Foto: José Juan Castro

Álgebra II

Relaciones de Ejercicios

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra II Relaciones de Ejercicios

Los Del DGIIM, `losdeldgiim.github.io`

Arturo Olivares Martos

Granada, 2025

Índice general

1. Preguntas de Teoría

Ejercicio 1. Define el concepto de subgrupo normal de un grupo. Demuestra el Tercer Teorema de Isomorfía para grupos (esto es, describe de qué forma son los subgrupos de un grupo cociente y cómo son los cocientes de un grupo cociente).

Definición 1.1. Sea G un grupo. Un subgrupo $N < G$ se dice *normal* en G, notado por $N \lhd G$, si:

$$xN = Nx \quad \forall x \in G.$$

En tal caso, tendremos que los conjuntos conciente $G/_N\!\sim$ y $G/\!\sim_N$ son iguales, por lo que podemos considerar simplemente el cociente G/N, cuyos elementos llamaremos *clases laterales* de N en G.

Cabe resaltar la propiedad más relevante de los subgrupos normales: dotan al conjunto cociente G/N de una estructura de grupo, como se puede ver en el siguiente teorema.

Teorema 1.1. *Sea G un grupo y N un subgrupo normal de G. Entonces, el conjunto cociente G/N es un grupo con la operación:*

$$\begin{array}{rccc} \cdot : & G/N \times G/N & \longrightarrow & G/N \\ & (xN, yN) & \longmapsto & (xy)N \end{array}$$

Este grupo se llama grupo cociente *de G por N. Además, la proyección canónica $p : G \to G/N$ es un homomorfismo de grupos.*

Vistos estos conceptos, enunciamos y demostramos el Tercer Teorema de Isomorfía para grupos, también llamado Teorema del Doble Cociente.

Teorema 1.2 (Tercer Teorema de Isomorfía)**.** *Sea G un grupo y $N \lhd G$ un subgrupo normal de G. Entonces, hay una biyección entre los subgrupos de G que contienen a N y los subgrupos de G/N, dada por $H \mapsto H/N$.*

Además, $H \lhd G \iff H/N \lhd G/N$, en cuyo caso:

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

Demostración. Dada la proyección canónica $p : G \to G/N$, consideramos las aplicaciones imagen directa e imagen inversa por p, dadas por:

$$\begin{array}{rccc} p_* : & \mathcal{P}(G) & \longrightarrow & \mathcal{P}(G/N) \\ & H & \longmapsto & \{p(h) \mid h \in H\} \end{array}$$

$$\begin{array}{rccc} p^*: & \mathcal{P}(G/N) & \longrightarrow & \mathcal{P}(G) \\ & J & \longmapsto & \{x \in G \mid p(x) \in J\} \end{array}$$

Definimos ahora los siguientes conjuntos:

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

Consideramos ahora las restricciones de p_* y p^* a los conjuntos $\mathcal{A}$ y $\mathcal{B}$ respectivamente, aunque las notaremos de la misma forma.

$$p_* : \mathcal{A} \to \mathcal{B}$$
$$p^* : \mathcal{B} \to \mathcal{A}$$

Veamos en primer lugar que están bien definidas:

- Sea $H \in \mathcal{A}$, por lo que $H < G$ y $N \subseteq H$. Veamos que $p_*(H) < G/N$.

  Como $H < G$ y p es un homomorfismo, tenemos que $p_*(H) < p_*(G) = G/N$, luego $p_*(H) \in \mathcal{B}$ y está bien definida.

  Veamos qué forma tiene $p_*(H)$. Como $N \lhd G$ y $N \subset H$, tenemos que $N \lhd H$, luego:

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

- Sea $J \in \mathcal{B}$, por lo que $J < G/N$. Veamos que $p^*(J) < G$ y que $N \subseteq p^*(J)$.

  Como $J < G/N$ y p es un homomorfismo, tenemos que $p^*(J) < p^*(G/N) = G$. Veamos ahora que $N \subseteq p^*(J)$. Sea ahora $n \in N$, luego:

  $$p(n) = nN = N \in J \implies n \in p^*(J).$$

  donde hemos usado que $N \in J$ puesto que N es el elemento neutro de G/N. Por tanto, $p^*(J) \in \mathcal{A}$ y está bien definida.

Veamos ahora que p_* y p^* son inversas entre sí, demostrando que componen la identidad en sus respectivos conjuntos:

- Sea $H \in \mathcal{A}$, y tenemos que:

  $$\begin{aligned} p^*(p_*(H)) = p^*(H/N) &= \{x \in G \mid p(x) \in H/N\} = \{x \in G \mid xN \in H/N\} = \\ &= \{x \in G \mid \exists h \in H : xN = hN\} = \{x \in G \mid x \in H\} = H \end{aligned}$$

- Sea $J \in \mathcal{B}$, y veamos que:

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

  donde en $(*)$ hemos empleado que p es sobreyectiva.

Por tanto, p_* y p^* son inversas entre sí, luego son biyecciones. La biyección mencionada en el enunciado es:

$$\begin{array}{rccc} p_*: & \mathcal{A} & \longrightarrow & \mathcal{B} \\ & H & \longmapsto & H/N \end{array}$$

Veamos ahora la segunda parte del enunciado.

$\Longrightarrow$) Sea $H \lhd G$, luego $H/N < G/N$. Sean ahora $x \in G$ y $h \in H$, tenemos que:

$$xN\ hN\ (xN)^{-1} = (xhx^{-1})N \overset{(*)}{=} h'N \in H/N$$

donde en $(*)$ hemos empleado que $H \lhd G$ luego $xhx^{-1} = h' \in H$. Por tanto, $H/N \lhd G/N$.

$\Longleftarrow$) Sea $H/N \lhd G/N$, luego $H < G$. Sea $x \in G$ y $h \in H$, tenemos que:

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

Por tanto, $H \lhd G$.

Tan solo nos queda demostrar la isomorfía mencionada en el enunciado. Consideramos las proyecciones canónicas $p_N : G \to G/N$ y $p_H : H \to H/N$. Como $N \subset H = \ker(p_H)$, por la Propiedad Universal del Conjunto Cociente, tenemos existe un único homomorfismo $\varphi : G/N \to G/H$ tal que $p_H = \varphi \circ p_N$, como se muestra en la Figura 1.1.

$$\begin{tikzcd} G \arrow[r, "p_N"] \arrow[dr, "p_H"'] & G/N \arrow[d, dotted, "\varphi"] \\ & G/H \end{tikzcd}$$

Figura 1.1: Situación de la Propiedad Universal del Conjunto Cociente.

Aplicando el Primer Teorema de Isomorfía a φ, tenemos que:

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

Como p_H es sobreyectiva, φ también lo es, luego $Im(\varphi) = G/H$. Veamos ahora que $\ker(\varphi) = H/N$:

$$\begin{aligned} \ker(\varphi) &= \{xN \in G/N \mid \varphi(xN) = H\} \\ &= \{xN \in G/N \mid p_H(x) = H\} \\ &= \{xN \in G/N \mid x \in H\} = H/N. \end{aligned}$$

Por tanto, tenemos que:

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

□

Por tanto, dado un grupo G y un subgrupo normal $N \lhd G$, todos los subgrupos de G/H son de la forma H/N para algún subgrupo $H < G$ con $N \subset H$. Además, dado un subgrupo normal $H/N \lhd G/N$, hemos visto que $H \lhd G$ y que:

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

Ejercicio 2. Define los conceptos de serie de composición y de serie derivada de un grupo y da dos definiciones de grupo resoluble demostrando su equivalencia. Razona que S_4 es resoluble pero que S_5 no lo es.

Antes de definir serie de composición, hemos de realizar varias definiciones:

Definición 1.2 (Serie)**.** Sea G un grupo. Una serie de G es una cadena de subgrupos $G_0, \ldots, G_r$ tales que:

$$G = G_0 > G_1 > \ldots > G_r = \{1\}.$$

En tal caso, diremos que es una serie de G de longitud r.

Definición 1.3 (Serie Normal)**.** Sea G un grupo. Una serie de G es normal si todos sus subgrupos son normales, es decir, si:

$$G_i \rhd G_{i+1} \quad \forall i = 0, \ldots, r-1.$$

En tal caso, notaremos la serie como:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{1\}.$$

Además, a los cocientes G_i/G_{i+1} de la serie los llamaremos *factores de la serie*.

Definición 1.4 (Refinamiento de una serie)**.** Sea G un grupo, y sea la siguiente serie de G:

$$G = G_0 > G_1 > \ldots > G_r = \{1\}. \tag{1.1}$$

Un refinamiento de la serie (1.1) es una serie de G de la forma:

$$G = H_0 > H_1 > \ldots > H_s = \{1\} \tag{1.2}$$

de forma que, para todo $i \in \{0, \ldots, r-1\}$, existe un $j \in \{0, \ldots, s-1\}$ tal que $G_i = H_j$. Es decir, si todo subgrupo de la serie (1.1) aperece en la serie (1.2) (por lo que $s \geqslant r$).

- Un refinamiento se dice *normal* si la serie (1.2) es normal.
- Un refinamiento se dice *propio* si, al menos, se ha añadido un subgrupo; es decir, $\exists j \in \{0, \ldots, s-1\}$ tal que $H_j \neq G_i$ para todo $i \in \{0, \ldots, r-1\}$.

Definición 1.5 (Serie de composición)**.** Sea G un grupo. Una serie de composición de G es una serie normal sin refinamientos propios.

Veamos ahora la definición de serie derivada. Previamente, hemos de definir algunos conceptos previos.

Definición 1.6 (Conmutador)**.** Sea G un grupo. El conmutador de dos elementos $x, y \in G$ es el elemento:

$$[x, y] = xyx^{-1}y^{-1} \in G$$

Definición 1.7 (Subgrupo conmutador)**.** Sea G un grupo. El subgrupo conmutador de G, denotado por $[G, G]$, es el subgrupo generado por todos los conmutadores de G:

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle.$$

Algunas propiedades importantes del subgrupo conmutador que usaremos en la demostración son las siguientes:

Proposición 1.3. *Sea G un grupo. Entonces:*

1. $G/[G,G]$ *es abeliano.*
2. $[G,G] \lhd G$.
3. *Si $N \lhd G$, entonces:*
$$G/N \text{ es abeliano} \iff [G,G] < N.$$
4. *Si $H < G$ es un subgrupo de G, entonces:*
$$[H,H] < [G,G].$$
5. $[G,G] = \{1\}$ *si y solo si G es abeliano.*

Definición 1.8 (Serie derivada)**.** Sea G un grupo. La serie derivada de G es la serie normal siguiente:
$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(k)} \rhd \ldots$$
donde $G^{(0)} = G$ y $G^{(k+1)} = [G^{(k)}, G^{(k)}]$ para todo $k \geqslant 0$.

Notemos que no tiene por qué existir un $k \in \mathbb{N}$ tal que $G^{(k)} = \{1\}$, por lo que la serie derivada puede ser infinita. En el caso de que exista, será un grupo resoluble.

Definición 1.9 (Grupo resoluble)**.** Sea G un grupo. Diremos que G es *resoluble* si su serie derivada es finita; es decir, si existe un $k \in \mathbb{N}$ tal que $G^{(k)} = \{1\}$.

Veamos ahora la caracterización buscada.

Proposición 1.4 (Caracterización de grupo resoluble)**.** *Un grupo G es resoluble si y solo si tiene una serie normal con factores abelianos.*

Demostración.

$\Longrightarrow$) Sea G un grupo resoluble, luego su serie derivada es finita. Por tanto, existe un $k \in \mathbb{N}$ tal que $G^{(k)} = \{1\}$. Sea esta:
$$G = G^0 \rhd G' \rhd G'' \rhd \ldots \rhd G^{(k)} = \{1\}.$$
Esta serie es normal, y sus factores son:
$$G^{(i)}/G^{(i+1)} = G^{(i)}/[G^{(i)}, G^{(i)}] \qquad \forall i = 0, \ldots, k-1.$$
Estos factores ya hemos mencionado anteriormente que son abelianos.

$\Longleftarrow$) Sea G un grupo con una serie normal con factores abelianos. Entonces, existe una serie normal de la forma:
$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_r = \{1\},$$
donde todos los factores son abelianos. Demostremos que $G^{(k)} < G_k$ para todo $k \in \{0, \ldots, r\}$:

- Para $k = 0$, queremos ver que $G^{(0)} = G < G_0$, lo cual es cierto.
- Supuesto cierto para k, veamos que $G^{(k+1)} < G_{k+1}$:
  Como $G_k \rhd G_{k+1}$ y G_k/G_{k+1} es abeliano, tenemos que:
  $$[G_k, G_k] < G_{k+1}$$
  Por tanto:
  $$G^{(k+1)} = [G^{(k)}, G^{(k)}] < [G_k, G_k] < G_{k+1}.$$
  donde en la primera desigualdad hemos empleado que $G^{(k)} < G_k$ por la hipótesis de inducción.

Por tanto, para todo $k \in \{0, \dots, r\}$ tenemos que $G^{(k)} < G_k$. Empleando el reultado en r, como $G_r = \{1\}$, tenemos que:
$$G^{(r)} < G_r = \{1\} \Longrightarrow G^{(r)} = \{1\}.$$
Por tanto, la serie derivada de G es finita, luego G es resoluble.

$\square$

Veamos ahora el ejemplo de los grupos S_n que se menciona en el enunciado. Queremos ver que S_4 es resoluble pero que S_5 no lo es.

- Veamos que S_4 es resoluble.

  Para ello, buscamos una serie normal suya con factores abelianos. Consideramos la serie:
  $$S_4 \rhd A_4 \rhd V \rhd \{1\},$$
  Veamos en primer lugar que es una serie normal:

  - $A_4 \lhd S_4$ pues $[S_4 : A_4] = 2$.
  - Veamos que $V \lhd A_4$. Dado $\sigma \in A_4$, y $\gamma \in V$, si $\gamma = 1$ entonces:
    $$\sigma\gamma\sigma^{-1} = 1 \in V$$
    Si $\gamma \neq 1$, entonces tomamos $x_1, x_2, x_3, x_4 \in \{1, 2, 3, 4\}$ distintos tales que $\gamma = (x_1\ x_2)(x_3\ x_4)$, y tenemos que:
    $$\sigma\gamma\sigma^{-1} = \sigma(x_1\ x_2)(x_3\ x_4)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2))(\sigma(x_3)\ \sigma(x_4))$$
    Como $\sigma \in A_4$, en particular es inyectiva, luego $\sigma(x_1), \sigma(x_2), \sigma(x_3), \sigma(x_4)$ son distintos, por lo que la permutación obtenida es un producto de 2 transposiciones disjuntas, luego:
    $$\sigma\gamma\sigma^{-1} \in V.$$
    En cualquier caso, tenemos que $\sigma\gamma\sigma^{-1} \in V$, luego $V \lhd A_4$.
  - Por último, $V \lhd \{1\}$ es trivial.

Veamos ahora que los factores son abelianos:

- $|S_4/A_4| = 2$ primo, luego $S_4/A_4 \cong \mathbb{Z}_2$, que es abeliano.
- $|A_4/V| = 3$ primo, luego $A_4/V \cong \mathbb{Z}_3$, que es abeliano.
- V es el subgrupo de Klein, que es abeliano.

Por tanto, S_4 es resoluble.

- Veamos ahora que S_5 no es resoluble.

  En este caso, será más fácil aplicar la definición. Veamos que $[S_n, S_n] = A_n$ para todo $n \geqslant 3$.

  $\subset)$ Como $A_n \lhd S_n$ y $S_n/A_n \cong \mathbb{Z}_2$ clíclico (abeliano), tenemos que:

  $$[S_n, S_n] < A_n.$$

  $\supset)$ Empleamos que:

  $$A_n = \langle (x\ y\ z) : x, y, z \in \{1, \ldots, n\}, x \neq y, x \neq z, y \neq z\rangle.$$

  Fijados $x, y, z \in \{1, \ldots, n\}$ distintos, tenemos que:

  $[(x\ y), (x\ z)] = (x\ y)(x\ z)(x\ y)^{-1}(x\ z)^{-1} = (x\ y)(x\ z)(x\ y)(x\ z) = (x\ y\ z) \in [S_n, S_n].$

  Por tanto, $A_n \subset [S_n, S_n]$.

  Por tanto, $A_n = [S_n, S_n]$. Entonces:

  $$S_5' = [S_5, S_5] = A_5.$$

  Como A_5 es simple por el Teorema de Abel, tenemos que los únicos subgrupos normales suyos son A_5 y $\{1\}$. Como S_5 no es abeliano, tenemos $[A_5, A_5] \neq \{1\}$, luego:

  $$A_5' = [A_5, A_5] = A_5.$$

  Por tanto, la serie derivada de S_5 es infinita:

  $$S_5 \rhd A_5 \rhd A_5 \rhd A_5 \rhd \ldots$$

  Por tanto, S_5 no es resoluble.

Ejercicio 3. Define, para un grupo G, los conceptos de G-conjunto X y de órbita y estabilizador de un elemento $x \in X$. Demuestra los resultados requeridos que conduzcan, en las condiciones oportunas, a la llamada fórmula de clases

$$|G| = |Z(G)| + \dots$$

Definición 1.10 (Acción)**.** Sea G un grupo y X un conjunto. Una acción de G sobre X es una aplicación:

$$\begin{array}{rccc} ac: & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & ac(g,x) \end{array}$$

tal que:

1. $ac(1,x) = x$ para todo $x \in X$.
2. $ac(g_1g_2,x) = ac(g_1, ac(g_2,x))$ para todo $g_1, g_2 \in G$ y $x \in X$.

En tal caso, diremos que G actúa (por la izquierda) sobre X y notaremos la acción como:

$$ac(g,x) = {}^gx \quad \forall g \in G, x \in X.$$

En este caso, diremos que X es un $G-$conjunto.

Proposición 1.5 (Órbita)**.** *Sea G un grupo y X un $G-$conjunto. Definimos la siguiente relación en X:*

$$x \sim y \iff \exists g \in G : y = {}^gx$$

Entonces, $\sim$ es una relación de equivalencia en X. A la clase de equivalencia de x la llamaremos órbita *de x y la denotaremos por* $\mathrm{Orb}(x)$*:*

$$\mathrm{Orb}(x) = \{y \in X \mid \exists g \in G : y = {}^gx\}.$$

Proposición 1.6 (Estabilizador)**.** *Sea G un grupo y X un $G-$conjunto. Definimos el estabilizador de un elemento $x \in X$ como el conjunto siguiente:*

$$\mathrm{Stab}_G(x) = \{g \in G \mid {}^gx = x\}.$$

Entonces, $\mathrm{Stab}_G(x) < G$ *es un subgrupo de G que llamaremos subgrupo estabilizador de x en G.*

Demostración. Fijado $x \in X$, es claro que $\mathrm{Stab}_G(x) \subset G$. Sean $g_1, g_2 \in \mathrm{Stab}_G(x)$, luego:

$${}^{g_1g_2^{-1}}x = {}^{g_1}\left({}^{g_2^{-1}}x\right) \overset{(*)}{=} {}^{g_1}\left({}^{g_2^{-1}}({}^{g_2}x)\right) = {}^{g_1g_2^{-1}g_2}x = {}^{g_1}\left({}^{1}x\right) = {}^{g_1}x \overset{(*)}{=} x.$$

donde en $(*)$ hemos empleado que $g_1, g_2 \in \mathrm{Stab}_G(x)$. Por tanto, $g_1g_2^{-1} \in \mathrm{Stab}_G(x)$, luego $\mathrm{Stab}_G(x)$ es un subgrupo de G. □

Definición 1.11 (Punto Fijo)**.** Sea G un grupo y X un $G-$conjunto. Un elemento $x \in X$ se dice *punto fijo* de la acción de G sobre X si:

$$^g x = x \quad \forall g \in G.$$

Al conjunto de todos los puntos fijos de la acción de G sobre X lo llamaremos *conjunto de puntos fijos* y lo denotaremos por $\operatorname{Fix}(X)$:

$$\operatorname{Fix}(X) = \{x \in X \mid {}^g x = x \quad \forall g \in G\}.$$

Con vistas a demostrar la fórmula de clases, consideramos X finito. Entonces, puesto que $\sim$ es una relación de equivalencia, las órbitas de la acción de G sobre X forman una partición de X. Sea Γ el conjunto formado por un un único representante de cada órbita de la acción de G sobre X. Entonces, tenemos que:

$$|X| = \sum_{x \in \Gamma} |\operatorname{Orb}(x)|.$$

Buscamos ahora simplificar esta expresión. Para ello, tenemos en cuenta la siguiente proposición, de demostración directa a partir de las definiciones anteriores.

Proposición 1.7. *Sea G un grupo finito y X un $G-$conjunto. Entonces, para todo $x \in X$, equivalen:*

$$x \in \operatorname{Fix}(X) \iff \operatorname{Orb}(x) = \{x\} \iff \operatorname{Stab}_G(x) = G.$$

Con esta proposición, podemos simplificar la expresión anterior considerando los puntos fijos. De esta forma, sea Γ' el conjunto formado por un único representante de cada órbita de la acción de G sobre X que no sea unitaria (que no sea un punto fijo), de forma que $\Gamma' \subset X \setminus \operatorname{Fix}(X)$. Entonces, tenemos que:

$$|X| = |\operatorname{Fix}(X)| + \sum_{x \in \Gamma'} |\operatorname{Orb}(x)|.$$

Por último, podemos evitarnos también el cálculo de las órbitas haciendo uso de la siguiente proposición.

Proposición 1.8. *Sea G un grupo finito y X un $G-$conjunto. Entonces:*

$$|\operatorname{Orb}(x)| = [G : \operatorname{Stab}_G(x)] \quad \forall x \in X.$$

Demostración. Sea $x \in X$, y consideramos el conjunto $G/_{\operatorname{Stab}_G(x)}\sim$ (no podemos considerar el grupo cociente puesto que no tenemos que $\operatorname{Stab}_G(x) \lhd G$). Definimos la aplicación siguiente:

$$\begin{array}{rccc} \varphi : & G/_{\operatorname{Stab}_G(x)}\sim & \longrightarrow & \operatorname{Orb}(x) \\ & g\operatorname{Stab}_G(x) & \longmapsto & {}^g x \end{array}$$

- Veamos que está bien definida. Sea $g_1 \operatorname{Stab}_G(x) = g_2 \operatorname{Stab}_G(x)$, por lo que $\exists h \in \operatorname{Stab}_G(x)$ tal que $g_1 = g_2 h$. Entonces:

  $$^{g_1}x = {}^{g_2 h}x = {}^{g_2}\left({}^h x\right) = {}^{g_2}x,$$

  donde en la última igualdad hemos empleado que $h \in \operatorname{Stab}_G(x)$, luego $^h x = x$.

- Veamos que es sobreyectiva. Sea $y \in \operatorname{Orb}(x)$, luego existe $g \in G$ tal que $y = {}^g x$. Por tanto:

$$\varphi(g \operatorname{Stab}_G(x)) = {}^g x = y.$$

- Veamos que es inyectiva. Sea $g_1 \operatorname{Stab}_G(x), g_2 \operatorname{Stab}_G(x) \in G/_{\operatorname{Stab}_G(x)}\sim$ tales que:

$$\varphi(g_1 \operatorname{Stab}_G(x)) = \varphi(g_2 \operatorname{Stab}_G(x)) \Longrightarrow {}^{g_1}x = {}^{g_2}x$$

  Veamos que $g_1 \operatorname{Stab}_G(x) = g_2 \operatorname{Stab}_G(x)$:

$${}^{g_1^{-1}g_2}x = {}^{g_1^{-1}}({}^{g_2}x) = {}^{g_1^{-1}}({}^{g_1}x) = {}^{g_1^{-1}g_1}x = {}^1x = x \Longrightarrow g_1^{-1}g_2 \in \operatorname{Stab}_G(x)$$

  Por tanto, $g_1 \operatorname{Stab}_G(x) = g_2 \operatorname{Stab}_G(x)$, luego φ es inyectiva.

Por tanto, φ es un biyectiva. Hasta aquí, notemos que no hemos empleado que G sea finito. En tal caso, empleando la definición de índice, tenemos que:

$$|\operatorname{Orb}(x)| = |G/_{\operatorname{Stab}_G(x)}\sim| = [G : \operatorname{Stab}_G(x)].$$

□

De esta forma, la fórmula de clases queda como sigue:

$$|X| = |\operatorname{Fix}(X)| + \sum_{x\in\Gamma'}[G : \operatorname{Stab}_G(x)].$$

Para llegar a la fórmula de clases mencionada en el enunciado, se emplea una acción en concreto, la acción de G sobre sí mismo por conjugación.

Proposición 1.9 (Acción por Conjugación)**.** *Sea G un grupo. Entonces, G actúa sobre sí mismo por conjugación de la forma siguiente:*

$$\begin{array}{rccl} ac: & G \times G & \longrightarrow & G \\ & (g,x) & \longmapsto & {}^g x = gxg^{-1} \end{array}$$

Calculemos los subconjuntos que aparecen en la fórmula de clases:

$$\begin{aligned} \operatorname{Fix}(G) &= \{x \in G \mid gxg^{-1} = x \quad \forall g \in G\} = \{x \in G \mid gx = xg \quad \forall g \in G\} =: Z(G) \\ \operatorname{Stab}_G(x) &= \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} =: C_G(x) \qquad \forall x \in G. \end{aligned}$$

Por tanto, la fórmula de clases buscada es (suponiendo que G es finito):

$$|G| = |Z(G)| + \sum_{x\in\Gamma'}[G : C_G(x)].$$

Ejercicio 4. Demuestra el Teorema de Cauchy (Si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p). Concluye que, si G es finito, entonces G es un $p-$grupo si y solo si su orden es una potencia de p.

Teorema 1.10 (de Cauchy)**.** *Sea G un grupo finito y p un primo que divide a $|G|$. Entonces, G tiene un elemento de orden p.*

Demostración. Consideramos el siguiente conjunto:

$$X = \{(a_1, \dots, a_p) \in G^p \mid a_1 a_2 \cdots a_p = 1\}.$$

Sea ahora $\sigma = (1\ 2\ \dots\ p) \in S_p$, y consideramos el siguiente grupo:

$$H = \langle \sigma \rangle = \{\sigma^k \mid k = 0, \dots, p-1\} < S_p.$$

Consideramos ahora la acción de H sobre X dada por:

$$\begin{array}{rrcl} ac: & H \times X & \longrightarrow & X \\ & (\sigma^k, (a_1, \dots, a_p)) & \longmapsto & {}^{\sigma^k}(a_1, \dots, a_p) = \left(a_{\sigma^k(1)}, \dots, a_{\sigma^k(p)}\right) \end{array}$$

- Para cada $(a_1, \dots, a_p) \in X$, tenemos que:
$$^{1}(a_1, \dots, a_p) = (a_1, \dots, a_p)$$

- Para cada $k, l \in \{0, \dots, p-1\}$, tenemos que:
$$\begin{aligned} {}^{\sigma^k}\left({}^{\sigma^l}(a_1, \dots, a_p)\right) &= {}^{\sigma^k}\left(a_{\sigma^l(1)}, \dots, a_{\sigma^l(p)}\right) = \left(a_{\sigma^k(\sigma^l(1))}, \dots, a_{\sigma^k(\sigma^l(p))}\right) \\ &= \left(a_{\sigma^{k+l}(1)}, \dots, a_{\sigma^{k+l}(p)}\right) = {}^{\sigma^{k+l}}(a_1, \dots, a_p) = {}^{\sigma^k \sigma^l}(a_1, \dots, a_p). \end{aligned}$$

Queremos trabajar con las órbitas de la acción de H sobre X. En primer lugar, para cada $(a_1, \dots, a_p) \in X$, tenemos que:

$$\begin{aligned} |\operatorname{Orb}((a_1, \dots, a_p))| = [H : \operatorname{Stab}_H((a_1, \dots, a_p))] &\Longrightarrow |\operatorname{Orb}((a_1, \dots, a_p))| \mid |H| = p \Longrightarrow \\ &\Longrightarrow |\operatorname{Orb}((a_1, \dots, a_p))| \in \{1, p\} \end{aligned}$$

Veamos cómo son las órbitas de la acción de H sobre X. Sea $(a_1, \dots, a_p) \in X$. Entonces:

$$\begin{aligned} \operatorname{Orb}((a_1, \dots, a_p)) &= \left\{{}^{\sigma^k}(a_1, \dots, a_p) \mid k = 0, \dots, p-1\right\} \\ &= \left\{(a_1, \dots, a_p), (a_2, a_3, \dots, a_p, a_1), \dots, (a_p, a_1, a_2, \dots, a_{p-1})\right\}. \end{aligned}$$

Por tanto, la órbita será unitaria si y solo si $a_1 = a_2 = \ldots = a_p$, en cuyo caso será de la forma $(a, a, \dots, a) \in X$, luego $a^p = 1$. Sabemos que al menos hay una órbita unitaria, pues $(1, 1, \dots, 1) \in X$. Queremos encontrar más. En vistas de aplicar la fórmula de clases, sea $r = |\operatorname{Fix}(X)|$ el número de órbitas unitarias de la acción de H sobre X y sea Γ el conjunto formado por un único representante de cada órbita no unitaria (de orden p) de la acción de H sobre X. Entonces, por la fórmula de clases, tenemos que:

$$|X| = |\operatorname{Fix}(X)| + \sum_{x \in \Gamma} |\operatorname{Orb}(x)| = r + |\Gamma| p.$$

Por otro lado, razonemos el cardinal de X. Las primeras $p-1$ componentes de un elemento de X pueden ser elegidas de forma arbitraria, mientras que la última queda determinada por las anteriores como:

$$a_p = (a_1 a_2 \cdots a_{p-1})^{-1}.$$

Por tanto, tenemos que:
$$|X| = |G|^{p-1}.$$

Uniendo ambas formas de calcular el cardinal de X, tenemos que:

$$|X| = |G|^{p-1} = r + |\Gamma|p \Longrightarrow r = |G|^{p-1} - |\Gamma|p.$$

Por hipótesis, $p \mid |G|$, luego $p \mid r$. Como p es primo ($p > 1$), tenemos que $r > 1$. Por tanto, $\exists a \in G$ tal que:

$$(1, 1, \dots, 1) \neq (a, a, \dots, a) \in X.$$

Por tanto, $a \neq 1$ verifica que $a^p = 1$, luego $\operatorname{ord}(a) \mid p$. Como p es primo y $a \neq 1$, tenemos que $\operatorname{ord}(a) = p$. Por tanto, tenemos lo pedido. □

Corolario 1.10.1. *Sea G un grupo finito y p un número primo. Entonces, G es un $p-$grupo si y solo si $|G|$ es una potencia de p.*

Demostración.

$\Longrightarrow$) Sea q un primo que divide a $|G|$. Por el Teorema de Cauchy, $\exists g \in G$ tal que $\operatorname{ord}(g) = q$. Como G es un $p-$grupo, tenemos que $\exists k \in \mathbb{N}$ tal que $q = p^k$, pero como p y q son primos, tenemos que $p = q$ y $k = 1$.

Por tanto, tenemos que el único primo que divide a $|G|$ es p, y considerando la descomposición en factores primos de $|G|$, tenemos que $\exists n \in \mathbb{N}$ tal que:

$$|G| = p^n.$$

$\Longleftarrow$) Sea $|G| = p^n$ para algún $n \in \mathbb{N}$. Como el orden de todo elemento de G divide a $|G|$, tenemos que, para todo $g \in G$, $\operatorname{ord}(g) \mid p^n$, luego $\operatorname{ord}(g) = p^k$ para algún $k \in \{0, \dots, n\}$. Por tanto, G es un $p-$grupo.

□

Ejercicio 5. Demuestra el Teorema de Burnside (el centro de un $p-$grupo finito es no trivial) y concluye, como consecuencia, que todo grupo de orden p^2 es abeliano. Clasifica entonces, salvo isomorfismo, todos los grupos de órdenes 4, 9 y 841.

Teorema 1.11 (de Burnside)**.** *Sea G un $p-$grupo finito. Entonces, $Z(G) \neq \{1\}$.*

Demostración. Sea G un $p-$grupo finito.

- Aunque no sería necesario, distinguimos el caso de G abeliano. En tal caso, $Z(G) = G$, luego $Z(G) \neq \{1\}$. Esto nos permite centrarnos en el caso de G no abeliano, y por tanto la acción de G sobre sí mismo por conjugación no es trivial.

Consideramos la fórmula de clases de la acción de G sobre sí mismo por conjugación. Sea $\Gamma \subset G \setminus Z(G)$ el conjunto formado por un único representante de cada órbita no unitaria. Entonces, tenemos que:

$$|G| = |Z(G)| + \sum_{x\in\Gamma}[G : C_G(x)].$$

Como G es un $p-$grupo finito, tenemos que $|G| = p^n$ para algún $n \in \mathbb{N}$. Por otro lado, como como G es finito, para cada $x \in \Gamma$ se tiene que $[G : C_G(x)]$ divide a $|G| = p^n$, luego $\exists k_x \in \{0, 1, \dots, n\}$ tal que:

$$[G : C_G(x)] = p^{k_x}$$

- Si $\exists x \in \Gamma$ tal que $k_x = 0$, entonces $|G| = |C_G(x)|$ y $C_G(x) = G$, luego $x \in Z(G)$, lo cual contradice que $x \in \Gamma \subset G \setminus Z(G)$.

Por tanto, tenemos que $k_x \in \{1, \dots, n\}$ para todo $x \in \Gamma$. Por tanto, despejando de la fórmula de clases, tenemos que:

$$|Z(G)| = |G| - \sum_{x\in\Gamma}[G : C_G(x)] = p^n - \sum_{x\in\Gamma} p^{k_x}$$

Como $k_x > 0$ para todo $x \in \Gamma$, el sumatorio es múltiplo de p, y por tanto $p \mid |Z(G)|$, de donde $|Z(G)| \geqslant p$. En particular, tenemos que $Z(G)$ no es trivial. □

Lema 1.12. *Sea G un grupo. Si $G/Z(G)$ es cíclico, entonces G es abeliano.*

Demostración. Supuesto que $G/Z(G)$ es cíclico, $\exists gZ(G) \in G/Z(G)$ tal que:

$$G/Z(G) = \langle gZ(G)\rangle.$$

Como las clases de equivalencia del cociente $G/Z(G)$ forman una partición de G, para cada $x \in G$ $\exists k \in \mathbb{Z}$ tal que:

$$x \in g^k Z(G).$$

En vistas de demostrar que G es abeliano, sean $a, b \in G$. Entonces, $\exists k_1, k_2 \in \mathbb{Z}$ tales que:

$$a \in g^{k_1} Z(G)$$
$$b \in g^{k_2} Z(G).$$

Por tanto, $\exists z_a, z_b \in Z(G)$ tales que:

$$a = g^{k_1} z_a$$
$$b = g^{k_2} z_b.$$

Entonces, puesto que $z_a, z_b \in Z(G)$:

$$ab = g^{k_1} z_a g^{k_2} z_b = g^{k_1+k_2} z_a z_b = g^{k_2} z_b g^{k_1} z_a = ba,$$

Puesto que a y b son arbitrarios, tenemos que G es abeliano. □

Corolario 1.12.1. *Sea G un $p-$grupo finito con $|G| = p^n$ para algún $n \in \mathbb{N}$. Entonces:*

$$|Z(G)| \neq p^{n-1}.$$

Demostración. Supongamos que $|Z(G)| = p^{n-1}$. Como $Z(G) \lhd G$, considerando el cociente tenemos que:

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^n}{|p^{n-1}|} = p.$$

Por tanto, $G/Z(G)$ es un grupo de orden primo, luego es cíclico. Como $G/Z(G)$ es cíclico, por el lema anterior G es abeliano, luego $Z(G) = G$ y $|Z(G)| = |G| = p^n$, lo cual contradice la hipótesis de que $|Z(G)| = p^{n-1}$. □

Sea ahora p un primo, y G un $p-$grupo finito con $|G| = p^2$. Como $Z(G) < G$ y el orden de todo subgrupo de G divide a $|G|$, tenemos que $|Z(G)| \in \{1, p, p^2\}$:

- Si $|Z(G)| = 1$, entonces $Z(G) = \{1\}$, en contradicción con el Teorema de Burnside.
- Si $|Z(G)| = p$, entonces $Z(G) = p^{2-1}$, en contradicción con el Corolario anterior.

Por tanto, $|Z(G)| = p^2$, luego $Z(G) = G$ y G es abeliano.

Clasificamos ahora los grupos de órdenes 4, 9 y 841 haciendo uso de que:

$$4 = 2^2 \qquad 9 = 3^2 \qquad 841 = 29^2.$$

Por el corolario anterior, todo grupo de dichos órdenes es abeliano (y es finito), luego empleamos el Teorema de Estructura de los Grupos Abelianos Finitos. Como el número 2 tan solo tiene dos particiones:

$$\begin{array}{rcl} 2 & = & 2 \\ 2 & = & 1+1 \end{array}$$

Entonces, podemos afirmar lo que sigue:

- Los grupos de orden 4 salvo isomorfismo son:
$$\mathbb{Z}_4 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$
- Los grupos de orden 9 salvo isomorfismo son:
$$\mathbb{Z}_9 \qquad \mathbb{Z}_3 \oplus \mathbb{Z}_3.$$
- Los grupos de orden 841 salvo isomorfismo son:
$$\mathbb{Z}_{841} \qquad \mathbb{Z}_{29} \oplus \mathbb{Z}_{29}$$

Ejercicio 6. (Teoremas de Sylow) Demuestra que, si G es un grupo finito, para cualquier potencia de un primo p que divida al orden del grupo existe un subgrupo cuyo orden es esa potencia de p. Define entonces el concepto de $p-$subgrupo de Sylow de un grupo finito G y concluye la existencia de $p-$subgrupos de Sylow de G.

Teorema 1.13. *Sea G un grupo finito y p un primo. Entonces, para todo $k \in \mathbb{N}$ tal que $p^k \mid |G|$, existe un subgrupo $H < G$ tal que $|H| = p^k$.*

Demostración. Demostramos por inducción sobre k.

- Para $k = 1$:

  Por el Teorema de Cauchy, $\exists g \in G$ tal que $\text{ord}(g) = p$. Entonces, el subgrupo $H = \langle g \rangle$ es un subgrupo de G de orden p.

- Para $k \in \mathbb{N}$, $k > 1$: Suponemos el resultado cierto para todo $l < k$. Esto es:

$$p^l \mid |G| \Longrightarrow \exists H < G : |H| = p^l \qquad \forall l < k.$$

  Demostrémoslo para k. Como $p^k \mid |G|$, $\exists n \in \mathbb{N}$ tal que:

$$|G| = p^k n$$

  Demostramos ahora el resultado para todo $n \in \mathbb{N}$ por inducción.

  - Para $n = 1$:
    Entonces, $|G| = p^k$, luego sea $H = G$. Entonces, $|H| = p^k$, luego el resultado es cierto.
  - Para $n \in \mathbb{N}$, $n > 1$:
    Suponemos el resultado cierto para todo $m < n$. Esto es:

$$|G| = p^k m \Longrightarrow \exists H < G : |H| = p^k \qquad \forall m < n.$$

    Veamos qué ocurre si $|G| = p^k n$. Distinguimos dos casos:

    - Si $\exists K < G$, $K \neq G$, tal que $p \nmid [G : K]$.
      En tal caso, como $|G| = [G : K]|K|$, y $p^k \mid |G|$, tenemos que:

$$p^k \mid |K| \Longrightarrow \exists s \in \mathbb{N} \text{ tal que } |K| = p^k s.$$

      Además, puesto que $K \neq G$, entonces $s < n$, luego por la segunda hipótesis de inducción, tenemos que:

$$\exists H < K < G : |H| = p^k.$$

    - Si para todo $K < G$, $K \neq G$, se tiene que $p \mid [G : K]$.
      Con vistas a aplicar la fórmula de clases de la acción de G sobre sí mismo por conjugación, definimos Γ como el conjunto formado por un único representante de cada órbita no unitaria de la acción de G sobre sí mismo por conjugación. Para cada $x \in \Gamma$, tenemos que:

$$x \in \Gamma \Longrightarrow x \notin Z(G) \Longrightarrow C_G(x) \neq G \Longrightarrow p \mid [G : C_G(x)].$$

Por tanto, por la fórmula de clases, tenemos que:

$$|G| = |Z(G)| + \sum_{x\in\Gamma}[G : C_G(x)] \Longrightarrow |Z(G)| = |G| - \sum_{x\in\Gamma}[G : C_G(x)].$$

Como $p \mid |G|$ y $p \mid [G : C_G(x)]$ para todo $x \in \Gamma$, tenemos que:

$$p \mid |Z(G)|$$

Por el Teorema de Cauchy, $\exists K < Z(G)$ tal que $|K| = p$. Como $K \subset Z(G)$, tenemos que $K \lhd G$, por lo que podemos considerar el cociente G/K. Entonces, tenemos que:

$$|G/K| = \frac{|G|}{|K|} = \frac{p^k n}{p} = p^{k-1}n.$$

Por tanto, $p^{k-1} \mid |G/K|$, luego por la primera hipótesis de inducción, tenemos que:

$$\exists L < G/K : |L| = p^{k-1}.$$

Por el Tercer Teorema de Isomorfía, considerando $H = p^*(L)$, tenemos que $K \lhd H < G$, con:

$$L = \frac{H}{K} \Longrightarrow |H| = |L||K| = p^{k-1}p = p^k.$$

Por tanto, hemos encontrado un subgrupo $H < G$ tal que $|H| = p^k$.

□

Una vez dado dicho teorema, definimos el concepto de $p-$subgrupo de Sylow de un grupo finito G.

Definición 1.12 ($p-$subgrupo de Sylow)**.** Sea G un grupo finito y p un primo. Un $p-$subgrupo de Sylow de G es un $p-$subgrupo de G cuyo orden es la mayor potencia de p que divide a $|G|$. Es decir, si $|G| = p^k m$ con $\text{mcd}(p, m) = 1$, entonces un $p-$subgrupo $H < G$ es un $p-$subgrupo de Sylow de G si $|H| = p^k$.

El siguiente corolario, consecuencia directa del Teorema anterior, nos garantiza la existencia de $p-$subgrupos de Sylow en un grupo finito G.

Corolario 1.13.1. *Sea G un grupo finito y p un primo tal que $p \mid |G|$. Entonces, G tiene un $p-$subgrupo de Sylow.*

Demostración. Como $p \mid |G|$, tenemos que $\exists k, m \in \mathbb{N}$ tales que:

$$|G| = p^k m \quad \text{con } \text{mcd}(p, m) = 1.$$

Por el Teorema anterior, como $p^k \mid |G|$, tenemos que:

$$\exists H < G : |H| = p^k.$$

Por tanto, H es un $p-$subgrupo de G. Además, como p^k es la mayor potencia de p que divide a $|G|$, tenemos que H es un $p-$subgrupo de Sylow de G. □

Ejercicio 7. (Teoremas de Sylow) Demuestra que todo $p-$subgrupo de un grupo finito G (con $|G| = p^k m$ y $\text{mcd}(p, m) = 1$) está contenido en un $p-$subgrupo de Sylow y que el número n_p de $p-$subgrupos de Sylow de G satisface que $n_p \mid m$ y que $n_p \equiv 1 \mod p$.

Lema 1.14. *Sea G un grupo finito y $P < G$ un $p-$subgrupo de Sylow de G. Si $H < N_G(P)$ es un $p-$subgrupo de $N_G(P)$, entonces $H \subset P$. Es decir, los $p-$subgrupos del normalizador de un $p-$subgrupo de Sylow estarán contenidos en el propio $p-$subgrupo de Sylow.*

Demostración. Como $P \lhd N_G(P)$, y $H < N_G(P)$, aplicamos el Segundo Teorema de Isomorfía como muestra la Figura 1.2.

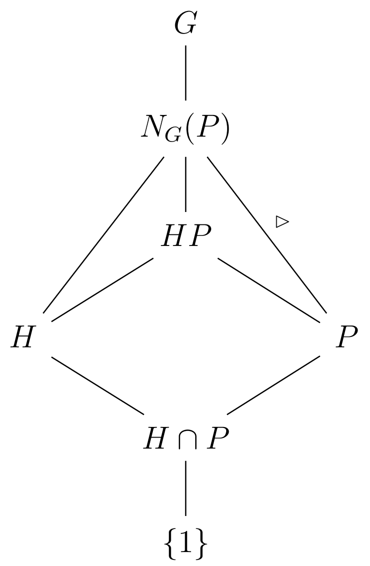


Figura 1.2: Segundo Teorema de Isomorfía

De esta forma, obtenemos:

- $HP < N_G(P)$.
- $H \cap P \lhd H$, $P \lhd HP$.
- El siguiente isomorfismo:
$$\frac{H}{H \cap P} \cong \frac{HP}{P}.$$

Gracias a dicho isomorfismo, definimos:

$$r = [H : H \cap P] = [HP : P] \geqslant 1.$$

Distinguimos dos casos:

- Si $r = 1$, entonces $HP = P$, luego $H \subset P$.

- Si $r > 1$, tenemos que:

$$P < HP < G \Longrightarrow [G : P] = [G : HP][HP : P] = [G : HP]r.$$

Supuesto que $p \mid r$, entonces $p \mid [G : P]$. No obstante, esto contradice que P es un $p-$subgrupo de Sylow de G, luego hemos llegado a una contradicción. Por tanto, $p \nmid r$.

Por otro lado, como la intersección de $p-$grupos es un $p-$grupo (basta ver la definición de $p-$grupo) y $r > 1$, tenemos que $\exists i \in \mathbb{N}$, $i > 0$, tal que:

$$r = [H : H \cap P] = \left|\frac{H}{H \cap P}\right| = p^i \Longrightarrow p \mid r.$$

Por tanto, hemos demostrado que $p \mid r$ y $p \nmid r$, lo cual es una contradicción. Por tanto, este caso no puede ocurrir.

Por tanto, concluimos que $H \subset P$. $\square$

Buscamos ahora demostrar en sí el Segundo Teorema de Sylow.

Teorema 1.15 (Segundo Teorema de Sylow)**.**

Sea G un grupo finito y p un número primo. Supongamos que $|G| = p^k m$ con $\mathrm{mcd}(p, m) = 1$. Sea además n_p el número de $p-$subgrupos de Sylow de G. Entonces:

1. *Todo $p-$subgrupo de G está contenido en un $p-$subgrupo de Sylow de G.*
2. *Cualesquiera dos $p-$subgrupos de Sylow de G son conjugados entre sí.*
3. *$n_p \mid m$ y $n_p \equiv 1 \mod p$.*

Demostración. Demostramos cada resultado por separado:

1. Previa a la demostración en si, veamos un resultado que nos será de ayuda. Definimos la acción de G sobre $\mathrm{Syl}_p(G)$ por conjugación:

$$\begin{array}{rccc} ac: & G \times \mathrm{Syl}_p(G) & \longrightarrow & \mathrm{Syl}_p(G) \\ & (g, P) & \longmapsto & gPg^{-1} \end{array}$$

Veamos que está bien definida. Es necesario ver que, fijado $g \in G,\ P \in \mathrm{Syl}_p(G)$, se tiene que $gPg^{-1} \in \mathrm{Syl}_p(G)$. Veamos que la siguiente aplicación es biyectiva:

$$\begin{array}{rccc} f: & P & \longrightarrow & gPg^{-1} \\ & p & \longmapsto & gpg^{-1} \end{array}$$

- Si $\widetilde{x} \in gPg^{-1}$, entonces $\exists p \in P$ tal que $\widetilde{x} = gpg^{-1}$. De esta forma:

$$f(p) = gpg^{-1} = \widetilde{x}$$

Por tanto, f es sobreyectiva.

- Dados $p_1, p_2 \in P$, si $f(p_1) = f(p_2)$, entonces:

$$gp_1g^{-1} = gp_2g^{-1} \Longrightarrow p_1 = p_2,$$

  luego f es inyectiva.

Por tanto, f es biyectiva, luego $|P| = |gPg^{-1}|$, y como $P \in \mathrm{Syl}_p(G)$, tenemos que $gPg^{-1} \in \mathrm{Syl}_p(G)$, luego la acción de G sobre $\mathrm{Syl}_p(G)$ por conjugación está bien definida.

Fijamos ahora para toda la demostración $P_1 \in \mathrm{Syl}_p(G)$, y estudiamos su órbita y su estabilizador:

$$\begin{aligned} \mathrm{Orb}(P_1) &= \{gP_1g^{-1} \mid g \in G\} \\ \mathrm{Stab}_G(P_1) &= \{g \in G \mid gP_1g^{-1} = P_1\} = N_G(P_1). \end{aligned}$$

Como $P_1 \lhd N_G(P_1) < G$, por el Teorema de Lagrange, tenemos que:

$$[G : P_1] = [G : N_G(P_1)][N_G(P_1) : P_1]$$

Por un lado, como $P_1 \in \mathrm{Syl}_p(G)$, y $|G| = p^k m$ con $\mathrm{mcd}(p, m) = 1$, tenemos que $[G : P_1] = m$. Además, $[G : N_G(P_1)] = [G : \mathrm{Stab}_G(P_1)] = |\operatorname{Orb}(P_1)|$, luego:

$$m = |\operatorname{Orb}(P_1)|[N_G(P_1) : P_1]. \tag{1.3}$$

Por tanto:

$$1 = \mathrm{mcd}(p, m) = \mathrm{mcd}\left(p, |\operatorname{Orb}(P_1)|[N_G(P_1) : P_1]\right) \Longrightarrow \mathrm{mcd}\left(p, |\operatorname{Orb}(P_1)|\right) = 1$$

de donde deducimos que $p \nmid |\operatorname{Orb}(P_1)|$. Visto esto, podemos comenzar con la demostración en sí.

Sea H un $p-$subgrupo de G. Definimos la siguiente acción:

$$\begin{array}{rrcl} ac: & H \times \mathrm{Orb}(P_1) & \longrightarrow & \mathrm{Orb}(P_1) \\ & (h, P) & \longmapsto & hPh^{-1} \end{array}$$

Veamos que está bien definida. Sea $P \in \mathrm{Orb}(P_1)$, entonces $\exists g \in G$ tal que $P = gP_1g^{-1}$. Entonces, tenemos que:

$$hPh^{-1} = h(gP_1g^{-1})h^{-1} = hgP_1g^{-1}h^{-1} = (hg)P_1(hg)^{-1}.$$

Como $hg \in G$, tenemos que $hPh^{-1} \in \mathrm{Orb}(P_1)$, luego está bien definida. Para todo $P \in \mathrm{Orb}(P_1)$, tenemos:

$$\mathrm{Stab}_H(P) = \{h \in H \mid hPh^{-1} = P\} = \{h \in H \mid hP = Ph\} = H \cap N_G(P)$$

Por un lado, $H \cap N_G(P) < H$. Por otro lado, como $P \in \mathrm{Orb}(P_1) \subset \mathrm{Syl}_p(G)$ y $H \cap N_G(P) < N_G(P)$ es un $p-$subgrupo de $N_G(P)$, por el Lema anteriormente demostrado tenemos que $H \cap N_G(P) < P$. Por tanto, tenemos que:

$$\mathrm{Stab}_H(P) = H \cap N_G(P) < H \cap P$$

Como además $P < N_G(P)$, tenemos que:

$$\mathrm{Stab}_H(P) = H \cap N_G(P) = H \cap P$$

En vistas de aplicar la fórmula de clases, sea Γ el conjunto formado por un único representante de cada órbita de la acción de H sobre $\mathrm{Orb}(P_1)$. Entonces, tenemos que:

$$|\operatorname{Orb}(P_1)| = \sum_{P\in\Gamma} |\operatorname{Orb}(P)| = \sum_{P\in\Gamma} [H : \mathrm{Stab}_H(P)] = \sum_{P\in\Gamma} [H : H \cap P] \tag{1.4}$$

Tenemos que cada sumando divide a $|H|$, que como es un $p-$subgrupo, es una potencia de p. Como cada sumando divide a una potencia de p y, por lo demostrado al inicio de la demostración, $p \nmid |\operatorname{Orb}(P_1)|$, $\exists \widetilde{P} \in \Gamma$ tal que:

$$[H : H \cap \widetilde{P}] = 1 \Longrightarrow H \cap \widetilde{P} = H \Longrightarrow H < \widetilde{P}.$$

Como $\widetilde{P} \in \Gamma \subset \mathrm{Orb}(P_1) \subset \mathrm{Syl}_p(G)$, tenemos que H está contenido en un $p-$subgrupo de Sylow de G.

2. Sean $P_1, P_2 \in \mathrm{Syl}_p(G)$. Como P_2 es un $p-$subgrupo de G, por el apartado anterior, tenemos que P_2 está contenido en un $p-$subgrupo de Sylow de G, que llamaremos $\widetilde{P}$ por seguir la misma notación. Además, por la demostración anterior $\widetilde{P} \in \mathrm{Orb}(P_1)$, luego $\exists g \in G$ tal que:

   $$\widetilde{P} = gP_1g^{-1}.$$

   Por tanto, $P_2 < \widetilde{P}$ pero, por ser ambos $p-$subgrupos de Sylow de G, $|P_2| = |\widetilde{P}|$, luego:

   $$P_2 = \widetilde{P} = gP_1g^{-1}$$

   Por tanto, P_1 y P_2 son conjugados entre sí.

3. Sea n_p el número de $p-$subgrupos de Sylow de G. Por el apartado anterior, tenemos que $\mathrm{Orb}(P_1) = \mathrm{Syl}_p(G)$, luego:

   $$n_p = |\operatorname{Syl}_p(G)| = |\operatorname{Orb}(P_1)|$$

   Por la Ecuación (1.3), tenemos que $n_p \mid m$. Para ver que $n_p \equiv 1 \mod p$, empleamos la Ecuación (1.4) con $H = P_1$:

   $$n_p = |\operatorname{Orb}(P_1)| = \sum_{P\in\Gamma} [P_1 : P_1 \cap P]$$

   Tenemos que $[P_1 : P_1 \cap P]$ es una potencia de p para todo $P \in \Gamma$.

   - Si $[P_1 : P_1 \cap P] = 1$, entonces $P_1 \cap P = P_1$, luego $P_1 \subset P$. Como $P \in \mathrm{Syl}_p(G)$, tenemos que $P_1 = P$. Por tanto, P_1 es el único elemento de Γ tal que $[P_1 : P_1 \cap P] = 1$; el resto de sumandos son potencias de p mayores que 1.

   Por tanto:

   $$n_p = 1 + \sum_{P\in\Gamma, P\neq P_1} [P_1 : P_1 \cap P] \Longrightarrow p \mid n_p - 1 \Longrightarrow n_p \equiv 1 \mod p.$$

□

Ejercicio 8. Prueba que todos los grupos de orden $2p$ siendo p un primo impar y también todos los de orden pq siendo p, q primos con $p > q$ y $q \nmid p-1$ son producto semidirecto. Clasifica los grupos de estos órdenes y concluye entonces con la clasificación de todos los grupos de órdenes 6, 10, 14, 15, 161 y 1994.

Comenzamos con el caso de $2p$ siendo p un primo impar. Sea G un grupo de orden $2p$. Sea n_2 el número de 2−subgrupos de Sylow de G y n_p el número de p−subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, tenemos que:

$$n_p \mid 2 \quad \text{y} \quad n_p \equiv 1 \mod p.$$

Por tanto, tenemos que $n_p = 1$, sea este P. Puesto que P es el único p−subgrupo de Sylow de G, tenemos que $P \lhd G$. Además, puesto que $|P| = p$ primo, tenemos que $P \cong C_p$, luego tiene $p-1$ elementos de orden p.

Por otro lado, por el Primer Teorema de Sylow, tenemos que $n_2 \geqslant 1$. Sea $Q \in \mathrm{Syl}_2(G)$ un 2−subgrupo de Sylow de G. Como $|Q| = 2$, tenemos que $Q \cong C_2$.

Buscamos demostrar que $G \cong P \rtimes Q$ es un producto semidirecto.

- En primer lugar, $P \lhd G$.
- $Q \cap P = \{1\}$, pues todos los elementos distintos del neutro de P son de orden p y todos los elementos distintos del neutro de Q son de orden 2, luego no pueden coincidir.
- Por otro lado, como $P \lhd G$, aplicamos el Segundo Teorema de Isomorfía y obtenemos $PQ < G$ con:

$$\frac{PQ}{P} \cong \frac{Q}{P \cap Q} \Longrightarrow |PQ| = \frac{|Q| \cdot |P|}{|P \cap Q|} = \frac{2p}{1} = 2p.$$

  Como $|PQ| = |G|$, tenemos que $PQ = G$.

Por tanto, $G \cong P \rtimes_\theta Q$ es un producto semidirecto, donde θ es la representación de G por permutaciones haciendo uso de la acción de Q sobre P por conjugación. Es decir, tenemos que:

$$\begin{array}{rccc} \theta: & Q & \longrightarrow & \mathrm{Aut}(P) \\ & q & \longmapsto & \theta(q) \end{array}$$

$$\begin{array}{rccc} \theta(q): & P & \longrightarrow & P \\ & p & \longmapsto & qpq^{-1} \end{array}$$

Buscamos ahora otro enfoque para determinar que son producto semidirecto. Como $P \cong C_p$, tenemos que $\mathrm{Aut}(P) \cong C_{p-1}$. Por tanto:

$$\begin{aligned} P \cong C_p &\Longrightarrow \exists x_p \in P \text{ tal que } P = \langle x_p \mid x_p^p = 1\rangle \\ Q \cong C_2 &\Longrightarrow \exists x_q \in Q \text{ tal que } Q = \langle x_q \mid x_q^2 = 1\rangle \\ \mathrm{Aut}(P) \cong C_{p-1} &\Longrightarrow \exists \widetilde{x}_p \in \mathrm{Aut}(P) \text{ tal que } \mathrm{Aut}(P) = \langle \widetilde{x}_p \mid \widetilde{x}_p^{p-1} = 1\rangle. \end{aligned}$$

Buscamos ahora los elementos de $\mathrm{Aut}(P)$. Como $P = \langle x_p \rangle$, por el Teorema de Dyck tenemos que los posibles isomorfismos son los que lleven x_p a un generador de

P (que como P es cíclico, son todos los elementos de orden p). Por tanto, estos son los siguientes:

$$\begin{aligned}
x_p &\mapsto \alpha_1(x_p) = x_p \\
x_p &\mapsto \alpha_2(x_p) = x_p^2 \\
&\vdots \\
x_p &\mapsto \alpha_{p-1}(x_p) = x_p^{p-1}.
\end{aligned}$$

De todos estos, tan solo buscamos quedarnos con los que nos son válidos. Como θ es un homomorfismo y $O(x_q) = 2$, tenemos que $O(\theta(x_q)) \mid 2$, luego $\operatorname{ord}(\theta(x_q)) \in \{1, 2\}$.

- Sea $\operatorname{ord}(\theta(x_q)) = 1$. Entonces $\theta(x_q) = Id_P$, luego θ es el homomorfismo trivial, y por tanto $G \cong P \times Q \cong C_p \times C_2 \cong C_{2p}$.
- Sea $\operatorname{ord}(\theta(x_q)) = 2$. Buscamos por tanto los elementos de $\operatorname{Aut}(P)$ de orden 2. Como en C_{p-1} tan solo hay un elemento de orden 2 $\left(\widetilde{x}_p^{\frac{p-1}{2}}\right)$ (donde usamos que p es primo impar), entonces tenemos que tan solo hay una elección posible para $\theta(x_q)$. Esta es la siguiente:

  $$\begin{array}{rccc}
  \alpha: & P & \longrightarrow & P \\
  & x & \longmapsto & x^{-1}
  \end{array}$$

  Como $\alpha = \alpha_{p-1}$, es un homomorfismo. Como esta elección es única, uniendo con el homomorfismo por conjugación anteriormente encontrado, tenemos que:

  $$qpq^{-1} = \theta(q)(p) = p^{-1} \Longrightarrow qp = p^{-1}q \qquad \forall p \in P,\ q \in Q.$$

  Buscamos establecer ahora un isomorfismo entre D_p y G. Vemos que:

  $$\begin{gathered}
  x_p^p = 1 \qquad x_q^2 = 1 \\
  x_q x_p = x_p^{-1} x_q \quad (x_q \in Q,\ x_p \in P).
  \end{gathered}$$

  Por tanto, por el Teorema de Dyck, existe un homomorfismo entre D_p y G. Como además $G = PQ = \langle x_p, x_q \rangle$ y $|G| = 2p = |D_p|$, tenemos que se trata de un isomorfismo. Por tanto, tenemos que:

  $$G \cong D_p.$$

Visto esto, podemos realizar las siguientes clasificaciones:

- Los grupos de orden $6 = 2 \cdot 3$ son C_6 y D_3.
- Los grupos de orden $10 = 2 \cdot 5$ son C_{10} y D_5.
- Los grupos de orden $14 = 2 \cdot 7$ son C_{14} y D_7.
- Los grupos de orden $1994 = 2 \cdot 997$ son C_{1994} y D_{997}.

Ahora, consideramos el caso de $|G| = pq$ siendo p, q primos con $p > q$ y $q \nmid p-1$. Sea n_p el número de $p-$subgrupos de Sylow de G y n_q el número de $q-$subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, tenemos que:

$$n_p \mid q \quad \text{y} \quad n_p \equiv 1 \mod p.$$

Como $n_p \leqslant q < p$, entonces $n_p = 1$, luego sea P el único $p-$subgrupo de Sylow de G. Como P es el único $p-$subgrupo de Sylow de G, tenemos que $P \lhd G$. Además, puesto que $|P| = p$ primo, tenemos que $P \cong C_p$.

Por otro lado, por el Segundo Teorema de Sylow, tenemos que:

$$n_q \mid p \quad \text{y} \quad n_q \equiv 1 \mod q.$$

Por tanto, como $n_q \mid p$, tenemos que $n_q \in \{1, p\}$.

- Si $n_q = p$, entonces:

  $$p \equiv 1 \mod q \Longrightarrow \exists k \in \mathbb{N} \text{ tal que } p - 1 = kq \Longrightarrow q \mid p - 1.$$

  No obstante, esto contradice la hipótesis de que $q \nmid p - 1$. Por tanto, este caso no puede ocurrir.

Por tanto, tenemos que $n_q = 1$, sea Q el único $q-$subgrupo de Sylow de G. Como Q es el único $q-$subgrupo de Sylow de G, tenemos que $Q \lhd G$. Además, puesto que $|Q| = q$ primo, tenemos que $Q \cong C_q$.

Como todos los subgrupos de Sylow de G son únicos, tenemos que:

$$G \cong P \times Q \cong C_p \times C_q \cong C_{pq}.$$

Por tanto, $G \cong C_{pq}$. Ya podemos realizar las siguientes clasificaciones:

- El único grupo de orden $15 = 3 \cdot 5$ $(3 \nmid 4)$ es C_{15}.
- El único grupo de orden $161 = 7 \cdot 23$ $(7 \nmid 22)$ es C_{161}.

Ejercicio 9. Clasifica, salvo isomorfismo, todos los grupos de orden 8.

Sea G un grupo de orden $8 = 2^3$. Si G es abeliano, entonces por el Teorema de Estructura de los Grupos Abelianos Finitos, están las siguientes posibilidades:

$$C_8 \qquad C_4 \oplus C_2 \qquad C_2 \oplus C_2 \oplus C_2.$$

Supongamos de aquí en adelante que G no es abeliano. Como $|G| = 8$, todos los elementos distintos del neutro de G son de orden $2, 4$ u 8. Como G no es abeliano, en particular no es cíclico, luego no puede haber un elemento de orden 8. Por tanto, todos los elementos distintos del neutro de G son de orden 2 o 4.

Supongamos que todos los elementos distintos del neutro de G son de orden 2. Dados $a, b \in G$, como $a, b \in G$, tenemos que:

$$1 = (ab)^2 = abab \Longrightarrow a = bab \Longrightarrow ab = ba.$$

Por tanto, G es abeliano, lo cual contradice el caso en el que estamos. Por tanto, no todos los elementos distintos del neutro de G son de orden 2, luego $\exists a \in G$ tal que $\operatorname{ord}(a) = 4$. Sea ahora $b \in G \setminus \langle a \rangle$. Veamos que $G = \langle a, b \rangle$:

- Como G es un grupo, entonces $\langle a, b \rangle \subset G$. Además, como $b \notin \langle a \rangle$, tenemos que $|\langle a, b \rangle| > |\langle a \rangle| = 4$. Como $|G| = 8$, tenemos que $|\langle a, b \rangle| = 8$, luego $G = \langle a, b \rangle$.

Por tanto, tenemos que $G = \langle a, b \rangle$ con $\operatorname{ord}(a) = 4$ y $b \notin \langle a \rangle$.

- Como $\langle a \rangle \lhd G$ por ser $[G : \langle a \rangle] = 2$, tenemos que $bab^{-1} \in \langle a \rangle$. Además, como el orden se mantiene invariante por conjugación, tenemos que:

  $$\operatorname{ord}(bab^{-1}) = \operatorname{ord}(a) = 4.$$

  Por tanto, $bab^{-1} \in \{a, a^3\}$. Veamos qué ocurre en cada caso:

  - Si $bab^{-1} = a$, entonces $ab = ba$, y como $G = \langle a, b \rangle$, tenemos que G es abeliano, lo cual contradice el supuesto inicial.

  Por tanto, tenemos que $bab^{-1} = a^3 = a^{-1}$.

Por comodidad, notemos $H = \langle a \rangle$. Sea ahora b^2, y veamos si $b^2 \in Hb$:

$$b^2 \in Hb \Longrightarrow b^2 = a^i b \Longrightarrow b = a^i \qquad i \in \{0, 1, 2, 3\}.$$

En cualquiera de los casos, llegamos a $b \in H$, lo cual contradice que $b \in G \setminus H$. Por tanto, tenemos que $b^2 \notin Hb$, luego $b^2 \in H$. Estudiemos en función del valor de b^2:

- Si $b^2 = a$, entonces $O(b) = 2 \cdot O(a) = 8$, lo que es una contradicción.
- Si $b^2 = a^3$, entonces $O(b) = 2 \cdot O(a^3) = 2 \cdot 4 = 8$, lo que es una contradicción.
- Supongamos $b^2 = 1$. En este caso:

  $$a^4 = 1 \qquad b^2 = 1 \qquad bab^{-1} = a^{-1}.$$

  Por tanto, por el Teorema de Dyck, tenemos que $G \cong D_4$.

- Si $b^2 = a^2$, entonces:

$$a^4 = 1 \qquad b^2 = a^2 \qquad bab^{-1} = a^{-1}.$$

  Por tanto, por el Teorema de Dyck, tenemos que $G \cong Q_2$.

Por tanto, los grupos de orden 8 no abelianos son:

$$D_4 \qquad Q_2.$$

Resumiendo, los grupos de orden 8 son:

$$C_8 \qquad C_4 \oplus C_2 \qquad C_2 \oplus C_2 \oplus C_2 \qquad D_4 \qquad Q_2.$$

Ejercicio 10. Prueba que todo grupo de orden 12 es un producto semidirecto y clasifica, salvo isomorfismo, todos los grupos de orden 12 identificándolos con productos semidirectos.

Sea G un grupo de orden $12 = 2^2 \cdot 3$. Sea n_2 el número de $2-$subgrupos de Sylow de G y n_3 el número de $3-$subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, tenemos que:

$$n_2 \mid 3 \quad \text{y} \quad n_2 \equiv 1 \mod 2.$$

Por tanto, tenemos que $n_2 \in \{1, 3\}$. En cualquier caso, cada $2-$subgrupo de Sylow de G tiene tres elementos de orden 2 o 4.

De igual forma, tenemos que:

$$n_3 \mid 4 \quad \text{y} \quad n_3 \equiv 1 \mod 3.$$

Por tanto, tenemos que $n_3 \in \{1, 4\}$. En cualquier caso, cada $3-$subgrupo de Sylow de G tiene dos elementos de orden 3.

Veamos que el siguiente caso no puede darse:

- $\underline{n_3 = 4,\ n_2 = 3}$:

  Como $n_3 = 4$, tenemos que G tiene cuatro $3-$subgrupos de Sylow, cada uno de los cuales tiene dos elementos de orden 3. Además, tienen intersección trivial, puesto que si tuviesen algún elemento de orden 3 en común, entonces sería un generador de ambos $3-$subgrupos de Sylow, luego serían iguales. Por tanto, hay $4 \cdot 2 = 8$ elementos de orden 3 en G. Los 4 elementos de orden $1, 2$ y 4 restantes deben formar un $2-$subgrupo de Sylow de G, que sería único y por tanto $n_2 = 1$. No obstante, esto contradice que $n_2 = 3$. Por tanto, este caso no puede ocurrir.

Por tanto, dado $P_2 \in \mathrm{Syl}_2(G)$ y $P_3 \in \mathrm{Syl}_3(G)$, uno de ellos será único y, por tanto, normal en G. Como $|P_2| = 4$ y $|P_3| = 3$, razonando por órdenes vemos que $P_2 \cap P_2 = \{1\}$ y, por el Segundo Teoría de Isomorfía (puesto que uno de los subgrupos es normal), tenemos que $P_2P_3 < G$ con:

$$|P_2P_3| = \frac{|P_2| \cdot |P_3|}{|P_2 \cap P_3|} = \frac{4 \cdot 3}{1} = 12.$$

Por tanto, $P_2P_3 = G$ y, entonces, $G \cong P_i \rtimes P_j$ (donde P_i es el grupo normal) es un producto semidirecto.

Para la clasificación, distinguimos en función de los valores de n_2 y n_3:

1. $\underline{n_2 = 1,\ n_3 = 1}$:

   En este caso, tenemos que P_2 y P_3 son únicos, luego son normales en G. Por tanto, tenemos que:

$$G \cong P_2 \times P_3$$

Como $|P_2| = 4 = 2^2$, es abeliano, y como $P_3 \cong C_3$, también es abeliano. Por tanto, G es abeliano. Por el Teorema de Estructura de los Grupos Abelianos Finitos, tenemos que:

$$G \cong C_4 \oplus C_3 \cong C_{12} \quad \vee \quad G \cong C_2 \oplus C_2 \oplus C_3 \cong C_2 \oplus C_6.$$

2. $\underline{n_3 = 1,\ n_2 = 3}$:

   En este caso, tenemos que $P_3 \lhd G$ y P_2 no es normal en G. Como $G \cong P_3 \rtimes P_2$, buscamos los siguientes homomorfismos:

$$\begin{array}{rccc} \theta: & P_2 & \longrightarrow & \mathrm{Aut}(P_3) \\ & p & \longmapsto & \theta(p) \end{array}$$

   Como $P_3 \cong C_3$, $\exists x \in P_3$ tal que:

$$P_3 = \langle x \mid x^3 = 1 \rangle.$$

   Veamos en primer lugar cuántos elementos tiene $\mathrm{Aut}(P_3)$:

$$|\operatorname{Aut}(P_3)| = \varphi(3) = 2.$$

   Por tanto, tan solo tiene el isomorfismo identidad, y el isomorfismo $x \mapsto x^{-1}$, que llamaremos α. Como $|P_2| = 4$, hay dos opciones:

   - $P_2 \cong C_4$:

     Por tanto, $\exists y \in P_2$ tal que:

$$P_2 = \langle y \mid y^4 = 1 \rangle.$$

     Como hemos visto antes, tan solo hay dos homomorfismos posibles:

     - Si $\theta(y) = Id_{P_3}$, entonces $G \cong P_3 \times P_2$, luego G es abeliano y por tanto $n_2 = 1$, lo cual contradice el supuesto inicial.

     Por tanto, tenemos que:

$$\begin{aligned} yxy^{-1} &= \theta(y)(x) = x^{-1} \\ x^3 &= 1 \\ y^4 &= 1 \end{aligned}$$

     Como $G = \langle x, y \rangle$, por el Teorema de Dyck, tenemos que:

$$G \cong \langle x, y \mid x^3 = 1,\ y^4 = 1,\ yxy^{-1} = x^{-1} \rangle = Q_3$$

   - $P_2 \cong C_2 \oplus C_2$:

     En este caso, P_2 tiene dos generadores, sean $y, z \in P_2$ tales que:

$$P_2 = \langle y, z \mid y^2 = 1,\ z^2 = 1 \rangle.$$

Aunque hay tres homomorfismos no triviales, todos ellos dan a grupos isomorfos entre sí. Uno de ellos es:

$$\begin{aligned}
\theta(y) &= Id_{P_3} \\
\theta(z) &= \alpha.
\end{aligned}$$

Por tanto, tenemos que:

$$\begin{aligned}
yxy^{-1} &= \theta(y)(x) = x \\
zxz^{-1} &= \theta(z)(x) = x^{-1} \\
zyz^{-1} &= \theta(z)(y) = y^{-1} \\
y^2 &= 1 \\
z^2 &= 1
\end{aligned}$$

Tenemos que $G = \langle xy, yz \rangle$, y además:

$$\begin{aligned}
(xy)^6 &= x^6 y^6 = 1 \\
(yz)^2 &= y^2 z^2 = 1 \\
(xy)(yz) &= xz \\
(yz)(xy)^{-1} &= yzyx^2 = zx^2
\end{aligned}$$

Como $zx^2 = xz$, tenemos que cumple las relaciones de D_6. Como $|G| = |D_6| = 12$, por el Teorema de Dyck, tenemos que:

$$G \cong D_6.$$

3. $\underline{n_2 = 1,\ n_3 = 4}$:

   En este caso, tenemos que $P_2 \lhd G$ y P_3 no es normal en G. Como $G \cong P_2 \rtimes P_3$, buscamos los siguientes homomorfismos:

$$\begin{array}{rccc}
\theta: & P_3 & \longrightarrow & \mathrm{Aut}(P_2) \\
 & p & \longmapsto & \theta(p)
\end{array}$$

   En este caso, como $P_2 \cong C_4$, o $P_2 \cong C_2 \oplus C_2$, hay dos opciones:

   a) $G \cong C_4 \rtimes P_3$:
   El único automorfismo no trivial de C_4 es el que lleva $x \mapsto x^{-1}$, cuyo orden es 2. Por tanto, no puede ser la imagen de ningún elemento de P_3, luego no hay automorfismos no triviales. Este caso no se contempla por tanto.

   b) $G \cong C_2 \oplus C_2 \rtimes P_3$:
   Como $|G| = 12$ y $n_3 \geqslant 1$, sabemos que $G \cong A_4$.

Resumiendo, los grupos de orden 12 son:

$$C_{12} \qquad C_2 \oplus C_6 \qquad D_6 \qquad A_4 \qquad Q_3$$

2. Relaciones de Ejercicios

2.1. Combinatoria y Teoría de Grafos

Ejercicio 2.1.1. Diez personas están sentadas alrededor de una mesa circular. Cada persona estrecha la mano a todos los demás excepto a la persona sentada directamente enfrente de la mesa. Dibuja un grafo que modele la situación.

La situación se puede modelar con el grafo de la Figura 2.1.
Su matriz de adyacencia es:

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

Ejercicio 2.1.2. Seis hermanos (Alonso, Bernardo, Carlos, Daniel, Enrique y Fernando) tienen que emparejarse para compartir habitación en el próximo curso escolar. Cada uno de ellos ha elaborado una lista con los nombres de aquellos con los que quiere emparejarse:

- Lista de Alonso: Daniel.
- Lista de Bernardo: Alonso, Enrique.
- Lista de Carlos: Daniel, Enrique.
- Lista de Daniel: Carlos.
- Lista de Enrique: Daniel, Bernardo, Fernando.
- Lista de Fernando: Alonso, Bernardo.

Dibuja el grafo dirigido que modela esta situación.

La situación se puede modelar con el grafo de la Figura 2.2, donde cada persona viene representada con un vértice con su inicial.

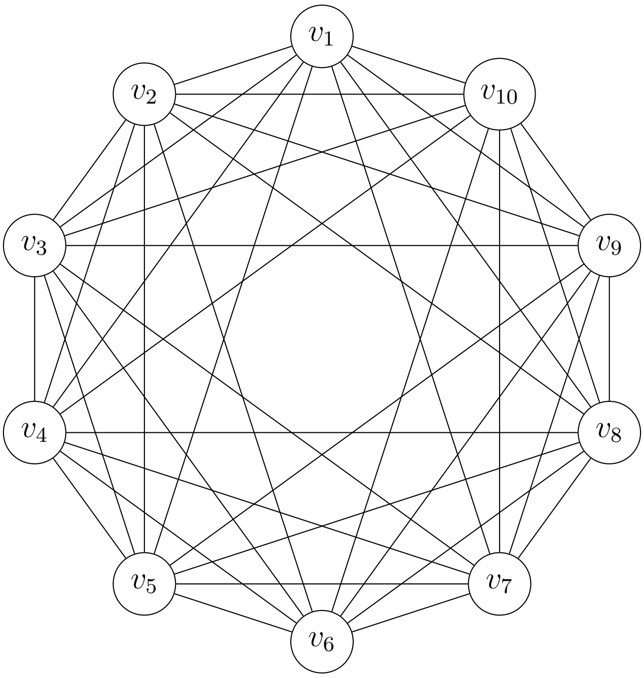


Figura 2.1: Situación del Ejercicio 2.1.1.

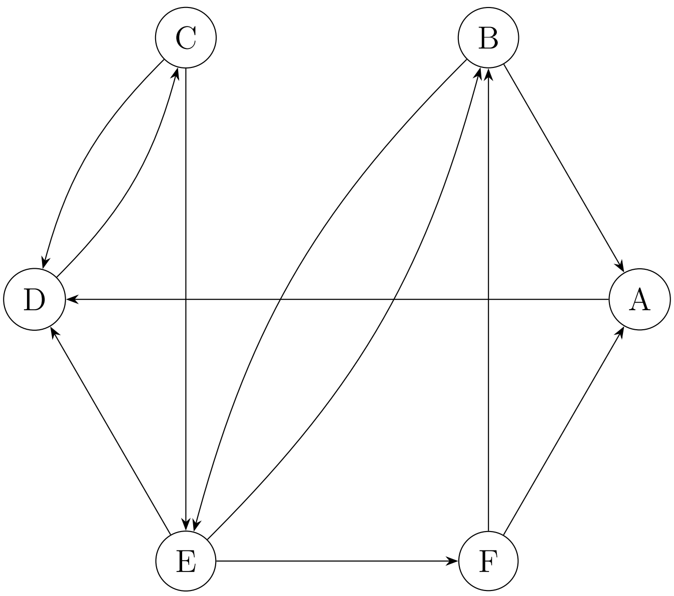
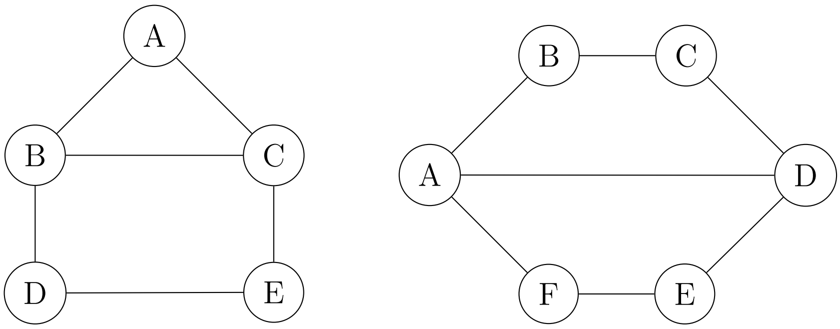


Figura 2.2: Situación del Ejercicio 2.1.2.



(a) Grafo 2.3a. (b) Grafo 2.3b.

Figura 2.3: Grafos para el ejercicio 2.1.3.

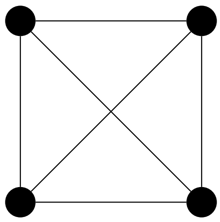


Figura 2.4: Grafo K_4.

Ejercicio 2.1.3. Expresa en forma matricial los grafos de la Figura 2.3.

La matriz de adyacencia del grafo 2.3a es:

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

La matriz de adyacencia del grafo 2.3b es:

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

Ejercicio 2.1.4. Sea G un grafo completo con cuatro vértices. Construye todos sus subgrafos salvo isomorfismo.

El grafo completo con cuatro vértices es K_4, representado en la Figura 2.4.

Para evitar pérdida de subgrafos, sabiendo que K_4 tiene 4 vértices, se pueden construir los siguientes subgrafos:

- No consideramos los subgrafos con 0 vértices.
- Tan solo hay un subgrafo con un vértice.

(a) $|E| = 0$. (b) $|E| = 1$.

Figura 2.5: Subgrafos de K_4 con 2 vértices, $|V| = 2$.

(a) $|E| = 0$. (b) $|E| = 1$. (c) $|E| = 2$. (d) $|E| = 3$.

Figura 2.6: Subgrafos de K_4 con 3 vértices, $|V| = 3$.

- Los subgrafos con dos vértices se encuentran en la Figura 2.5.
- Los subgrafos con tres vértices se encuentran en la Figura 2.6.
- Los subgrafos con cuatro vértices se encuentran en la Figura 2.7.

Ejercicio 2.1.5. ¿Son isomorfos los grafos de la Figura 2.8? ¿Y los de la Figura 2.9? ¿Y los de la Figura 2.10?

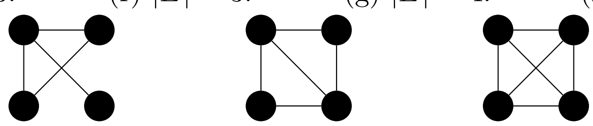
Veamos que los grafos de la Figura 2.8 son isomorfos. Sea $G(V, E)$ el grafo 2.8a y $G'(V', E')$ el grafo 2.8b. Las biyecciones $h_E : E \to E'$ y $h_V : V \to V'$ vienen dadas por:

$$\begin{array}{rcccc} h_V & : & V & \to & V' \\ & & A & \mapsto & A \\ & & B & \mapsto & B \\ & & C & \mapsto & D \\ & & D & \mapsto & C \\ & & E & \mapsto & E \end{array}$$

$$\begin{array}{rrcl} h_E : & E & \longrightarrow & E' \\ & e = \{u, v\} & \longmapsto & e' = \{h_V(u), h_V(v)\} \end{array}$$

(a) $|E| = 0$. (b) $|E| = 1$. (c) $|E| = 2$. (d) $|E| = 2$.

(e) $|E| = 3$. (f) $|E| = 3$. (g) $|E| = 4$. (h) $|E| = 4$.

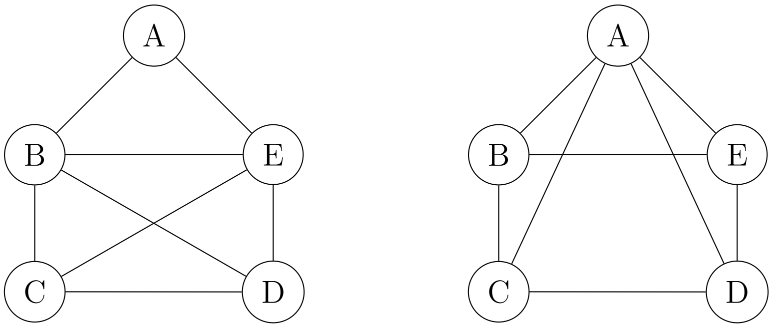


(i) $|E| = 4$. (j) $|E| = 5$. (k) $|E| = 6$.

Figura 2.7: Subgrafos de K_4 con 4 vértices, $|V| = 4$.

(a) Grafo 2.8a. (b) Grafo 2.8b.

Figura 2.8: Primer par de grafos para el ejercicio 2.1.5.



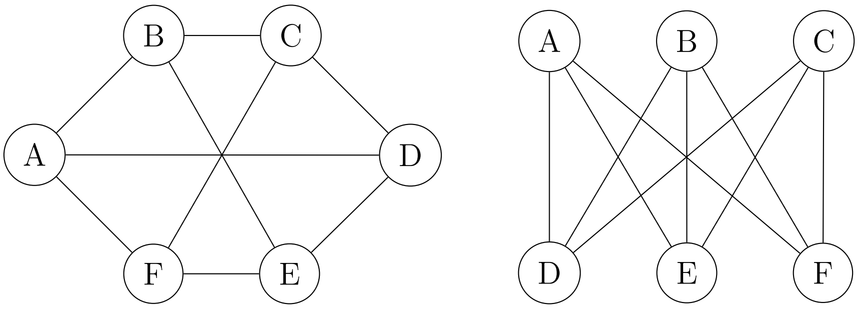
(a) Grafo 2.9a. (b) Grafo 2.9b.

Figura 2.9: Segundo par de grafos para el ejercicio 2.1.5.

Respecto al par de grafos de la Figura 2.9, sabemos que no son isomorfos puesto que no tienen la misma sucesión de grafos; pues notando por $G(E, V)$ al grafo 2.9a y $G'(E', V')$ al grafo 2.9b, se tiene que:

$$D_4(G) = 2 \neq 1 = D_4(G')$$

Por último, veamos que los grafos de la Figura 2.10 son isomorfos. Sea $G(V, E)$ el grafo 2.10a y $G'(V', E')$ el grafo 2.10b. Las biyecciones $h_E : E \to E'$ y $h_V : V \to V'$



(a) Grafo 2.10a. (b) Grafo 2.10b.

Figura 2.10: Tercer par de grafos para el ejercicio 2.1.5.

vienen dadas por:

$$\begin{array}{rcccl} h_V & : & V & \to & V' \\ & & A & \mapsto & A \\ & & B & \mapsto & D \\ & & C & \mapsto & C \\ & & D & \mapsto & B \\ & & E & \mapsto & E \\ & & F & \mapsto & F \end{array}$$

$$\begin{array}{rrcl} h_E : & E & \longrightarrow & E' \\ & e = \{u, v\} & \longmapsto & e' = \{h_V(u), h_V(v)\} \end{array}$$

Ejercicio 2.1.6. Demostrar que, en cualquier grafo, el número de vértices de grado impar es par. (Así, en un grupo de personas, el número total de personas que estrechan la mano de un número impar de otras personas es siempre par).

Sea el grafo $G(V, E)$ con V el conjunto de vértices y E el conjunto de aristas. Sea I el conjunto de vértices de grado impar:

$$I = \{v \in V \mid \deg(v) \text{ es impar}\}.$$

Usamos ahora el Lema de Apretón de Manos, descomponiendo V en dos conjuntos disjuntos, I y su complemento $\overline{I}$:

$$\sum_{v \in V} \deg(v) = \sum_{v \in I} \deg(v) + \sum_{v \notin I} \deg(v) = 2|E| \Longrightarrow \sum_{v \in I} \deg(v) = 2|E| - \sum_{v \notin I} \deg(v).$$

Por tanto, como $2|E|$ es par, y la suma y resta de números pares es par, tenemos que:

$$\sum_{v \in I} \deg(v) \text{ es par}$$

Por la definición de I, sabemos que dicha sumatoria es una suma de números impares cuya suma es par. Por tanto, como la suma de dos números impares es par, y la suma de un número par y un número impar es impar, tenemos que la cantidad de elementos en I ha de ser par.

$$|I| \text{ es par}$$

Ejercicio 2.1.7. Demostrar que si cada vértice de un grafo G es de grado 2, cada componente conexa de G es un ciclo.

Fijada una componente conexa del grafo G, seleccionamos un vértice suyo fijo, sea este v_0. Como $\deg v_0 = 2$, este tendrá dos vértices adyacentes, por lo que seleccionamos uno de ellos; sea este v_1. Como $\deg v_1 = 2$, entonces también tendrá dos vecinos, pero uno de ellos ya lo hemos visitado (v_0), por lo que seleccionamos el otro vecino; sea este v_3.

Repitiendo dicho algoritmo seleccionando vértices que no hayamos seleccionado, eventualmente llegaremos a v_0 (ya que en caso contrario V no sería finito). Por tanto, habríamos construido un ciclo. Además, como la elección está fijada y se trata de una componente conexa, habremos recorrido todos los vértices de la componente conexa luego, efectivamente, la componente conexa es un ciclo.

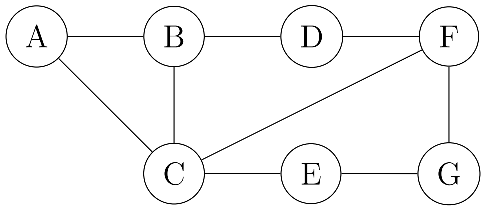


Figura 2.11: Grafo para el ejercicio 2.1.8.

Ejercicio 2.1.8. Los siguientes hechos se conocen de las personas A, B, C, D, E, F, G:

- A habla inglés.
- B habla inglés y español.
- C habla inglés, italiano y ruso.
- D habla japonés y español.
- E habla alemán e italiano.
- F habla francés, japonés y ruso.
- G habla francés y alemán.

Demostrar que cada par de personas entre estas siete puede comunicarse (con la ayuda de intérpretes, si es necesario, tomados de los cinco restantes).

Construiremos un grafo, en el que dos personas están conectadas por una arista si hablan el mismo idioma. Dicho grafo es el de la Figura 2.11. Como se trata de un grafo conexo, dada una persona p, podemos llegar a cualquier otra persona q mediante un camino simple (que representan los intérpretes). Por tanto, cada par de personas puede comunicarse.

Ejercicio 2.1.9. Demuestra que en todo grafo con más de un vértice existen dos vértices con el mismo grado.

Supongamos un grafo $G(V, E)$ con $|V| > 1$. Como hay $|V|$ vértices, el grado máximo posible es $|V| - 1$ (que representaría que dicho vértice está conectado con todos los demás). Por tanto, los posibles grados son:

$$0, 1, 2, \dots, |V| - 1.$$

No obstante, veamos que no todos son posibles; ya que si hay un vértice de grado 0, entonces no puede haber vértices de grado $|V|-1$ (pues dichos vértices no podrían estar conectados con el vértice de grado 0). Por tanto, hay $|V|$ vértices y el número de grados posibles es menor que $|V|$; por lo que, por el principio del palomar, hay al menos dos vértices con el mismo grado.

Ejercicio 2.1.10. Prueba que si un grafo G contiene solo dos vértices de grado impar entonces ambos han de encontrarse en la misma componente conexa.

Por reducción al absurdo, supongamos que los dos vértices de grado impar se encuentran en componentes conexas distintas; y consideramos $G'(V', E')$ la componente conexa que contiene a uno de ellos (sin pérdida de generalidad, sea v_1) y $G''(V'', E'')$ la componente conexa que contiene al otro (sea v_2). Como componentes conexas que son, podemos considerarlos como subgrafos de G, por lo que G' (se podría trabajar análogamente con G'') cumple el Lema del Apretón de Manos:

$$\sum_{v\in V'} \deg(v) = 2|E'| \Longrightarrow \left(\sum_{\substack{v\in V'\\ v\neq v_1}} \deg(v)\right) + \deg(v_1) = 2|E'|$$

No obstante, la sumatoria sabemos que es una suma de grados pares (pues todos los vértices de G' son de grado par, salvo v_1), por lo que es par; y la suma de un número par y un número impar es impar; por lo que no es posible que su suma valga $2|E'|$ (que es par). Por tanto, por reducción al absurdo, los dos vértices de grado impar han de encontrarse en la misma componente conexa.

Ejercicio 2.1.11. ¿Existe algún grafo regular de grado 5 con 25 vértices?

No, por el Ejericio 2.1.6 (25 es impar).

Ejercicio 2.1.12. ¿Existe un grafo completo con 595 lados?

En un grafo completo, sabemos que:

$$|E| = \frac{|V|(|V|-1)}{2}.$$

Suponiendo que fuese posible, como $|E| = 595$, tendríamos que:

$$595 = \frac{|V|(|V|-1)}{2} \Longrightarrow |V|^2 - |V| - 1190 = 0 \Longrightarrow |V| = \frac{1 \pm \sqrt{1 + 4\cdot 1190}}{2} = \frac{1 \pm 69}{2} \Longrightarrow |V| = 35$$

Por tanto, sí es posible, y este es el grafo K_{35}.

Ejercicio 2.1.13. ¿Existe un grafo con 6 vértices cuyos grados sean 1, 2, 2, 3, 4 y 4 respectivamente?

Buscamos saber si dicha sucesión es gráfica. Para ello, aplicamos el Algoritmo de Havel-Hakimi:

4	4	3	2	2	1	Eliminamos el 4 y restamos uno a los 4 términos siguientes
	3	2	1	1	1	Eliminamos el 3 y restamos uno a los 3 términos siguientes
		1	0	0	1	Reordenamos los términos
		1	1	0	0	Eliminamos el 1 y restamos uno al término siguiente
			0	0	0	

Figura 2.12: Grafo con sucesión de grados $0, 0, 0$.

Figura 2.13: Grafo con sucesión de grados $1, 1, 0, 0$.

Llegados a este punto, como la sucesión $0, 0, 0$ es gráfica, entonces la sucesión $1, 2, 2, 3, 4, 4$ también lo es. Reconstruimos para ello el grafo; partiendo de la sucesión $0, 0, 0$, cuyo grafo es el de la Figura 2.12.

La siguiente sucesión es $1, 1, 0, 0$, que resultó en la sucesión $\mathbf{0}, 0, 0$; por lo que hemos de añadir un vértice de grado 1 que se conecte con uno de los vértices de grado 0; obteniendo el grafo de la Figura 2.13.

La siguiente sucesión es $3, 2, 1, 1, 1$, que resultó en la sucesión $\mathbf{1,0,0}, 1$; por lo que hemos de añadir un vértice de grado 3 que se conecte con un vértice de grado 1 y dos de grado 0; obteniendo el grafo de la Figura 2.14.

La siguiente sucesión es $4, 4, 3, 2, 2, 1$, que resultó en la sucesión $\mathbf{3,2,1,1}, 1$; por lo que hemos de añadir un vértice de grado 4 que se conecte con un vértice de grado 3, uno de grado 2 y dos de grado 1; obteniendo el grafo de la Figura 2.15.

Ejercicio 2.1.14. En cada uno de los siguientes casos, dibuja un grafo de Euler que verifique las condiciones, o prueba que tal grafo no existe:

1. Con un número par de vértices y un número par de lados.

   Además de $K_{n,m}$ con m, n pares; el grafo de la Figura 2.16 cumple con las condiciones.

2. Con un número par de vértices y un número impar de lados.

   El grafo de la Figura 2.17 cumple con las condiciones.

3. Con un número impar de vértices y un número par de lados.

   Además de K_5, el grafo de la Figura 2.18 cumple con las condiciones.

4. Con un número impar de vértices y un número impar de lados.

   Además de K_3, el grafo de la Figura 2.19 cumple con las condiciones.

Ejercicio 2.1.15. Encuentra un circuito de Euler para los grafos de la Figura 2.20.

Para el grafo de la Figura 2.20a, un circuito de Euler es:

$$A \to B \to D \to G \to H \to D \to E \to B \to C \to E \to H \to I \to E \to F \to I \to J \to F \to C \to A$$

Para el grafo de la Figura 2.20b, un circuito de Euler es:

$$B \to A \to C \to B \to E \to C \to D \to F \to E \to D \to B$$

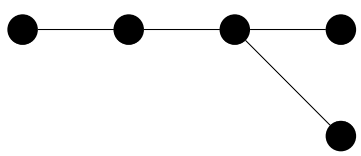


Figura 2.14: Grafo con sucesión de grados $3, 2, 1, 1, 1$.

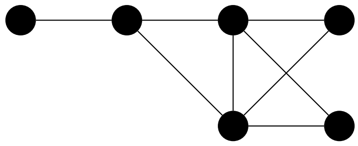


Figura 2.15: Grafo con sucesión de grados $4, 4, 3, 2, 2, 1$.

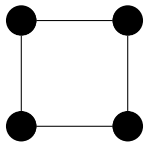


Figura 2.16: Grafo para el Ejercicio 2.1.14.1.

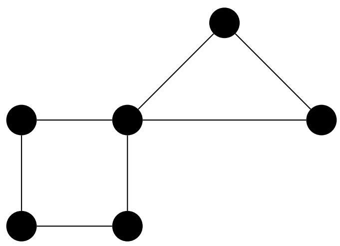


Figura 2.17: Grafo para el Ejercicio 2.1.14.2.

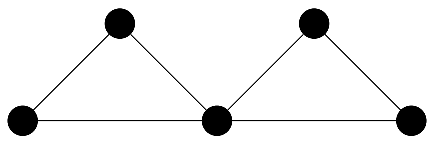


Figura 2.18: Grafo para el Ejercicio 2.1.14.3.

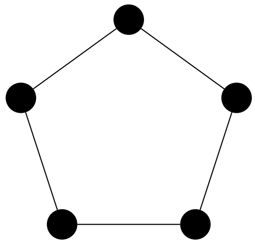
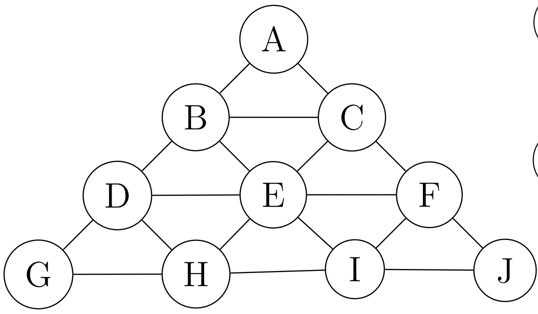
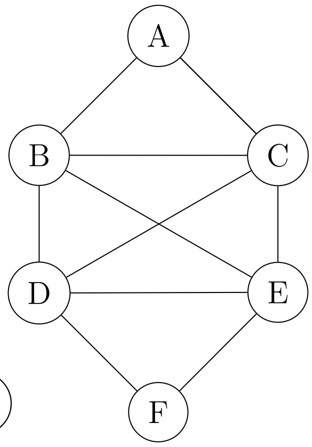


Figura 2.19: Grafo para el Ejercicio 2.1.14.4.

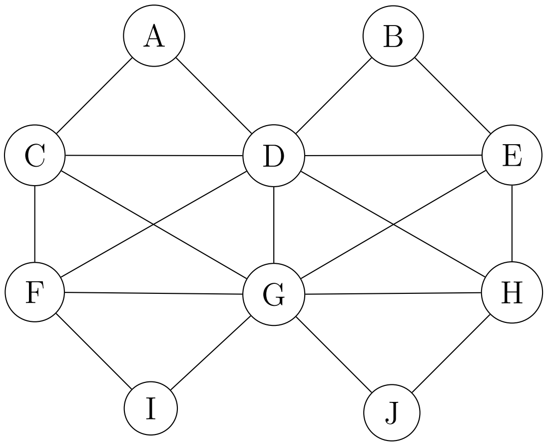


(a) Grafo 2.20a.

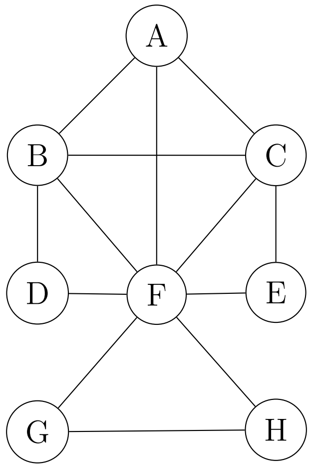


(b) Grafo 2.20b.

Figura 2.20: Grafos para el ejercicio 2.1.15.



(a) Grafo 2.21a.



(b) Grafo 2.21b.

Figura 2.21: Grafos para el ejercicio 2.1.16.

Ejercicio 2.1.16. Encuentra un camino de Euler para los grafos de la Figura 2.21.

Para el grafo de la Figura 2.21a, un circuito de Euler es:

$$D \to C \to G \to D \to F \to I \to G \to F \to C \to A \to D \to E \to B \to D \to H \to E \to G \to J \to H \to G$$

Para el grafo de la Figura 2.21b, un circuito de Euler es:

$$A \to B \to C \to A \to F \to D \to B \to F \to C \to E \to F \to G \to H \to F$$

Ejercicio 2.1.17. Encontrar un circuito de Euler en el grafo de la Figura 2.22 y un camino de Euler en el grafo de la Figura 2.23.

Para el grafo de la Figura 2.22, un circuito de Euler es:

$$A \to G \to B \to C \to E \to F \to L \to K \to J \to L \to I \to H \to B \to I \to J \to E \to D \to C \to J \to B \to A$$

Para el grafo de la Figura 2.23, un camino de Euler es:

$$E \to B \to F \to E \to A \to B \to C \to D \to G \to C \to H \to G \to F \to A$$

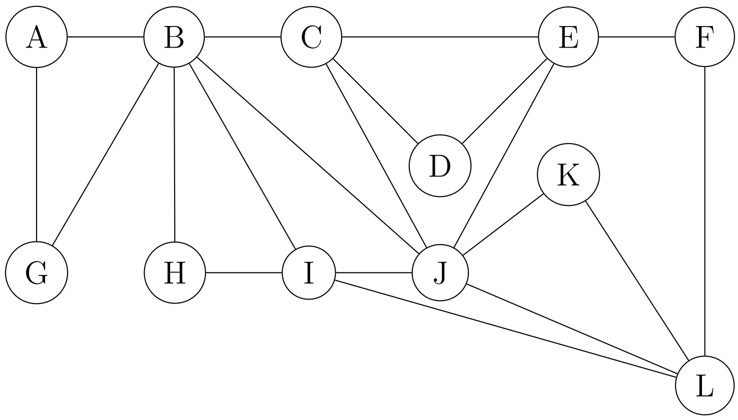


Figura 2.22: Primer grafo para el ejercicio 2.1.17.

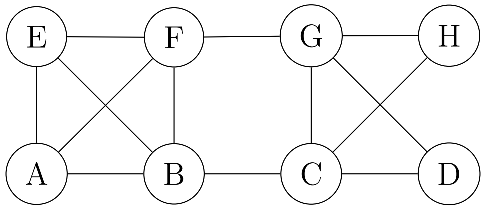


Figura 2.23: Segundo grafo para el ejercicio 2.1.17.

Ejercicio 2.1.18. ¿Para qué valores de n el grafo K_n es un circuito de Euler?

El grafo K_n sabemos que es conexo y, al ser completo, todos los vértices tienen grado $n-1$. Además, para que un grafo conexo sea de Euler, todos sus vértices han de tener grado par. Por tanto, $n-1$ ha de ser par, es decir, n ha de ser impar. Por tanto, el grafo K_n es un circuito de Euler si y solo si n es impar.

Ejercicio 2.1.19. Un viajante vive en la ciudad A y se supone que visita las ciudades B, C y D antes de volver a A. Encontrar la ruta más corta que consuma este viaje si las distancias entre las cuatro ciudades son, en Km:

- 120 entre A y B.
- 70 entre B y C.
- 140 entre A y C.
- 180 entre A y D.
- 100 entre B y D.
- 110 entre C y D.

Representamos el problema mediante el grafo de la Figura 2.24, que es K_4 con las distancias entre las ciudades. Se trata del problema del Viajante del comercio, un problema NP-completo para el que no se conoce una solución y que ya fue estudiado en Algorítmica. Sin embargo, el trabajar solo con 4 nodos, podemos aplicar fuerza bruta para estudiar todos los caminos, sin mucha dificultad. Observemos que elegir un camino que salga de A, pase por todos los nodos y vuelva a A es equivalente

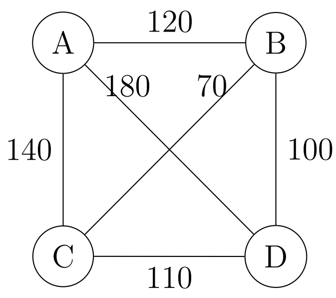


Figura 2.24: Grafo para el ejercicio 2.1.19.

a elegir 3 nodos de un conjunto de 3 nodos, por lo que tenemos $V_3^3 = P_3 = 3!$ posibilidades:

1. $B - C - D$
2. $B - D - C$
3. $C - B - D$
4. $C - D - B$
5. $D - B - C$
6. $D - C - B$

Sin embargo, observemos que nos da igual el orden (si recorremos el camino uvw o el wvu, es el mismo coste) en el que los visitamos, por lo que nos quedamos con 3 posibilidades (al ser los caminos 1 y 6, 2 y 4; y 3 y 5 iguales):

1. $B - C - D = 120 + 70 + 110 + 180 = 480$
2. $B - D - C = 120 + 100 + 110 + 140 = 470$
3. $C - B - D = 180 + 100 + 70 + 140 = 490$

Concluimos que el camino óptimo es: $A - B - D - C$, con un coste de 470.

Ejercicio 2.1.20. El grafo línea $L(G)$ de un un grafo G se define como sigue: Los vértices de $L(G)$ son los lados de G, $V(L(G)) = E(G)$; y dos vértices en $L(G)$ son adyacentes si y solo si los lados correspondientes en G comparten un vértice. Demostrar:

1. Si G es un grafo conexo regular de grado r, entonces $L(G)$ es un grafo de Euler.

   Por ser G un grafo conexo, tenemos que todos los vértices están conectados; y por tanto lo están también los lados de G. Es decir, dados dos lados cualesquiera de G, siempre podemos encontrar una sucesión de vértices adyacentes que los conecten; por lo que $L(G)$ es conexo.

   Veamos ahora que el grado de cada vértice de $L(G)$ es par. Dado un vértice e de $L(G)$, este representa un lado de G que conecta dos vértices de G, sea $\gamma_G(e) = \{v_1, v_2\}$. Por cada lado de G incidente a v_1 o v_2 (excepto e), hay un vértice adyacente a e en $L(G)$; por lo que:

$$\deg_{L(G)}(e) = \deg_G(v_1) + \deg_G(v_2) - 2$$

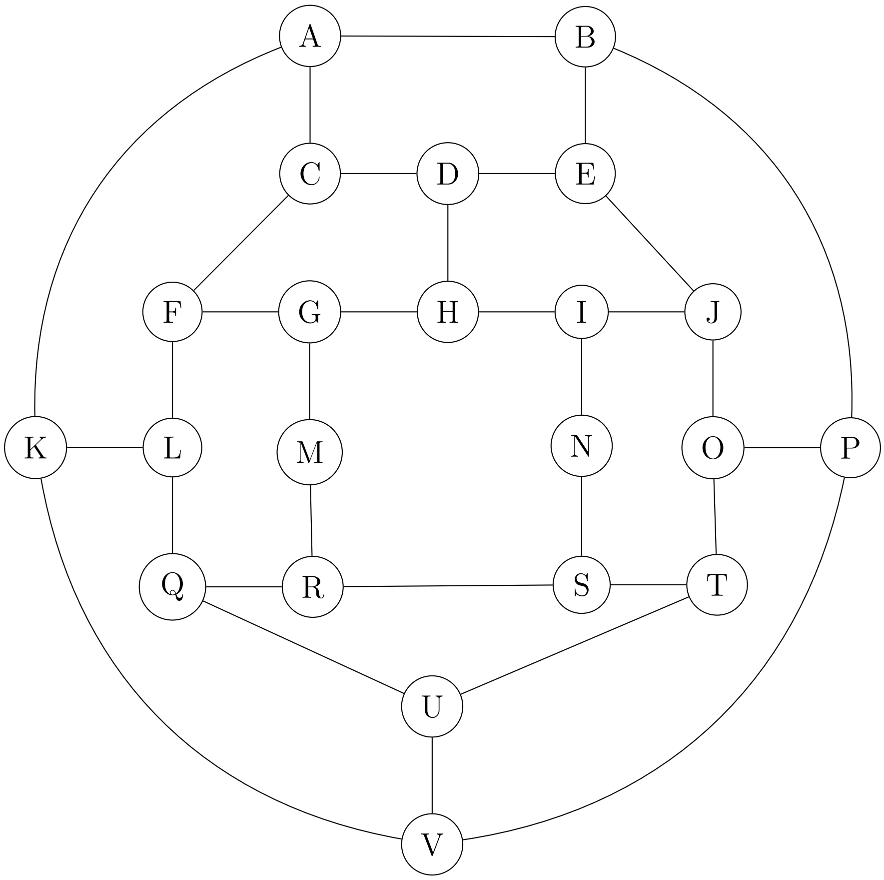


Figura 2.25: Primer grafo para el ejercicio 2.1.21.

donde se resta 2 por el lado e que comparten v_1 y v_2. Por ser G regular de grado r, tenemos que:

$$\deg_{L(G)}(e) = r + r - 2 = 2r - 2 = 2(r-1)$$

Por tanto, como e es un vértice arbitrario de $L(G)$, tenemos de hecho que $L(G)$ es regular de grado $2(r-1)$, es decir, todos los vértices de $L(G)$ tienen grado par. Por tanto, $L(G)$ es un grafo de Euler.

2. Si G es un grafo de Euler entonces $L(G)$ es Hamiltoniano.

   Supongamos que G es un grafo de Euler, por lo que podemos encontrar una sucesión de lados $e_1, e_2, \dots, e_n$ que recorren todos los lados de G una vez sin repetir ninguno. Por la definición de $L(G)$, cada vértice de $L(G)$ representa un lado de G; por lo que la sucesión de lados de G se convierte en una sucesión de vértices de $L(G)$ que recorre todos los vértices de $L(G)$ una vez sin repetir ninguno. Además, esto es posible porque dos lados adyacentes en G comparten un vértice, por lo que serán vértices adyacentes en $L(G)$. Por tanto, $L(G)$ es Hamiltoniano.

Ejercicio 2.1.21. De entre los grafos de la Figura 2.25 y la Figura 2.26, ¿cuáles contienen un circuito de Hamilton?

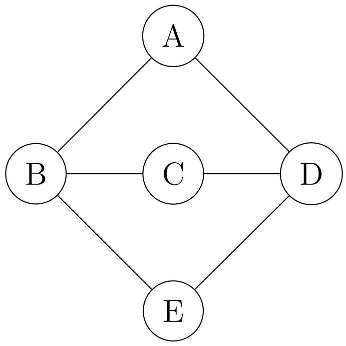


Figura 2.26: Segundo grafo para el ejercicio 2.1.21.

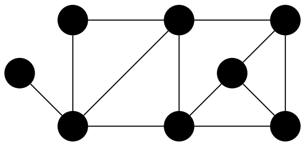


Figura 2.27: Grafo para el ejercicio 2.1.22.1.

Respecto al grafo de la Figura 2.25, se comprueba que no cumple ninguna de las condiciones suficientes para ser Hamiltoniano; aunque sí cumple todas las condiciones necesarias. Por tanto, hemos de buscar el circuito de Hamilton a ciegas. Este es:

$$A \to K \to V \to P \to H \to E \to J \to O \to T \to U \to Q \to L \to F \to G \to M \to$$
$$\to R \to S \to N \to I \to H \to D \to C \to A$$

Respecto al grafo de la Figura 2.26, este no es Hamiltoniano.

Ejercicio 2.1.22.

1. Prueba, utilizando el algoritmo explicado en clase, que la sucesión $4 \geqslant 4 \geqslant 4 \geqslant 3 \geqslant 3 \geqslant 3 \geqslant 2 \geqslant 1$ es gráfica y, utilizando dicho algoritmo, encuentra un grafo que tenga como sucesión de grados la correspondiente.

   Aplicamos el Algoritmo de Havel-Hakimi, y posteriormente construimos el grafo correspondiente, que se muestra en la Figura 2.27.

4	4	4	3	3	3	2	1	Eliminamos el 4 y restamos uno a los 4 términos siguientes
	3	3	2	2	3	2	1	Reordenamos los términos
	3	3	3	2	2	2	1	Eliminamos el 3 y restamos uno a los 3 términos siguientes
		2	2	1	2	2	1	Reordenamos los términos
		2	2	2	2	1	1	Eliminamos el 2 y restamos uno a los 2 términos siguientes
			1	1	2	1	1	Reordenamos los términos
			2	1	1	1	1	Eliminamos el 2 y restamos uno a los 2 términos siguientes
				0	0	1	1	

2. El grafo con matriz de adyacencia M dada por:

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

es de Euler o en él hay un camino de Euler entre dos vértices. Razona cuál es la situación y encuentra, en su caso, el circuito o el camino de Euler que existe.

Sabemos que el grado del vértice v_i es la suma de los elementos de la fila i de la matriz de adyacencia. Calculando los grados de los vértices, obtenemos tenemos que todos son pares a excepción de los vértices v_1 y v_8, por lo que hay un camino de Euler entre ellos. Este lo construimos con el algoritmo de Fleury, obteniendo el camino:

$$v_1 \to v_2 \to v_3 \to v_4 \to v_6 \to v_7 \to v_8 \to v_5 \to v_2 \to v_7 \to v_1 \to v_6 \to$$
$$\to v_3 \to v_1 \to v_4 \to v_7 \to v_5 \to v_6 \to v_2 \to v_4 \to v_8$$

Ejercicio 2.1.23.

1. En el grafo G cuya matriz de adyacencia es

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

determina el número de aristas y la sucesión de grados de los vértices y, caso de que G sea de Euler, describe un circuito de Euler en él usando el algoritmo apropiado.

Tenemos que:

$$\begin{array}{llll} \deg v_1 = 4 & \deg v_2 = 2 & \deg v_3 = 4 & \deg v_4 = 4 \\ \deg v_5 = 2 & \deg v_6 = 4 & \deg v_7 = 2 & \deg v_8 = 4 \end{array}$$

Por tanto, usando el Lema del Apretón de Manos, tenemos que:

$$\sum_{v \in V} \deg v = 4+2+4+4+2+4+2+4 = 26 = 2|E| \Longrightarrow |E| = 13$$

La sucesión de grados por tanto es:

$$0, 0, 3, 0, 5$$

Realizando un recorrido del grafo, vemos que el grafo es conexo; y como todos sus vértices tienen grado par, es de Euler. Por tanto, aplicamos el algoritmo de Fleury para encontrar un circuito de Euler, obteniendo el circuito:

$$v_1 \to v_2 \to v_8 \to v_6 \to v_1 \to v_4 \to v_3 \to v_6 \to v_4 \to v_8 \to v_7 \to v_3 \to v_5 \to v_1$$

2. Calcula el número de vértices de un grafo plano, conexo y regular de grado 5 con 20 caras.

   Por ser plano y conexo, tenemos que:

   $$|V| + 20 = |E| + 2$$

   Por el Lema del Apretón de Manos, tenemos que:

   $$\sum_{v \in V} \deg v = 2|E| \Longrightarrow 5|V| = 2|E|$$

   Resolvemos por tanto el siguiente sistema:

   $$\begin{aligned} |V| + 20 &= |E| + 2 \\ 5|V| &= 2|E| \Longrightarrow |E| = {}^5\!/_2 \cdot |V| \end{aligned}$$

   Por tanto, tenemos que:

   $$|V| + 20 = {}^5\!/_2 \cdot |V| + 2 \Longrightarrow |V| = {}^{18\cdot 2}\!/_3 = 12$$

Ejercicio 2.1.24.

1. La siguiente matriz es la matriz de incidencia o adyacencia de un grafo. Razona qué caso es y dibuja el correspondiente grafo.

   $$M = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

   ¿Es el grafo anterior de Euler o Hamilton? Razona la respuesta y da un circuito de Euler o Hamilton en caso de que los haya.

   Como no se trata de una matriz cuadrada, no puede ser de adyacencia, por lo que se trata de una matriz de incidencia. El grafo correspondiente es el de la Figura 2.28.

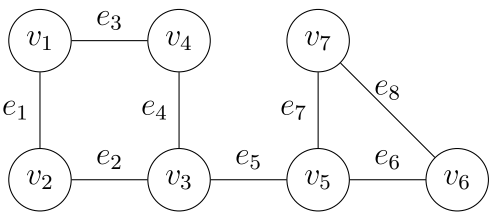


Figura 2.28: Grafo para el ejercicio 2.1.24.1.

Los grados de los vértices son la suma de las filas de la matriz de incidencia, obteniendo:

$$\begin{array}{llll} \deg v_1 = 2 & \deg v_2 = 2 & \deg v_3 = 3 & \deg v_4 = 2 \\ \deg v_5 = 3 & \deg v_6 = 2 & \deg v_7 = 2 & \end{array}$$

Por tanto, no se trata de un grafo de Euler (pues hay vértices de grado impar), pero sí tiene un camino de Euler entre los vértices v_3 y v_5, que es:

$$v_3 \overset{e_4}{\Longrightarrow} v_4 \overset{e_3}{\Longrightarrow} v_1 \overset{e_1}{\Longrightarrow} v_2 \overset{e_2}{\Longrightarrow} v_3 \overset{e_5}{\Longrightarrow} v_5 \overset{e_6}{\Longrightarrow} v_6 \overset{e_8}{\Longrightarrow} v_7 \overset{e_7}{\Longrightarrow} v_5$$

Además, no es un grafo de Hamilton, pues contiene una arista puente. Esto implica que no se podrá construir un circuito (aunque no sabemos nada sobre camino) de Hamilton en él.

2. Aplica el algoritmo para comprobar si la siguiente sucesión

$$6 \geqslant 4 \geqslant 4 \geqslant 3 \geqslant 3 \geqslant 3 \geqslant 3 \geqslant 3$$

es, o no es, una sucesión gráfica y, en caso de serlo, también aplica el algoritmo para encontrar un grafo que la tenga como sucesión de grados.

No se trata de una sucesión gráfica, pues la suma de los grados es impar, lo que contradice el Lema del Apretón de Manos:

$$\sum_{v \in V} \deg v = 6 + 4 + 4 + 3 + 3 + 3 + 3 + 3 = 29$$

Ejercicio 2.1.25. Razona cuál es la respuesta correcta en cada una de las siguientes cuestiones (todos los grafos a los que se hace referencia son simples, no tienen lazos ni lados paralelos):

1. El grafo completo K_n:

   a) Es siempre de Euler.

   b) Es siempre de Hamilton.

   c) Dependiendo de n puede ser, o no, de Hamilton o de Euler.

Sabemos que K_n es conexo y que todos sus vértices tienen grado $n-1$. Por tanto, en primer lugar vemos que:

$$K_n \text{ es de Euler} \iff n \text{ es impar}$$

Por otro lado, sabemos que, para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = n - 1 + n - 1 = 2n - 2 \geqslant n \iff n \geqslant 2$$

Por tanto, sabemos que K_n con $n \geqslant 2$ es de Hamilton. Aunque K_1 sí es de Hamilton, K_2 no lo es. Por tanto, tenemos que:

$$K_n \text{ es de Hamilton} \qquad \forall n \in \mathbb{N} \setminus \{2\}$$

Por tanto, la respuesta correcta es la **c)**.

2. He encontrado un grafo plano y conexo con 200 vértices y:

   a) Un número par de caras y un número impar de lados.

   b) Un número par de lados y un número impar de caras.

   c) Un número par de lados y caras.

   Por ser plano y conexo, sabemos que:

   $$200 + |C| = |E| + 2$$

   Por tanto, o bien $|E|$ y $|C|$ son ambos pares, o ambos impares. Por tanto, la respuesta correcta es la **c)**.

3. Tengo un grafo con un solo vértice de grado impar v:

   a) Puedo encontrar un camino que empiece en ese vértice v, recorra todos los lados del grafo solo una vez y vuelva a él.

   b) Si añado un lado que conecte ese vértice con otro cualquiera del grafo, pongamos w, puedo encontrar un camino que empiece en v, recorra todos los lados del grafo (incluido el que he añadido) solo una vez y termine en w.

   c) Es imposible tener un grafo como ese.

   Por el Ejercicio 2.1.6, sabemos que el número de vértices de grado impar en un grafo es par. Por tanto, la respuesta correcta es la **c)**.

4. En un grafo plano con cinco componentes conexas y 24 lados:

   a) El número de vértices y el número de caras son opuestos módulo 30.

   b) El número de vértices y el número de caras son congruentes módulo 30.

   c) Ninguna de las anteriores es cierta.

Por ser plano, tenemos que:

$$|V| + |C| = 24 + 1 + 5 = 30$$

Por tanto, la respuesta correcta es la **a)**.

5. Dado un grafo regular de grado 1, entonces:

   a) El grafo no puede ser conexo.

   b) El grafo tiene tantas componentes conexas como vértices.

   c) El grafo tiene tantas componentes conexas como lados.

   La respuesta correcta es la **c)**.

6. Un grafo regular conexo de grado 11 con veinte vértices:

   a) Es siempre de Euler.

   b) Es siempre de Hamilton.

   c) Ninguna de las dos respuestas anteriores es cierta.

   Como es regular de grafo 11 (impar), sabemos que no es de Euler. Por otro lado, sabemos que, para cada par de vértices no adyacentes, se verifica que:

   $$\deg v_i + \deg v_j = 11 + 11 = 22 \geqslant 20$$

   Por tanto, sabemos que es de Hamilton. Por tanto, la respuesta correcta es la **b)**.

7. Elija la respuesta correcta:

   a) Sólo hay dos grafos con cuatro vértices y cuatro lados no isomorfos.

   b) Todos los grafos con cuatro vértices y cuatro lados son isomorfos.

   c) Sólo hay tres grafos con cuatro vértices y cuatro lados no isomorfos.

   En el Ejercicio 2.1.4 vimos que la respuesta correcta es la **a)**.

8. Un grafo cuya matriz de adyacencia es

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

   a) Es de Euler.

   b) No es de Euler pero hay un camino de Euler entre dos vértices.

   c) No es de Euler pero sus componentes conexas sí lo son.

No es de Euler, pues no es conexo. Sus componentes conexas, formadas por los vértices $\{v_1, v_2, v_3\}$ y $\{v_4, v_5, v_6, v_7\}$ respectivamente, sí son de Euler por ser conexas y tener todos los grados pares. Por tanto, la respuesta correcta es la **c)**.

9. Un grafo cuya matriz de incidencia es

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

a) Es de Hamilton.

b) No es de Hamilton pero sus componente conexas sí lo son.

c) No es de Hamilton y tampoco lo son sus componentes conexas.

Este grafo es conexo (el vértice v_3 está conectado con todos los demás). Además, como $\deg v_5 = 1$, sabemos que no es de Hamilton. Por tanto, la respuesta correcta es la **c)**.

10. La siguiente matriz

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

a) Puede ser la matriz de adyacencia de un grafo pero no la de incidencia.

b) Puede ser la matriz de incidencia de un grafo pero no la de adyacencia.

c) No puede ser la matriz de adyacencia ni la de incidencia de un grafo.

Como $a_{13} = 0 \neq 1 = a_{31}$, la matriz no es simétrica y por tanto no puede ser la matriz de adyacencia de un grafo. Por otro lado, como la suma de la tercera columna es 3, si se tratase de la matriz de incidencia, tendríamos una arista que conecta tres vértices, lo que no es posible en un grafo simple. Por tanto, la respuesta correcta es la **c)**.

Ejercicio 2.1.26.

1. Prueba, utilizando el algoritmo explicado en clase, que la sucesión dada por $3 \geqslant 3 \geqslant 2 \geqslant 2 \geqslant 2 \geqslant 2 \geqslant 2$ es gráfica y, utilizando dicho algoritmo, encuentra un grafo en que los grados de sus vértices sean los términos de esa sucesión. Prueba que el grafo es plano y que satisface el teorema de la característica de Euler.

Aplicamos el Algoritmo de Havel-Hakimi, y posteriormente construimos el grafo correspondiente, que se muestra en la Figura 2.29.

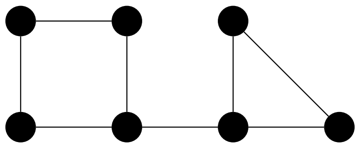


Figura 2.29: Grafo para el ejercicio 2.1.26.1.

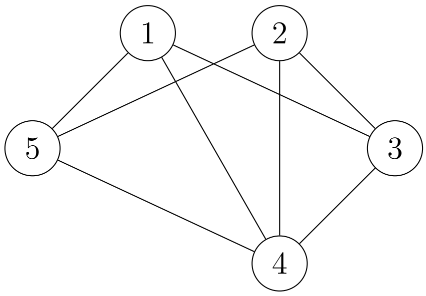


Figura 2.30: Grafo G_1 para el ejercicio 2.1.26.2.

3	3	2	2	2	2	2	Eliminamos el 3 y restamos uno a los 3 términos siguientes
	2	1	1	2	2	2	Reordenamos los términos
	2	2	2	2	1	1	Eliminamos el 2 y restamos uno a los 2 términos siguientes
		1	1	2	1	1	Reordenamos los términos
		2	1	1	1	1	Eliminamos el 2 y restamos uno a los 2 términos siguientes
			0	0	1	1	

2. Considera los grafos G_1 dado por el diagrama de la Figura 2.30 y G_2 con matriz de incidencia

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

   Estudia si son o no isomorfos, si son o no planos, si son o no de Euler o si hay un camino de Euler (en caso afirmativo aplica el algoritmo para calcular un circuito o un camino de Euler) y si son o no de Hamilton (encontrando el camino en caso afirmativo).

   Estudiamos cada aspecto:

   - No son isomorfos, puesto que G_1 no tiene vértices de grado 2 y G_2 sí (v_5).
   - En ambos casos, tanto para G_1 como para G_2, tenemos que:

     $$|V| = 5 \quad |E| = 8$$

     Además, tenemos que:

     - Para K_5: $|V| = 5$, $|E| = 10$.
     - Para $K_{3,3}$: $|V| = 6$, $|E| = 9$.

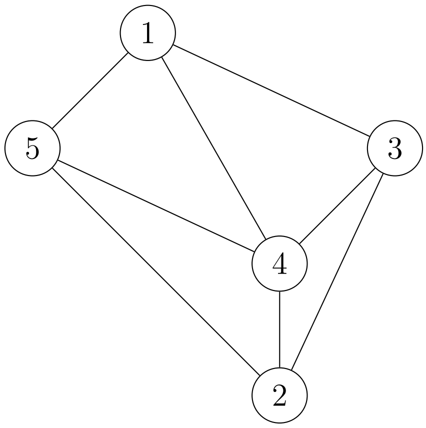


Figura 2.31: Representación plana de G_1 (Figura 2.30).

Como $|E| = 8 < 9, 10$, y toda contracción de un grafo reduce el número de aristas, sabemos que ningún subgrafo de ninguno de los dos podrá contraerse a K_5 o a $K_{3,3}$. Por tanto, por el Teorema de Kuratowski, sabemos que ambos son planos. De hecho, en la Figura 2.31 se muestra la representación plana de G_1 (Figura 2.30).

- Ninguno de ellos es de Euler, puesto que tienen vértices de grado impar.
- G_1 no tiene ningún camino de Euler, puesto que hay más de dos vértices de grado impar. G_1, no obstante, sí tiene un camino de Euler de v_1 a v_4:

$$v_1 \xRightarrow{e_1} v_2 \xRightarrow{e_3} v_4 \xRightarrow{e_2} v_1 \xRightarrow{e_8} v_3 \xRightarrow{e_4} v_2 \xRightarrow{e_5} v_5 \xRightarrow{e_7} v_3 \xRightarrow{e_6} v_4$$

- Respecto al circuito de Hamilton, estudiamos en primer lugar G_1. Sus grados son:

$$\deg v_1 = 3 \qquad \deg v_2 = 3 \qquad \deg v_3 = 3 \qquad \deg v_4 = 4 \qquad \deg v_5 = 3$$

Por tanto, dados dos vértices cualesquiera no adyacentes, se verifica que:

$$\deg v_i + \deg v_j \geqslant 6 \geqslant 5 \Longrightarrow G_1 \text{ es de Hamilton}$$

Un posible recorrido de Hamilton para G_1 es:

$$1 \to 3 \to 2 \to 5 \to 4 \to 1$$

Por otro lado, estudiamos G_2. Sus grados son:

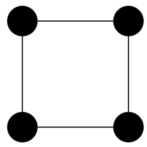
$$\deg v_1 = 3 \qquad \deg v_2 = 4 \qquad \deg v_3 = 4 \qquad \deg v_4 = 3 \qquad \deg v_5 = 2$$

Por tanto, dados dos vértices cualesquiera no adyacentes, se verifica que:

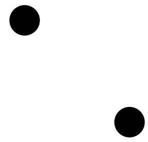
$$\deg v_i + \deg v_j \geqslant 5 \geqslant 5 \Longrightarrow G_2 \text{ es de Hamilton}$$

Un posible recorrido de Hamilton para G_2 es:

$$v_1 \xRightarrow{e_1} v_2 \xRightarrow{e_5} v_5 \xRightarrow{e_7} v_3 \xRightarrow{e_6} v_4 \xRightarrow{e_2} v_1$$



(a) Grafo G.



(b) Grafo G'.

Figura 2.32: Grafos para el ejercicio 2.1.27.2.

Ejercicio 2.1.27.

1. Si G es un grafo completo con 6 vértices entonces:

    a) G es regular de grado 5.

    b) G tiene 20 aristas.

    c) G es de Euler y de Hamilton.

    Sabemos que K_6 es regular de grado 5 y:

    $$|E| = \frac{6 \cdot 5}{2} = 15$$

    Además, aunque sí es de Hamilton, no es de Euler, por lo que la respuesta correcta es la **a)**.

2. Sea G' un subgrafo completo (pleno) de un grafo G. Entonces:

    a) Si G es de Euler también G' es de Euler.

    b) Si G es de Hamilton también G' es de Hamilton.

    c) Ninguna de las anteriores.

    Consideramos el contraejemplo de la Figura 2.32. El grafo G de la Figura 2.32a es de Euler y de Hamilton, pero su subgrafo completo G' de la Figura 2.32b no es ni de Euler ni de Hamilton. Por tanto, la respuesta correcta es la **c)**.

3. Seleccione la respuesta correcta:

    a) Sólo hay dos grafos con cuatro vértices y 5 lados no isomorfos.

    b) Todos los grafos con cuatro vértices y 5 lados son isomorfos.

    c) Todos los grafos con cuatro vértices y cinco lados son de Euler.

    En el Ejercicio 2.1.4 vimos que la respuesta correcta es la **b)**.

4. Sea G un grafo plano conexo regular de grado 6 con 15 caras. Entonces:

    a) G tiene 13 vértices.

    b) El número de vértices es el triple del de aristas.

    c) No existe un tal grafo.

Por ser plano y conexo, sabemos que:

$$|V| + 15 = |E| + 2$$

Por ser regular de grado 6, sabemos que:

$$2|E| = 6|V| \Longrightarrow |E| = 3|V|$$

Por tanto, sustituyendo en la primera ecuación, obtenemos:

$$|V| + 15 = 3|V| + 2 \Longrightarrow |V| = \frac{13}{2}$$

Por tanto, la respuesta correcta es la **c)**.

5. Salvo isomorfismos, grafos con 50 vértices y 1225 aristas:

   a) Solo hay 1.
   b) Hay 2.
   c) No existen grafos en esas condiciones.

   Tan solo hay uno, y se trata de K_{50}, por lo que la respuesta correcta es la **a)**.

Ejercicio 2.1.28.

1. Considera la sucesión $4, 4, 4, 4, 4$.

   a) Utiliza el algoritmo dado en clase para probar que la sucesión es una sucesión gráfica y para dibujar un grafo G que la tenga como sucesión gráfica.

   Aplicamos el Algoritmo de Havel-Hakimi, y posteriormente construimos el grafo correspondiente, que se muestra en la Figura 2.33 y se observa que $G = K_5$.

4	4	4	4	4	Eliminamos el 4 y restamos uno a los 4 términos siguientes
	3	3	3	3	Eliminamos el 3 y restamos uno a los 3 términos siguientes
		2	2	2	Eliminamos el 2 y restamos uno a los 2 términos siguientes
			1	1	Eliminamos el 1 y restamos uno al término siguiente
				0	

   b) Calcula las matrices incidencia y adyacencia del grafo G obtenido en el apartado anterior.

   La matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

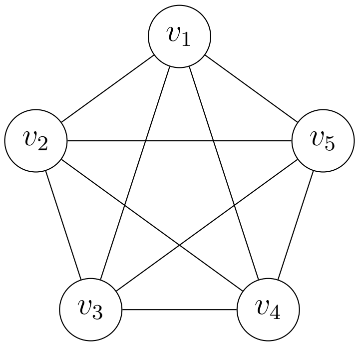


Figura 2.33: Grafo G del ejercicio 2.1.28.1.

La matriz de incidencia es:

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

c) ¿Es G de Euler o tiene un camino de Euler? En caso afirmativo, utiliza el algoritmo dado en clase para calcular el circuito o el camino de Euler.

Sí es de Euler, puesto que todos los vértices son de grado par. Un posible circuito de Euler es:

$$v_1 \to v_3 \to v_5 \to v_2 \to v_4 \to v_1 \to v_2 \to v_3 \to v_4 \to v_5 \to v_1$$

d) ¿Es G de Hamilton? En caso afirmativo calcula el circuito de Hamilton.

Sí, puesto que para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 4 + 4 = 8 \geqslant 5$$

Un posible circuito de Hamilton es:

$$v_1 \to v_2 \to v_3 \to v_4 \to v_5 \to v_1$$

e) ¿Es G plano? En caso afirmativo comprueba la fórmula de la característica de Euler.

No, ya se ha demostrado que $G = K_5$ no es plano; ya que $|V| = 5$, $|E| = 10$ pero:

$$|E| \nleqslant 3|V| - 6$$

2. Demuestra que si G es un grafo de Euler con n vértices que solo tiene 2 vértices de grado 2 entonces $|E| \geqslant 2n - 2$.

Sean $v_1, v_2 \in V$ los vértices de grado 2. Por ser de Euler, tenemos que $\deg v$ es par para todo $v \in V$. Por tanto, como v_1 y v_2 son los únicos vértices de grado 2, tenemos que:

$$\deg v \geqslant 4 \ \forall v \in V \setminus \{v_1, v_2\}$$

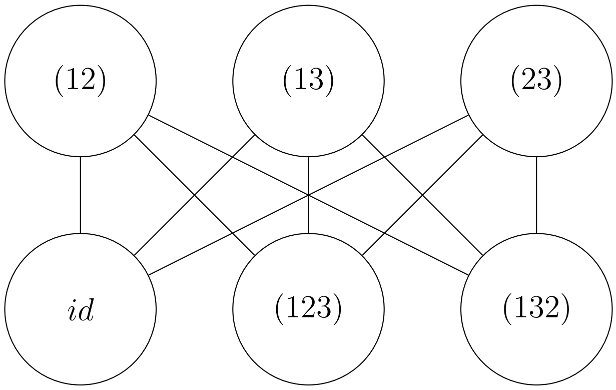


Figura 2.34: Grafo para el ejercicio 2.1.29.

Por tanto, tenemos que:

$$|E| = \frac{1}{2}\sum_{v\in V} \deg v = \frac{1}{2}\left(2+2+\sum_{v\in V\setminus\{v_1,v_2\}} \deg v\right)$$
$$\geqslant \frac{1}{2}\left(2+2+4(n-2)\right) = 2n-2$$

Ejercicio 2.1.29.

1. Considera el subconjunto $X = \{(12),(13),(23)\} \subset S_3$ y el siguiente grafo G: Los vértices de G son los elementos de S_3 y hay un lado entre dos vértices x e y si $xy^{-1} \in X$.

   a) Dibuja el grafo.
   Calculemos en primer lugar los lados. Dados $x, y \in S_3$, tenemos que:

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

   Veamos ahora que hay un lado entre dos vértices $x, y \in S_3$ si y solo si $\varepsilon(x) \neq \varepsilon(y)$.

   $\Rightarrow$) Supongamos que hay un lado entre $x, y \in S_3$; por lo que $xy^{-1} \in X$. Por tanto:

   $$\varepsilon(xy^{-1}) = \varepsilon(x)\varepsilon(y) \in \varepsilon(X) = \{-1\} \Longrightarrow \varepsilon(x) \neq \varepsilon(y)$$

   $\Leftarrow$) Supongamos que $\varepsilon(x) \neq \varepsilon(y)$. Por tanto, $\varepsilon(xy^{-1}) = \varepsilon(x)\varepsilon(y) = -1$. Como las únicas permutaciones de S_3 impares son las transposiciones, tenemos que $xy^{-1} \in X$.

   Por tanto, el grafo es el de la Figura 2.34. Tenemos efectivamente que se trata de $K_{3,3}$, siendo las dos particiones de S_3 los conjuntos de permutaciones con signatura par e impar, respectivamente.

   b) Calcula sus matrices de incidencia y adyacencia.
   Numeramos los vértices de G como sigue:

   $$\{(12),(13),(23),(id),(123),(132)\}$$

La matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

La matriz de incidencia es:

$$B = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

c) ¿Es de Euler o tiene un camino de Euler? En caso afirmativo aplica el algoritmo dado en clase para calcular un ciclo o un camino de Euler.

No es de Euler ni hay un camino de Euler, puesto que hay más de dos vértices de grado impar.

d) ¿Es de Hamilton? En caso afirmativo calcula el ciclo de Hamilton.

Sí es de Hamilton, puesto que para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 3 + 3 = 6 \geqslant 6 = |V|$$

Un posible ciclo de Hamilton es:

$$(id) \to (12) \to (123) \to (23) \to (132) \to (13) \to (id)$$

e) ¿Es plano? En caso afirmativo comprueba la fórmula de Euler.

No es plano, puesto que es el mismo $K_{3,3}$.

2. Si G es un grafo con n vértices y m lados. Prueba que $m \leqslant \frac{n(n-1)}{2}$ y que se da la igualdad si y solo si $G = K_n$ es el grafo completo.

Por el Lema del Apretón de Manos, sabemos que:

$$\sum_{v\in V} \deg v = 2|E| \Longrightarrow m = |E| = \frac{\sum\limits_{v\in V} \deg v}{2}$$

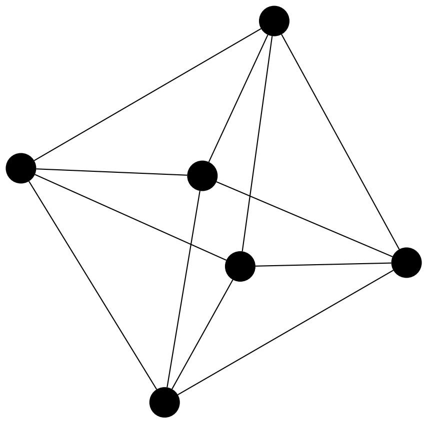


Figura 2.35: Octaedro para el ejercicio 2.1.30.

Por otro lado, sabemos que el grado máximo de un vértice en un grafo con n vértices es $n-1$ (ya que en caso contrario sería necesario que hubiese lados paralelos o lazos, algo que no consideramos). Por tanto, tenemos que:

$$m \leqslant \frac{\sum_{v\in V}(n-1)}{2} = \frac{\sum_{i=1}^{n}(n-1)}{2} = \frac{n(n-1)}{2}$$

Además, se da la igualdad si y solo si G es el grafo regular de n vértices y grado $n-1$, es decir, K_n.

Ejercicio 2.1.30. Demuestra, utilizando el algoritmo explicado en clase, que la sucesión gráfica asociada a un octaedro (poliedro regular con 6 vértices, 8 caras y 12 aristas) es gráfica y, utilizando dicho algoritmo, encuentra un grafo G en que los grados de sus vértices sean los términos de esa sucesión. Encuentra las matrices de adyacencia e incidencia de G.

Comprueba que el grafo G es plano y estudia si es de Euler y, en caso afirmativo, determina por algún algoritmo explicado en clase un circuito de Euler para G. ¿Es G un grafo de Hamilton? Razona la respuesta.

En primer lugar, dibujamos el octaedro, que se muestra en la Figura 2.35, para poder así obtener la sucesión gráfica asociada, que es:

$$4, 4, 4, 4, 4, 4$$

Aplicamos el Algoritmo de Havel-Hakimi, y obtenemos el grafo de la Figura 2.36.

4	4	4	4	4	4	Eliminamos el 4 y restamos uno a los 4 términos siguientes
	3	3	3	3	4	Reordenamos los términos
	4	3	3	3	3	Eliminamos el 4 y restamos uno a los 4 términos siguientes
		2	2	2	2	Eliminamos el 2 y restamos uno a los 2 términos siguientes
			1	1	2	Reordenamos los términos
			2	1	1	Eliminamos el 2 y restamos uno a los 2 términos siguientes
				0	0	

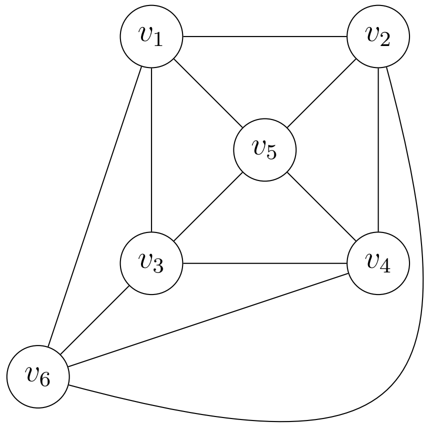


Figura 2.36: Grafo para el ejercicio 2.1.30.

La matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

La matriz de incidencia es:

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

El grafo es plano, puesto que se da una representación en la que no se cruzan aristas. Además, es de Euler, puesto que todos los vértices son de grado par. Un posible circuito de Euler es:

$$v_1 \to v_3 \to v_6 \to v_4 \to v_3 \to v_5 \to v_4 \to v_2 \to v_5 \to v_1 \to v_2 \to v_6 \to v_1$$

Además, el grafo también es de Hamilton, puesto que para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 4 + 4 = 8 \geqslant 6 = |V|$$

De hecho, un posible circuito de Hamilton es:

$$v_1 \to v_5 \to v_2 \to v_4 \to v_3 \to v_6 \to v_1$$

Ejercicio 2.1.31. Razona cuál es la respuesta correcta en cada una de las siguientes cuestiones (todos los grafos a los que se hace referencia son simples, no tienen lazos ni lados paralelos):

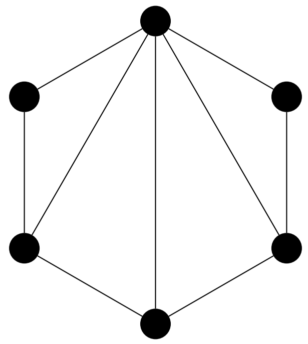


Figura 2.37: Grafo plano para el ejercicio 2.1.31.2.

1. La sucesión $70, 69, 68, \dots, 3, 2, 1$.

   a) Es una sucesión gráfica y su grafo asociado es el completo K_{70}.

   b) Es una sucesión gráfica pero su grafo asociado no es K_{70}.

   c) No es una sucesión gráfica.

   Supongamos que es gráfica. Entonces, tenemos que:

$$\sum_{v\in V} \deg v = \sum_{i=1}^{70} i = \frac{70 \cdot 71}{2} = 35 \cdot 71 \text{ impar}$$

   Por tanto, no puede ser gráfica, ya que la suma de los grados de los vértices debe ser par. Por tanto, la respuesta correcta es la **c)**.

2. Tengo un grafo conexo con 6 vértices y 9 lados:

   a) Puedo asegurar que es plano.

   b) Puedo asegurar que no es plano.

   c) Puede ser plano o no serlo.

   Tenemos que $|E| = 9 \leqslant 12 = 3|V| - 6$, por lo que puede ser plano. De hecho, el grafo de la Figura 2.37 es plano y $K_{3,3}$ no lo es, mientras que ambos son conexos con 6 vértices y 9 lados. Por tanto, la respuesta correcta es la **c)**.

3. La sucesión $4, 4, 4, 4$:

   a) No es una sucesión gráfica pero si le añadimos al final un 2 sí lo es.

   b) No es una sucesión gráfica pero si le añadimos al final un 3 sí lo es.

   c) No es una sucesión gráfica pero si le añadimos al final un 4 sí lo es.

   No es gráfica, puesto que si hay 4 vértices el mayor grado posible es 3. No obstante, si le añadimos un 4 al final, sí es gráfica, ya que es la sucesión correspondiente a K_5. Por tanto, la respuesta correcta es la **c)**.

4. Puedo encontrar un grafo plano conexo con:

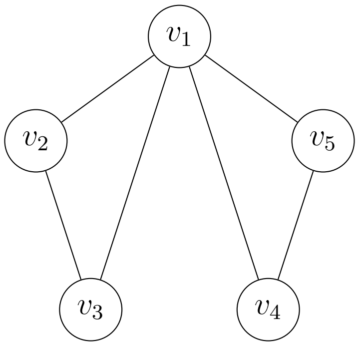


Figura 2.38: Grafo G del ejercicio 2.1.31.5.

a) Un número impar de vértices, un número impar de lados y un número impar de caras.

b) Un número par de vértices, un número par de lados y un número impar de caras.

c) Un número impar de vértices, un número par de lados y un número impar de caras.

Sabemos que:

$$|V| + |F| = 2 + |E|$$

Por tanto, de entre las tres opciones, la única que puede cumplir la fórmula de Euler es la **c)**.

5. La sucesión $4, 2, 2, 2, 2$:

a) Es la sucesión de grados de un grafo de Euler y de Hamilton.

b) Es la sucesión de grados de un grafo de Hamilton y no de Euler.

c) Es la sucesión de grados de un grafo de Euler y no de Hamilton.

El grafo de la Figura 2.38 tiene la sucesión de grados dada. Este es de Euler, con el circuito:

$$v_1 \to v_3 \to v_2 \to v_1 \to v_4 \to v_5 \to v_1$$

No obstante, no es de Hamilton. Por tanto, la respuesta correcta es la **c)**.

6. Un grafo regular de grado 7:

a) Tiene que tener al menos 8 vértices y un número impar de lados.

b) Tiene que tener al menos 8 vértices pero puede tener un número impar o par de lados.

c) Lo único que puedo afirmar sobre él es que tiene un número par de vértices.

Efectivamente, tiene que tener al menos 8 vértices. Respecto del número de lados, por el Lema del Apretón de Manos tenemos que:

$$2|E| = 7|V|$$

Por tanto, podemos afirmar que ha de tener un número par de vértices. El grafo K_8 es regular de grado 7 y tiene 28 lados. El grafo regular de grado 7 con 10 vértices tiene 35 aristas, por lo que la respuesta correcta es la **b)**.

Ejercicio 2.1.32. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle(1\ 2\ 3)\rangle$.

1. Construye el conjunto cociente $S_4/_{H}\!\sim$ de clases laterales por la izquierda xH.

   Por el Teorema de Lagrange, sabemos que:
$$[S_4 : H] = \frac{|S_4|}{|H|} = \frac{4!}{3} = 8$$
   Por tanto, hemos de encontrar 8 clases laterales por la izquierda distintas:
$$\begin{aligned}
1H &= \{1, (1\ 2\ 3), (1\ 3\ 2)\} = (1\ 2\ 3)H = (1\ 3\ 2)H\\
(1\ 2)H &= \{(1\ 2), (2\ 3), (1\ 3)\} = (2\ 3)H = (1\ 3)H\\
(1\ 4)H &= \{(1\ 4), (1\ 2\ 3\ 4), (1\ 3\ 2\ 4)\} = (1\ 2\ 3\ 4)H = (1\ 3\ 2\ 4)H\\
(2\ 4)H &= \{(2\ 4), (1\ 4\ 2\ 3), (1\ 3\ 4\ 2)\} = (1\ 4\ 2\ 3)H = (1\ 3\ 4\ 2)H\\
(3\ 4)H &= \{(3\ 4), (1\ 2\ 4\ 3), (1\ 4\ 3\ 2)\} = (1\ 2\ 4\ 3)H = (1\ 4\ 3\ 2)H\\
(1\ 2\ 4)H &= \{(1\ 2\ 4), (1\ 4)(2\ 3), (1\ 3\ 4)\} = (1\ 4)(2\ 3)H = (1\ 3\ 4)H\\
(1\ 4\ 2)H &= \{(1\ 4\ 2), (2\ 3\ 4), (1\ 3)(2\ 4)\} = (2\ 3\ 4)H = (1\ 3)(2\ 4)H\\
(1\ 4\ 3)H &= \{(1\ 4\ 3), (1\ 2)(3\ 4), (2\ 4\ 3)\} = (1\ 2)(3\ 4)H = (2\ 4\ 3)H
\end{aligned}$$
   Por tanto, el conjunto cociente es:
$$S_4/_{H}\!\sim = \{1H, (1\ 2)H, (1\ 4)H, (2\ 4)H, (3\ 4)H, (1\ 2\ 4)H, (1\ 4\ 2)H, (1\ 4\ 3)H\}$$

2. Para cada clase xH denotamos $m(xH)$ al máximo común divisor de los órdenes de los elementos en xH. Considera el grafo G con vértices las clases xH y en el que hay un lado entre xH e yH si $m(xH)$ divide a $m(yH)$ o $m(yH)$ divide a $m(xH)$. Identifica el grafo G dando la sucesión de grados de sus vértices y su matriz de adyacencia. ¿Es G de Euler, de Hamilton o plano?

   Calculamos $m(xH)$ para cada clase:
$$\begin{gathered}
m(1H) = m((1\ 2\ 4)H) = m((1\ 4\ 2)H) = m((1\ 4\ 3)H) = 1\\
m((1\ 2)H) = m((1\ 4)H) = m((2\ 4)H) = m((3\ 4)H) = 2
\end{gathered}$$
   Por tanto el grafo resultante es el grafo completo de 8 vértices; es decir, K_8. La sucesión de grados de sus vértices es:
$$\{D_0(K_8), D_1(K_8), \dots, D_7(K_8)\} = \{0, \dots, 0, 8\}$$
   Su matriz de adyacencia es:
$$A = \begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & 1 & 0 & 1 & 1 & 1 & 1 & 1\\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 1\\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1\\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 1\\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 1\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}$$

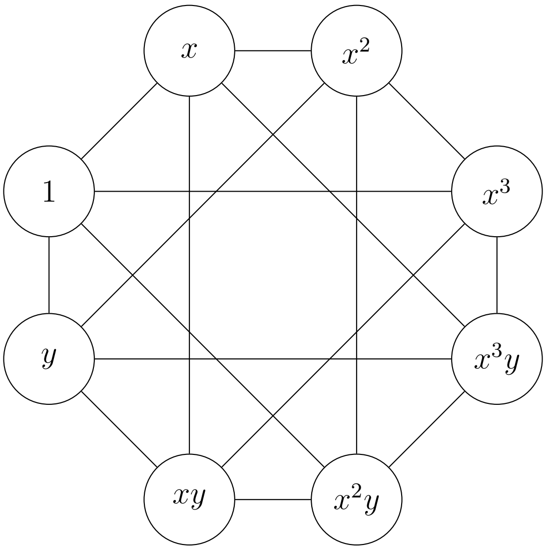


Figura 2.39: Grafo G del ejercicio 2.1.33.

No es de Euler, puesto que tiene vértices de grado impar. Tampoco es plano, puesto que puede contraerse a K_5. No obstante, sí es de Hamilton, puesto que para cada par de vértices no adyacentes, se verifica que:

$$\deg v_i + \deg v_j = 8 + 8 = 16 \geqslant 8 = |V|$$

De hecho, un posible ciclo de Hamilton es:

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

3. Considera el subgrafo G' obtenido a partir de G eliminando la clase $1H$, ¿es G' de Euler? En caso afirmativo aplica el algoritmo dado en clase para calcular un circuito de Euler.

   Tras eliminar la clase $1H$, obtenemos el grafo completo K_7, que es de Euler puesto que todos sus vértices tienen grado 6 (par).

Ejercicio 2.1.33. Se considera el grupo $Q_2^{\text{abs}} = \langle x, y \mid x^4 = 1, x^2 = y^2, yx = x^{-1}y \rangle$ y el grafo G cuyos vértices son los elementos de Q_2^{abs} y en el que, para cualquier $a \in Q_2^{\text{abs}}$, hay un lado entre a y ax y también un lado entre a y ay.

1. Comprueba que G es un grafo regular dando la sucesión de grados de sus vértices y calcula su matriz de adyacencia.

   Calculamos los elementos de Q_2^{abs}:

   $$Q_2 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$$

   El grafo es el de la Figura 2.39.

La matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Por tanto, su sucesión de grados es:

$$0, 0, 0, 0, 8, 0, 0, 0$$

Se trata por tanto de un grafo regular de grado 4 y 8 vértices. En particular, vemos que se trata de $K_{4,4}$, con la descomposición:

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

2. Razona si G es un grafo de Hamilton o plano.

   Para cada par de vértices no adyacentes, se verifica que:

   $$\deg v_i + \deg v_j = 4 + 4 = 8 \geqslant 8 = |V|$$

   Por tanto, G es de Hamilton, con un posible circuito:

   $$1 \to x \to x^2 \to x^3 \to x^3y \to x^2y \to xy \to y \to 1$$

   No obstante, no es plano, ya que $K_{4,4}$ puede contraerse a $K_{3,3}$.

3. Razona si G es un grafo de Euler y, en caso afirmativo, aplica el algoritmo dado en clase para calcular un circuito de Euler.

   Sí es de Euler, puesto que todos los vértices son de grado par. Un posible circuito de Euler es:

   $$\begin{aligned} 1 \to x \to x^2 \to x^3 \to x^3y \to x^2y \to xy \to y \to 1 \to x^3 \to xy \to x \to \\ \to x^3y \to y \to x^2 \to x^2y \to 1 \end{aligned}$$

Ejercicio 2.1.34. Se considera el grupo $D_4 = \langle r, s \mid r^4 = 1, s^2 = 1, sr = r^{-1}s \rangle$ y el grafo G cuyos vértices son los elementos de D_4 y en el que, para cualquier $a \in D_4$, hay un lado entre a y ar y también un lado entre a y as.

1. Comprueba que G es un grafo regular dando la sucesión de grados de sus vértices y calcula su matriz de adyacencia.

   Calculamos los elementos de D_4:

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

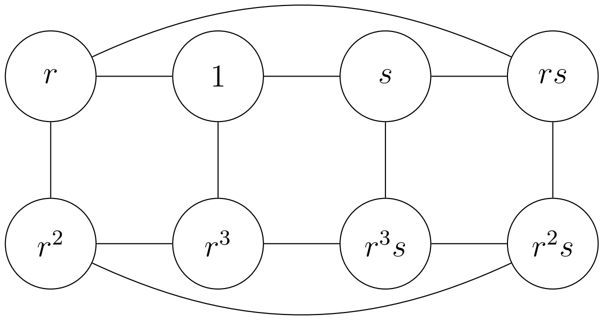


Figura 2.40: Grafo G del ejercicio 2.1.34.

El grafo es el de la Figura 2.40.

Su matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Por tanto, su sucesión de grados es:

$$0, 0, 0, 8, 0, 0, 0, 0$$

Se trata por tanto de un grafo regular de grado 3 y 8 vértices.

2. Razona si G es un grafo de Hamilton o plano.

   Sí es de Hamilton, con un posible circuito:

   $$1 \to r \to r^2 \to r^3 \to r^3s \to r^2s \to rs \to s \to 1$$

   Además, en la Figura 2.40 se puede ver que G es plano.

3. Razona si G es un grafo de Euler y, en caso afirmativo, aplica el algoritmo dado en clase para calcular un circuito de Euler.

   No es de Euler, puesto que hay más de dos vértices de grado impar.

Ejercicio 2.1.35. Se considera el grupo $D_5 = \langle r, s \mid r^5 = 1, s^2 = 1, sr = r^{-1}s \rangle$ y el grafo G cuyos vértices son los elementos de D_5 y en el que, para cualquier $a \in D_5$, hay un lado entre a y ar y también un lado entre a y as.

1. Calcula la sucesión de grados de G y razona si G es un grafo de Euler, de Hamilton o plano.

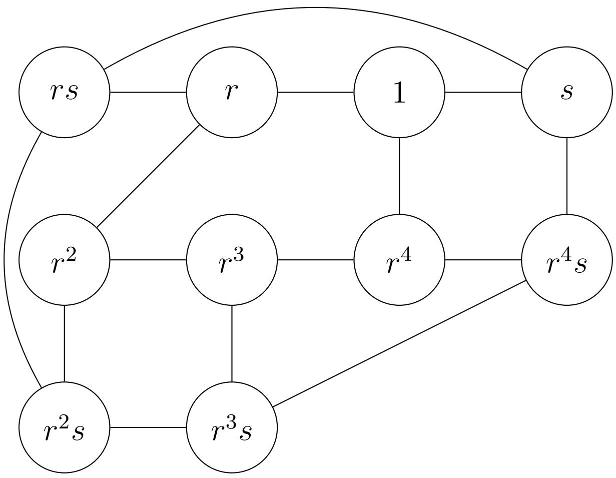


Figura 2.41: Grafo G del ejercicio 2.1.35.

Calculamos los elementos de D_5:

$$D_5 = \{1, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$$

El grafo es el de la Figura 2.41.

Tenemos que la sucesión de grados es:

$$0, 0, 0, 10, 0, 0, 0, 0, 0, 0, 0$$

Por tanto, se trata de un grafo regular de grado 3 y 10 vértices. Como hay más de dos vértices de grado impar, no es de Euler ni hay un camino de Euler. Además, en la Figura 2.41 se puede ver que G es plano. También es de Hamilton, con un posible circuito:

$$rs \to r^2s \to r^3s \to r^4s \to r^4 \to r^3 \to r^2 \to r \to 1 \to s \to rs$$

2. Considera un nuevo grafo G' obtenido añadiendo a G un nuevo vértice adyacente a todos los de G. Razona si G' es un grafo de Euler y, en caso afirmativo, aplica algún algoritmo dado en clase para calcular un circuito de Euler.

El grafo G' sí será de Euler, puesto que todos los vértices anteriores tendrán grado 4 y el nuevo vértice tendrá grado 10. Por tanto, será de Euler.

Ejercicio 2.1.36. Razona cuál es la respuesta correcta en cada una de las siguientes cuestiones. Todos los grafos a los que se hace referencia son simples (es decir, no tienen lazos ni lados paralelos).

1. La matriz

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

es la de adyacencia de un grafo que:

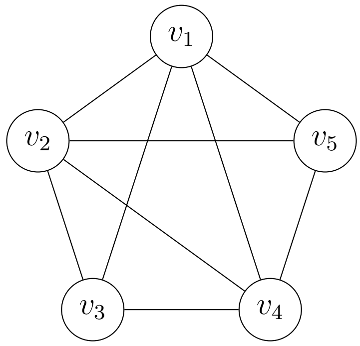


Figura 2.42: Grafo del ejercicio 2.1.36.1.

a) Es de Euler.

b) No es de Hamilton.

c) Es plano.

El grafo en cuestión se encuentra en la Figura 2.42. Sabemos que no es de Euler por tener vértices de grado impar. No obstante, sí es de Hamilton, con el circuito:

$$v_1 \to v_2 \to v_3 \to v_4 \to v_5 \to v_1 \to v_3 \to v_5 \to v_4 \to v_2 \to v_1$$

Por último, veamos si es plano sabiendo que $|E| = 9$ y $|V| = 5$. Como $|V| = 5 < 6$, ningún subgrafo suyo se puede contraer a $K_{3,3}$; y como $|E| = 9 < 10$, no se puede contraer a K_5; y por tanto es plano. Por tanto, la respuesta correcta es la **c)**.

2. Un grafo plano conexo regular de grado 8 con 23 caras:

a) No existe.

b) Tiene 12 aristas.

c) Tiene 9 vértices.

Por ser un grafo plano conexo, sabemos que:

$$|V| + 23 = 2 + |E|$$

Por ser regular de grado 8, sabemos que:

$$2|E| = 8|V| \Longrightarrow |E| = 4|V|$$

Por tanto, sustituyendo en la primera ecuación, obtenemos:

$$|V| + 23 = 2 + 4|V| \Longrightarrow 3|V| = 21$$

Por tanto, $|V| = 7$; pero esto no es posible si es regular de grado 8. Por tanto, la respuesta correcta es la **a)**.

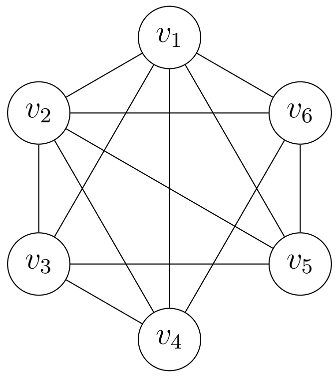


Figura 2.43: Grafo del ejercicio 2.1.36.4.

3. Se tiene que:

   a) Un grafo que es de Euler y de Hamilton siempre es plano.

   b) Un grafo que es plano y de Euler siempre es de Hamilton.

   c) Ninguna de las respuestas anteriores es cierta.

   La opción a) es falsa, y como contraejemplo podemos emplear K_5, que es de Euler y de Hamilton, pero no es plano. La opción b) es falsa, y como contraejemplo podemos emplear el grafo de la Figura 2.38, que es plano y de Euler, pero no es de Hamilton. Por tanto, la respuesta correcta es la **c)**.

4. Se tiene que:

   a) La sucesión $5, 5, 4, 2, 2, 2$ es la sucesión gráfica de un grafo plano.

   b) La sucesión $5, 5, 4, 4, 4, 4$ es la sucesión gráfica de un grafo de Hamilton.

   c) La sucesión $5, 4, 4, 3, 3, 3$ es la sucesión gráfica de un grafo de Euler.

   En primer lugar, la sucesión de la opción a) no es gráfica, por lo que esta opción no es correcta. La sucesión de la opción c) tampoco es gráfica (puesto que el número de vértices de grado impar debe ser par), por lo que tampoco es correcta. Para comprobar que la sucesión de la opción b) es la asociada a un grafo de Hamilton, lo vemos representado en la Figura 2.43, y el circuito de Hamilton es:

$$v_1 \to v_2 \to v_3 \to v_4 \to v_6 \to v_5 \to v_1$$

Ejercicio 2.1.37. Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle(1\ 2\ 3)\rangle$.

1. Construye el conjunto cociente $S_4/\sim_H$ de clases laterales por la derecha Hx, $x \in S_4$.

   Por el Teorema de Lagrange, sabemos que:

$$[S_4 : H] = |S_4/\sim_H| = \frac{|S_4|}{|H|} = \frac{4!}{3} = 8$$

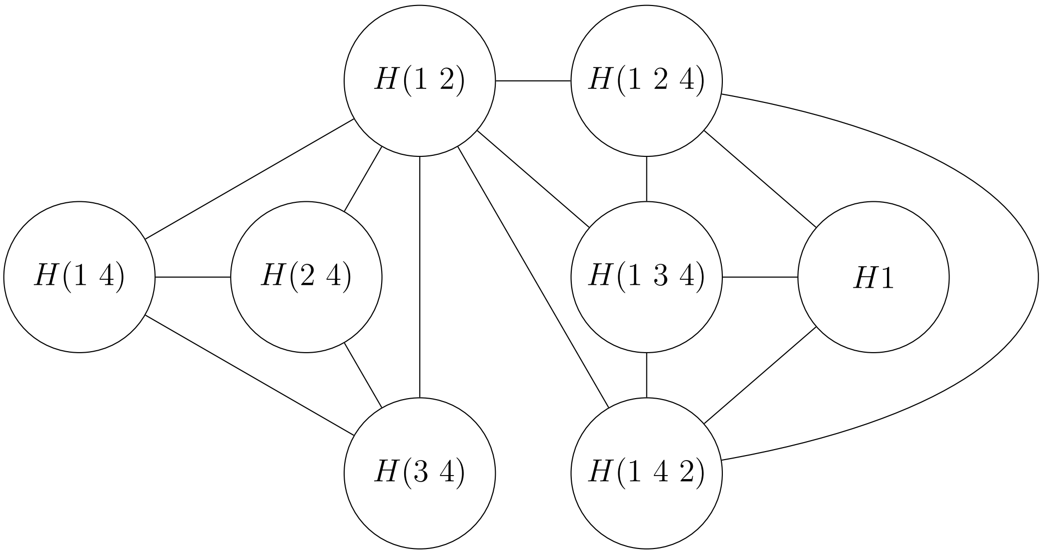


Figura 2.44: Grafo G del ejercicio 2.1.37.

Por tanto, hemos de encontrar 8 clases laterales por la derecha distintas:

$$\begin{aligned}
H1 &= \langle (1\ 2\ 3) \rangle = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H(1\ 2\ 3) = H(1\ 3\ 2)\\
H(1\ 2) &= \{(1\ 2), (1\ 3), (2\ 3)\} = H(1\ 3) = H(2\ 3)\\
H(1\ 4) &= \{(1\ 4), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\} = H(1\ 4\ 2\ 3) = H(1\ 4\ 3\ 2)\\
H(2\ 4) &= \{(2\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4)\} = H(1\ 2\ 4\ 3) = H(1\ 3\ 2\ 4)\\
H(3\ 4) &= \{(3\ 4), (1\ 2\ 3\ 4), (1\ 3\ 4\ 2)\} = H(1\ 2\ 3\ 4) = H(1\ 3\ 4\ 2)\\
H(1\ 2\ 4) &= \{(1\ 2\ 4), (1\ 3)(2\ 4), (2\ 4\ 3)\} = H(1\ 3)(2\ 4) = H(2\ 4\ 3)\\
H(1\ 3\ 4) &= \{(1\ 3\ 4), (2\ 3\ 4), (1\ 2)(3\ 4)\} = H(2\ 3\ 4) = H(1\ 2)(3\ 4)\\
H(1\ 4\ 2) &= \{(1\ 4\ 2), (1\ 4\ 3), (1\ 4)(2\ 3)\} = H(1\ 4\ 3) = H(1\ 4)(2\ 3)
\end{aligned}$$

Por tanto, el conjunto cociente es:

$$S_4/\sim_H = \{H1, H(1\ 2), H(1\ 4), H(2\ 4), H(3\ 4), H(1\ 2\ 4), H(1\ 3\ 4), H(1\ 4\ 2)\}$$

2. Para cada clase Hx denotamos $n(Hx)$ al mínimo común múltiplo de los órdenes de los elementos en Hx. Considera el grafo G con vértices las clases Hx y en el que hay un lado entre Hx e Hy si $n(Hx)$ divide a $n(Hy)$ o $n(Hy)$ divide a $n(Hx)$. Identifica el grafo G dando la sucesión de grados de sus vértices y su matriz de adyacencia. ¿Es G de Euler, de Hamilton o plano?

   Tenemos que:

$$\begin{gathered}
n(H1) = 3 \qquad n(H(1\ 2)) = 2\\
n(H(1\ 4)) = n(H(2\ 4)) = n(H(3\ 4)) = 4\\
n(H(1\ 2\ 4)) = n(H(1\ 3\ 4)) = n(H(1\ 4\ 2)) = 6
\end{gathered}$$

   El grafo es el de la Figura 2.44.

   La sucesión de grados de dicho grafo G es:

$$\{D_0(G), D_1(G), D_2(G), D_3(G), D_4(G), D_5(G), D_6(G), D_7(G)\} = \{0, 0, 0, 4, 3, 0, 1, 0\}$$

Su matriz de Adyacencia, considerando la numeración

$$H1, H(1\ 2), H(1\ 4), H(2\ 4), H(3\ 4), H(1\ 2\ 4), H(1\ 3\ 4), H(1\ 4\ 2)$$

es la siguiente:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Como vemos, este grafo sí es plano. Además, como tiene vértices de grado impar, no es de Euler. Por último, tampoco es de Hamilton, pues el vértice $H(1\ 2)$ divide al grafo en dos componentes conexas, por lo que habría que pasar por él dos veces para hacer un circuito de Hamilton.

3. Considera, si es posible, un subgrafo G' de G obtenido al suprimir una arista entre dos vértices de G de grado impar. ¿Es G' de Euler? ¿Hay un camino de Euler entre dos vértices de G'? En caso afirmativo aplica algún algoritmo dado en clase para calcular un circuito o camino de Euler en G'.

Supongamos que quitamos la arista entre $H(2\ 4)$ y $H(1\ 4)$. Entonces, todos los vértices de G' tendrán grado par a excepción de dos de ellos, $H(3\ 4)$ y $H1$. Por tanto, G' no es de Euler pero sí admite un camino de Euler entre esos dos nodos. Este por ejemplo sería:

$$H(3\,4) \to H(1\,2) \to H(1\,4) \to H(3\,4) \to H(2\,4) \to H(1\,2) \to H(1\,4\,2) \to H1 \to$$
$$\to H(1\,3\,4) \to H(1\,4\,2) \to H(1\,2\,4) \to H(1\,3\,4) \to H(1\,2) \to H(1\,2\,4) \to H1$$

Ejercicio 2.1.38. Se considera el grupo A_4 y su subgrupo $H = \langle(1\ 2)(3\ 4)\rangle$. Se considera el grafo G con vértices las clases laterales por la izquierda de H en A_4, xH, y en el que hay un lado entre xH e yH si $m(xH)$ divide a $m(yH)$ o $m(yH)$ divide a $m(xH)$, donde $m(Hx)$ denota el máximo común divisor de los órdenes de los elementos en xH. Razone cuál de las siguientes es la respuesta correcta:

a) G es plano pero no es de Hamilton.

b) G no es plano y tiene dos vértices conectados por un camino de Euler.

c) G es de Hamilton pero no es de Euler.

Por el Teorema de Lagrange, sabemos que:

$$[A_4 : H] = |A_4/_H\!\sim| = \frac{|A_4|}{|H|} = \frac{12}{2} = 6$$

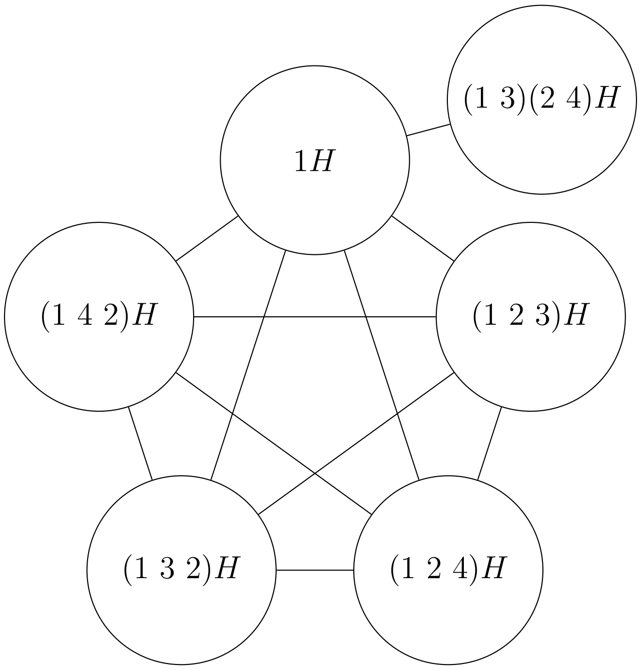


Figura 2.45: Grafo G del ejercicio 2.1.38.

Por tanto, hemos de encontrar 6 clases laterales por la izquierda distintas:

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

Por tanto, el conjunto cociente es:

$$A_4/{}_H\!\sim\, = \{1H, (1\ 3)(2\ 4)H, (1\ 2\ 3)H, (1\ 2\ 4)H, (1\ 3\ 2)H, (1\ 4\ 2)H\}$$

Tenemos que:

$$m(1H) = 1 \qquad m((1\ 3)(2\ 4)H) = 2$$
$$m((1\ 2\ 3)H) = m((1\ 2\ 4)H) = m((1\ 3\ 2)H) = m((1\ 4\ 2)H) = 3$$

El grafo es el de la Figura 2.45. Sabemos que no es de Hamilton por tener un vértice de grado 1. Además, no es plano, pues un subgrafo suyo es K_5. Aunque no es de Euler por tener vértices de grado impar, sí tiene un camino de Euler entre $(1\ 3)(2\ 4)H$ y $1H$, puesto que son los únicos vértices de grado impar. Por tanto, la respuesta correcta es la **b)**.

Ejercicio 2.1.39 (Extraordinaria DGIIM 2024/2025)**.** Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle(1\ 2\ 3\ 4)\rangle$.

1. Construye el conjunto cociente $S_4/{}_H\!\sim$ de clases laterales por la izquierda xH. ¿Es $H < S_4$?

Por el Teorema de Lagrange, sabemos que:

$$[S_4 : H] = |S_4/_H\sim| = \frac{|S_4|}{|H|} = \frac{4!}{4} = 6$$

Por tanto, hemos de encontrar 6 clases laterales por la izquierda distintas:

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

Por tanto, el conjunto cociente es:

$$S_4/_H\sim = \{1H, (1\ 2)H, (1\ 3)H, (1\ 4)H, (2\ 3)H, (3\ 4)H\}$$

2. Para cada clase xH denotamos $m(xH)$ al máximo común divisor de los órdenes de los elementos en xH. Considera el grafo G con vértices las clases xH y en el que hay un lado entre dos clases xH e yH si $m(xH) = m(yH)$. Identifica el grafo G dando la sucesión de grados de sus vértices y su matriz de adyacencia. ¿Es G de Euler, de Hamilton o plano?

   Calculamos $m(xH)$ para cada clase:

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

   Por tanto, el grafo consiste de K_5 con un vértice adicional ($(1\ 3)H$) aislado. Por tanto, el grafo no es plano, ni de Euler ni de Hamilton. La sucesión de grados de dicho grafo G es:

$$\{D_0(G), D_1(G), D_2(G), D_3(G), D_4(G), D_5(G)\} = \{1, 0, 0, 0, 5, 0\}$$

   Su matriz de Adyacencia, considerando la numeración

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

   es la siguiente:

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

   Podemos ver que se trata de K_5 con un vértice aislado. Por tanto, es plano, pero no es de Euler ni de Hamilton.

3. Considera el subgrafo G' obtenido a partir de G eliminando la clase $(13)H$. ¿Es G' de Euler?

   El grafo resultante es K_5, que sabemos que sí es de Euler.

Ejercicio 2.1.40. Razona cuál es la respuesta correcta en cada una de las siguientes cuestiones. Todos los grafos a los que se hace referencia son simples (es decir, no tienen lazos ni lados paralelos).

1. Se tiene que:

   a) Hay un grafo conexo regular de grado 6 con 22 caras y 24 aristas.

   Como menciona caras, suponemos que es plano. Por tanto, tenemos que:

   $$|V| + 22 = 2 + 24 \Longrightarrow |V| = 4$$

   Comprobemos ahora que se cumple el Lema del Apretón de Manos:

   $$\sum_{v \in V} \deg v = 6 \cdot |V| = 24 \neq 48 = 2 \cdot |E|$$

   Por tanto, esta opción no es correcta.

   b) La sucesión $4, 4, 4, 3, 3$ es la sucesión gráfica de un grafo plano que tiene un camino de Euler entre dos vértices.

   Esta opción es correcta; ya que se trata de K_5 quitándole una arista. Como K_5 es de Euler, el camino buscado será el ciclo de Euler de K_5 sin cerrarlo.

   c) Un grafo conexo y plano es de Euler si y solo si es de Hamilton.

   Esta opción es incorrecta, puesto que K_4 es conexo, plano y de Hamilton, pero no es de Euler.

2. La matriz

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

   es la de adyacencia de un grafo:

   a) Con 11 aristas y que es de Euler y de Hamilton.

   b) Que es conexo y plano pero no de Hamilton.

   c) Que no es de Hamilton ni plano ni de Euler.

   El grafo descrito es K_5 al que le hemos añadido un vértice adicional conectado mediante una única arista a uno de los vértices de K_5. Como dicho vértice tiene grado 1, entonces el grafo no es de Euler ni de Hamilton. Además, como un subgrafo suyo es K_5, en particular dicho subgrafo se puede contraer a K_5, por lo que tampoco es plano. Por tanto, la opción correcta es la **c)**.

Ejercicio 2.1.41 (Parcial DGIIM 2024/25)**.** Considera el grupo simétrico S_4 y el subgrupo suyo $H = \langle(1\ 3\ 4)\rangle$.

1. Construye el conjunto cociente $S_4/\sim_H$ de clases laterales por la derecha Hx, $x \in S_4$.

   Por el Teorema de Lagrange, sabemos que:

$$[S_4 : H] = |S_4/\sim_H| = \frac{|S_4|}{|H|} = \frac{4!}{3} = 8$$

   Por tanto, hemos de encontrar 8 clases laterales por la derecha distintas:

$$\begin{aligned}
H1 &= \{1, (1\ 3\ 4), (1\ 4\ 3)\} = H(1\ 3\ 4) = H(1\ 4\ 3)\\
H(1\ 2) &= \{(1\ 2), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3)\} = H(1\ 2\ 3\ 4) = H(1\ 2\ 4\ 3)\\
H(1\ 3) &= \{(1\ 3), (1\ 4), (3\ 4)\} = H(1\ 4) = H(3\ 4)\\
H(2\ 3) &= \{(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 3\ 2)\} = H(1\ 3\ 2\ 4) = H(1\ 4\ 3\ 2)\\
H(2\ 4) &= \{(2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3)\} = H(1\ 3\ 4\ 2) = H(1\ 4\ 2\ 3)\\
H(1\ 2\ 3) &= \{(1\ 2\ 3), (1\ 2\ 4), (1\ 2)(3\ 4)\} = H(1\ 2\ 4) = H(1\ 2)(3\ 4)\\
H(1\ 3\ 2) &= \{(1\ 3\ 2), (1\ 4)(2\ 3), (2\ 4\ 3)\} = H(1\ 4)(2\ 3) = H(2\ 4\ 3)\\
H(1\ 4\ 2) &= \{(1\ 4\ 2), (2\ 3\ 4), (1\ 3)(2\ 4)\} = H(2\ 3\ 4) = H(1\ 3)(2\ 4)
\end{aligned}$$

   Por tanto, el conjunto cociente es:

$$S_4/\sim_H = \{H1, H(1\ 2), H(1\ 3), H(2\ 3), H(2\ 4), H(1\ 2\ 3), H(1\ 3\ 2), H(1\ 4\ 2)\}$$

2. Para cada clase Hx denotamos $n(Hx)$ al mínimo común múltiplo de los órdenes de los elementos en Hx. Considera el grafo G con vértices las clases Hx y en el que hay un lado entre Hx y Hy si $n(Hx)$ divide a $n(Hy)$ o $n(Hy)$ divide a $n(Hx)$. Identifica el grafo G dando la sucesión de grados de sus vértices y su matriz de adyacencia.

   Calculamos $n(Hx)$ para cada clase:

$$\begin{gathered}
n(H1) = 3 \qquad n(H(1\ 3)) = 2\\
n(H(1\ 2)) = n(H(2\ 3)) = n(H(2\ 4)) = 4\\
n(H(1\ 2\ 3)) = n(H(1\ 3\ 2)) = n(H(1\ 4\ 2)) = 6
\end{gathered}$$

   El grafo es el de la Figura 2.46.

   La sucesión de grados de dicho grafo G es:

$$\{D_0(G), D_1(G), D_2(G), D_3(G), D_4(G), D_5(G), D_6(G), D_7(G)\} = \{0, 0, 0, 4, 3, 0, 1, 0\}$$

   Su matriz de Adyacencia, considerando la numeración

$$H1, H(1\ 3), H(2\ 4), H(1\ 2), H(2\ 3), H(1\ 2\ 3), H(1\ 3\ 2), H(1\ 4\ 2)$$

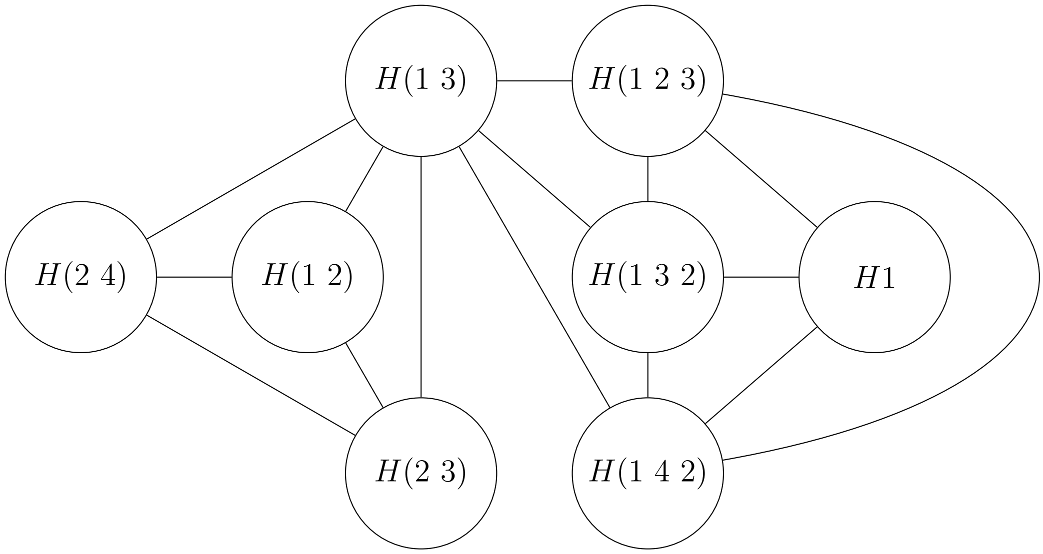


Figura 2.46: Grafo G del ejercicio 2.1.41.

es la siguiente:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

3. ¿Hay alguna condición suficiente que asegure que G es de Hamilton? ¿Y necesaria para ser plano? ¿Es G de Euler, de Hamilton o plano?

   No, no verifica ninguna de las dos, puesto que G no es de Hamilton. No obstante, sí es plano, por lo que verifica las condiciones necesarias para ser plano. Por último, puesto que tiene vértices de grado impar, no es de Euler.

4. Considera el subgrafo G' de G obtenido al suprimir la arista entre las clases $H(2\ 3)$ y $H(2\ 4)$. ¿Es G' de Hamilton, plano o de Euler? ¿Hay un camino de Euler entre dos vértices de G'? En caso afirmativo aplica algún algoritmo dado en clase para calcular un circuito o camino de Euler en G'.

   Sigue sin ser de Euler ni de Hamilton, aunque sí es plano. De nuevo, sí hay un camino de Euler entre $H(1\ 2)$ y $H1$. Este sería:

$$H(1\,2) \to H(2\,4) \to H(1\,3) \to H(1\,2) \to H(2\,3) \to H(1\,3) \to H(1\,4\,2) \to H1 \to$$
$$\to H(1\,3\,2) \to H(1\,4\,2) \to H(1\,2\,3) \to H(1\,3) \to H(1\,3\,2) \to H(1\,2\,3) \to H1$$

2.2. Grupos: generalidades y ejemplos

Ejercicio 2.2.1. Describir explícitamente la tabla de multiplicar de los grupos $\mathbb{Z}_n^\times$ para $n = 4$, $n = 6$ y $n = 8$, donde por $\mathbb{Z}_n^\times$ denotamos al grupo de las unidades del anillo $\mathbb{Z}_n$.

Sabemos que, fijado $n \in \mathbb{N}$, las unidades del anillo $\mathbb{Z}_n$ son:

$$\mathcal{U}(\mathbb{Z}_n) = \mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid \text{mcd}(a, n) = 1\}$$

Describimos entonces a continuación las tablas de multiplicar de los grupos $\mathbb{Z}_4^\times$, $\mathbb{Z}_6^\times$ y $\mathbb{Z}_8^\times$.

- Para $n = 4$:

$\cdot$	1	3
1	1	3
3	3	1

- Para $n = 6$:

$\cdot$	1	5
1	1	5
5	5	1

- Para $n = 8$:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Ejercicio 2.2.2. Describir explícitamente la tabla de multiplicar de los grupos $\mathbb{Z}_p^\times$ para $p = 2$, $p = 3$, $p = 5$ y $p = 7$.

- Para $p = 2$:

$\cdot$	1
1	1

- Para $p = 3$:

$\cdot$	1	2
1	1	2
2	2	1

- Para $p = 5$:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- Para $p = 7$:

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Ejercicio 2.2.3. Calcular el inverso de 7 en los grupos $\mathbb{Z}_{11}^{\times}$ y $\mathbb{Z}_{37}^{\times}$.

Para calcular el inverso de un elemento a en un grupo $\mathbb{Z}_n^{\times}$, basta con encontrar un elemento b tal que $ab = 1$ en $\mathbb{Z}_n$.

- Para $\mathbb{Z}_{11}^{\times}$:

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

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

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

Ejercicio 2.2.4. Describir explícitamente los grupos μ_n (de raíces n-ésimas de la unidad) para $n = 3$, $n = 4$ y $n = 8$, dando su tabla de multiplicar.

- Para $n = 3$:

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

$\cdot$	1	ξ_3	ξ_3^2
1	1	ξ_3	ξ_3^2
ξ_3	ξ_3	ξ_3^2	1
ξ_3^2	ξ_3^2	1	ξ_3

- Para $n = 4$:

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

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

- Para $n = 8$:

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

$\cdot$	1	ξ_8	ξ_8^2	ξ_8^3	ξ_8^4	ξ_8^5	ξ_8^6	ξ_8^7
1	1	ξ_8	i	ξ_8^3	-1	ξ_8^5	$-i$	ξ_8^7
ξ_8	ξ_8	i	ξ_8^3	-1	ξ_8^5	$-i$	ξ_8^7	1
ξ_8^2	i	ξ_8^3	-1	ξ_8^5	$-i$	ξ_8^7	1	ξ_8
ξ_8^3	ξ_8^3	-1	ξ_8^5	$-i$	ξ_8^7	1	ξ_8	i
ξ_8^4	-1	ξ_8^5	$-i$	ξ_8^7	1	ξ_8	i	ξ_8^3
ξ_8^5	ξ_8^5	$-i$	ξ_8^7	1	ξ_8	i	ξ_8^3	-1
ξ_8^6	$-i$	ξ_8^7	1	ξ_8	i	ξ_8^3	-1	ξ_8^5
ξ_8^7	ξ_8^7	1	ξ_8	i	ξ_8^3	-1	ξ_8^5	$-i$

Ejercicio 2.2.5. En el conjunto $\mathbb{Q}^\times := \{q \in \mathbb{Q} \mid q \neq 0\}$ de los números racionales no nulos, se considera la operación de división, dada por $(x, y) \mapsto {}^x\!/\!_y = xy^{-1}$. ¿Nos da esta operación una estructura de grupo en $\mathbb{Q}^\times$?

Veamos qué condiciones han de cumplirse para que se tenga la propiedad asociativa. Sean $a, b, c \in \mathbb{Q}^\times$, entonces:

$$\frac{{}^a\!/\!_b}{c} = \frac{a}{{}^b\!/\!_c} \iff \frac{a}{bc} = \frac{ac}{b} \iff ab = abc^2 \iff 1 = c^2$$

Por tanto, tomando por ejemplo $2, 3, 4 \in \mathbb{Q}^\times$ no se tiene la propiedad asociativa, por lo que no se tiene un grupo.

Ejercicio 2.2.6. Sea G un grupo en el que $x^2 = 1$ para todo $x \in G$. Demostrar que el grupo G es abeliano.

Dados $x, y \in G$, se tiene que:

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

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

Ejercicio 2.2.7. Sea G un grupo. Demostrar que son equivalentes:

1. G es abeliano.
2. $\forall x, y \in G$ se verifica que $(xy)^2 = x^2y^2$.
3. $\forall x, y \in G$ se verifica que $(xy)^{-1} = x^{-1}y^{-1}$.

Demostración.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

Ejercicio 2.2.8. Demostrar que si en un grupo G, $x, y \in G$ verifican que $xy = yx$ entonces, para todo $n \in \mathbb{N} \setminus \{0\}$, se tiene que $(xy)^n = x^ny^n$.

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 $n + 1$.

$$\begin{aligned}(xy)^{n+1} &= (xy)^n(xy) = x^ny^nxy \\ &= x^nxy^nx = x^{n+1}y^{n+1}\end{aligned}$$

Por tanto, por inducción, se tiene que $(xy)^n = x^ny^n$ para todo $n \in \mathbb{N} \setminus \{0\}$.

Ejercicio 2.2.9. 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:

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

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 $f^{-1} \circ f = \mathrm{Id}_{\mathbb{R}}$):

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

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

Ejercicio 2.2.10.

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

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

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

   Por tanto, los elementos de $\operatorname{GL}_2(\mathbb{Z}_2)$ 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 2.2.11. Dar las tablas de grupo para los grupos D_3, D_4, D_5 y D_6.

Recordamos que:

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

- Para D_3:

$\cdot$	1	r	r^2	s	sr	sr^2
1	1	r	r^2	s	sr	sr^2
r	r	r^2	1	sr^2	s	sr
r^2	r^2	1	r	sr	sr^2	s
s	s	sr	sr^2	1	r	r^2
sr	sr	sr^2	s	r^2	1	r
sr^2	sr^2	s	sr	r	r^2	1

- Para D_4:

$\cdot$	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

- Para D_5:

$\cdot$	1	r	r^2	r^3	r^4	s	sr	sr^2	sr^3	sr^4
1	1	r	r^2	r^3	r^4	s	sr	sr^2	sr^3	sr^4
r	r	r^2	r^3	r^4	1	sr^4	s	sr	sr^2	sr^3
r^2	r^2	r^3	r^4	1	r	sr^3	sr^4	s	sr	sr^2
r^3	r^3	r^4	1	r	r^2	sr^2	sr^3	sr^4	s	sr
r^4	r^4	1	r	r^2	r^3	sr	sr^2	sr^3	sr^4	s
s	s	sr	sr^2	sr^3	sr^4	1	r	r^2	r^3	r^4
sr	sr	sr^2	sr^3	sr^4	s	r^4	1	r	r^2	r^3
sr^2	sr^2	sr^3	sr^4	s	sr	r^3	r^4	1	r	r^2
sr^3	sr^3	sr^4	s	sr	sr^2	r^2	r^3	r^4	1	r
sr^4	sr^4	s	sr	sr^2	sr^3	r	r^2	r^3	r^4	1

- Para D_6:

$\cdot$	1	r	r^2	r^3	r^4	r^5	s	sr	sr^2	sr^3	sr^4	sr^5
1	1	r	r^2	r^3	r^4	r^5	s	sr	sr^2	sr^3	sr^4	sr^5
r	r	r^2	r^3	r^4	r^5	1	sr^5	s	sr	sr^2	sr^3	sr^4
r^2	r^2	r^3	r^4	r^5	1	r	sr^4	sr^5	s	sr	sr^2	sr^3
r^3	r^3	r^4	r^5	1	r	r^2	sr^3	sr^4	sr^5	s	sr	sr^2
r^4	r^4	r^5	1	r	r^2	r^3	sr^2	sr^3	sr^4	sr^5	s	sr
r^5	r^5	1	r	r^2	r^3	r^4	sr	sr^2	sr^3	sr^4	sr^5	s
s	s	sr	sr^2	sr^3	sr^4	sr^5	1	r	r^2	r^3	r^4	r^5
sr	sr	sr^2	sr^3	sr^4	sr^5	s	r^5	1	r	r^2	r^3	r^4
sr^2	sr^2	sr^3	sr^4	sr^5	s	sr	r^4	r^5	1	r	r^2	r^3
sr^3	sr^3	sr^4	sr^5	s	sr	sr^2	r^3	r^4	r^5	1	r	r^2
sr^4	sr^4	sr^5	s	sr	sr^2	sr^3	r^2	r^3	r^4	r^5	1	r
sr^5	sr^5	s	sr	sr^2	sr^3	sr^4	r	r^2	r^3	r^4	r^5	1

Ejercicio 2.2.12. Demostrar que el conjunto de rotaciones respecto al origen del plano euclídeo junto con el conjunto de simetrías respecto a las rectas que pasan por el origen, es un grupo.

Denotamos por G al conjunto de rotaciones respecto al origen del plano euclídeo junto con el conjunto de simetrías respecto a las rectas que pasan por el origen. Notemos que no se trata de ningún grupo diédrico:

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

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 2.2.13. Sea G un grupo y sean $a, b \in G$ tales que $ba = ab^k$, $a^n = 1 = b^m$ con $n, m > 0$.

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

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

donde en $(*)$ se ha usado el apartado anterior.

Por tanto, se tiene para todo $i, j \in \mathbb{N}$.

4. Demostrar que todo elemento de $\langle a, b \rangle$ puede escribirse como $a^r b^s$ cumpliendo $0 \leqslant r < n$, $0 \leqslant s < m$.

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

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

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 2.2.15. 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 2.2.16. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas en los ejercicios anteriores.

Observación. Aquí tratamos a S_7 como un subgrupo de S_9, donde consideramos cada permutación del conjunto $\{1,2,3,4,5,6,7\}$ como una permutación del conjunto $\{1,\ldots,9\}$ 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 2.2.17. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas en los ejercicios anteriores.

1. Calcular el orden de la permutación producto s_1s_2. ¿Coincide dicho orden con el producto de los órdenes de s_1 y s_2?

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

Por el Corolario **??**, se tiene que:

$$\begin{aligned} O(s_1s_2) &= 6 \\ O(s_1) &= \text{mcm}(4,2) = 4 \\ O(s_2) &= \text{mcm}(2,5) = 10 \end{aligned}$$

Por tanto, $O(s_1s_2) \neq O(s_1)O(s_2)$.

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

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

3. Calcular la permutación $(s_1)^{-1}$, y expresarla como producto de ciclos disjuntos.

$$\begin{aligned} s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ (s_1)^{-1} &= (5\ 4\ 3\ 1)(7\ 6) \end{aligned}$$

4. Calcular la permutación $(p_1)^{-1}$ y expresarla matricialmente.

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

5. Calcular la permutación $p_2(s_2)^2(p_1)^{-1}$. ¿Cuál es su orden?

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

Ejercicio 2.2.18. Sean s_1, s_2, p_1 y p_2 las permutaciones dadas anteriormente. Sean también $s_3 = (2\ 4\ 6)$ y $s_4 = (1\ 2\ 7)(2\ 4\ 6\ 1)(5\ 3)$. ¿Cuál es la paridad de las permutaciones s_1, $s_4p_1p_2$ y p_2s_3?

$$\begin{aligned} s_1 &= (1\ 3\ 4\ 5)(6\ 7) \\ s_4p_1p_2 &= (1\ 7)(2\ 3)(4\ 6\ 5\ 8) \\ p_2s_3 &= (1\ 9\ 5\ 3\ 2\ 4)(6\ 8) \end{aligned}$$

Por tanto:

$$\begin{aligned} \varepsilon(s_1) &= 1 \\ \varepsilon(s_4p_1p_2) &= -1 \\ \varepsilon(p_2s_3) &= 1 \end{aligned}$$

Ejercicio 2.2.19. En el grupo S_3, se consideran las permutaciones $\sigma = (1\ 2\ 3)$ y $\tau = (1\ 2)$.

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

   Sabemos que $|S_3| = 3! = 6$. Dividimos S_3 en dos conjuntos, uno con las permutaciones pares (P) y otro con las impares (I).
$$\begin{aligned} P &= \{1, \sigma, \sigma^2\} \\ I &= \{\tau, \sigma\tau, \sigma^2\tau\} \end{aligned}$$

   Como $O(\sigma) = 3$, tenemos que las tres permutaciones pares son distintas. Supongamos ahora que dos permutaciones impares son iguales. Entonces, componiendo por la derecha con τ^{-1}, obtenemos que dos permutaciones pares serían iguales, algo que hemos descartado. Por tanto, las tres permutaciones impares son distintas.
$$|P| = |I| = 3$$

   Como una permutación par no puede ser igual a una impar, tenemos que $P \cap I = \emptyset$. Por tanto:
$$\left.\begin{array}{rcl} |P \cup I| & = & |P| + |I| = 6 = |S_3| \\ & \wedge & \\ P \cup I & \subset & S_3 \end{array}\right\} \Longrightarrow S_3 = P \cup I$$

   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 2.2.20. Describir los diferentes ciclos del grupo S_4. Expresar todos los elementos de S_4 como producto de ciclos disjuntos.

Veamos cuántos ciclos de longitud m hay en un S_n. Cada una de las elecciones es una variación de n elementos tomados de m en m. Como además un mismo ciclo de longitud m puede empezar en m posiciones distintas, tenemos que el número de ciclos de longitud m es:
$$\frac{V_n^m}{m} = \frac{n!}{m(n-m)!}$$

Por tanto, los ciclos son:

l	Nº	Ciclos
1	1	id
2	6	(1 2), (1 3), (1 4), (2 3), (2 4), (3 4)
3	8	(1 2 3), (1 2 4), (1 3 2), (1 3 4), (1 4 2), (1 4 3), (2 3 4), (2 4 3)
4	6	(1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)

Tenemos ahora que $|S_4| = 4! = 24$. Como ya hemos dado 21 elementos, nos faltan 3. Estos son los elementos que no son ciclos, y son los siguientes:

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

Ejercicio 2.2.21. Demostrar que el conjunto de transposiciones

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

genera al grupo simétrico S_n.
Demostramos por doble inclusión que:

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

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

$\supset$) Dado $\sigma \in S_n$, veamos que $\sigma \in \langle(1,2),(2,3),\dots,(n-1,n)\rangle$. Por ser una permutación, tenemos que σ es producto de transposiciones. Por tanto, basta con demostrar que cualquier transposición se puede escribir como producto de elementos de $\{(1,2),(2,3),\dots,(n-1,n)\}$.

Sea una transposición (i, j), y sin pérdida de generalidad, supongamos que $i < j$. Entonces, se tiene que:

$$(i, j) = (i, i{+}1)(i{+}1, i{+}2) \cdots (j{-}2, j{-}1)(j{-}1, j)(j{-}2, j{-}1) \cdots (i{+}1, i{+}2)(i, i{+}1)$$

Por tanto, $\sigma \in \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$.

Ejercicio 2.2.22. Demostrar que el conjunto $\{(1, 2, \dots, n), (1, 2)\}$ genera al grupo simétrico S_n.

Demostramos por doble inclusión que:

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

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

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

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

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:

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

Por tanto:

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

Ejercicio 2.2.23. Demostrar que para cualquier permutación $\alpha \in S_n$ se verifica que $\varepsilon(\alpha) = \varepsilon(\alpha^{-1})$, donde ε denota la signatura, o paridad, de una permutación.

Sabemos que la paridad depende del número de ciclos de longitud par que tiene una permutación en su descomposición en ciclos disjuntos. Como este valor es el mismo para una permutación y su inversa, se tiene que $\varepsilon(\alpha) = \varepsilon(\alpha^{-1})$.

Ejercicio 2.2.24. Demostrar que si $(x_1\ x_2\ \cdots\ x_r) \in S_n$ es un ciclo de longitud r, entonces

$$\varepsilon(x_1 x_2 \cdots x_r) = (-1)^{r-1}.$$

- Si r es par, entonces hay un solo ciclo de longitud par, y por tanto $\varepsilon(x_1 x_2 \cdots x_r) = -1$. Como además $r - 1$ es impar, se tiene que $(-1)^{r-1} = -1$.
- Si r es impar, entonces hay un solo ciclo de longitud impar, y 0 ciclos de longitud par. Por tanto, $\varepsilon(x_1 x_2 \cdots x_r) = 1$. Como además $r - 1$ es par, se tiene que $(-1)^{r-1} = 1$.

Ejercicio 2.2.25. 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 2.2.26.

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.

   $$\begin{gathered} 1 = f(1) = f((-1) \cdot (-1)) = f(-1) \cdot f(-1) = 4 \cdot 4 = 16 = 1 \\ 4 = f(-1) = f(i \cdot i) = f(i) \cdot f(i) = 2 \cdot 2 = 4 \\ 4 = f(-1) = f((-i) \cdot (-i)) = f(-i) \cdot f(-i) = 3 \cdot 3 = 9 = 4 \\ 3 = f(-i) = f((-1) \cdot i) = f(-1) \cdot f(i) = 4 \cdot 2 = 8 = 3 \\ 2 = f(i) = f((-1) \cdot (-i)) = f(-1) \cdot f(-i) = 4 \cdot 3 = 12 = 2 \\ 1 = f(1) = f(i \cdot (-i)) = f(i) \cdot f(-i) = 2 \cdot 3 = 6 = 1 \end{gathered}$$

   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 $-i$:

$$\begin{gathered}
4 = g(-1) = g(i \cdot i) = g(i) \cdot g(i) = 3 \cdot 3 = 9 = 4 \\
4 = g(-1) = g((-i) \cdot (-i)) = g(-i) \cdot g(-i) = 2 \cdot 2 = 4 \\
3 = g(i) = g((-1) \cdot (-i)) = g(-1) \cdot g(-i) = 4 \cdot 2 = 8 = 3 \\
2 = g(-i) = g((-1) \cdot i) = g(-1) \cdot g(i) = 4 \cdot 3 = 12 = 2 \\
1 = g(1) = g(i \cdot (-i)) = g(i) \cdot g(-i) = 3 \cdot 2 = 6 = 1
\end{gathered}$$

Ejercicio 2.2.27. 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:

$$\begin{gathered}
1 = f(1, 1) = f[(1, -1)(1, -1)] = f(1, -1)f(1, -1) = 3 \cdot 3 = 9 = 1 \\
1 = f(1, 1) = f[(-1, 1)(-1, 1)] = f(-1, 1)f(-1, 1) = 5 \cdot 5 = 25 = 1 \\
1 = f(1, 1) = f[(-1, -1)(-1, -1)] = f(-1, -1)f(-1, -1) = 7 \cdot 7 = 49 = 1 \\
7 = f(-1, -1) = f[(1, -1)(-1, 1)] = f(1, -1)f(-1, 1) = 3 \cdot 5 = 15 = 7 \\
5 = f(-1, 1) = f[(1, -1)(-1, -1)] = f(1, -1)f(-1, -1) = 3 \cdot 7 = 21 = 5 \\
3 = f(1, -1) = f[(-1, 1)(-1, -1)] = f(-1, 1)f(-1, -1) = 5 \cdot 7 = 35 = 3
\end{gathered}$$

Por tanto, f es un isomorfismo entre ambos grupos.

Ejercicio 2.2.28. 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 2.2.22, mientras que el generador de $\mathrm{GL}_2(\mathbb{Z}_2)$ se ha visto en el Ejercicio 2.2.10.

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

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, 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.

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

Entonces, existe un único homomorfismo $g : S_3 \to \mathrm{GL}_2(\mathbb{Z}_2)$ 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 2.2.29. Sea $\mathbb{K}$ un cuerpo y considérese la operación binaria

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

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:

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

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:

$$\begin{aligned} f(x \otimes y) &= 1 - (x \otimes y) = 1 - (x + y - xy) = 1 - x - y + xy \\ f(x)f(y) &= (1 - x)(1 - y) = 1 - x - (1 - x)y = 1 - x - y + xy \end{aligned}$$

Por tanto, f es un homomorfismo entre ambos grupos. Además, es biyectiva, ya que su inversa es $f^{-1}(x) = 1-x$. Por tanto, f es un isomorfismo entre ambos grupos.

Ejercicio 2.2.30.

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 Teoría.

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

   En primer lugar, tenemos que:

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

   Calculamos los órdenes de D_4:

   $$\begin{gathered} O(1) = 1 \qquad O(r) = O(r^3) = 4 \\ O(r^2) = O(s) = O(sr) = O(sr^2) = O(sr^3) = 2 \end{gathered}$$

   Por otro lado, calculamos los órdenes de Q_2:

   $$\begin{gathered} O(1) = 1 \qquad O(-1) = 2 \\ O(\pm i) = O(\pm j) = O(\pm k) = 4 \end{gathered}$$

   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 2.2.31. Calcular el orden de:

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

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

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

   $$\begin{aligned} &O(1) = 1 \\ &O(3) = O(4) = O(5) = O(9) = 5 \\ &O(2) = O(6) = O(7) = O(8) = 10 \\ &O(10) = 2 \end{aligned}$$

Ejercicio 2.2.32. Demostrar que un grupo generado por dos elementos distintos de orden dos, que conmutan entre sí, consiste del 1, de esos elementos y de su producto y es isomorfo al grupo de Klein.

Sea $G = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$. Entonces, por el Ejercicio 2.2.13 tenemos:

$$G = \{1, a, b, ab\}$$

Sea ahora el grupo de Klein el siguiente:

$$\begin{aligned} V &= \{1,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\} \\ &= \langle (1\ 2)(3\ 4),\ (1\ 3)(2\ 4) \rangle \end{aligned}$$

Por tanto, hemos de encontrar un isomorfismo entre ambos grupos. 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, 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, $G \cong V$. Como G es abeliano, V también lo es.

Ejercicio 2.2.33. Sea G un grupo y sean $a, b \in G$.

1. Demostrar que $O(b) = O(aba^{-1})$ (un elemento y su conjugado tienen el mismo orden).

   Para todo $n \in \mathbb{N}$, se tiene que:

   $$1 = (aba^{-1})^n = ab^n a^{-1} \iff a^{-1} = b^n a^{-1} \iff 1 = b^n$$

   Comprobemos ahora que $O(b) = O(aba^{-1})$:

   - Si $O(b) = \infty$, supongamos por reducción al absurdo que $\exists n \in \mathbb{N}$ tal que $(aba^{-1})^n = 1$. Entonces, se tiene que $b^n = 1$, lo que contradice que $O(b) = \infty$.
   - Si $O(b) = n$, entonces se tiene que $b^n = 1$, por lo que $(aba^{-1})^n = 1$ y por tanto $O(aba^{-1}) \leqslant n$. 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 $O(ba) = O(ab)$.

   Considerando ahora $ba \in G$, se tiene que:

$$O(ba) \stackrel{(*)}{=} O(a\ ba\ a^{-1}) = O(a\ b \cdot 1) = O(ab)$$

   donde en $(*)$ hemos usado el apartado anterior.

Ejercicio 2.2.34. Sea G un grupo y sean $a, b \in G$, $a \neq 1 \neq b$, tales que $a^2 = 1$ y $ab^2 = b^3a$. Demostrar que $O(a) = 2$ y que $O(b) = 5$.

Comprobemos en primer lugar que $O(a) = 2$. Por hipótesis, tenemos que $a^2 = 1$, por lo que $O(a) \mid 2$. Por tanto, $O(a) = 1$ o $O(a) = 2$. Como $a \neq 1$, se tiene que $O(a) = 2$. Veamos ahora que $O(b) = 5$. Tenemos que:

$$\begin{aligned} ab^2 = b^3a &\Longrightarrow b^2 = ab^3a \Longrightarrow \\ &\Longrightarrow b^4 = (ab^3a)(ab^3a) = ab^6a = a(ab^3a)(ab^3a)(ab^3a)a = b^9 \Longrightarrow 1 = b^5 \end{aligned}$$

Por tanto, $O(b) \mid 5$. Por tanto, $O(b) = 1$ o $O(b) = 5$. Como $b \neq 1$, se tiene que $O(b) = 5$.

Ejercicio 2.2.35. 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 $n \in \mathbb{Z}$, $n < 0$.

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

   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 Teoría.

Ejercicio 2.2.36.

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

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

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

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

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

   Opción 1 Por reducción al absurdo, supongamos que existe un isomorfismo $f : \mathbb{Q} \to \mathbb{Z}$. 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.

   Opción 2 (Notemos que usaremos conceptos del Tema 3)

   Por reducción al absurdo, supongamos que existe un isomorfismo dado por $f : \mathbb{Z} \to \mathbb{Q}$. Como $Z = \langle 1 \rangle$ y f es un epimorfismo, entonces tendremos $\mathbb{Q} = \langle f(1) \rangle$. Supongamos que $f(1) = \frac{a}{b}$ con $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. Entonces, se tiene que:

   $$\mathbb{Q} = \left\langle \frac{a}{b} \right\rangle = \left\{ \frac{ka}{b} \mid k \in \mathbb{Z} \right\}$$

   Sabemos que $a/2b \in \mathbb{Q}$, por lo que $\exists k \in \mathbb{Z}$ tal que:

   $$\frac{ka}{b} = \frac{a}{2b} \Longrightarrow 2kab = ab \Longrightarrow 2ka = a \Longrightarrow \begin{cases} a = 0 \\ k = 1/2 \notin \mathbb{Z} \end{cases}$$

   Por tanto, $a = 0$. Entonces:

   $$f(1) = \frac{0}{b} = 0 \stackrel{(*)}{=} f(0)$$

   donde en $(*)$ hemos usado que f es un homomorfismo entre grupos aditivos. Por tanto, f no es inyectiva, lo que contradice que sea un isomorfismo.

Ejercicio 2.2.37. 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.

Observación. Notemos que este ejercicio es consecuencia directa del Ejercicio 2.2.7, pero lo hacemos por motivos didácticos.

Ejercicio 2.2.38. 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 2.2.39. Demostrar que no existe ningún cuerpo $\mathbb{K}$ tal que sus grupos aditivo $(\mathbb{K}, +)$ y $(\mathbb{K}^*, \cdot)$ sean isomorfos.

Si $\mathbb{K}$ es finito, entonces:

$$|\mathbb{K}^*| = |\mathbb{K}| - 1 \neq |\mathbb{K}|$$

Por tanto, no pueden ser isomorfos. Si $\mathbb{K}$ es infinito, entonces supongamos por reducción al absurdo que existe un isomorfismo $f : \mathbb{K} \to \mathbb{K}^*$. 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.

2.3. Subgrupos, Generadores, Retículos y Grupos cíclicos

Ejercicio 2.3.1. Describir todos los elementos de los grupos alternados A_n, consistentes en las permutaciones pares del S_n correspondiente, para:

1. $n = 2$.

$$\begin{aligned} S_2 &= \{1, (1\ 2)\} \\ A_2 &= \{1\} \end{aligned}$$

2. $n = 3$.

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

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 2.3.2. Sea D_n el grupo diédrico. Demostrar que el subgrupo de D_n generado por los elementos $\{r^j s, r^k s\}$ es todo el grupo D_n siempre que $0 \leqslant j < k < n$ 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 2.3.3.

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 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:

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

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

$\Longrightarrow$) 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 2.3.5. Sean $a, b \in G$ dos elementos de un grupo que conmutan entre sí, esto es, para los que $ab = ba$, y de manera que sus órdenes son primos relativos, esto es, $\mathrm{mcd}(O(a), O(b)) = 1$.

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

   Opicón 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 $\operatorname{mcd}(O(a), O(b))$, 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 $\operatorname{mcd}(O(a), O(b)) = 1$, entonces $|\langle a \rangle \cap \langle b \rangle| = 1$. Por tanto, $\langle a \rangle \cap \langle b \rangle = \{1\}$.

   Opción 2 Demostrémoslo por doble inclusión.

   $\supseteq$) Como $\langle a \rangle$ y $\langle b \rangle$ son subgrupos de G, entonces $\langle a \rangle \cap \langle b \rangle$ es un subgrupo de G, y en particular es un grupo. Por tanto, $1 \in \langle a \rangle \cap \langle b \rangle$.

   $\subseteq$) Sea $x \in \langle a \rangle \cap \langle b \rangle$.

   - Como $x \in \langle a \rangle$, entonces $x = a^s$ para algún $s \in \mathbb{Z}$.
   - Como $x \in \langle b \rangle$, entonces $x = b^t$ para algún $t \in \mathbb{Z}$.

   Por tanto:

   $$1 = (a^{O(a)})^s = (a^s)^{O(a)} = x^{O(a)} = (b^t)^{O(a)} = b^{tO(a)} \implies O(b) \mid tO(a)$$

   Como $\operatorname{mcd}(O(a), O(b)) = 1$, entonces $O(b) \mid t$, por lo que $\exists k \in \mathbb{Z}$ tal que $t = kO(b)$. Por tanto:

   $$x = b^t = b^{kO(b)} = (b^{O(b)})^k = 1^k = 1$$

   Por tanto, $\langle a \rangle \cap \langle b \rangle \subset \{1\}$.

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

   Puesto que conmutan, tenemos que:

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

   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 $\operatorname{mcd}(n, m) = 1$. Por tanto:

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

Ejercicio 2.3.6. Encontrar un grupo G y elementos $a, b \in G$ tales que sus órdenes sean primos relativos, pero para los que no se verifique la igualdad $O(ab) = O(a)O(b)$ del ejercicio anterior.

En primer lugar, hemos de tener que no conmuten. Por tanto, consideremos el grupo S_3 y los elementos:

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

Tenemos que $O(a) = 2$ y $O(b) = 3$, y por tanto $\operatorname{mcd}(O(a), O(b)) = 1$. 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 2.3.7. Sea G un grupo y $a, b \in G$ dos elementos de orden finito. ¿Es ab necesariamente de orden finito?

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

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

Calculamos ahora el orden de ab. Por inducción, demostraremos que:

$$(ab)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

- <u>Caso base:</u> $n = 1$.

$$(ab)^1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

- <u>Supuesto cierto para n, demostramos para $n + 1$:</u>

$$(ab)^{n+1} = (ab)^n(ab) = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -(n+1) \\ 0 & 1 \end{pmatrix}$$

Por tanto, como en $(ab)^n \neq I_2$ para todo $n \in \mathbb{N}$, entonces $O(ab) = \infty$.

Ejercicio 2.3.8. En el grupo S_3 se considera el conjunto

$$H = \{1, (1\ 2\ 3), (1\ 3\ 2)\}.$$

1. Demostrar que H es un subgrupo de S_3.

   Opción 1. Por ser S_3 finito, tan solo hemos de comprobar que H es cerrado para el producto. Como vimos, no es necesario comprobar si uno de los elementos es el neutro.

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

   Por tanto, $H < S_3$.

   Opción 2. Demostremos que $H = \langle(1\ 2\ 3)\rangle$.

   $\subseteq$) Tan solo será necesario ver que $(1\ 2\ 3)^2 = (1\ 3\ 2)$, y se tendría de manera inmediata que $H \subseteq \langle(1\ 2\ 3)\rangle$.

   $\supseteq$) Sea $x \in \langle(1\ 2\ 3)\rangle$. Entonces $x = (1\ 2\ 3)^n$ para algún $n \in \mathbb{Z}$. Como $O((1\ 2\ 3)) = 3$, entonces $n \in \{0, 1, 2\}$. Por tanto:

$$x \in \{(1\ 2\ 3)^0, (1\ 2\ 3)^1, (1\ 2\ 3)^2\} = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = H$$

2. Describir las diferentes clases de S_3 módulo H.

   Por el Teorema de Lagrange, sabemos que:

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

   Calculamos ahora las clases de equivalencia de $S_3/\, {}_H\!\sim$:

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

   Como ya hemos encontrado dos clases de equivalencia distintas, entonces hemos encontrado todas las posibles.

$$S_3/\, {}_H\!\sim = \{H, (1\ 2)H\}$$

   Calculamos ahora las clases de equivalencia de $S_3/ \sim_H$:

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

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

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

Ejercicio 2.3.9. 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:

   - <u>$r = 2$:</u> $G = G_0 \geqslant G_1 \geqslant G_2$. Por el apartado anterior, sabemos que:
     $$[G : G_2] = [G : G_1][G_1 : G_2]$$

- Supuesto cierto para r, demostramos para $r+1$: Por hipótesis de inducción, sabemos que:
$$[G : G_r] = \prod_{i=0}^{r-1} [G_i : G_{i+1}]$$
Por otro lado, como $G_{r+1} \leqslant G_r \leqslant G$, 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 2.3.10.

1. Demostrar que si G es un grupo de orden 4, entonces se tiene que o bien G es cíclico, o bien es isomorfo al grupo de Klein.

   Como $|G| = 4$, entonces $O(x) \mid 4$ para todo $x \in G$. Por tanto, $O(x) \in \{1, 2, 4\}$. Consideramos los siguientes casos:

   - Supongamos $\exists x \in G \mid O(x) = 4$:
   En este caso, como x tiene 4 potencias distintas, entonces:
   $$\langle x \rangle = \{1, x, x^2, x^3\} \subset G$$
   Como además $|\langle x \rangle| = 4 = |G|$, entonces $G = \langle x \rangle$. Por tanto, G es cíclico, $G = C_4$.
   - Supongamos $\nexists x \in G \mid O(x) = 4$:
   En este caso, $\forall x \in G$, $O(x) \in \{1, 2\}$. Como $O(x) = 1 \iff x = 1$, entonces G tiene 3 elementos de orden 2. Sea $x \in G$ tal que $O(x) = 2$.

     En este caso, $\langle x \rangle = \{1, x\} \subset G$. Como $|G| = 4$, ha de existir un elemento $y \in G$ tal que $y \notin \langle x \rangle$ y $O(y) = 2$.

Veamos que G cumple las relaciones del grupo de Klein abstracto:

$$V^{\text{abs}} = \langle a, b \mid a^2 = b^2 = 1,\ ab = ba \rangle$$

Sabemos que $x^2 = y^2 = 1$. Ahora, nos falta ver que $xy = yx$. Como $xy \in G$, entonces $O(xy) \in \{1, 2\}$. En cualquier caso, $(xy)^2 = 1$, por lo que:

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

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:

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

Veamos en primer lugar los elementos de G. Sabemos que $\{1, x, x^2\} \subset G$. Veamos ahora que y no puede ser uno de estos elementos:

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

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.

$$\begin{tikzcd}
 & V \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle(1\ 2)(3\ 4)\rangle \arrow[dr, dash] & \langle(1\ 3)(2\ 4)\rangle \arrow[d, dash] & \langle(1\ 4)(2\ 3)\rangle \arrow[dl, dash] \\
 & \{1\} &
\end{tikzcd}$$

Figura 2.47: Diagrama de Hasse para los subgrupos del grupo de Klein.

- Si $yx = x^2$, entonces $y = x$, lo cual es una contradicción.
- Si $yx = y$, entonces $x = 1$, lo cual es una contradicción.
- Si $yx = xy$, entonces G es abeliano. En este caso, veamos que $O(xy) = 6$:

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

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

1. El grupo V de Klein.

   La complejidad en todo este ejercicio será hallar todos los subgrupos de un cierto grupo. Una vez hallados, dibujar los Diagramas de Hasse no será complicado.

   Sabemos que $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Por el Teorema de Lagrange, sabemos que los subgrupos de V han de tener orden 1, 2 o 4. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 4 es V. Veamos ahora los subgrupos de orden 2. Como 2 es primo, entonces los subgrupos de orden 2 han de ser cíclicos. Por tanto, los subgrupos de orden 2 son:

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

   Por tanto, el retículo de subgrupos de V es el de la Figura 2.47.

2. El grupo simétrico S_3.

   Sabemos que $|S_3| = 6$. Por el Teorema de Lagrange, sabemos que los subgrupos de S_3 han de tener orden 1, 2, 3 o 6. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 6 es S_3. Veamos ahora los subgrupos de orden 2 y 3. Como 2 y 3 son primos, entonces los subgrupos de orden 2 y 3 han de ser cíclicos. Sabemos que:

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

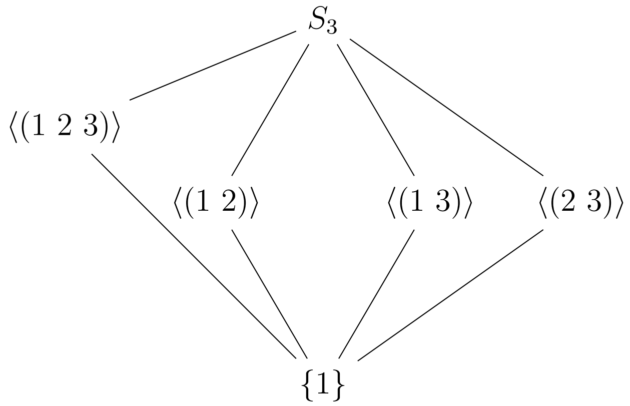


Figura 2.48: Diagrama de Hasse para los subgrupos de S_3.

Por tanto, los subgrupos de orden 2 son:

$$\begin{aligned}\langle(1\ 2)\rangle &= \{1, (1\ 2)\}\\ \langle(1\ 3)\rangle &= \{1, (1\ 3)\}\\ \langle(2\ 3)\rangle &= \{1, (2\ 3)\}\end{aligned}$$

Por otro lado, los subgrupos de orden 3 son:

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

Notemos que no ha hecho falta calcular $\langle(1\ 3\ 2)\rangle$ puesto que, $\langle x\rangle = \langle x^{-1}\rangle$. Por tanto, el retículo de subgrupos de S_3 es el de la Figura 2.48.

3. El grupo diédrico D_4.

   Sabemos que $|D_4| = 8$. Por el Teorema de Lagrange, sabemos que los subgrupos de D_4 han de tener orden 1, 2, 4 u 8. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 8 es D_4. Veamos ahora los subgrupos de orden 2 y 4. Como 2 es primo, entonces los subgrupos de orden 2 han de ser cíclicos. Sabemos que:
   $$D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

   Calculemos el orden de los elementos de D_4:

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

   Por tanto, los subgrupos de orden 2 son:

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

Calculamos ahora los subgrupos de orden 4. Sabemos que:

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

No obstante, busquemos más grupos de orden 4, algo que no será sencillo. Dado un subgrupo H, como $H = \langle H\rangle$, entonces siempre podemos encontrar un conjunto de generadores suyo. Buscaremos por tanto conjuntos de generadores con 1, 2, 3 y 4 elementos.

- Con un elemento:
  Los subgrupos generados por un único elemento sabemos que son cíclicos y el orden del elemento ha de ser el orden del grupo. Por tanto, el único subgrupo de D_4 de orden 4 es:
  $$\langle r\rangle = \{1, r, r^2, r^3\} = \langle r^3\rangle$$
- Con dos elementos:
  A partir de aquí, es más complejo. Sabemos que los generadores no han de ser ni r ni r^3, pues estos generarían un grupo de orden mayor que 4. Además, incluir a 1 como generador no tiene sentido. Por último, notemos que x y x^{-1} generan el mismo grupo. Las posibles combinaciones son:
  $$\begin{aligned}
  \langle s, r^2\rangle &= \{1, s, r^2, sr^2\}\\
  \langle s, sr\rangle &= D_4 \text{ pues } r = s\cdot sr\\
  \langle s, sr^2\rangle &= \langle s, r^2\rangle \text{ pues } s\cdot sr^2 = r^2\\
  \langle s, sr^3\rangle &\supset \langle r^3\rangle \text{ pues } s\cdot sr^3 = r^3\\
  \langle sr, r^2\rangle &= \{1, sr, sr^3, r^2\}\\
  \langle sr, sr^2\rangle &\supset \langle r\rangle \text{ pues } sr\cdot sr^2 = ssr^3r^2 = r\\
  \langle sr, sr^3\rangle &= \langle sr, r^2\rangle \text{ pues } sr\cdot sr^3 = r^2\\
  \langle r^2, sr^2\rangle &= \langle s, r^2\rangle \text{ pues } sr^2\cdot r^2 = s\\
  \langle r^2, sr^3\rangle &= \langle sr, r^2\rangle \text{ pues } sr^3\cdot r^2 = sr\\
  \langle sr^2, sr^3\rangle &= D_4 \text{ pues } r = sr^2\cdot sr^3 \text{ y } sr^3\cdot r = s
  \end{aligned}$$
  Por tanto, y en resumen, los únicos subgrupos de D_4 de orden 4 generados por dos elementos son:
  $$\begin{aligned}
  \langle s, r^2\rangle &= \{1, s, r^2, sr^2\}\\
  \langle sr, r^2\rangle &= \{1, sr, sr^3, r^2\}
  \end{aligned}$$
- Con tres elementos:
  Supongamos (pues en otro caso ya se habría estudiado) que todos los elementos generadores son de orden 2 y distintos. Sean estos x, y y z. Como $\langle x, y\rangle$ nos proporciona un subgrupo de orden 4 o mayor, caben dos posibilidades:
  - Al añadir z como generador, no se generen más elementos. En este caso, $\langle x, y, z\rangle = \langle x, y\rangle$, caso ya estudiado.

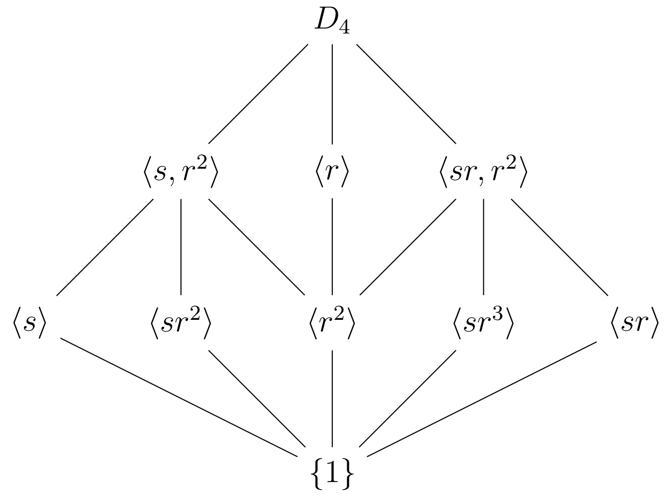


Figura 2.49: Diagrama de Hasse para los subgrupos de D_4.

- Al añadir z como generador, se generen más elementos. En este caso, $\langle x, y, z\rangle = D_4$.

- <u>Con cuatro elementos:</u>

  Supongamos (pues en otro caso ya se habría estudiado) que todos los elementos generadores son de orden 2 y distintos. Entonces, como también el 1 pertenecerá a dicho subgrupo, tenemos que este grupo será D_4.

Por tanto, los únicos subgrupos de D_4 de orden 4 son:

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

Por tanto, el retículo de subgrupos de D_4 es el de la Figura 2.49.

4. El grupo cuaternio Q_2.

   Sabemos que $|Q_2| = 8$. Por el Teorema de Lagrange, sabemos que los subgrupos de Q_2 han de tener orden 1, 2, 4 u 8. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 8 es Q_2. Veamos en primer lugar el orden de los elementos de Q_2:

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

   Como 2 es primo, los subgrupos de orden 2 han de ser cíclicos y generados por un elemento de orden 2. Por tanto, el único subgrupo de orden 2 es:

   $$\langle -1\rangle = \{1, -1\}$$

   Respecto a los subgrupos de orden 4, buscaremos conjuntos de generadores de $1, 2, 3$ y 4 elementos.

$$\begin{tikzcd}[arrows=-]
 & Q_2 \arrow[dl] \arrow[d] \arrow[dr] & \\
\langle i \rangle \arrow[dr] & \langle j \rangle \arrow[d] & \langle k \rangle \arrow[dl] \\
 & \langle -1 \rangle \arrow[d] & \\
 & \{1\} &
\end{tikzcd}$$

Figura 2.50: Diagrama de Hasse para los subgrupos del grupo de los cuaternios.

- Con un elemento:

  Los subgrupos generados por un único elemento sabemos que son cíclicos y el orden del elemento ha de ser el orden del grupo. Por tanto, estos son:

$$\begin{aligned}
\langle i \rangle &= \{1, i, -1, -i\} \\
\langle j \rangle &= \{1, j, -1, -j\} \\
\langle k \rangle &= \{1, k, -1, -k\}
\end{aligned}$$

- Con dos elementos:

  Supongamos (pues en otro caso ya se habría estudiado) que los generadores no son de orden 4. Entonces tan solo puede ser el 1 y el -1, caso ya estudiado. Por tanto, no consideramos ni este caso ni los generados por más elementos.

Por tanto, el retículo de subgrupos de Q_2 es el de la Figura 2.50.

5. El grupo alternado A_4.

   Sabemos que $|A_4| = 12$. Por el Teorema de Lagrange, sabemos que los subgrupos de A_4 han de tener orden 1, 2, 3, 4, 6 o 12. El subgrupo de orden 1 es $\{1\}$, y el subgrupo de orden 12 es A_4. Veamos ahora los subgrupos de orden 2, 3, 4 y 6. Para ello, antes de nada, mostremos los elementos de A_4:

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

   Como $V < A_4$, entonces los subgrupos de V son subgrupos de A_4. Estos son:

$$\begin{aligned}
\langle (1\ 2)(3\ 4) \rangle &= \{1, (1\ 2)(3\ 4)\} \\
\langle (1\ 3)(2\ 4) \rangle &= \{1, (1\ 3)(2\ 4)\} \\
\langle (1\ 4)(2\ 3) \rangle &= \{1, (1\ 4)(2\ 3)\} \\
V &= \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle
\end{aligned}$$

Veamos si hay más subgrupos de orden 2. Como 2 es primo, estos han de ser cíclicos generados por un elemento de orden 2; pero no hay más elementos de orden 2 en A_4. Por tanto, los subgrupos de orden 2 son los anteriormente mencionados.

Veamos ahora los subgrupos de orden 3. Como 3 es primo, estos han de ser cíclicos generados por un elemento de orden 3. Además, hemos de tener en cuenta que $\langle x \rangle = \langle x^{-1} \rangle$. Por tanto, los subgrupos de orden 3 son:

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

Veamos ahora los subgrupos de orden 4. Como 4 no es primo, no es tan sencillo. Buscaremos que estén generados por 1, 2, 3 y 4 elementos.

- Con un elemento:
  Los subgrupos generados por un único elemento sabemos que son cíclicos y el orden del elemento ha de ser el orden del grupo. Como no hay elementos de orden 4, no hay subgrupos de orden 4 generados por un único elemento.
- Con dos elementos:
  Supongamos (pues en otro caso ya se habría estudiado) que los dos elementos son distintos y de orden 2 (pues el orden de todo elemento debe dividir al orden del subgrupo al que pertenece). Entonces, llegamos al grupo de Klein, caso ya estudiado. Por tanto, no consideramos generadores de más elementos.

Respecto a los subgrupos de orden 6, en el ejemplo de la página **??** se vió que no existen subgrupos de orden 6 en A_4. Por tanto, el retículo de subgrupos de A_4 es el de la Figura 2.51.

Ejercicio 2.3.12. Fijado un número primo p, describe el retículo de subgrupos del grupo cíclico C_{p^n}. En particular, describe el retículo de subgrupos del grupo cíclico C_8.

Sabemos que, para cada divisor de p^n, existe un subgrupo de C_{p^n} de ese orden. En concreto, los únicos subgrupos de C_{p^n} son los de la forma $\langle x^{p^k} \rangle$ con $k \in \{0, \dots, n\}$. Además:

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

Por tanto, $\langle x^{p^k} \rangle = C_{p^{n-k}}$. Además, fijado $k \in \{0, \dots, n\}$, tenemos que $\langle x^{p^{k+1}} \rangle \subset \langle x^{p^k} \rangle$, puesto que $x^{p^{k+1}} = (x^{p^k})^p$. Por tanto, el retículo de subgrupos de C_{p^n} es el de la Figura 2.52.

En particular, para C_8, tenemos que $p = 2$ y $n = 3$. Por tanto, el retículo de subgrupos de C_8 es el de la Figura 2.53.

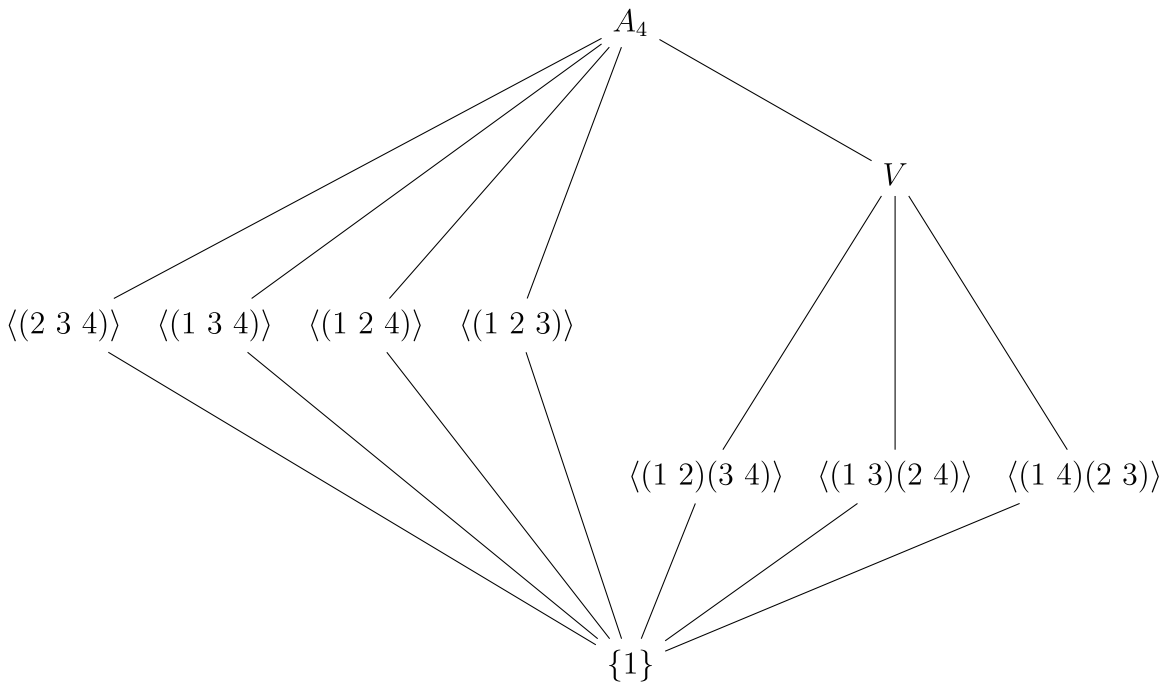


Figura 2.51: Diagrama de Hasse para los subgrupos del grupo alternado A_4.

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

Figura 2.52: Retículo de subgrupos de C_{p^n} para el Ejercicio 2.3.12.

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

Figura 2.53: Retículo de subgrupos de C_8 para el Ejercicio 2.3.12.

$$
\begin{tikzcd}
G \arrow[d, dash] \\
\{1\}
\end{tikzcd}
$$

Figura 2.54: Retículo de subgrupos de para el Ejercicio 2.3.13.

$$
\begin{tikzcd}
 & C_6 = \langle x \rangle \arrow[dl, dash] \arrow[ddr, dash] & \\
C_3 = \langle x^2 \rangle \arrow[ddr, dash] & & \\
 & & C_2 = \langle x^3 \rangle \arrow[dl, dash] \\
 & \{1\} = \langle x^6 \rangle = \langle 1 \rangle &
\end{tikzcd}
$$

Figura 2.55: Retículo de subgrupos de C_6 para el Ejercicio 2.3.14.

Ejercicio 2.3.13. Demostrar que un grupo finito $G \neq \{1\}$ carece de subgrupos propios, esto es, que su retículo de subgrupos es el de la Figura 2.54 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.

$\Longleftarrow$) 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 2.3.14. 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:

$$
\begin{aligned}
\langle x^2 \rangle &= \{1, x^2, x^4\} \\
\langle x^3 \rangle &= \{1, x^3\}
\end{aligned}
$$

   Por tanto, el retículo de subgrupos de C_6 es el de la Figura 2.55.

2. C_{12}.

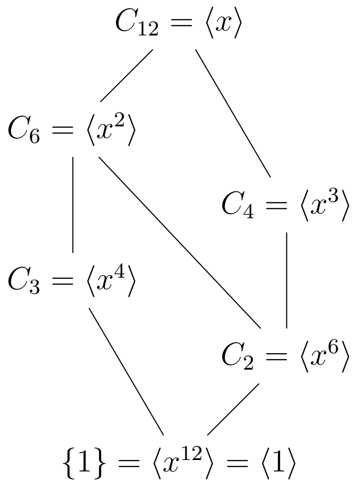


Figura 2.56: Retículo de subgrupos de C_{12} para el Ejercicio 2.3.14.

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

$$\begin{aligned}
\langle x^2 \rangle &= \{1, x^2, x^4, x^6, x^8, x^{10}\} \\
\langle x^3 \rangle &= \{1, x^3, x^6, x^9\} \\
\langle x^4 \rangle &= \{1, x^4, x^8\} \\
\langle x^6 \rangle &= \{1, x^6\}
\end{aligned}$$

Por tanto, el retículo de subgrupos de C_{12} es el de la Figura 2.56.

Ejercicio 2.3.15. Se considera el grupo cíclico C_{136} de orden 136, con generador t. ¿Qué relación hay entre los subgrupos $H_1 = \langle t^{48}, t^{72} \rangle$ y $H_2 = \langle t^{46} \rangle$?

Estudiamos en primer lugar el grupo H_2. Como $O(t) = 136$, entonces:

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

Por otro lado:

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

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

Opción 1. 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.

Opción 2. Sabemos que $|\mathbb{Z}_7^\times| = 6$. Por el Ejercicio 2.3.10, sabemos que hay dos posibilidades, o bien $\mathbb{Z}_7^\times$ es cíclico, o bien $\mathbb{Z}_7^\times \cong D_3$. No obstante, no puede ser isomorfo a D_3, puesto que D_3 no es abeliano y $\mathbb{Z}_7^\times$ sí lo es. Por tanto, $\mathbb{Z}_7^\times$ es cíclico.

Ejercicio 2.3.17. Sea G un grupo y sea C_n el grupo cíclico de orden n generado por x. Demostrar que:

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

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

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

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

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, $O(g) = n$.

Partimos de:

$$\theta_g \text{ es monomorfismo } \iff \ker(\theta_g) = \{1\}$$

Calculemos el núcleo de θ_g:

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

Como $O(x) = n$, sabemos que $x^k \neq 1$ para $k \in \{1, \dots, n-1\}$. Por tanto:

$$\ker(\theta_g) = \{1\} \iff g^k \neq 1 \ \forall k \in \{1, \dots, n-1\} \iff O(g) \geqslant n$$

Como partimos de que $O(g) \mid n$, entonces:

$$\theta_g \text{ es monomorfismo } \iff O(g) = n$$

4. Existe un isomorfismo de grupos

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

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

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

Para cada $r \in \{1, \ldots, n-1\}$ con $\operatorname{mcd}(r, n) = 1$ (es decir, $r \in \mathcal{U}(\mathbb{Z}_n)$), definimos el siguiente automorfismo de C_n:

$$\begin{array}{rccc} f_r : & C_n & \longrightarrow & C_n \\ & x & \longmapsto & x^r \end{array}$$

Comprobemos en primer lugar que se trata de un automorfismo. Puesto que $C_n \cong \mathbb{Z}_n$, entonces C_n es abeliano y, de ahí, se tiene de forma directa que f_r es un homomorfismo. Veamos que es inyectivo:

- Inyectividad: Supongamos $k, l \in \{0, \ldots, n-1\}$ tales que $f_r(x^k) = f_r(x^l)$. Entonces, $x^{rk} = x^{rl} \implies x^{r(k-l)} = 1$. Como $O(x) = n$, se tiene que $n \mid r(k-l)$. Como además $\operatorname{mcd}(r, n) = 1$, entonces $n \mid k - l$, tenemos que $k, l \in \{0, \ldots, n-1\}$, entonces $k - l = 0$. Por tanto, $k = l$.

Por tanto, por ser inyectivo y ser C_r finito, entonces f_r biyectivo. Por tanto, f_r es un automorfismo. Esto nos permite definir la siguiente función:

$$\begin{array}{rccc} \Phi : & \mathcal{U}(\mathbb{Z}_n) & \longrightarrow & \operatorname{Aut}(C_n) \\ & r & \longmapsto & f_r \end{array}$$

Dividimos la demostración en varios aspectos:

Bien definida: Veamos en primer lugar que Φ está bien definida. Para ello, consideramos $r, s \in \mathbb{Z}$ tales que $[r] = [s]$. Entonces, $s = r + tn$ para algún $t \in \mathbb{Z}$. Veamos que $f_r = f_s$. Supongamos $\langle x \rangle = C_n$. Entonces, para cada $k \in \{0, \ldots, n-1\}$, se tiene que:

$$f_r(x^k) = x^{rk}$$
$$f_s(x^k) = x^{sk} = \left(x^{r+tn}\right)^k = x^{rk}x^{tnk} = x^{rk} \cdot (x^n)^{tk} = x^{rk} \cdot 1 = x^{rk}$$

Por tanto, $f_r = f_s$, y por tanto Φ está bien definida.

Homomorfismo: Veamos ahora que Φ es un homomorfismo. Para ello, consideramos $r, s \in \mathcal{U}(\mathbb{Z}_n)$:

$$\Phi(rs) = f_{rs} \qquad \Phi(r) \circ \Phi(s) = f_r \circ f_s$$

Comprobamos que se trata del mismo automorfismo:

$$f_{rs}(x) = x^{rs} = (x^s)^r = f_r(f_s(x)) = (f_r \circ f_s)(x) \qquad \forall x \in C_n$$

Por tanto, Φ es un homomorfismo.

Inyectividad: Veamos ahora que $\ker(\Phi) = \{1\}$. Para ello, supongamos que $\exists k \in \mathcal{U}(\mathbb{Z}_n) \setminus \{1\}$ tal que $\Phi(k) = f_k = id$. Entonces, para $x \in C_n$ con $O(x) = n$, se tiene que:

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

Como además $k \in \mathcal{U}(\mathbb{Z}_n)$, entonces $k < n$, luego $k - 1 = 0$ y por tanto $k = 1$. Por tanto, $\ker(\Phi) = \{1\}$, y por tanto Φ es monomorfismo.

Sobreyectividad: Veamos ahora que Φ es sobreyectivo. Para ello, consideramos $f \in \operatorname{Aut}(C_n)$. Consideramos $x \in C_n$ tal que $\operatorname{mcd}(x, n) = 1$, de forma que $C_n = \langle x \rangle$. Entonces, $f(x) \in C_n$, por lo que $f(x) = x^r$ para algún $r \in \{0, \ldots, n-1\}$. Además, como f es un epimorfismo, entonces $C_n = \langle f(x) \rangle = \langle x^r \rangle$. Por tanto, $\operatorname{mcd}(r, n) = 1$, y por tanto $r \in \mathcal{U}(\mathbb{Z}_n)$. Veamos que $f = f_r$:

$$f(x^k) = f(x)^k = (x^r)^k = x^{rk} = f_r(x^k) \qquad \forall k \in \{0, \ldots, n-1\}$$

Por tanto, Φ es sobreyectivo. Por tanto, Φ es un isomorfismo.

Una vez demostrado eso, como $\mathcal{U}(\mathbb{Z}_n)$ es finito, entonces $\operatorname{Aut}(C_n)$ es finito, con:

$$|\operatorname{Aut}(C_n)| = |\mathcal{U}(\mathbb{Z}_n)| = \varphi(n)$$

Además, como $\mathcal{U}(\mathbb{Z}_n)$ es abeliano, entonces $\operatorname{Aut}(C_n)$ es abeliano.

Ejercicio 2.3.18.

1. Describir explícitamente el grupo de automorfismos $\operatorname{Aut}(C_8)$.

   Por el Ejercicio 2.3.17, sabemos que $\operatorname{Aut}(C_8) \cong \mathcal{U}(\mathbb{Z}_8)$. Calculemos $\mathcal{U}(\mathbb{Z}_8)$:

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

   Por tanto, hay cuatro automorfismos en $\operatorname{Aut}(C_8)$, que son $f_1 = id$, f_3, f_5 y f_7 (tal y como definíamos en el Ejercicio 2.3.17). Veámoslo explícitamente en la siguiente tabla:

x	$f_1(x)$	$f_3(x)$	$f_5(x)$	$f_7(x)$
1	1	1	1	1
x	x	x^3	x^5	x^7
x^2	x^2	x^6	x^2	x^6
x^3	x^3	x	x^7	x^5
x^4	x^4	x^4	x^4	x^4
x^5	x^5	x^7	x	x^3
x^6	x^6	x^2	x^6	x^2
x^7	x^7	x^5	x^3	x

2. Demostrar que $\operatorname{Aut}(C_8)$ es isomorfo al grupo de Klein.

Por el apartado anterior, sabemos que $|\operatorname{Aut}(C_8)| = 4$. Por el Ejercicio 2.3.10, sabemos que hay dos posibilidades, o bien $\operatorname{Aut}(C_8)$ es cíclico, o bien $\operatorname{Aut}(C_8) \cong V$.

Supongamos que $\operatorname{Aut}(C_8)$ es cíclico. Entonces, $\exists f \in \operatorname{Aut}(C_8) \mid O(f) = 4$. Para cada $x \in C_8$, tenemos que:

$$\begin{aligned}
(f_3 \circ f_3)(x) &= f_3(x^3) = x^9 = x \\
(f_5 \circ f_5)(x) &= f_5(x^5) = x^{25} = x \\
(f_7 \circ f_7)(x) &= f_7(x^7) = x^{49} = x
\end{aligned}$$

Por tanto, $O(f_3) = O(f_5) = O(f_7) = 2$, lo cual es una contradicción. Por tanto, $\operatorname{Aut}(C_8)$ no es cíclico, y por tanto $\operatorname{Aut}(C_8) \cong V$.

2.4. Grupos cociente. Teoremas de isomorfismo. Productos

Ejercicio 2.4.1. Demostrar que si $G \leqslant S_n$, entonces $G \subseteq A_n$ o bien se tiene que $[G : G \cap A_n] = 2$. Concluir que un subgrupo de S_n consiste sólo en permutaciones pares, o bien contiene el mismo número de permutaciones pares que de impares.

Sea $G \leqslant S_n$ un subgrupo de S_n. O bien $G \subseteq A_n$ (en cuyo caso consiste sólo de permutaciones pares); o bien $\exists \sigma \in G$ tal que $\sigma \notin A_n$, es decir, $\varepsilon(\sigma) = -1$. Para ver que $[G : G \cap A_n] = 2$, hay varias posibilidades.

Opción 1: Consideramos el homomorfismo $\varepsilon : G \to \{-1, 1\}$ dado por la aplicación signatura. Calculemos su núcleo y su imagen:

$$\ker(\varepsilon) = \{\sigma \in G \mid \varepsilon(\sigma) = 1\} = A_n \cap G,$$
$$Im(\varepsilon) = \{\varepsilon(\sigma) \mid \sigma \in G\} \overset{(*)}{=} \{-1, 1\}$$

donde vamos a razonar el por qué de $(*)$. Como $1 \in G$ por ser este un grupo, entonces $1 \in Im(\varepsilon)$, y como $\exists \sigma \in G$ tal que $\varepsilon(\sigma) = -1$, entonces $-1 \in Im(\varepsilon)$. Por lo tanto, $Im(\varepsilon) = \{-1, 1\}$. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{\ker(\varepsilon)} \cong Im(\varepsilon) \implies \frac{G}{A_n \cap G} \cong \{-1, 1\} \cong \mathbb{Z}_2.$$

Por definición de índice, se tiene que:

$$[G : A_n \cap G] = \left|\frac{G}{A_n \cap G}\right| = |\mathbb{Z}_2| = 2$$

Opción 2: Por el Teorema de Lagrange, sabemos que:

$$[S_n : A_n] = \frac{|S_n|}{|A_n|} = 2 \Longrightarrow A_n \lhd S_n$$

Aplicando el Segundo Teorema de Isomorfía a G y A_n, tenemos que:

$$\frac{G}{G \cap A_n} \cong \frac{GA_n}{A_n}$$

Veamos qué grupo es GA_n. En primer lugar, para $1 \in G$ vemos que $A_n \subset GA_n$. No obstante, como $\exists \sigma \in G$ con $\varepsilon(\sigma) = -1$, entonces $A_n \neq GA_n$, por lo que $|GA_n| > |A_n| = {}^{|S_n|}/_{2}$. Como $|GA_n| \mid |S_n|$, ha de ser $|GA_n| = |S_n|$, por lo que $GA_n = S_n$. Por tanto:

$$\frac{G}{G \cap A_n} \cong \frac{S_n}{A_n}$$

Por definición de índice, se tiene que:

$$[G : A_n \cap G] = \left|\frac{G}{A_n \cap G}\right| = \left|\frac{S_n}{A_n}\right| = \frac{|S_n|}{|A_n|} = 2$$

En cualquier caso, hemos visto que $[G : A_n \cap G] = 2$. Por el Teorema de Lagrange, se tiene que $|G| = 2 \cdot |G \cap A_n|$, por lo que la mitad de las permutaciones de G son pares. Como una permutación o bien es par o es impar, entonces la otra mitad ha de tener signatura impar. Por tanto, contiene el mismo número de permutaciones pares que de impares.

Ejercicio 2.4.2. Sea $\mathbb{K}$ un cuerpo.

1. Se considera la siguiente aplicación:

$$\begin{array}{rccc} \det : & \mathrm{GL}_n(\mathbb{K}) & \longrightarrow & \mathbb{K}^\times \\ & G & \longmapsto & \det(G) \end{array}$$

Demostrar que dicha aplicación es un epimorfismo de grupos. ¿Cuál es el núcleo de este homomorfismo?

Para comprobar que se trata de un homomorfismo, tomamos $A, B \in \mathrm{GL}_n(\mathbb{K})$ y por las propiedades de la determinante, se tiene que:

$$\det(AB) = \det(A) \cdot \det(B)$$

Por otro lado, para cada $a \in \mathbb{K}^\times$, se considera la siguiente matriz:

$$A_a = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Como $\det(A_a) = a \neq 0$, entonces $A_a \in \mathrm{GL}_n(\mathbb{K})$. Como $\det(A_a) = a$, se tiene que det es sobreyectiva. Por lo tanto, det es un epimorfismo de grupos. Su núcleo es:

$$\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{K}) \mid \det(A) = 1\} = \mathrm{SL}_n(\mathbb{K})$$

2. Si $\mathbb{K}$ es un cuerpo finito con q elementos, determinar el orden del grupo $\mathrm{SL}_n(\mathbb{K})$.

Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{\mathrm{GL}_n(\mathbb{K})}{\mathrm{SL}_n(\mathbb{K})} \cong \mathbb{K}^\times$$

Por el Teorema de Lagrange, se tiene que:

$$|\mathrm{SL}_n(\mathbb{K})| = \frac{|\mathrm{GL}_n(\mathbb{K})|}{|\mathbb{K}^\times|} = \frac{|\mathrm{GL}_n(\mathbb{K})|}{q-1} = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{q-1}$$

Ejercicio 2.4.3. Sea $n \in \mathbb{N} \setminus \{0\}$, y sea G un grupo verificando que para todo par de elementos $x, y \in G$ se tiene que $(xy)^n = x^n y^n$. Se definen:

$$\begin{aligned} H &= \{x \in G \mid x^n = 1\}, \\ K &= \{x^n \mid x \in G\}. \end{aligned}$$

Demostrar que $H, K \lhd G$, y que $|K| = [G : H]$.

Definimos en primer lugar la siguiente aplicación:

$$\begin{array}{rccc} f: & G & \longrightarrow & G \\ & x & \longmapsto & x^n \end{array}$$

Para demostrar que se trata de un homomorfismo emplearemos la propiedad dada en el enunciado $(*)$:

$$f(xy) = (xy)^n \overset{(*)}{=} x^n y^n = f(x)f(y) \qquad \forall x, y \in G$$

Por tanto, f es un homomorfismo. Como $\{1\}, G < G$, entonces los siguientes grupos son subgrupos de G:

$$\begin{aligned} f^*(\{1\}) &= \{x \in G \mid f(x) = 1\} = \{x \in G \mid x^n = 1\} = H = \ker(f), \\ f_*(G) &= \{f(x) \mid x \in G\} = \{x^n \mid x \in G\} = K = Im(f). \end{aligned}$$

Por tanto, tenemos que $H, K < G$. Probamos ahora que son grupos normales en G. Como $H = \ker f$ y f es un homomorfismo, se tiene que $H \lhd G$. Ahora probamos que K es normal en G. Tomamos $x \in G$ y $k \in K$ (por lo que $\exists y \in G$ tal que $k = y^n$). Entonces, consideramos $xyx^{-1} \in G$ y calculamos:

$$xkx^{-1} = x(y^n)x^{-1} = (xyx^{-1})^n \in K$$

Por tanto, $K \lhd G$. Para probar que $|K| = [G : H]$, tomamos el homomorfismo f anteriormente descrito. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{H} \cong K \implies |K| = \left|\frac{G}{H}\right| = [G : H]$$

Ejercicio 2.4.4. Para un grupo G se define su *centro* como

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

1. Demostrar que $Z(G) < G$.

   Como $Z(G) \subset G$, hay dos principales posibilidades, ambas equivalentes:

   Opción 1: Comprobamos las tres condiciones que caracterizan a los subgrupos:

   - $1 \in Z(G)$: Para todo $x \in G$, se tiene que $1x = x1 = x$.
   - $a, b \in Z(G) \implies ab \in Z(G)$: Para todo $x \in G$, se tiene que:

     $$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

   - $a \in Z(G) \implies a^{-1} \in Z(G)$: Para todo $x \in G$, se tiene que:

     $$a^{-1}x = (x^{-1}a)^{-1} = (ax^{-1})^{-1} = xa^{-1}.$$

   Opción 2: Dados $a, b \in Z(G)$, comprobemos que $ab^{-1} \in Z(G)$:

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

En cualquier caso, $Z(G)$ es un subgrupo de G.

2. Demostrar que $Z(G) \lhd G$.

De nuevo, hay dos posibilidades:

Opción 1: Para $x \in G$. Entonces:

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

Opción 2: Empleamos la caracterización de subgrupo normal. Para $x \in G$ y $z \in Z(G)$, buscamos ver que $xzx^{-1} \in Z(G)$:

$$xzx^{-1}y = zxx^{-1}y = zy = yz = yzxx^{-1} = yxzx^{-1} \qquad \forall y \in G.$$

En ambos casos, se tiene que $Z(G) \lhd G$.

3. Demostrar que G es abeliano si, y sólo si, $G = Z(G)$.

$$G = Z(G) \iff G = \{a \in G \mid ax = xa\, \forall x \in G\} \iff ax = xa\, \forall a, x \in G \iff G \text{ es abeliano.}$$

4. Demostrar que si $G/Z(G)$ es cíclico, entonces G es abeliano.

Como $G/Z(G)$ es cíclico, entonces existe $x \in G$ tal que $G/Z(G) = \langle xZ(G)\rangle$. Como las clases de equivalencia forman una partición disjunta de G, para cada $y \in G$ existe $k \in \mathbb{Z}$ tal que $y \in x^k Z(G)$. Buscamos ahora demostrar que G es abeliano. Dados $a, b \in G$, entonces existen $p, q \in \mathbb{Z}$ tales que $a \in x^p Z(G)$ y $b \in x^q Z(G)$. Entonces, existen $z_a, z_b \in Z(G)$ tales que $a = x^p z_a$ y $b = x^q z_b$. Por tanto:

$$ab = (x^p z_a)(x^q z_b) = x^{p+q} z_a z_b = x^q z_b x^p z_a = (x^q z_b)(x^p z_a) = ba$$

Por tanto, $ab = ba$ para todo $a, b \in G$, por lo que G es abeliano.

Ejercicio 2.4.5. Determinar el centro del grupo diédrico D_4. Observar que el cociente $D_4/Z(D_4)$ es abeliano, aunque D_4 no lo sea (compárese este hecho con el tercer apartado del ejercicio anterior).

El grupo D_4 está formado por las siguientes rotaciones y reflexiones:

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

Sabemos que $Z(D_4)$ es un subgrupo normal de D_4. En primer lugar, sabemos que $1 \in Z(D_4)$. Veamos que $r^2 \in Z(D_4)$. En primer lugar, vemos que conmuta con todas las potencias de r. Veamos ahora que conmuta con el resto de elementos:

$$\begin{aligned} r^2 s &= rsr^3 = sr^6 = sr^2 \\ r^2\ sr &= sr^2 r = sr\ r^2 \\ r^2\ sr^2 &= srr^2 r = s = sr^4 = sr^2\ r^2 \\ r^2\ sr^3 &= sr = sr^5 = sr^3\ r^2 \end{aligned}$$

Por tanto, $\{1, r^2\} \subset Z(D_4)$. Además, tenemos que:

$$\begin{aligned}
sr = r^3 s \neq rs &\Longrightarrow s, r \notin Z(D_4)\\
sr^3 = r^9 s = rs \neq r^3 s &\Longrightarrow r^3 \notin Z(D_4)\\
sr\ s = r^3 \neq r &\Longrightarrow sr \notin Z(D_4)\\
sr^3\ s = r \neq r^3 &\Longrightarrow sr^3 \notin Z(D_4)
\end{aligned}$$

Como $|Z(D_4)|$ divide a $|D_4| = 8$ y $2 \leqslant |Z(D_4)| \leqslant 3$, se tiene que $|Z(D_4)| = 2$. Por tanto,

$$Z(D_4) = \{1, r^2\}$$

Veamos que $D_4/Z(D_4)$ es abeliano. Sabemos que:

$$|D_4/Z(D_4)| = \frac{|D_4|}{|Z(D_4)|} = \frac{8}{2} = 4$$

Por tanto, $D_4/Z(D_4)$ es isomorfo a V o a C_4. Por el último apartado del ejercicio anterior, si fuese $D_4/Z(D_4)$ isomorfo a C_4, entonces D_4 sería abeliano. Como no lo es, se tiene que $D_4/Z(D_4) \cong V$. Como V es abeliano, se tiene que $D_4/Z(D_4)$ también lo es.

Ejercicio 2.4.6. Determinar el centro de los grupos S_n y A_n para $n \geqslant 2$.

Para $n = 2$, tenemos que:

$$\begin{aligned}
S_2 = \{1, (1\ 2)\} &\implies Z(S_2) = S_2\\
A_2 = \{1\} &\implies Z(A_2) = A_2
\end{aligned}$$

Calculamos ahora $Z(S_n)$ para $n \geqslant 3$. Sea $\sigma \neq 1 \in S_n$. Entonces,$\exists i, j \in \{1, \dots, n\}$ tales que $i \neq j$ y $\sigma(i) = j$. Consideramos ahora $k \in \{1, \dots, n\}$ tal que $k \neq i, j$, y sea la permutación $\tau = (j\ k)$. Entonces:

$$\begin{aligned}
\sigma\tau(i) = \sigma(i) = j\\
\tau\sigma(i) = \tau(j) = k
\end{aligned}$$

Por tanto, $\sigma\tau \neq \tau\sigma$. Como σ es arbitrario, se tiene que $Z(S_n) = \{1\}$ para $n \geqslant 3$.

Trabajamos ahora con A_n. En primer lugar, para $n = 3$ tenemos que $|A_3| = 3$ primo, por lo que A_3 es cíclico y en particular abeliano. Por tanto, $Z(A_3) = A_3$.

Para $n \geqslant 4$, sea $\sigma \in A_n$ tal que $\sigma \neq 1$. Entonces, $\exists i, j \in \{1, \dots, n\}$ tales que $i \neq j$ y $\sigma(i) = j$. Consideramos ahora $k, l \in \{1, \dots, n\} \setminus \{i, j\}$, tal que $k \neq l$. Consideramos ahora $\tau = (j\ k\ l) \in A_n$. Entonces:

$$\begin{aligned}
\sigma\tau(i) = \sigma(i) = j\\
\tau\sigma(i) = \tau(j) = k
\end{aligned}$$

Por tanto, $\sigma\tau \neq \tau\sigma$. Como σ es arbitrario, se tiene que $Z(A_n) = \{1\}$ para $n \geqslant 4$. Notemos que hemos tenido que imponer que $n \geqslant 4$ para que podamos elegir 4 elementos distintos.

Ejercicio 2.4.7. Determinar el centro del grupo D_n para $n \geqslant 3$.

Dado $z \in D_n$, como $D_n = \langle r, s\rangle$ entonces $z \in Z(D_n)$ si y sólo si z conmuta con r y con s. Distinguimos según los elementos de D_n:

- $1 \in Z(D_n)$ para todo $n \geqslant 3$.
- Fijado $m \in \{1, \dots, n-1\}$, veamos si $r^m \in Z(D_n)$.

  $r^m\ r = r^{m+1} = r\ r^m$

  $r^m\ s = sr^{m(n-1)} = sr^{-m} = sr^{n-m} = s\ r^m \iff r^{n-m} = r^m \overset{(*)}{\iff} n-m = m \iff n = 2m$

  donde en $(*)$ hemos usado que $n-m, m \in \{1, \dots, n-1\}$. Por tanto, hay que distinguir según la paridad de n:

  - Si n es impar, entonces $r^m \notin Z(D_n)$ para todo $m \in \{1, \dots, n-1\}$.
  - Si n es par, entonces $r^{n/2} \in Z(D_n)$, y $r^m \notin Z(D_n)$ para todo valor de $m \in \{1, \dots, n-1\} \setminus \{n/2\}$.

- Fijado $m \in \{0, \dots, n-1\}$, veamos si $sr^m \in Z(D_n)$.

$$\begin{aligned} sr^m\ r &= sr^{m+1} = r^{(m+1)(n-1)}s = r^{mn-m+n-1}s = r^{n-m-1}s \\ r\ sr^m &= r\ r^{n-m}s = r^{n-m+1}s \end{aligned}$$

  Por tanto, se necesita que $r^{n-m-1} = r^{n-m+1}$, y equivalentemente se necesita que $r^{-1} = r$, es decir, que $r^2 = 1$. Esto es cierto para $n = 2$, pero no para $n \geqslant 3$. Por tanto, $sr^m \notin Z(D_n)$ para todo $m \in \{0, \dots, n-1\}$.

En resumen, tenemos que:

- Si n es impar, entonces $Z(D_n) = \{1\}$.
- Si n es par, entonces $Z(D_n) = \{1, r^{n/2}\}$.

Ejercicio 2.4.8. Sean H y K dos subgrupos finitos de un grupo G, uno de ellos normal. Demostrar que

$$|H||K| = |HK||H \cap K|.$$

Sean $H, K < G$, y $K \lhd G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

Tomando índices y usando el Teorema de Lagrange, se tiene que:

$$\left|\frac{HK}{K}\right| = \frac{|HK|}{|K|} = \left|\frac{H}{H \cap K}\right| = \frac{|H|}{|H \cap K|} \Longrightarrow |H||K| = |HK||H \cap K|.$$

Si por el contrario $H \lhd G$, entonces:

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

y de igual forma se llega a la misma conclusión.

Ejercicio 2.4.9. Sea G finito y $N \lhd G$. Probar que $G/N \cong G$ si, y sólo si, $N = \{1\}$, y que $G/N \cong \{1\}$ si, y sólo si, $N = G$.

Veamos que $G/N \cong G$ si, y sólo si, $N = \{1\}$.

$\Longrightarrow$) Supongamos que $G/N \cong G$. Entonces, por el Teorema de Lagrange, se tiene que:
$$|G| = |G/N| = \frac{|G|}{|N|} \Longrightarrow |N| = 1 \Longrightarrow N = \{1\}.$$

$\Longleftarrow$) Supongamos que $N = \{1\}$.

Opción 1: Opción Directa

$$G/N = G/\{1\} = \{x\{1\} \mid x \in G\} = \{\{x\} \mid x \in G\}$$

Consideramos ahora la proyección canónica $p : G \to G/N$. Sabemos que es un homomorfismo sobreyectivo. Veamos ahora que es inyectivo. Sean $x, y \in G$ tales que $p(x) = p(y)$. Entonces, tenemos que:

$$p(x) = p(y) \Longrightarrow x\{1\} = y\{1\} \Longrightarrow \{x\} = \{y\} \Longrightarrow x = y.$$

Por tanto, p es un isomorfismo, luego $G/N \cong G$.

Opción 2: Definimos ahora el homomorfismo siguiente:

$$\begin{array}{rccc} f: & G & \longrightarrow & G \\ & x & \longmapsto & x \end{array}$$

Tenemos que:

$$\begin{aligned} &\ker(f) = \{x \in G \mid f(x) = 1\} = \{x \in G \mid x = 1\} = \{1\} = N, \\ &Im(f) = \{f(x) \mid x \in G\} = \{x \mid x \in G\} = G \end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

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

Veamos ahora que $G/N \cong \{1\}$ si, y sólo si, $N = G$.

$\Longrightarrow$) Supongamos que $G/N \cong \{1\}$. Entonces, por el Teorema de Lagrange, se tiene que:
$$1 = |G/N| = \frac{|G|}{|N|} \Longrightarrow |G| = |N|$$

Como $N \leqslant G$, se tiene que $N \subset G$, y por tanto $N = G$.

$\Longleftarrow$) Supongamos que $N = G$. Entonces, definimos el homomorfismo siguiente:

$$\begin{array}{rccc} f: & G & \longrightarrow & \{1\} \\ & x & \longmapsto & 1 \end{array}$$

Entonces, tenemos que:

$$\begin{aligned}
\ker(f) &= \{x \in G \mid f(x) = 1\} = \{x \in G \mid 1 = 1\} = G = N, \\
Im(f) &= \{f(x) \mid x \in G\} = \{1 \mid x \in G\} = \{1\}
\end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{N} \cong \{1\}$$

Observación. Notemos que en las implicaciones hacia la izquierda no es necesario suponer que G es finito. Lo usaremos por tanto sin esta restricción.

Ejercicio 2.4.10. Sean G y H dos grupos cuyos órdenes sean primos relativos. Probar que si $f : G \to H$ es un homomorfismo, entonces necesariamente $f(x) = 1$ para todo $x \in G$, es decir, que el único homomorfismo entre ellos es el trivial.

Opción 1

Como $|G|$ y $|H|$ son primos relativos, en particular son grupos finitos. Por ser f un homomorfismo, se tiene que $f(G) < H$, luego $|f(G)| \mid |H|$. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{\ker(f)} \cong f(G) \implies |G| = |\ker(f)| \cdot |f(G)| \Longrightarrow |f(G)| \mid |G|$$

Como $\text{mcd}(|G|, |H|) = 1$, se tiene que $|f(G)| = 1$. Como además $f(G)$ es un grupo, se tiene que $f(G) = \{1\}$. Por tanto, f es el homomorfismo trivial.

Opción 2

Sea $y \in f(G)$. Entonces, $\exists x \in G$, tal que $f(x) = y$. Como G es finito, $\exists n \in \mathbb{N}$ tal que $\text{ord}(x) = n$, luego $n \mid |G|$. Por otro lado:

$$1 = f(1) = f(x^n) = f(x)^n = y^n \in H \Longrightarrow \text{ord}(y) \mid n$$

Como $\text{ord}(y) \mid n$ y $n \mid |G|$, se tiene que $\text{ord}(y) \mid |G|$. Por tanto, como $y \in H$, entonces $\text{ord}(y) \mid |H|$. Por tanto, $\text{ord}(y)$ divide a $\text{mcd}(|G|, |H|)$. Como $|G|$ y $|H|$ son primos relativos, se tiene que $\text{mcd}(|G|, |H|) = 1$, luego $\text{ord}(y) = 1$. Por tanto, $y = 1$ para todo $y \in f(G)$, luego $f(x) = 1$ para todo $x \in G$. Por tanto, f es el homomorfismo trivial.

Ejercicio 2.4.11. Sean $H, K \leqslant G$, y sea $N \lhd G$ un subgrupo normal de G tal que $HN = KN$. Demostrar que

$$\frac{H}{H \cap N} \cong \frac{K}{K \cap N}.$$

Aplicamos dos veces el Segundo Teorema de Isomorfía:

- Consideramos $H, N \leqslant G$, con $N \lhd G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

- Consideramos $K, N \leqslant G$, con $N \lhd G$. Entonces, por el Segundo Teorema de Isomorfía, se tiene que:
$$\frac{KN}{N} \cong \frac{K}{K \cap N}$$

Como $KN = HN$ y "ser isomorfo" es una relación de equivalencia, se tiene que:

$$\frac{H}{H \cap N} \cong \frac{HN}{N} = \frac{KN}{N} \cong \frac{K}{K \cap N}$$

Ejercicio 2.4.12. Sea $N \lhd G$ tal que N y G/N son abelianos. Sea H un subgrupo cualquiera de G. Demostrar que existe un subgrupo normal $K \lhd H$ tal que K y H/K son abelianos.

Por el Segundo Teorema de Isomorfía, se tiene que $K = H \cap N \lhd H$. Como $K \subset N$ y K es un grupo, entonces $K \leqslant N$. Como N es abeliano, se tiene que K también lo es. Nos falta por ver que H/K es abeliano. Por el Segundo Teorema de Isomorfía, se tiene que:
$$\frac{H}{K} \cong \frac{HN}{N}$$

Veamos ahora que $HN/N \leqslant G/N$. Como $HN \subset G$, por definición de conjunto cociente se tiene que $HN/N \subset G/N$. Como HN/N es un grupo, se tiene que $HN/N \leqslant G/N$. Como G/N es abeliano, se tiene que HN/N también lo es. Por tanto, por el Segundo Teorema de Isomorfía, se tiene que H/K es abeliano.

Ejercicio 2.4.13. Sea G un grupo finito, y sean $H, K \leqslant G$, con $K \lhd G$ y tales que $|H|$ y $[G : K]$ son primos relativos. Demostrar que $H \subseteq K$.

Por el Segundo Teorema de Isomorfía, se tiene que:

$$\frac{H}{H \cap K} \cong \frac{HK}{K}$$

Como $HK \leqslant G$, entonces $HK/K \leqslant G/K$. Por tanto $\left|\frac{H}{H\cap K}\right| = \left|\frac{HK}{K}\right|$ divide a $\left|\frac{G}{K}\right| = [G : K]$. Por otro lado:

$$\left|\frac{H}{H \cap K}\right| = \frac{|H|}{|H \cap K|} \Longrightarrow |H| = |H \cap K| \cdot \left|\frac{H}{H \cap K}\right| \Longrightarrow \left|\frac{H}{H \cap K}\right| \mid |H|$$

Como $\text{mcd}(|H|, [G : K]) = 1$, se tiene que $\left|\frac{H}{H\cap K}\right| = 1$. Por tanto, $|H| = |H \cap K|$, y como $H \cap K \subset H$, se tiene que $H \cap K = H$. Por tanto, $H \subset K$.

Ejercicio 2.4.14. Sea G un grupo.

1. Demostrar que para cada $a \in G$ la aplicación $\varphi_a : G \to G$ definida por $\varphi_a(x) = axa^{-1}$, es un automorfismo de G. φ_a se llama automorfismo interno o de conjugación de G definido por a.

   Vemos en primer lugar que está bien definida, puesto que un grupo es cerrado para inversos y productos. Por tanto, $\varphi_a(x) \in G$ para todo $x \in G$. Veamos ahora que es un isomorfismo:

- Para ver que es un homomorfismo:

$$\varphi_a(xy) = a(xy)a^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y) \qquad \forall x, y \in G$$

- Para ver que es inyectiva, sean $x, y \in G$ de forma que:

$$\varphi_a(x) = axa^{-1} = aya^{-1} = \varphi_a(y)$$

Entonces, aplicando dos veces la propiedad cancelativa, tenemos que:

$$axa^{-1} = aya^{-1} \Longrightarrow ax = ay \Longrightarrow x = y$$

- Para ver que es sobreyectiva, sea $y \in G$, tomamos $x = a^{-1}ya$. Entonces:

$$\varphi_a(x) = \varphi_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = aa^{-1}yaa^{-1} = y$$

Concluimos que φ_a es un automorfismo de G.

2. Demostrar que la siguiente aplicación es un homomorfismo:

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & \mathrm{Aut}(G) \\ & a & \longmapsto & \varphi_a \end{array}$$

Para esto, es necesario probar que, fijados $a, b \in G$, se tiene que:

$$\varphi_{ab} = \varphi_a \circ \varphi_b$$

Tenemos que:

$$\varphi_{ab}(x) = (ab)x(ab)^{-1} = (ab)x(b^{-1}a^{-1}) = a(bxb^{-1})a^{-1} = a\varphi_b(x)a^{-1} = \varphi_a(\varphi_b(x)) \qquad \forall x \in G$$

Por tanto, $\varphi_{ab} = \varphi_a \circ \varphi_b$. Por tanto, φ es un homomorfismo de grupos.

3. Demostrar que el conjunto de automorfismos internos de G, que se denota $\mathrm{Int}(G)$, es un subgrupo normal de $\mathrm{Aut}(G)$.

Para ello, en primer lugar es necesario ver que $\mathrm{Int}(G) < \mathrm{Aut}(G)$. Considerados $a, b \in G$, tenemos que:

$$\begin{aligned}(\varphi_a \circ \varphi_b^{-1})(x) &= \varphi_a\left(b^{-1}xb\right) = a\left(b^{-1}xb\right)a^{-1} = ab^{-1}xba^{-1} = \\ &= (ab^{-1})x(ab^{-1})^{-1} = \varphi_{ab^{-1}}(x) \qquad \forall x \in G\end{aligned}$$

Veamos ahora que $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$. Para ello es necesario ver que se tiene $f \circ \varphi \circ f^{-1} \in \mathrm{Int}(G)$ para todo $f \in \mathrm{Aut}(G)$ y $\varphi \in \mathrm{Int}(G)$. Sea $f \in \mathrm{Aut}(G)$ y $\varphi_a \in \mathrm{Int}(G)$. Entonces, tenemos que:

$$\begin{aligned}(f \circ \varphi_a \circ f^{-1})(x) &= f\left(\varphi_a(f^{-1}(x))\right) = f\left(a(f^{-1}(x))a^{-1}\right) \\ &= f(a)f(f^{-1}(x))f(a^{-1}) = f(a)xf(a^{-1}) = \varphi_{f(a)}(x) \in \mathrm{Int}(G)\end{aligned}$$

Por tanto, $f \circ \varphi_a \circ f^{-1} \in \mathrm{Int}(G)$, y por tanto $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$.

4. Demostrar que $G/Z(G) \cong \text{Int}(G)$.

   Buscamos aplicar el Primer Teorema de Isomorfía al homomorfismo φ del apartado 2. Tenemos que:

$$\begin{aligned}
\ker(\varphi) &= \{a \in G \mid \varphi_a = \text{Id}_G\} = \{a \in G \mid \varphi_a(x) = x \ \forall x \in G\} \\
&= \{a \in G \mid axa^{-1} = x \ \forall x \in G\} = \{a \in G \mid ax = xa \ \forall x \in G\} = Z(G) \\
Im(\varphi) &= \{\varphi_a \mid a \in G\} = \{f \in \text{Aut}(G) \mid f(x) = axa^{-1} \ \forall x \in G\} = \text{Int}(G)
\end{aligned}$$

   Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{Z(G)} \cong \text{Int}(G)$$

5. Demostrar que $\text{Int}(G) = \{\text{Id}_G\}$ si y sólo si G es abeliano.

   Opción 1.

   $\Longrightarrow$) Supongamos que $\text{Int}(G) = \{\text{Id}_G\}$. Entonces, para todo $a \in G$, se tiene que:
$$\varphi_a = \text{Id}_G \Longrightarrow axa^{-1} = x \ \forall x \in G$$
   Por tanto, $ax = xa \ \forall x \in G$. Como a es arbitrario, se tiene que G es abeliano.

   $\Longleftarrow$) Supongamos que G es abeliano. Entonces, para todo $a \in G$, se tiene que:
$$\varphi_a(x) = axa^{-1} = aa^{-1}x = x \ \forall x \in G$$
   Por tanto, $\varphi_a = \text{Id}_G$. Como a es arbitrario, concluimos entonces que $\text{Int}(G) = \{\text{Id}_G\}$.

   Opción 2. (Esta opción solo es válida si G es finito).
   Como $G/Z(G) \cong \text{Int}(G)$, aplicando el Ejercicio 2.4.9, tenemos que:

$$\text{Int}(G) = \{1\} \Longleftrightarrow G = Z(G) \Longleftrightarrow G \text{ es abeliano}$$

Ejercicio 2.4.15. Demostrar que el grupo de automorfismos de un grupo no abeliano no puede ser cíclico.

Sea G un grupo no abeliano. Por el recíproco del Ejercicio 2.4.4.4, sabemos que $G/Z(G)$ no es cíclico. Como $G/Z(G) \cong \text{Int}(G)$, se tiene que $\text{Int}(G)$ no es cíclico. Como $\text{Int}(G) < \text{Aut}(G)$ y todo subgrupo de un grupo cíclico es cíclico, se tiene que $\text{Aut}(G)$ no es cíclico.

Ejercicio 2.4.16. Demostrar que $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

Sabemos que:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V^{\text{abs}} = \langle x, y \mid x^2 = y^2 = 1, xy = yx\rangle$$

Construimos ahora automorfismos de $\mathbb{Z}_2 \times \mathbb{Z}_2$. Sabemos que todos los elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ (a excepción del neutro) son de orden 2, y además este grupo es conmutativo. Por tanto, con el Teorema de Dyck podemos constuir automorfismos de forma sencilla. Haciendo uso de que $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (1,0),(0,1) \rangle$, tenemos los siguientes automorfismos:

	f_1	f_2	f_3	f_4	f_5	f_6
$f_i(1,0)$	$(1,0)$	$(1,0)$	$(0,1)$	$(0,1)$	$(1,1)$	$(1,1)$
$f_i(0,1)$	$(0,1)$	$(1,1)$	$(1,0)$	$(1,1)$	$(0,1)$	$(1,0)$

Además, no puede haber más automorfismos, puesto que fijada la imagen de un elemento generador, la imagen del otro elemento generador tan solo tiene dos posibilidades, puesto que no puede ser el neutro. Por tanto, tenemos que:

$$|\operatorname{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)| = 6$$

Por tanto, $\operatorname{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ es un grupo de orden 6, por lo que es cíclico o es isomorfo a $D_3 \cong S_3$. Tenemos que:

$$(f_2 \circ f_3)(1,0) = f_2(f_3(1,0)) = f_2(0,1) = (1,1)$$
$$(f_3 \circ f_2)(1,0) = f_3(f_2(1,0)) = f_3(1,0) = (0,1)$$

Por tanto, $f_2 \circ f_3 \neq f_3 \circ f_2$, por lo que $\operatorname{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ no es abeliano y por tanto no es cíclico. Por tanto, $\operatorname{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

Ejercicio 2.4.17. Demostrar que los grupos S_3, $\mathbb{Z}_{p^n}$ (con p primo) y $\mathbb{Z}$ no son producto directo internos de subgrupos propios.

1. S_3.

   Como $|S_3| = 6$, entonces sus subgrupos propios son de orden 2 y 3. Por reducción al absurdo, supongamos que $S_3 \cong K_1 \times \cdots \times K_n$ con $K_i < S_3$. Entonces, $6 = |K_1||K_2| \cdots |K_n|$, y como $|K_i|$ son divisores de 6, se tiene que $|K_i| = 2$ o $|K_i| = 3$. Como $6 = 2 \cdot 3$ es la única opción, se tiene que $n = 2$. Por tanto, $S_3 \cong K_1 \times K_2$ con $K_1, K_2 < S_3$. Sin pérdida de generalidad, supongamos que $|K_1| = 2$ y $|K_2| = 3$. Entonces, $K_1 \cong C_2$ y $K_2 \cong C_3$. Por tanto, $S_3 = K_1 \times K_2 \cong C_2 \oplus C_3$. Como C_2 y C_3 son cíclicos con $\operatorname{mcd}(|C_2|, |C_3|) = 1$, se tiene que $C_2 \oplus C_3$ es cíclico. Por tanto, S_3 es cíclico, lo cual es una contradicción.

2. $\mathbb{Z}_{p^n}$.

   Por ser $\mathbb{Z}_{p^n}$ un grupo cíclico de orden p^n, todos sus subgrupos propios son cíclicos de orden p^k con $k \in \{1, \ldots, n-1\}$. Por reducción al absurdo, supongamos que $\exists p_1, \cdots, p_k \in \{1, \ldots, n-1\}$ tales que $\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{p_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{p_k}}$. Entonces, como $\mathbb{Z}_{p^{p_i}}$ es cíclico, se tiene que $\mathbb{Z}_{p^{p_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{p_k}}$ es cíclico si y solo si $\operatorname{mcd}(p^{p_1}, \ldots, p^{p_k}) = 1$. Como p^{p_i} son potencias de un mismo primo, se tiene que $\operatorname{mcd}(p^{p_1}, \ldots, p^{p_k}) \geqslant p$. Por tanto, $\mathbb{Z}_{p^{p_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{p_k}}$ no es cíclico. Por tanto, $\mathbb{Z}_{p^n}$ no es producto directo interno de subgrupos propios.

3. $\mathbb{Z}$.

   Sabemos que todos los subgrupos de $\mathbb{Z}$ son de la forma $k\mathbb{Z}$, con $k \in \mathbb{N}$. Por tanto, por reducción al absurdo, supongamos que $\exists p_1, \cdots, p_k \in \mathbb{N}$ tales que $\mathbb{Z} \cong p_1\mathbb{Z} \oplus \cdots \oplus p_k\mathbb{Z} \overset{(*)}{\cong} \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. Veamos no obstante que $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ no es cíclico.

Supongamos que $\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$ es cíclico. Entonces, existe $(x_1,\ldots,x_k)\in\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$ tal que:

$$\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}=\langle(x_1,\ldots,x_k)\rangle$$

Sea ahora $(1,0,\ldots,0)\in\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$. Entonces, existe $n\in\mathbb{N}$ tal que:

$$(1,0,\ldots,0)=n(x_1,\ldots,x_k)\Longrightarrow x_2=\cdots=x_k=0$$

Sea ahora $(0,1,0,\ldots,0)\in\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$. Entonces, existe $m\in\mathbb{N}$ tal que:

$$(0,1,0,\ldots,0)=m(x_1,0,\ldots,0)\Longrightarrow 1=m\cdot 0$$

Por tanto, hemos llegado a una contradicción. Por tanto, $\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$ no es cíclico. Por tanto, $\mathbb{Z}$ no es producto directo interno de subgrupos propios.

En $(*)$, el isomorfismo es el siguiente (que se prueba fácilmente que es un isomorfismo):

$$\begin{array}{rccc} f: & n\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & x/n \end{array}$$

Ejercicio 2.4.18. En cada uno de los siguientes casos, decidir si el grupo G es o no producto directo interno de los subgrupos H y K.

1. $G=\mathbb{R}^\times$, $H=\{\pm1\}$, $K=\{x\in\mathbb{R}\mid x>0\}$.

   Es directo que que $G=HK$ y $H\cap K=\{1\}$. Como $H,K<G$ y G es abeliano, se tiene que $H,K\lhd G$. Por tanto, $G\cong H\times K$.

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

   Fijados $a,b,c\in\mathbb{R}$, sean las siguientes matrices:

   $$A=\begin{pmatrix} a & 0\\ 0 & c\end{pmatrix}\in H$$
   $$B=\begin{pmatrix} 1 & b\\ 0 & 1\end{pmatrix}\in K$$

   Entonces:

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

   Como $ab\neq bc$ en general, se tiene que $AB\neq BA$. Por tanto, por la caracterización del producto directo interno, se tiene que G no es producto directo interno de H y K.

3. $G = \mathbb{C}^\times$, $H = \{z \in \mathbb{C} \mid |z| = 1\}$, $K = \{x \in \mathbb{R} \mid x > 0\}$.

   Dado $z \in G$, podemos escribir:

$$z = \frac{z}{|z|} \cdot |z| \qquad \frac{z}{|z|} \in H,\ |z| \in K$$

   Por tanto, $G = HK$. Además, $H \cap K = \{1\}$, y como $H, K < G$ y G es abeliano, se tiene que $H, K \lhd G$. Por tanto, $G \cong H \times K$.

Ejercicio 2.4.19. Sean G, H y K grupos. Demostrar que:

1. $H \times K \cong K \times H$.

   Definimos el isomorfismo:

$$\begin{array}{rccc} f: & H \times K & \longrightarrow & K \times H \\ & (h,k) & \longmapsto & (k,h) \end{array}$$

   Vemos que f es un isomorfismo:

   - f es un homomorfismo:

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f(h_1h_2, k_1k_2) = (k_1k_2, h_1h_2) \\ &= (k_1,h_1)(k_2,h_2) = f(h_1,k_1)f(h_2,k_2) \end{aligned}$$

   - f es inyectiva:

$$\begin{aligned} \ker(f) &= \{(h,k) \in H \times K \mid f(h,k) = (1,1)\} \\ &= \{(h,k) \in H \times K \mid (k,h) = (1,1)\} = \{(1,1)\} \end{aligned}$$

   - f es sobreyectiva:
     Dado $(k,h) \in K \times H$, tomamos $(h,k) \in H \times K$. Entonces:

$$f(h,k) = (k,h) \qquad \forall (h,k) \in H \times K$$

   Por tanto, f es un isomorfismo.

2. $G \times (H \times K) \cong (G \times H) \times K$.

   Definimos el isomorfismo:

$$\begin{array}{rccc} f: & G \times (H \times K) & \longrightarrow & (G \times H) \times K \\ & (g,(h,k)) & \longmapsto & ((g,h),k) \end{array}$$

   Vemos que f es un isomorfismo:

   - f es un homomorfismo:

$$\begin{aligned} f((g_1,(h_1,k_1))(g_2,(h_2,k_2))) &= f(g_1g_2,(h_1h_2,k_1k_2)) \\ &= ((g_1g_2,h_1h_2),k_1k_2) = \\ &= ((g_1,h_1),k_1)((g_2,h_2),k_2) = \\ &= f(g_1,(h_1,k_1))f(g_2,(h_2,k_2)) \end{aligned}$$

- f es inyectiva:

$$\begin{aligned}\ker(f) &= \{(g,(h,k)) \in G\times(H\times K) \mid f(g,(h,k)) = ((1,1),1)\} \\ &= \{(g,(h,k)) \in G\times(H\times K) \mid ((g,h),k) = ((1,1),1)\} = \{(1,(1,1))\}\end{aligned}$$

- f es sobreyectiva:
Dado $((g,h),k) \in (G\times H)\times K$, tomamos $(g,(h,k)) \in G\times(H\times K)$. Entonces:

$$f(g,(h,k)) = ((g,h),k) \qquad \forall (g,(h,k)) \in G\times(H\times K)$$

Por tanto, f es un isomorfismo.

Ejercicio 2.4.20. Dados isomorfismos de grupos $A\cong K$ y $B\cong H$, demostrar que $A\times B\cong K\times H$.

Sea $f : A\to K$ y $g : B\to H$ los isomorfismos. Definimos la siguiente aplicación:

$$\begin{array}{rccc} h: & A\times B & \longrightarrow & K\times H \\ & (a,b) & \longmapsto & (f(a),g(b)) \end{array}$$

Veamos que h es un homomorfismo. Fijados $(a_1,b_1),(a_2,b_2)\in A\times B$, tenemos que:

$$\begin{aligned}h((a_1,b_1)(a_2,b_2)) &= h(a_1a_2,b_1b_2) = (f(a_1a_2),g(b_1b_2)) \\ &= (f(a_1)f(a_2),g(b_1)g(b_2)) = (f(a_1),g(b_1))(f(a_2),g(b_2)) \\ &= h(a_1,b_1)h(a_2,b_2) \qquad \forall (a_1,b_1),(a_2,b_2)\in A\times B\end{aligned}$$

Por tanto, h es un homomorfismo. Veamos ahora que es inyectiva. Para ello, tenemos que:

$$\begin{aligned}\ker(h) &= \{(a,b)\in A\times B \mid h(a,b) = (1,1)\} \\ &= \{(a,b)\in A\times B \mid (f(a),g(b)) = (1,1)\} = \\ &= \{(a,b)\in A\times B \mid f(a)=1 \land g(b)=1\} = \\ &= \{(1,1)\}\end{aligned}$$

Por tanto, h es inyectiva. Veamos ahora que es sobreyectiva. Dado $(k,h)\in K\times H$, tomamos $(a,b)\in A\times B$ tales que $f(a)=k$ y $g(b)=h$ (que existe por ser f,g biyectivas). Entonces:

$$h(a,b) = (f(a),g(b)) = (k,h) \qquad \forall (a,b)\in A\times B$$

Por tanto, h es sobreyectiva. Concluimos que h es un isomorfismo.

Ejercicio 2.4.21. Sean H,K,L y M grupos tales que $H\times K\cong L\times M$. ¿Se verifica necesariamente que $H\cong L$ y $K\cong M$?

Sabemos que $C_2\oplus C_3$ es cíclico de orden 6, luego $C_2\oplus C_3\cong C_6$. Además, sabemos que para todo grupo G, se tiene que $G\cong G\times\{1\}$ usando como isomorfismo la aplicación:

$$\begin{array}{rccc} f: & G & \longrightarrow & G\times\{1\} \\ & x & \longmapsto & (x,1) \end{array}$$

Por tanto, $C_2 \oplus C_3 \cong C_6 \cong C_6 \times \{1\}$.

No obstante, $|C_2| \neq |C_6|$ y $|C_3| \neq |1|$. Por tanto, tomando $H = C_2$, $K = C_3$, $L = C_6$ y $M = \{1\}$, se tiene que $H \times K \cong L \times M$. Sin embargo, no se verifica que $H \cong L$ y $K \cong M$.

Ejercicio 2.4.22. Demostrar que no todo subgrupo de un producto directo $H \times K$ es de la forma $H_1 \times K_1$, con $H_1 \leqslant H$ y $K_1 \leqslant K$.

Trabajamos con el grupo directo $\mathbb{Z}_2 \times \mathbb{Z}_2$. El grupo $\mathbb{Z}_2$ no tiene subgrupos propios, y por tanto los subgrupos suyos son $\{0\}$ y $\mathbb{Z}_2$. Por tanto, los subgrupos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ que se descomponen como producto directo de subgrupos de $\mathbb{Z}_2$ son:

- $\{0\} \times \{0\} = \{(0, 0)\}$
- $\{0\} \times \mathbb{Z}_2 = \{(0, 0), (0, 1)\}$
- $\mathbb{Z}_2 \times \{0\} = \{(0, 0), (1, 0)\}$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$

No obstante, consideramos el subgrupo de $\mathbb{Z}_2 \times \mathbb{Z}_2$ dado por:

$$\langle (1, 1)\rangle = \{(0, 0), (1, 1)\} \qquad O((1, 1)) = \mathrm{mcm}(2, 2) = 2$$

Este subgrupo no es de la forma $H_1 \times K_1$, con $H_1 \leqslant H$ y $K_1 \leqslant K$. Por tanto, no todo subgrupo de un producto directo $H \times K$ es de la forma $H_1 \times K_1$, con $H_1 \leqslant H$ y $K_1 \leqslant K$.

Ejercicio 2.4.23. Sean H, K dos grupos y sean $H_1 \lhd H$, $K_1 \lhd K$. Demostrar que $H_1 \times K_1 \lhd H \times K$ y que

$$\frac{H \times K}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}.$$

Como $H_1 < H$ y $K_1 < K$, se tiene que $H_1 \times K_1 < H \times K$. Veamos ahora que $H_1 \times K_1 \lhd H \times K$. Para cada $(h, k) \in H \times K$ y $(h_1, k_1) \in H_1 \times K_1$, tenemos que:

$$(h, k)(h_1, k_1)(h, k)^{-1} = (hh_1h^{-1}, kk_1k^{-1}) \in H_1 \times K_1$$

por ser $H_1 \lhd H$ y $K_1 \lhd K$. Por tanto, $H_1 \times K_1 \lhd H \times K$. Para ver el isomorfismo, consideramos la siguiente aplicación:

$$\begin{array}{rccc} f: & H \times K & \longrightarrow & \dfrac{H}{H_1} \times \dfrac{K}{K_1} \\ & (h, k) & \longmapsto & (hH_1, kK_1) \end{array}$$

Vemos que f es un homomorfismo:

$$\begin{aligned} f((h_1, k_1)(h_2, k_2)) &= f(h_1h_2, k_1k_2) = (h_1h_2H_1, k_1k_2K_1) \\ &= (h_1H_1 \cdot h_2H_1, k_1K_1 \cdot k_2K_1) = (h_1H_1, k_1K_1)(h_2H_1, k_2K_1) \\ &= f(h_1, k_1)f(h_2, k_2) \qquad \forall (h_1, k_1), (h_2, k_2) \in H \times K \end{aligned}$$

Calculamos ahora su núcleo e imagen:

$$\begin{aligned}
\ker(f) &= \{(h,k) \in H \times K \mid f(h,k) = (H_1, K_1)\} \\
&= \{(h,k) \in H \times K \mid (hH_1, kK_1) = (H_1, K_1)\} = \\
&= \{(h,k) \in H \times K \mid hH_1 = H_1 \wedge kK_1 = K_1\} = H_1 \times K_1 \\
Im(f) &= \left\{(hH_1, kK_1) \in \frac{H}{H_1} \times \frac{K}{K_1} \mid (h,k) \in H \times K\right\} = \\
&= \left\{(hH_1, kK_1) \in \frac{H}{H_1} \times \frac{K}{K_1} \mid h \in H \wedge k \in K\right\} = \frac{H}{H_1} \times \frac{K}{K_1}
\end{aligned}$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{H \times K}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}$$

Ejercicio 2.4.24. Sean $H, K \lhd G$ tales que $H \cap K = \{1\}$. Demostrar que G es isomorfo a un subgrupo de $G/H \times G/K$.

Definimos la aplicación:

$$\begin{array}{rccc}
f: & G & \longrightarrow & G/H \times G/K \\
& g & \longmapsto & (gH, gK)
\end{array}$$

Vemos que f es un homomorfismo:

$$f(gh) = (ghH, ghK) = (gH, gK)(hH, hK) = f(g)f(h) \qquad \forall g, h \in G$$

Calculamos su núcleo:

$$\begin{aligned}
\ker(f) &= \{g \in G \mid f(g) = (H, K)\} \\
&= \{g \in G \mid (gH, gK) = (H, K)\} = \\
&= \{g \in G \mid gH = H \wedge gK = K\} = H \cap K = \{1\}
\end{aligned}$$

Por tanto, tenemos que:

$$\frac{G}{\ker(f)} = \frac{G}{\{1\}} \cong G$$

Por tanto, por el Primer Teorema de Isomorfía, se tiene que:

$$G \cong \frac{G}{\ker(f)} \cong Im(f)$$

Como $G < G$ y f es un homomorfismo, se tiene que $Im(f) < G/H \times G/K$. Por tanto, G es isomorfo a $Im(f)$, que es un subgrupo de $G/H \times G/K$.

Ejercicio 2.4.25. Sean $H, K \lhd G$ tales que $HK = G$. Demostrar que

$$\frac{G}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{H} \times \frac{G}{K}.$$

La demostración no es directa, y la dividiremos en dos partes. Por un lado, demostraremos la primera relación de isomofía, y posteriormente veremos la segunda.

Por el Segundo Teorema de Isomorfía aplicado dos veces, se tiene de forma directa que $H \cap K \lhd H, K$. Veamos ahora que $H \cap K \lhd G$. Para ello, tomamos $g \in G$ y $x \in H \cap K$. Como $G = HK$, tenemos que $g = hk$ con $h \in H$ y $k \in K$. Entonces:

$$\begin{aligned} gxg^{-1} &= (hk)x(hk)^{-1} = (hk)x(k^{-1}h^{-1}) = \\ &= h(kxk^{-1})h^{-1} \overset{(*)}{=} h\widetilde{k}h^{-1} \overset{(**)}{\in} H \cap K \end{aligned}$$

donde $(*)$ se cumple porque $H \cap K \lhd K$, por lo que $kxk^{-1} = \widetilde{k} \in K$ y $(**)$ se cumple porque $H \cap K \lhd H$, por lo que $h\widetilde{k}h^{-1} \in H$. Por tanto, $H \cap K \lhd G$, y el primer cociente tiene sentido.

Definimos la aplicación:

$$\begin{array}{rccc} f: & G & \longrightarrow & \dfrac{H}{H \cap K} \times \dfrac{K}{H \cap K} \\ & g & \longmapsto & (h(H \cap K), k(H \cap K)) \end{array}$$

Veamos que está bien definida, puesto que la descomposición no tiene por qué ser única. Sean $k_1, k_2 \in K$ y $h_1, h_2 \in H$ tales que $g = k_1h_1 = k_2h_2$. Entonces, en primer lugar vemos que $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$. Por tanto:

- $h_1 = k_1^{-1}k_2h_2$, con $k_1^{-1}k_2 \in K \cap K$ y $h_2 \in H$, por lo que $h_1(H \cap K) = h_2(H \cap K)$.
- $k_1 = k_2h_1^{-1}h_2$, con $h_1^{-1}h_2 \in H \cap H$ y $k_2 \in K$, por lo que $k_1(H \cap K) = k_2(H \cap K)$.

Por tanto, f está bien definida. Veamos que es un homomorfismo. Dados $g_1, g_2 \in G$, $\exists h_1, h_2 \in H$ y $k_1, k_2 \in K$ tales que $g_1 = h_1k_1$ y $g_2 = h_2k_2$. Entonces:

$$\begin{aligned} f(g_1g_2) &= f(h_1k_1h_2k_2) = \\ &= (h_1h_2(H \cap K), k_1k_2(H \cap K)) = \\ &= (h_1(H \cap K), k_1(H \cap K))(h_2(H \cap K), k_2(H \cap K)) \\ &= f(g_1)f(g_2) \qquad \forall g_1, g_2 \in G \end{aligned}$$

Calculamos su núcleo:

$$\begin{aligned} \ker(f) &= \{g \in G \mid f(g) = (H \cap K, H \cap K)\} \\ &= \{g = hk \in G \mid (h(H \cap K), k(H \cap K)) = (H \cap K, H \cap K)\} = \\ &= \{g = hk \in G \mid h(H \cap K) = H \cap K \land k(H \cap K) = H \cap K\} = \\ &= \{g = hk \in G \mid h, k \in H \cap K\} \overset{(*)}{=} H \cap K \end{aligned}$$

donde $(*)$ se cumple porque la inclusión $\ker f \subseteq H \cap K$ se cumple por ser $H \cap K$ cerrado para el producto; mientras que la inclusión $H \cap K \subseteq \ker f$ se cumple tomando $g = g \cdot 1$.

Veamos ahora que es sobreyectiva. Dado $(h(H \cap K), k(H \cap K)) \in \frac{H}{H \cap K} \times \frac{K}{H \cap K}$, tomamos $g = hk \in G$. Entonces:

$$f(g) = f(hk) = (h(H \cap K), k(H \cap K)) \qquad \forall g \in G$$

Por tanto, f es sobreyectiva. Por el Primer Teorema de Isomorfía, se tiene que:

$$\frac{G}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K}$$

Llegamos a este punto, tan solo nos falta probar que:

$$\frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{H} \times \frac{G}{K}$$

Para ello, aplicamos en primer lugar dos veces el Segundo Teorema de Isomorfía.

- $H, K < G$ y $K \lhd G$:
$$\frac{G}{K} \cong \frac{H}{H \cap K}$$
- $H, K < G$ y $H \lhd G$:
$$\frac{G}{H} \cong \frac{K}{H \cap K}$$

Por tanto, tenemos que:

$$\frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{K} \times \frac{G}{H}$$

Como $G/H \times G/K \cong G/K \times G/H$, tenemos que:

$$\frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{K} \times \frac{G}{H} \cong \frac{G}{H} \times \frac{G}{K}$$

Por tanto, se cumple la segunda relación de isomorfía. Concluimos que:

$$\frac{G}{H \cap K} \cong \frac{H}{H \cap K} \times \frac{K}{H \cap K} \cong \frac{G}{H} \times \frac{G}{K}$$

Ejercicio 2.4.26. Demostrar que si G es un grupo que es producto directo interno de subgrupos H y K, y $N \lhd G$ tal que $N \cap H = \{1\} = N \cap K$, entonces N es abeliano.

En primer lugar, veamos que N conmuta con H; es decir, que dado $n \in N$ y $h \in H$, se tiene que $nh = hn$. Equivalentemente, veremos que $nhn^{-1}h^{-1} = 1$.

- Como N es un grupo, $n^{-1} \in N$. Como $H < G$, $h \in G$. Como $N \lhd G$, tenemos que $hn^{-1}h^{-1} \in N$. Como N es cerrado para el producto, tenemos que:
$$n\ hn^{-1}h^{-1} \in N$$
- Como $N < G$, $n \in G$. Como $H \lhd G$ por la caracterización del producto directo interno, tenemos que $nhn^{-1} \in H$. Como H es cerrado para el producto, tenemos que:
$$nhn^{-1}h^{-1} \in H$$

Por tanto, $nhn^{-1}h^{-1} \in N \cap H$. Como $N \cap H = \{1\}$, tenemos que $nhn^{-1}h^{-1} = 1$. Por tanto, $nh = hn$ para todo $n \in N$ y $h \in H$. De forma análoga, como $K \lhd G$, tenemos que $nk = kn$ para todo $n \in N$ y $k \in K$. Sea ahora $g \in G$ y $n \in N$. Entonces, como $G = HK$, tenemos que $g = hk$ con $h \in H$ y $k \in K$. Entonces:

$$gn = (hk)n = h(kn) = h(nk) = (hn)k = (nh)k = n(hk) = ng$$

Por tanto, $gn = ng$ para todo $g \in G$ y $n \in N$. Como $N < G$, tenemos que N es abeliano.

Ejercicio 2.4.27. Dar un ejemplo de un grupo G que sea producto directo interno de dos subgrupos propios H y K, y que contenga a un subgrupo normal no trivial N tal que $N \cap H = \{1\} = N \cap K$. Concluir que para $N \lhd H \times K$ es posible que se tenga

$$N \neq (N \cap (H \times \{1\})) \times (N \cap (\{1\} \times K)).$$

Sea $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $H = \langle (1,0) \rangle$ y $K = \langle (0,1) \rangle$. Sabemos que $G \cong V$ abeliano, luego $H, K \lhd G$. Además, $H \cap K = \{(0,0)\}$. Por último, se tiene que $G = HK$. Por tanto, G es producto directo interno de H y K. Sea ahora:

$$N = \langle (1,1) \rangle = \{(0,0), (1,1)\}$$

Sabemos que $N < G$, luego $N \lhd G$. Además, $N \cap H = \{(0,0)\} = N \cap K$. Por tanto, se cumple la condición del ejercicio.

Sea ahora $\varphi : G \to H \times K$ el isomorfismo correspondiente. Sea ahora el subgrupo $\varphi(N) < H \times K$. Como el ser normal se mantiene por homomorfismo, $\varphi(N) \lhd H \times K$. Veamos ahora que:

$$\begin{aligned}
\varphi((0,0)) &= ((0,0),(0,0)) \\
\varphi((1,1)) &= ((1,0),(0,1)) \\
\varphi(N) &= \{((0,0),(0,0)),((1,0),(0,1))\}
\end{aligned}$$

Por tanto, $\varphi(N)$ no puede ser producto cartesiano, puesto que $((0,0),(0,1))$ debería pertenecer también. Por tanto:

$$\varphi(N) \neq (\varphi(N) \cap (H \times \{1\})) \times (\varphi(N) \cap (\{1\} \times K)).$$

Y se tiene demostrado lo pedido.

Ejercicio 2.4.28. Sea G un grupo finito que sea producto directo interno de dos subgrupos H y K tales que $\text{mcd}(|H|, |K|) = 1$. Demostrar que para todo subgrupo $N \leqslant G$ se verifica que $N \cong (N \cap H) \times (N \cap K)$.

Sean $H, K < G$ tales que $G \cong H \times K$ y $\text{mcd}(|H|, |K|) = 1$. Consideramos además el subgrupo $N < G$. Antes de definir explícitamente el isomorfismo, sea $n \in N$. Como $G = H \times K$, tenemos que $\exists! h \in H$ y $k \in K$ tales que $n = hk$. Veamos que, además, $h \in N$ y $k \in N$. Sea $a = \text{ord}(h)$ y $b = \text{ord}(k)$.

- Veamos que $h \in N$. Calculamos n^b:

$$n^b = (hk)^b \stackrel{(*)}{=} h^b k^b = h^b \in N$$

donde en $(*)$ hemos empleado que G es producto interno de H y K.

Por otro lado, como $a \mid |H|$ y $b \mid |K|$, como $\text{mcd}(|H|, |K|) = 1$, tenemos que $\text{mcd}(a, b) = 1$. Consideramos sus coeficientes de Bézout $u, v \in \mathbb{Z}$ tales que:

$$au + bv = 1$$

Entonces, tenemos que:

$$h = h^1 = h^{au+bv} = h^{au}h^{bv} = (h^a)^u(h^b)^v = 1^u(h^b)^v = (h^b)^v \in N$$

Por tanto, $h \in N$.

- Veamos que $k \in N$. Calculamos n^a:

$$n^a = (hk)^a \stackrel{(*)}{=} h^a k^a = k^a \in N$$

donde en $(*)$ hemos empleado que G es producto interno de H y K. Por otro lado, como $a \mid |H|$ y $b \mid |K|$, como $\text{mcd}(|H|, |K|) = 1$, tenemos que $\text{mcd}(a, b) = 1$. Consideramos sus coeficientes de Bézout $u, v \in \mathbb{Z}$ tales que:

$$au + bv = 1$$

Entonces, tenemos que:

$$k = k^1 = k^{au+bv} = k^{au}k^{bv} = (k^a)^u(k^b)^v = (k^a)^u 1^v = (k^a)^u \in N$$

Por tanto, $k \in N$.

Por tanto, para todo $n \in N$, tenemos que $\exists! h \in N \cap H$ y $k \in N \cap K$ tales que $n = hk$. Definimos la aplicación:

$$\begin{array}{rccl} f: & N & \longrightarrow & (N \cap H) \times (N \cap K) \\ & n = hk & \longmapsto & (h, k) \end{array}$$

Por lo anteriormente visto, f está bien definida. Veamos que es un homomorfismo. Fijados $n_1 = h_1k_1$ y $n_2 = h_2k_2$, tenemos que:

$$\begin{aligned} f(n_1n_2) &= f(h_1k_1h_2k_2) = f((h_1h_2)(k_1k_2)) = (h_1h_2, k_1k_2) \\ &= (h_1, k_1)(h_2, k_2) = f(n_1)f(n_2) \qquad \forall n_1, n_2 \in N \end{aligned}$$

Calculamos su núcleo:

$$\begin{aligned} \ker(f) &= \{n \in N \mid f(n) = (1, 1)\} \\ &= \{n = hk \in N \mid (h, k) = (1, 1)\} = \\ &= \{n = hk \in N \mid h = 1 \land k = 1\} = \{1\} \end{aligned}$$

Por tanto, f es inyectiva. Veamos ahora que es sobreyectiva. Dado $(h, k) \in (N \cap H) \times (N \cap K)$, consideramos $n = hk \in N$. Entonces:

$$f(n) = f(hk) = (h, k) \qquad \forall (h, k) \in (N \cap H) \times (N \cap K)$$

Por tanto, f es sobreyectiva. Concluimos que f es un isomorfismo, y por tanto:

$$N \cong (N \cap H) \times (N \cap K).$$

Ejercicio 2.4.29. Sea G un grupo y sea $f : G \to G$ un endomorfismo idempotente (esto es, verificando que $f^2 = f$) y tal que $Im(f) \lhd G$. Demostrar que

$$G \cong Im(f) \times \ker(f).$$

Opción 1. Método Directo

Sea la siguiente aplicación:

$$\begin{array}{rrcl} \varphi : & Im(f) \times \ker(f) & \longrightarrow & G \\ & (x, y) & \longmapsto & xy \end{array}$$

Veamos que φ es un isomorfismo. Para ello, previamente veremos que para todo $x \in Im(f)$, se tiene que $f(x) = x$. Dado $x \in Im(f)$, existe $y \in G$ tal que $f(y) = x$. Entonces:

$$f(x) = f(f(y)) = f^2(y) \stackrel{(*)}{=} f(y) = x$$

donde en $(*)$ se cumple porque f es idempotente.

Homomorfismo

Veamos que φ es homomorfismo. Para cada $(x_1, y_1), (x_2, y_2) \in Im(f) \times \ker(f)$, tenemos que:

$$\varphi((x_1, y_1)(x_2, y_2)) = \varphi(x_1x_2, y_1y_2) = x_1x_2y_1y_2$$
$$\varphi(x_1, y_1)\varphi(x_2, y_2) = (x_1y_1)(x_2y_2) = x_1y_1x_2y_2$$

Veamos que $x_2y_1 = y_1x_2$. Es decir, que dados $x \in Im(f)$ y $y \in \ker(f)$, tenemos que $xy = yx$. Como $Im(f) \lhd G$, y $\ker f \subset G$, tenemos que $yxy^{-1} \in Im(f)$. Por lo visto anteriormente, $f(yxy^{-1}) = yxy^{-1}$. Aplicando que f es un homomorfismo (estamos demostrando que φ lo es, pero sabemos que f lo es), tenemos que:

$$yxy^{-1} = f(yxy^{-1}) = f(y)f(x)f(y^{-1}) = f(y)xf(y)^{-1} \stackrel{(*)}{=} 1x1 = x \Longrightarrow yx = xy$$

donde en $(*)$ se cumple porque $y \in \ker(f)$ y $x \in Im(f)$.

Por tanto, φ es un homomorfismo.

Inyectividad

Veamos que φ es inyectiva. Para ello, sean $(x_1, y_1), (x_2, y_2) \in Im(f) \times \ker(f)$ tales que $\varphi(x_1, y_1) = \varphi(x_2, y_2)$. Entonces:

$$x_1y_1 = x_2y_2 \Longrightarrow x_2^{-1}x_1 = y_2y_1^{-1} \in \ker(f) \cap Im(f)$$

Veamos ahora que $\ker(f) \cap Im(f) = \{1\}$. Sea $x \in \ker(f) \cap Im(f)$. Como $x \in \ker(f)$, tenemos que $f(x) = 1$, y como $x \in Im(f)$, $f(x) = x$. Entonces $1 = f(x) = x$, por lo que $x = 1$. Por tanto, $\ker(f) \cap Im(f) = \{1\}$, por lo que:

$$x_2^{-1}x_1 = 1 \Longrightarrow x_1 = x_2$$
$$y_2y_1^{-1} = 1 \Longrightarrow y_1 = y_2$$

Por tanto, φ es inyectiva.

Sobreyectividad

Veamos que es sobreyectiva. Dado $g \in G$, tomamos $x = f(g) \in Im(f)$ e $y = f(g^{-1})g$. Veamos en primer lugar que $y \in \ker(f)$:

$$f(y) = f(f(g^{-1})g) = f(f(g^{-1}))f(g) = f^2(g^{-1})f(g) = f(g^{-1})f(g) = f(g^{-1}g) = f(1) = 1$$

Por tanto, $y \in \ker(f)$. Veamos ahora que $\varphi(x, y) = g$. Entonces:

$$\varphi(x, y) = \varphi(f(g), f(g^{-1})g) = f(g)f(g^{-1})g = f(gg^{-1})g = f(1)g = 1g = g$$

Por tanto, φ es sobreyectiva.

Concluimos que φ es un isomorfismo. Por tanto, $G \cong Im(f) \times \ker(f)$.

Opción 2.

En primer lugar, sabemos que $\ker f \lhd G$, y por hipótesis $Im(f) \lhd G$. Veamos ahora que $\ker(f) \cap Im(f) = \{1\}$. Previamente veremos que para todo $x \in Im(f)$, se tiene que $f(x) = x$. Dado $x \in Im(f)$, existe $y \in G$ tal que $f(y) = x$. Entonces:

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

donde en $(*)$ se cumple porque f es idempotente. Sea ahora $x \in \ker(f) \cap Im(f)$. Como $x \in \ker(f)$, tenemos que $f(x) = 1$, y como $x \in Im(f)$, $f(x) = x$. Entonces $1 = f(x) = x$, por lo que $x = 1$. Por tanto, $\ker(f) \cap Im(f) = \{1\}$. Veamos ahora que $G = \ker(f)Im(f)$:

$\supseteq$) Como $\ker(f), Im(f) < G$, y G es un grupo, tenemos que $\ker(f)Im(f) \subset G$.

$\subseteq$) Sea $g \in G$. Consideramos ahora $x = f(g) \in Im(f)$ e $y = f(g^{-1})g$. Veamos en primer lugar que $y \in \ker(f)$:

$$f(y) = f(f(g^{-1})g) = f(f(g^{-1}))f(g) = f^2(g^{-1})f(g) = f(g^{-1})f(g) = f(g^{-1}g) = f(1) = 1$$

Por tanto, $y \in \ker(f)$. Veamos ahora que $g = xy$. Entonces:

$$xy = f(g)f(g^{-1})g = f(gg^{-1})g = f(1)g = 1g = g$$

Por tanto, $g = xy \in \ker(f)Im(f)$.

Por tanto, $G = \ker(f)Im(f)$. Por la condición suficiente de producto directo interno, tenemos que $G \cong \ker(f) \times Im(f)$.

Ejercicio 2.4.30. Sea S un subconjunto de un grupo G. Se llama *centralizador* de S en G al conjunto

$$C_G(S) = \{x \in G \mid xs = sx \ \forall s \in S\}$$

y se llama *normalizador* de S en G al conjunto

$$N_G(S) = \{x \in G \mid xS = Sx\}.$$

1. Demostrar que $N_G(S) \leqslant G$.

   Comprobamos las tres condiciones:

   - $1 \in N_G(S)$, ya que $1S = S1 = S$.
   - Sea $x, y \in N_G(S)$. Entonces $xS = Sx$ y $yS = Sy$. Entonces:
   $$(xy)S = x(yS) = x(Sy) = (xS)y = (Sx)y = S(xy)$$
   Por tanto, es cerrado para el producto.
   - Sea $x \in N_G(S)$, $xS = Sx$. Entonces:
   $$xS = Sx \Longrightarrow S = x^{-1}Sx \Longrightarrow Sx^{-1} = x^{-1}S \Longrightarrow x^{-1} \in N_G(S)$$
   Por tanto, es cerrado para inversos.

2. Demostrar que $C_G(S) \lhd N_G(S)$.

   Veamos en primer lugar que $C_G(S) \leqslant N_G(S)$. Para ello, vemos en primer lugar que $C_G(S) \subseteq N_G(S)$. Fijado $x \in C_G(S)$, tenemos que $xs = sx$ para todo $s \in S$, por lo que:
   $$xS = \{xs \mid s \in S\} = \{sx \mid s \in S\} = Sx$$
   Por tanto, $xS = Sx$, y tenemos que $C_G(S) \subseteq N_G(S)$. Como además se tiene que $C_G(S), N_G(S) < G$, tenemos que $C_G(S) < N_G(S)$.

   Comprobamos ahora que $C_G(S) \lhd N_G(S)$. Para ello, tomamos $x \in N_G(S)$ y $y \in C_G(S)$, y veamos que $xyx^{-1} \in C_G(S)$. Para ello, tomamos $s \in S$, y como $x \in N_G(S)$, tenemos que $xS = Sx$, por lo que $sx = xs'$ con $s' \in S$ y por tanto $x^{-1}sx \in S$. Entonces:
   $$yx^{-1}sx = x^{-1}sxy \Longrightarrow xyx^{-1}s = sxyx^{-1} \Longrightarrow xyx^{-1} \in C_G(S)$$

3. Demostrar que si $S \leqslant G$ entonces $S \lhd N_G(S)$.

   Sea $s \in S$. Veamos que $s \in N_G(S)$, es decir que $sS = Ss$.

   $\subset$) Sea $x \in sS$. Entonces, $\exists s' \in S$ tal que $x = ss'$. Entonces, como $ss'(s^{-1}) \in S$, tenemos que:
   $$x = ss' = ss'(s^{-1})s \in Ss$$

   $\supset$) Sea $x \in Ss$. Entonces, $\exists s' \in S$ tal que $x = s's$. Entonces, como $(s^{-1})s's \in S$, tenemos que:
   $$x = s's = ss^{-1}s's \in sS$$

   Por tanto, $S \subset N_G(S)$. Como además $S, N_G(S) < G$, tenemos que $S < N_G(S)$. Veamos ahora que $S \lhd N_G(S)$. Para ello, tomamos $x \in N_G(S)$ y $s \in S$, y veamos que $xsx^{-1} \in S$. Entonces:
   $$xsx^{-1} \overset{(*)}{=} s'xx^{-1} = s' \in S$$
   donde en $(*)$ hemos empleado que $x \in N_G(S)$, por lo que $xS = Sx$.

Ejercicio 2.4.31. Sea G un grupo y H y K subgrupos suyos con $H \subseteq K$. Entonces demostrar que H es normal en K si y sólo si $K < N_G(H)$. (Así, el normalizador $N_G(H)$ queda caracterizado como el mayor subgrupo de G en el que H es normal.)

$\Longrightarrow$) Sea $H \lhd K$, y veamos que $K \subset N_G(H)$. Como $H \lhd K$, tenemos que $kH = Hk$ para todo $k \in K$, luego $K \subset N_G(H)$. Como además $K, N_G(H) < G$, tenemos que $K < N_G(H)$.

$\Longleftarrow$) Sea $K < N_G(H)$, luego $K \subset N_G(H)$. Entonces, para todo $k \in K$, tenemos que $kH = Hk$. Por tanto, $H \lhd K$.

Ejercicio 2.4.32. Sea G un grupo.

1. Demostrar que $C_G(Z(G)) = G$ y que $N_G(Z(G)) = G$.

   Veamos en primer lugar que $C_G(Z(G)) = G$.

   $\subset$) Sea $x \in C_G(Z(G))$, luego trivialmente $x \in G$.

   $\supset$) Sea $x \in G$, luego $xz = zx$ para todo $z \in Z(G)$. Por tanto, $x \in C_G(Z(G))$.

   Veamos ahora que $N_G(Z(G)) = G$.

   $\subset$) Sea $x \in N_G(Z(G))$, luego trivialmente $x \in G$.

   $\supset$) Sea $x \in G$, luego $xz = zx$ para todo $z \in Z(G)$. Por tanto, $xZ(G) = Z(G)x$, luego $x \in N_G(Z(G))$.

   Análogamente, también podríamos haber usando que $G = C_G(Z(G))$ y sabiendo que $C_G(Z(G)) \lhd N_G(Z(G))$.

2. Si G es un grupo y $H < G$ ¿Cuándo es $G = N_G(H)$? ¿Y cuándo es $G = C_G(H)$?

   Por el ejercicio anterior, que nos caracteriza el normalizador, sabemos que:

   $$G = N_G(H) \Longleftrightarrow H \lhd G$$

   Por otro lado, sabemos que $C_G(H) = G$ si y sólo si $H \subset Z(G)$.

3. Si $H \leqslant G$ con $|H| = 2$, demostrar que $N_G(H) = C_G(H)$. Deducir que $H \lhd G$ si y sólo si $H \subset Z(G)$.

   Si $|H| = 2$, entonces $H = \{1, h\}$ con $h \in G \setminus \{1\}$, luego $h = h^{-1}$. Veamos que $N_G(H) = C_G(H)$.

   $\subset$) Sea $x \in N_G(H)$, luego $xH = Hx$. Como $xh \in Hx$, entonces hay dos opciones:

   - $xh = 1$, luego $x = h^{-1}$. Por tanto, $xh = h^{-1}h = 1 = hh^{-1} = hx$.
   - $xh = h$, luego $x = 1$. Por tanto, $xh = 1h = h = h1 = hx$.

   En cual caso, $xh = hx$, luego $x \in C_G(H)$.

   $\supset$) Como $C_G(H) \lhd N_G(H)$, se tiene.

   Demostramos ahora que $H \lhd G$ si y sólo si $H \subset Z(G)$.

$\Longrightarrow$) Como $H \lhd G$, por el apartado anterior tenemos que $G = N_G(H)$. Como acacaba de ver que $N_G(H) = C_G(H)$, tenemos que $G = C_G(H)$. Por tanto, para todo $x \in G$, tenemos que $xh = hx$ para todo $h \in H$. Por tanto, $H \subset Z(G)$.

$\Longleftarrow$) Como $H \subset Z(G)$, tenemos que $C_G(H) = G$. Por tanto, se tiene que $N_G(H) = C_G(H) = G$, luego $H \lhd G$.

Ejercicio 2.4.33. Sea G un grupo arbitrario. Para dos elementos $x, y \in G$ se define su *conmutador* como el elemento

$$[x, y] = xyx^{-1}y^{-1}.$$

Observación. (El conmutador recibe tal nombre porque $[x, y]yx = xy$.)

Como $[x, y]^{-1} = [y, x]$, el inverso de un conmutador es un conmutador. Sin embargo el producto de dos conmutadores no tiene porqué ser un conmutador. Entonces se define el *subgrupo conmutador* o (primer) *subgrupo derivado* de G, denotado $[G, G]$, como el subgrupo generado por todos los conmutadores de G.

1. Demostrar que, $\forall a, x, y \in G$, se tiene que $a[x, y]a^{-1} = [axa^{-1}, aya^{-1}]$.

$$[axa^{-1}, aya^{-1}] = axa^{-1}aya^{-1}ax^{-1}a^{-1}ay^{-1}a^{-1} = axyx^{-1}y^{-1}a^{-1} = a[x, y]a^{-1}$$

2. Demostrar que $[G, G] \lhd G$.

Tenemos que:

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle$$

Como $[x, y] \in G$ para todo $x, y \in G$ y $[G, G]$ es un grupo, tenemos que $[G, G] < G$. Veamos que $[G, G] \lhd G$. Para ello, tomamos $g \in G$ y $z \in [G, G]$. Entonces, como $z \in [G, G]$, tenemos que:

$$z = [x_1, y_1] \cdots [x_n, y_n] \qquad x_i, y_i \in G \ \forall i = 1, \dots, n$$

Entonces:

$$\begin{aligned} gzg^{-1} &= g[x_1, y_1] \cdots [x_n, y_n]g^{-1} = \\ &= g[x_1, y_1]g^{-1}g[x_2, y_2]g^{-1} \cdots g[x_n, y_n]g^{-1} = \\ &= [gx_1g^{-1}, gy_1g^{-1}] \cdots [gx_ng^{-1}, gy_ng^{-1}] \in [G, G] \end{aligned}$$

3. Demostrar que el grupo cociente $G/[G, G]$, que se representa por G^{ab}, es un grupo abeliano (que se llama el abelianizado de G).

Dados $x, y \in G$, hemos de ver que $x[G, G]y[G, G] = y[G, G]x[G, G]$. Usando el producto en el cociente, hemos de ver que:

$$xy[G, G] = yx[G, G]$$

Consideramos ahora $[y^{-1}, x^{-1}] \in [G, G]$. Entonces:

$$xy[y^{-1}, x^{-1}] = xyy^{-1}x^{-1}yx = yx$$

Por tanto, $xy[G, G] = yx[G, G]$, luego $G/[G, G]$ es abeliano.

4. Demostrar que G es abeliano si y sólo si $[G, G] = 1$.

$\Longrightarrow$) Si G es abeliano, entonces:

$$\begin{aligned}[G, G] &= \langle [x, y] \mid x, y \in G \rangle = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle = \\ &= \langle xx^{-1}yy^{-1} \mid x, y \in G \rangle = \langle 1 \mid x, y \in G \rangle = \{1\}\end{aligned}$$

$\Longleftarrow$) Si $[G, G] = 1$, entonces dados $x, y \in G$, tenemos que $[x, y] = 1$, luego:

$$1 = [x, y] = xyx^{-1}y^{-1} = xy(yx)^{-1} \Longrightarrow xy = yx$$

Por tanto, G es abeliano.

5. Sea $N \lhd G$. Demostrar que el grupo cociente G/N es abeliano si y sólo si $[G, G] < N$ (así que el grupo $[G, G]$ es el menor subgrupo normal de G tal que el cociente es abeliano).

$\Longrightarrow$) Sea G/N abeliano, y consideramos la proyección en el cociente:

$$\begin{array}{rccc} p: & G & \longrightarrow & G/N \\ & g & \longmapsto & gN \end{array}$$

Sabemos que p es un homomorfismo. Dados $x, y \in G$, tenemos que:

$$p([x, y]) = p(xyx^{-1}y^{-1}) = p(x)p(y)p(x)^{-1}p(y)^{-1} = 1$$

Por tanto, por ser p un homomorfismo, tenemos que $p([G, G]) = \{1\}$, luego $[G, G] \subseteq \ker p = N$. Por tanto, como además $[G, G]$ es un grupo, se tiene que $[G, G] < N$.

$\Longleftarrow$) Sea $[G, G] < N$. Sean ahora $x, y \in G$, y buscamos ver que $xyN = yxN$. Tenemos que:

$$xy[y^{-1}, x^{-1}] = xyy^{-1}x^{-1}yx = yx$$

Como $[y^{-1}, x^{-1}] \in [G, G] < N$, tenemos que $xyN = yxN$. Por tanto:

$$(xN)(yN) = xyN = yxN = (yN)(xN)$$

Por tanto, G/N es abeliano.

Ejercicio 2.4.34.

1. Calcular el subgrupo conmutador de los grupos S_3, A_4, D_4 y Q_2.

   a) S_3:
   Recordemos que el subgrupo conmutador de G es el menor subgrupo normal de G tal que el cociente es abeliano. El diagrama de Hasse de S_3 conviene tenerlo presente, y se encuentra en la Figura 2.48. Comprobemos cada subgrupo de S_3, de menor a mayor orden:

   - $\{1\}$ efectivamente cumple que $\{1\} \lhd S_3$, pero:

     $$S_3/\{1\} \cong S_3$$

     Por tanto, el cociente no es abeliano, luego $\{1\} \neq [S_3, S_3]$.

- $\langle(1\ 2)\rangle$.

$$(2\ 3)(1\ 2)(2\ 3)^{-1} = (2\ 3)(1\ 2)(2\ 3) = (1\ 3) \notin \langle(1,2)\rangle$$

Por tanto, $\langle(1\ 2)\rangle \ntriangleleft S_3$, luego $\langle(1\ 2)\rangle \neq [S_3, S_3]$.

- $\langle(13)\rangle$.

$$(2\ 3)(1\ 3)(2\ 3)^{-1} = (2\ 3)(1\ 3)(2\ 3) = (1\ 2) \notin \langle(1,3)\rangle$$

Por tanto, $\langle(1\ 3)\rangle \ntriangleleft S_3$, luego $\langle(1\ 3)\rangle \neq [S_3, S_3]$.

- $\langle(2\ 3)\rangle$.

$$(1\ 2)(2\ 3)(1\ 2)^{-1} = (1\ 2)(2\ 3)(1\ 2) = (1\ 3) \notin \langle(2,3)\rangle$$

Por tanto, $\langle(2\ 3)\rangle \ntriangleleft S_3$, luego $\langle(2\ 3)\rangle \neq [S_3, S_3]$.

- $\langle(1\ 2\ 3)\rangle$.
Sabemos que $|\langle(1\ 2\ 3)\rangle| = 3$, por lo que $[S_3 : \langle(1\ 2\ 3)\rangle] = 2$, luego $\langle(1\ 2\ 3)\rangle \lhd S_3$. Por tanto, es un candidato a ser el subgrupo conmutador. Veamos si $S_3/\langle(1\ 2\ 3)\rangle$ es abeliano:

$$\left|\frac{S_3}{\langle(1\ 2\ 3)\rangle}\right| = \frac{|S_3|}{|\langle(1\ 2\ 3)\rangle|} = \frac{6}{3} = 2 \Longrightarrow \frac{S_3}{\langle(1\ 2\ 3)\rangle} \cong C_2$$

Por tanto, $S_3/\langle(1\ 2\ 3)\rangle$ es abeliano, luego:

$$[S_3, S_3] = \langle(1\ 2\ 3)\rangle = A_3$$

b) A_4:
El diagrama de Hasse de A_4 conviene tenerlo presente, y se encuentra en la Figura 2.51. Comprobemos cada subgrupo de A_4, de menor a mayor orden:

- $\{1\}$ efectivamente cumple que $\{1\} \lhd A_4$, pero:

$$A_4/\{1\} \cong A_4$$

Por tanto, el cociente no es abeliano, luego $\{1\} \neq [A_4, A_4]$.

- $\langle(1\ 2)(3\ 4)\rangle$.

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

Por tanto, $(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 2\ 3)^{-1} \notin \langle(1\ 2)(3\ 4)\rangle$, luego $\langle(1\ 2)(3\ 4)\rangle \ntriangleleft A_4$, luego $\langle(1\ 2)(3\ 4)\rangle \neq [A_4, A_4]$.

- $\langle(1\ 3)(2\ 4)\rangle$.

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

Por tanto, $(1\ 2\ 3)(1\ 3)(2\ 4)(1\ 2\ 3)^{-1} \notin \langle(1\ 3)(2\ 4)\rangle$, luego $\langle(1\ 3)(2\ 4)\rangle \ntriangleleft A_4$, luego $\langle(1\ 3)(2\ 4)\rangle \neq [A_4, A_4]$.

- $\langle(1\ 4)(2\ 3)\rangle$.

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

  Por tanto, $(1\,2\,3)(1\,4)(2\,3)(1\,2\,3)^{-1} \notin \langle(1\,4)(2\,3)\rangle$, luego $\langle(1\,4)(2\,3)\rangle \not\triangleleft A_4$, luego $\langle(1\ 4)(2\ 3)\rangle \neq [A_4, A_4]$.
- $\langle(1\ 2\ 3)\rangle$.

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

  Por tanto, $(1\,2)(3\,4)(1\,2\,3)(1\,2)(3\,4) \notin \langle(1\,2\,3)\rangle$, luego $\langle(1\,2\,3)\rangle \not\triangleleft A_4$, luego $\langle(1\ 2\ 3)\rangle \neq [A_4, A_4]$.
- $\langle(2\ 3\ 4)\rangle$.

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

  Por tanto, $(1\,2)(3\,4)(2\,3\,4)(1\,2)(3\,4) \notin \langle(2\,3\,4)\rangle$, luego $\langle(2\,3\,4)\rangle \not\triangleleft A_4$, luego $\langle(2\ 3\ 4)\rangle \neq [A_4, A_4]$.
- $\langle(1\ 3\ 4)\rangle$.

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

  Por tanto, $(1\,2)(3\,4)(1\,3\,4)(1\,2)(3\,4) \notin \langle(1\,3\,4)\rangle$, luego $\langle(1\,3\,4)\rangle \not\triangleleft A_4$, luego $\langle(1\ 3\ 4)\rangle \neq [A_4, A_4]$.
- $\langle(1\ 2\ 4)\rangle$.

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

  Por tanto, $(1\,3)(2\,4)(1\,2\,4)(1\,3)(2\,4) \notin \langle(1\,2\,4)\rangle$, luego $\langle(1\,2\,4)\rangle \not\triangleleft A_4$, luego $\langle(1\ 2\ 4)\rangle \neq [A_4, A_4]$.
- V.
  En Teoría vimos que el subgrupo de Klein V es normal en A_4. Veamos que A_4/V es abeliano:

$$\left|\frac{A_4}{V}\right| = \frac{|A_4|}{|V|} = \frac{12}{4} = 3 \Longrightarrow \frac{A_4}{V} \cong C_3$$

  Por tanto, A_4/V es abeliano, luego:

$$[A_4, A_4] = V$$

c) D_4:
El diagrama de Hasse de D_4 conviene tenerlo presente, y se encuentra en la Figura 2.49. Comprobemos cada subgrupo de D_4, de menor a mayor orden:

- $\{1\}$ efectivamente cumple que $\{1\} \triangleleft D_4$, pero:

$$D_4/\{1\} \cong D_4$$

  Por tanto, el cociente no es abeliano, luego $\{1\} \neq [D_4, D_4]$.

- $\langle r^2 \rangle$.
  En el Ejercicio 2.4.5 vimos que:
  $$Z(D_4) = \langle r^2 \rangle$$
  Como además $Z(D_4) \lhd D_4$, tenemos que $\langle r^2 \rangle \lhd D_4$. Veamos que $D_4/\langle r^2 \rangle$ es abeliano:
  $$\left| \frac{D_4}{\langle r^2 \rangle} \right| = \frac{|D_4|}{|\langle r^2 \rangle|} = \frac{8}{2} = 4$$
  Por tanto, es isomorfo a C_4 o a V, ambos abelianos. Por tanto, $D_4/\langle r^2 \rangle$ es abeliano, luego:
  $$[D_4, D_4] = \langle r^2 \rangle$$

d) Q_2:
El diagrama de Hasse de Q_2 conviene tenerlo presente, y se encuentra en la Figura 2.50. Comprobemos cada subgrupo de Q_2, de menor a mayor orden:

- $\{1\}$ efectivamente cumple que $\{1\} \lhd Q_2$, pero:
  $$Q_2/\{1\} \cong Q_2$$
  Por tanto, el cociente no es abeliano, luego $\{1\} \neq [Q_2, Q_2]$.
- $\langle -1 \rangle = \{1, -1\}$.
  Sea $g \in Q_2$. Entonces:
  $$g(-1)g^{-1} = -(gg^{-1}) = -1 \in \langle -1 \rangle$$
  Por tanto, $\langle -1 \rangle \lhd Q_2$. Veamos que $Q_2/\langle -1 \rangle$ es abeliano:
  $$\left| \frac{Q_2}{\langle -1 \rangle} \right| = \frac{|Q_2|}{|\langle -1 \rangle|} = \frac{8}{2} = 4$$
  Por tanto, es isomorfo a C_4 o a V, ambos abelianos. Por tanto, $Q_2/\langle -1 \rangle$ es abeliano, luego:
  $$[Q_2, Q_2] = \langle -1 \rangle$$

2. Demostrar que, para $n \geqslant 3$, el subgrupo conmutador de S_n es A_n y que éste es el único subgrupo de S_n de orden $n!/2$.

Veamos que $[S_n, S_n] = A_n$.

$\subset$) Tenemos que $[S_n : A_n] = 2$, luego $A_n \lhd S_n$. Como además $S_n/A_n \cong \mathbb{Z}_2$ (abeliano), $[S_n, S_n] \subseteq A_n$.

$\supset$) Sean $i, j, k \in \{1, \ldots, n\}$ tres naturales distintos. Entonces:
$$(i\ j\ k) = (i\ j)(j\ k) = (i\ j)(i\ k)(i\ j)(i\ k) = (i\ j)(i\ k)(i\ j)^{-1}(i\ k)^{-1} = [(i\ j), (i\ k)]$$
Por tanto, como los $3-$ciclos son generadores de A_n, entonces se tiene que $A_n \subseteq [S_n, S_n]$.

Por tanto, $[S_n, S_n] = A_n$. Supongamos ahora que H es un subgrupo de S_n tal que $|H| = {}^{n!}/_{2}$. Entonces:

$$[S_n : H] = \frac{|S_n|}{|H|} = \frac{n!}{{}^{n!}/_{2}} = 2 \Longrightarrow H \lhd S_n$$

Además, el cociente S_n/H es un grupo de orden 2, luego es cíclico, y por tanto abeliano. Por tanto, $A_n = [S_n, S_n] < H$ Y $|H| = |[S_n, S_n]| = |A_n|$, luego $H = A_n$. Por tanto, A_n es el único subgrupo de S_n de orden ${}^{n!}/_{2}$.

2.5. Grupos resolubles

Ejercicio 2.5.1. Sea $N \lhd G$ un subgrupo normal y simple de un grupo G. Demostrar que si G/N tiene una serie de composición entonces G tiene una serie de composición.

Consideramos la serie de composición de G/N:

$$G/N = N_0 \rhd N_1 \rhd \cdots \rhd N_{r-1} \rhd N_r = \{1N\}.$$

Por el Tercer Teorema de Isomorfía, como $N_i < G/N$ para todo $i \in \{0, 1, \dots, r\}$ existe $G_i < G$ tal que $N \lhd G_i$ cumpliendo que:

$$N_i = G_i/N \quad \forall i \in \{0, 1, \dots, r\}.$$

Para considerar la serie buscada, hemos de probar que $G_i < G_{i-1}$ para todo $i \in \{1, \dots, r\}$. Como $N_i \subset N_{i-1}$ por la biyección del Tercer Teorema de Isomorfía se tiene que $G_i \subset G_{i-1}$; y como G_i es un grupo, se tiene que $G_i < G_{i-1}$. Consideramos por tanto la siguiente serie (donde notemos que hemos añadido el $\{1\}$):

$$G = G_0 > G_1 > \cdots > G_{r-1} > G_r = N > \{1\}$$

Nos falta ahora por ver que $G_i \lhd G_{i-1}$ para todo $i \in \{1, \dots, r\}$. Por el Tercer Teorema de Isomorfía, como $G_i/N \lhd G/N$, se tiene que $G_i \lhd G$. Como además $G_i < G_{i-1}$, se tiene que $G_i \lhd G_{i-1}$. Por último, sabemos que $\{1\} \lhd N$. Por tanto, consideramos la siguiente serie normal:

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = N \rhd \{1\}.$$

Veamos que dicha serie es de composición. Para ello, hemos de ver que los factores son simples. Por ser la serie de partida de composición, sabemos que el siguiente grupo cociente es simple:

$$\frac{G_{i-1}/N}{G_i/N} \qquad \forall i \in \{1, \dots, r\}$$

Por el Tercer Teorema de Isomorfía, se tiene que:

$$\frac{G_{i-1}}{G_i} \cong \frac{G_{i-1}/N}{G_i/N} \qquad \forall i \in \{1, \dots, r\}$$

Como el "ser simple" es una propiedad que se conserva bajo isomorfismos, se tiene que:

$$G_{i-1}/G_i \text{ es simple } \forall i \in \{1, \dots, r\}.$$

Falta por compronar que $N/\{1\}$ es simple, algo que se tiene de forma directa puesto que $N/\{1\} \cong N$ y N es simple. Por tanto, la serie

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = N \rhd \{1\}$$

tiene todos sus factores simples, y por tanto es de composición. Notemos además que $l(G) = l(G/N) + 1$.

Ejercicio 2.5.2. Sea G un grupo abeliano. Demostrar que G tiene series de composición si y sólo si G es finito.

$\Longleftarrow$) Si G es finito, entonces hemos visto que G tiene series de composición.

$\Longrightarrow$) Si G tiene una serie de composición, veamos ahora que G es finito. Consideramos la serie de composición:

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = \{1\}.$$

Como G es abeliano, todos sus subgrupos son abelianos, y por tanto todos sus factores son abelianos. Además, por ser serie de composición, todos los factores son simples. Por la caracterización de los grupos abelianos y simples, todos los factores son de orden primo (en particular, finitos).

A continuación, desarrollamos la siguiente idea. Dado un grupo A y un subgrupo suyo $B \lhd A$, si B es finito y A/B es finito, entonces A es finito. Notemos que a priori no podemos aplicar el Teorema de Lagrange, puesto que A no es necesariamente finito. Sin embargo como las clases de equivalencia del cociente A/B forman una partición de A, se tiene que:

$$A = \bigcup_{i=1}^{|A/B|} a_i B$$

Como B es finito, entonces $|a_i B| = |B|$ para todo $i \in \{1, \dots, |A/B|\}$; luego $|A| = |B| \cdot |A/B|$, y en particular A es finito.

Aplicando esta idea a la serie de composición de G, obtenemos en primer que G_{r-1} es finito, puesto que $G_{r-1}/\{1\}$ y $\{1\}$ son finitos. Análogamente, G_{r-2} es finito, puesto que G_{r-2}/G_{r-1} y G_{r-1} son finitos. Por inducción sobre r, se tiene que $G_0 = G$ es finito.

Ejercicio 2.5.3. Sea H un subgrupo normal de un grupo finito G. Demostrar que existe una serie de composición de G uno de cuyos términos es H.

Como G es finito, entonces G tiene una serie de composición. Consideramos ahora la siguiente serie normal:

$$G \rhd H \rhd \{1\}.$$

Como G admite una serie de composición, por el Teorema de Jordan-Holder dicha serie normal puede refinarse a una serie de composición.

Ejercicio 2.5.4. Se define la longitud de un grupo finito G, denotada $l(G)$, como la longitud de cualquiera de sus series de composición. Demostrar que si H es un subgrupo normal de G entonces:

$$l(G) = l(H) + l(G/H) \qquad \text{fact}(G) = \text{fact}(H) \cup \text{fact}(G/H).$$

Observación. Notemos que los factores de composición de G no tienen por qué ser únicos, por lo que a priori no podemos hablar de $\text{fact}(G)$ como un conjunto. No obstante, son únicos salvo isomorfismos (y reordenamientos, pero al trabajar con conjuntos no es necesario tener en cuenta el orden). Por tanto, dos conjuntos $\text{fact}(G)$ pueden ser distintos, pero sus elementos son isomorfos entre sí.

Por el Ejercicio 2.5.3, G tiene una serie de composición que contiene a H. Consideramos la serie de composición:

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = H \rhd G_{r+1} \rhd \cdots \rhd G_{r+m-1} \rhd G_{r+m} = \{1\}.$$

Vemos claramente que $l(G) = r + m$ y $l(H) = r + m - r = m$. Además:

$$\text{fact}(H) = \bigcup_{i=r+1}^{r+m-1} G_i/G_{i+1} \qquad \text{fact}(G) = \bigcup_{i=0}^{r+m-1} G_i/G_{i+1}.$$

Hemos de calcular ahora una serie de composición de G/H. Como $H \lhd G$ se tiene que $H \lhd G_i$ para todo $i \in \{0, 1, \ldots, r\}$. Por el Tercer Teorema de Isomorfía, como $G_{i-1} \rhd G_i$, se tiene que $G_{i-1}/H \rhd G_i/H$ para todo $i \in \{1, \ldots, r\}$. Por tanto, la serie

$$G/H = G_0/H \rhd G_1/H \rhd \cdots \rhd G_{r-1}/H \rhd G_r/H = H/H = \{1H\}$$

es una serie normal de G/H. Además, por el Tercer Teorema de Isomorfía, se tiene que:

$$\frac{G_{i-1}/H}{G_i/H} \cong G_{i-1}/G_i \qquad \forall i \in \{1, \ldots, r\}.$$

Como G_{i-1}/G_i es simple por ser un factor de composición, y los factores se conservan bajo isomorfismos, se tiene que los factores de la serie de composición de G/H son simples. Por tanto, la serie de G/H es de composición, luego se cumple que $l(G/H) = r$ y se tiene que:

$$l(H) + l(G/H) = m + r = l(G).$$

Por otro lado, los factores de la serie de composición de G/H son isomorfos por el Tercer Teorema de Isomorfía a:

$$\text{fact}(G/H) = \bigcup_{i=0}^{r} G_i/G_{i+1}$$

Por tanto, se tiene que:

$$\text{fact}(G/H) \cup \text{fact}(H) = \bigcup_{i=0}^{r+m-1} G_i/G_{i+1} = \text{fact}(G).$$

Ejercicio 2.5.5. Encontrar todas las series de composición, calcular la longitud y la lista de factores de composición de los siguientes grupos:

1. El grupo diédrico D_4.

   Conviene tener presente el Diagrama de Hasse de D_4, presente en la Figura 2.49. Simplemente lo usaremos para buscar todas las series normales de D_4

que no admitan refinamientos, consiguiendo así todas las series de composición. Para ello, iremos desde D_4 hasta $\{1\}$ por el grafo del retículo sin saltarnos vértices (evitando así los refinamientos) y yendo solo por los subgrupos normales en el anterior.

En este caso, como todos los índices de un grupo en su subgrupo adyacente son 2, todas las relaciones de inclusión dadas en el grafo son en realidad de normalidad. De hecho, todas las series de composición son las siguientes:

$$\begin{gathered}
D_4 \rhd \langle r^2, s\rangle \rhd \langle s\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, s\rangle \rhd \langle sr^2\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, s\rangle \rhd \langle r^2\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle r^2\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle sr\rangle \rhd \{1\} \\
D_4 \rhd \langle r^2, sr\rangle \rhd \langle sr^3\rangle \rhd \{1\} \\
D_4 \rhd \langle r\rangle \rhd \langle r^2\rangle \rhd \{1\}
\end{gathered}$$

Como vemos:

$$\begin{aligned}
l(D_4) &= 3 \\
\operatorname{fact}(D_4) &= \{\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2\}
\end{aligned}$$

Observación. Notemos que, puesto que dos series de composición de un mismo grupo G son isomorfas, para calcular la lista de factores de composición de un grupo G o su longitud basta con calcular una serie de composición, no todas. Se calculan todas puesto que es parte del ejercicio.

2. El grupo alternado A_4.

   El Diagrama de Hasse de A_4 está presente en la Figura 2.51. Además, se vió que el único subgrupo normal propio de A_4 es V. Por tanto, las series de composición son las siguientes:

$$\begin{gathered}
A_4 \rhd V \rhd \langle (1\ 2)(3\ 4)\rangle \rhd \{1\} \\
A_4 \rhd V \rhd \langle (1\ 3)(2\ 4)\rangle \rhd \{1\} \\
A_4 \rhd V \rhd \langle (1\ 4)(2\ 3)\rangle \rhd \{1\}
\end{gathered}$$

   Como vemos:

$$\begin{aligned}
l(A_4) &= 3 \\
\operatorname{fact}(A_4) &= \{\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2\}
\end{aligned}$$

3. El grupo simétrico S_4.

   En primer lugar, sabemos que las siguientes son series de composición de S_4:

$$\begin{gathered}
S_4 \rhd A_4 \rhd V \rhd \langle (1\ 2)(3\ 4)\rangle \rhd \{1\} \\
S_4 \rhd A_4 \rhd V \rhd \langle (1\ 3)(2\ 4)\rangle \rhd \{1\} \\
S_4 \rhd A_4 \rhd V \rhd \langle (1\ 4)(2\ 3)\rangle \rhd \{1\}
\end{gathered}$$

No obstante, podría suceder que tuviese más grupos normales. Supongamos que existe $N \lhd S_4$ tal que $N \neq A_4$ y $N \neq \{1\}$.

- Si este contiene a un $n-$ciclo $\gamma \in N$, veamos que contiene a todos los $n-$ciclos. Dado otro $n-$ciclo $\sigma \in S_4$, sean:

$$\gamma = (x_1 \ \ldots \ x_n) \in N$$
$$\sigma = (y_1 \ \ldots \ y_n) \in S_4$$

  Definimos ahora $\tau \in S_4$ como:

$$\tau(x_k) = y_k \qquad \forall k \in \{1, \ldots, n\}$$
$$\tau(k) = k \qquad \forall k \in \{1, \ldots, 4\} \setminus \{x_1, \ldots, x_n\}$$

  De esta forma, tenemos que $\sigma = \tau\gamma\tau^{-1}$. Como N es normal, se tiene que $\sigma = \tau\gamma\tau^{-1} \in N$. Por tanto, N contiene todos los $n-$ciclos.

- Si N contiene un producto de dos transposiciones disjuntas $\gamma \in N$, veamos que contiene a todos los productos de dos transposiciones disjuntas. Sea $\gamma = \gamma_1\gamma_2 \in N$ un producto de dos transposiciones disjuntas, y sea $\sigma = \sigma_1\sigma_2 \in S_4$ un producto de dos transposiciones disjuntas.

$$\gamma = \gamma_1\gamma_2 = (x_1 \ x_2)(x_3 \ x_4) \in N$$
$$\sigma = \sigma_1\sigma_2 = (y_1 \ y_2)(y_3 \ y_4) \in S_4$$

  Definimos $\tau \in S_4$ como:

$$\tau(x_n) = y_n \qquad \forall n \in \{1, \ldots, 4\}$$
$$\tau(k) = k \qquad \forall k \in \{1, \ldots, 4\} \setminus \{x_1, x_2, y_1, y_2\}$$

  De esta forma, tenemos que:

$$\tau\gamma\tau^{-1} = \tau\gamma_1\tau^{-1}\tau\gamma_2\tau^{-1} = (\tau(x_1) \ \tau(x_2))(\tau(x_3) \ \tau(x_4)) = (y_1 \ y_2)(y_3 \ y_4) = \sigma \in N.$$

  Por tanto, N contiene todos los productos de dos transposiciones disjuntas.

Este es el concepto de clase de conjugación, concepto que no se ha tratado pero no es difícil de entender. En S_4 hay:

- 1 $1-$ciclo (la identidad).
- 6 $2-$ciclos.
- 8 $3-$ciclos.
- 6 $4-$ciclos.
- 3 productos de dos transposiciones disjuntas.

Efecetivamente, se tiene que $|A_4| = 12 = 1+8+3$. Sea entonces N un subgrupo normal propio de S_4.

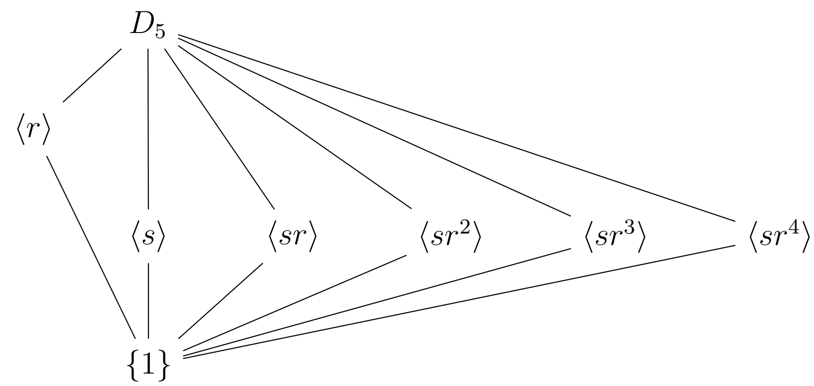


Figura 2.57: Diagrama de Hasse para los subgrupos del grupo D_5.

- Supongamos que N contiene un $2-$ciclo. Entonces, $|N| \geqslant 1{+}6 = 7$. Como $|N|$ es divisor de $|S_4| = 24$, se tiene que $|N| = 12$, luego faltarían 5 elementos. No obstante, esto no es posible (puesto que no hay ninguna clase de conjugación con 5 elementos). Por tanto, ningún $2-$ciclo pertenece a N.
- De forma análoga, se ve que no hay $4-$ciclos en N.

Como no hay $2-$ciclos ni $4-$ciclos, se tiene que $N \subset A_4$. Como N es un grupo, se tiene que $N < A_4$. Si N no es normal en A_4, entonces tampoco lo es en S_4, por lo que N es normal en A_4 y entonces será necesario pasar por A_4 en la serie de composición. Por tanto, las únicas series de composición de S_4 son las anteriormente vistas:

$$S_4 \rhd A_4 \rhd V \rhd \langle(1\ 2)(3\ 4)\rangle \rhd \{1\}$$
$$S_4 \rhd A_4 \rhd V \rhd \langle(1\ 3)(2\ 4)\rangle \rhd \{1\}$$
$$S_4 \rhd A_4 \rhd V \rhd \langle(1\ 4)(2\ 3)\rangle \rhd \{1\}$$

Como vemos:

$$l(S_4) = 4$$
$$\text{fact}(S_4) = \{\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2\}$$

4. El grupo diédrico D_5.

   Calculamos el orden de cada elemento de D_5:

$$O(r) = O(r^2) = O(r^3) = O(r^4) = 5$$
$$O(s) = O(sr) = O(sr^2) = O(sr^3) = O(sr^4) = 2$$

   Todo subgrupo de D_5 será de orden primo, luego será cíclico. El diagrama de Hasse de D_5 está presente en la Figura 2.57.

   Veamos que los subgrupos generados por elementos de orden 2 no son normales.

   - $r\ s\ r^4 = sr^3 \notin \langle s\rangle$.

- $r\ sr\ r^4 = sr^4 \notin \langle sr \rangle$.
- $r\ sr^2\ r^4 = sr^{10} = s \notin \langle sr^2 \rangle$.
- $r\ sr^3\ r^4 = sr^{11} = sr \notin \langle sr^3 \rangle$.
- $r\ sr^4\ r^4 = sr^{12} = sr^2 \notin \langle sr^4 \rangle$.

Por tanto, el único subgrupo normal de D_5 es $\langle r \rangle$. Por tanto, la única serie de composición es la siguiente:

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

Como vemos:

$$\begin{aligned} l(D_5) &= 2 \\ \operatorname{fact}(D_5) &= \{\mathbb{Z}_2, \mathbb{Z}_5\} \end{aligned}$$

5. El grupo de cuaterniones Q_2.

   El Diagrama de Hasse de Q_2 está presente en la Figura 2.50. Como todos los índices son 2, todas las relaciones de inclusión son de normalidad. Por tanto, las series de composición son las siguientes:

$$\begin{gathered} Q_2 \rhd \langle i \rangle \rhd \{-1\} \rhd \{1\} \\ Q_2 \rhd \langle j \rangle \rhd \{-1\} \rhd \{1\} \\ Q_2 \rhd \langle k \rangle \rhd \{-1\} \rhd \{1\} \end{gathered}$$

   Como vemos:

$$\begin{aligned} l(Q_2) &= 3 \\ \operatorname{fact}(Q_2) &= \{\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2\} \end{aligned}$$

6. El grupo cíclico C_{24}.

   Sabemos que los subgrupos de C_{24} son cíclicos, y por tanto abelianos. Por tanto, todos los subgrupos son normales. El Diagrama de Hasse de C_{24} está presente en la Figura 2.58.

   Las series de composición son, por tanto, las siguientes:

$$\begin{gathered} C_{24} \rhd \langle C_{12} \rangle \rhd \langle C_6 \rangle \rhd \langle C_3 \rangle \rhd \{1\} \\ C_{24} \rhd \langle C_{12} \rangle \rhd \langle C_6 \rangle \rhd \langle C_2 \rangle \rhd \{1\} \\ C_{24} \rhd \langle C_{12} \rangle \rhd \langle C_4 \rangle \rhd \langle C_2 \rangle \rhd \{1\} \\ C_{24} \rhd \langle C_8 \rangle \rhd \langle C_4 \rangle \rhd \langle C_2 \rangle \rhd \{1\} \end{gathered}$$

   Como vemos:

$$\begin{aligned} l(C_{24}) &= 4 \\ \operatorname{fact}(C_{24}) &= \{\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3\} \end{aligned}$$

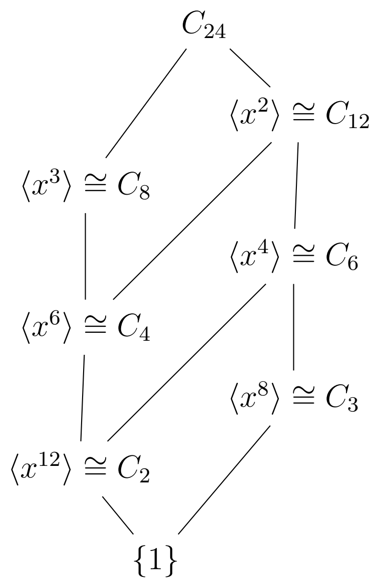


Figura 2.58: Diagrama de Hasse para los subgrupos del grupo C_{24}.

7. El grupo simétrico S_5.

   Como A_5 es normal en S_5, se tiene que la siguiente es una serie normal:

   $$S_5 \rhd A_5 \rhd \{1\}$$

   Además, S_5/A_5 es simple por ser de orden primo, mientras que $A_5/\{1\} \cong A_5$ es simple por el Lema de Abel. Por tanto, la serie es de composición.

   No obstante, podría suceder que tuviese más grupos normales. Supongamos que existe $N \lhd S_5$ tal que $N \neq A_5$ y $N \neq \{1\}$. Por una demostración análoga a la de S_4, las clases de conjugación de S_5 son las siguientes:

   - 1 1−ciclo (la identidad).
   - 10 2−ciclos.
   - 20 3−ciclos.
   - 30 4−ciclos.
   - 24 5−ciclos.
   - 15 productos de dos transposiciones disjuntas.
   - 20 productos de un 2−ciclo y un 3−ciclo.

   Efecetivamente, se tiene que $|A_5| = 60 = 1 + 20 + 24 + 15$. Sea entonces N un subgrupo normal propio de S_4.

   - Supongamos que N contiene un 2−ciclo. Entonces, $|N| \geqslant 1+10 = 11$, que no divide a 120. Como la siguiente clase de conjugación más pequeña es de 15 elementos, sabemos que $|N| > 26$. Por tanto, $|N| \in \{30, 40, 60\}$. Para, desde 11 podemos sumár un múltiplo de 10, es necesario que contenga a los 24 5−ciclos y a los 15 productos de dos transposiciones disjuntas, luego $|N| \geqslant 11 + 15 + 24 = 50$, luego $|N| = 60$, por lo que tan solo nos falta por determinar 10 elementos. No obstante, todas las clases restantes son de más de 10 elementos. Por tanto, no puede contener ningún $2-$ciclo.

- Supongamos que N contiene un $4-$ciclo. Entonces, $|N| \geqslant 1 + 30 = 31$, que no divide a 120. Por tanto, $|N| \in \{40, 60\}$. Para, desde 31 podemos sumar un múltiplo de 10, es necesario que contenga a los 24 $5-$ciclos y a los 15 productos de dos transposiciones disjuntas, pero $31+24+15 > 60$. Por tanto, no puede contener ningún $4-$ciclo.
- Supongamos que N contiene un producto de un $2-$ciclo y un $3-$ciclo. Entonces, $|N| \geqslant 1+20 = 21$, que no divide a 120. Como la siguiente clase de conjugación más pequeña es de 10 elementos, sabemos que $|N| > 31$. Por tanto, $|N| \in \{40, 60\}$. Para, desde 21 podemos sumar un múltiplo de 10, es necesario que contenga a los 24 $5-$ciclos y a los 15 productos de dos transposiciones disjuntas, luego $|N| \geqslant 21 + 15 + 24 = 60$, luego $|N| = 60$. Por tanto, N está formado por:
  - 1 $1-$ciclo (la identidad).
  - 20 productos de un $2-$ciclo y un $3-$ciclo.
  - 24 $5-$ciclos.
  - 15 productos de dos transposiciones disjuntas.

  No obstante, veamos que N no es un subgrupo de S_5 puesto que no es cerrado por producto:

  $$(1\ 2)(3\ 4\ 5)\ (1\ 2)(3\ 4) = (1\ 2)(1\ 2)(3\ 4\ 5)(3\ 4) = (3\ 4\ 5)(3\ 4) = (3\ 5) \notin N$$

  Por tanto, no puede contener ningún producto de un $2-$ciclo y un $3-$ciclo.

Por tanto, $N \subset A_5$. Como N es un grupo, se tiene que $N < A_5$. Si N no es normal en A_5, entonces tampoco lo es en S_5, por lo que N es normal en A_5. No obstante, A_5 es simple, luego $N = A_5$. Por tanto, la única serie de composición de S_5 es la siguiente:

$$S_5 \rhd A_5 \rhd \{1\}$$

Como vemos:

$$l(S_5) = 2$$
$$\text{fact}(S_5) = \{\mathbb{Z}_2, A_5\}$$

Ejercicio 2.5.6. Sea G un grupo finito, y

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

una serie normal de G. Demostrar que

$$l(G) = \sum_{i=0}^{r-1} l\left(\frac{G_i}{G_{i+1}}\right), \quad \text{fact}(G) = \bigcup_{i=0}^{r-1} \text{fact}\left(\frac{G_i}{G_{i+1}}\right).$$

Como G es finito y $G_1 \lhd G$, por el Ejercicio 2.5.4 se tiene que:

$$\begin{aligned} l(G) &= l(G_1) + l(G/G_1) \\ \text{fact}(G) &= \text{fact}(G_1) \cup \text{fact}(G/G_1). \end{aligned}$$

Como G_1 es finito y $G_2 \lhd G_1$, por el Ejercicio 2.5.4 se tiene que:

$$\begin{aligned} l(G) = l(G_1) + l(G/G_1) &= l(G_2) + l(G_1/G_2) + l(G/G_1) \\ &= l(G_2) + l(G_1/G_2) + l(G/G_1) \\ \text{fact}(G) &= \text{fact}(G_1) \cup \text{fact}(G/G_1) = \text{fact}(G_2) \cup \text{fact}(G_1/G_2) \cup \text{fact}(G/G_1). \end{aligned}$$

Iterando hasta usar que $G_r \lhd G_{r-1}$, se tiene que:

$$\begin{aligned} l(G) &= \sum_{i=0}^{r-1} l(G_i/G_{i+1}) + \cancel{l(G_r)} \\ \text{fact}(G) &= \bigcup_{i=0}^{r-1} \text{fact}(G_i/G_{i+1}) \cup \cancel{\text{fact}(G_r)}. \end{aligned}$$

Ejercicio 2.5.7. Si $G_1, G_2, \dots, G_r$ son grupos finitos, demostrar que

$$l(G_1 \times G_2 \times \cdots \times G_r) = \sum_{i=1}^{r} l(G_i), \quad \text{fact}(G_1 \times G_2 \times \cdots \times G_r) = \bigcup_{i=1}^{r} \text{fact}(G_i).$$

Demostramos por inducción sobre r.

- Para $r = 1$ se tiene trivialmente.
- Supuesto cierto para r, demostrémoslo para $r + 1$.

  Buscamos demostrarlo aplicando el Ejercicio 2.5.4. Para ello, necesitamos un subgrupo normal de $G_1 \times \cdots \times G_r \times G_{r+1}$. Definimos:

  $$\begin{array}{rccc} \pi: & G_1 \times \cdots \times G_r \times G_{r+1} & \longrightarrow & G_1 \times \cdots \times G_r \\ & (g_1, g_2, \dots, g_r, g_{r+1}) & \longmapsto & (g_1, g_2, \dots, g_r) \end{array}$$

  Tenemos que π es un homomorfismo con:

  $$\begin{aligned} \ker(\pi) &= \{1\} \times \cdots \times \{1\} \times G_{r+1} \\ Im(\pi) &= G_1 \times \cdots \times G_r. \end{aligned}$$

  Por el Primer Teorema de Isomorfía, se tiene que:

  $$\frac{G_1 \times \cdots \times G_r \times G_{r+1}}{\{1\} \times \cdots \times \{1\} \times G_{r+1}} \cong G_1 \times \cdots \times G_r.$$

  Veamos ahora que $\{1\} \times \cdots \times \{1\} \times G_{r+1}$ es isomorfo a G_{r+1}. Definimos:

  $$\begin{array}{rccc} \phi: & \{1\} \times \cdots \times \{1\} \times G_{r+1} & \longrightarrow & G_{r+1} \\ & (1, \dots, 1, g_{r+1}) & \longmapsto & g_{r+1} \end{array}$$

Vemos claramente que ϕ es un isomorfismo, luego $\{1\}\times\cdots\times\{1\}\times G_{r+1} \cong G_{r+1}$.

Vistos ambos aspectos, como $\{1\} \times \cdots \times \{1\} \times G_{r+1} = \ker(\pi) \lhd G_1 \times \cdots \times G_r \times G_{r+1}$ por el Ejercicio 2.5.4, se tiene que:

$$l(G_1 \times \cdots \times G_r \times G_{r+1}) = l(\{1\} \times \cdots \times \{1\} \times G_{r+1}) + l\left(\frac{G_1 \times \cdots \times G_r \times G_{r+1}}{\{1\} \times \cdots \times \{1\} \times G_{r+1}}\right)$$

Como las series de composición de dos grupos isomorfas son isomorfas, tenemos que:

$$l(G_1 \times \cdots \times G_r \times G_{r+1}) = l(G_{r+1}) + l\left(G_1 \times \cdots \times G_r\right) \overset{(*)}{=} l(G_{r+1}) + \sum_{i=1}^{r} l(G_i) = \sum_{i=1}^{r+1} l(G_i).$$

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

De igual forma, usando de nuevo el Ejercicio 2.5.4 se tiene que:

$$\begin{aligned}
\operatorname{fact}(G_1 \times \cdots \times G_r \times G_{r+1}) &= \operatorname{fact}(\{1\} \times \cdots \times \{1\} \times G_{r+1}) \cup \operatorname{fact}\left(\frac{G_1 \times \cdots \times G_r \times G_{r+1}}{\{1\} \times \cdots \times \{1\} \times G_{r+1}}\right) \\
&\overset{(*)}{=} \operatorname{fact}(G_{r+1}) \cup \operatorname{fact}(G_1 \times \cdots \times G_r) \\
&\overset{(**)}{=} \operatorname{fact}(G_{r+1}) \cup \bigcup_{i=1}^{r} \operatorname{fact}(G_i) = \bigcup_{i=1}^{r+1} \operatorname{fact}(G_i).
\end{aligned}$$

donde en $(**)$ hemos usado la hipótesis de inducción y en $(*)$ hemos empleado que las series de composición de dos grupos isomorfas son isomorfas, luego sus factores de composición son isomorfos y por tanto el conjunto fact de ambos grupos es el mismo (salvo la observacón que hicimos de isomorfismos en el Ejercicio 2.5.4).

Por tanto, se ha demostrado el resultado por inducción.

Ejercicio 2.5.8. Sea G un grupo cíclico de orden p^n con p primo. Demostrar que $l(G) = n$ y que $\operatorname{fact}(G) = (\mathbb{Z}_p, \mathbb{Z}_p, \overset{(n)}{\ldots}, \mathbb{Z}_p)$ (n veces).

Conviene tener presente el diagrama de Hasse de los subgrupos de $G = \langle g \rangle$, presente en la Figura 2.52. Además, como G es cíclico, en particular es abeliano y todos sus subgrupos son abelianos, luego todas las relaciones de inclusión son de normalidad. Por tanto, la única serie de composición es la siguiente:

$$G = \langle g^{p^0} \rangle \rhd \langle g^{p} \rangle \rhd \langle g^{p^2} \rangle \rhd \cdots \rhd \langle g^{p^{n-1}} \rangle \rhd \langle g^{p^n} \rangle = \{1\}$$

De esta serie de composición se deduce que $l(G) = n$. Veamos cuáles son los factores de composición:

$$\left|\frac{\langle g^{p^i} \rangle}{\langle g^{p^{i+1}} \rangle}\right| = \frac{|\langle g^{p^i} \rangle|}{|\langle g^{p^{i+1}} \rangle|} = \frac{O(g^{p^i})}{O(g^{p^{i+1}})} = \frac{p^n/\operatorname{mcd}(p^n,p^i)}{p^n/\operatorname{mcd}(p^n,p^{i+1})} = \frac{\operatorname{mcd}(p^n, p^{i+1})}{\operatorname{mcd}(p^n, p^i)} = \frac{p^{i+1}}{p^i} = p. \quad \forall i \in \{0, \ldots, n-1\}$$

Por tanto, se tiene que:

$$\frac{\langle g^{p^i}\rangle}{\langle g^{p^{i+1}}\rangle} \cong \mathbb{Z}_p \qquad \forall i \in \{0,\dots,n-1\}$$

Por tanto, los factores de composición son:

$$\text{fact}(G) = \left(\mathbb{Z}_p, \mathbb{Z}_p, \overset{(n)}{\dots}, \mathbb{Z}_p\right).$$

Ejercicio 2.5.9. Sea G un grupo cíclico de orden n. Si la descomposición de n en factores primos es $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, demostrar que

$$l(G) = e_1 + e_2 + \cdots + e_r,$$

y que

$$\text{fact}(G) = (\mathbb{Z}_{p_1}, \overset{(e_1)}{\dots}\ \mathbb{Z}_{p_1}, \dots, \mathbb{Z}_{p_r}, \overset{(e_r)}{\dots}, \mathbb{Z}_{p_r}).$$

Aplica el resultado cuando $n = 12$ y compara su longitud y factores de composición con los del grupo $\mathbb{Z}_2 \times \mathbb{Z}_6$.

Sabemos que $\text{mcd}(p_1, \dots, p_r) = 1$, luego $\text{mcd}(p_1^{e_1}, \dots, p_r^{e_r}) = 1$. Por tanto, se tiene que:

$$\prod_{i=1}^{r} C_{p_i^{e_i}} \qquad \text{es cíclico}$$

Además, se tiene que:

$$\left|\prod_{i=1}^{r} C_{p_i^{e_i}}\right| = \prod_{i=1}^{r} |C_{p_i^{e_i}}| = \prod_{i=1}^{r} p_i^{e_i} = n.$$

Por tanto, $G \cong \prod\limits_{i=1}^{r} C_{p_i^{e_i}}$. Como dos grupos isomorfos tienen series de composición isomorfas, se tiene que:

$$l(G) = l\left(\prod_{i=1}^{r} C_{p_i^{e_i}}\right) \overset{(*)}{=} \sum_{i=1}^{r} l\left(C_{p_i^{e_i}}\right) \overset{(**)}{=} \sum_{i=1}^{r} e_i$$

donde en $(*)$ hemos usado el Ejercicio 2.5.7 y en $(**)$ el Ejercicio 2.5.8.

Veamos ahora cuáles son los factores de composición. Como las series de composición de dos grupos isomorfos son isomorfas y, por tanto, sus factores de composición son isomorfos, se tiene que:

$$\begin{aligned}\text{fact}(G) &= \text{fact}\left(\prod_{i=1}^{r} C_{p_i^{e_i}}\right) \overset{(*)}{=} \bigcup_{i=1}^{r} \text{fact}\left(C_{p_i^{e_i}}\right) \overset{(**)}{=} \bigcup_{i=1}^{r} \left(\mathbb{Z}_{p_i}, \mathbb{Z}_{p_i}, \overset{(e_i)}{\dots}, \mathbb{Z}_{p_i}\right) \\ &= (\mathbb{Z}_{p_1}, \overset{(e_1)}{\dots}\ \mathbb{Z}_{p_1}, \dots, \mathbb{Z}_{p_r}, \overset{(e_r)}{\dots}, \mathbb{Z}_{p_r}).\end{aligned}$$

donde en $(*)$ hemos usado el Ejercicio 2.5.7 y en $(**)$ el Ejercicio 2.5.8. Por tanto, se ha demostrado el resultado.

Aplicándolo ahora a $n = 12$, se tiene que $12 = 2^2 \cdot 3^1$, luego:

$$\begin{aligned} l(\mathbb{Z}_{12}) &= 2 + 1 = 3 \\ \mathrm{fact}(\mathbb{Z}_{12}) &= (\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3). \end{aligned}$$

Queremos calcular ahora la longitud y factores de composición de $\mathbb{Z}_2 \times \mathbb{Z}_6$. Como este no es cíclico, calculamos su longitud y factores de composición usando el Ejercicio 2.5.7:

$$\begin{aligned} l(\mathbb{Z}_2 \times \mathbb{Z}_6) &= l(\mathbb{Z}_2) + l(\mathbb{Z}_6) = 1 + 1 + 1 = 3 \\ \mathrm{fact}(\mathbb{Z}_2 \times \mathbb{Z}_6) &= \mathrm{fact}(\mathbb{Z}_2) \cup \mathrm{fact}(\mathbb{Z}_6) = (\mathbb{Z}_2) \cup (\mathbb{Z}_2, \mathbb{Z}_3) = (\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3). \end{aligned}$$

Comprobamos por tanto que, aun no siendo isomorfos (puesto que uno es cíclico y el otro no), se cumple que:

$$\begin{aligned} l(\mathbb{Z}_{12}) &= l(\mathbb{Z}_2 \times \mathbb{Z}_6) = 3 \\ \mathrm{fact}(\mathbb{Z}_{12}) &= \mathrm{fact}(\mathbb{Z}_2 \times \mathbb{Z}_6) = (\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3). \end{aligned}$$

Notemos que si dos grupos son isomorfos entonces tienen la misma longitud y los mismos factores de composición, pero el recíproco no es cierto.

Ejercicio 2.5.10. Sea D_n el grupo diédrico de orden $2n$. Si la descomposición de n en factores primos es $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, demostrar que

$$l(D_n) = e_1 + e_2 + \cdots + e_r + 1,$$

y que

$$\mathrm{fact}(D_n) = (\mathbb{Z}_{p_1}, \overset{(e_1)}{\ldots} \mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_r}, \overset{(e_r)}{\ldots}, \mathbb{Z}_{p_r}, \mathbb{Z}_2).$$

Sabemos que la siguiente serie es una serie normal de D_n:

$$D_n \rhd \langle r \rangle \rhd \{1\}$$

Por tanto, por el Ejercicio 2.5.6 se tiene que:

$$\begin{aligned} l(D_n) &= l\left(\frac{D_n}{\langle r \rangle}\right) + l\left(\frac{\langle r \rangle}{\{1\}}\right) \\ \mathrm{fact}(D_n) &= \mathrm{fact}\left(\frac{D_n}{\langle r \rangle}\right) \cup \mathrm{fact}\left(\frac{\langle r \rangle}{\{1\}}\right) \end{aligned}$$

Sabemos que $|D_n/\langle r \rangle| = {}^{2n}/_{n} = 2$, luego $D_n/\langle r \rangle \cong \mathbb{Z}_2$. Por otro lado, sabemos que $\langle r \rangle$ es cíclico de orden n, luego $\langle r \rangle \cong \mathbb{Z}_n$. Como la longitud y los factores se mantienen bajo isomorfismos, y usando el Ejercicio 2.5.9 con $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ y 2 primo, se tiene que:

$$\begin{aligned} l(D_n) &= l\left(\frac{D_n}{\langle r \rangle}\right) + l\left(\frac{\langle r \rangle}{\{1\}}\right) = l(\mathbb{Z}_2) + l(\mathbb{Z}_n) = 1 + (e_1 + e_2 + \cdots + e_r) \\ &= e_1 + e_2 + \cdots + e_r + 1 \\ \mathrm{fact}(D_n) &= \mathrm{fact}\left(\frac{D_n}{\langle r \rangle}\right) \cup \mathrm{fact}\left(\frac{\langle r \rangle}{\{1\}}\right) = \mathrm{fact}(\mathbb{Z}_2) \cup \mathrm{fact}(\mathbb{Z}_n) \\ &= (\mathbb{Z}_2) \cup \left(\mathbb{Z}_{p_1}, \overset{(e_1)}{\ldots} \mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_r}, \overset{(e_r)}{\ldots}, \mathbb{Z}_{p_r}\right) \\ &= (\mathbb{Z}_{p_1}, \overset{(e_1)}{\ldots} \mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_r}, \overset{(e_r)}{\ldots}, \mathbb{Z}_{p_r}, \mathbb{Z}_2). \end{aligned}$$

Ejercicio 2.5.11. Demostrar que D_n, S_2, S_3 y S_4 son grupos resolubles.

1. D_n.

   Una serie normal de D_n es la siguiente:

   $$D_n \rhd \langle r \rangle \rhd \{1\}$$

   Sus factores son:

   $$\frac{D_n}{\langle r \rangle} \cong \mathbb{Z}_2$$
   $$\frac{\langle r \rangle}{\{1\}} \cong \langle r \rangle \cong \mathbb{Z}_n$$

   Por tanto, todos sus factores son abelianos, luego D_n es resoluble.

2. S_2.

   La serie derivada de S_2 es la siguiente:

   $$S_2 \rhd \{1\}$$

   Donde he empleado que $S_2 \cong C_2$ es abeliano, luego $[S_2, S_2] = \{1\}$. Por tanto, S_2 es resoluble.

3. S_3.

   Sabemos que $S_3' = [S_3, S_3] = A_3 \cong C_3$ abeliano, luego la serie derivada de S_3 es la siguiente:

   $$S_3 \rhd A_3 \rhd \{1\}$$

   Por tanto, S_3 es resoluble.

4. S_4.

   Una serie normal de S_4 es la siguiente:

   $$S_4 \rhd A_4 \rhd V \rhd \{1\}$$

   Sus factores son:

   $$\frac{S_4}{A_4} \cong \mathbb{Z}_2$$
   $$\frac{A_4}{V} \cong \mathbb{Z}_3$$
   $$\frac{V}{\{1\}} \cong V$$

   Donde V es el grupo de Klein, que es abeliano. Por tanto, todos sus factores son abelianos, luego S_4 es resoluble.

Ejercicio 2.5.12. Sean H y K subgrupos normales de un grupo G tales que G/H y G/K son ambos resolubles. Demostrar que $G/(H \cap K)$ también es resoluble.

Por el Segundo Teorema de Isomorfía, como $H \lhd G$, tenemos $(H \cap K) \lhd K$ y:

$$\frac{K}{H \cap K} \cong \frac{KH}{H}$$

Este Teorema también afirma que $KH < G$, luego $KH/H < G/H$. Como G/H es resoluble, se tiene que KH/H es resoluble. Por tanto, $K/(H \cap K)$ es resoluble.

Por otro lado, como $K, H \lhd G$, se tiene que $(H \cap K) \lhd G$. Como $(H \cap K) \subset K$ y $K \lhd G$, por el Tercer Teorema de Isomorfía se tiene que $H/(H \cap K) \lhd G/(H \cap K)$ y:

$$\frac{G/(H \cap K)}{K/(H \cap K)} \cong \frac{G}{K}$$

Como G/K es resoluble, se tiene que $G/(H \cap K)/K/(H \cap K)$ es resoluble (puesto que esta propiedad se mantiene por isomorfismo).

Como $\dfrac{G/(H \cap K)}{K/(H \cap K)}$ y $K/(H \cap K)$ son ambos resolubles, entonces $G/(H \cap K)$ es resoluble.

Ejercicio 2.5.13. Sea G un grupo resoluble y sea H un subgrupo normal no trivial de G. Demostrar que existe un subgrupo no trivial A de H que es abeliano y normal en G.

Como $H < G$, entonces H es resoluble. Consideramos su serie derivada:

$$H \rhd H' \rhd H'' \rhd \cdots \rhd H^{(n)} = \{1\}$$

Como $H \neq \{1\}$, $n \neq 0$. Sea ahora $A = H^{(n-1)}$ (que podemos considerarlo puesto que $n \neq 0$). Como $[A, A] = [H^{(n-1)}, H^{(n-1)}] = H^{(n)} = \{1\}$, se tiene que A es abeliano. Nos falta por ver que $A \lhd G$.

Consideramos la siguiente serie normal de G:

$$G \rhd H \rhd H' \rhd H'' \rhd \cdots \rhd H^{(n)} = \{1\}$$

Veamos que $H^{(i)} \lhd G$ para todo $i \in \{0, \dots, n\}$.

- Para $i = 0$, $G \lhd H$, luego se tiene que $H^0 \lhd G$.
- Supuesto cierto para i, veamos que se cumple para $i + 1$.

  Sabemos que $H^{(i)} \lhd G$, y queremos ver que $[H^{(i)}, H^{(i)}] \lhd G$. Como se tiene que $[H^{(i)}, H^{(i)}] = \langle [x, y] \mid x, y \in H^{(i)} \rangle$ y $[x, y]^{-1} = [y, x]$, tan solo es necesario comprobarlo sobre los generadores. Por tanto, sea $x, y \in H^{(i)}$, $g \in G$. Entonces:

  $$g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$$

  Como $H^{(i)} \lhd G$, se tiene que $gxg^{-1}, gyg^{-1} \in H^{(i)}$, luego concluimos que $[gxg^{-1}, gyg^{-1}] \in [H^{(i)}, H^{(i)}]$. Por tanto, $H^{(i+1)} = [H^{(i)}, H^{(i)}] \lhd G$.

Por tanto, $H^{(i)} \lhd G$ para todo $i \in \{0, \ldots, n\}$. En particular, $A = H^{(n-1)} \lhd G$.

Ejercicio 2.5.14. Demuestra que todo p-grupo finito es resoluble.

Esto equivale a probar que, para todo $n \in \mathbb{N}$, todo grupo de orden p^n es resoluble. Vamos a demostrarlo por inducción sobre n.

- Caso base: $n = 1$.

  Sea G un grupo de orden p. Entonces, G es cíclico, luego abeliano y por tanto resoluble.

- Paso inductivo: Supongamos que todo grupo de orden p^k, con $k \in \mathbb{N}$, $k < n$ es resoluble. Demostremos que todo grupo de orden p^n es resoluble.

  Sea G un grupo de orden p^n. El procedimiento será ver que $Z(G)$, $G/Z(G)$ son ambos resolubles, y por tanto G es resoluble.

  Sabemos en primer lugar que $Z(G)$ es abeliano, luego resoluble. Por otro lado, sabemos que $|Z(G)| \mid |G|$, luego $|Z(G)| = p^k$ para algún $k \in \{0, \ldots, n\}$. Además, como G es un p-grupo, en particular su centro es no trivial, luego $k \neq 0$. Por tanto, tenemos que:

  $$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^n}{p^k} = p^{n-k}$$

  Como $n-k < n$, por la hipótesis de inducción se tiene que $G/Z(G)$ es resoluble.

  Como $Z(G)$ y $G/Z(G)$ son ambos resolubles, entonces G es resoluble.

Por tanto, se ha demostrado que todo grupo de orden p^n es resoluble para todo $n \in \mathbb{N}$.

Ejercicio 2.5.15. Demuestra que todo grupo de orden pq, con p y q primos, es un grupo resoluble.

Sea G un grupo de orden pq, y supongamos sin pérdida de generalidad que $p \geqslant q$. Sea n_p el número de $p-$subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, se tiene que:

$$\begin{aligned} n_p &\equiv 1 \mod p \\ n_p &\mid q \end{aligned}$$

Como $n_p \mid q$, entonces $n_p \leqslant q \leqslant p$. Como $n_p \equiv 1 \mod p$, concluimos que $n_p = 1$. Sea P el único p-subgrupo de Sylow de G. Como es el único, entonces $P \lhd G$. Por ser un $p-$subgrupo de Sylow de G, entonces $|P| = p$. Por tanto, tenemos que:

- $|P| = p$ primo, luego P es cíclico y abeliano, luego P es resoluble.
- $|G/P| = q$ primo, luego G/P es cíclico y abeliano, luego G/P es resoluble.

Por tanto, como P y G/P son ambos resolubles, entonces G es resoluble.

Ejercicio 2.5.16. Demuestra que todo grupo de orden p^2q, con p y q primos, es un grupo resoluble.

Opción 1.

Sea G un grupo de orden p^2q. Sea n_p el número de $p-$subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, se tiene que:

$$n_p \equiv 1 \mod p$$
$$n_p \mid q$$

Por la segunda condición, tenemos que $n_p \in \{1, q\}$. Hay dos opciones:

- $\underline{n_p = 1}$.
  En tal caso, sea P el único p-subgrupo de Sylow de G. Como es el único, entonces $P \lhd G$. Por ser un $p-$subgrupo de Sylow de G, entonces $|P| = p^2$. Por tanto, tenemos que:
  - $|P| = p^2$, luego P es un $p-$grupo, luego resoluble.
  - $|G/P| = q$, luego G/P es un $q-$grupo, luego resoluble.

  Por tanto, como P y G/P son ambos resolubles, entonces G es resoluble.
- $\underline{n_p = q}$: Sea n_q el número de $q-$subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, se tiene que:

  $$n_q \equiv 1 \mod q$$
  $$n_q \mid p^2$$

  Por la segunda condición, tenemos que $n_q \in \{1, p, p^2\}$.
  - Si $n_q = p$, como $n_q \equiv 1 \mod q$, entonces $\exists k \in \mathbb{N}$ tal que:

    $$p = 1 + kq$$

    Como $n_p \mid q$, $\exists k' \in \mathbb{N}$ tal que $q = k'n_p$, luego:

    $$p = 1 + k'kn_p$$

    Por último, como $n_p \equiv 1 \mod p$, $\exists k''' \in \mathbb{N}$ tal que $n_p = 1 + k''p$, luego:

    $$p = 1 + k'k''(1 + k''')p > p$$

    Lo cual es una contradicción, luego $n_q \neq p$.
  - Si $n_q = p^2$, tenemos que hay p^2 q-subgrupos de Sylow de G; es decir, hay p^2 subgrupos de orden q. Sean estos $Q_1, \dots, Q_{p^2}$. Fijado $i \in \{1, \dots, p^2\}$, tenemos que $|Q_i| = q$, luego todo elemento distinto de 1 de Q_i tiene orden q. Por tanto, cada Q_i tiene $q - 1$ elementos de orden q.
    - Supongamos que $\exists i, j \in \{1, \dots, p^2\}$ tales que $i \neq j$ y $Q_i \cap Q_j \neq \{1\}$. Como $Q_i \cap Q_j < Q_i$ y el orden de un subgrupo divide el orden del grupo, tenemos que $Q_i \cap Q_j = Q_i$, luego $Q_i = Q_j$, en contradicción con que $i \neq j$.

Por tanto, $Q_i \cap Q_j = \{1\}$ para todo $i, j \in \{1, \ldots, p^2\}$ tales que $i \neq j$. Como hay p^2 subgrupos de orden q y cada uno de ellos tiene $q-1$ elementos de orden q todos ellos distintos, sabemos que hay $p^2(q-1)$ elementos de orden q en G.
Por otro lado, como $n_p = q$, tenemos que hay q p-subgrupos de Sylow de G. Sean estos $P_1, \ldots, P_q$. Fijado $i \in \{1, \ldots, q\}$, tenemos que $|P_i| = p^2$, luego todo elemento distinto de 1 de P_i tiene orden p o p^2. En este caso no podemos garantizar que las intersecciones sean triviales (puesto que podrían tener orden p), pero fijado $i \in \{1, \ldots, q\}$, P_i tiene p^2-1 elementos de orden p o p_2. Además, sabemos que $\exists j \in \{1, \ldots, q\}$ tal que $P_j \cap P_i \neq P_i$ (pues si no, P_i sería el único p-subgrupo de Sylow de G y por tanto $n_p = 1$). Por tanto, sabemos que, al menos, hay $p^2 - 1$ elementos de orden p o p^2 en G (los de P_i) pero no son los únicos (pues P_j tiene algún elemento de orden p o p^2 distinto de los de P_i).
En conclusión, hemos demostrado que hay $p^2(q-1)$ elementos de orden q y hay más de $p^2 - 1$ elementos de orden p o p^2 en G. Por tanto, tenemos que:

$$|G| = p^2q > p^2 - 1 + p^2(q-1) + 1 = p^2 - 1 + p^2q - p^2 + 1 = p^2q$$

Lo cual es una contradicción, luego $n_q \neq p^2$.

Por tanto, $n_q = 1$. Sea Q el único q-subgrupo de Sylow de G. Como es el único, entonces $Q \lhd G$. Por ser un q-subgrupo de Sylow de G, entonces $|Q| = q$. Por tanto, tenemos que:

- $|Q| = q$ primo, luego Q es un q-grupo, luego resoluble.
- $|G/Q| = p^2$, luego G/Q es un p-grupo, luego resoluble.

Por tanto, como Q y G/Q son ambos resolubles, entonces G es resoluble.

En cualquier caso, hemos visto que G es resoluble.

Opción 2.
Distinguimos casos:

- Si $p = q$, entonces tenemos un grupo de orden $|G| = p^3$:
  - Si G es abeliano, entonces será resoluble.
  - Si G no es abeliano, entonces sabemos por Burnside que $|Z(G)| \geqslant p$ y que $|Z(G)| < p^2$, por lo que $|Z(G)| = p$, luego $Z(G) \cong \mathbb{Z}_p$, luego $Z(G)$ es resoluble. Además, tenemos que $Z(G) \lhd G$, con:

    $$|G/Z(G)| = p^2$$

    Y sabemos que todo grupo de orden p^2 es abeliano, luego resoluble. En definitiva, G es resoluble, por ser $Z(G)$ y $G/Z(G)$ resolubles.
- Si $p > q$, el Segundo Teorema de Sylow nos dice que:

$$\left.\begin{array}{r} n_p \mid q \\ n_p \equiv 1 \mod p \end{array}\right\} \Longrightarrow \left\{\begin{array}{r} n_p < q < p \\ n_p \equiv 1 \mod p \end{array}\right. \Longrightarrow n_p = 1$$

Como tenemos un único $p-$subgrupo de Sylow de G, llamémoslo $P < G$, será $P \lhd G$, con $|P| = p^2$, luego P es abeliano y en particular, resoluble. Como:

$$|G/P| = q$$

Tendremos que $G/P \cong \mathbb{Z}_q$, luego también será resoluble, de donde G será resoluble.

- Si $p < q$, el Segundo Teorema de Sylow nos dice que:

$$\left.\begin{array}{r} n_q \mid p^2 \\ n_q \equiv 1 \mod q \end{array}\right\} \Longrightarrow n_q \in \{1, p, p^2\}$$

Distinguimos casos:

  - Si $n_q = p$, entonces tenemos que $p \equiv 1 \mod q$, de donde $q \mid p - 1$ con $p - 1 < p < q$, <u>contradicción</u>.
  - Si $n_q = p^2$, de la misma forma tendremos que $q \mid p^2-1 = (p-1)(p+1)$. Como q es primo, ha de ser $q \mid p - 1$ o $q \mid p + 1$, por definición de primo. El caso $q \mid p - 1$ lo hemos discutido en el punto superior y es imposible.

    Suponemos por tanto que $q \mid p+1$, y como $p < q$, ha de ser $q = p+1$. Como solo hay dos primos consecutivos, tendremos que $q = 3$ y $p = 2$, por lo que estamos en un grupo de orden 12 con más de un $3-$subgrupo de Sylow ($n_3 = 2^2 = 4$), luego $G \cong A_4$ (por un ejercicio de la relación de $p-$grupos), y A_4 es resoluble:

$$A_4 \rhd V \rhd \{1\}$$

    Luego G también lo será.
  - Si $n_q = 1$, tenemos entonces la existencia de un único $q-$subgrupo de Sylow $Q \lhd G$ con $|Q| = q$, luego este será resoluble. Además:

$$|G/Q| = p^2$$

    También será resoluble, luego G es resoluble.

Ejercicio 2.5.17. Demuestra que si p_1, p_2, p_3 son tres primos tales que $p_3 > p_1p_2$ entonces cualquier grupo de orden $p_1p_2p_3$ es resoluble.

Sea G un grupo de orden $p_1p_2p_3$. Sea n_{p_3} el número de p_3-subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, se tiene que:

$$\begin{aligned} n_{p_3} &\equiv 1 \mod p_3 \\ n_{p_3} &\mid p_1p_2 \end{aligned}$$

Por la segunda condición, tenemos que $n_{p_3} \in \{1, p_1, p_2, p_1p_2\}$.

- Si $n_{p_3} = p_1$:

  Como $n_{p_3} \equiv 1 \mod p_3$, entonces $\exists k \in \mathbb{N}$ tal que:

$$p_1 = 1 + kp_3 \Longrightarrow p_1p_2 = p_2 + kp_2p_3 > p_3$$

  Lo cual es una contradicción, luego $n_{p_3} \neq p_1$.

- Si $n_{p_3} = p_2$:

  Como $n_{p_3} \equiv 1 \mod p_3$, entonces $\exists k \in \mathbb{N}$ tal que:

  $$p_2 = 1 + kp_3 \Longrightarrow p_1p_2 = p_1 + kp_1p_3 > p_3$$

  Lo cual es una contradicción, luego $n_{p_3} \neq p_2$.

- Si $n_{p_3} = p_1p_2$:

  Como $n_{p_3} \equiv 1 \mod p_3$, entonces $\exists k \in \mathbb{N}$ tal que:

  $$p_1p_2 = 1 + kp_3 > p_3$$

  Lo cual es una contradicción, luego $n_{p_3} \neq p_1p_2$.

Por tanto, $n_{p_3} = 1$. Sea P el único p_3-subgrupo de Sylow de G. Como es el único, entonces $P \lhd G$. Por ser un p_3-subgrupo de Sylow de G, entonces $|P| = p_3$. Por tanto, tenemos que:

- $|P| = p_3$ primo, luego P es un p_3-grupo, luego resoluble.
- $|G/P| = p_1p_2$, y por tanto es resoluble por el Ejercicio 2.5.15.

Por tanto, como P y G/P son ambos resolubles, entonces G es resoluble.

Ejercicio 2.5.18.

1. Demuestra que todo grupo de orden 70 es resoluble.

   Tenemos que $70 = 2 \cdot 5 \cdot 7$. Por el Segundo Teorema de Sylow, se tiene que:

   $$\begin{aligned} &n_7 \equiv 1 \mod 7 \\ &n_7 \mid 10 \end{aligned}$$

   Por tanto, $n_7 = 1$. Entonces existe P único 7-subgrupo de Sylow de G. Como es el único, entonces $P \lhd G$. Por ser un 7-subgrupo de Sylow de G, entonces $|P| = 7$. Por tanto, tenemos que:

   - $|P| = 7$ primo, luego P es un 7-grupo, luego resoluble.
   - $|G/P| = 10 = 5 \cdot 2$, y por tanto es resoluble por el Ejercicio 2.5.15.

   Por tanto, como P_7 y G/P_7 son ambos resolubles, entonces G es resoluble.

2. Demuestra que todo grupo de orden 24 es resoluble.

   Sea G un grupo de orden 24. Sea n_3 el número de $3-$subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, se tiene que:

   $$\begin{aligned} &n_3 \equiv 1 \mod 3 \\ &n_3 \mid 8 \end{aligned}$$

   Por tanto, $n_3 \in \{1, 4\}$.

- Si $n_3 = 1$, entonces existe P único 3-subgrupo de Sylow de G. Como es el único, entonces $P \lhd G$. Por ser un 3-subgrupo de Sylow de G, entonces $|P| = 3$. Por tanto, tenemos que:
  - $|P| = 3$ primo, luego P es un 3-grupo, luego resoluble.
  - $|G/P| = 8$, luego G/P es un 2-grupo, luego resoluble.

  Por tanto, como P y G/P son ambos resolubles, entonces G es resoluble.
- Si $n_3 = 4$, entonces hay 4 3-subgrupos de Sylow de G:
  $$\mathrm{Syl}_3(G) = \{P_1, P_2, P_3, P_4\}$$
  Consideramos ahora la acción por conjugación de G sobre $\mathrm{Syl}_3(G)$. Sea ϕ su representación por permutaciones:
  $$\begin{array}{rccc} \phi: & G & \longrightarrow & \mathrm{Perm}(\mathrm{Syl}_3(G)) \\ & g & \longmapsto & \phi_g \end{array}$$
  Como $|\,\mathrm{Syl}_3(G)| = 4$, tenemos que $\mathrm{Perm}(\mathrm{Syl}_3(G)) = S_4$. Por tanto, ϕ es un homomorfismo de G en S_4.
  - Si $\ker(\phi) = \{1\}$, entonces por el Primer Teorema de Isomorfía:
    $$G \cong G/\{1\} = G/\ker(\phi) \cong Im(\phi)$$
    Como $Im(\phi) < S_4$ y S_4 es resoluble, entonces $Im(\phi)$ es resoluble, y como esta propiedad se mantiene por isomorfismo, entonces G es resoluble.
  - Si $\ker(\phi) = G$, entonces ϕ es el homomorfismo trivial, luego G:
    $$\phi_g(P_i) = {}^gP_i = gP_ig^{-1} = P_i \qquad \forall g \in G, \forall P_i \in \mathrm{Syl}_3(G)$$
    Como $P_i = gP_ig^{-1}$ para todo $g \in G$, entonces $P_i \lhd G$, luego P_i es el único 3-subgrupo de Sylow de G, lo que contradice que $n_3 = 4$. Este caso no es posible.
  - Si $\ker(\phi) \neq \{1\}, G$, entonces:
    - Como $\ker(\phi) < G$, sabemos que $|\ker(\phi)| \mid |G| = 24$, luego:
      $$|\ker(\phi)| \in \{2, 3, 4, 6, 8, 12\}$$
      Veamos si $\ker(\phi)$ es resoluble:
      - Si $|\ker(\phi)| \in \{2, 3, 4, 8\}$, entonces $\ker(\phi)$ es un p-grupo, luego resoluble.
      - Si $|\ker(\phi)| = 6 = 3 \cdot 2$, es resoluble por el Ejercicio 2.5.15.
      - Si $|\ker(\phi)| = 12 = 3 \cdot 2^2$, es resoluble por el Ejercicio 2.5.17.

      Por tanto, en cualquiera de estos casos, $\ker(\phi)$ es resoluble.
    - Por el Primer Teorema de Isomorfía, tenemos que:
      $$G/\ker(\phi) \cong Im(\phi)$$
      Como $Im(\phi) < S_4$ y S_4 es resoluble, entonces $Im(\phi)$ es resoluble, y como esta propiedad se mantiene por isomorfismo, entonces $G/\ker(\phi)$ es resoluble.

Por tanto, como $\ker(\phi)$ y $G/\ker(\phi)$ son ambos resolubles, entonces G es resoluble.

En cualquier caso, G es resoluble.

En conclusión, hemos visto que G es resoluble.

3. Demuestra que todo grupo de orden 100 es resoluble.

Tenemos que $100 = 2^2 \cdot 5^2$. Por el Segundo Teorema de Sylow, se tiene que:

$$\begin{aligned} n_5 &\equiv 1 \mod 5 \\ n_5 &\mid 4 \end{aligned}$$

Por tanto, $n_5 = 1$. Entonces existe P único 5-subgrupo de Sylow de G. Como es el único, entonces $P \lhd G$. Por ser un 5-subgrupo de Sylow de G, entonces $|P| = 25$. Por tanto, tenemos que:

- $|P| = 25 = 5^2$, luego P es un 5-grupo, luego resoluble.
- $|G/P| = 4$, luego G/P es un 2-grupo, luego resoluble.

Por tanto, como P y G/P son ambos resolubles, entonces G es resoluble.

4. Demuestra que todo grupo de orden 48 es resoluble.

Tenemos que $48 = 2^4 \cdot 3$. Por el Segundo Teorema de Sylow, se tiene que:

$$\begin{aligned} n_3 &\equiv 1 \mod 3 \\ n_3 &\mid 16 \end{aligned}$$

Por tanto, $n_3 \in \{1, 4, 16\}$. Por otro lado:

$$\begin{aligned} n_2 &\equiv 1 \mod 2 \\ n_2 &\mid 3 \end{aligned}$$

Por tanto, $n_2 \in \{1, 3\}$. Distinguimos en función de los valores de n_2:

- Si $n_2 = 1$, entonces existe Q único 2-subgrupo de Sylow de G. Como es el único, entonces $Q \lhd G$. Por ser un 2-subgrupo de Sylow de G, entonces $|Q| = 16$. Por tanto, tenemos que:
  - $|Q| = 16 = 2^4$, luego Q es un 2-grupo, luego resoluble.
  - $|G/Q| = 3$, luego G/Q es un 3-grupo, luego resoluble.

  Por tanto, como Q y G/Q son ambos resolubles, entonces G es resoluble.
- Si $n_2 = 3$, entonces hay tres subgrupos de Sylow de orden 2. Sea $\mathrm{Syl}_2(G) = \{Q_1, Q_2, Q_3\}$. Consideramos ahora la acción por conjugación de G sobre $\mathrm{Syl}_2(G)$. Sea ϕ su representación por permutaciones:

  $$\begin{array}{rccl} \phi: & G & \longrightarrow & \mathrm{Perm}(\mathrm{Syl}_2(G)) \\ & g & \longmapsto & \phi_g \end{array}$$

  Como $|\,\mathrm{Syl}_2(G)| = 3$, tenemos que $\mathrm{Perm}(\mathrm{Syl}_2(G)) = S_3$. Por tanto, ϕ es un homomorfismo de G en S_3.

- Si $\ker(\phi) = \{1\}$, entonces por el Primer Teorema de Isomorfía:

  $$G \cong G/\{1\} = G/\ker(\phi) \cong Im(\phi)$$

  Como $Im(\phi) < S_3$ y S_3 es resoluble, entonces $Im(\phi)$ es resoluble, y como esta propiedad se mantiene por isomorfismo, entonces G es resoluble.
- Si $\ker(\phi) = G$, entonces ϕ es el homomorfismo trivial, luego:

  $$\phi_g(Q_i) = {}^gQ_i = gQ_ig^{-1} = Q_i \qquad \forall g \in G, \forall Q_i \in \mathrm{Syl}_2(G)$$

  Como $Q_i = gQ_ig^{-1}$ para todo $g \in G$, entonces $Q_i \lhd G$, luego Q_i es el único 2-subgrupo de Sylow de G, lo que contradice que $n_2 = 3$. Este caso no es posible.
- Si $\ker(\phi) \neq \{1\}, G$, entonces:
  - Como $\ker(\phi) < G$, sabemos que $|\ker(\phi)| \mid |G| = 48$, luego:

    $$|\ker(\phi)| \in \{2, 3, 4, 6, 8, 12, 16, 24\}$$

    Veamos si $\ker(\phi)$ es resoluble:
    - Si $|\ker(\phi)| \in \{2, 3, 4, 8, 16\}$, entonces $\ker(\phi)$ es un p-grupo, luego resoluble.
    - Si $|\ker(\phi)| = 6 = 3 \cdot 2$, es resoluble por el Ejercicio 2.5.15.
    - Si $|\ker(\phi)| = 12 = 3 \cdot 2^2$, es resoluble por el Ejercicio 2.5.17.
    - Si $|\ker(\phi)| = 24$, es resoluble por el segundo apartado de este ejercicio.

    Por tanto, en cualquiera de estos casos, $\ker(\phi)$ es resoluble.
  - Por el Primer Teorema de Isomorfía, tenemos que:

    $$G/\ker(\phi) \cong Im(\phi)$$

    Como $Im(\phi) < S_3$ y S_3 es resoluble, entonces $Im(\phi)$ es resoluble, y como esta propiedad se mantiene por isomorfismo, entonces $G/\ker(\phi)$ es resoluble.

  Por tanto, como $\ker(\phi)$ y $G/\ker(\phi)$ son ambos resolubles, entonces G es resoluble.

En cualquier caso, G es resoluble.

En conclusión, hemos visto que G es resoluble.

5. Sea G un grupo de orden 200. Demuestra que $G \times D_{41}$ es resoluble.

Veamos que todo grupo de orden 200 es resoluble. Tenemos que $200 = 2^3 \cdot 5^2$. Por el Segundo Teorema de Sylow, se tiene que:

$$\begin{aligned} n_5 &\equiv 1 \mod 5 \\ n_5 &\mid 8 \end{aligned}$$

Por tanto, $n_5 = 1$. Entonces existe P único 5-subgrupo de Sylow de G. Como es el único, entonces $P \lhd G$. Por ser un 5-subgrupo de Sylow de G, entonces $|P| = 25$. Por tanto, tenemos que:

- $|P| = 25 = 5^2$, luego P es un 5-grupo, luego resoluble.
- $|G/P| = 8$, luego G/P es un 2-grupo, luego resoluble.

Por tanto, como P y G/P son ambos resolubles, entonces G es resoluble.

Como $|D_{41}| = 82 = 2 \cdot 41$ y 41 es primo, por el Ejercicio 2.5.15 sabemos que D_{41} es resoluble.

Por tanto, como G y D_{41} son ambos resolubles, entonces $G \times D_{41}$ es resoluble.

6. Demuestra que todo grupo de orden 63 es soluble (sin usar que es un caso particular de un grupo de orden p^2q con p y q primos).

   Sea G un grupo de orden $63 = 3^2 \cdot 7$. Sea n_7 el número de 7−subgrupos de Sylow de G. Por el Segundo Teorema de Sylow, se tiene que:

$$n_7 \equiv 1 \mod 7$$
$$n_7 \mid 9$$

   Por tanto, $n_7 = 1$. Entonces existe P único 7-subgrupo de Sylow de G. Como es el único, entonces $P \lhd G$. Por ser un 7-subgrupo de Sylow de G, entonces $|P| = 7$. Por tanto, tenemos que:

   - $|P| = 7$ primo, luego P es un 7-grupo, luego resoluble.
   - $|G/P| = 9 = 3^2$, luego G/P es un 3-grupo, luego resoluble.

   Por tanto, como P y G/P son ambos resolubles, entonces G es resoluble.

2.6. $G-$conjuntos y p-grupos

Ejercicio 2.6.1. Si X es un $G-$conjunto, demostrar que $x^g = {}^{g^{-1}}x,\ x \in X, g \in G$, define una acción por la derecha de G sobre X.

En primer lugar, vemos que se trata de una aplicación de $G \times X$ en X. Veamos ahora que cumple las condiciones necesarias para ser una acción por la derecha:

- $x^1 = x$ para todo $x \in X$.
$$x^1 = {}^{1^{-1}}x = {}^1x = x$$
- $(x^g)^h = x^{gh}$ para todo $x \in X$ y $g, h \in G$.
$$(x^g)^h = {}^{h^{-1}}(x^g) = {}^{h^{-1}}\left({}^{g^{-1}}x\right) = {}^{h^{-1}g^{-1}}x = {}^{(gh)^{-1}}x = x^{gh}$$

Por tanto, se trata de una acción por la derecha de G sobre X.

Ejercicio 2.6.2. Sea G un grupo y N un subgrupo normal abeliano de G. Demostrar que G/N actúa sobre N por conjugación y obtener entonces un homomorfismo $\varphi : G/N \to \mathrm{Aut}(N)$.

Veamos en primer lugar que G/N actúa sobre N por conjugación. Es decir, que la siguiente aplicación es una acción de G/N sobre N:

$$\begin{array}{rccc} ac: & G/N \times N & \longrightarrow & N \\ & (gN, n) & \longmapsto & {}^{gN}n = gng^{-1} \end{array}$$

Veamos en primer lugar que está bien definida. Sean $g_1, g_2 \in G$ de forma que $g_1N = g_2N$. Entonces $\exists n' \in N$ tal que $g_1 = g_2n'$. Entonces:

$${}^{g_1N}n = g_1ng_1^{-1} = g_2n'n(g_2n')^{-1} = g_2n'n(n')^{-1}g_2^{-1} \overset{(*)}{=} g_2n'(n')^{-1}ng_2^{-1} = g_2ng_2^{-1} = {}^{g_2N}n$$

donde en $(*)$ hemos usado que N es abeliano. Por tanto, la acción está bien definida. Veamos ahora que se trata de una acción.

- ${}^{1N}n = 1n1^{-1} = n$ para todo $n \in N$.
- Comprobemos la segunda propiedad:
$${}^{(g_1N)(g_2N)}n = {}^{g_1g_2N}n = g_1g_2ng_2^{-1}g_1^{-1} = g_1\left({}^{g_2N}n\right)g_1^{-1} = {}^{g_1N}\left({}^{g_2N}n\right).$$

Buscamos ahora el homomorfismo $\varphi : G/N \to \mathrm{Aut}(N)$. En primer lugar, consideramos el siguiente homomorfismo:

$$\begin{array}{rccc} \Phi: & G/N & \longrightarrow & \mathrm{Perm}(N) \\ & gN & \longmapsto & {}^{gN}(\cdot) = ac(gN, \cdot) \end{array}$$

Es necesario ver que, fijado $gN \in G/N$, la aplicación siguiente, además de pertenecer a $\mathrm{Perm}(N)$, pertenece a $\mathrm{Aut}(N)$:

$$\begin{array}{rccc} f: & N & \longrightarrow & N \\ & n & \longmapsto & {}^{gN}n = gng^{-1} \end{array}$$

Sabemos que es biyectiva, por lo que tan solo nos queda probar que es un homomorfismo. Sean $n_1, n_2 \in N$:

$$f(n_1n_2) = {}^{gN}(n_1n_2) = g(n_1n_2)g^{-1} = gn_1g^{-1}gn_2g^{-1} = f(n_1)f(n_2).$$

Por tanto, f es un homomorfismo. La aplicación φ pedida entonces es:

$$\begin{array}{rrcl} \varphi: & G/N & \longrightarrow & \mathrm{Aut}(N) \\ & gN & \longmapsto & f = {}^{gN}(\cdot) \end{array}$$

Ejercicio 2.6.3. Sean S y T dos $G-$conjuntos. Se define la *acción diagonal* de G sobre el producto cartesiano $S \times T$ mediante ${}^x(s,t) = ({}^xs, {}^xt)$. Demostrar que, para la acción diagonal, el estabilizador de (s,t) es la intersección de los estabilizadores de s y t en las acciones dadas.

Fijados $s \in S$ y $t \in T$, el estabilizador de (s,t) es:

$$\begin{aligned} \mathrm{Stab}_G(s,t) &= \{g \in G \mid {}^g(s,t) = (s,t)\} = \{g \in G \mid ({}^gs, {}^gt) = (s,t)\} \\ &= \{g \in G \mid {}^gs = s \wedge {}^gt = t\} = \{g \in G \mid {}^gs = s\} \cap \{g \in G \mid {}^gt = t\} \\ &= \mathrm{Stab}_G(s) \cap \mathrm{Stab}_G(t). \end{aligned}$$

Ejercicio 2.6.4. Demostrar que si G contiene un elemento x que tiene exactamente dos conjugados, entonces G tiene un subgrupo normal propio.

Observación. Considerar el centralizador de x.

Consideramos la acción por conjugación de G sobre sí mismo:

$$\begin{array}{rrcl} ac: & G \times G & \longrightarrow & G \\ & (g,h) & \longmapsto & {}^gh = ghg^{-1} \end{array}$$

Calculamos el centralizador de x:

$$C_G(\{x\}) = \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid {}^gx = x\} = \mathrm{Stab}_G(x)$$

Por tanto, $C_G(\{x\}) = \mathrm{Stab}_G(x) < G$. Veamos ahora que es normal en G. Calculemos la órbita de x:

$$\mathrm{Orb}(x) = \{y \in G \mid \exists g \in G \text{ tal que } y = {}^gx\} = \{y \in G \mid \exists g \in G \text{ tal que } y = gxg^{-1}\} = \mathrm{Cl}_G(x)$$

Como x tiene exactamente dos conjugados (él mismo y otro elemento $y \in G$), tenemos que $|\mathrm{Orb}(x)| = 2$. Por tanto:

$$[G : C_G(\{x\})] = |\mathrm{Orb}(x)| = 2 \implies C_G(\{x\}) \lhd G$$

Observación. Notemos que, aun sin saber si G es finito, la igualdad anterior tiene perfecto sentido, puesto que $|\mathrm{Orb}(x)| = 2$ y $[G : C_G(\{x\})]$ indica el número de clases en el conjunto cociente, que sabemos que es biyectivo con $\mathrm{Orb}(x)$, luego es 2.

Por tanto, $C_G(\{x\})$ es un subgrupo normal de G. Tan solo falta por comprobar que es propio.

- Si $C_G(\{x\}) = G$, entonces:

$$2 = |\operatorname{Orb}(x)| = [G : \operatorname{Stab}_G(x)] = [G : C_G(\{x\})] = 1 \implies \text{Contradicción.}$$

- Si $C_G(\{x\}) = \{1\}$, entonces:

$$2 = |\operatorname{Orb}(x)| = [G : \operatorname{Stab}_G(x)] = [G : C_G(\{x\})] = [G : \{1\}] = |G|$$

Por tanto, $G = \{1, x\}$. Calculemos el número de conjugados de 1 y de x:

$$\begin{aligned} \operatorname{Cl}_G(1) &= \{g1g^{-1} \mid g \in G\} = \{1\} \\ \operatorname{Cl}_G(x) &= \{gxg^{-1} \mid g \in G\} = \{1x1, xxx^{-1}\} = \{x\} \end{aligned}$$

Por tanto, ambos tienen un único conjugado. Por tanto, no se puede dar este caso.

Por tanto, $C_G(\{x\})$ es un subgrupo normal propio de G.

Ejercicio 2.6.5. Encontrar todos los grupos finitos que tienen exactamente dos clases de conjugación.

Sea G un grupo finito con $|G| = n$ que tiene exactamente dos clases de conjugación; a saber, $\exists x_1, x_2 \in G$ tales que $\operatorname{Cl}_G(x_1) \neq \operatorname{Cl}_G(x_2)$. Considerando la acción de G sobre sí mismo por conjugación, tenemos que:

$$\operatorname{Orb}(x) = \operatorname{Cl}_G(x) \qquad \forall x \in G$$

Como las órbitas forman una partición de G, tenemos que:

$$|G| = |\operatorname{Orb}(x_1)| + |\operatorname{Orb}(x_2)| = |\operatorname{Cl}_G(x_1)| + |\operatorname{Cl}_G(x_2)|$$

Calculamos no obstante la clase de conjugación del $1 \in G$:

$$\operatorname{Cl}_G(1) = \{g1g^{-1} \mid g \in G\} = \{gg^{-1} \mid g \in G\} = \{1\}$$

Por tanto, $|\operatorname{Cl}_G(1)| = 1$. Supongamos sin pérdida de generalidad que $1 \in \operatorname{Cl}_G(x_1)$. Entonces:

$$n = |\operatorname{Cl}_G(x_1)| + |\operatorname{Cl}_G(x_2)| = 1 + |\operatorname{Cl}_G(x_2)| \Longrightarrow |\operatorname{Cl}_G(x_2)| = n - 1$$

Por otro lado, como $|\operatorname{Cl}_G(x_2)| = [G : \operatorname{Stab}_G(x_2)]$, tenemos que $|\operatorname{Cl}_G(x_2)|$ divide a $|G|$; es decir, $(n-1) \mid n$. Por tanto, $n = 2$, y tenemos por tanto que:

$$G \cong \mathbb{Z}_2$$

Ejercicio 2.6.6. Describir explícitamente las clases de conjugación del grupo D_4.

Consideramos el grupo D_4:

$$\begin{aligned} D_4 &= \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \\ &= \{s^i r^j \mid i = 0, 1, j = 0, 1, 2, 3\} \end{aligned}$$

Tenemos que:

$$\begin{aligned}
\mathrm{Cl}_{D_4}(1) &= \{(s^i r^j)1(s^i r^j)^{-1} \mid i=0,1, j=0,1,2,3\} = \{1\}\\
\mathrm{Cl}_{D_4}(r) &= \{(s^i r^j)r(s^i r^j)^{-1} \mid i=0,1, j=0,1,2,3\} = \{s^i r^j\ r\ r^{-j} s^{-i} \mid i=0,1, j=0,1,2,3\}\\
&= \{s^i r s^i \mid i=0,1\} = \{r, r^3\} = \mathrm{Cl}_{D_4}(r^3)\\
\mathrm{Cl}_{D_4}(r^2) &= \{(s^i r^j)r^2(s^i r^j)^{-1} \mid i=0,1, j=0,1,2,3\} = \{s^i r^j\ r^2\ r^{-j} s^{-i} \mid i=0,1, j=0,1,2,3\}\\
&= \{s^i r^2 s^{-i} \mid i=0,1\} = \{r^2\}\\
\mathrm{Cl}_{D_4}(s) &= \{(s^i r^j)s(s^i r^j)^{-1} \mid i=0,1, j=0,1,2,3\} = \{s^i r^j\ s\ r^{-j} s^{-i} \mid i=0,1, j=0,1,2,3\}
\end{aligned}$$

Este último no es tan sencillo, puesto que r y s no conmutan. Calculamos en primer lugar para $s=0$, sabiendo que las clases de conjugación son cerradas para inversos.

$$\begin{aligned}
r\ s\ r^{-1} &= r\ s\ r^3 = sr^6 = sr^2 \in \mathrm{Cl}_{D_4}(s)\\
r^2\ s\ r^{-2} &= r^2\ s\ r^2 = sr^6 r^2 = s \in \mathrm{Cl}_{D_4}(s)\\
r^3\ s\ r^{-3} &= r^3\ s\ r = sr^9 r = sr^2 \in \mathrm{Cl}_{D_4}(s)
\end{aligned}$$

Por otro lado, para $s=1$, tenemos que:

$$s\ s\ s = s \qquad \text{y } s\ sr^2\ s = r^2 s = sr^6 = sr^2$$

Por tanto, $\mathrm{Cl}_{D_4}(s) = \{s, sr^2\} = \mathrm{Cl}_{D_4}(sr^2)$. Tan solo queda por tanto calcular la clase de conjugación de sr y de sr^3.

$$r\ sr\ r^{-1} = r\ sr\ r^3 = rs = sr^3 \in \mathrm{Cl}_{D_4}(sr)$$

Por tanto, tenemos que $\mathrm{Cl}_{D_4}(sr) = \mathrm{Cl}_{D_4}(sr^3)$. Como las clases de conjugación forman una partición de D_4, tenemos que:

$$\begin{aligned}
\mathrm{Cl}_{D_4}(1) &= \{1\}\\
\mathrm{Cl}_{D_4}(r) &= \{r, r^3\}\\
\mathrm{Cl}_{D_4}(r^2) &= \{r^2\}\\
\mathrm{Cl}_{D_4}(s) &= \{s, sr^2\}\\
\mathrm{Cl}_{D_4}(sr) &= \{sr, sr^3\}
\end{aligned}$$

Ejercicio 2.6.7. Se dice que la acción de un grupo finito G sobre un conjunto X es *transitiva* si hay una sola órbita para esta acción (es decir, si para cada $x, y \in X$ existe algún $g \in G$ tal que ${}^g x = y$). Demostrar que si G actúa transitivamente sobre un conjunto X con n elementos, entonces $|G|$ es un múltiplo de n.

Sea $x \in X$. Como las órbitas forman una partición de X y hay una única órbita, tenemos que:

$$n = |X| = |\operatorname{Orb}(x)|$$

Como además tenemos que $|\operatorname{Orb}(x)| = [G : \mathrm{Stab}_G(x)]$, tenemos que:

$$|G| = n \cdot |\mathrm{Stab}_G(x)|$$

Por tanto, $|G|$ es un múltiplo de n.

Ejercicio 2.6.8. Un subgrupo $G \leqslant S_n$ se dice *transitivo* si la acción de G sobre $\{1, 2, \ldots, n\}$ es transitiva. Encontrar todos los subgrupos transitivos de S_3 y S_4.

1. S_3.

   Consideramos la acción natural de S_3 sobre $\{1, 2, 3\}$ dada por:

   $$\begin{array}{rrcl} ac: & S_3 \times \{1,2,3\} & \longrightarrow & \{1,2,3\} \\ & (\sigma, i) & \longmapsto & {}^\sigma i = \sigma(i) \end{array}$$

   Consideramos ahora la restricción de la acción a $G \leqslant S_3$, que sigue siendo una acción. Buscamos ahora los subgrupos transitivos $G \leqslant S_3$. En primer lugar, por el Ejercicio anterior, sabemos que $|G|$ es un múltiplo de 3. Además, como $|S_3| = 6$, tenemos que $|G|$ divide a 6. Por tanto, $|G| \in \{3, 6\}$. Es decir, $G \in \{A_3, S_3\}$. Comprobemos si estos son transitivos.

   Dados $x, y \in \{1, 2, 3\}$ distintos, consideramos el tercer elemento $z \in \{1, 2, 3\}$. Sea ahora $\sigma = (x\ y\ z) \in S_3 \cap A_3$. Entonces:

   $${}^\sigma x = y$$

   Entonces, S_3 y A_3 son transitivos. Por tanto, los únicos subgrupos transitivos de S_3 son S_3 y A_3.

2. S_4.

   Consideramos la acción natural de S_4 sobre $\{1, 2, 3, 4\}$ dada por:

   $$\begin{array}{rrcl} ac: & S_4 \times \{1,2,3,4\} & \longrightarrow & \{1,2,3,4\} \\ & (\sigma, i) & \longmapsto & {}^\sigma i = \sigma(i) \end{array}$$

   Consideramos ahora la restricción de la acción a $G \leqslant S_4$, que sigue siendo una acción. Buscamos ahora los subgrupos transitivos $G \leqslant S_4$. En primer lugar, por el Ejercicio anterior, sabemos que $|G|$ es un múltiplo de 4. Además, como $|S_4| = 24$, tenemos que $|G|$ divide a 24. Por tanto, $|G| \in \{4, 8, 12, 24\}$.

   - Si $|G| = 24$, entonces $G = S_4$. Dados por tanto $x, y \in \{1, 2, 3, 4\}$ distintos, consideramos un tercer elemento $z \in \{1, 2, 3, 4\} \setminus \{x, y\}$. Entonces, tomando $\sigma = (x\ y\ z) \in S_4$:

     $${}^\sigma x = y$$

     Entonces, S_4 es transitivo.
   - Si $|G| = 12$, entonces $G = A_4$. Empleando el mismo razonamiento que en el caso anterior, tenemos que $\sigma \in A_4$ y, por tanto, ${}^\sigma x = y$. Entonces, A_4 es transitivo.
   - Si $|G| = 8$, entonces es un $2-$subgrupo de Sylow de S_4. Calculemos cuántos $2-$subgrupos de Sylow de S_4 hay. Como $|S_4| = 24 = 2^3 \cdot 3$, notando por n_2 al número de $2-$subgrupos de Sylow de S_4, por el Segundo Teorema de Sylow tenemos que:

     $$n_2 \equiv 1 \mod 2 \qquad \land \qquad n_2 \mid 3$$

Por tanto, puede ser $n_2 = 1$ o $n_2 = 3$. Puesto que S_4 no contiene subgrupos de orden 8 normales, tenemos que $n_2 = 3$. Por tanto, hay tres subgrupos de orden 8 en S_4. Probando, llegamos a que estos son:

- $\langle(1\ 2\ 3\ 4),(1\ 3)\rangle$.
  Sea $a = (1\ 2\ 3\ 4)$ y $b = (1\ 3)$. Entonces, tenemos que:
  $$\begin{aligned} ab &= (1\ 2\ 3\ 4)(1\ 3) = (1\ 4)(2\ 3) \\ ba^3 &= (1\ 3)(1\ 2\ 3\ 4)^3 = (1\ 3)(1\ 4\ 3\ 2) = (1\ 4)(2\ 3) \end{aligned}$$
  Por tanto, $ab = ba^3$. Por el Teorema de Dyck, este grupo es isomorfo a D_4, luego es de orden 8. Veamos si es transitivo. Para ello, vemos que:
  $$a^0(1) = 1 \qquad a^1(1) = 2 \qquad a^2(1) = 3 \qquad a^3(1) = 4$$
  Por tanto, $\mathrm{Orb}(1) = \{1, 2, 3, 4\}$. Por tanto, como $\mathrm{Orb}(x)$ es una partición de $\{1, 2, 3, 4\}$, tenemos que la única órbita es $\{1, 2, 3, 4\}$. Por tanto, es transitivo.
- $\langle(1\ 3\ 2\ 4),(1\ 2)\rangle$.
  Sea $a = (1\ 2\ 3\ 4)$ y $b = (1\ 2)$. Entonces, tenemos que:
  $$\begin{aligned} ab &= (1\ 3\ 2\ 4)(1\ 2) = (1\ 4)(2\ 3) \\ ba^3 &= (1\ 2)(1\ 3\ 2\ 4)^3 = (1\ 2)(1\ 4\ 2\ 3) = (1\ 4)(2\ 3) \end{aligned}$$
  Por tanto, $ab = ba^3$. Por el Teorema de Dyck, este grupo es isomorfo a D_4, luego es de orden 8. Veamos si es transitivo. Para ello, vemos que:
  $$a^0(1) = 1 \qquad a^1(1) = 3 \qquad a^2(1) = 2 \qquad a^3(1) = 4$$
  Por tanto, $\mathrm{Orb}(1) = \{1, 2, 3, 4\}$. Por tanto, como $\mathrm{Orb}(x)$ es una partición de $\{1, 2, 3, 4\}$, tenemos que la única órbita es $\{1, 2, 3, 4\}$. Por tanto, es transitivo.
- $\langle(1\ 2\ 3\ 4),(2\ 4)\rangle$.
  Sea $a = (1\ 2\ 3\ 4)$ y $b = (2\ 4)$. Entonces, tenemos que:
  $$\begin{aligned} ab &= (1\ 2\ 3\ 4)(2\ 4) = (1\ 2)(3\ 4) \\ ba^3 &= (2\ 4)(1\ 2\ 3\ 4)^3 = (2\ 4)(1\ 4\ 3\ 2) = (1\ 2)(3\ 4) \end{aligned}$$
  Por tanto, $ab = ba^3$. Por el Teorema de Dyck, este grupo es isomorfo a D_4, luego es de orden 8. Veamos si es transitivo. Para ello, vemos que:
  $$a^0(1) = 1 \qquad a^1(1) = 2 \qquad a^2(1) = 3 \qquad a^3(1) = 4$$
  Por tanto, $\mathrm{Orb}(1) = \{1, 2, 3, 4\}$. Por tanto, como $\mathrm{Orb}(x)$ es una partición de $\{1, 2, 3, 4\}$, tenemos que la única órbita es $\{1, 2, 3, 4\}$. Por tanto, es transitivo.

- Si $|G| = 4$, entonces es cíclico o isomorfo a V.

- Sea $G \cong \mathbb{Z}_4$, y sea $a \in G$ un generador. Entonces, por ser a una biyección en $\{1,2,3,4\}$, tenemos que:

$$\{a^0(1), a^1(1), a^2(1), a^3(1)\} = \{1,2,3,4\}$$

Por tanto, $\mathrm{Orb}(1) = \{1,2,3,4\}$. Por tanto, como $\mathrm{Orb}(x)$ es una partición de $\{1,2,3,4\}$, tenemos que la única órbita es $\{1,2,3,4\}$. Por tanto, es transitivo.

- Sea $G \cong V$. Entonces, está formado por la identidad y 3 elementos de orden 2 de forma que el producto de dos de ellos es el tercero. Los elementos de orden 2 son transposiciones o productos de transposiciones. Como es de orden 4, ha de generarse con dos elementos.

  - Si G está generado por dos productos de transposiciones disjuntas, entonces $G = V$. Veamos sí es transitivo. Sean $i, j \in \{1,2,3,4\}$ distintos. Entonces, sean $k, l \in \{1,2,3,4\} \setminus \{i, j\}$ distintos, de forma que $(i\ j)(k\ l) \in G$. Entonces:

  $$^{(i\ j)(k\ l)}i = j$$

  Por tanto, como j era arbitrario, tenemos que:

  $$\mathrm{Orb}(i) = \{1,2,3,4\}$$

  Por tanto, como $\mathrm{Orb}(x)$ es una partición de $\{1,2,3,4\}$, tenemos que la única órbita es $\{1,2,3,4\}$. Por tanto, es transitivo.

  - Si G está generado por dos transposiciones no disjuntas, entonces $\exists i, j, k \in \{1,2,3,4\}$ distintos tales que:

  $$G = \langle (i\ j), (i\ k) \rangle$$

  Entonces:

  $$(i\ j)(i\ k) = (i\ k\ j)$$

  Por tanto, contendría un elemento de orden 3, que no puede ser, puesto que G es de orden 4. Por tanto, no se puede dar este caso.

  - Si G está generado por dos transposiciones disjuntas, entonces $\exists i, j, k, l \in \{1,2,3,4\}$ distintos tales que:

  $$G = \langle (i\ j), (k\ l) \rangle$$

  Entonces, tenemos que:

  $$G = \langle (i\ j), (k\ l) \rangle = \{1, (i\ j), (k\ l), (i\ j)(k\ l)\}$$

  En este caso, $\mathrm{Orb}(i) = \{1, i, j\} \neq \{1,2,3,4\}$. Por tanto, no es transitivo.

  - Si G está generado por una transposición y un producto de transposiciones disjuntas, caben dos casos:

- ◇ $G = \langle (i\ j), (i\ j)(k\ l) \rangle$, donde $i, j, k, l \in \{1, 2, 3, 4\}$ son distintos. Entonces:
$$(i\ j)(i\ j)(k\ l) = (k\ l)$$
Por tanto, $G = \langle (i\ j), (k\ l) \rangle$, que es un caso ya visto.
- ◇ $G = \langle (i\ j), (i\ k)(j\ l) \rangle$, donde $i, j, k, l \in \{1, 2, 3, 4\}$ son distintos. Entonces:
$$(i\ j)(i\ k)(j\ l) = (i\ k\ j\ l)$$
No obstante, este elemento es de orden 4, por lo que no puede ser, puesto que G sería cíclico. Por tanto, no se puede dar este caso.

Como hemos visto, los únicos subgrupos transitivos de S_4 son:

- S_4.
- A_4.
- Los tres subgrupos de orden 8 isomorfos a D_4:
  - $\langle (1\ 2\ 3\ 4), (1\ 3) \rangle$.
  - $\langle (1\ 3\ 2\ 4), (1\ 2) \rangle$.
  - $\langle (1\ 2\ 3\ 4), (2\ 4) \rangle$.
- Los grupos cíclicos de orden 4 y V.

Ejercicio 2.6.9. Sea $n \in \mathbb{N}$. Una *partición* de n es una sucesión no decreciente de enteros positivos cuya suma es n. Dada una permutación $\sigma \in S_n$, la descomposición en ciclos disjuntos (incluyendo los ciclos de longitud 1) de $\sigma = \gamma_1\gamma_2 \cdots \gamma_r$ determina una partición $n_1, n_2, \dots, n_r$ de n donde cada n_i es la longitud del ciclo γ_i. Dos permutaciones en S_n se dice que son del mismo tipo si determinan la misma partición de n. Demostrar:

1. Dos elementos de S_n son conjugados si y solo si son del mismo tipo.

$\Longrightarrow$) Sean $\sigma, \tau \in S_n$ dos elementos conjugados; es decir, $\exists \gamma \in S_n$ tal que $\gamma\sigma\gamma^{-1} = \tau$. Consideramos ahora la descomposición en ciclos disjuntos (incluyendo los de longitud 1) de σ:
$$\sigma = \sigma_1 \cdots \sigma_r$$
Por tanto, tenemos que:
$$\tau = \gamma\sigma\gamma^{-1} = (\gamma\sigma_1\gamma^{-1}) \cdots (\gamma\sigma_r\gamma^{-1})$$
Además, sabemos que la longitud de σ_i coincide con la de $\gamma\sigma_i\gamma^{-1}$ para todo $i \in \{1, \dots, r\}$. Por tanto, τ y γ determinan la misma partición y por tanto son del mismo tipo.

$\Longleftarrow$) Sean $\sigma, \tau \in S_n$ dos elementos del mismo tipo; y sea $n_1, \dots, n_r$ la partición de n que determinan. Consideramos por tanto ambas particiones en ciclos disjuntos (incluyendo los ciclos de longitud uno):
$$\sigma = \sigma_1 \cdots \sigma_r = (a_{11}\ a_{12} \cdots a_{1n_1})(a_{21}\ a_{22} \cdots a_{2n_2}) \cdots (a_{r1}\ a_{r2} \cdots a_{rn_r})$$
$$\tau = \tau_1 \cdots \tau_r = (b_{11}\ b_{12} \cdots b_{1n_1})(b_{21}\ b_{22} \cdots b_{2n_2}) \cdots (b_{r1}\ b_{r2} \cdots b_{rn_r})$$

Consideramos ahora $\gamma \in S_n$ cuya representación matricial es:

$$\gamma = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n_1} & \cdots & a_{r1} & a_{r2} & \cdots & a_{rn_r} \\ b_{11} & b_{12} & \cdots & b_{1n_1} & \cdots & b_{r1} & b_{r2} & \cdots & b_{rn_r} \end{pmatrix}$$

Entonces, tenemos que:

$$\begin{aligned} \gamma\sigma\gamma^{-1} &= \gamma(\sigma_1 \cdots \sigma_r)\gamma^{-1} = \gamma\sigma_1 \cdots \gamma\sigma_r\gamma^{-1} \\ &= (\gamma\sigma_1\gamma^{-1})(\gamma\sigma_2\gamma^{-1}) \cdots (\gamma\sigma_r\gamma^{-1}) = \tau_1\tau_2 \cdots \tau_r = \tau \end{aligned}$$

Por tanto, σ y τ son conjugados.

2. El número de clases de conjugación de S_n es igual al número de particiones de n.

   $\leqslant$) Sean $\sigma, \tau \in S_n$ dos elementos tal que $\mathrm{Cl}_{S_n}(\sigma) \neq \mathrm{Cl}_{S_n}(\tau)$. Entonces, no son conjugados. Por tanto, no son del mismo tipo y determinan distintas particiones de n. Por tanto, el número de clases de conjugación de S_n es menor o igual al número de particiones de n.

   $\geqslant$) Veamos en primer lugar que, dada una partición de n, existe al menos un elemento de S_n que determina dicha partición. Sea $n_1, n_2, \ldots, n_r$ la partición de n. Consideramos el siguiente elemento de S_n:

   $$\sigma = (1\ 2\ \cdots\ n_1)(n_1{+}1\ n_1{+}2\ \cdots\ n_1{+}n_2)\cdots(n_1{+}\cdots{+}n_{r-1}{+}1\ n_1{+}\cdots{+}n_{r-1}{+}2\ \cdots\ n)$$

   Entonces, σ es un elemento de S_n que determina la partición $n_1, n_2, \ldots, n_r$. Por tanto, existe al menos un elemento de S_n que determina cada partición de n.

   Ahora, dados dos elementos $\sigma, \tau \in S_n$ que determinan particiones distintas de n, tenemos que σ y τ no son del mismo tipo. Por tanto, no son conjugados. Por tanto, $\mathrm{Cl}_{S_n}(\sigma) \neq \mathrm{Cl}_{S_n}(\tau)$. Por tanto, el número de clases de conjugación de S_n es mayor o igual al número de particiones de n.

   Como conclusión, tenemos que el número de clases de conjugación de S_n es igual al número de particiones de n.

Ejercicio 2.6.10. Calcular el número de clases de conjugación de S_5. Dar un representante de cada una y encontrar el orden de cada clase. Calcular el estabilizador de $(1\ 2\ 3)$ bajo la acción de conjugación de S_5 sobre sí mismo.

Por el ejercicio anterior, sabemos que hay tantas clases de conjugación como particiones de n:

Partición	Representante	Orden
1 1 1 1 1	id_5	1
1 1 1 2	(1 2)	10
1 2 2	(1 2)(3 4)	15
1 1 3	(1 2 3)	20
2 3	(1 2)(3 4 5)	20
1 4	(1 2 3 4)	30
5	(1 2 3 4 5)	24

Para calcular el orden de cada clase, usamos que:

$$|\operatorname{Cl}_{S_5}(\sigma)| = \frac{5!}{\prod\limits_{i=1}^{5} m_i! \cdot i^{m_i}}$$

donde m_i es el número de ciclos de longitud i en la descomposición en ciclos disjuntos de σ. Por tanto, tenemos que:

$$\begin{aligned}
|\operatorname{Cl}_{S_5}(id_5)| &= \frac{5!}{5! \cdot 1^5} = 1 \\
|\operatorname{Cl}_{S_5}((1\ 2))| &= \frac{5!}{3! \cdot 1^3 \cdot 1! \cdot 2^1} = \frac{120}{6 \cdot 2} = 10 \\
|\operatorname{Cl}_{S_5}((1\ 2)(3\ 4))| &= \frac{5!}{2! \cdot 2^2} = \frac{120}{2 \cdot 4} = 15 \\
|\operatorname{Cl}_{S_5}((1\ 2\ 3))| &= \frac{5!}{2! \cdot 1^2 \cdot 3^1} = \frac{120}{2 \cdot 3} = 20 \\
|\operatorname{Cl}_{S_5}((1\ 2)(3\ 4\ 5))| &= \frac{5!}{1! \cdot 1^1 \cdot 3^1 \cdot 2^1} = \frac{120}{1 \cdot 3 \cdot 2} = 20 \\
|\operatorname{Cl}_{S_5}((1\ 2\ 3\ 4))| &= \frac{5!}{1! \cdot 1^1 \cdot 4^1} = \frac{120}{1 \cdot 4} = 30 \\
|\operatorname{Cl}_{S_5}((1\ 2\ 3\ 4\ 5))| &= \frac{5!}{1! \cdot 5^1} = \frac{120}{1 \cdot 5} = 24
\end{aligned}$$

Calculamos ahora el estabilizador de $(1\ 2\ 3)$:

$$\begin{aligned}
\operatorname{Stab}_{S_5}((1\ 2\ 3)) &= \{\gamma \in S_5 \mid \gamma(1\ 2\ 3)\gamma^{-1} = (1\ 2\ 3)\} = \\
&= \{\gamma \in S_5 \mid (\gamma(1)\ \gamma(2)\ \gamma(3)) = (1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)\}
\end{aligned}$$

A simple vista, vemos que:

$$id_5,\ (4\ 5),\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 3)(4\ 5),\ (1\ 3\ 2)(4\ 5) \in \operatorname{Stab}_{S_5}((1\ 2\ 3))$$

No obstante, podría haber más. Comprobemos que no:

$$|\operatorname{Stab}_{S_5}((1\ 2\ 3))| = \frac{|S_5|}{|\operatorname{Orb}((1\ 2\ 3))|} = \frac{|S_5|}{|\operatorname{Cl}_{S_5}((1\ 2\ 3))|} = \frac{120}{20} = 6$$

Por tanto:

$$\operatorname{Stab}_{S_5}((1\ 2\ 3)) = \{id_5,\ (4\ 5),\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 3)(4\ 5),\ (1\ 3\ 2)(4\ 5)\}$$

Ejercicio 2.6.11. Sea G un grupo finito y $\Phi : G \to \operatorname{Perm}(G)$ la representación regular izquierda (que corresponde a la acción de G sobre sí mismo por traslación por la izquierda).

1. Demostrar que si x es un elemento de G de orden n y $|G| = nm$, entonces $\Phi(x)$ es un producto de $n-$ciclos. Deducir que $\Phi(x)$ es una permutación impar si y solo si el orden de x es par y el cociente del orden de G y el de x es impar.

Sea $x \in G$ con $\text{ord}(x) = n$. Entonces, $\Phi(x) \in \text{Perm}(G)$, y como $|G| = nm$, tenemos que $\Phi(x) \in S_{nm}$. Sea ahora $k \in G$. Con vistas de estudiar la descomposición de $\Phi(x)$ en ciclos disjuntos, veamos las imágenes sucesivas de k bajo $\Phi(x)$:

$$k \mapsto xk \mapsto x^2k \mapsto \cdots \mapsto x^{n-1}k \mapsto x^nk = k$$

Por tanto, k pertenece al ciclo $(k\ xk\ x^2k\ \cdots\ x^{n-1}k)$ de $\Phi(x)$. Como k era arbitrario, hemos visto que $\Phi(x)$ es producto de $n-$ciclos. Además, todos estos son trivialmente disjuntos.

Como en la representación de $\Phi(x)$ deben aparecer los nm elementos de G, tenemos que el número de ciclos de longitud n en la descomposición de $\Phi(x)$ es:

$$\frac{|G|}{n} = \frac{nm}{n} = m$$

Por tanto, $\Phi(x)$ está formada por m ciclos de longitud n disjuntos. Como una permutación es par si y solo si el número de ciclos de longitud par es par, tenemos que:

$$\varepsilon(\Phi(x)) = -1 \iff \text{el número de ciclos de longitud par es impar}$$

Como el 0 es par, al menos uno de los ciclos de longitud n ha de ser par, luego n ha de ser par. Además, como el número de ciclos de longitud n es m, tenemos que m ha de ser impar. Por tanto:

$$\varepsilon(\Phi(x)) = -1 \iff n \text{ es par y } m \text{ es impar}$$

Como $m = \dfrac{|G|}{n}$, se tiene lo pedido.

2. Demostrar que si $Im(\Phi)$ contiene una permutación impar entonces G tiene un subgrupo de índice 2.

   Supongamos que $Im(\Phi)$ contiene una permutación impar. Entonces, existe $x \in G$ tal que $\varepsilon(\Phi(x)) = -1$. Como tanto Φ como ε son homomorfismos, consideramos el homomorfismo composición:

$$\varepsilon \circ \Phi : G \to \{-1, 1\}$$

   Veamos si ese homomorfismo es sobreyectivo. Como $\varepsilon(\Phi(x)) = -1$, tenemos que:

$$(\varepsilon \circ \Phi)(x) = -1 \Longrightarrow -1 \in Im(\varepsilon \circ \Phi)$$

   Por otro lado, considerando $1 \in G$, tenemos que:

$$(\varepsilon \circ \Phi)(1) = \varepsilon(\Phi(1)) = \varepsilon(id_G) = 1$$

   Por tanto, $Im(\varepsilon \circ \Phi) = \{-1, 1\}$. Por el Primero Teorema de Isomorfía, tenemos que:

$$\frac{G}{\ker(\varepsilon \circ \Phi)} \cong Im(\varepsilon \circ \Phi) = \{-1, 1\}$$

Como G es finito, tenemos que:

$$[G : \ker(\varepsilon \circ \Phi)] = |Im(\varepsilon \circ \Phi)| = 2$$

Por tanto, $\ker(\varepsilon \circ \Phi)$ es un subgrupo de G de índice 2.

3. Demostrar que si $|G| = 2k$ con k impar, entonces G tiene un subgrupo de índice 2.

   Observación. Usar el Teorema de Cauchy para obtener un elemento de orden 2 y entonces usar los dos apartados anteriores.

   Por el Teorema de Cauchy, como $2 \mid |G|$, existe $x \in G$ tal que $\operatorname{ord}(x) = 2$. Además, como $|G| = 2k$ con k impar; y $\operatorname{ord}(x) = 2$ par, por el primer apartado, tenemos que $\Phi(x)$ es una permutación impar. Por el segundo apartado, tenemos que G tiene un subgrupo de índice 2.

Ejercicio 2.6.12. Sea G un $p-$grupo finito actuando sobre un conjunto finito X. Demostrar que

$$|X| \equiv |\operatorname{Fix}(X)| \mod p.$$

Sea G un $p-$grupo finito y sea X un conjunto finito sobre el que actúa. Como G es finito, $\exists n \in \mathbb{N}$ tal que $|G| = p^n$. En vistas de aplicar la fórmula de clases, definimos Γ como un conjunto que tiene un representante de cada órbita no unitaria de la acción de G sobre X. Entonces, tenemos que:

$$|X| = |\operatorname{Fix}(X)| + \sum_{x \in \Gamma} |\operatorname{Orb}(x)|$$

Demostrar lo pedido equivale a demostrar que:

$$X - |\operatorname{Fix}(X)| = \sum_{x \in \Gamma} |\operatorname{Orb}(x)| \equiv 0 \mod p$$

Fijado $x \in \Gamma$, tenemos que $|\operatorname{Orb}(x)| > 1$. Como $|\operatorname{Orb}(x)| = [G : \operatorname{Stab}_G(x)]$, tenemos que $|\operatorname{Orb}(x)| \mid |G| = p^n$. Uniendo ambas afirmaciones, tenemos que $|\operatorname{Orb}(x)| = p^{k_x}$ con $k_x \in \{1, \dots, n\}$.

Por tanto, $|\operatorname{Orb}(x)| \equiv 0 \mod p$ para todo $x \in \Gamma$. Por tanto, la suma de los términos de la suma es congruente a 0 módulo p. Por tanto:

$$|X| - |\operatorname{Fix}(X)| = \sum_{x \in \Gamma} |\operatorname{Orb}(x)| \equiv 0 \mod p$$

como queríamos demostrar.

Ejercicio 2.6.13. Sea G un $2-$grupo finito que actúa sobre un conjunto finito X cuya cardinalidad es un número impar. ¿Podemos afirmar que existe al menos un punto de X que queda fijo bajo la acción de G? ¿Podemos decir lo mismo si $|X|$ es par?

Por la fórmula de clases, definiendo Γ como un conjunto que tiene un representante de cada órbita no unitaria de la acción de G sobre X, tenemos que:

$$|X| = |\operatorname{Fix}(X)| + \sum_{x\in\Gamma} |\operatorname{Orb}(x)|$$

Dado $x \in \Gamma$, tenemos que $|\operatorname{Orb}(x)| = [G : \operatorname{Stab}_G(x)]$. Como G es un $2-$grupo, tenemos que $|G| = 2^k$ con $k \in \mathbb{N}$. Por tanto, $|\operatorname{Orb}(x)|$ es una potencia de 2. Además, como $x \in \Gamma$, tenemos que $|\operatorname{Orb}(x)| > 1$. Por tanto, $|\operatorname{Orb}(x)|$ es un número par para todo $x \in \Gamma$. Por tanto, la suma de los términos de la suma es par. Como $|X|$ es impar, tenemos que $|\operatorname{Fix}(X)|$ es impar. Por tanto, existe al menos un punto de X que queda fijo bajo la acción de G.

Si $|X|$ es par, entonces $|\operatorname{Fix}(X)|$ es par, pero podría ser 0. Por tanto, no podemos afirmar que existe al menos un punto de X que queda fijo bajo la acción de G.

Ejercicio 2.6.14. Sea $C_n = \langle a \mid a^n = 1\rangle$ un grupo cíclico de orden n. Describir sus subgrupos de Sylow.

Sea $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ la factorización de n en primos. Entonces, para cada $i \in \{1, \dots, m\}$, tenemos que el p_i-subgrupo de Sylow de C_n es único, puesto que C_n es cíclico luego abeliano, y por tanto sus subgrupos son normales. Por tanto, el p_i-subgrupo de Sylow de C_n es el único subgrupo de orden $p_i^{k_i}$ de C_n.

$$P_{p_i} = \left\langle a^{\left(\frac{n}{(p_i^{k_i})}\right)} \right\rangle$$

Ejercicio 2.6.15. Sea G un grupo finito y $|G| = pn$ con p primo y $p > n$. Demostrar que G contiene un subgrupo normal de orden p y que todo subgrupo de G de orden p es normal en G.

Buscamos obtener n_p. Como $p > n$, sabemos que $\operatorname{mcd}(p, n) = 1$. Por tanto, por el Teorema de Sylow, tenemos que:

$$\begin{aligned} &n_p \equiv 1 \mod p \\ &n_p \mid n \end{aligned}$$

Por tanto, $n_p \leqslant n < p$, luego $n_p = 1$. Por tanto, existe un único $p-$subgrupo de Sylow de G (de orden p), que es normal. Llamémoslo P_p, y tendrá orden $|P_p| = p$.

Sea ahora H un subgrupo de G de orden p. Entonces, este es un $p-$subgrupo de Sylow de G, luego $H = P_p$.

Ejercicio 2.6.16. Sea H un subgrupo de un grupo finito G con $[G : H] = p$ primo y p el menor primo que divide a $|G|$. Demostrar que entonces H es normal en G.

Como no sabemos si H es normal en G, no podemos considerar el grupo cociente pero sí el conjunto de las clases laterales por la izquierda de H en G, que denotamos por $G/\sim_H$. Consideramos la acción de G sobre $G/\sim_H$ por traslación por la izquierda, y consideramos su representación por permutaciones

$$\Phi : G \to \operatorname{Perm}(G/\sim_H)$$

Como $|G/\sim_H| = [G:H] = p$, tenemos que Φ es un homomorfismo de grupos entre G y S_p:

$$\Phi : G \to S_p$$

En vistas de aplicar el Primer Teorema de Isomorfía, calculamos el núcleo de Φ:

$$\begin{aligned}\ker(\Phi) &= \{g \in G \mid \Phi(g) = id_{S_p}\}\\ &= \{g \in G \mid g \cdot (aH) = (aH) \text{ para todo } a \in G\} \subset\\ &\subset \{g \in G \mid gH = H\} = \{g \in G \mid g \in H\} = H\end{aligned}$$

Por el Primer Teorema de Isomorfía, tenemos que:

$$G/\ker(\Phi) \cong Im(\Phi) \leqslant S_p$$

Por tanto, como $|S_p| = p!$ con p primo, tenemos que $|G/\ker(\Phi)|$ divide a $p!$. Por otro lado, $|G/\ker(\Phi)|$ divide a $|G|$. Como p es el menor primo que divide a $|G|$, tenemos que $|G/\ker(\Phi)| = p$. Por último, como $\ker(\Phi) \lhd G$ y $\ker(\Phi) \leqslant H$, tenemos que $\ker(\Phi) \lhd H$. Por tanto:

$$p = [G:\ker(\Phi)] = [G:H]\cdot[H:\ker(\Phi)] = p\cdot[H:\ker(\Phi)] \Longrightarrow [H:\ker(\Phi)] = 1$$

Por tanto, $|\ker(\Phi)| = |H|$. Como $\ker(\Phi) \leqslant H$, tenemos que $\ker(\Phi) = H$. Por tanto, $\ker(\Phi) = H$ es un subgrupo normal de G, concluyendo así la demostración.

Ejercicio 2.6.17. Sea p un número primo. Demostrar:

1. Todo grupo no abeliano de orden p^3 tiene un centro de orden p.

   Sea G un grupo no abeliano de orden p^3. Entonces, G es un $p-$grupo. Por ser $Z(G) < G$, tenemos que $|Z(G)| = p^k$ con $k \in \{0, 1, 2, 3\}$.

   - Por ser un $p-$grupo, $Z(G)$ es no trivial, luego $k > 0$.
   - Por no ser abeliano, $Z(G) \neq G$, luego $k < 3$.
   - Por ser un $p-$grupo, $|Z(G)| \neq p^{3-1}$, luego $k < 2$.

   Por tanto, $k = 1$. Por tanto, $|Z(G)| = p$.

2. Existen únicamente dos grupos no isomorfos de orden p^2.

   Todo grupo de orden p^2 es abeliano. Consideramos el grupo cíclico C_{p^2} y el grupo directo $C_p \times C_p$. Estos son de orden p^2 y no son isomorfos entre sí, puesto que uno es cíclico y el otro no ($\text{mcd}(p,p) = p \neq 1$).

   Sea ahora G otro grupo de orden p^2 que no es isomorfo a los anteriores. Por el Teorema de Cauchy, existe $x \in G$ tal que $\text{ord}(x) = p$. Sea también $y \in G \setminus \langle x \rangle$ otro elemento de G (que es posible puesto que $|G| = p^2 > p$). Consideramos:

   $$H = \langle x \rangle \qquad K = \langle y \rangle$$

   - Como $y \in G$, entonces $\text{ord}(y) \in \{1, p, p^2\}$. Como $y \notin H$, tenemos que $\text{ord}(y) \neq 1$. Como G no es cíclico, tenemos que $\text{ord}(y) \neq p^2$. Por tanto, $\text{ord}(y) = p$.

- Como $\mathrm{ord}(x) = p$ y $\mathrm{ord}(y) = p$, supongamos que $\exists g \in \langle x\rangle \cap \langle y\rangle$, $g \neq 1$. Entonces, como todos los elementos distintos de 1 de un grupo cíclico de orden primo son generadores, tenemos que:

$$\langle g\rangle = \langle x\rangle = \langle y\rangle$$

Esto no obstante contradice la elección de $y \in G \setminus \langle x\rangle$. Por tanto, $\langle x\rangle \cap \langle y\rangle = \{1\}$.

- Como G es abeliano, tenemos que $H, K \lhd G$.
- Veamos que $HK = G$. Por el Segundo Teorema de Isomorfía, tenemos que:

$$\frac{H}{H\cap K} \cong \frac{HK}{K} \Longrightarrow |HK| = \frac{|H|}{|H\cap K|}\cdot |K| = |H|\cdot|K| = p\cdot p = p^2$$

Por tanto, $HK < G$ y $|HK| = p^2 = |G|$, luego $HK = G$.

Por la caracterización de producto directo interno, tenemos que:

$$G \cong H\times K \cong C_p\times C_p$$

Por tanto, G es isomorfo a $C_p\times C_p$, luego G es isomorfo a uno de los grupos que hemos considerado antes.

3. Todo subgrupo normal de orden p de un $p-$grupo finito está contenido en el centro.

Sea G un $p-$grupo finito y sea $H \lhd G$ un subgrupo normal de orden p. Como es de orden p, $\exists h \in H$ con $\mathrm{ord}(h) = p$, de forma que:

$$H = \langle h\rangle$$

Por tanto, para ver que $H \leqslant Z(G)$, bastará con ver que $h \in Z(G)$. Fijado $g \in G$, buscamos ver que $gh = hg$. Como $H \lhd G$, tenemos que:

$$ghg^{-1} \in H \Longrightarrow \exists k \in \{0,\dots,p-1\} \text{ tal que } ghg^{-1} = h^k$$

Si demostramos que $k = 1$, lo tendremos.

- Supongamos $k = 0$. Entonces, $ghg^{-1} = 1$, luego $gh = g$ y $h = 1$, luego $\mathrm{ord}(h) = 1 \neq p$, lo cual es una contradicción.
- Supongamos $k > 1$. Como $g \in G$ y G es un $p-$grupo, $\exists m \in \mathbb{N}$ tal que $\mathrm{ord}(g) = p^m$. Entonces, tenemos que:

Ejercicio 2.6.18. Demostrar que si $N \lhd G$ y N y G/N son $p-$grupos entonces G es un $p-$grupo.

Para demostrar que G es un $p-$grupo, puesto que G no tiene por qué ser finito, hemos de comprobar que el orden de todo elemento de $G\setminus\{1\}$ es una potencia de p. Sea $g \in G\setminus\{1\}$ un elemento cualquiera. Distinguimos dos casos:

- Si $g \in N$, entonces como N es un $p-$grupo y $g \neq 1$, tenemos que $\operatorname{ord}(g)$ es una potencia de p.
- Si $g \notin N$, entonces como G/N es un $p-$grupo y $gN \neq N$, tenemos que $\operatorname{ord}(gN)$ es una potencia de p. Por tanto, existe $k \in \mathbb{N}$ tal que:

$$(gN)^{p^k} = N \Longrightarrow g^{p^k}N = N \Longrightarrow g^{p^k} \in N$$

Si $g^{p^k} = 1$, entonces $\operatorname{ord}(g)$ divide a p^k, y como $g \neq 1$, tenemos que $\operatorname{ord}(g)$ es una potencia de p. Si $g^{p^k} \neq 1$, entonces como N es un $p-$grupo, tenemos que $\operatorname{ord}(g^{p^k})$ es una potencia de p. Por tanto, $\exists k' \in \mathbb{N}$ tal que:

$$\left(g^{p^k}\right)^{p^{k'}} = 1 \Longrightarrow g^{p^{k+k'}} = 1$$

Por tanto, $\operatorname{ord}(g)$ divide a $p^{k+k'}$, luego $\operatorname{ord}(g)$ es una potencia de p.

Ejercicio 2.6.19. Si G es un grupo de orden p^n, p primo, demostrar que para todo k, $0 \leqslant k \leqslant n$, existe un subgrupo normal de G de orden p^k.

Demostramos por inducción sobre n.

- Para $n = 1$, tenemos que $|G| = p$, luego G es cíclico, luego abeliano, luego todo subgrupo de G es normal.
- Supongamos que para todo $p-$grupo de orden p^m, con $m < n$, se cumple que para todo k, $0 \leqslant k \leqslant m$, existe un subgrupo normal de orden p^k.

Sea G un $p-$grupo de orden p^n, y consideramos su centro $Z(G)$. Como $Z(G) \neq \{1\}$ y $Z(G) < G$, tenemos que $|Z(G)| = p^k$ con $k \in \{1, \dots, n\}$. Como $p \mid |Z(G)|$, por el Teorema de Cauchy, existe $N < Z(G)$ tal que $|N| = p$. Como $Z(G) \lhd G$, se tiene que $N \lhd G$, lo que nos permite considerar:

$$|G/N| = \frac{|G|}{|N|} = \frac{p^n}{p} = p^{n-1}$$

Por tanto, G/N es un $p-$grupo de orden p^{n-1}. Por la hipótesis de inducción, tenemos que para todo k, $0 \leqslant k \leqslant n-1$, existe $L_k \lhd G/N$ tal que $|L_k| = p^k$. Por el Tercer Teorema de Isomorfía, tenemos que, para cada $k \in \{0, \dots, n-1\}$, existe $H_k < G$, con $N \lhd H_k \lhd G$, tal que $L_k = H_k/N$. Por tanto, tenemos que:

$$|H_k| = |H_k/N| \cdot |N| = |L_k| \cdot |N| = p^k \cdot p = p^{k+1}$$

Por tanto, para cada $k' \in \{1, \dots, n\}$, existe $W_{k'} = H_{k'-1}$ tal que $|W_{k'}| = p^{k'}$ y $W_{k'} \lhd G$. Falta ver el resultado para $k = 0$, pero esto es directo tomando $W_0 = \{1\}$, que es un subgrupo normal de G de orden $1 = p^0$. Por tanto, hemos visto que para todo $k \in \{0, \dots, n\}$, existe un subgrupo normal de G de orden p^k.

Por tanto, hemos demostrado que para todo $p-$grupo G de orden p^n, con p primo, y para todo $k \in \{0, \dots, n\}$, existe un subgrupo normal de G de orden p^k.

Ejercicio 2.6.20. Hallar todos los subgrupos de Sylow de los grupos S_3 y S_4.

Observación. Para los $2-$subgrupos de Sylow de S_4, observar primero que todos deben contener al subgrupo de Klein V, y, al menos, una trasposición τ, y que como consecuencia se pueden obtener como producto de V por el grupo cíclico generado por τ.

1. S_3.

   Sabemos que $|S_3| = 6 = 2 \cdot 3$. Calculamos los $p-$subgrupos de Sylow, con $p \in \{2, 3\}$.

   - $2-$subgrupo de Sylow.
     Por el Segundo Teorema de Sylow, tenemos que:
     $$n_2 \equiv 1 \mod 2 \qquad n_2 \mid 3$$
     Por tanto, $n_2 \in \{1, 3\}$.

   Como hay más de un grupo de orden 2 en S_3, tenemos que $n_2 = 3$. Estos grupos son:
   $$\langle (1\ 2) \rangle, \quad \langle (1\ 3) \rangle, \quad \langle (2\ 3) \rangle$$

   - $3-$subgrupo de Sylow.
     Por el Segundo Teorema de Sylow, tenemos que:
     $$n_3 \equiv 1 \mod 3 \qquad n_3 \mid 2$$
     Por tanto, $n_3 = 1$. El único $3-$subgrupo de Sylow de S_3 es:
     $$P_3 = \langle (1\ 2\ 3) \rangle$$

2. S_4.

   Sabemos que $|S_4| = 24 = 2^3 \cdot 3$. Calculamos los $p-$subgrupos de Sylow, con $p \in \{2, 3\}$.

   - $3-$subgrupo de Sylow.
     Por el Segundo Teorema de Sylow, tenemos que:
     $$n_3 \equiv 1 \mod 3 \qquad n_3 \mid 8$$
     Por tanto, $n_3 \in \{1, 4\}$. Como hay más de un grupo de orden 3 en S_4, tenemos que $n_3 = 4$. Estos grupos son:
     $$\langle (1\ 2\ 3) \rangle, \quad \langle (1\ 2\ 4) \rangle, \quad \langle (1\ 3\ 4) \rangle, \quad \langle (2\ 3\ 4) \rangle$$

   - $2-$subgrupo de Sylow.
     Por el Segundo Teorema de Sylow, tenemos que:
     $$n_2 \equiv 1 \mod 2 \qquad n_2 \mid 3$$
     Por tanto, $n_2 \in \{1, 3\}$. En el Ejercicio 2.6.8, vimos que estos grupos son:

- $\langle(1\ 2\ 3\ 4), (1\ 3)\rangle$.
- $\langle(1\ 3\ 2\ 4), (1\ 2)\rangle$.
- $\langle(1\ 2\ 3\ 4), (2\ 4)\rangle$.

Ejercicio 2.6.21. Hallar todos los subgrupos de Sylow de los grupos $\mathbb{Z}_{600}$, Q_2, D_5, D_6, A_4, A_5, S_5.

1. $\mathbb{Z}_{600}$.

   Tenemos $600 = 2^3 \cdot 3 \cdot 5^2$. Calculamos los $p-$subgrupos de Sylow, para valores de $p \in \{2, 3, 5\}$. Como $\mathbb{Z}_{600}$ es cíclico, en particular es abeliano, y por tanto sus subgrupos son normales, luego son únicos.

   - $2-$subgrupo de Sylow.
     Es un grupo cíclico de orden 8, luego es isomorfo a $\mathbb{Z}_8$. De hecho:
     $$P_2 = \langle 3 \cdot 5^2\rangle = \langle 75\rangle \cong \mathbb{Z}_8$$
   - $3-$subgrupo de Sylow.
     Es un grupo cíclico de orden 3, luego es isomorfo a $\mathbb{Z}_3$. De hecho:
     $$P_3 = \langle 2^3 \cdot 5^2\rangle = \langle 200\rangle \cong \mathbb{Z}_3$$
   - $5-$subgrupo de Sylow.
     Es un grupo cíclico de orden 25, luego es isomorfo a $\mathbb{Z}_{25}$. De hecho:
     $$P_5 = \langle 2^3 \cdot 3\rangle = \langle 24\rangle \cong \mathbb{Z}_{25}$$

2. Q_2.

   Sabemos que $|Q_2| = 8 = 2^3$. Además, como $Q_2 \lhd Q_2$, el único $2-$subgrupo de Sylow de Q_2 es Q_2 mismo. Por tanto, el único subgrupo de Sylow de Q_2 es Q_2.

3. D_5.

   Sabemos que $|D_5| = 10 = 2 \cdot 5$. Calculamos los $p-$subgrupos de Sylow, con $p \in \{2, 5\}$.

   - $2-$subgrupos de Sylow.
     Por el Segundo Teorema de Sylow, tenemos que:
     $$n_2 \equiv 1 \mod 2 \qquad n_2 \mid 5$$
     Por tanto, $n_2 \in \{1, 5\}$. Se tiene que $n_2 = 5$, puesto que hay 5 elementos de orden 2 en D_5. Estos grupos son:
     $$\langle sr^i\rangle \qquad \forall i \in \{0, 1, 2, 3, 4\}$$
   - $5-$subgrupo de Sylow.
     Sea H un $5-$subgrupo de Sylow de D_5. Como $|D_5| = 10$ y $|H| = 5$, tenemos que $[D_5 : H] = 2$, luego H es normal en D_5, luego es el único $5-$subgrupo de Sylow de D_5. Como además 5 es primo, H es cíclico. Por tanto:
     $$H = \langle r\rangle$$

4. D_6.

   Sabemos que $|D_6| = 12 = 2^2 \cdot 3$. Calculamos los $p-$subgrupos de Sylow, con $p \in \{2, 3\}$.

   - $2-$subgrupos de Sylow.

     Por el Segundo Teorema de Sylow, tenemos que:

     $$n_2 \equiv 1 \mod 2 \qquad n_2 \mid 3$$

     Por tanto, $n_2 \in \{1, 3\}$. Como no hay elementos de orden 4 en D_6, no puede ser cíclico. Por tanto, ha de estar generado por más de un elemento de orden 2:

     $$\begin{aligned} \langle r^3, s\rangle &= \{1, r^3, s, sr^3\} \\ \langle r^3, sr\rangle &= \{1, r^3, sr, sr^4\} \\ \langle r^3, sr^2\rangle &= \{1, r^3, sr, sr^5\} \end{aligned}$$

     Como estos son tres $2-$subgrupos de Sylow de D_6, estos son los únicos.

   - $3-$subgrupos de Sylow.

     Por el Segundo Teorema de Sylow, tenemos que:

     $$n_3 \equiv 1 \mod 3 \qquad n_3 \mid 4$$

     Por tanto, $n_3 \in \{1, 4\}$. Como además los subgrupos son de orden 3, son cíclicos, luego buscamos elementos de orden 3 en D_6. Todos los elementos de la forma sr^i con $i \in \{0, \dots, 5\}$ tienen orden 2. Por tanto, el único $3-$subgrupo es:

     $$\langle r^2\rangle$$

5. A_4.

   Sabemos que $|A_4| = 12 = 2^2 \cdot 3$. Calculamos los $p-$subgrupos de Sylow, con $p \in \{2, 3\}$.

   - $2-$subgrupos de Sylow.

     Como V es un $2-$subgrupo de Sylow de A_4 y $V \lhd A_4$, tenemos que V es el único $2-$subgrupo de Sylow de A_4.

   - $3-$subgrupos de Sylow.

     Por el Segundo Teorema de Sylow, tenemos que:

     $$n_3 \equiv 1 \mod 3 \qquad n_3 \mid 4$$

     Por tanto, $n_3 \in \{1, 4\}$. Como A_4 tiene 8 elementos de orden 3, tenemos que $n_3 = 4$. Por tanto, los $3-$subgrupos de Sylow son:

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

6. A_5.

   Sabemos que $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. Calculamos los $p-$subgrupos de Sylow, con $p \in \{2, 3, 5\}$.

   - $2-$subgrupos de Sylow.
     Por el Segundo Teorema de Sylow, tenemos que:
     $$n_2 \equiv 1 \mod 2 \qquad n_2 \mid 15$$
     Por tanto, $n_2 \in \{1, 3, 5, 15\}$. En A_5 no hay elementos de orden 4, y los únicos de orden 2 son lo productos de transposiciones. Veamos cuántas hay:
     $$|\operatorname{Cl}_{A_5}((1\ 2)(3\ 4))| = \frac{5!}{2^2 \cdot 2!} = \frac{120}{8} = 15$$
     Por tanto, como mínimo habrá estos 5 $2-$subgrupos de Sylow:
     $$\begin{aligned}
     \langle (1\ 2)(3\ 4),\ (1\ 3)(2\ 4) \rangle &= \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \\
     \langle (1\ 2)(3\ 5),\ (1\ 3)(2\ 5) \rangle &= \{1, (1\ 2)(3\ 5), (1\ 3)(2\ 5), (1\ 5)(2\ 3)\} \\
     \langle (1\ 2)(4\ 5),\ (1\ 4)(2\ 5) \rangle &= \{1, (1\ 2)(4\ 5), (1\ 4)(2\ 5), (1\ 5)(2\ 4)\} \\
     \langle (1\ 3)(4\ 5),\ (1\ 4)(3\ 5) \rangle &= \{1, (1\ 3)(4\ 5), (1\ 4)(3\ 5), (1\ 5)(2\ 3)\} \\
     \langle (2\ 3)(4\ 5),\ (2\ 4)(3\ 5) \rangle &= \{1, (2\ 3)(4\ 5), (2\ 4)(3\ 5), (2\ 5)(3\ 4)\}
     \end{aligned}$$
     Se comprueba que, efectivamente, estos son 5 $2-$subgrupos de Sylow de A_5. Por tanto, $n_2 = 5$.

   - $3-$subgrupos de Sylow. Por el Segundo Teorema de Sylow, tenemos que:
     $$n_3 \equiv 1 \mod 3 \qquad n_3 \mid 20$$
     Por tanto, $n_3 \in \{1, 4, 10\}$. Veamos cuántos elementos de orden 3 hay en A_5:
     $$|\operatorname{Cl}_{A_5}((1\ 2\ 3))| = \frac{5!}{3! \cdot 2} = 20$$
     Por tanto, hay 10 $3-$subgrupos de Sylow, que son:
     $$\begin{aligned}
     \langle (1\ 2\ 3) \rangle &= \{1, (1\ 2\ 3), (1\ 3\ 2)\} \\
     \langle (1\ 2\ 4) \rangle &= \{1, (1\ 2\ 4), (1\ 4\ 2)\} \\
     \langle (1\ 2\ 5) \rangle &= \{1, (1\ 2\ 5), (1\ 5\ 2)\} \\
     \langle (1\ 3\ 4) \rangle &= \{1, (1\ 3\ 4), (1\ 4\ 3)\} \\
     \langle (1\ 3\ 5) \rangle &= \{1, (1\ 3\ 5), (1\ 5\ 3)\} \\
     \langle (1\ 4\ 5) \rangle &= \{1, (1\ 4\ 5), (1\ 5\ 4)\} \\
     \langle (2\ 3\ 4) \rangle &= \{1, (2\ 3\ 4), (2\ 4\ 3)\} \\
     \langle (2\ 3\ 5) \rangle &= \{1, (2\ 3\ 5), (2\ 5\ 3)\} \\
     \langle (2\ 4\ 5) \rangle &= \{1, (2\ 4\ 5), (2\ 5\ 4)\} \\
     \langle (3\ 4\ 5) \rangle &= \{1, (3\ 4\ 5), (3\ 5\ 4)\}
     \end{aligned}$$

- $5-$subgrupos de Sylow.

  Por el Segundo Teorema de Sylow, tenemos que:

  $$n_5 \equiv 1 \mod 5 \qquad n_5 \mid 12$$

  Por tanto, $n_5 \in \{1, 6\}$. Veamos cuántos elementos de orden 5 hay en A_5:

  $$|\operatorname{Cl}_{A_5}((1\ 2\ 3\ 4\ 5))| = \frac{5!}{5} = 24$$

  Por tanto, hay 6 $5-$subgrupos de Sylow, que son:

  $$\begin{gathered}\langle(1\ 2\ 3\ 4\ 5)\rangle\\ \langle(1\ 2\ 3\ 5\ 4)\rangle\\ \langle(1\ 2\ 5\ 3\ 4)\rangle\\ \langle(1\ 5\ 2\ 3\ 4)\rangle\\ \langle(1\ 2\ 4\ 3\ 5)\rangle\\ \langle(1\ 2\ 4\ 5\ 3)\rangle\end{gathered}$$

7. S_5.

Ejercicio 2.6.22. Demostrar que D_4 es isomorfo a los $2-$subgrupos de Sylow de S_4.

Observación. Considerar la representación asociada a la acción de D_4 sobre los vértices del cuadrado.

Este ejercicio ya se resolvió en el Ejercicio 2.6.8, donde vimos que los $2-$subgrupos de Sylow de S_4 son isomorfos a D_4 aplicando el Teorema de Dyck.

Ejercicio 2.6.23. Demostrar que todo grupo de orden 12 con más de un $3-$subgrupo de Sylow es isomorfo al grupo alternado A_4.

Observación. Considerar la acción por traslación de un tal grupo sobre el conjunto de clases módulo P, siendo P un $3-$subgrupo de Sylow. Probar que dicha acción es fiel.

Sea G un grupo de orden 12 con más de un $3-$subgrupo de Sylow. Por el Segundo Teorema de Sylow, tenemos que:

$$n_3 \equiv 1 \mod 3 \qquad n_3 \mid 4$$

Por tanto, $n_3 \in \{1, 4\}$. Como G tiene más de un $3-$subgrupo de Sylow, tenemos que $n_3 = 4$. Sean por tanto:

$$\operatorname{Syl}_3 = \{P_1, P_2, P_3, P_4\}$$

Como cada P_i es un grupo de orden 3, es cíclico. De esta forma, supongamos que $\exists x \neq 1$ tal que $x \in P_i \cap P_j$ con $i \neq j$. Entonces, tenemos que:

$$P_i = \langle x\rangle = \{1, x, x^2\} = P_j$$

Por tanto, $P_i = P_j$, lo cual es una contradicción. Por tanto, tenemos que:

$$P_1 \cap P_2 = P_1 \cap P_3 = P_1 \cap P_4 = P_2 \cap P_3 = P_2 \cap P_4 = P_3 \cap P_4 = \{1\}$$

Por tanto, los $3-$subgrupos de Sylow son disjuntos dos a dos.

Consideramos la acción de G sobre el conjunto de clases módulo P_1. Como P_1 no es normal en G, no podemos considerar el grupo cociente, pero consideramos el conjunto de las clases por la izquierda:

$$G/\sim_{P_1} = \{gP_1 \mid g \in G\}$$

Sea por tanto la siguiente acción:

$$\begin{array}{rrcl} ac: & G \times G/\sim_{P_1} & \longrightarrow & G/\sim_{P_1} \\ & (g, hP_1) & \longmapsto & (gh)P_1 \end{array}$$

Veamos que está bien definida. Sea $g \in G$ y $h_1P_1, h_2P_1 \in G/\sim_{P_1}$ tales que $h_1P_1 = h_2P_1$. Entonces:

$$(gh_1)P_1 = (gh_2)P_1 \iff (gh_1)^{-1}(gh_2) \in P_1 \iff h_1^{-1}h_2 \in P_1 \iff h_1P_1 = h_2P_1$$

Por tanto, la acción está bien definida. Veamos que efectivamente es una acción:

$$\begin{gathered} {}^1hP_1 = (1h)P_1 = hP_1 \qquad \forall hP_1 \in G/\sim_{P_1} \\ {}^{g_1}({}^{g_2}hP_1) = {}^{g_1}(g_2h)P_1 = (g_1g_2h)P_1 = {}^{g_1g_2}hP_1 \qquad \forall g_1, g_2 \in G,\ hP_1 \in G/\sim_{P_1} \end{gathered}$$

Por tanto, consideramos su representación por permutaciones asociada a la acción:

$$\begin{array}{rrcl} \Phi: & G & \longrightarrow & \mathrm{Perm}(G/\sim_{P_1}) \\ & g & \longmapsto & {}^g(\cdot P_1) \end{array}$$

Veamos el cardinal del conjunto de clases:

$$|G/\sim_{P_1}| = [G : P_1] = \frac{|G|}{|P_1|} = \frac{12}{3} = 4$$

Por tanto, tenemos que:

$$\begin{array}{rrcl} \Phi: & G & \longrightarrow & S_4 \\ & g & \longmapsto & (g(\cdot))\, P_1 \end{array}$$

Calculamos que se trata de una acción fiel:

$$\begin{aligned} \ker(\Phi) &= \{g \in G \mid {}^g(\cdot P_1) = Id_{G/\sim_{P_1}}\} \\ &= \{g \in G \mid {}^g(hP_1) = hP_1\ \forall hP_1 \in G/\sim_{P_1}\} \\ &= \{g \in G \mid (gh)P_1 = hP_1\ \forall hP_1 \in G/\sim_{P_1}\} \\ &= \{g \in G \mid h^{-1}gh \in P_1\ \forall h \in G\} \\ &= \{g \in G \mid g \in hP_1h^{-1}\ \forall h \in G\} \end{aligned}$$

Por el Segundo Teorema de Sylow, todos los $3-$subgrupos de Sylow son conjugados entre sí, luego hP_1h^{-1} es un $3-$subgrupo de Sylow de G para todo $h \in G$. Por tanto, tenemos que:

$$\ker(\Phi) \subset \bigcap_{h\in G} hP_1h^{-1} \subset \bigcap_{i=1}^{4} P_i = \{1\}$$

Por tanto, $\ker(\Phi) = \{1\}$, luego la acción es fiel.

Por el Primer Teorema de Isomorfía, tenemos que:

$$G \cong G/\{1\} = G/\ker(\Phi) \cong \Im(\Phi) \subset S_4$$

Por tanto, hemos visto que G es isomorfo a un subgrupo de S_4. Como $|G| = 12$ y el único subgrupo de orden 12 de S_4 es A_4, tenemos que:

$$G \cong A_4$$

Por tanto, hemos demostrado que todo grupo de orden 12 con más de un $3-$subgrupo de Sylow es isomorfo al grupo alternado A_4.

Ejercicio 2.6.24.

1. Demostrar que no existen grupos simples de orden 12. Más concretamente, demostrar que todo grupo de orden 12 admite un subgrupo normal de orden 3 o de orden 4.

   Sea G un grupo de orden $12 = 3 \cdot 2^2$. Por el Segundo Teorema de Sylow, tenemos que:

   $$n_3 \mid 4 \qquad n_3 \equiv 1 \mod 3$$

   Por tanto, $n_3 \in \{1, 4\}$.

   - Si $n_3 = 1$, entonces el $3-$subgrupo de Sylow es normal con cardinal 3 (luego no es propio), por lo que G no es simple.
   - Si $n_3 = 4$, aplicamos de nuevo el Segundo Teorema de Sylow:

     $$n_2 \mid 3 \qquad n_2 \equiv 1 \mod 2$$

     Por tanto, $n_2 \in \{1, 3\}$.

     - Si $n_2 = 1$, entonces el $2-$subgrupo de Sylow es normal con cardinal 4 (luego no es propio), por lo que G no es simple.
     - Si $n_2 = 3$, $n_3 = 4$.
       Estudiamos la situación.
       - Como $n_3 = 4$, tenemos 4 $3-$subgrupos de Sylow (todos ellos disjuntos), por lo que tenemos $4 \cdot 2 = 8$ elementos de orden 3.
       - Como $n_2 = 3$, tenemos 3 $2-$subgrupos de Sylow, pero no podemos garantizar que sean disjuntos. Fijado $P \in \mathrm{Syl}_2(G)$, este tendrá 3 elementos de orden 2 o 4. Además, puesto que los $2-$subgrupos de Sylow son distintos, al menos habrá otro elemento de orden 2 o 4 distinto. Por tanto, tenemos al menos 4 elementos de orden 2 o 4.

Por tanto, tenemos:

- 1 elemento de orden 1.
- 8 elementos de orden 3.
- Al menos 4 elementos de orden 2 o 4.

Esto implica que el grupo tiene al menos 13 elementos, lo cual es una contradicción. Por tanto, este caso no puede darse.

Por tanto, hemos visto que $n_3 = 1$ (en cuyo caso G tiene un subgrupo normal de orden 3) o $n_2 = 1$ (en cuyo caso G tiene un subgrupo normal de orden 4). Por tanto, todo grupo de orden 12 admite un subgrupo normal de orden 3 o de orden 4.

2. Demostrar que no existen grupos simples de orden 28. Más concretamente, probar que todo grupo de orden 28 contiene un subgrupo normal de orden 7.

   Sea G un grupo de orden $28 = 7 \cdot 2^2$. Por el Segundo Teorema de Sylow, tenemos que:
   $$n_7 \mid 4 \qquad n_7 \equiv 1 \mod 7$$
   Por tanto, $n_7 = 1$. Por tanto el $7-$subgrupo de Sylow es normal con cardinal 7 (luego no es propio), por lo que G no es simple.

3. Demostrar que no existen grupos simples de orden 56. Más concretamente, probar que todo grupo de orden 56 contiene un subgrupo normal de orden 7 o de orden 8.

   Sea G un grupo de orden $56 = 7 \cdot 2^3$. Por el Segundo Teorema de Sylow, tenemos que:
   $$n_7 \mid 8 \qquad n_7 \equiv 1 \mod 7$$
   Por tanto, $n_7 \in \{1, 8\}$.

   - Si $n_7 = 1$, entonces el $7-$subgrupo de Sylow es normal con cardinal 7 (luego no es propio), por lo que G no es simple.
   - Si $n_7 = 8$, aplicamos de nuevo el Segundo Teorema de Sylow:
     $$n_2 \mid 7 \qquad n_2 \equiv 1 \mod 2$$
     Por tanto, $n_2 \in \{1, 7\}$.
     - Si $n_2 = 1$, entonces el $2-$subgrupo de Sylow es normal con cardinal 8 (luego no es propio), por lo que G no es simple.
     - Si $n_2 = 7$, $n_7 = 8$.
       - Como $n_7 = 8$, hay 8 $7-$subgrupos de Sylow (todos ellos distintos), por lo que tenemos $8 \cdot 6 = 48$ elementos de orden 7. Como $n_2 = 7$, tenemos 7 $2-$subgrupos de Sylow, pero no podemos garantizar que sean disjuntos. Fijado $P \in \mathrm{Syl}_2(G)$, este contendrá 7 elementos de orden 2, 4 o 8. Además, puesto que los $2-$subgrupos de Sylow son distintos, al menos habrá otro elemento de orden 2, 4 o 8 distinto. Por tanto, tenemos al menos 8 elementos de orden 2, 4 o 8.

Por tanto, tenemos:

- 1 elemento de orden 1.
- 48 elementos de orden 7.
- 8 elementos de orden 2, 4 o 8.

Esto implica que el grupo tiene al menos 57 elementos, lo cual es una contradicción. Por tanto, este caso no puede darse.

Por tanto, hemos visto que $n_7 = 1$ (en cuyo caso G tiene un subgrupo normal de orden 7) o $n_2 = 1$ (en cuyo caso G tiene un subgrupo normal de orden 8).

4. Demostrar que no existen grupos simples de orden 148.

Sea G un grupo de orden $148 = 37 \cdot 2^2$. Por el Segundo Teorema de Sylow, tenemos que:

$$n_{37} \mid 4 \qquad n_{37} \equiv 1 \mod 37$$

Por tanto, $n_{37} = 1$. Por tanto el $37-$subgrupo de Sylow es normal con cardinal 37 (luego no es propio), por lo que G no es simple.

5. Demostrar que no existen grupos simples de orden 200. Sea G un grupo de orden $200 = 5^2 \cdot 2^3$. Por el Segundo Teorema de Sylow, tenemos que:

$$n_5 \mid 8 \qquad n_5 \equiv 1 \mod 5$$

Por tanto, $n_5 = 1$. Por tanto el $5-$subgrupo de Sylow es normal con cardinal 5^2 (luego no es propio), por lo que G no es simple.

6. Demostrar que no existen grupos simples de orden 351. Sea G un grupo de orden $351 = 3^3 \cdot 13$. Por el Segundo Teorema de Sylow, tenemos que:

$$n_{13} \mid 27 \qquad n_{13} \equiv 1 \mod 13$$

Por tanto, $n_{13} \in \{1, 27\}$.

- Si $n_{13} = 1$, entonces el $13-$subgrupo de Sylow es normal con cardinal 13 (luego no es propio), por lo que G no es simple.
- Si $n_{13} = 27$, aplicamos de nuevo el Segundo Teorema de Sylow:

$$n_3 \mid 13 \qquad n_3 \equiv 1 \mod 3$$

Por tanto, $n_3 \in \{1, 13\}$.

- Si $n_3 = 1$, entonces el $3-$subgrupo de Sylow es normal con cardinal 27 (luego no es propio), por lo que G no es simple.
- Si $n_3 = 13$, $n_{13} = 27$.
  - Como $n_{13} = 27$, tenemos 27 $13-$subgrupos de Sylow (todos ellos distintos), por lo que tenemos $27 \cdot 12 = 324$ elementos de orden 13.

- Como $n_3 = 13$, tenemos 13 $3-$subgrupos de Sylow, pero no podemos garantizar que sean disjuntos. Fijado $P \in \mathrm{Syl}_3(G)$, este contendrá 26 elementos de orden 3, 9 o 27. Además, puesto que los $3-$subgrupos de Sylow son distintos, al menos habrá otro elemento de orden 3, 9 o 27 distinto. Por tanto, tenemos al menos 27 elementos de orden 3, 9 o 27.

Por tanto, tenemos:

- 1 elemento de orden 1.
- 324 elementos de orden 13.
- 27 elementos de orden $3, 9$ o 27.

Esto implica que el grupo tiene más de 351 elementos, lo cual es una contradicción. Por tanto, este caso no puede darse.

Por tanto, hemos visto que $n_{13} = 1$ (en cuyo caso G tiene un subgrupo normal de orden 13) o $n_3 = 1$ (en cuyo caso G tiene un subgrupo normal de orden 27).

Ejercicio 2.6.25. Calcular el número de elementos de orden 7 que tiene un grupo simple de orden 168.

Sabemos que $168 = 2^3 \cdot 3 \cdot 7$. Como cada elemento de orden 7 va a generar un grupo cíclico de orden 7, buscamos el número de subgrupos de Sylow de orden 7. Por la descomposición de 168, sabemos que dichos grupos serán $7-$subgrupos de Sylow. Por el Segundo Teorema de Sylow, tenemos que:

$$n_7 \equiv 1 \mod 7 \qquad n_7 \mid 24$$

Por tanto, $n_7 \in \{1, 8\}$.

- Si $n_7 = 1$, entonces el $7-$subgrupo de Sylow es normal con cardinal 7 (luego no es propio), por lo que G no es simple.

Por tanto, $n_7 = 8$. Por tanto, hay exactamente 8 subgrupos de orden 7. Cada uno de los elementos de orden 7 del grupo pertenece a un único subgrupo de orden 7, y será un generador de estos. Además, sabemos que el número de elementos de orden 7 de un grupo cíclico de orden 7 viene dado por la función $\varphi(7) = 6$. Por tanto, el número de elementos de orden 7 de un grupo simple de orden 168 es:

$$8 \cdot 6 = 48$$

2.7. Clasificación de grupos abelianos finitos

Ejercicio 2.7.1. Calcular los órdenes de todos los elementos de los distintos grupos abelianos de orden 8, 12, 16 y 24.

1. Sea G un grupo abeliano de $|G| = 8$.

   Como $|G| = 8 = 2^3$, por la estructura de los grupos abelianos finitos, tenemos que hay tres posibilidades:

   a) $G \cong C_8$.
   Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo cíclico $C_8 \cong \mathbb{Z}_8$.

   $$O(x) = \frac{8}{\text{mcd}(x, 8)}.$$

   Por tanto, los órdenes de los elementos de C_8 son:

   $$O(0) = 1, \quad O(1) = O(3) = O(5) = O(7) = 8, \quad O(2) = O(6) = 4, \quad O(4) = 2.$$

   Por tanto, hay un elemento de orden 1, cuatro de orden 8, dos de orden 4 y uno de orden 2.

   b) $G \cong C_4 \oplus C_2$.

   $$O(x, y) = \text{mcm}(O(x), O(y)) \qquad \forall x \in C_4, y \in C_2.$$

   Los órdenes de $\mathbb{Z}_2$ son:

   $$O(0) = 1, \quad O(1) = 2.$$

   Los órdenes de $\mathbb{Z}_4$ son:

   $$O(0) = 1, \quad O(1) = O(3) = 4, \quad O(2) = 2.$$

   Por tanto, los órdenes de los elementos de $C_4 \oplus C_2$ son:

   $$O(0,0) = 1, \quad O(1,0) = O(1,1) = O(3,0) = O(3,1) = 4,$$
   $$O(2,0) = O(2,1) = 2, \quad O(0,1) = 2.$$

   Por tanto, hay un elemento de orden 1, cuatro de orden 4 y tres de orden 2.

   c) $G \cong C_2 \oplus C_2 \oplus C_2$.
   Los órdenes de $\mathbb{Z}_2$ son:

   $$O(0) = 1, \quad O(1) = 2.$$

   Por tanto, los órdenes de los elementos de $C_2 \oplus C_2 \oplus C_2$ son:

   $$O(0,0,0) = 1,$$
   $$O(x, y, z) = 2 \qquad \forall x, y, z \in \{0, 1\} \text{ tal que } x + y + z \neq 0.$$

   Por tanto, hay un elemento de orden 1 y siete de orden 2.

2. Sea G un grupo abeliano de $|G| = 12$.

   Como $|G| = 12 = 2^2 \cdot 3$, por la estructura de los grupos abelianos finitos, tenemos que hay varias posibilidades:

   a) $G \cong C_{12}$.
   Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo cíclico $C_{12} \cong \mathbb{Z}_{12}$.
   $$O(x) = \frac{12}{\text{mcd}(x, 12)}.$$
   Por tanto, los órdenes de los elementos de C_{12} son:
   $$O(0) = 1, \quad O(1) = O(5) = O(7) = O(11) = 12, \quad O(2) = O(10) = 6,$$
   $$O(3) = O(9) = 4, \quad O(4) = O(8) = 3, \quad O(6) = 2.$$

   b) $G \cong C_6 \oplus C_2$.
   Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo cíclico $C_6 \cong \mathbb{Z}_6$ y de $C_2 \cong \mathbb{Z}_2$. Los órdenes de $\mathbb{Z}_2$ son:
   $$O(0) = 1, \quad O(1) = 2.$$
   Los órdenes de $\mathbb{Z}_6$ son:
   $$O(0) = 1, \quad O(1) = O(5) = 6, \quad O(2) = O(4) = 3, \quad O(3) = 2.$$
   Por tanto, los órdenes de los elementos de $C_6 \oplus C_2$ son:
   $$\begin{gathered} O(0,0) = 1, \\ O(1,0) = O(5,0) = O(1,1) = O(5,1) = 6, \\ O(2,0) = O(4,0) = 3, \\ O(2,1) = O(4,1) = 6, \\ O(3,0) = O(3,1) = 2, \\ O(0,1) = 2. \end{gathered}$$

3. Sea G un grupo abeliano de $|G| = 16$.

   Como $|G| = 16 = 2^4$, por la estructura de los grupos abelianos finitos, tenemos que hay varias posibilidades:

   a) $G \cong C_{16}$.
   Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo cíclico $C_{16} \cong \mathbb{Z}_{16}$.
   $$O(x) = \frac{16}{\text{mcd}(x, 16)}.$$
   Por tanto, los órdenes de los elementos de C_{16} son:
   $$\begin{gathered} O(0) = 1, \\ O(1) = O(3) = O(5) = O(7) = O(9) = O(11) = O(13) = O(15) = 16, \\ O(2) = O(6) = O(10) = O(14) = 8, \\ O(4) = O(12) = 4. \end{gathered}$$

b) $G \cong C_8 \oplus C_2$.

Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo cíclico $C_8 \cong \mathbb{Z}_8$ y de $C_2 \cong \mathbb{Z}_2$. Los órdenes de $\mathbb{Z}_2$ son:

$$O(0) = 1, \quad O(1) = 2.$$

Los órdenes de $\mathbb{Z}_8$ los hemos calculado en el primer apartado:

$$O(0) = 1, \quad O(1) = O(3) = O(5) = O(7) = 8, \quad O(2) = O(6) = 4, \quad O(4) = 2.$$

Por tanto, los órdenes de los elementos de $C_8 \oplus C_2$ son:

$$\begin{gathered} O(0,0) = 1, \qquad O(0,1) = 2, \\ O(1,0) = O(3,0) = O(5,0) = O(7,0) = 8, \\ O(1,1) = O(3,1) = O(5,1) = O(7,1) = 8, \\ O(2,0) = O(6,0) = O(2,1) = O(6,1) = 4, \\ O(4,0) = O(4,1) = 2. \end{gathered}$$

c) $G \cong C_4 \oplus C_4$.

Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo cíclico $C_4 \cong \mathbb{Z}_4$. Los órdenes de $\mathbb{Z}_4$ son:

$$O(0) = 1, \quad O(1) = O(3) = 4, \quad O(2) = 2.$$

Por tanto, los órdenes de los elementos de $C_4 \oplus C_4$ son:

$$\begin{gathered} O(0,0) = 1 \\ O(0,1) = O(0,3) = O(1,1) = O(1,3) = O(2,1) = O(2,3) = O(3,1) = O(3,3) = 4, \\ O(1,0) = O(1,2) = O(3,0) = O(3,2) = 4, \\ O(0,2) = O(2,0) = O(2,2) = 2 \end{gathered}$$

d) $G \cong C_4 \oplus C_2 \oplus C_2$.

Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo $C_4 \oplus C_2 \oplus C_2$. Los órdenes de $C_4 \oplus C_2$ ya los hemos calculado anteriormente:

$$\begin{gathered} O(0,0) = 1, \\ O(1,0) = O(1,1) = O(3,0) = O(3,1) = 4, \\ O(2,0) = O(2,1) = 2, \\ O(0,1) = 2. \end{gathered}$$

Los órdenes de C_2 son:

$$O(0) = 1, \quad O(1) = 2.$$

Por tanto, los órdenes de los elementos de $C_4 \oplus C_2 \oplus C_2$ son:

$$\begin{gathered}
O(0,0,0) = 1, \\
O(1,0,0) = O(1,1,0) = O(3,0,0) = O(3,1,0) = 4, \\
O(2,0,0) = O(2,1,0) = 2, \\
O(0,1,0) = 2, \\
O(0,0,1) = 2, \\
O(1,0,1) = O(1,1,1) = O(3,0,1) = O(3,1,1) = 4, \\
O(2,0,1) = O(2,1,1) = 2, \\
O(0,1,1) = 2.
\end{gathered}$$

e) $G \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2$.
Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo $C_2 \oplus C_2 \oplus C_2 \oplus C_2$. Los órdenes de $C_2 \oplus C_2 \oplus C_2$ ya los hemos calculado anteriormente:

$$\begin{aligned}
&O(0,0,0) = 1, \\
&O(x,y,z) = 2 \qquad \forall x,y,z \in \{0,1\} \text{ tal que } x+y+z \neq 0.
\end{aligned}$$

Por tanto, los órdenes de los elementos de $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ son:

$$\begin{aligned}
&O(0,0,0,0) = 1, \\
&O(x,y,z,w) = 2 \qquad \forall x,y,z,w \in \{0,1\} \text{ tal que } x+y+z+w \neq 0.
\end{aligned}$$

4. Sea G un grupo abeliano de $|G| = 24$.

Como $|G| = 24 = 2^3 \cdot 3$, por la estructura de los grupos abelianos finitos, tenemos que hay varias posibilidades:

a) $G \cong C_{24}$.
Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo cíclico $C_{24} \cong \mathbb{Z}_{24}$.

$$O(x) = \frac{24}{\text{mcd}(x,24)}.$$

Por tanto, los órdenes de los elementos de C_{24} son:

$$\begin{gathered}
O(0) = 1, \\
O(1) = O(5) = O(7) = O(11) = O(13) = O(17) = O(19) = O(23) = 24, \\
O(2) = O(10) = O(14) = O(22) = 12, \\
O(3) = O(9) = O(15) = 8, \\
O(4) = O(20) = 6, \\
O(6) = O(18) = 4, \\
O(8) = O(16) = 3, \\
O(12) = 2.
\end{gathered}$$

b) $G \cong C_{12} \oplus C_2$.

Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo cíclico $C_{12} \cong \mathbb{Z}_{12}$ y de $C_2 \cong \mathbb{Z}_2$. Los órdenes de $\mathbb{Z}_1 2$ los hemos calculado anteriormente:

$$\begin{gathered} O(0) = 1, \\ O(1) = O(5) = O(7) = O(11) = 12, \\ O(2) = O(10) = 6, \\ O(3) = O(9) = 4, \\ O(4) = O(8) = 3, \\ O(6) = 2. \end{gathered}$$

Los órdenes de $\mathbb{Z}_2$ son:

$$O(0) = 1, \quad O(1) = 2.$$

Por tanto, los órdenes de los elementos de $C_{12} \oplus C_2$ son:

$$\begin{gathered} O(0,0) = 1, \\ O(1,0) = O(5,0) = O(7,0) = O(11,0) = 12, \\ O(2,0) = O(10,0) = 6, \\ O(3,0) = O(9,0) = 4, \\ O(4,0) = O(8,0) = 3, \\ O(6,0) = 2, \\ O(0,1) = 2, \\ O(1,1) = O(5,1) = O(7,1) = O(11,1) = 12, \\ O(2,1) = O(10,1) = 6, \\ O(3,1) = O(9,1) = 4, \\ O(4,1) = O(8,1) = 6, \\ O(6,1) = 2. \end{gathered}$$

c) $G \cong C_6 \oplus C_2 \oplus C_2$.

Como el orden se mantiene bajo isomorfismos, basta con encontrar el orden de los elementos del grupo $C_6 \oplus C_2 \oplus C_2$. Los órdenes de $C_6 \oplus C_2$ ya los hemos calculado anteriormente:

$$\begin{gathered} O(0,0) = 1, \\ O(1,0) = O(5,0) = O(1,1) = O(5,1) = 6, \\ O(2,0) = O(4,0) = 3, \\ O(2,1) = O(4,1) = 6, \\ O(3,0) = O(3,1) = 2, \\ O(0,1) = 2. \end{gathered}$$

Los órdenes de C_2 son:

$$O(0) = 1, \quad O(1) = 2.$$

Por tanto, los órdenes de los elementos de $C_6 \oplus C_2 \oplus C_2$ son:

$$\begin{gathered}
O(0,0,0)=1, \\
O(1,0,0)=O(5,0,0)=O(1,1,0)=O(5,1,0)=6, \\
O(2,0,0)=O(4,0,0)=3, \\
O(2,1,0)=O(4,1,0)=6, \\
O(3,0,0)=O(3,1,0)=2, \\
O(0,1,0)=2, \\
O(0,0,1)=2, \\
O(1,0,1)=O(5,0,1)=O(1,1,1)=O(5,1,1)=6, \\
O(2,0,1)=O(4,0,1)=O(2,1,1)=O(4,1,1)=6, \\
O(3,0,1)=O(3,1,1)=2, \\
O(0,1,1)=2.
\end{gathered}$$

Ejercicio 2.7.2. Para los siguientes grupos calcular sus descomposiciones cíclicas.

1. $G_1 = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ con operación dada por multiplicación módulo 65.

   Vemos que G_1 es un abeliano con $|G_1| = 16$. Entonces, por el Ejercicio 2.7.1, sabemos que G_1 es isomorfo a uno de los siguientes grupos:

   a) C_{16}.
   b) $C_8 \oplus C_2$.
   c) $C_4 \oplus C_4$.
   d) $C_4 \oplus C_2 \oplus C_2$.
   e) $C_2 \oplus C_2 \oplus C_2 \oplus C_2$.

   Para distinguir, calculamos los órdenes de los elementos de G_1:

$$\begin{gathered}
O(1)=1, \\
O(8)=O(12)=O(18)=O(21)=O(27)=O(31)=O(34)=4 \\
O(38)=O(44)=O(47)=O(53)=O(57)=4, \\
O(14)=O(51)=O(64)=2.
\end{gathered}$$

   Por tanto, la única posibilidad es que $G_1 \cong C_4 \oplus C_4$.

2. $G_2 = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$ con operación dada por multiplicación módulo 135.

   Vemos que G_2 es un abeliano con $|G_2| = 24$. Entonces, por el Ejercicio 2.7.1, sabemos que G_2 es isomorfo a uno de los siguientes grupos:

   a) C_{24}.
   b) $C_{12} \oplus C_2$.

c) $C_6 \oplus C_2 \oplus C_2$.

Para distinguir, calculamos los órdenes de los elementos de G_2 (es tedioso, pero sencillo. En nuestro caso, lo hemos implementado mediante un sencillo programa). Nos bastaría con calcular:

$$O(28) = O(53) = O(82) = O(107) = 4$$

Por tanto, la única posibilidad es que:

$$G_2 \cong C_6 \oplus C_2 \oplus C_2.$$

3. $G_3 = \{1, 7, 17, 23, 49, 55, 65, 71\}$ con operación dada por multiplicación módulo 96.

   Vemos que G_3 es un abeliano con $|G_3| = 8$. Entonces, por el Ejercicio 2.7.1, sabemos que G_3 es isomorfo a uno de los siguientes grupos:

   a) C_8.
   b) $C_4 \oplus C_2$.
   c) $C_2 \oplus C_2 \oplus C_2$.

   Para distinguir, calculamos los órdenes de los elementos de G_3. De nuevo, es tedioso, pero sencillo. Basta con calcular:

$$O(17) = O(49) = O(65) = 2 \qquad O(7) = 4$$

   Por tanto, la única posibilidad es que:

$$G_3 \cong C_4 \oplus C_2.$$

4. $G_4 = \{1, 4, 11, 14, 16, 19, 26, 29, 31, 34, 41, 44\}$ con operación dada por multiplicación módulo 45.

   Vemos que G_4 es un abeliano con $|G_4| = 12$. Entonces, por el Ejercicio 2.7.1, sabemos que G_4 es isomorfo a uno de los siguientes grupos:

   a) C_{12}.
   b) $C_6 \oplus C_2$.

   Para distinguir, calculamos los órdenes de los elementos de G_4. De nuevo, es tedioso, pero sencillo. Basta con calcular:

$$O(19) = O(26) = O(44) = 2$$

   Por tanto, la única posibilidad es que:

$$G_4 \cong C_6 \oplus C_2.$$

Ejercicio 2.7.3. Calcular la descomposición cíclica y cíclica primaria de los grupos abelianos $C_{24} \oplus C_{40} \oplus C_{35}$ y $C_{14} \oplus C_{100} \oplus C_{40}$. ¿Son isomorfos?

Tenemos que:

$$\begin{aligned} 24 &= 2^3 \cdot 3, \\ 40 &= 2^3 \cdot 5, \\ 35 &= 5 \cdot 7, \\ 14 &= 2 \cdot 7, \\ 100 &= 2^2 \cdot 5^2, \\ 40 &= 2^3 \cdot 5. \end{aligned}$$

Por tanto, vemos a simple vista sin necesidad de hacer cálculos que no tienen el mismo orden, luego no son isomorfos. Trabajamos ahora con cada uno por separado.

1. Para $C_{24} \oplus C_{40} \oplus C_{35}$:

   Tenemos que:

$$\begin{aligned} C_{24} \oplus C_{40} \oplus C_{35} &\cong C_{2^3} \oplus C_3 \oplus C_{2^3} \oplus C_5 \oplus C_5 \oplus C_7 \\ &\cong C_{2^3} \oplus C_{2^3} \oplus C_3 \oplus C_5 \oplus C_5 \oplus C_7 \end{aligned}$$

   Por tanto, esa es la descomposición cíclica primaria:

$$C_{24} \oplus C_{40} \oplus C_{35} \cong C_{2^3} \oplus C_{2^3} \oplus C_3 \oplus C_5 \oplus C_5 \oplus C_7.$$

   En vistas de calcular la descomposición cíclica, tenemos la siguiente matriz:

$$\begin{pmatrix} 2^3 & 2^3 \\ 3 & 1 \\ 5 & 5 \\ 7 & 1 \end{pmatrix} \Longrightarrow \left\{ \begin{array}{l} d_1 = 2^3 \cdot 3 \cdot 5 \cdot 7 = 840, \\ d_2 = 2^3 \cdot 5 = 40 \end{array} \right.$$

   Por tanto, la descomposición cíclica es:

$$C_{24} \oplus C_{40} \oplus C_{35} \cong C_{840} \oplus C_{40}.$$

2. Para $C_{14} \oplus C_{100} \oplus C_{40}$:

   Tenemos que:

$$\begin{aligned} C_{14} \oplus C_{100} \oplus C_{40} &\cong C_2 \oplus C_7 \oplus C_{2^2} \oplus C_{5^2} \oplus C_{2^3} \oplus C_5 \\ &\cong C_{2^3} \oplus C_{2^2} \oplus C_2 \oplus C_{5^2} \oplus C_5 \oplus C_7 \end{aligned}$$

   Por tanto, esa es la descomposición cíclica primaria:

$$C_{14} \oplus C_{100} \oplus C_{40} \cong C_{2^3} \oplus C_{2^2} \oplus C_2 \oplus C_{5^2} \oplus C_5 \oplus C_7.$$

En vistas de calcular la descomposición cíclica, tenemos la siguiente matriz:

$$\begin{pmatrix} 2^3 & 2^2 & 2 \\ 5^2 & 5 & 1 \\ 7 & 1 & 1 \end{pmatrix} \Longrightarrow \left\{ \begin{array}{l} d_1 = 2^3 \cdot 5^2 \cdot 7 = 1400, \\ d_2 = 2^2 \cdot 5 = 20, \\ d_3 = 2 \end{array} \right.$$

Por tanto, la descomposición cíclica es:

$$C_{14} \oplus C_{100} \oplus C_{40} \cong C_{1400} \oplus C_{20} \oplus C_2.$$

Como vemos, las descomposiciones cíclicas son diferentes, lo que también nos indica que los grupos no son isomorfos.

Ejercicio 2.7.4. Sea G el grupo de las simetrías de un rectángulo (no cuadrado). Probar que G es un grupo abeliano. Calcular sus descomposiciones cíclica y cíclica primaria.

Las simetrías de un rectángulo se muestran en la Figura 2.59. Para ver que se

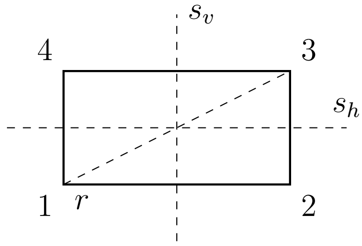


Figura 2.59: Simetrías de un rectángulo.

trata de un grupo, damos su tabla de Cayley:

$\cdot$	e	r	s_v	s_h
e	e	r	s_v	s_h
r	r	e	s_h	s_v
s_v	s_v	s_h	e	r
s_h	s_h	s_v	r	e

Como vemos, G es un grupo. Además, es abeliano porque la tabla es simétrica respecto a la diagonal principal. Como $|G| = 4$, hay dos opciones:

1. $G \cong C_4$.
2. $G \cong C_2 \oplus C_2$.

Como G no es cíclico (pues todos los elementos tienen orden 2), tenemos que:

$$G \cong C_2 \oplus C_2.$$

Esta es tanto su descomposición cíclica como cíclica primaria.

Ejercicio 2.7.5. Sea G un grupo abeliano de orden n y $l(G)$ su longitud. Si la descomposición de n en factores primos es $n = p_1^{e_1} \cdots p_r^{e_r}$, demostrar que

$$l(G) = e_1 + \cdots + e_r,$$

y que

$$\text{fact}(G) = (C_{p_1}, \overset{(e_1)}{\ldots}, C_{p_1}, \ldots, C_{p_r}, \overset{(e_r)}{\ldots}, C_{p_r}).$$

En particular, todos los grupos abelianos del mismo orden tienen la misma longitud y la misma lista de factores de composición.

Como G es abeliano, es resoluble y el enunciado tiene sentido. Calculamos su descomposición cíclica primaria, de forma que $\exists t_1, t_2, \ldots, t_r \in \mathbb{N}$ de forma que, para el $i-$ésimo entero t_i existe una partición de e_i en t_i sumandos:

$$\begin{gathered} n_{i1} \geqslant n_{i2} \geqslant \cdots \geqslant n_{it_i} \geqslant 1, \\ e_i = n_{i1} + n_{i2} + \cdots + n_{it_i}. \end{gathered}$$

De esta forma, tenemos que:

$$G \cong \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{t_i} C_{p_i^{n_{ij}}}.$$

Por el Ejercicio 2.5.7, tenemos que:

$$\begin{aligned} l(G) &= \sum_{i=1}^{r} \sum_{j=1}^{t_i} n_{ij} \overset{(*)}{=} \sum_{i=1}^{r} e_i = e_1 + \cdots + e_r \\ \text{fact}(G) &= \bigcup_{i=1}^{r} \bigcup_{j=1}^{t_i} \text{fact}(C_{p_i^{n_{ij}}}) \end{aligned}$$

donde en $(*)$ hemos empleado que es una partición y, por tanto, suman e_i.

Por el Ejercicio 2.5.8, como $C_{p_i^{n_{ij}}}$ es cíclico, tenemos que:

$$\text{fact}(C_{p_i^{n_{ij}}}) = (C_{p_i}, \overset{(n_{ij})}{\ldots}, C_{p_i}) \qquad \forall i, j.$$

Por tanto, tenemos que:

$$\text{fact}(G) = \bigcup_{i=1}^{r} \bigcup_{j=1}^{t_i} (C_{p_i}, \overset{(n_{ij})}{\ldots}, C_{p_i}) \overset{(*)}{=} \bigcup_{i=1}^{r} (C_{p_i}, \overset{(e_i)}{\ldots}, C_{p_i}) = (C_{p_1}, \overset{(e_1)}{\ldots}, C_{p_1}, \ldots, C_{p_r}, \overset{(e_r)}{\ldots}, C_{p_r}).$$

donde, de nuevo, en $(*)$ hemos empleado que es una partición y, por tanto, suman e_i. Hemos demostrado por tanto lo pedido.

Ejercicio 2.7.6. Listar todos los grupos abelianos no isomorfos de orden 10, 16, 20, 30, 40, 108 y 360, dando sus factores invariantes, divisores elementales y descomposiciones cíclicas y cíclicas primarias.

	Fact. Inv.	**Div. element.**	**Desc. cíclica primaria**	**Desc. cíclica**
$\begin{pmatrix} 2 \\ 5 \end{pmatrix}$	$d_1 = 2 \cdot 5 = 10$	$\{2; 5\}$	$C_2 \oplus C_5$	C_{10}

Tabla 2.1: Grupos abelianos de orden 10.

	Fact. Inv.	**Div. element.**	**Desc. cíclica primaria**	**Desc. cíclica**
$\begin{pmatrix} 2^4 \end{pmatrix}$	$d_1 = 2^4 = 16$	$\{2^4\}$	C_{16}	C_{16}
$\begin{pmatrix} 2^3 & 2 \end{pmatrix}$	$d_1 = 2^3 = 8$ $d_2 = 2$	$\{2^3; 2\}$	$C_8 \oplus C_2$	$C_8 \oplus C_2$
$\begin{pmatrix} 2^2 & 2^2 \end{pmatrix}$	$d_1 = 2^2 = 4$ $d_2 = 2^2 = 4$	$\{2^2; 2^2\}$	$C_4 \oplus C_4$	$C_4 \oplus C_4$
$\begin{pmatrix} 2^2 & 2 & 2 \end{pmatrix}$	$d_1 = 2^2 = 4$ $d_2 = 2$ $d_3 = 2$	$\{2^2; 2; 2\}$	$C_4 \oplus C_2 \oplus C_2$	$C_4 \oplus C_2 \oplus C_2$
$\begin{pmatrix} 2 & 2 & 2 & 2 \end{pmatrix}$	$d_1 = 2$ $d_2 = 2$ $d_3 = 2$ $d_4 = 2$	$\{2; 2; 2; 2\}$	$C_2 \oplus C_2 \oplus C_2 \oplus C_2$	$C_2 \oplus C_2 \oplus C_2 \oplus C_2$

Tabla 2.2: Grupos abelianos de orden 16.

1. Para $|G| = 10 = 2 \cdot 5$. Mostrado en la Tabla 2.1.

2. Para $|G| = 16 = 2^4$. Mostrado en la Tabla 2.2.

3. Para $|G| = 20 = 2^2 \cdot 5$. Mostrado en la Tabla 2.3.

4. Para $|G| = 30 = 2 \cdot 3 \cdot 5$. Mostrado en la Tabla 2.4.

5. Para $|G| = 40 = 2^3 \cdot 5$. Mostrado en la Tabla 2.5.

6. Para $|G| = 108 = 2^2 \cdot 3^3$. Mostrado en la Tabla 2.6.

7. Para $|G| = 360 = 2^3 \cdot 3^2 \cdot 5$. Mostrado en la Tabla 2.7.

Ejercicio 2.7.7. Calcular la forma normal, los factores invariantes y los divisores elementales de las siguientes matrices:

$$A_1 = \begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 7 & 10 & 6 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} -22 & -48 & -267 \\ -4 & -4 & 31 \\ -4 & -24 & 105 \\ 4 & -6 & -6 \end{pmatrix},$$
$$A_3 = \begin{pmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{pmatrix}, \qquad A_4 = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix}.$$

1. A_1:

	Fact. Inv.	Div. element.	Desc. cíclica primaria	Desc. cíclica
$\begin{pmatrix}2^2\\5\end{pmatrix}$	$d_1 = 2^2 \cdot 5 = 20$	$\{2^2; 5\}$	$C_4 \oplus C_5$	C_{20}
$\begin{pmatrix}2 & 2\\5 & 1\end{pmatrix}$	$d_1 = 2 \cdot 5 = 10$ $d_2 = 2$	$\{2; 2; 5\}$	$C_2 \oplus C_2 \oplus C_5$	$C_{10} \oplus C_2$

Tabla 2.3: Grupos abelianos de orden 20.

	Fact. Inv.	Div. element.	Desc. cíclica primaria	Desc. cíclica
$\begin{pmatrix}2\\3\\5\end{pmatrix}$	$d_1 = 2 \cdot 3 \cdot 5 = 30$	$\{2; 3; 5\}$	$C_2 \oplus C_3 \oplus C_5$	C_{30}

Tabla 2.4: Grupos abelianos de orden 30.

$$A_1 = \begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 7 & 10 & 6 \end{pmatrix} \xrightarrow{F_4' = F_4 + F_2} \begin{pmatrix} 0 & 2 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 1 & 6 & 0 \end{pmatrix} \xrightarrow{F_4 \leftrightarrow F_1} \begin{pmatrix} 1 & 6 & 0 \\ -6 & -4 & -6 \\ 6 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow[F_1' = F_1 - 3F_4]{C_1' = C_1 - C_3}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & -6 \\ 0 & 6 & 6 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow{F_2 \leftrightarrow F_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 6 & 6 \\ 0 & -4 & -6 \end{pmatrix} \xrightarrow[F_3' = F_3 - 3F_2]{F_4' = F_4 + 2F_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & -6 \end{pmatrix} \xrightarrow{F_4' = F_4 + F_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Por tanto, la forma normal de A_1 es:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Sus factores invariantes son $d_1 = 1$, $d_2 = 2$ y $d_3 = 6$. Los divisores elementales son $\{2; 2; 3\}$.

2. A_2:

$$A_2 = \begin{pmatrix} -22 & -48 & -267 \\ -4 & -4 & 31 \\ -4 & -24 & 105 \\ 4 & -6 & -6 \end{pmatrix} \xrightarrow{F_2' = F_2 + 5F_4} \begin{pmatrix} -22 & -48 & -267 \\ 16 & -34 & 1 \\ -4 & -24 & 105 \\ 4 & -6 & -6 \end{pmatrix} \xrightarrow{F_2 \leftrightarrow F_1} \begin{pmatrix} 16 & -34 & 1 \\ -22 & -48 & -267 \\ -4 & -24 & 105 \\ 4 & -6 & -6 \end{pmatrix}$$

$$\xrightarrow{C_3 \leftrightarrow C_1} \begin{pmatrix} 1 & -34 & 16 \\ -267 & -48 & -22 \\ 105 & -24 & -4 \\ -6 & -6 & 4 \end{pmatrix} \xrightarrow[F_2' = F_2 + 267F_1]{F_3' = F_3 - 105F_1} \begin{pmatrix} 1 & -34 & 16 \\ 0 & -9126 & 4250 \\ 0 & 3546 & -1684 \\ -6 & -6 & 4 \end{pmatrix} \xrightarrow{F_4' = F_4 + 6F_1}$$

$$\begin{pmatrix} 1 & -34 & 16 \\ 0 & -9126 & 4250 \\ 0 & 3546 & -1684 \\ 0 & -210 & 100 \end{pmatrix} \xrightarrow[C_2' = C_2 + 34C_1]{C_3' = C_3 - 16C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -9126 & 4250 \\ 0 & 3546 & -1684 \\ 0 & -210 & 100 \end{pmatrix} \xrightarrow[F_2' = F_2 - 43F_4]{F_3' = F_3 + 17F_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -96 & -50 \\ 0 & -24 & 16 \\ 0 & -210 & 100 \end{pmatrix}$$

	Fact. Inv.	Div. element.	Desc. cíclica primaria	Desc. cíclica
$\begin{pmatrix} 2^3 \\ 5 \end{pmatrix}$	$d_1 = 40$	$\{2^3; 5\}$	$C_8 \oplus C_5$	C_{40}
$\begin{pmatrix} 2^2 & 2 \\ 5 & 1 \end{pmatrix}$	$d_1 = 20$ $d_2 = 2$	$\{2^2; 2; 5\}$	$C_4 \oplus C_2 \oplus C_5$	$C_{20} \oplus C_2$
$\begin{pmatrix} 2 & 2 & 2 \\ 5 & 1 & 1 \end{pmatrix}$	$d_1 = 10$ $d_2 = 2$ $d_3 = 2$	$\{2; 2; 2; 5\}$	$C_2 \oplus C_2 \oplus C_2 \oplus C_5$	$C_{10} \oplus C_2 \oplus C_2$

Tabla 2.5: Grupos abelianos de orden 40.

	Fact. Inv.	Div. element.	Desc. cíclica primaria	Desc. cíclica
$\begin{pmatrix} 2^2 \\ 3^3 \end{pmatrix}$	$d_1 = 108$	$\{2^2; 3^3\}$	$C_4 \oplus C_{27}$	C_{108}
$\begin{pmatrix} 2 & 2 \\ 3^3 & 1 \end{pmatrix}$	$d_1 = 54$ $d_2 = 2$	$\{2; 2; 3^3\}$	$C_2 \oplus C_2 \oplus C_{27}$	$C_{54} \oplus C_2$
$\begin{pmatrix} 2^2 & 1 \\ 3^2 & 3 \end{pmatrix}$	$d_1 = 36$ $d_2 = 3$	$\{2^2; 3^2; 3\}$	$C_4 \oplus C_9 \oplus C_3$	$C_{36} \oplus C_3$
$\begin{pmatrix} 2 & 2 \\ 3^2 & 3 \end{pmatrix}$	$d_1 = 18$ $d_2 = 6$	$\{2; 2; 3^2; 3\}$	$C_2 \oplus C_2 \oplus C_9 \oplus C_3$	$C_{18} \oplus C_6$
$\begin{pmatrix} 2^2 & 1 & 1 \\ 3 & 3 & 3 \end{pmatrix}$	$d_1 = 12$ $d_2 = 3$ $d_3 = 3$	$\{2^2; 3; 3; 3\}$	$C_4 \oplus C_3 \oplus C_3 \oplus C_3$	$C_{12} \oplus C_3 \oplus C_3$
$\begin{pmatrix} 2 & 2 & 1 \\ 3 & 3 & 3 \end{pmatrix}$	$d_1 = 6$ $d_2 = 6$ $d_3 = 3$	$\{2; 2; 3; 3; 3\}$	$C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_3$	$C_6 \oplus C_6 \oplus C_3$

Tabla 2.6: Grupos abelianos de orden 108.

$$\xrightarrow{F_2'=-(F_2+3F_3)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 168 & 2 \\ 0 & -24 & 16 \\ 0 & -210 & 100 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 168 \\ 0 & 16 & -24 \\ 0 & 100 & -210 \end{pmatrix} \xrightarrow{C_3'=C_3-84C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 16 & -1368 \\ 0 & 100 & -8610 \end{pmatrix}$$

$$\xrightarrow[F_3'=F_3-8F_2]{F_4'=F_4-50F_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1368 \\ 0 & 0 & -8610 \end{pmatrix} \xrightarrow{F_4'=F_4+4F_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1368 \\ 0 & 0 & -402 \end{pmatrix} \xrightarrow{F_3'=F_3-3F_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -162 \\ 0 & 0 & -402 \end{pmatrix}$$

$$\xrightarrow{F_4'=F_4-2F_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -162 \\ 0 & 0 & -78 \end{pmatrix} \xrightarrow{F_3'=-(F_3-2F_3)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & -78 \end{pmatrix} \xrightarrow{F_4'=F_4+13F_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Por tanto, la forma normal de A_2 es:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

	Fact. Inv.	Div. element.	Desc. cíclica primaria	Desc. cíclica
$\begin{pmatrix} 2^3 \\ 3^2 \\ 5 \end{pmatrix}$	$d_1 = 360$	$\{2^3; 3^2; 5\}$	$C_8 \oplus C_9 \oplus C_5$	C_{360}
$\begin{pmatrix} 2^2 & 2 \\ 3^2 & 1 \\ 5 & 1 \end{pmatrix}$	$d_1 = 180$ $d_2 = 2$	$\{2^2; 2; 3^2; 5\}$	$C_4 \oplus C_2 \oplus C_9 \oplus C_5$	$C_{180} \oplus C_2$
$\begin{pmatrix} 2^3 & 1 \\ 3 & 3 \\ 5 & 1 \end{pmatrix}$	$d_1 = 120$ $d_2 = 3$	$\{2^3; 3; 3; 5\}$	$C_8 \oplus C_3 \oplus C_3 \oplus C_5$	$C_{120} \oplus C_3$
$\begin{pmatrix} 2^2 & 2 \\ 3 & 3 \\ 5 & 1 \end{pmatrix}$	$d_1 = 60$ $d_2 = 6$	$\{2^2; 2; 3; 3; 5\}$	$C_4 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$	$C_{60} \oplus C_6$
$\begin{pmatrix} 2 & 2 & 2 \\ 3^2 & 1 & 1 \\ 5 & 1 & 1 \end{pmatrix}$	$d_1 = 90$ $d_2 = 2$ $d_3 = 2$	$\{2; 2; 2; 3^2; 5\}$	$C_2 \oplus C_2 \oplus C_2 \oplus C_9 \oplus C_5$	$C_{90} \oplus C_2 \oplus C_2$
$\begin{pmatrix} 2 & 2 & 2 \\ 3 & 3 & 1 \\ 5 & 1 & 1 \end{pmatrix}$	$d_1 = 30$ $d_2 = 6$ $d_3 = 2$	$\{2; 2; 3; 3; 5\}$	$C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_5$	$C_{30} \oplus C_6 \oplus C_2$

Tabla 2.7: Grupos abelianos de orden 360.

Sus factores invariantes son $d_1 = 1$, $d_2 = 2$ y $d_3 = 6$. Los divisores elementales son $\{2; 2; 3\}$.

3. A_3:

$$A_3 = \begin{pmatrix} 9 & 4 & 5 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{pmatrix} \xrightarrow{F_1'=F_1+2F_2} \begin{pmatrix} 1 & 4 & -1 \\ -4 & 0 & -3 \\ -6 & -4 & -2 \end{pmatrix} \xrightarrow[F_2'=F_2+4F_1]{F_3'=F_3+6F_1} \begin{pmatrix} 1 & 4 & -1 \\ 0 & 16 & -7 \\ 0 & 20 & -8 \end{pmatrix}$$
$$\xrightarrow[C_2'=C_2-4C_1]{C_3'=C_3+C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 16 & -7 \\ 0 & 20 & -8 \end{pmatrix} \xrightarrow{F_3'=-(F_3-F_2)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 16 & -7 \\ 0 & -4 & 1 \end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{F_2\leftrightarrow F_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & -7 & 16 \end{pmatrix}$$
$$\xrightarrow{F_3'=-(F_3+7F_2)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & 0 & 12 \end{pmatrix} \xrightarrow{C_3'=C_3+4C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 12 \end{pmatrix}$$

Por tanto, la forma normal de A_3 es:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 12 \end{pmatrix}$$

Sus factores invariantes son $d_1 = 1$, $d_2 = 1$ y $d_3 = 12$. Los divisores elementales son $\{4; 3\}$.

4. A_4:

$$A_4 = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_2'=C_2+C_1} \begin{pmatrix} 4 & 4 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{F_1'=-(F_1-F_2)} \begin{pmatrix} -4 & 2 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_1}$$

$$\begin{pmatrix} 2 & -4 & 0 \\ 6 & 0 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{F_2'=F_2-3F_1} \begin{pmatrix} 2 & -4 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_2'=C_2+2C_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_3'=C_3+C_2}$$

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 12 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{F_2'=F_2-F_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 4 \\ 0 & 0 & 8 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 12 \\ 0 & 8 & 0 \end{pmatrix} \xrightarrow{F_3'=F_3-2F_2}$$

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 12 \\ 0 & 0 & -24 \end{pmatrix} \xrightarrow{C_3'=-(C_3-3C_2)} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 24 \end{pmatrix}$$

Por tanto, la forma normal de A_4 es:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 24 \end{pmatrix}$$

Sus factores invariantes son $d_1 = 2$, $d_2 = 4$ y $d_3 = 24$. Los divisores elementales son $\{2; 4; 8; 3\}$.

Ejercicio 2.7.8. Para los siguientes grupos abelianos calcular sus rangos y sus descomposiciones cíclicas y cíclicas primarias. ¿Son algunos de estos grupos isomorfos?

1. $G_1 = \left\langle a, b, c \;\middle|\; \begin{array}{rcl} 3a + 9b + 9c & = & 0 \\ 9a - 3b + 9c & = & 0 \end{array} \right\rangle$.

   Su matriz de relaciones es:

   $$A_1 = \begin{pmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \end{pmatrix}.$$

   Calculamos su forma normal:

   $$A_1 = \begin{pmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \end{pmatrix} \xrightarrow{F_2'=F_2-3F_1} \begin{pmatrix} 3 & 9 & 9 \\ 0 & -30 & -18 \end{pmatrix} \xrightarrow[C_2'=C_2-3C_1]{C_3'=C_3-3C_1}$$

   $$\begin{pmatrix} 3 & 0 & 0 \\ 0 & -30 & -18 \end{pmatrix} \xrightarrow{C_2'=C_2-2C_3} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & -18 \end{pmatrix} \xrightarrow{C_3'=C_3+3C_2} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}$$

   Por tanto, la forma normal de G_1 es:

   $$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}$$

   Su rango es:

   $$3 - 2 = 1.$$

   Su descomposición cíclica es:

   $$G_1 \cong \mathbb{Z} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_6.$$

   Su descomposición cíclica primaria es:

   $$G_1 \cong \mathbb{Z} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3.$$

2. $G_2 = \left\langle a, b, c \;\middle|\; \begin{array}{rcl} 2a+2b+3c & = & 0 \\ 5a+2b-3c & = & 0 \end{array} \right\rangle$.

Su matriz de relaciones es:

$$A_2 = \begin{pmatrix} 2 & 2 & 3 \\ 5 & 2 & -3 \end{pmatrix}.$$

Calculamos su forma normal:

$$A_2 = \begin{pmatrix} 2 & 2 & 3 \\ 5 & 2 & -3 \end{pmatrix} \xrightarrow{F_2'=F_2-2F_1} \begin{pmatrix} 2 & 2 & 3 \\ 1 & -2 & -9 \end{pmatrix} \xrightarrow{F_2\leftrightarrow F_1} \begin{pmatrix} 1 & -2 & -9 \\ 2 & 2 & 3 \end{pmatrix} \xrightarrow{F_2'=F_2-2F_1}$$
$$\begin{pmatrix} 1 & -2 & -9 \\ 0 & 6 & 21 \end{pmatrix} \xrightarrow[C_2'=C_2+2C_1]{C_3'=C_3+9C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 21 \end{pmatrix} \xrightarrow{C_3'=C_3-3C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 3 \end{pmatrix} \xrightarrow{C_2\leftrightarrow C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 6 \end{pmatrix}$$
$$\xrightarrow{C_3'=C_3-2C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$$

Por tanto, la forma normal de G_2 es:

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

Su rango es:

$$3-2=1.$$

Su descomposición cíclica, que coincide con su descomposición cíclica primaria, es:

$$G_2 \cong \mathbb{Z} \oplus \mathbb{Z}_3.$$

3. $G_3 = \left\langle a, b, c, d \;\middle|\; \begin{array}{rcl} a+3b+2c & = & 0 \\ 5a+17b+12c & = & 0 \\ 6a+4c & = & 0 \end{array} \right\rangle$.

Su matriz de relaciones es:

$$A_3 = \begin{pmatrix} 1 & 3 & 2 & 0 \\ 5 & 17 & 12 & 0 \\ 6 & 0 & 4 & 0 \end{pmatrix}.$$

Calculamos su forma normal:

$$A_3 = \begin{pmatrix} 1 & 3 & 2 & 0 \\ 5 & 17 & 12 & 0 \\ 6 & 0 & 4 & 0 \end{pmatrix} \xrightarrow[F_2'=F_2-5F_1]{F_3'=F_3-6F_1} \begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & -18 & -8 & 0 \end{pmatrix} \xrightarrow[C_2'=C_2-3C_1]{C_3'=C_3-2C_1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & -18 & -8 & 0 \end{pmatrix}$$
$$\xrightarrow{F_3'=F_3+9F_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 10 & 0 \end{pmatrix} \xrightarrow{C_3'=C_3-C_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 10 & 0 \end{pmatrix}$$

Por tanto, la forma normal de G_3 es:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 10 & 0 \end{pmatrix}$$

Su rango es:
$$4 - 3 = 1.$$

Su descomposición cíclica es:
$$G_3 \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10}.$$

Su descomposición cíclica primaria es:
$$G_3 \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5.$$

4. $G_4 = \left\langle a, b, c \;\middle|\; \begin{array}{rcl} 12a + 4b + 6c & = & 0 \\ -4a + 2b + 8c & = & 0 \\ -2a + 16b + 34c & = & 0 \end{array} \right\rangle.$

Su matriz de relaciones es:
$$A_4 = \begin{pmatrix} 12 & 4 & 6 \\ -4 & 2 & 8 \\ -2 & 16 & 34 \end{pmatrix}.$$

Calculamos su forma normal:
$$A_4 = \begin{pmatrix} 12 & 4 & 6 \\ -4 & 2 & 8 \\ -2 & 16 & 34 \end{pmatrix} \xrightarrow{F_1'=F_1+5F_3} \begin{pmatrix} 2 & 84 & 176 \\ -4 & 2 & 8 \\ -2 & 16 & 34 \end{pmatrix} \xrightarrow[F_2'=F_2+2F_1]{F_3'=F_3+F_1} \begin{pmatrix} 2 & 84 & 176 \\ 0 & 170 & 360 \\ 0 & 100 & 210 \end{pmatrix} \xrightarrow[C_2'=C_2-42C_1]{C_3'=C_3-88C_1}$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 170 & 360 \\ 0 & 100 & 210 \end{pmatrix} \xrightarrow{F_2'=F_2-2F_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -30 & -60 \\ 0 & 100 & 210 \end{pmatrix} \xrightarrow{F_3'=F_3+3F_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -30 & -60 \\ 0 & 10 & 30 \end{pmatrix} \xrightarrow{F_2 \leftrightarrow F_3}$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 10 & 30 \\ 0 & -30 & -60 \end{pmatrix} \xrightarrow{F_3'=F_3+3F_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 10 & 30 \\ 0 & 0 & 30 \end{pmatrix} \xrightarrow{C_3'=C_3-3C_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 30 \end{pmatrix}$$

Por tanto, la forma normal de G_4 es:
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 30 \end{pmatrix}$$

Su rango es:
$$3 - 3 = 0.$$

Su descomposición cíclica es:
$$G_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{30}.$$

Su descomposición cíclica primaria es:
$$G_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3.$$

5. $G_5 = \mathbb{Z}_{24} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{35}$.

   En este caso, su rango es 0 por ser abeliano finito. Su descomposición cíclica primaria es:
$$G_5 \cong \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_5.$$

   Su tabla asociada para obtener la descomposición cíclica es:
$$\begin{pmatrix} 2^3 & 2^3 \\ 5 & 5 \\ 7 & 1 \\ 3 & 1 \end{pmatrix} \Longrightarrow \begin{cases} d_1 = 840 \\ d_2 = 40 \end{cases}$$

   Por tanto, su descomposición cíclica es:
$$G_5 \cong \mathbb{Z}_{840} \oplus \mathbb{Z}_{40}.$$

Por último, y puesto que las descomposiciones cíclica y cíclica primaria son únicas salvo isomorfismos, podemos concluir que ninguno de estos grupos es isomorfo a otro, ya que sus descomposiciones cíclicas y cíclicas primarias son distintas.

Ejercicio 2.7.9. Dados los grupos abelianos:
$$\begin{aligned} G &= \left\langle a,b,c,d \;\middle|\; \begin{array}{rcl} a+2c-d &=& 0 \\ a+5c+5d &=& 0 \\ 2a+4c+2d &=& 0 \end{array} \right\rangle, \\ H &= \mathbb{Z}^3/K, \end{aligned}$$

donde K es el subgrupo con generadores $\{(1,2,7),(1,4,7),(-1,0,2)\}$. Calcular:

1. El rango, los factores invariantes y los divisores elementales de cada uno de ellos.

   Comenzamos por G. Su matriz de relaciones es:
$$A_G = \begin{pmatrix} 1 & 0 & 2 & -1 \\ 1 & 0 & 5 & 5 \\ 2 & 0 & 4 & 2 \end{pmatrix}.$$

   Calculamos su forma normal:
$$A_G = \begin{pmatrix} 1 & 0 & 2 & -1 \\ 1 & 0 & 5 & 5 \\ 2 & 0 & 4 & 2 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_4} \begin{pmatrix} 1 & -1 & 2 & 0 \\ 1 & 5 & 5 & 0 \\ 2 & 2 & 4 & 0 \end{pmatrix} \xrightarrow[F_2'=F_2-F_1]{F_3'=F_3-2F_1} \begin{pmatrix} 1 & -1 & 2 & 0 \\ 0 & 6 & 3 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix} \xrightarrow[C_2'=C_2+C_1]{C_3'=C_3-2C_1}$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 6 & 3 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix} \xrightarrow{F_2'=F_2-F_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 3 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix} \xrightarrow{C_2'=-(C_2-C_3)} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & -4 & 0 & 0 \end{pmatrix} \xrightarrow{F_3'=F_3+4F_2}$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix} \xrightarrow{C_3'=C_3-3C_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix}$$

Por tanto, la forma normal de G es:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix}$$

Su rango es:

$$4 - 3 = 1.$$

Sus factores invariantes son $d_1 = 1$, $d_2 = 1$ y $d_3 = 12$. Sus divisores elementales son $\{4; 3\}$.

Respecto a H, por el Primer Teorema de Isomorfía tenemos que:

$$H = \mathbb{Z}^3/K \cong \left\langle a, b, c \;\middle|\; \begin{array}{rcl} a + 2b + 7c & = & 0 \\ a + 4b + 7c & = & 0 \\ -a + 2c & = & 0 \end{array} \right\rangle$$

Su matriz de relaciones es:

$$A_H = \begin{pmatrix} 1 & 2 & 7 \\ 1 & 4 & 7 \\ -1 & 0 & 2 \end{pmatrix}.$$

Calculamos su forma normal:

$$A_H = \begin{pmatrix} 1 & 2 & 7 \\ 1 & 4 & 7 \\ -1 & 0 & 2 \end{pmatrix} \xrightarrow[F_2'=F_2-F_1]{F_3'=F_3+F_1} \begin{pmatrix} 1 & 2 & 7 \\ 0 & 2 & 0 \\ 0 & 2 & 9 \end{pmatrix} \xrightarrow[C_2'=C_2-2C_1]{C_3'=C_3-7C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 2 & 9 \end{pmatrix} \xrightarrow{C_3'=C_3-4C_2}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -8 \\ 0 & 2 & 1 \end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{F_2\leftrightarrow F_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & -8 & 2 \end{pmatrix} \xrightarrow{F_3'=F_3+8F_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 18 \end{pmatrix} \xrightarrow{C_3'=C_3-2C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 18 \end{pmatrix}$$

Por tanto, la forma normal de H es:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 18 \end{pmatrix}$$

Su rango es:

$$3 - 3 = 0.$$

Sus factores invariantes son $d_1 = 1$, $d_2 = 1$ y $d_3 = 18$. Sus divisores elementales son $\{2; 9\}$.

2. Sus descomposiciones cíclicas y cíclicas primarias.

   La descomposición cíclica de G es:

$$G \cong \mathbb{Z} \oplus \mathbb{Z}_{12}.$$

La descomposición cíclica primaria de G es:

$$G \cong \mathbb{Z} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3.$$

La descomposición cíclica de H es:

$$H \cong \mathbb{Z}_{18}$$

La descomposición cíclica primaria de H es:

$$H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_9.$$

3. Las descomposiciones cíclica y cíclica primaria de $G \oplus H$.

   La descomposición cíclica primaria de $G \oplus H$ es:

$$G \oplus H \cong \mathbb{Z} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{18} \cong \mathbb{Z} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9.$$

   La descomposición cíclica de $G \oplus H$ es:

$$G \oplus H \cong \mathbb{Z} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_6.$$

Ejercicio 2.7.10.

1. Encuentra todos los grupos abelianos distintos, salvo isomorfismo, de orden 500. Da para cada uno de ellos sus descomposiciones cíclica y cíclica primaria.

   Para encontrar los grupos abelianos de orden 500, comenzamos por descomponer 500 en factores primos:

$$500 = 2^2 \cdot 5^3.$$

   Los grupos abelianos de orden 500 se muestran en la Tabla 2.8.

2. Calcula las descomposiciones cíclica y cíclica primaria de

$$G = \left\langle a, b, c \;\middle|\; \begin{array}{rcl} 3a - 3b + 9c & = & 0 \\ 6a + 12b - 9c & = & 0 \\ 12b + 9c & = & 0 \end{array} \right\rangle.$$

   ¿Cuántos elementos tiene G? ¿Tiene algún elemento de orden 6?

   Su matriz de relaciones es:

$$A_G = \begin{pmatrix} 3 & -3 & 9 \\ 6 & 12 & -9 \\ 0 & 12 & 9 \end{pmatrix}.$$

   Calculamos su forma normal:

	Fact. Inv.	Div. element.	Desc. cíclica primaria	Desc. cíclica
$\begin{pmatrix} 2^2 \\ 5^3 \end{pmatrix}$	$d_1 = 500$	$\{2^2; 5^3\}$	$C_4 \oplus C_{125}$	C_{500}
$\begin{pmatrix} 2 & 2 \\ 5^3 & 1 \end{pmatrix}$	$d_1 = 250$ $d_2 = 2$	$\{2; 2; 5^3\}$	$C_2 \oplus C_2 \oplus C_{125}$	$C_{250} \oplus C_2$
$\begin{pmatrix} 2^2 & 1 \\ 5^2 & 5 \end{pmatrix}$	$d_1 = 100$ $d_2 = 5$	$\{2^2; 5^2; 5\}$	$C_4 \oplus C_{25} \oplus C_5$	$C_{100} \oplus C_5$
$\begin{pmatrix} 2 & 2 \\ 5^2 & 5 \end{pmatrix}$	$d_1 = 50$ $d_2 = 10$	$\{2; 2; 5^2; 5\}$	$C_2 \oplus C_2 \oplus C_{25} \oplus C_5$	$C_{50} \oplus C_{10}$
$\begin{pmatrix} 2^2 & 1 & 1 \\ 5 & 5 & 5 \end{pmatrix}$	$d_1 = 20$ $d_2 = 5$ $d_3 = 5$	$\{2^2; 5; 5; 5\}$	$C_4 \oplus C_5 \oplus C_5 \oplus C_5$	$C_{20} \oplus C_5 \oplus C_5$
$\begin{pmatrix} 2 & 2 & 1 \\ 5 & 5 & 5 \end{pmatrix}$	$d_1 = 10$ $d_2 = 10$ $d_3 = 5$	$\{2; 2; 5; 5; 5\}$	$C_2 \oplus C_2 \oplus C_5 \oplus C_5 \oplus C_5$	$C_{10} \oplus C_{10} \oplus C_5$

Tabla 2.8: Grupos abelianos de orden 500.

$$A_G = \begin{pmatrix} 3 & -3 & 9 \\ 6 & 12 & -9 \\ 0 & 12 & 9 \end{pmatrix} \xrightarrow{F_2'=F_2-2F_1} \begin{pmatrix} 3 & -3 & 9 \\ 0 & 18 & -27 \\ 0 & 12 & 9 \end{pmatrix} \xrightarrow[C_2'=C_2+C_1]{C_3'=C_3-3C_1} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 18 & -27 \\ 0 & 12 & 9 \end{pmatrix}$$

$$\xrightarrow{C_2'=C_2-C_3} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 45 & -27 \\ 0 & 3 & 9 \end{pmatrix} \xrightarrow{F_2 \leftrightarrow F_3} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 9 \\ 0 & 45 & -27 \end{pmatrix} \xrightarrow{F_3'=-(F_3-15F_2)} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 9 \\ 0 & 0 & 162 \end{pmatrix}$$

$$\xrightarrow{C_3'=C_3-3C_2} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 162 \end{pmatrix}$$

Por tanto, la forma normal de G es:

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 162 \end{pmatrix}$$

Su rango es:

$$3 - 3 = 0.$$

Su descomposición cíclica es:

$$G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{162}.$$

Su descomposición cíclica primaria es:

$$G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^4}.$$

Por tanto:

$$|G| = 3^2 \cdot 2 \cdot 3^4 = 2 \cdot 3^6 = 729 \cdot 2 = 1458.$$

El orden de un elemento de un producto directo es el mínimo común múltiplo de los órdenes de sus componentes. Buscamos en primer lugar un elemento de orden 6 en $\mathbb{Z}_{162}$.

$$\operatorname{ord}\left(\frac{162}{6}\right) = \operatorname{ord}(27) = 6.$$

Por tanto, un elemento de orden 6 en el producto directo es:

$$g = (0, 0, 27) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{162}.$$

Calculando la preimagen de g mediante el isomorfismo, como este mantiene el orden de los elementos, tenemos que G tiene al menos un elemento de orden 6.

Ejercicio 2.7.11. Dados los grupos abelianos

$$\begin{aligned} G &= \left\langle a, b, c \;\middle|\; \begin{array}{rcl} 2a - 6b + 18c &=& 0 \\ 6a + 6c &=& 0 \end{array} \right\rangle, \\ H &= \mathbb{Z}^3 / \langle (1, -9, 3), (1, -7, 1), (1, -1, 1) \rangle. \end{aligned}$$

1. Calcula sus rangos, descomposiciones cíclicas y cíclicas primarias.

   Comenzamos por G. Su matriz de relaciones es:

   $$A_G = \begin{pmatrix} 2 & -6 & 18 \\ 6 & 0 & 6 \end{pmatrix}.$$

   Calculamos su forma normal:

   $$\begin{aligned} A_G = \begin{pmatrix} 2 & -6 & 18 \\ 6 & 0 & 6 \end{pmatrix} &\xrightarrow{F_2' = F_2 - 3F_1} \begin{pmatrix} 2 & -6 & 18 \\ 0 & 18 & -48 \end{pmatrix} \xrightarrow[C_2' = C_2 + 3C_1]{C_3' = C_3 - 9C_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 18 & -48 \end{pmatrix} \\ &\xrightarrow{C_3' = C_3 + 3C_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 18 & 6 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 18 \end{pmatrix} \xrightarrow{C_3' = C_3 - 3C_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix} \end{aligned}$$

   Por tanto, la forma normal de G es:

   $$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix}$$

   Su rango es:

   $$3 - 2 = 1.$$

   Su descomposición cíclica es:

   $$G \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

   Su descomposición cíclica primaria es:

   $$G \cong \mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3.$$

Respecto a H, por el Primer Teorema de Isomorfía tenemos que:

$$\begin{aligned} H &= \mathbb{Z}^3/\langle(1,-9,3),(1,-7,1),(1,-1,1)\rangle \\ &\cong \left\langle a,b,c \;\middle|\; \begin{array}{rcl} a-9b+3c &=& 0 \\ a-7b+c &=& 0 \\ a-b+c &=& 0 \end{array} \right\rangle. \end{aligned}$$

Su matriz de relaciones es:

$$A_H = \begin{pmatrix} 1 & -9 & 3 \\ 1 & -7 & 1 \\ 1 & -1 & 1 \end{pmatrix}.$$

Calculamos su forma normal:

$$A_H = \begin{pmatrix} 1 & -9 & 3 \\ 1 & -7 & 1 \\ 1 & -1 & 1 \end{pmatrix} \xrightarrow{F_2'=F_2-F_1} F_3' = F_3 - F_1 \begin{pmatrix} 1 & -9 & 3 \\ 0 & 2 & -2 \\ 0 & 8 & -2 \end{pmatrix} \xrightarrow[C_2'=C_2+9C_1]{C_3'=C_3-3C_1}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -2 \\ 0 & 8 & -2 \end{pmatrix} \xrightarrow{F_3'=F_3-4F_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -2 \\ 0 & 0 & 6 \end{pmatrix} \xrightarrow{C_3'=C_3+C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Por tanto, la forma normal de H es:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Su rango es:

$$3 - 3 = 0.$$

Su descomposición cíclica es:

$$H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

Su descomposición cíclica primaria es:

$$H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3.$$

2. ¿Son isomorfos? ¿Lo son sus subgrupos de torsión?

   Como sus descomposiciones cíclicas y cíclicas primarias son distintas, G y H no son isomorfos. Sus subgrupos de torsión no obstante sí son isomorfos, ya que ambos son isomorfos a $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

3. ¿Cuántos elementos de orden 6 tiene H? ¿Y G?

   Tenemos que el grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ tiene los siguientes elementos de orden 6:

   $$(0,1,1),(0,1,2),(1,0,1),(1,0,2),(1,1,1),(1,1,2).$$

Por tanto, H tiene 6 elementos de orden 6 (las respectivas preimágenes de estos elementos en H). Por otro lado, como el único elemento de orden finito de $\mathbb{Z}$ es el elemento 0, $\mathbb{Z} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$ tiene los siguientes elementos de orden 6:

$$(0,0,1,1),(0,0,1,2),(0,1,0,1),(0,1,0,2),(0,1,1,1),(0,1,1,2)$$

Por tanto, G tiene también 6 elementos de orden 6 (las respectivas preimágenes de estos elementos en G).

4. ¿Cuántos grupos hay, salvo isomorfismos, con los mismos elementos que H?

   Sabemos que $|H| = 12 = 2^2 \cdot 3$.

Ejercicio 2.7.12.

1. Calcula la descomposición cíclica y cíclica primaria de todos los grupos abelianos no isomorfos de orden 484.

   Para encontrar los grupos abelianos de orden 484, comenzamos por descomponer 484 en factores primos:

$$484 = 2^2 \cdot 11^2.$$

   Los grupos abelianos de orden 484 se muestran en la Tabla 2.9.

	Fact. Inv.	**Div. element.**	**Desc. cíclica primaria**	**Desc. cíclica**
$\begin{pmatrix} 2^2 \\ 11^2 \end{pmatrix}$	$d_1 = 484$	$\{2^2; 11^2\}$	$C_4 \oplus C_{121}$	C_{484}
$\begin{pmatrix} 2 & 2 \\ 11^2 & 1 \end{pmatrix}$	$d_1 = 242$ $d_2 = 2$	$\{2; 2; 11^2\}$	$C_2 \oplus C_2 \oplus C_{121}$	$C_{242} \oplus C_2$
$\begin{pmatrix} 2^2 & 1 \\ 11 & 11 \end{pmatrix}$	$d_1 = 44$ $d_2 = 11$	$\{2^2; 11; 11\}$	$C_4 \oplus C_{11} \oplus C_{11}$	$C_{44} \oplus C_{11}$
$\begin{pmatrix} 2 & 2 \\ 11 & 11 \end{pmatrix}$	$d_1 = 22$ $d_2 = 22$	$\{2; 2; 11; 11\}$	$C_2 \oplus C_2 \oplus C_{11} \oplus C_{11}$	$C_{22} \oplus C_{22}$

Tabla 2.9: Grupos abelianos de orden 484.

2. Sea

$$G = \left\langle a, b, c \;\middle|\; \begin{array}{rcl} 2a + b + 4c & = & 0 \\ 2a + 2b + 6c & = & 0 \end{array} \right\rangle,$$

   y $H = \mathbb{Z}^2/K$, con K el subgrupo de $\mathbb{Z}^2$ generado por los pares $(2,3)$ y $(6,3)$. Razona, calculando las descomposiciones cíclica y cíclica primaria de ambos, que no son isomorfos.

   Comenzamos por G. Su matriz de relaciones es:

$$A_G = \begin{pmatrix} 2 & 1 & 4 \\ 2 & 2 & 6 \end{pmatrix}.$$

   Calculamos su forma normal:

$$A_G = \begin{pmatrix} 2 & 1 & 4 \\ 2 & 2 & 6 \end{pmatrix} \xrightarrow{C_1 \leftrightarrow C_2} \begin{pmatrix} 1 & 2 & 4 \\ 2 & 2 & 6 \end{pmatrix} \xrightarrow{F_2' = F_2 - 2F_1} \begin{pmatrix} 1 & 2 & 4 \\ 0 & -2 & -2 \end{pmatrix} \xrightarrow[C_2'=C_2-2C_1]{C_3' = C_3 - 4C_1}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & -2 \end{pmatrix} \xrightarrow{C_3' = C_3 - C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \end{pmatrix} \xrightarrow{C_2' = -C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

Por tanto, la forma normal de G es:

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

Su descomposición cíclica, que coincide con su descomposición cíclica primaria, es:

$$G \cong \mathbb{Z} \oplus \mathbb{Z}_2.$$

Respecto a H, por el Primer Teorema de Isomorfía tenemos que:

$$\begin{aligned} H &= \mathbb{Z}^2 / \langle (2,3), (6,3) \rangle \\ &\cong \left\langle a, b \;\middle|\; \begin{array}{rcl} 2a + 3b & = & 0 \\ 6a + 3b & = & 0 \end{array} \right\rangle. \end{aligned}$$

Su matriz de relaciones es:

$$A_H = \begin{pmatrix} 2 & 3 \\ 6 & 3 \end{pmatrix}.$$

Calculamos su forma normal:

$$A_H = \begin{pmatrix} 2 & 3 \\ 6 & 3 \end{pmatrix} \xrightarrow{C_1' = -(C_1 - C_2)} \begin{pmatrix} 1 & 3 \\ -3 & 3 \end{pmatrix} \xrightarrow{F_2' = F_2 + 3F_1} \begin{pmatrix} 1 & 3 \\ 0 & 12 \end{pmatrix} \xrightarrow{C_2' = C_2 - 3C_1} \begin{pmatrix} 1 & 0 \\ 0 & 12 \end{pmatrix}$$

Por tanto, la forma normal de H es:

$$\begin{pmatrix} 1 & 0 \\ 0 & 12 \end{pmatrix}$$

Su descomposición cíclica es:

$$H \cong \mathbb{Z}_{12}.$$

Su descomposición cíclica primaria es:

$$H \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3.$$

Como vemos, G y H tienen descomposiciones cíclicas y cíclicas primarias distintas, por lo que no son isomorfos.

Ejercicio 2.7.13.

1. Encuentra todos los grupos abelianos distintos, salvo isomorfismo, de orden 1176. Da para cada uno de ellos sus descomposiciones cíclica y cíclica primaria.

   Para encontrar los grupos abelianos de orden 1176, comenzamos por descomponer 1176 en factores primos:

   $$1176 = 2^3 \cdot 3 \cdot 7^2.$$

   Los grupos abelianos de orden 1176 se muestran en la Tabla 2.10.

	Fact. Inv.	Div. element.	Desc. cíclica primaria	Desc. cíclica
$\begin{pmatrix} 2^3 \\ 3 \\ 7^2 \end{pmatrix}$	$d_1 = 1176$	$\{2^3; 3; 7^2\}$	$C_8 \oplus C_3 \oplus C_{49}$	C_{1176}
$\begin{pmatrix} 2^2 & 2 \\ 3 & 1 \\ 7^2 & 1 \end{pmatrix}$	$d_1 = 588$ $d_2 = 2$	$\{2^2; 2; 3; 7^2\}$	$C_4 \oplus C_2 \oplus C_3 \oplus C_{49}$	$C_{588} \oplus C_2$
$\begin{pmatrix} 2 & 2 & 2 \\ 3 & 1 & 1 \\ 7^2 & 1 & 1 \end{pmatrix}$	$d_1 = 294$ $d_2 = 2$ $d_3 = 2$	$\{2; 2; 2; 3; 7^2\}$	$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_{49}$	$C_{294} \oplus C_2 \oplus C_2$
$\begin{pmatrix} 2^3 & 1 \\ 3 & 1 \\ 7 & 7 \end{pmatrix}$	$d_1 = 168$ $d_2 = 7$	$\{2^3; 3; 7; 7\}$	$C_8 \oplus C_3 \oplus C_7 \oplus C_7$	$C_{168} \oplus C_7$
$\begin{pmatrix} 2^2 & 2 \\ 3 & 1 \\ 7 & 7 \end{pmatrix}$	$d_1 = 84$ $d_2 = 14$	$\{2^2; 2; 3; 7; 7\}$	$C_4 \oplus C_2 \oplus C_3 \oplus C_7 \oplus C_7$	$C_{84} \oplus C_{14}$
$\begin{pmatrix} 2 & 2 & 2 \\ 3 & 1 & 1 \\ 7 & 7 & 1 \end{pmatrix}$	$d_1 = 42$ $d_2 = 14$ $d_3 = 2$	$\{2; 2; 2; 3; 7; 7\}$	$C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_7 \oplus C_7$	$C_{42} \oplus C_{14} \oplus C_2$

Tabla 2.10: Grupos abelianos de orden 1176.

2. Calcula las descomposiciones cíclica y cíclica primaria del grupo abeliano dado en términos de generadores y relaciones siguiente:

$$G = \left\langle x, y, z \;\middle|\; \begin{array}{ccc} 2x & = & 5y \\ 2y & = & 5z \\ 2z & = & 5x \end{array} \right\rangle.$$

¿Qué tipo de órdenes tienen sus elementos?

Su matriz de relaciones es:

$$A_G = \begin{pmatrix} 2 & -5 & 0 \\ 0 & 2 & -5 \\ -5 & 0 & 2 \end{pmatrix}.$$

Calculamos su forma normal:

$$A_G = \begin{pmatrix} 2 & -5 & 0 \\ 0 & 2 & -5 \\ -5 & 0 & 2 \end{pmatrix} \xrightarrow{F_3'=-(F_3+2F_1)} \begin{pmatrix} 2 & -5 & 0 \\ 0 & 2 & -5 \\ 1 & 10 & -2 \end{pmatrix} \xrightarrow{F_1 \leftrightarrow F_3} \begin{pmatrix} 1 & 10 & -2 \\ 0 & 2 & -5 \\ 2 & -5 & 0 \end{pmatrix} \xrightarrow{F_3'=F_3-2F_1}$$
$$\begin{pmatrix} 1 & 10 & -2 \\ 0 & 2 & -5 \\ 0 & -25 & 4 \end{pmatrix} \xrightarrow[C_2'=C_2-10C_1]{C_3'=C_3+2C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -5 \\ 0 & -25 & 4 \end{pmatrix} \xrightarrow{F_2'=-(F_2+F_3)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 23 & 1 \\ 0 & -25 & 4 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3}$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 23 \\ 0 & 4 & -25 \end{pmatrix} \xrightarrow{F_3'=-(F_3-4F_2)} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 23 \\ 0 & 0 & 117 \end{pmatrix} \xrightarrow{C_3'=C_3-23C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 117 \end{pmatrix}$$

Por tanto, la forma normal de G es:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 117 \end{pmatrix}$$

Su descomposición cíclica es:

$$G \cong \mathbb{Z}_{117}$$

Su descomposición cíclica primaria es:

$$G \cong \mathbb{Z}_9 \oplus \mathbb{Z}_{13}.$$

Estudiemos los órdenes de $\mathbb{Z}_9 \oplus \mathbb{Z}_{13}$.

- Estudiamos los órdenes de los elementos de $\mathbb{Z}_9$:

$$O(0) = 1$$
$$O(1) = O(2) = O(4) = O(5) = O(7) = O(8) = 9$$
$$O(3) = O(6) = 3$$

- Todos los elementos de $\mathbb{Z}_{13}$ excepto el elemento 0 tienen orden 13.
- Por tanto, $\mathbb{Z}_9 \oplus \mathbb{Z}_{13}$ tiene:
  - 1 elemento de orden 1 (el elemento $(0, 0)$),
  - 6 elementos de orden 9.
  - 2 elementos de orden 3.
  - 12 elementos de orden 13 (los elementos de la forma $(0, k)$ con $k \in \{1, 2, \ldots, 12\}$),
  - $2 \cdot 12 = 24$ elementos de orden $13 \cdot 3 = 39$.
  - $6 \cdot 12 = 72$ elementos de orden $9 \cdot 13 = 117$.

Como el orden de un elemento se mantiene por isomorfismos, G tiene:

- 1 elemento de orden 1 (el elemento 0),
- 6 elementos de orden 9.
- 2 elementos de orden 3.
- 12 elementos de orden 13 (los elementos de la forma $(0, k)$ con $k \in \{1, 2, \ldots, 12\}$),
- $2 \cdot 12 = 24$ elementos de orden $13 \cdot 3 = 39$.
- $6 \cdot 12 = 72$ elementos de orden $9 \cdot 13 = 117$.

Ejercicio 2.7.14. Calcular las descomposiciones cíclica y cíclica primaria del siguiente grupo abeliano dados en términos de generadores y relaciones:

$$G = \left\langle a, b, c, d \;\middle|\; \begin{array}{rcl} 9a + 9b + c + 8d & = & 0 \\ 63a - b + 63c + 64d & = & 0 \\ 56a - 8b + 64c + 56d & = & 0 \end{array} \right\rangle.$$

¿Tiene G elementos de orden infinito? ¿Y de orden finito? Calcular cuántos grupos abelianos no isomorfos hay con el mismo orden que la torsión de G.

Comenzamos por calcular la matriz de relaciones de G:

$$A_G = \begin{pmatrix} 9 & 9 & 1 & 8 \\ 63 & -1 & 63 & 64 \\ 56 & -8 & 64 & 56 \end{pmatrix}.$$

Calculamos su forma normal:

$$A_G = \begin{pmatrix} 9 & 9 & 1 & 8 \\ 63 & -1 & 63 & 64 \\ 56 & -8 & 64 & 56 \end{pmatrix} \xrightarrow{C_3 \leftrightarrow C_1} \begin{pmatrix} 1 & 9 & 9 & 8 \\ 63 & -1 & 63 & 64 \\ 64 & -8 & 56 & 56 \end{pmatrix} \xrightarrow{F_3'=F_3-F_2} \begin{pmatrix} 1 & 9 & 9 & 8 \\ 63 & -1 & 63 & 64 \\ 1 & -7 & -7 & -8 \end{pmatrix}$$
$$\xrightarrow[F_2'=F_2-63F_1]{F_3'=F_3-F_1} \begin{pmatrix} 1 & 9 & 9 & 8 \\ 0 & -568 & -504 & -440 \\ 0 & -16 & -16 & -16 \end{pmatrix} \xrightarrow{\cdots} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -568 & -504 & -440 \\ 0 & -16 & -16 & -16 \end{pmatrix} \xrightarrow{F_2'=-(F_2-35F_3)}$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 8 & -56 & -120 \\ 0 & -16 & -16 & -16 \end{pmatrix} \xrightarrow{F_3'=F_3+2F_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 8 & -56 & -120 \\ 0 & 0 & -128 & -256 \end{pmatrix} \xrightarrow[C_3'=C_3+7C_2]{C_4'=C_4+15C_2}$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & -128 & -256 \end{pmatrix} \xrightarrow[C_3'=-C_3]{C_4'=C_4-2C_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 128 & 0 \end{pmatrix}$$

Por tanto, la forma normal de G es:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 128 & 0 \end{pmatrix}$$

Su descomposición cíclica, que coincide con su descomposición cíclica primaria, es:

$$G \cong \mathbb{Z} \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{128}.$$

Por tanto, G tiene elementos de orden infinito (los de la forma $(k, 0, 0)$ con $k \in \mathbb{Z}^*$) y de orden finito (los de la forma $(0, k, l)$ con $k \in \{0, 1, \dots, 7\}$ y $l \in \{0, 1, \dots, 127\}$). La torsión de G es:

$$T(G) = \mathbb{Z}_8 \oplus \mathbb{Z}_{128}. \Longrightarrow |T(G)| = 8 \cdot 128 = 2^{10}$$

Por tanto, hay tantos grupos abelianos no isomorfos de orden 2^{10} como particiones del número 10 en sumandos. Probando con las particiones del número 10 (es tedioso, pero sencillo), llegamos a que hay 42 grupos abelianos no isomorfos de orden 2^{10}.

Ejercicio 2.7.15. Calcular las descomposiciones cíclica y cíclica primaria de todos los grupos abelianos no isomorfos de orden 13916. Identifica la componente 3−primaria de cualquiera de esos grupos.

Para encontrar los grupos abelianos de orden 13916, comenzamos por descomponer 13916 en factores primos:

$$13916 = 2^2 \cdot 7^2 \cdot 71.$$

	Fact. Inv.	Div. element.	Desc. cíclica primaria	Desc. cíclica
$\begin{pmatrix} 2^2 \\ 7^2 \\ 71 \end{pmatrix}$	$d_1 = 13916$	$\{2^2; 7^2; 71\}$	$C_4 \oplus C_{49} \oplus C_{71}$	C_{13916}
$\begin{pmatrix} 2 & 2 \\ 7^2 & 1 \\ 71 & 1 \end{pmatrix}$	$d_1 = 6958$ $d_2 = 2$	$\{2; 2; 7^2; 71\}$	$C_2 \oplus C_2 \oplus C_{49} \oplus C_{71}$	$C_{6958} \oplus C_2$
$\begin{pmatrix} 2^2 & 1 \\ 7 & 7 \\ 71 & 1 \end{pmatrix}$	$d_1 = 1988$ $d_2 = 7$	$\{2^2; 7; 7; 71\}$	$C_4 \oplus C_7 \oplus C_7 \oplus C_{71}$	$C_{1988} \oplus C_7$
$\begin{pmatrix} 2 & 2 \\ 7 & 7 \\ 71 & 1 \end{pmatrix}$	$d_1 = 994$ $d_2 = 14$	$\{2; 2; 7; 7; 71\}$	$C_2 \oplus C_2 \oplus C_7 \oplus C_7 \oplus C_{71}$	$C_{994} \oplus C_{14}$

Tabla 2.11: Grupos abelianos de orden 13916.

Los grupos abelianos de orden 13916 se muestran en la Tabla 2.11.

Como ninguno de los grupos abelianos de orden 13916 tiene un divisor elemental potencia de 3, entonces no tiene componente 3−primaria (es trivial), puesto que no hay grupos de orden potencia de 3.