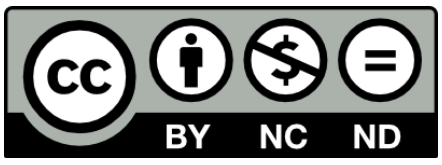
Álgebra II

Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Álgebra II

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán
Arturo Olivares Martos

Granada, 2025

Índice general

1. Relaciones de Ejercicios

1.1. Grupos: generalidades y ejemplos

Ejercicio 1.1.1. 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 1.1.2. 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 1.1.3. 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 $\mathbb{Z}_{11}^\times$:

$$7 \cdot 8 = 56 = 1 \Longrightarrow 7^{-1} = 8$$

- Para $\mathbb{Z}_{37}^\times$:

$$7 \cdot 16 = 112 = 1 \Longrightarrow 7^{-1} = 16$$

Ejercicio 1.1.4. 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 $n = 3$:

$$\mu_3 = \left\{1, \xi_3, \xi_3^2 \mid \xi_3 = \cos\left(\frac{2\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{3}\right)\right\} =$$
$$= \left\{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\right\}$$

$\cdot$	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 $n = 4$:

$$\mu_4 = \left\{1, \xi_4, \xi_4^2, \xi_4^3 \mid \xi_4 = \cos\left(\frac{\pi}{2}\right) + i\,\mathrm{sen}\left(\frac{\pi}{2}\right)\right\} =$$
$$= \left\{1, \xi_4, \xi_4^2, \xi_4^3 \mid \xi_4 = i\right\} = \{1, i, -1, -i\}$$

$\cdot$	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 $n = 8$:

$$\mu_8 = \left\{1, \xi_8, \xi_8^2, \xi_8^3, \xi_8^4, \xi_8^5, \xi_8^6, \xi_8^7 \mid \xi_8 = \cos\left(\frac{\pi}{4}\right) + i\,\mathrm{sen}\left(\frac{\pi}{4}\right)\right\} =$$
$$= \left\{1, \xi_8, \xi_8^2, \xi_8^3, \xi_8^4, \xi_8^5, \xi_8^6, \xi_8^7 \mid \xi_8 = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right\} =$$
$$= \left\{1, \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}, i, -\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}, -1, -\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}, -i, \frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\right\}$$

$\cdot$	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 1.1.5. 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 1.1.6. 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:

$$(xy)(xy) = (xy)^2 = 1 \Longrightarrow (xy)^{-1} = xy$$
$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

Por tanto, $xy = yx$ para todo $x, y \in G$, por lo que G es abeliano.

Ejercicio 1.1.7. 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.

$1 \Longrightarrow 2)$ Dados $x, y \in G$, se tiene que:

$$(xy)^2 = xyxy \overset{(*)}{=} x^2y^2$$

donde en $(*)$ se ha usado que G es abeliano.

$2 \Longrightarrow 1)$ Dados $x, y \in G$, se tiene que:

$$\begin{aligned}(xy)^2 &= (xy)(xy) = xyxy \\ &\overset{(*)}{=} x^2y^2\end{aligned}$$

donde en $(*)$ se ha usado la hipótesis. Por la propiedad cancelativa, se tiene que:

$$\cancel{x}yx\cancel{y} = x\cancel{^2}y\cancel{^2} \Longrightarrow xy = yx$$

Como se tiene para todo $x, y \in G$, entonces G es abeliano.

$1 \Longrightarrow 3)$ Dados $x, y \in G$, se tiene que:

$$(xy)^{-1} = y^{-1}x^{-1} \overset{(*)}{=} x^{-1}y^{-1}$$

donde en $(*)$ se ha usado que G es abeliano.

$3 \Longrightarrow 1)$ Dados $x, y \in G$, tenemos que:

$$(xy)^{-1} \overset{(*)}{=} x^{-1}y^{-1} = (yx)^{-1} \Longrightarrow \left((xy)^{-1}\right)^{-1} = \left((yx)^{-1}\right)^{-1} \Longrightarrow xy = yx$$

donde en $(*)$ se ha usado la hipótesis. Por tanto, como se tiene para todo $x, y \in G$, entonces G es abeliano.

□

Ejercicio 1.1.8. 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: $n = 1$.
$$(xy)^1 = xy = yx = x^1y^1$$
- 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 1.1.9. Demostrar que el conjunto de las aplicaciones $f : \mathbb{R} \to \mathbb{R}$, 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:

$$G = \{f : \mathbb{R} \to \mathbb{R} \mid \exists a, b \in \mathbb{R},\ a \neq 0 \text{ tales que } f(x) = ax + b\ \forall x \in \mathbb{R}\}$$

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:

$$f(x) = ax + b, \qquad g(x) = cx + d$$

Entonces, se tiene que:

$$(f \circ g)(x) = f(g(x)) = a(cx + d) + b = acx + ad + b \in G$$
$$(g \circ f)(x) = g(f(x)) = c(ax + b) + d = acx + cb + d \in G$$

Por tanto, G es cerrado bajo la composición de funciones. Ahora, tomando $a = 1$ y $b = 0$, se tiene que $\mathrm{Id}_{\mathbb{R}} \in G$. Veamos que $(G, \circ, \mathrm{Id}_{\mathbb{R}})$ 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 $f \circ f^{-1} = \mathrm{Id}_{\mathbb{R}}$, puesto que en la definición no se impone $f^{-1} \circ f = \mathrm{Id}_{\mathbb{R}}$):

  $$(f \circ f^{-1})(z) = a\left(a^{-1}(z - b)\right) + b = z \qquad \forall z \in \mathbb{R}$$

  Por tanto, para todo $f \in G$, existe $f^{-1} \in G$ tal que $f \circ f^{-1} = \mathrm{Id}_{\mathbb{R}}$.

Ejercicio 1.1.10.

1. Demostrar que $|\mathrm{GL}_2(\mathbb{Z}_2)| = 6$, describiendo explícitamente todos los elementos que forman este grupo.

   Sea $A \in \mathrm{GL}_2(\mathbb{Z}_2)$:

   $$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Longrightarrow |A| = ad - bc \neq 0 \Longrightarrow ad \neq bc$$

   Por tanto, los elementos de $\mathrm{GL}_2(\mathbb{Z}_2)$ son:

   $$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$
   $$A_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad A_5 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \qquad A_6 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

2. Sea $\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ y $\beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Demostrar que

$$\mathrm{GL}_2(\mathbb{Z}_2) = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}.$$

Tenemos que:

$$1 = A_1, \qquad \alpha = A_5, \qquad \alpha^2 = A_6, \qquad \beta = A_4, \qquad \alpha\beta = A_3, \qquad \alpha^2\beta = A_2$$

3. Escribir, utilizando la representación anterior, la tabla de multiplicar de $\mathrm{GL}_2(\mathbb{Z}_2)$.

$\cdot$	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 1.1.11. 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 1.1.12. 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:

$$D_n \subsetneq G \qquad \forall n \in \mathbb{N}$$

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, $\mathrm{Id}_{\mathbb{R}^2} \in G$. Veamos que $(G, \circ, \mathrm{Id}_{\mathbb{R}^2})$ 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 $f \circ f^{-1} = \mathrm{Id}_{\mathbb{R}^2}$.

- 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 $f \circ f^{-1} = \mathrm{Id}_{\mathbb{R}^2}$.

Por tanto, $(G, \circ, \mathrm{Id}_{\mathbb{R}^2})$ es un grupo.

Ejercicio 1.1.13. 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 $i = 0, \ldots, m-1$ 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 $i+1$.
   $$b^{i+1}a = bb^i a = bab^{ik} = ab^k b^{ik} = ab^{k(i+1)}$$

2. Demostrar que para todo $j = 0, \ldots, n-1$ 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 $j+1$.
   $$ba^{j+1} = ba^j a = a^j b^{k^j} a \overset{(*)}{=} a^j ab^{k^j k} = a^{j+1} b^{k^{j+1}}$$
   donde en $(*)$ se ha usado el apartado anterior.

3. Demostrar que para todo $i = 0, \ldots, m-1$ y todo $j = 0, \ldots, n-1$ 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 $j+1$.

$$b^i a^{j+1} = b^i a^j a = a^j b^{ik^j} a \overset{(*)}{=} a^j a b^{ik^j k} = a^{j+1} b^{ik^{j+1}}$$

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 $0 \leqslant r < n$, $0 \leqslant s < m$.

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:

$$x = a^{r'} b^{s'} \qquad r', s' \in \mathbb{N} \cup \{0\}$$

Supuesto $r' \geqslant n$, sea $r = r' \mod n$ $(r' = nk + r)$ y se tiene que:

$$a^{r'} = a^{nk+r} = (a^n)^k \cdot a^r = a^r$$

Además, se cumple que $0 \leqslant r < n$. Análogamente, supuesto $s' \geqslant m$, sea $s = s' \mod m$ $(s' = mk + s)$ y se tiene que:

$$b^{s'} = b^{mk+s} = (b^m)^k \cdot b^s = b^s$$

Además, se cumple que $0 \leqslant s < m$. Por tanto:

$$x = a^{r'} b^{s'} = a^r b^s \qquad 0 \leqslant r < n,\ 0 \leqslant s < m$$

Observación. Notemos que D_n es un caso particular de este grupo, donde:

$$a = r, \qquad b = s, \qquad k = n - 1, \qquad m = 2, \qquad n = n$$

Ejercicio 1.1.14. Sean $s_1, s_2 \in S_7$ las permutaciones dadas por

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

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:

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

Descomponiendo en ciclos disjuntos, se tiene que:

$$\begin{aligned} s_2 &= (1\ 5)(2\ 7\ 3\ 6\ 4) \\ s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ s_1s_2 &= (2\ 6\ 5\ 3\ 7\ 4) \\ s_2s_1 &= (1\ 6\ 3\ 2\ 7\ 4) \\ s_2^2 &= (2\ 3\ 4\ 7\ 6) \end{aligned}$$

Ejercicio 1.1.15. Dadas las permutaciones

$$p_1 = (1\ 3\ 2\ 8\ 5\ 9)(2\ 6\ 3), \qquad p_2 = (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5),$$

hallar la descomposición de la permutación producto p_1p_2 como producto de ciclos disjuntos.

Usando la notación matricial, se tiene que:

$$p_1p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 6 & 4 & 8 & 3 & 7 & 2 & 9 \end{pmatrix}$$

Descomponiendo en ciclos disjuntos, se tiene que:

$$p_1p_2 = (2\ 5\ 8)(3\ 6)$$

Ejercicio 1.1.16. 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 $\{1, \ldots, 9\}$ que deja fijos a los elementos 8 y 9.

1. Descomponer la permutación $s_1s_2s_1s_2$ como producto de ciclos disjuntos.

$$\begin{aligned} s_1s_2s_1s_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 6 & 7 & 3 & 2 & 8 & 9 \end{pmatrix} \\ &= (2\ 5\ 7)(3\ 4\ 6) \end{aligned}$$

2. Expresar matricialmente la permutación $p_3 = p_2p_1p_2$ y obtener su descomposición como ciclos disjuntos.

$$\begin{aligned} p_3 = p_2p_1p_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 1 & 4 & 6 & 2 & 7 & 8 & 5 \end{pmatrix} \\ &= (1\ 9\ 5\ 6\ 2\ 3) \end{aligned}$$

3. Descomponer la permutación s_2p_2 como producto de ciclos disjuntos y expresarla matricialmente.

$$\begin{aligned} s_2p_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 2 & 6 & 5 & 3 & 4 & 1 \end{pmatrix} \\ &= (1\ 9)(2\ 8\ 4)(3\ 7)(5\ 6) \end{aligned}$$

Ejercicio 1.1.17. 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 **??**, se tiene que:

$$\begin{aligned} O(s_1 s_2) &= 6 \\ O(s_1) &= \mathrm{mcm}(4,2) = 4 \\ O(s_2) &= \mathrm{mcm}(2,5) = 10 \end{aligned}$$

   Por tanto, $O(s_1 s_2) \neq O(s_1)O(s_2)$.

2. Calcular el orden de $s_1(s_2)^{-1}(s_1)^{-1}$.

$$\begin{aligned} s_1(s_2)^{-1}(s_1)^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 1 & 6 & 7 & 2 & 4 \end{pmatrix} = \\ &= (1\ 3)(2\ 5\ 7\ 4\ 6) O(s_1(s_2)^{-1}(s_1)^{-1}) = \mathrm{mcm}(2,5) = 10 \end{aligned}$$

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?

$$\begin{aligned} p_2 &= (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5) \\ (s_2)^2 &= (2\ 3\ 4\ 7\ 6) \\ (p_1)^{-1} &= (1\ 9\ 5\ 8\ 3)(2\ 6) \\ p_2(s_2)^2(p_1)^{-1} &= (1\ 3\ 6)(2\ 5\ 3)(1\ 9\ 2\ 8\ 5)(2\ 3\ 4\ 7\ 6)(1\ 9\ 5\ 8\ 3)(2\ 6) \\ &= (1\ 5\ 6\ 2\ 8\ 4\ 7)(3\ 9) \\ O(p_2(s_2)^2(p_1)^{-1}) &= \mathrm{mcm}(7,2) = 14 \end{aligned}$$

Ejercicio 1.1.18. 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 1.1.19. 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:
$$\left.\begin{array}{rcl} |P \cup I| & = & |P| + |I| = 6 = |S_3| \\ & \wedge & \\ P \cup I & \subset & S_3 \end{array}\right\} \Longrightarrow S_3 = P \cup I$$

   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 1.1.20. 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 1.1.21. Demostrar que el conjunto de transposiciones
$$\{(1,2),(2,3),\ldots,(n-1,n)\}$$
genera al grupo simétrico S_n.
Demostramos por doble inclusión que:
$$\langle(1,2),(2,3),\ldots,(n-1,n)\rangle = S_n$$

$\subset$) Dado $\sigma \in \langle(1,2),(2,3),\ldots,(n-1,n)\rangle$, entonces como S_n es cerrado por producto, se tiene que $\sigma \in S_n$.

$\supset$) Dado $\sigma \in S_n$, veamos que $\sigma \in \langle(1,2),(2,3),\ldots,(n-1,n)\rangle$. 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 $\{(1,2),(2,3),\ldots,(n-1,n)\}$.

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, $\sigma \in \langle (1, 2), (2, 3), \ldots, (n-1, n) \rangle$.

Ejercicio 1.1.22. Demostrar que el conjunto $\{(1, 2, \ldots, n), (1, 2)\}$ genera al grupo simétrico S_n.

Demostramos por doble inclusión que:

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

$\subset$) Dado $\sigma \in \langle (1, 2, \ldots, n), (1, 2) \rangle$, entonces como S_n es cerrado por producto, se tiene que $\sigma \in S_n$.

$\supset$) Dado $\sigma \in S_n$, veamos que $\sigma \in \langle (1, 2, \ldots, n), (1, 2) \rangle$. En primer lugar, definimos $\tau = (1, 2, \ldots, n)$. Entonces, se tiene que:

$$\tau^k(j) = j + k \qquad \forall k, j \in \{1, \ldots, n\},\ k + j \leqslant n$$

Además, por las propiedades de los conjugados, tenemos que:

$$\tau^{(k-1)}(1, 2)\tau^{-(k-1)} = (\tau^{k-1}(1), \tau^{k-1}(2)) = (k, k+1) \qquad \forall k \in \mathbb{N},\ k < n$$

Entonces, tenemos que:

$$\{(1, 2), (2, 3), \ldots, (n-1, n)\} \subset \langle (1, 2, \ldots, n), (1, 2) \rangle$$

Por tanto:

$$\sigma \in S_n = \langle (1, 2), (2, 3), \ldots, (n-1, n) \rangle \subset \langle (1, 2, \ldots, n), (1, 2) \rangle$$

Ejercicio 1.1.23. 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 1.1.24. 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 1.1.25. Encontrar un isomorfismo $\mu_2 \cong \mathbb{Z}_3^\times$.

Definimos la aplicación $f : \mu_2 \to \mathbb{Z}_3^\times$ 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:

$$f(x) = f(1 \cdot x) = f(1) \cdot f(x) = 1 \cdot f(x) = f(x) \qquad \forall x \in \mu_2$$

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 1.1.26.

1. Demostrar que la aplicación $f : \mu_4 \to \mathbb{Z}_5^\times$ dada por:

   $$1 \mapsto 1, \qquad -1 \mapsto 4, \qquad i \mapsto 2, \qquad -i \mapsto 3,$$

   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 $g : \mu_4 \to \mathbb{Z}_5^\times$ 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:

   $$O(2) = O(3) = 4 \qquad O(4) = 2$$

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:

$$1 \mapsto 1, \qquad -1 \mapsto 4, \qquad i \mapsto 3, \qquad -i \mapsto 2,$$

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 1.1.27. Encontrar un isomorfismo $\mu_2 \times \mu_2 \cong \mathbb{Z}_8^\times$.

Sea $f : \mu_2 \times \mu_2 \to \mathbb{Z}_8^\times$ 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 1.1.28. Demostrar, haciendo uso de las representaciones conocidas, que $D_3 \cong S_3 \cong \mathrm{GL}_2(\mathbb{Z}_2)$.

En primer lugar, tenemos que:

$$\begin{aligned} |D_3| &= 2 \cdot 3 = 6 \\ |S_3| &= 3! = 6 \\ |\mathrm{GL}_2(\mathbb{Z}_2)| &= (2^2 - 1)(2^2 - 2) = 6 \end{aligned}$$

Ahora, damos generadores para cada grupo. El generador de S_3 se ha visto en el Ejercicio 1.1.22, mientras que el generador de $\mathrm{GL}_2(\mathbb{Z}_2)$ se ha visto en el Ejercicio 1.1.10.

$$\begin{aligned} D_3 &= \langle r, s \mid r^3 = 1,\ s^2 = 1,\ sr = r^{-1}s \rangle \\ S_3 &= \langle (1\ 2\ 3), (1\ 2) \rangle \\ \mathrm{GL}_2(\mathbb{Z}_2) &= \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \end{aligned}$$

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 **??**), 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 $\mathrm{GL}_2(\mathbb{Z}_2)$ cumple las relaciones de D_3.

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

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

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

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

$$g(r) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad g(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Como además $\{g(r), g(s)\}$ son un generador de $\mathrm{GL}_2(\mathbb{Z}_2)$, tenemos que se trata de un epimorfismo, y como además $|S_3| = |\,\mathrm{GL}_2(\mathbb{Z}_2)|$, se trata de un isomorfismo. Por tanto, $S_3 \cong \mathrm{GL}_2(\mathbb{Z}_2)$.

Por ser $\cong$ una relación de equivalencia, tenemos que:

$$D_3 \cong S_3 \cong \mathrm{GL}_2(\mathbb{Z}_2)$$

Ejercicio 1.1.29. Sea $\mathbb{K}$ un cuerpo y considérese la operación binaria

$$\begin{array}{rccc} \otimes: & \mathbb{K}\times\mathbb{K} & \longrightarrow & \mathbb{K} \\ & (a,b) & \longmapsto & a\otimes b = a+b-ab. \end{array}$$

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:

$$\begin{array}{rccc} f: & \mathbb{K}\setminus\{1\} & \longrightarrow & \mathbb{K}^* \\ & x & \longmapsto & 1-x \end{array}$$

Veamos en primer lugar que está bien definida.

$$f(x)=1-x=0 \iff x=1\notin\mathbb{K}\setminus\{1\}$$

Veamos ahora que es un homomorfismo. Dados $x, y \in \mathbb{K} \setminus \{1\}$, tenemos que:

$$f(x \otimes y) = 1 - (x \otimes y) = 1 - (x + y - xy) = 1 - x - y + xy f(x)f(y) \quad = (1-x)(1-y) = 1 - x - ($$

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 1.1.30.

1. Probar que si $f : G \to G'$ 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 **??**.

2. Listar los órdenes de los diferentes elementos del grupo Q_2 y del grupo D_4 y concluir que D_4 y Q_2 no son isomorfos.

   En primer lugar, tenemos que:

   $$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$$
   $$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

   Calculamos los órdenes de D_4:

   $$O(1) = 1 \qquad O(r) = O(r^3) = 4$$
   $$O(r^2) = O(s) = O(sr) = O(sr^2) = O(sr^3) = 2$$

   Por otro lado, calculamos los órdenes de Q_2:

   $$O(1) = 1 \qquad O(-1) = 2$$
   $$O(\pm i) = O(\pm j) = O(\pm k) = 4$$

   Por tanto no es posible establecer un isomorfismo $f : D_4 \to Q_2$ de forma que cumpla

   $$O(x) = O(f(x)) \qquad \forall x \in D_4$$

   Por tanto, D_4 y Q_2 no son isomorfos.

Ejercicio 1.1.31. Calcular el orden de:

1. La permutación $\sigma = (1\ 8\ 10\ 4)(2\ 8)(5\ 1\ 4\ 8) \in S_{15}$.

   $$\sigma = (2\ 10\ 4)(5\ 8)$$
   $$O(\sigma) = \text{mcm}(3, 2) = 6$$

2. Cada elemento del grupo $\mathbb{Z}_{11}^{\times}$.

   $$O(1) = 1$$
   $$O(3) = O(4) = O(5) = O(9) = 5$$
   $$O(2) = O(6) = O(7) = O(8) = 10$$
   $$O(10) = 2$$

Ejercicio 1.1.32. 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 1.1.13 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. Comprobemos que los elementos generadores de V cumplen las relaciones de G:

$$\begin{aligned} O((1\ 2)(3\ 4)) = \operatorname{mcm}(2,2) = 2 &\Longrightarrow [(1\ 2)(3\ 4)]^2 = 1 \\ O((1\ 3)(2\ 4)) = \operatorname{mcm}(2,2) = 2 &\Longrightarrow [(1\ 3)(2\ 4)]^2 = 1 \\ (1\ 2)(3\ 4)\ (1\ 3)(2\ 4) &= (1\ 4)(2\ 3) \\ (1\ 3)(2\ 4)\ (1\ 2)(3\ 4) &= (1\ 4)(2\ 3) \end{aligned}$$

Por tanto, por el Teorema de Dyck (Teorema **??**), se tiene que existe un único homomorfismo $f : G \to V$ cumpliendo:

$$\begin{aligned} a &\mapsto (1\ 2)(3\ 4) \\ b &\mapsto (1\ 3)(2\ 4) \end{aligned}$$

Como además $\{f(a), f(b)\}$ son un generador de V, tenemos que se trata de un epimorfismo, y como además $|G| = |V|$, se trata de un isomorfismo. Por tanto, $G \cong V$.

Ejercicio 1.1.33. 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 $O(aba^{-1}) \leqslant n$. Por otro lado, supongamos que $\exists m \in \mathbb{N}$, con $m < n$, tal que $(aba^{-1})^m = 1$. Entonces, se tiene que $b^m = 1$, lo que contradice que $O(b) = n$. Por tanto, $O(aba^{-1}) = n$.

En cualquier caso, se tiene que $O(b) = O(aba^{-1})$.

2. Demostrar que $O(ba) = O(ab)$.

   Por el apartado anterior, considerando ahora $ba \in G$, se tiene:

$$O(ba) = O(a\ ba\ a^{-1}) = O(ab)$$

Ejercicio 1.1.34. 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:

$$ab^2 = b^3a \Longrightarrow b^2 = ab^3a \Longrightarrow$$
$$\Longrightarrow b^4 = (ab^3a)(ab^3a) = ab^6a = a(ab^3a)(ab^3a)(ab^3a)a = b^9 \Longrightarrow 1 = b^5$$

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 1.1.35. Sea $f : G \to H$ 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 $n \in \mathbb{Z}$, $n < 0$.

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

   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:

$$\begin{array}{rccc} i: & \mathbb{R}^* & \longrightarrow & \mathbb{C}^* \\ & x & \longmapsto & x \end{array}$$

   Comprobemos que se trata de un homomorfismo:

$$i(x \cdot y) = x \cdot y = i(x) \cdot i(y) \qquad \forall x, y \in \mathbb{R}^*$$

   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 **??**.

Ejercicio 1.1.36.

1. Demostrar que los grupos multiplicativos $\mathbb{R}^*$ (de los reales no nulos) y $\mathbb{C}^*$ (de los complejos no nulos) no son isomorfos.

   En $\mathbb{C}^*$, tenemos que $O(i) = 4$. Busquemos $x \in \mathbb{R}^*$ tal que $O(x) = 4$.

   $$x^4 = 1 \iff x = \pm 1$$

   No obstante, $O(1) = 1$ y $O(-1) = 2$. Por tanto, no pueden ser isomorfos.

2. Demostrar que los grupos aditivos $\mathbb{Z}$ y $\mathbb{Q}$ no son isomorfos.

   Por reducción al absurdo, supongamos que existe un isomorfismo $f : \mathbb{Q} \to \mathbb{Z}$. Entonces, consideramos $f^{-1}(1) = q \in \mathbb{Q}$, que sabemos que existe por ser f biyectiva. Entonces, se tiene que:

   $$1 = f(q) = f\left(\frac{q}{2} + \frac{q}{2}\right) = f\left(\frac{q}{2}\right) + f\left(\frac{q}{2}\right) = 2f\left(\frac{q}{2}\right) \Longrightarrow f\left(\frac{q}{2}\right) = \frac{1}{2} \notin \mathbb{Z}$$

   Por tanto, hemos llegado a una contradicción y , por tanto, hemos probado que no puede existir tal isomorfismo.

Ejercicio 1.1.37. Sea G un grupo. Demostrar:

1. G es abeliano $\iff$ La aplicación $f : G \to G$ dada por $f(x) = x^{-1}$ es un homomorfismo de grupos.

   $\Longrightarrow$) Supongamos que G es abeliano. Entonces, para todo $x, y \in G$, se tiene que:

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

   donde en $(*)$ hemos usado que G es abeliano. Por tanto, f es un homomorfismo.

   $\Longleftarrow$) 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 $f : G \to G$ dada por $f(x) = x^2$ es un homomorfismo de grupos.

   $\Longrightarrow$) 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.

$\Longleftarrow$) Supongamos que f es un homomorfismo. Entonces, para todo $x, y \in G$, se tiene que:

$$xyxy = f(xy) = f(x)f(y) = x^2y^2 \Longrightarrow xy = yx$$

Por tanto, G es abeliano.

Ejercicio 1.1.38. Si G es un grupo cíclico demostrar que cualquier homomorfismo de grupos $f : G \to H$ 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 1.1.39. 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 $f : \mathbb{K} \to \mathbb{K}^*$. 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:

   $$(x - 1)(x + 1) = 0 \qquad \forall x \in \mathbb{K}^* \setminus \{1\}$$

   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:

   $$(-1)(-1) = 1 \Longrightarrow O(-1) = 2$$

   Por ser el orden conservado en un isomorfismo, tenemos que:

   $$O(f^{-1}(-1)) = 2 \Longrightarrow f^{-1}(-1) + f^{-1}(-1) = 0 \Longrightarrow f^{-1}(-1)\,(1 + 1) = 0$$

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:

$$f^{-1}(-1) = 0 \Longrightarrow f(0) = -1$$

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.

1.2. Subgrupos, Generadores, Retículos y Grupos cíclicos

Ejercicio 1.2.1. 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. $n = 4$.

$$\begin{aligned} S_4 = \{&1, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4),\\ &(1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4),\\ &(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}\\ A_4 = \{&1, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),\\ &(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \end{aligned}$$

Ejercicio 1.2.2. 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 $0 \leqslant j < k < n$ 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 $0 \leqslant m < n$, 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 1.2.3.

1. Demostrar que el subgrupo de $\mathrm{SL}_2(\mathbb{Z}_3)$ 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 $\mathrm{SL}_2(\mathbb{Z}_3)$ 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}:

$$\begin{aligned} i^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ j^2 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ ji &= \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \\ i^3 j &= \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \end{aligned}$$

Por tanto, i, j cumplen las relaciones de Q_2^{abs}. Por el Teorema de Teorema de Dyck, existe un único homomorfismo $f : Q_2^{abs} \to \langle i, j \rangle$ 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:

$$\begin{aligned} \langle i, j \rangle &= \{1, i, i^2, i^3, j, ij, i^2 j, i^3 j\} \\ |Q_2^{abs}| &= 8 = |\langle i, j \rangle| \end{aligned}$$

  Por tanto, f es un isomorfismo.

Por tanto, $\langle i, j \rangle \cong Q_2^{abs} \cong Q_2$.

2. Demostrar que $\mathrm{SL}_2(\mathbb{Z}_3)$ 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:

$$O(\pm i) = O(\pm j) = O(\pm k) = 4 \qquad O(-1) = 2$$

Supongamos ahora $\exists H \leqslant S_4$ 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 $\exists f : \mathrm{SL}_2(\mathbb{Z}_3) \to S_4$ un isomorfismo, y consideramos la restricción a $Q = \langle i, j \rangle \cong Q_2$. Sabemos que la siguiente aplicación es un isomorfismo:

$$\begin{array}{rccc} f_{\big|_Q}: & Q & \longrightarrow & f_*(Q) \\ & x & \longmapsto & f(M) \end{array}$$

Por tanto, $Q_2 \cong Q \cong f_*(Q)$. Además, como f_* es un homomorfismo y se tiene $Q < \mathrm{SL}_2(\mathbb{Z}_3)$, 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, $\mathrm{SL}_2(\mathbb{Z}_3) \ncong S_4$.

Ejercicio 1.2.4. Razonar que un subconjunto no vacío $X \subseteq G$ de un grupo G es un subgrupo de G si, y sólo si, $X = \langle X \rangle$.

$\Longrightarrow$) 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, $X = \langle X \rangle$.

$\Longleftarrow$) 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 1.2.5. Sean $a, b \in G$ dos elementos de un grupo que conmutan entre sí, esto es, para los que $ab = ba$, y de manera que sus órdenes son primos relativos, esto es, $\text{mcd}(O(a), O(b)) = 1$.

1. Razonar que $\langle a \rangle \cap \langle b \rangle = \{1\}$.

   Puesto que la intersección de dos subgrupos es un subgrupo, sabemos que $\langle a \rangle \cap \langle b \rangle$ es un subgrupo de G, y por tanto $1 \in \langle a \rangle \cap \langle b \rangle \neq \emptyset$. Por tanto, podemos considerar $x \in \langle a \rangle \cap \langle b \rangle$.

   Como menciona el $\text{mcd}(O(a), O(b))$, podemos considerar que ambos órdenes son finitos. Por el Teorema de Lagrange, sabemos que:

   $$|\langle a \rangle \cap \langle b \rangle| \mid |\langle a \rangle| = O(a)$$
   $$|\langle a \rangle \cap \langle b \rangle| \mid |\langle b \rangle| = O(b)$$

   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, $\langle a \rangle \cap \langle b \rangle = \{1\}$.

2. Demostrar que $O(ab) = O(a)O(b)$.

   Puesto que conmutan, tenemos que:

   $$(ab)^k = a^k b^k \qquad \forall k \in \mathbb{Z}$$

   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 $(ab)^t = 1$.

$$1 = (ab)^t = a^t b^t \implies a^t = b^{-t} \in \langle a \rangle \cap \langle b \rangle = \{1\} \implies \left\{ \begin{array}{l} a^t = 1 \Longrightarrow n \mid t \\ a^t = 1 \Longrightarrow m \mid t \end{array} \right\} \overset{(*)}{\Longrightarrow} nm \mid t$$

   donde en $(*)$ hemos usado que $\text{mcd}(n, m) = 1$. Por tanto:

   $$O(ab) = nm = O(a)O(b)$$

Ejercicio 1.2.6. 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:

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

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 1.2.7. Sea G un grupo y $a, b \in G$ dos elementos de orden finito. ¿Es ab necesariamente de orden finito?

Observación. Considerar el grupo $\mathrm{GL}_2(\mathbb{Q})$ 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:

$$a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 \implies O(a) = 4$$
$$b^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$
$$b^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 \implies O(b) = 6$$

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 1.2.8. 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.

   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.

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

   Por tanto, $H < S_3$.

2. Describir las diferentes clases de S_3 módulo H.

   Por el Teorema de Lagrange, sabemos que:

$$|S_3| = [S_3 : H] \cdot |H| \Longrightarrow [S_3 : H] = \frac{6}{3} = 2 \Longrightarrow |S_3/_H\sim| = |S_3/\sim_H| = 2$$

   Calculamos ahora las clases de equivalencia de $S_3/_H\sim$:

$$1H = \{1x \mid x \in H\} = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H$$
$$(1\ 2)H = \{(1\ 2)x \mid x \in H\} = \{(1\ 2), (1\ 2)(1\ 2\ 3), (1\ 2)(1\ 3\ 2)\} = \{(1\ 2), (2\ 3), (1\ 3)\} \neq H$$

   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 $S_3/\sim_H$:

$$H1 = \{x1 \mid x \in H\} = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H$$
$$H(1\ 2) = \{x(1\ 2) \mid x \in H\} = \{(1\ 2), (1\ 2\ 3)(1\ 2), (1\ 3\ 2)(1\ 2)\} = \{(1\ 2), (1\ 3), (2\ 3)\} \neq H$$

   Por tanto, hemos encontrado todas las clases de equivalencia de $S_3/\sim_H$.

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

Ejercicio 1.2.9. Sea G un grupo finito.

1. Demostrar que si $H \leqslant G$ 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 Teorma 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 $G_2 \leqslant G_1 \leqslant G$, entonces

$$[G : G_2] = [G : G_1][G_1 : G_2],$$

Por un lado, como $G_2 \leqslant G$, entonces:

$$|G| = [G : G_2] \cdot |G_2|$$

Por otro lado, como $G_1 \leqslant G$, y $G_2 \leqslant G_1$, 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

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_{r-1} \geqslant G_r,$$

entonces

$$[G : G_r] = \prod_{i=0}^{r-1} [G_i : G_{i+1}].$$

Demotrsamos por inducción sobre r:

- $\underline{r = 2:}$ $G = G_0 \geqslant G_1 \geqslant G_2$. Por el apartado anterior, sabemos que:

$$[G : G_2] = [G : G_1][G_1 : G_2]$$

- $\underline{\text{Supuesto cierto para } r\text{, demostramos para } r+1:}$ Por hipótesis de inducción, sabemos que:

$$[G : G_r] = \prod_{i=0}^{r-1} [G_i : G_{i+1}]$$

Por otro lado, como $G_{r+1} \leqslant G_r \leqslant G$, 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

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_{r-1} \geqslant G_r = \{1\},$$

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 1.2.10.

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:

     $$xyxy = 1 \Longrightarrow yxy = x \Longrightarrow xy = yx$$

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

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:

$$y = x^2 \Longrightarrow 1 = y^2 = x^4 = x \Longrightarrow x = 1$$

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.
- 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 $O(xy) = 6$:

  $$(xy)^2 = x^2 \qquad (xy)^3 = y \qquad (xy)^4 = x \qquad (xy)^5 = x^2y \qquad (xy)^6 = 1$$

  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 1.2.11. Describir los retículos de subgrupos de los siguientes grupos:

1. El grupo V de Klein.
2. El grupo simétrico S_3.
3. El grupo diédrico D_4.
4. El grupo cuaternio Q_2.

$$\begin{array}{c} C_{p^n} = \langle x \rangle \\ | \\ \vdots \\ | \\ C_{p^2} = \langle x^{p^{n-2}} \rangle \\ | \\ C_p = \langle x^{p^{n-1}} \rangle \\ | \\ \{1\} = \langle x^{p^n} \rangle = \langle 1 \rangle \end{array}$$

Figura 1.1: Retículo de subgrupos de C_{p^n} para el Ejercicio 1.2.12.

$$\begin{array}{c} C_8 = \langle x \rangle \\ | \\ C_4 = \langle x^2 \rangle \\ | \\ C_2 = \langle x^4 \rangle \\ | \\ \{1\} = \langle x^8 \rangle = \langle 1 \rangle \end{array}$$

Figura 1.2: Retículo de subgrupos de C_8 para el Ejercicio 1.2.12.

5. El grupo alternado A_4.

Ejercicio 1.2.12. 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 $k \in \{0, \ldots, n\}$. Además:

$$O(x^{p^k}) = \frac{O(x)}{\text{mcd}(O(x), p^k)} = \frac{p^n}{\text{mcd}(p^n, p^k)} = \frac{p^n}{p^k} = p^{n-k}$$

Por tanto, $\langle x^{p^k} \rangle = C_{p^{n-k}}$. Además, fijado $k \in \{0, \ldots, n\}$, 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 1.1.

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 1.2.

Ejercicio 1.2.13. Demostrar que un grupo finito $G \neq \{1\}$ carece de subgrupos propios, esto es, que su retículo de subgrupos es el de la Figura 1.3 si, y sólo si, $G = C_p$ es un grupo cíclico de orden primo.

$\Longrightarrow$) 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.

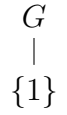


Figura 1.3: Retículo de subgrupos de para el Ejercicio 1.2.13.

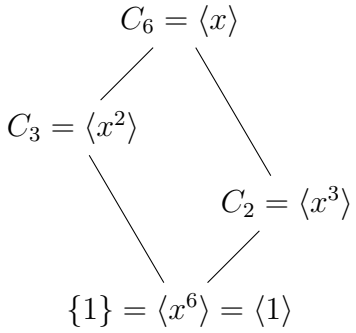


Figura 1.4: Retículo de subgrupos de C_6 para el Ejercicio 1.2.14.

$\Longleftarrow$) 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 1.2.14. Describir los retículos de subgrupos de los grupos cíclicos siguentes:

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, $O(x^k) = \frac{6}{\text{mcd}(6,k)} = \frac{6}{k}$. Por tanto, estos son:

   $$\langle x^2 \rangle = \{1, x^2, x^4\}$$
   $$\langle x^3 \rangle = \{1, x^3\}$$

   Por tanto, el retículo de subgrupos de C_6 es el de la Figura 1.4.

2. C_{12}.

   Sabemos que los subgrupos propios de C_{12} son de la forma $\langle x^k \rangle$ con $k \in \{2, 3, 4, 6\}$. Además, $O(x^k) = \frac{12}{\text{mcd}(12,k)} = \frac{12}{k}$. 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 1.5.

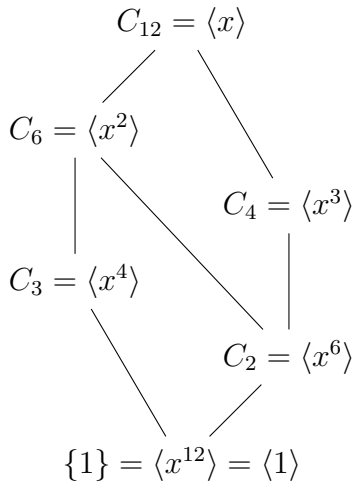


Figura 1.5: Retículo de subgrupos de C_{12} para el Ejercicio 1.2.14.

Ejercicio 1.2.15. 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:

$$H_2 = \langle t^{46} \rangle = \langle t^{\mathrm{mcd}(136,46)} \rangle = \langle t^2 \rangle$$

Por otro lado:

$$\begin{aligned} H_1 &= \langle t^{48}, t^{72} \rangle = \langle t^{48} \rangle \vee \langle t^{72} \rangle = \langle t^{\mathrm{mcd}(136,48)} \rangle \vee \langle t^{\mathrm{mcd}(136,72)} \rangle \\ &= \langle t^8 \rangle \vee \langle t^8 \rangle = \langle t^8 \rangle \end{aligned}$$

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 1.2.16. Demostrar que el grupo de unidades $\mathbb{Z}_7^\times$ es un grupo cíclico.

Veamos que $O(5) = 6$:

$$\begin{aligned} 5^2 &= 4 \\ 5^3 &= 6 \\ 5^4 &= 2 \\ 5^5 &= 3 \\ 5^6 &= 1 \end{aligned}$$

Por tanto, $\mathbb{Z}_7^\times = \langle 5 \rangle$ es un grupo cíclico.

Ejercicio 1.2.17. Sea G un grupo y sea C_n el grupo cíclico de orden n generado por x. Demostrar que:

1. Si $\theta : C_n \to G$ es un homomorfismo de grupos, entonces:

$$O(\theta(x)) \mid n, \quad \text{y} \quad \theta(x^k) = \theta(x)^k \quad \forall k \in \{0, \ldots, n-1\}.$$

Para la primera parte, queremos ver que $(\theta(x))^n = 1$. Sabemos que:

$$1 = \theta(1) = \theta(x^n) = \theta(x)^n \Longrightarrow O(\theta(x)) \mid n$$

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 $\theta_g : C_n \to G$ 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 $\theta_g : C_n \to G$ 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, $O(g) = n$.

   $\Longrightarrow$) Supongamos que θ_g es monomorfismo, y veamos que $O(g) = n$. Como $O(g) \mid n$, entonces $O(g) \leqslant n$. Supongamos ahora $m \in \mathbb{Z}$ tal que $g^m = 1$. Entonces:

   $$\theta_g(1) = 1 = g^m = \theta_g(x)^m = \theta_g(x^m)$$

   Por ser θ_g monomorfismo, entonces $x^m = 1$, y por tanto $m \geqslant n$. Por tanto, $O(g) = n$.

   $\Longleftarrow$) Supongamos que $O(g) = n$, y veamos que θ_g es monomorfismo. Para ello, calculemos el núcleo de θ_g:

   $$\begin{aligned}\ker(\theta_g) &= \{x \in C_n \mid \theta_g(x) = 1\} = \{x^k \mid k \in \{0, \dots, n-1\}, \quad \theta_g(x^k) = 1\} \\ &= \{x^k \mid k \in \{0, \dots, n-1\}, \quad g^k = 1\}\end{aligned}$$

   Como $O(g) = n$, entonces $g^k = 1 \iff k = 0$. Por tanto, $\ker(\theta_g) = \{1\}$, y por tanto θ_g es monomorfismo.

4. Existe un isomorfismo de grupos

   $$\mathcal{U}(\mathbb{Z}_n) \cong \mathrm{Aut}(C_n),$$

   dado por $r \mapsto f_r$ para cada $r = 1, \dots, n-1$ con $\mathrm{mcd}(r, n) = 1$, donde el automorfismo f_r se define mediante $f_r(x) = x^r$.

   En particular, $\mathrm{Aut}(C_n)$ es un grupo abeliano de orden $\varphi(n)$.

Ejercicio 1.2.18.

1. Describir explícitamente el grupo de automorfismos $\mathrm{Aut}(C_8)$.
2. Demostrar que $\mathrm{Aut}(C_8)$ es isomorfo al grupo de Klein.