Ejercicio 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.

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

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

$$(s_2)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 7 & 5 & 2 & 6 \end{pmatrix} \qquad (s_2)^2 = (2\,3\,4\,7\,6)$$

Ejercicio 15. Dadas las permutaciones

son composiciones

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

calculamos en ese orden

hallar la descomposición de la permutación producto $p_1 p_2$ como producto de ciclos disjuntos.

$$p_1 p_2 = (1\,3\,2\,8\,5\,9)(2\,6\,3)(1\,3\,6)(2\,5\,3)(1\,9\,2\,8\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 6 & 4 & 8 & 3 & 7 & 2 & 9 \end{pmatrix} = (2\,5\,8)(3\,6)$$

Ejercicio 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 $\mathbb{Z}_n$.

Procedemos por conocer $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid \exists v \in \mathbb{Z}_n \; av = 1\}$. Por tanto

$n = 4$, $\mathbb{Z}_4^\times = \{[1]\}$

*	[1]
[1]	[1]

$n = 6$ $\mathbb{Z}_6^\times = \{[1]\}$

*	[1]
[1]	[1]

$n = 8$, $\mathbb{Z}_8^\times = \{[1], [3]\}$

*	[1]	[3]
[1]	[1]	[3]
[3]	[3]	[1]

Ejercicio 2. Describir explícitamente la tabla de multiplicar de los grupos $\mathbb{Z}_p^\times$ para $p = 2$, $p = 3$, $p = 5$ y $p = 7$.

Siguiendo la definición del ejercicio 1.

$p = 2$ $\mathbb{Z}_2^* = \{[1]\}$

*	[1]
[1]	[1]

$p = 3$ $\mathbb{Z}_3^\times = \{[1], [2]\}$

*	[1]	[2]
[1]	[1]	[2]
[2]	[2]	[1]

A partir de aquí notaremos de la siguiente forma $[x] = x$

$p=5 \quad \mathbb{Z}_5^{\times} = \{1,2,3\}$

*	1	2	3
1	1	2	3
2	2	4	1
3	3	1	4

$p=7 \quad \mathbb{Z}_7^{\times} = \{1,2,3,4,5\}$

*	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	1	3
3	3	6	2	5	1
4	4	1	5	2	6
5	5	3	1	6	4

Ejercicio 3. Calcular el inverso de 7 en los grupos $\mathbb{Z}_{11}^{\times}$ y $\mathbb{Z}_{37}^{\times}$.

Sabiendo que en ambos casos el neutro es $[1]$ buscamos $x \in \mathbb{Z}_{11}^{\times}$ e $y \in \mathbb{Z}_{37}^{\times}$ tal que $[7x] = [1]$.

$\mathbb{Z}_{11}^{\times} = \{1,2,3,4,5,6,7,8,9,10\} \Rightarrow x = 8$ pues $[7 \cdot 8] = [56] = [1]$ pues $7 \cdot 8 \bmod 11 = 1$, entonces $[7]^{-1} = [8]$

$\mathbb{Z}_{37}^{\times}$ contiene a todos los números del 1 a 36 pues 37 es primo. Luego $x = 16$ pues $7 \cdot 16 \bmod 37 = 1$ entonces $[7]^{-1} = [16]$

Ejercicio 5. En el conjunto $\mathbb{Q}^{\times} := \{q \in \mathbb{Q} | \, q \neq 0\}$ de los números racionales no nulos, se considera la operación de división, dada por $(x, y) \mapsto \frac{x}{y} = xy^{-1}$. ¿Nos da esta operación una estructura de grupo en $\mathbb{Q}^{\times}$?

Para ello, debemos comprobar las propiedades de los grupos con la división:

- Asociativa: Dados $x, y, z \in \mathbb{Q}^{\times}$, $((x, y), z) = (\frac{x}{y}, z) = (xy^{-1}, z) = (xy^{-1}z^{-1}) = (xy^{-1})z^{-1} = x(y^{-1}z^{-1}) = x(zy)^{-1}$

$$(x,(y,z)) = (x, yz^{-1}) = (x(yz^{-1})^{-1}) = x\,zy^{-1}$$

Por tanto, no nos da una estructura de grupo pues no cumple la asociativa

Ejercicio 6. Sea G un grupo en el que $x^2 = 1$ para todo $x \in G$. Demostrar que el grupo G es abeliano.

Debemos ver que el producto es conmutativo, pero si $xx = 1$ estamos diciendo que $x^{-1} = x$ luego.

Dados $x, y \in G \quad xyxy = 1 \Leftrightarrow yxy = x \Leftrightarrow xy = yx$

Por tanto, el grupo es abeliano.

Ejercicio 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 $(xy)^{-1} = x^{-1}y^{-1}$.

Demostramos cada implicación.

$1 \Rightarrow 2)$

Si G es abeliano, dados $x, y \in G$ tenemos que $xy = yx$ luego

$$(xy)^2 = (xy)(xy) = xyyx = xy^2x = xxy^2 = x^2y^2$$

$\underline{2 \Rightarrow 3)}$ Veamos qué ocurre con $(x^{-1}y^{-1})^2 \overset{2}{=} (x^{-1})^2(y^{-1})^2 = x^{-1}x^{-1}y^{-1}y^{-1} \Rightarrow x^{-1}y^{-1} = y^{-1}x^{-1} = (xy)^{-1}$

$(x^{-1}y^{-1})^2 = x^{-1}y^{-1}x^{-1}y^{-1}$

$\underline{3 \Rightarrow 1)}$ $xy = ((xy)^{-1})^{-1} \overset{3}{=} (x^{-1}y^{-1})^{-1} = yx$

Ejercicio 8. Demostrar que si en un grupo G, $x, y \in G$ verifican que $xy = yx$ entonces, para todo $n \geq 1$, se tiene que $(xy)^n = x^n y^n$.

Procedemos por inducción

$n=1$ es trivial pues $xy = xy$

Supuesto para n lo vemos para $n+1$:

$(xy)^{n+1} = (xy)^n xy = x^n y^n xy = x^n x y^n y = x^{n+1} y^{n+1}$ $\square$

Ejercicio 9. Si $a, b \in \mathbb{R}$, $a \neq 0$, demostrar que el conjunto de las aplicaciones $f : \mathbb{R} \to \mathbb{R}$, tales que $f(x) = ax + b$, es un grupo con la composición como ley de composición.

$y = ax + b$

$x = \frac{y-b}{a}$

Para ello, probamos las propiedades:

i) Asociativa: derivado de la asociatividad de la composición

ii) Existencia de neutro: la identidad es el neutro

iii) Existencia de simétrico, dado f buscamos g tal que $g \circ f = id$, es decir, que $\forall x \in \mathbb{R}$ $(g \circ f)(x) = x$

$(g \circ f)(x) = x$ sii $g = f^{-1}$ de donde se ve que g viene dada por $g(x) = \frac{x-b}{a}$

Por tanto, tenemos ya probado que la estructura definida es un grupo

Ejercicio 11. Dar las tablas de grupo para los grupos D_3, D_4, D_5 y D_6.

D_3

	1	r	r^2	s	rs	r^2s
1	1	r	r^2	s	rs	r^2s
r	r	r^2	1	rs	r^2s	s
r^2	r^2	1	r	r^2s	s	rs
s	s	r^2s	rs	1	r^2	r
rs	rs	s	r^2s	r	1	r^2
r^2s	r^2s	rs	s	r^2	r	1

D_4, D_5 y D_6 son análogos y basta conocer que $D_n = \langle r, s \mid rs = sr^{-1}, r^n = 1, s^2 = 1 \rangle$ BIEN

Ejercicio 16. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas en los ejercicios anteriores.

1. Descomponer la permutación $s_1 s_2 s_1 s_2$ como producto de ciclos disjuntos.
2. Expresar matricialmente la permutación $p_3 = p_2 p_1 p_2$ y obtener su descomposición como ciclos disjuntos.
3. Descomponer la permutación $s_2 p_2$ como producto de ciclos disjuntos y expresarla matricialmente
   Nota: 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. $s_1 s_2 s_1 s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 4 & 6 & 7 & 3 & 2 \end{pmatrix} = (2\,5\,7)(3\,4\,6)$

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

3. $s_2 p_2 = (1\,5)(2\,7\,3\,6\,4)(1\,3\,6)(2\,5\,3)(1\,9\,2\,8\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 2 & 6 & 5 & 3 & 4 & 1 \end{pmatrix} = (1\,9)(2\,8\,4)(3\,7)(5\,6)$

Ejercicio 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?
2. Calcular el orden de $s_1(s_2)^{-1}(s_1)^{-1}$.
3. Calcular la permutación $(s_1)^{-1}$, y expresarla como producto de ciclos disjuntos.
4. Calcular la permutación $(p_1)^{-1}$ y expresarla matricialmente.
5. Calcular la permutación $p_2(s_2)^2(p_1)^{-1}$. ¿Cuál es su orden?

1. $O(s_1 s_2) = 6 \quad O(s_1)\, O(s_2) = 4 \cdot 10 = 40$

2. $s = s_1 (s_2)^{-1} (s_1)^{-1} = (1345)(67)(51)(46372)(5431)(76) \Rightarrow O(s) = 20$

3. $s_1^{-1} = (76)(5431)$

4. $p_1^{-1} = (958231)(362) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 6 & 4 & 8 & 3 & 7 & 2 & 5 \end{pmatrix} = (19582)(36)$

5. $p_2 (s_2)^2 (p_1)^{-1} = (136)(253)(19285)(15)(27364)(15)(27364)(19582)(36) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}$

$= (15647)(2938)$

Luego orden es $mcm(5,4) = 20$

Ejercicio 18. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas anteriormente. Sean también $s_3 = (2\,4\,6)$, $s_4 = (1\,2\,7)(2\,4\,6\,1)(5\,3)$. ¿Cuál es la paridad de las permutaciones s_1, $s_4 p_1 p_2$ y $p_2 s_3$?

Para ver la paridad de una permutación usaremos que, para $\sigma \in S_n$ $n \in \mathbb{N}$

σ es par (impar) $\iff$ nº de subciclos de la descomposición con longitud par es par (impar)

$s_1 = (1345)(67) \qquad s_2 = (15)(27364)$

Por tanto s_1 es par

$p_1 = (13859)(26) \qquad p_2 = (1953286) \qquad s_4 = (17)(246)(35)$

$s_4 p_1 p_2 = (17)(246)(35)(13859)(26)(1953286)$

Por tanto $s_4 p_1 p_2$ es impar

$p_2 s_3 = (1953286)(246)$

Por tanto $p_2 s_3$ es par

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Ejercicio 19. En el grupo S_3, se consideran las permutaciones $\sigma = (1\,2\,3)$ y $\tau = (1\,2)$.

1. Demostrar que
$$S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}. \tag{0.1}$$

2. Reescribir la tabla de multiplicar de S_3 empleando la anterior expresión de los elementos de S_3.

3. Probar que
$$\sigma^3 = 1, \tau^2 = 1, \tau\sigma = \sigma^2\tau. \tag{0.2}$$

4. Observar que es posible escribir toda la tabla de multiplicar de S_3 usando simplemente la descripción (0.1) y las relaciones (0.2).

1. Sabemos que $S_3 = \{1, (12), (13), (23), (123), (132)\}$, veamos cómo obtener la expresión dada.

$(12) = \tau \qquad (123) = \sigma \qquad \sigma\tau = (123)(12) = (13)$

$\sigma^2 = (123)(123) = (132) \qquad \sigma^2\tau = (132)(13) = (23)$

Por tanto, queda demostrado el resultado

2.

S_3	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

Donde hemos usado que

$\sigma^3=1$, $\tau^2=1$, $\tau\sigma=\sigma^2\tau$

Se ve fácil haciendo las cuentas

3. Es fácil ver que basta con hacer las cuentas.

Ejercicio 21. Demostrar que el conjunto de transposiciones

$$\{(1,2),(2,3),\dots,(n-1,n)\}$$

genera al grupo simétrico S_n.

Es un resultado visto en clase pues $\forall \sigma \in S_n$, σ se puede escribir como producto de trasposiciones de esa forma

Ejercicio 22. Demostrar que el conjunto $\{(1,2,\dots,n),(1,2)\}$ general al grupo simétrico S_n.

Sabemos que $(1\ 2\ 3\ 4\ 5 \dots n) = (12)(23)\dots(n{-}1\ n)$ luego el grupo contiene al grupo de las trasposiciones, es decir, genera a S_n $\forall n \in \mathbb{N}$.

Ejercicio 23. Demostrar que para cualquier permutación $\alpha \in S_n$ se verifica que $s(\alpha) = s(\alpha^{-1})$, donde s denota la ***signatura***, o paridad, de una permutación.

Dada $\alpha \in S_n$, sabemos que admite una descomposición única salvo desordenaciones de ciclos disjuntos, es decir, $\alpha = \sigma_1 \dots \sigma_n$ $n \in \mathbb{N}$ $n \in \mathbb{N}$.

De esta manera, como $\mathcal{E}(\alpha) = \mathcal{E}(\sigma_1)\mathcal{E}(\sigma_2)\dots\mathcal{E}(\sigma_n)$ y se cumple que $\alpha^{-1} = \sigma_1^{-1}\dots\sigma_n^{-1}$ obtenemos que

$$\mathcal{E}(\alpha^{-1}) = \mathcal{E}(\sigma_1^{-1})\dots\mathcal{E}(\sigma_n^{-1})$$

La idea principal es mantener las longitudes.

Pero como $O(\sigma_i) = O(\sigma_i^{-1})$ pues sólo se ha invertido el sentido del ciclo obtenemos que $\mathcal{E}(\sigma_i) = \mathcal{E}(\sigma_i^{-1})$ $\forall i \in \Delta_n$

Ejercicio 24. Demostrar que si $(x_1x_2\cdots x_r) \in S_n$ es un ciclo de longitud r, entonces

$$s(x_1x_2\cdots x_r) = (-1)^{r-1}.$$

Sabemos que todo ciclo se puede descomponer de la forma (si $\sigma = (x_1 \dots x_r)$)

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

Es decir, en $r-1$ trasposiciones luego $s(\sigma) = s(x_1x_2)\dots s(x_{r-1}x_r)$ pero $s(x_ix_j) = -1$ $\forall i,j \in \Delta_r$ luego

$s(\sigma) = (-1)^{r-1}$ $\forall r \in \mathbb{N}$ $\square$

Ejercicio 25. Encontrar un isomorfismo $\mu_2 \cong \mathbb{Z}_3^\times$.

Como μ_n = raíces n-ésimas de la unidad tenemos que $\mu_2 = \{1,-1\}$ y $\mathcal{U}(\mathbb{Z}_3) = \{1,2\}$ y construimos el isomorfismo

$$f: \mu_2 \longrightarrow \mathcal{U}(\mathbb{Z}_3)$$
$$1 \longmapsto \bar{1}$$
$$-1 \longmapsto \bar{2}$$

pues es inyectivo y sobreyectivo a parte de ser un homomorfismo de grupos: $f(xy) = f(x)f(y) \wedge f(1) = 1$.

Ejercicio 26. 1. Demostrar que la aplicación

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

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 $\mathbb{Z}_5$.

2. Encontrar otro isomorfismo entre estos dos grupos que sea distinto del anterior.

1. Sí pues es biyectivo y es homomorfismo
2. $f: \mu_4 \longrightarrow \mathcal{U}(\mathbb{Z}_5)$

$$1 \longmapsto \bar{1}$$
$$-1 \longmapsto \bar{4}$$
$$i \longmapsto \bar{3}$$
$$-i \longmapsto \bar{2}$$

Ejercicio 27. Encontrar un isomorfismo $\mu_2 \times \mu_2 \cong \mathbb{Z}_8^\times$.

$$f: \mu_2 \times \mu_2 \longrightarrow \mathcal{U}(\mathbb{Z}_8)$$
$$(1,1) \longmapsto \bar{1}$$
$$(1,-1) \longmapsto \bar{3}$$
$$(-1,1) \longmapsto \bar{5}$$
$$(-1,-1) \longmapsto \bar{7}$$

$\mu_2 \times \mu_2 = \{(1,1)\,(1,-1)\,(-1,1)\,(-1,-1)\}$

$\mathcal{U}(\mathbb{Z}_8) = \{1,3,5,7\}$

Podemos usar Dyck viendo que ambos son isomorfos a V^{abs}

Ejercicio 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 $i = 0, \cdots, m-1$ se verifica $b^i a = ab^{ik}$.
2. Demostrar que para todo $j = 0, \cdots, n-1$ se verifica $ba^j = a^j b^{k^j}$.
3. Demostrar que para todo $i = 0, \cdots, m-1$ y todo $j = 0, \cdots, n-1$ se verifica $b^i a^j = a^j b^{ik^j}$.
4. Demostrar que todo elemento de $\langle a, b \rangle$ puede escribirse como $a^r b^s$ con $0 \leq r < n$, $0 \leq s < m$.

Ejercicio 28. Demostrar, haciendo uso de las representaciones conocidas, que $D_3 \cong S_3 \cong GL_2(\mathbb{Z}_2)$.

Haremos uso del teorema de Dyck pues, de partida, sabemos que:

i) $|D_3| = |S_3| = |GL_2(\mathbb{Z}_2)|$

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

$S_3 = \langle (12), (123) \rangle$

$GL_2(\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$

Entonces, como $(12)^2 = \cancel{(12)}\ 1$, $(123)^3 = \cancel{(123)}\ 1$ y $(123)(12) = (13)$, $(12)(123)^2 = (13)$, luego por el teorema de Dyck tenemos que $D_3 \cong S_3$

De la misma forma identificando $r = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ y $s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ obtenemos que $D_3 \cong GL_2(\mathbb{Z}_2)$. Por tanto, basta aplicar transitividad para ver la cadena de isomorfía dada

Ejercicio 29. Sea K un cuerpo y considérese la operación binaria

$$\otimes : K \times K \to K \quad a \otimes b = a + b - ab\,.$$

Demostrar que $(K - \{1\}, \otimes)$ es un grupo isomorfo al grupo multiplicativo K^*.

Quién es K^* $\Rightarrow$ pensar en $\mathbb{C}^*$

Ejercicio 30.

1. Probar que si $f : G \cong G'$ es un isomorfismo de grupos, entonces $o(a) = o(f(a))$, para todo elemento $a \in G$.
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.

1. Sea $a \in G \mid O(a) = n$, $n \in \mathbb{N} \Rightarrow a^n = 1$. De esta manera, consideramos $f(a^n) = f(1) = 1$ por ser f homomorfismo. Además, $f(a^n) = (f(a))^n$ luego $O(f(a)) = n$. Veamos que n es el menor exponente posible; pues si $\exists m \in \mathbb{N} \mid a^m = 1 \Rightarrow n \mid m$ en G pero $f(a^m) = (f(a))^m = f(1) = 1$ luego m podría ser el orden de $f(a)$ en G'; pero en ese caso la aplicación f perdería su biyectividad.

2. Sabemos que:

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

donde

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

$O(1) = 1$ $\qquad O(r) = 4$

$O(-1) = 2$ $\qquad O(r^2) = 2$

$O(r^3) = 4$

Luego $Q_2 \not\cong D_4$.

Si tenemos los mismos órdenes $\Rightarrow$ biyección

Ejercicio 31. Calcular el orden de:

1. la permutación $\sigma = (1\ 8\ 10\ 4)(2\ 8)(5\ 1\ 4\ 8) \in S_{15}$. $\sim = (2\ 10\ 4)(5\ 8)$
2. cada elemento del grupo $\mathbb{Z}_{11}^{\times}$.

1. Pasar por ciclos disjuntos.

2. $\mathcal{U}(\mathbb{Z}_{11})$

$$\boxed{o([a]^k) = \frac{o(a)}{d} \text{ donde } d = \text{mcd}(u,k)}$$ no visto pero lo veremos

$o([2]) = 10 = o([8]) = o([7]) = o([6])$

$o([4]) = 5 = o([5]) = o([9]) = o([3])$

$o([10]) = 2$.

Ejercicio 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.

Nos definen el grupo $\mathcal{G} = \langle x, y \mid x^2 = 1 = y^2 \wedge xy = yx \rangle$ que tal y como lo vimos en clase

$$\mathcal{G} \equiv V^{abs}$$

y $V^{abs} = \{1, x, y, xy\}$. Además, $V^{abs} \cong V$ por lo visto en clase.

Ejercicio 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).
2. Demostrar que $o(ba) = o(ab)$

1. Una forma de verlo es, si $\mathcal{G}$ es un grupo definimos $\bar{\mathcal{G}}_a$ como su conjugado, es decir

$$\bar{\mathcal{G}}_a = \{ aba^{-1} \mid b \in \mathcal{G} \}$$

debido a la elección de a, aba^{-1} es único para cada $b \in \mathcal{G}$ luego podemos establecer un isomorfismo $f_a : \mathcal{G} \longrightarrow \bar{\mathcal{G}}_a$ que es sobreyectivo pues $|\mathcal{G}| = |\bar{\mathcal{G}}_a|$ y es

$$b \longmapsto aba^{-1}$$

inyectivo por la elección de a. Por tanto, como $\mathcal{G} \cong \bar{\mathcal{G}}_a$ obtenemos que $o(b) = o(aba^{-1})\ \forall b \in \mathcal{G}$.

Si $O(b)=\infty \Rightarrow O(aba^{-1})=\infty$ pues en caso de que $O(aba^{-1})=n \Rightarrow ab^n a^{-1}=1 \Rightarrow b^n=1$

2. Si $O(ab)=\infty \Rightarrow O(ba)=\infty$ pues si $O(ba)=n \Rightarrow (ba)^n=b(ab)^{n-1}a=1$ luego $(ab)^{n-1}=b^{-1}a^{-1}$

entonces $(ab)^{-1}=(ab)^{n-1}$, es decir, $O(ab)=n$!!

Si $O(ab)=n \Leftrightarrow (ab)^n=1 \Leftrightarrow$ (haciendo la misma op) $\Leftrightarrow O(ba)=n$

Ejercicio 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 $o(b)=5$.

Es claro que $O(a)=2$ y veamos que $G \cong D_5$, basta identificar $a \equiv s$ y $b \equiv r$

debemos comprobar que $b^5=1$:

$$\underbrace{b^2=ab^3a}_{} \Rightarrow \underbrace{b^2a=ab^3}_{}$$

$$\left.\begin{array}{l} ab^6=ab^2b^2b^2=aab^3aab^3aab^3a=b^3b^3b^3a=b^9a \\ ab^6=ab^3b^3=b^2b^2a=b^4a \end{array}\right\} \Rightarrow b^9a=b^4a \Rightarrow b^5=1 \Rightarrow o(b)=5$$

Ejercicio 35. Sea $f: G \to H$ un homomorfismo de grupos. Demostrar:

1. $f(x^n)=f(x)^n \quad \forall n \in \mathbb{Z}$.
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?
3. Si f es un isomorfismo entonces G es abeliano $\Leftrightarrow H$ es abeliano.

Todo esto está demostrado en los apuntes

Ejercicio 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.

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

De hecho, $O(i)=4$ y $\nexists x \neq \{1,-1\} \mid O(x)=4$

1. Basta con ver que los reales* son densos en $\mathbb{C}^*$ luego $\mathbb{R}^* \subset \mathbb{C}^*$ pero $\mathbb{C}^* \not\subset \mathbb{R}^*$, es decir, no pueden ser isomorfos. Sería tanto como decir que $\mathbb{R}$ y $\mathbb{R}^2$ son isomorfos; pero dim $\mathbb{R}=1$ y dim $\mathbb{R}^2=2$

2. De nuevo, $\mathbb{Q}$ es denso en $\mathbb{R}$ pero $\mathbb{Z}$ no lo es. De hecho, ¿$\mathbb{Q} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$?

Supongamos $\underset{\text{homom.}}{f}: \mathbb{Q} \longrightarrow \mathbb{Z}$ no trivial $\Rightarrow f(1)=n \in \mathbb{Z}$ entonces $\forall r \in \mathbb{Z}^+ \Rightarrow r\, f(\tfrac{1}{r})=f(1)=n$ luego $r \mid n$

Ejercicio 37. Sea G un grupo. Demostrar:

1. G es abeliano $\Leftrightarrow$ la aplicación $f : G \to G$ dada por $f(x) = x^{-1}$ es un homomorfismo de grupos.
2. G es abeliano $\Leftrightarrow$ la aplicación $f : G \to G$ dada por $f(x) = x^2$ es un homomorfismo de grupos.

1 $\Rightarrow$) Dados $x, y \in G$, $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$ $\wedge$ $f(x)f(y) = x^{-1}y^{-1}$ luego f es homomorfismo

$\Leftarrow$) Dados $x, y \in G$ sabemos que $(x^{-1})^{-1} = x$ $\wedge$ $(y^{-1})^{-1} = y$ luego $xy = f(f(x))f(f(y)) = f(f(x)f(y)) = f(x^{-1}y^{-1})$
$= (x^{-1}y^{-1})^{-1} = yx$

2. $\Rightarrow$) Dados $x, y \in G$ $f(xy) = (xy)^2 = (xy)(yx) = xy^2x = x^2y^2 = f(x)f(y)$ luego es homomorfismo

$\Leftarrow$) Dados $x, y \in G$ veamos que $xy = yx$

Ejercicio 38. Si G es un grupo cíclico demostrar que cualquier homomorfismo de grupos $f : G \to H$ está determinado por la imagen del generador.

Como G es cíclico $\Rightarrow \exists a \in G \mid G = \langle a \rangle \Rightarrow$ si $x \in G$, $x = a^n$ para algún $n \in \mathbb{N}$. Entonces
$f(x) = f(a^n) = (f(a))^n$

Ejercicio 39. Demostrar que no existe ningún cuerpo K tal que sus grupos aditivo $(K, +)$ y $(K^*, .)$ sean isomorfos.

Supongamos que lo sean $\Rightarrow \exists \varphi\ (K^*, \cdot) \longrightarrow (K, +)$ entonces $0 = \varphi(1) = \varphi((-1)(-1)) = \varphi(-1) + \varphi(-1) = 2\varphi(-1)$

Si $car(K) \neq 2 \Rightarrow \varphi(1) = \varphi(-1)$ y no sería inyectiva (φ).

Si $car(K) = 2 \Rightarrow \forall x \in K\ \exists! y \in K \mid \varphi^{-1}(y) = x \Rightarrow x^2 = \varphi^{-1}(y+y) = \varphi^{-1}(2y) = \varphi^{-1}(0) = 1 \Rightarrow x = 1$ luego no pueden ser isomorfos