdots [x_n, y_n]g^{-1} = \\ &= g[x_1, y_1]g^{-1}g[x_2, y_2]g^{-1} \cdots g[x_n, y_n]g^{-1} = \\ &= [gx_1g^{-1}, gy_1g^{-1}] \cdots [gx_ng^{-1}, gy_ng^{-1}] \in [G, G] \end{aligned}$$

3. Demostrar que el grupo cociente $G/[G, G]$, que se representa por G^{ab} , es un grupo abeliano (que se llama el abelianizado de G).

Dados $x, y \in G$, hemos de ver que $x[G, G]y[G, G] = y[G, G]x[G, G]$. Usando el producto en el cociente, hemos de ver que:

$$xy[G, G] = yx[G, G]$$

Consideramos ahora $[y^{-1}, x^{-1}] \in [G, G]$. Entonces:

$$xy[y^{-1}, x^{-1}] = xyy^{-1}x^{-1}yx = yx$$

Por tanto, $xy[G, G] = yx[G, G]$, luego $G/[G, G]$ es abeliano.

4. Demostrar que G es abeliano si y sólo si $[G, G] = 1$.

\implies) Si G es abeliano, entonces:

$$\begin{aligned} [G, G] &= \langle [x, y] \mid x, y \in G \rangle = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle = \\ &= \langle xx^{-1}yy^{-1} \mid x, y \in G \rangle = \langle 1 \mid x, y \in G \rangle = \{1\} \end{aligned}$$

\impliedby) Si $[G, G] = 1$, entonces dados $x, y \in G$, tenemos que $[x, y] = 1$, luego:

$$1 = [x, y] = xyx^{-1}y^{-1} = xy(yx)^{-1} \implies xy = yx$$

Por tanto, G es abeliano.

5. Sea $N \triangleleft G$. Demostrar que el grupo cociente G/N es abeliano si y sólo si $[G, G] < N$ (así que el grupo $[G, G]$ es el menor subgrupo normal de G tal que el cociente es abeliano).

\implies) Sea G/N abeliano, y consideramos la proyección en el cociente:

$$\begin{aligned} p: G &\longrightarrow G/N \\ g &\longmapsto gN \end{aligned}$$

Sabemos que p es un homomorfismo. Dados $x, y \in G$, tenemos que:

$$p([x, y]) = p(xyx^{-1}y^{-1}) = p(x)p(y)p(x)^{-1}p(y)^{-1} = 1$$

Por tanto, por ser p un homomorfismo, tenemos que $p([G, G]) = \{1\}$, luego $[G, G] \subseteq \ker p = N$. Por tanto, como además $[G, G]$ es un grupo, se tiene que $[G, G] < N$.

\impliedby) Sea $[G, G] < N$. Sean ahora $x, y \in G$, y busquemos ver que $xyN = yxN$. Tenemos que:

$$xy[y^{-1}, x^{-1}] = xy y^{-1} x^{-1} y x = yx$$

Como $[y^{-1}, x^{-1}] \in [G, G] < N$, tenemos que $xyN = yxN$. Por tanto:

$$(xN)(yN) = xyN = yxN = (yN)(xN)$$

Por tanto, G/N es abeliano.

Ejercicio 7.4.34.

1. Calcular el subgrupo conmutador de los grupos S_3 , A_4 , D_4 y Q_2 .

a) S_3 :

Recordemos que el subgrupo conmutador de G es el menor subgrupo normal de G tal que el cociente es abeliano. El diagrama de Hasse de S_3 conviene tenerlo presente, y se encuentra en la Figura 7.48. Comprobemos cada subgrupo de S_3 , de menor a mayor orden:

- $\{1\}$ efectivamente cumple que $\{1\} \triangleleft S_3$, pero:

$$S_3/\{1\} \cong S_3$$

Por tanto, el cociente no es abeliano, luego $\{1\} \neq [S_3, S_3]$.

- $\langle(1\ 2)\rangle$.

$$(2\ 3)(1\ 2)(2\ 3)^{-1} = (2\ 3)(1\ 2)(2\ 3) = (1\ 3) \notin \langle(1, 2)\rangle$$

Por tanto, $\langle(1\ 2)\rangle \not\trianglelefteq S_3$, luego $\langle(1\ 2)\rangle \neq [S_3, S_3]$.

- $\langle(13)\rangle$.

$$(2\ 3)(1\ 3)(2\ 3)^{-1} = (2\ 3)(1\ 3)(2\ 3) = (1\ 2) \notin \langle(1, 3)\rangle$$

Por tanto, $\langle(1\ 3)\rangle \not\trianglelefteq S_3$, luego $\langle(1\ 3)\rangle \neq [S_3, S_3]$.

- $\langle(2\ 3)\rangle$.

$$(1\ 2)(2\ 3)(1\ 2)^{-1} = (1\ 2)(2\ 3)(1\ 2) = (1\ 3) \notin \langle(2, 3)\rangle$$

Por tanto, $\langle(2\ 3)\rangle \not\trianglelefteq S_3$, luego $\langle(2\ 3)\rangle \neq [S_3, S_3]$.

- $\langle(1\ 2\ 3)\rangle$.

Sabemos que $|\langle(1\ 2\ 3)\rangle| = 3$, por lo que $[S_3, \langle(1\ 2\ 3)\rangle] = 2$, luego $\langle(1\ 2\ 3)\rangle \triangleleft S_3$. Por tanto, es un candidato a ser el subgrupo conmutador. Veamos si $S_3/\langle(1\ 2\ 3)\rangle$ es abeliano:

$$\left| \frac{S_3}{\langle(1\ 2\ 3)\rangle} \right| = \frac{|S_3|}{|\langle(1\ 2\ 3)\rangle|} = \frac{6}{3} = 2 \implies \frac{S_3}{\langle(1\ 2\ 3)\rangle} \cong C_2$$

Por tanto, $S_3/\langle(1\ 2\ 3)\rangle$ es abeliano, luego:

$$[S_3, S_3] = \langle(1\ 2\ 3)\rangle = A_3$$

b) A_4 :

El diagrama de Hasse de A_4 conviene tenerlo presente, y se encuentra en la Figura 7.51. Comprobemos cada subgrupo de A_4 , de menor a mayor orden:

- $\{1\}$ efectivamente cumple que $\{1\} \triangleleft A_4$, pero:

$$A_4/\{1\} \cong A_4$$

Por tanto, el cociente no es abeliano, luego $\{1\} \neq [A_4, A_4]$.

- $\langle(1\ 2)(3\ 4)\rangle$.

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

Por tanto, $(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} \notin \langle(1\ 2)(3\ 4)\rangle$, luego $\langle(1\ 2)(3\ 4)\rangle \not\trianglelefteq A_4$, luego $\langle(1\ 2)(3\ 4)\rangle \neq [A_4, A_4]$.

- $\langle(1\ 3)(2\ 4)\rangle$.

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

Por tanto, $(1\ 2\ 3)(1\ 3)(2\ 4)(1\ 2\ 3)^{-1} \notin \langle(1\ 3)(2\ 4)\rangle$, luego $\langle(1\ 3)(2\ 4)\rangle \not\trianglelefteq A_4$, luego $\langle(1\ 3)(2\ 4)\rangle \neq [A_4, A_4]$.

- $\langle (1\ 4)(2\ 3) \rangle$.

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

Por tanto, $(1\ 2\ 3)(1\ 4)(2\ 3)(1\ 2\ 3)^{-1} \notin \langle (1\ 4)(2\ 3) \rangle$, luego $\langle (1\ 4)(2\ 3) \rangle \not\triangleleft A_4$,
luego $\langle (1\ 4)(2\ 3) \rangle \neq [A_4, A_4]$.

- $\langle (1\ 2\ 3) \rangle$.

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

Por tanto, $(1\ 2)(3\ 4)(1\ 2\ 3)(1\ 2)(3\ 4) \notin \langle (1\ 2\ 3) \rangle$, luego $\langle (1\ 2\ 3) \rangle \not\triangleleft A_4$,
luego $\langle (1\ 2\ 3) \rangle \neq [A_4, A_4]$.

- $\langle (2\ 3\ 4) \rangle$.

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

Por tanto, $(1\ 2)(3\ 4)(2\ 3\ 4)(1\ 2)(3\ 4) \notin \langle (2\ 3\ 4) \rangle$, luego $\langle (2\ 3\ 4) \rangle \not\triangleleft A_4$,
luego $\langle (2\ 3\ 4) \rangle \neq [A_4, A_4]$.

- $\langle (1\ 3\ 4) \rangle$.

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

Por tanto, $(1\ 2)(3\ 4)(1\ 3\ 4)(1\ 2)(3\ 4) \notin \langle (1\ 3\ 4) \rangle$, luego $\langle (1\ 3\ 4) \rangle \not\triangleleft A_4$,
luego $\langle (1\ 3\ 4) \rangle \neq [A_4, A_4]$.

- $\langle (1\ 2\ 4) \rangle$.

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

Por tanto, $(1\ 3)(2\ 4)(1\ 2\ 4)(1\ 3)(2\ 4) \notin \langle (1\ 2\ 4) \rangle$, luego $\langle (1\ 2\ 4) \rangle \not\triangleleft A_4$,
luego $\langle (1\ 2\ 4) \rangle \neq [A_4, A_4]$.

- V .

En Teoría vimos que el subgrupo de Klein V es normal en A_4 . Veamos que A_4/V es abeliano:

$$\left| \frac{A_4}{V} \right| = \frac{|A_4|}{|V|} = \frac{12}{4} = 3 \implies \frac{A_4}{V} \cong C_3$$

Por tanto, A_4/V es abeliano, luego:

$$[A_4, A_4] = V$$

c) D_4 :

El diagrama de Hasse de D_4 conviene tenerlo presente, y se encuentra en la Figura 7.49. Comprobemos cada subgrupo de D_4 , de menor a mayor orden:

- $\{1\}$ efectivamente cumple que $\{1\} \triangleleft D_4$, pero:

$$D_4/\{1\} \cong D_4$$

Por tanto, el cociente no es abeliano, luego $\{1\} \neq [D_4, D_4]$.

- $\langle r^2 \rangle$.

En el Ejercicio 7.4.5 vimos que:

$$Z(D_4) = \langle r^2 \rangle$$

Como además $Z(D_4) \triangleleft D_4$, tenemos que $\langle r^2 \rangle \triangleleft D_4$. Veamos que $D_4/\langle r^2 \rangle$ es abeliano:

$$\left| \frac{D_4}{\langle r^2 \rangle} \right| = \frac{|D_4|}{|\langle r^2 \rangle|} = \frac{8}{2} = 4$$

Por tanto, es isomorfo a C_4 o a V , ambos abelianos. Por tanto, $D_4/\langle r^2 \rangle$ es abeliano, luego:

$$[D_4, D_4] = \langle r^2 \rangle$$

d) Q_2 :

El diagrama de Hasse de Q_2 conviene tenerlo presente, y se encuentra en la Figura 7.50. Comprobemos cada subgrupo de Q_2 , de menor a mayor orden:

- $\{1\}$ efectivamente cumple que $\{1\} \triangleleft Q_2$, pero:

$$Q_2/\{1\} \cong Q_2$$

Por tanto, el cociente no es abeliano, luego $\{1\} \neq [Q_2, Q_2]$.

- $\langle -1 \rangle = \{1, -1\}$.

Sea $g \in Q_2$. Entonces:

$$g(-1)g^{-1} = -(gg^{-1}) = -1 \in \langle -1 \rangle$$

Por tanto, $\langle -1 \rangle \triangleleft Q_2$. Veamos que $Q_2/\langle -1 \rangle$ es abeliano:

$$\left| \frac{Q_2}{\langle -1 \rangle} \right| = \frac{|Q_2|}{|\langle -1 \rangle|} = \frac{8}{2} = 4$$

Por tanto, es isomorfo a C_4 o a V , ambos abelianos. Por tanto, $Q_2/\langle -1 \rangle$ es abeliano, luego:

$$[Q_2, Q_2] = \langle -1 \rangle$$

2. Demostrar que, para $n \geq 3$, el subgrupo conmutador de S_n es A_n y que éste es el único subgrupo de S_n de orden $n!/2$.

Veamos que $[S_n, S_n] = A_n$.

⊂) Tenemos que $[S_n : A_n] = 2$, luego $A_n \triangleleft S_n$. Por tanto, $[S_n, S_n] \subseteq A_n$.

⊃) Sean $i, j, k \in \{1, \dots, n\}$ tres naturales distintos. Entonces:

$$(i j k) = (i j)(j k) = (i j)(i k)(i j)(i k) = (i j)(i k)(i j)^{-1}(i k)^{-1} = [(i j), (i k)]$$

Por tanto, como los 3-ciclos son generadores de A_n , entonces $A_n \subseteq [S_n, S_n]$.

Por tanto, $[S_n, S_n] = A_n$. Supongamos ahora que H es un subgrupo de S_n tal que $|H| = n!/2$. Entonces:

$$[S_n : H] = \frac{|S_n|}{|H|} = \frac{n!}{n!/2} = 2 \implies H \triangleleft S_n$$

Además, el cociente S_n/H es un grupo de orden 2, luego es cíclico, y por tanto abeliano. Por tanto, $A_n = [S_n, S_n] < H$ Y $|H| = |[S_n, S_n]| = |A_n|$, luego $H = A_n$. Por tanto, A_n es el único subgrupo de S_n de orden $n!/2$.