Álgebra II

Examen VII

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra II
Examen VII

Los Del DGIIM, `losdeldgiim.github.io`

José Manuel Sánchez Varbas

Granada, 2025

Asignatura Álgebra II.

Curso Académico 2024-25.

Grado Doble Grado en Ingeniería Informática y Matemáticas.

Grupo Único.

Profesor Aurora Inés del Río Cabeza.

Descripción Convocatoria Ordinaria.

Fecha 18 de Junio de 2025.

Duración 2 horas y 30 minutos.

Ejercicio 1 (1 punto)**.** Prueba, utilizando el algoritmo explicado en clase, que la sucesión

$$3 \geq 3 \geq 2 \geq 2 \geq 2 \geq 2 \geq 2$$

es gráfica y, utilizando dicho algoritmo, encuentra un grafo en que los grados de sus vértices sean los términos de esa sucesión. Prueba que el grafo es plano y que satisface el teorema de la característica de Euler.

Ejercicio 2 (3 puntos)**.** Se considera el grupo diédrico

$$D_9 = \langle r, s \mid r^9 = s^2 = 1,\ rs = sr^8 \rangle$$

(a) Calcula el orden de cada uno de los elementos de D_9.

(b) Calcula el número de subgrupos de Sylow de D_9 y descríbelos.

(c) ¿Es D_9 resoluble? En caso afirmativo, calcula la longitud y los factores de composición de D_9.

(d) Demuestra que el centralizador de r^i, con $i = 1, \ldots, 8$, es el subgrupo $\langle r \rangle$.

(e) Calcula el centro de D_9.

(f) ¿Es normal el subgrupo $H = \langle s \rangle \subseteq D_9$? En caso contrario, calcula su normalizador en D_9.

(g) Consideremos el subgrupo $N = \langle r^3, s \rangle \subseteq D_9$, prueba que N es isomorfo a D_3.

(h) ¿Es N un subgrupo normal de D_9?

Ejercicio 3 (2 puntos)**.** Una presentación del grupo abeliano A está dada por:

$$A = \left\langle x, y, z, t \;\middle|\; \begin{array}{rcrcrcrl} 12x & + & 18y & + & 6z & & & = 0 \\ 9x & + & 9y & + & 9z & + & 6t & = 0 \\ 6x & + & 9y & + & 27z & + & 6t & = 0 \end{array} \right\rangle$$

(a) Calcula, de forma razonada, el rango (de la parte libre) y las descomposiciones cíclica y cíclica primaria de A y, si $T(A)$ denota el grupo de torsión de A, determina su longitud y sus factores de composición.

(b) Clasifica, dando sus descomposiciones cíclica y cíclica primaria, todos los grupos abelianos cuyo orden sea el orden de $T(A)$ e identifica cuál de ellos es justamente $T(A)$.

Ejercicio 4 (2 puntos)**.** Sea G un grupo de orden 28.

(a) Razona que G es el producto semidirecto $P_7 \rtimes P_2$ con P_7 y P_2 un 7-subgrupo y un 2-subgrupo de Sylow de G, respectivamente.

(b) Razona que si G tiene un elemento de orden 4, entonces hay exactamente dos productos semidirectos (no isomorfos) $P_7 \rtimes P_2$: uno de ellos abeliano y el otro no abeliano, da una presentación de este último.

(c) Concluye que hay sólo 4 grupos de orden 28, dos abelianos y dos no abelianos. Da las descomposiciones cíclicas de los abelianos y presentaciones de los no abelianos.

Ejercicio 5 (2 puntos)**.** Demuestra el Teorema de Cauchy. Concluye que, si G es finito, entonces G es un p-grupo si y sólo si su orden es una potencia de p.

Ejercicio 1. Aplicamos el Algoritmo de Havel-Hakimi, y posteriormente construimos el grafo correspondiente, que se muestra en la Figura 1.

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	Reordenamos los términos
			1	1	0	0	Eliminamos el 1 y restamos uno al término siguiente
				0	0	0	Obtenemos una sucesión gráfica

Por el Teorema de Havel-Hakimi, la sucesión de partida

$$3 \geq 3 \geq 2 \geq 2 \geq 2 \geq 2 \geq 2$$

es gráfica. Reconstruimos el grafo añadiendo un vértice y las correspondientes aristas en cada paso.

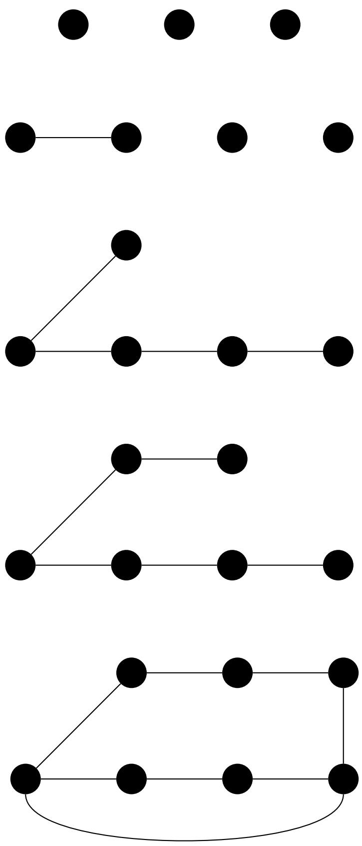

Figura 1: Grafo Correspondiente a la Sucesión Gráfica $3 \geq 3 \geq 2 \geq 2 \geq 2 \geq 2 \geq 2$

Como vemos, el grafo es plano, puesto que se da una representación en la que no se cruzan las aristas. Por último, verificar la característica de Euler significa que $v - a + c = 2$, es decir, la suma del número de vértices menos el número de aristas más el número de caras debe ser igual a 2. Tenemos $v = 7$ vértices, $a = 8$ aristas, y $c = 3$ caras (dos interiores, y la cara exterior), por lo que

$$v - a + c = 7 - 8 + 3 = 2$$

y se verifica la característica de Euler, como se pedía comprobar.

Ejercicio 2. Lo resolvemos por apartados.

(a) Calcula el orden de cada uno de los elementos de D_9.

En primer lugar, por el Teorema de Lagrange, vemos que

$$x \in D_9 \Longrightarrow O(x) \mid |D_9| = 18 \Longrightarrow O(x) \in \{1, 2, 3, 6, 9, 18\}$$

Ahora, antes de hallar el orden de cada elemento, probamos que

$$O(sr^i) = 2 \quad \forall i \in \{1, \dots, 9\}$$

Basta comprobar que

$$(sr^i)^2 = (sr^i)(sr^i) \overset{(*)}{=} (r^{-i}s)(sr^i) = r^{-i}(ss)r^i = r^{-i}(s^2)r^i \overset{(**)}{=} r^{-i}r^i = r^{-i+i} = 1$$

donde en $(*)$ se ha usado que $sr^i = r^{-i}s, \quad \forall i \in \{1, \dots, 9\}$, y en $(**)$ se ha usado que $s^2 = 1$. Como $sr^i \neq 1 \quad \forall i \in \{1, \dots, 9\}$, tenemos que

$$O(sr^i) = 2 \quad \forall i \in \{1, \dots, 9\}$$

Con lo anterior, ya podemos calcular el orden de cada elemento de D_9:

- $O(x) \neq 18 \quad \forall x \in D_9$, ya que en caso contrario habría un elemento de orden 18, lo cual implicaría que D_9 es cíclico, luego abeliano, cosa que sabemos que es falsa.
- $O(x) = 1 \iff x = 1$.
- $O(x) = 2 \iff x = sr^i \quad \forall i \in \{1, \dots, 9\}$.
- $O(x) \in \{3, 6, 9\} \iff x = r^i \quad \forall i \in \{1, \dots, 9\}$.
- Hallamos el orden de cada r^i:

$$O(r^i) = \frac{9}{\operatorname{mcd}(9, i)} \Longrightarrow \begin{cases} O(r^i) = 9 & i \in \{1, 2, 4, 5, 7, 8\} \\ O(r^i) = 3 & i \in \{3, 6\} \end{cases}$$

Vemos que no hay elementos de orden 6 en D_9.

(b) Calcula el número de subgrupos de Sylow de D_9 y descríbelos.

Factorizamos

$$|D_9| = 18 = 2 \cdot 3^2$$

Por el Primer Teorema de Sylow, tenemos garantizada la existencia de 2-subgrupos y 3-subgrupos de Sylow en D_9. Vamos a obtenerlos:

- 3-subgrupos de Sylow. Sea n_3 el número de 3-subgrupos de Sylow en D_9. Por el Segundo Teorema de Sylow, tenemos que

$$n_3 \mid 2 \quad \wedge \quad n_3 \equiv 1 \mod 3 \Longrightarrow n_3 = 1$$

Hay un único 3-subgrupo de Sylow, pongamos P_3, que además, por ser el único 3-subgrupo de Sylow, será normal, $P_3 \lhd D_9$, y $|P_3| = 3^2 = 9$, luego, por el Corolario del Teorema de Burnside, será abeliano (tiene orden cuadrado de un primo), y este debe ser $P_3 \cong \langle r \rangle \cong C_9$ (los únicos 9 elementos de D_9 que forman un grupo abeliano son los generados por las potencias de r. Además, P_3 es un 3-grupo, y como hemos visto en el apartado a) los únicos elementos de órdenes potencias de 3, $(1, 3, 9)$, en D_9 son las rotaciones $r^i \quad i \in \{1, \dots, 9\}$)

- 2-subgrupos de Sylow. Sea n_2 el número de 2-subgrupos de Sylow en D_9. Por el Segundo Teorema de Sylow, tenemos que

$$n_2 \mid 9 \quad \wedge \quad n_2 \equiv 1 \mod 2 \Longrightarrow n_2 \in \{1, 3, 9\}$$

Ahora, si P_2 es un 2-subgrupo de Sylow, entonces $|P_2| = 2$. En particular P_2 es cíclico, luego abeliano. Recordando que en el apartado a) habíamos probado que $O(x) = 2 \iff x = sr^i \quad \forall i \in \{1, \dots, 9\}$, y teniendo en cuenta que $sr^i \neq sr^j \quad \forall i \neq j \ i, j \in \{1, \dots, 9\}$, entonces, cada $\langle sr^i \rangle$ es un 2-subgrupo de Sylow distinto, y por tanto, tenemos que $n_2 = 9$, y no puede haber más 2-subgrupos de Sylow, por lo recién encontrado con el Segundo Teorema de Sylow. Así pues, hay nueve 2-subgrupos de Sylow, y cada uno es de la forma $\langle sr^i \rangle \quad i \in \{1, \dots, 9\}$.

(c) ¿Es D_9 resoluble? En caso afirmativo, calcula la longitud y los factores de composición de D_9.

En el apartado b) hemos visto que P_3 era el único 3-subgrupo de Sylow, y que, por tanto, era normal en D_9, $P_3 \lhd D_9$. Entonces D_9 sí es resoluble, ya que encontramos la siguiente serie de composición

$$D_9 \rhd P_3 \rhd \{1\}$$

que alcanza el $\{1\}$ y todos sus factores, $D_9/P_3 \cong C_2$ y $P_3/\{1\} \cong C_9$, son cíclicos, y por tanto, abelianos. Por definición, D_9 es resoluble, y vemos que la longitud de la serie es 2, y sus factores de composición son C_2 y C_9. Aunque no se pida, sus índices son, respectivamente, ${}^{|D_9|}/_{|P_3|} = 2$ y ${}^{|P_3|}/_{|\{1\}|} = 9$, por lo que la serie quedaría como sigue:

$$D_9 \overset{2}{\rhd} P_3 \overset{9}{\rhd} \{1\}$$

(d) Demuestra que el centralizador de r^i, con $i = 1, \dots, 8$, es el subgrupo $\langle r \rangle$.

Por definición, el centralizador en D_9 de r^i es, para cada $i \in \{1, \dots, 8\}$, el siguiente
$$C_{D_9}(r^i) = \{x \in D_9 : xr^i = r^i x\}$$

Vamos a probar que $C_{D_9}(r^i) = \langle r \rangle$ por doble contenido.

$\supseteq$) Sea $x \in \langle r \rangle \Longrightarrow x = r^j$ para cierto $j \in \{1, \dots, 9\}$. Entonces
$$r^j r^i = r^{j+i} = r^{i+j} = r^i r^j \Longrightarrow x \in C_{D_9}(r^i)$$

$\subseteq$) Sea $x \in C_{D_9}(r^i)$ para un $i \in \{1, \dots, 8\}$ fijo. Distinguimos en función de la forma de los elementos de D_9. Si $x \in D_9$, puede ser $x = r^k$ con $k \in \{1, \dots, 9\}$, o $x = sr^k$, con $k \in \{1, \dots, 9\}$.

- Si $x = r^k$ con $k \in \{1, \dots, 9\}$, entonces $x \in \langle r \rangle$, y ya hemos terminado este caso.
- Vamos ahora a llegar a contradicción con que $x \in C_{D_9}(r^i)$ si $x = sr^k$, con $k \in \{1, \dots, 9\}$. Por reducción al absurdo, supongamos que $\exists x = sr^k \in C_{D_9}(r^i)$. Entonces por estar x en el centralizador se verifica que $(sr^k)(r^i) = (r^i)(sr^k)$. Recordando que $sr^j = r^{-j}s \quad \forall j \in \{1, \dots, 9\}$, vemos que
$$\begin{cases} (sr^k)r^i = sr^{k+i} = r^{-(k+i)}s \\ r^i(sr^k) = r^i r^{-k} s = r^{(i-k)}s \end{cases}$$
  Igualando ambas expresiones, se obtiene
$$r^{-(k+i)}s = r^{(i-k)}s \overset{(1)}{\Longleftrightarrow} r^{-(k+i)} = r^{i-k} \overset{(2)}{\Longleftrightarrow} r^{(i-k)+(k+i)} = 1 \Longleftrightarrow r^{2i} = 1$$
  donde en (1) se ha multiplicado por la derecha en ambos miembros de la igualdad por s, y se ha usado que $s^2 = 1$, y en (2) se ha hecho lo mismo, pero con r^{k+i}.

  Ahora, como $O(r) = 9$, necesariamente debe ser $9 \mid 2i$, para algún $i \in \{1, \dots, 8\}$, pero como además $\text{mcd}(9, 2) = 1$, debe ser $9 \mid i$, con $i \in \{1, \dots, 8\}$. Contradicción que viene de suponer que $\exists x = sr^k \in C_{D_9}(r^i)$.

Como i era fijo, pero arbitrario, concluimos que $C_{D_9}(r^i) = \langle r \rangle$ para cada $i \in \{1, \dots, 8\}$.

(e) Calcula el centro de D_9.

Por definición, el centro de D_9 es

$$Z(D_9) = \{x \in D_9 : xy = yx \quad \forall y \in D_9\}$$

Sabemos que $Z(D_9) < D_9$ (además es normal), luego $\{1\} \subseteq Z(D_9)$. Veamos ahora que $Z(D_9) \subseteq \{1\}$, siguiendo un razonamiento similar al que se ha hecho en el apartado d), pero encontrando contraejemplos.

- Si $x = sr^k$ con $k \in \{1, \dots, 9\}$, entonces, si $x \in Z(D_9)$, en particular x conmutaría con r, pero:

$$(sr^k)r = sr^{k+1} = r^{-(k+1)}s$$
$$r(sr^k) = r(r^{-k}s) = r^{1-k}s$$

Igual que en el apartado d)

$$r^{-(k+1)}s = r^{1-k}s \iff r^{-(k+1)} = r^{1-k} \iff r^{(1-k)+(k+1)} = 1 \iff r^2 = 1$$

Cosa que sabemos que es falsa. Por tanto, $x \notin Z(D_9)$.

- Si $x = r^k$ con $k \in \{1, \dots, 9\}$, entonces, si $x \in Z(D_9)$, en particular, x conmutaría con s, luego $r^k s = sr^k$, pero, por otro lado, sabemos que $sr^k = r^{-k}s$, por lo que, igualando ambas expresiones de sr^k, llegamos a que:

$$r^k s = sr^k = r^{-k}s \iff r^k = r^{-k} \iff r^{2k} = 1$$

Aplicando el mismo argumento que en el apartado d), $9 \mid 2k \quad \wedge \quad \text{mcd}(9, 2) = 1 \Longrightarrow 9|k$, con $k \in \{1, \dots, 9\}$. Necesariamente entonces $k = 9$, y $x = r^9 = 1$.

Concluimos entonces que $Z(D_9) = \{1\}$. Nótese que si D_9 fuera un p-grupo, por el Teorema de Burnside, $Z(D_9)$ sería no trivial.

(f) ¿Es normal el subgrupo $H = \langle s \rangle \subseteq D_9$? En caso contrario, calcula su normalizador en D_9.

Usando la caracterización de los subgrupos normales, $H \lhd D_9 \iff \forall h \in H, \forall x \in D_9 \Longrightarrow xhx^{-1} \in H$. Tomando $s = h \in H$, y $r = x \in D_9$, vemos que

$$rsr^{-1} = rsr^8 = rr^{-8}s = r^{-7}s = sr^7 \notin H = \langle s \rangle = \{1, s\}$$

Por lo tanto, H no es normal en D_9. Por definición, su normalizador es

$$N_{D_9}(H) \overset{def}{=} \{x \in D_9 : xH = Hx\} = \{x \in D_9 : xHx^{-1} = H\}$$

Sabemos que el normalizador se caracteriza como el mayor subgrupo (en este caso de D_9) en el que H es normal. Así, $x \in N_{D_9}(H) \iff \forall h \in H, \exists h' \in H : xhx^{-1} = h'$

Basta comprobar la conjugación para los dos generadores de D_9, r y s. Como la conjugación preserva órdenes, y $O(s) = 2$, entonces $xsx^{-1} = s \iff xs = sx$. Distinguimos entre los dos posibles tipos de elementos de D_9, como venimos haciendo hasta ahora.

- Si $x = r^k$ con $k \in \{1, \dots, 9\}$, entonces

$$r^k s = sr^k = r^{-k}s \Longrightarrow r^{2k} = 1 \Longrightarrow 9 \mid 2k \Longrightarrow 9 \mid k$$

  lo cual implica que $k = 9$, y entonces $x = r^9 = 1$. Así, $1 \in N_{D_9}(H)$, y $r^k \notin N_{D_9}(H)$ para cada $k \in \{1, \dots, 8\}$.

- Si $x = sr^k$ con $k \in \{1, \dots, 9\}$, entonces

$$(sr^k)s = s(sr^k) \iff (sr^k)s = r^k \iff (r^{-k}s)s = r^k \iff r^{2k} = 1$$

  lo que implica que $9 \mid 2k \Longrightarrow 9 \mid k \Longrightarrow k = 9$, de donde $x = sr^9 = s$. Así, $s \in N_{D_9}(H)$, y vemos que, junto con el neutro, no hay más elementos en $N_{D_9}(H)$, por lo que concluimos que $N_{D_9}(H) = H = \langle s \rangle = \{1, s\}$

(g) Consideremos el subgrupo $N = \langle r^3, s \rangle \subseteq D_9$, prueba que N es isomorfo a D_3.

Vemos que los elementos de N serán de la forma $r^{3i} \quad i \in \{1, \dots, 9\}$, o bien $sr^{3i} \quad i \in \{1, \dots, 9\}$. Como por el apartado a) sabemos que $O(r^3) = 3$, entonces $|\langle r^3 \rangle| = 3$, y $\langle r^3 \rangle = \{1, r^3, r^6\}$. Ahora, añadiéndole el generador s, tenemos los otros 3 elementos, y podemos dar N por extensión: $N = \{1, r^3, r^6, s, sr^3, sr^6\}$ Como $sr^i \neq sr^j \quad \forall i \neq j,\ i, j \in \{1, \dots, 9\}$, también será $sr^{3i} \neq sr^{3j}$ puesto que $3i \neq 3j \iff i \neq j$, entonces los tres elementos s, sr^3, sr^6 son distintos, por lo que $|N| = 6 = 2 \cdot 3 = |D_3|$.

Buscamos aplicar el Teorema de Dyck, para poder encontrar un homomorfismo $f : N \to D_3$. Para ello, veamos que r^3 y s verifican las relaciones de r y s en D_3, que son $r^3 = 1$, $s^2 = 1$ y $rs = sr^{-1} = sr^2$.

$$(r^3)^3 = 1^3 = 1$$
$$s^2 = 1$$
$$r^3 s = s(r^3)^2 = sr^6 = r^{-6}s \iff r^3 = r^{-6} = r^{-3} \cdot r^{-3} = (r^3)^{-1} \cdot (r^3)^{-1} = 1$$

Donde hemos usado que $O(r^3) = 1$ en D_3 para la primera y tercera relación. Así pues, pues el Teorema de Dyck, existe un homomorfismo $f : N \to D_3$ de tal manera que $f(r^3) = r \in D_3$ y $f(s) = s \in D_3$. Como $D_3 = \langle r, s \rangle$, f es un epimorfismo y como $|N| = |D_3| = 6$, entonces f será un isomorfismo, luego

$$N \cong D_3$$

(h) ¿Es N un subgrupo normal de D_9?

Usando nuevamente la caracterización de subgrupo normal de un grupo, se tiene que $N \lhd D_9 \iff \forall n \in N, \forall x \in D_9 \Longrightarrow xnx^{-1} \in N$. Tomando $s = n \in N$, y $r = x \in D_9$, vemos que

$$rsr^{-1} = (sr^8)r^{-1} = sr^7 \notin N$$

porque $sr^i \in N \iff i \in \{3, 6, 9\}$. Como $i = 7$, $rsr^{-1} \notin N$, luego N no es un subgrupo normal de D_9.

Ejercicio 3. (a) Calcula, de forma razonada, el rango (de la parte libre) y las descomposiciones cíclica y cíclica primaria de A y, si $T(A)$ denota el grupo de torsión de A, determina su longitud y sus factores de composición.

La matriz de relaciones es $M = \begin{pmatrix} 12 & 18 & 6 & 0 \\ 9 & 9 & 9 & 6 \\ 6 & 9 & 27 & 6 \end{pmatrix} = (m_{ij})_{\substack{1\leq i\leq 3 \\ 1\leq j\leq 4}}$

Como $\operatorname{mcd}((m_{ij})_{\substack{1\leq i\leq 3 \\ 1\leq j\leq 4}}) = \operatorname{mcd}(12, 18, 6, 0, 9, 27) = 3$, buscamos que

$$m_{11} = 3 \quad \wedge \quad m_{1j} = 0 \quad \wedge \quad m_{i1} = 0, \quad i, j > 1$$

$$\begin{pmatrix} 12 & 18 & 6 & 0 \\ 9 & 9 & 9 & 6 \\ 6 & 9 & 27 & 6 \end{pmatrix} \xrightarrow{F_1 \leftrightarrow F_3} \begin{pmatrix} 6 & 9 & 27 & 6 \\ 9 & 9 & 9 & 6 \\ 12 & 18 & 6 & 0 \end{pmatrix} \xrightarrow[F_3-2F_1]{F_2-F_1} \begin{pmatrix} 6 & 9 & 27 & 6 \\ 3 & 0 & -18 & 0 \\ 0 & 0 & -48 & -12 \end{pmatrix} \xrightarrow{F_1 \leftrightarrow F_2}$$

$$\begin{pmatrix} 3 & 0 & -18 & 0 \\ 6 & 9 & 27 & 6 \\ 0 & 0 & -48 & -12 \end{pmatrix} \xrightarrow{C_3+6C_1} \begin{pmatrix} 3 & 0 & 0 & 0 \\ 6 & 9 & 63 & 6 \\ 0 & 0 & -48 & -12 \end{pmatrix} \xrightarrow{F_2-2F_1} \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 9 & 63 & 6 \\ 0 & 0 & -48 & -12 \end{pmatrix}$$

Ahora como $\operatorname{mcd}((m_{ij})_{\substack{2\leq i\leq 3 \\ 2\leq j\leq 4}}) = \operatorname{mcd}(9, 63, 6, 0, -48, -12) = 3$, buscamos que

$$m_{22} = 3 \quad \wedge \quad m_{2j} = 0 \quad \wedge \quad m_{i2} = 0, \quad i, j > 2$$

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 9 & 63 & 6 \\ 0 & 0 & -48 & -12 \end{pmatrix} \xrightarrow{C_2-C_4} \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 63 & 6 \\ 0 & 12 & -48 & -12 \end{pmatrix} \xrightarrow{F_3-4F_2} \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 63 & 6 \\ 0 & 0 & -300 & -36 \end{pmatrix} \xrightarrow[C_3-21C_2]{C_4-2C_2}$$

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -300 & -36 \end{pmatrix}$$

Por último, vemos que $\operatorname{mcd}((m_{ij})_{\substack{3\leq i\leq 3 \\ 3\leq j\leq 4}}) = \operatorname{mcd}(-300, -36) = 12$, buscamos que $m_{33} = 12$ y que $m_{34} = 0$

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -300 & -36 \end{pmatrix} \xrightarrow{-F_3} \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 300 & 36 \end{pmatrix} \xrightarrow{C_3-8C_4} \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 12 & 36 \end{pmatrix} \xrightarrow{C_4-3C_3}$$

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix}$$

De esta manera, como tenemos 4 generadores, y el rango de la matriz es $r = 3$, tendremos que

$$A \cong \mathbb{Z} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{12}$$

Esta es su descomposición cíclica. El rango de la parte libre es 1, y su grupo de torsión es:

$$T(A) \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_4) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9$$

con $|T(A)| = 3 \cdot 3 \cdot 12 = 108 = 2^3 \cdot 3^3$

La descomposición cíclica primaria de A es $A \cong \mathbb{Z} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9$

Ahora, hallamos la longitud y los factores de composición de $T(A)$. Para ello, usaremos que, dado un grupo, una serie normal es de composición si, y sólo si, sus factores son grupos simples, y que un grupo es abeliano y simple si, y sólo si, es de orden primo.

Definimos:

a) $G_0 = T(A) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

b) $G_1 = \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

c) $G_2 = \mathbb{Z}_4 \oplus \mathbb{Z}_3$

d) $G_3 = \mathbb{Z}_4$

e) $G_4 = 2\mathbb{Z}_4 \cong \mathbb{Z}_2$

f) $G_5 = \{0\}$

Cada cociente G_{k-1}/G_k es abeliano y simple para $k \in \{1, 2, 3\}$, porque es de orden primo 3, y para $k \in \{4, 5\}$, igual, pero siendo el orden primo 2.

Por construcción, tenemos la siguiente serie de composición:

$$G_0 \overset{3}{\rhd} G_1 \overset{3}{\rhd} G_2 \overset{3}{\rhd} G_3 \overset{2}{\rhd} G_4 \overset{2}{\rhd} G_5 = \{0\}$$

De esta manera, la longitud de composición es 5.

(b) Clasifica, dando sus descomposiciones cíclica y cíclica primaria, todos los grupos abelianos cuyo orden sea el orden de $T(A)$ e identifica cuál de ellos es justamente $T(A)$.

Sea G un grupo abeliano, verificando que $|G| = |T(A)| = 108 = 2^2 \cdot 3^3$.

Clasificamos:

Divisores elementales	desc. cíclica primaria	factores invariantes	desc. cíclica
$\{2^2, 3^3\}$	$C_4 \oplus C_{27}$	$d_1 = 2^2 \cdot 3^3 = 108$	C_{108}
$\{2^2, 3, 3^2\}$	$C_4 \oplus C_3 \oplus C_9$	$d_1 = 2^2 \cdot 3^2 = 36$ $d_2 = 3$	$C_{36} \oplus C_3$
$\{2^2, 3, 3, 3\}$	$C_4 \oplus C_3 \oplus C_3 \oplus C_3$	$d_1 = 2^2 \cdot 3 = 12$ $d_2 = 3$ $d_3 = 3$	$C_{12} \oplus C_3 \oplus C_3$
$\{2, 2, 3^3\}$	$C_2 \oplus C_2 \oplus C_{27}$	$d_1 = 2 \cdot 3^3 = 54$ $d_2 = 2$	$C_{54} \oplus C_2$
$\{2, 2, 3, 3^2\}$	$C_2 \oplus C_2 \oplus C_3 \oplus C_9$	$d_1 = 2 \cdot 3^2 = 18$ $d_2 = 2 \cdot 3 = 6$	$C_{18} \oplus C_6$
$\{2, 2, 3, 3, 3\}$	$C_2 \oplus C_2 \oplus C_3 \oplus C_3 \oplus C_3$	$d_1 = 2 \cdot 3 = 6$ $d_2 = 2 \cdot 3 = 6$ $d_3 = 3$	$C_6 \oplus C_6 \oplus C_3$

Por medio de los factores invariantes, vemos que el grupo que coincide con $T(A)$ es el que tiene factores invariantes $(3, 3, 12)$, que sería el resultante de considerar como divisores elementales, según la clasificación anterior, $\{2^2, 3, 3, 3\}$, es decir:

$$T(A) \cong C_{12} \oplus C_3 \oplus C_3 \cong C_3 \oplus C_3 \oplus C_{12}$$

Ejercicio 4. (a) Razona que G es el producto semidirecto $P_7 \rtimes P_2$ con P_7 y P_2 un 7-subgrupo y un 2-subgrupo de Sylow de G, respectivamente.

Como $|G| = 28 = 2^2 \cdot 7$, por el Primer Teorema de Sylow tenemos garantizada la existencia de 2-subgrupos de Sylow y 7-subgrupos de Sylow en G. Sea n_7 el número de 7-subgrupos de Sylow que hay en G. Entonces, por el Segundo Teorema de Sylow, tenemos que

$$n_7 \mid 4 \quad \wedge \quad n_7 \equiv 1 \mod 7 \Longrightarrow n_7 = 1$$

Hay un único 7-subgrupo de Sylow, pongamos P_7, que además, por ser el único 7-subgrupo de Sylow, será normal, $P_7 \lhd G$ con $|P_7| = 7$.

Ahora, consideramos un 2-subgrupo de Sylow, P_2. Buscamos aplicar la Propiedad Universal del Producto Semidirecto. Primero, veamos por reducción al absurdo que $P_2 \cap P_7 = \{1\}$. Si $P_2 \cap P_7 \neq \{1\} \Longrightarrow \exists x \in P_2 \cap P_7$ tal que $x \neq 1$. Entonces, por el Teorema de Lagrange, $O(x) \mid |P_2| = 4 \quad \wedge \quad O(x) \mid |P_7| = 7$, por lo que $O(x) \in \{1, 2, 4\} \cap \{1, 7\} \Longrightarrow O(x) = 1 \iff x = 1$, contradicción que viene de suponer que $P_2 \cap P_7 \neq \{1\}$. Así, debe ser $P_2 \cap P_7 = \{1\}$. Ahora, por el Segundo Teorema de Isomorfía:

$$\frac{P_2}{P_2 \cap P_7} \cong \frac{P_2 P_7}{P_7} \Longrightarrow |P_2 P_7| = \frac{|P_2||P_7|}{|P_2 \cap P_7|} = 4 \cdot 7 = 28 = |G|$$

de esta manera, $P_2 P_7 = G$, y como $P_7 \lhd G$, entonces G es el producto semidirecto de P_7 y P_2, es decir, $G \cong P_7 \rtimes P_2$.

(b) Razona que si G tiene un elemento de orden 4, entonces hay exactamente dos productos semidirectos (no isomorfos) $P_7 \rtimes P_2$: uno de ellos abeliano y el otro no abeliano, da una presentación de este último.

Sea $y \in G$, con $O(y) = 4$. Entonces, por el Teorema de Lagrange, $O(y) \mid |G|$, y vemos que $|\langle y \rangle| = 4 = |P_2|$, por lo que $\langle y \rangle$ es un 2-subgrupo de Sylow, y además $\langle y \rangle \cong C_4$. Consideramos $\langle y \rangle \cong P_2$, así como $P_7 \cong C_7$. Ahora, buscamos homomorfismos $\theta : C_4 \to \mathrm{Aut}(C_7)$. Primero veamos los generadores de C_7. Sea $a \in C_7$ tal que $\langle a \rangle \cong C_7$. Como $\varphi(7) = 6$, habrá 6 generadores, que son aquellos coprimos con 7, es decir:

$$\langle a^i \rangle \quad i \in \{1, \dots, 6\}$$

Para cada $i \in \{1, \dots, 6\}$, definimos entonces el automorfismo

$$\begin{array}{rccc} \varphi_i : & \langle a \rangle & \longrightarrow & \langle a \rangle \\ & a & \longmapsto & a^i \end{array}$$

Ahora, hay que ver cuáles de entre todos estos son automorfismos válidos. Trabajamos con $i \in \{1, \dots, 6\}$ fijo, y vemos que dado que $O(y) = 4 \Longrightarrow O(\theta(y)) \mid 4 \Longrightarrow O(\theta(y)) \in \{1, 2, 4\}$

Veamos que $O(\theta(y)) \neq 4$. Como $\theta(y) \in \mathrm{Aut}(C_7) \Longrightarrow O(\theta(y)) \mid |\mathrm{Aut}(C_7)| = 6$. Por tanto, tenemos que $O(\theta(y)) \mid 4 \quad \wedge \quad O(\theta(y)) \mid 6 \Longrightarrow O(\theta(y)) \mid \mathrm{mcd}(4, 6) = 2$. Así, $O(\theta(y)) \in \{1, 2\}$. Distinguimos en función de estos dos valores.

- Si $O(\theta(y)) = 1$, entonces $\theta(y) = \varphi_1$, y por tanto, θ es el homomorfismo trivial, y $G \cong P_7 \times P_2$, que es abeliano, por ser producto directo de abelianos ($P_7 \cong C_7$, luego cíclico, luego abeliano, y P_2 tiene orden cuadrado de un primo, luego, por el Corolario del Teorema de Burnside, es abeliano).
- Si $O(\theta(y)) = 2$, hay que comprobar cuáles son los automorfismos que tienen orden 2:

  $$(\varphi_i \circ \varphi_i)(a) = \varphi_i(\varphi_i(a)) = \varphi_i(a^i) = (a^i)^i = a^{i \cdot i} = a^{i^2}$$

  Ahora, $O(\varphi_i) = 2 \iff a^{i^2} = a \iff i^2 \equiv 1 \mod 7 \iff i \in \{1, 6\}$. Como $O(\theta(y)) \neq 1 \Longrightarrow i \neq 1$, luego $i = 6$ necesariamente, y el único automorfismo válido sería φ_6. Por tanto:

  $$yay^{-1} = \varphi_6(a) = a^6 = a^{-1} \Longrightarrow ya = a^{-1}y$$

  Así pues, obtenemos que G es isomorfo a un grupo no abeliano con la siguiente presentación $G \cong \langle a, y : a^7 = 1, y^4 = 1, ya = a^{-1}y \rangle$.

(c) Concluye que hay sólo 4 grupos de orden 28, dos abelianos y dos no abelianos. Da las descomposiciones cíclicas de los abelianos y presentaciones de los no abelianos.

Como $|G| = 28 = 2^2 \cdot 7$, y hemos visto en el apartado a) que $G \cong P_7 \rtimes P_2$, los posibles isomorfismos a grupos abelianos o no abelianos vendrán determinados por el homomorfismo que se tome, y de a quién sea isomorfo P_2. Como $|P_2| = 4$, hay dos posibles isomorfismos que son $P_2 \cong C_4$ o $P_2 \cong C_2 \times C_2 \cong V^{abs}$ (nótese que ambos isomorfismos son distintos, puesto que C_4 es cíclico, y V^{abs} no). También hemos visto en el apartado b) que los únicos homomorfismos válidos eran aquellos que llegaban a los automorfismos φ_1 (el trivial), o φ_6 (el no trivial). Con esto, distinguimos, en primer lugar, si se toma la acción trivial o no, y, en caso de no tomarse, del isomorfismo que se tome de P_2. Recordemos que dado un grupo G y un conjunto no vacío X, dar una acción de G sobre X equivale a dar un homomorfismo de grupos de G en $\text{Perm}(X)$ (este homomorfismo es la representación de G por permutaciones).

- Si se toma la acción trivial, entonces $G \cong P_7 \times P_2$, y como $P_7 \cong C_7$ y $P_2 \cong C_4$, entonces G es abeliano, por ser producto directo de grupos cíclicos, luego abelianos. Clasificamos como en el apartado b) del ejercicio 3:

Divisores elementales	desc. cíclica primaria	factores invariantes	desc. cíclica
$\{2^2, 7\}$	$C_4 \oplus C_7$	$d_1 = 2^2 \cdot 7 = 28$	C_{28}
$\{2, 2, 7\}$	$C_2 \oplus C_2 \oplus C_7$	$d_1 = 2 \cdot 7 = 14$ $d_2 = 2$	$C_{14} \oplus C_2$

- En caso de no tomar la acción trivial, distinguimos según los isomorfismos de P_2 que se tomen, $P_2 \cong C_4$ o $P_2 \cong V^{abs}$.
  - Si $P_2 \cong C_4$, entonces, por el apartado b), G es isomorfo a un grupo no abeliano con la presentación siguiente

$$G \cong \langle a, y : a^7 = 1, y^4 = 1, ya = a^{-1}y \rangle$$

  - Si $P_2 \cong C_2 \times C_2 \cong V^{abs}$, recordamos que V^{abs} se puede presentar como $V^{abs} = \langle b, c : b^2 = c^2 = 1, bc = cb \rangle = \{1, b, c, bc\}$ Sabemos que para $n \geqslant 3$, si $\theta : C_2 \to \text{Aut}(C_n)$, dado por $\theta(y)(x) = x^{-1} \quad \forall y \in C_2$, $\forall x \in C_n$, entonces $C_n \rtimes_\theta C_2 \cong D_n$. Este homomorfismo coincide con el homomorfismo $\theta : P_2 \to \text{Aut}(C_7)$, que llega al automorfismo φ_6, y entonces $G \cong P_7 \rtimes P_2 \cong C_7 \rtimes_\theta (C_2 \times C_2) \cong (C_7 \rtimes_\theta C_2) \times C_2 \cong D_7 \times C_2$, de tal manera que G no es abeliano, por no serlo D_7.

    La presentación de este último grupo no abeliano será entonces

$$G \cong \langle a, b, c : a^7 = 1, b^2 = c^2 = 1, bab^{-1} = a^{-1}, algo \rangle$$

    Como $\theta : V^{abs} \to \text{Aut}(C_7)$, entonces $\text{Im}(\theta) = \langle \varphi_6 \rangle$, y ya hemos visto que $O(\varphi_6) = 2$ en el apartado b), por lo que $|\langle \varphi_6 \rangle| = 2$, y entonces, por el Primer Teorema de Isomorfía:

$$\frac{V^{abs}}{\ker\theta} \cong \mathrm{Im}(\theta) \cong C_2 \Longrightarrow |\ker\theta| = \frac{|V^{abs}|}{|C_2|} = \frac{4}{2} = 2$$

Ahora, tomando $b, c \in V^{abs}$ los dos generadores, hay cuatro posibilidades para el par $(\theta(b), \theta(c))$:

- Si $\theta(b) = \theta(c) = \varphi_1$, estamos en el caso de la acción trivial, ya estudiado.
- Si $\theta(b) = \varphi_6$, entonces $\mathrm{Im}(\theta) = \langle\theta(b)\rangle$, y entonces $\theta(c) = \varphi_1$, luego $\ker(\theta) = \langle c\rangle$. En tal caso, como

  $$\ker\theta = \{h \in V^{abs} : \theta(h) = \varphi_1\} = \{h \in V^{abs} : \theta(h)(k) = k \quad \forall k \in P_7\} =$$
  $$= \{h \in V^{abs} : hkh^{-1} = k \quad \forall k \in P_7\}$$

  por estar $c \in \ker\theta$, tomando $a \in P_7$, se tiene que $cac^{-1} = a \iff ca = ac \iff [c, a] = 1$. Por la presentación de V^{abs}, ya sabemos que $bc = cb$ luego $[b, c] = [c, b] = 1$, y obtenemos la presentación final del último grupo no abeliano.

  $$G \cong \langle a, b, c : a^7 = 1, b^2 = c^2 = 1, bab^{-1} = a^{-1}, [c, a] = [c, b] = 1\rangle$$

- Si $\theta(c) = \varphi_6$, entonces $\mathrm{Im}(\theta) = \langle\theta(c)\rangle$, y entonces $\theta(b) = \varphi_1$, luego $\ker(\theta) = \langle b\rangle$, y el resultado que se obtendría sería el mismo que en el caso anterior cambiando los papeles de b con los de c.
- Si $\theta(b) = \theta(c) = \varphi_6$, entonces

  $$\theta(bc) = \theta(b)\theta(c) = \varphi_6^2 = \varphi_1$$

  donde en la primera igualdad se ha usado que θ es un homomorfismo, y en la tercera que $O(\varphi_6) = 2$. Entonces, $\ker(\theta) = \langle bc\rangle$, y $\mathrm{Im}(\theta) = \langle\varphi_6\rangle$ Definiendo $c' = bc$ y $b' = b$ como nuevos generadores, comprobamos que cumplen todas las relaciones: $O(b') = 2$, pues $b' = b$, y $O(b) = 2$. $O(c') = 2$, pues

  $$(c')^2 = (c')(c') = (bc)(bc) = bccb = bc^2b = b^2 = 1$$

  donde se han usado las relaciones de V^{abs}.

  Como $\theta(b') = \theta(b) = \varphi_6$, se sigue cumpliendo que $b'a(b')^{-1} = a^{-1}$.

  También se verifica que

  $$c'a(c')^{-1} = (bc)a(bc)^{-1} = (bc)a(c^{-1}b^{-1}) = b(cac^{-1})b^{-1} = b(a^{-1})b^{-1} =$$
  $$= (bab^{-1})^{-1} = (a^{-1})^{-1} = a$$

  Vemos por último que $[b', c'] = 1$, pues

  $$b'c' = b(bc) = c$$

  $$c'b' = (bc)b = (cb)b = c$$

donde en la penúltima igualdad se ha usado la relación de V^{abs}. En definitiva, la presentación resultante es la misma pero con otros nombres:

$$G \cong \langle a, b', c' : a^7 = 1, (b')^2 = (c')^2 = 1, (b')a(b')^{-1} = a^{-1}, [c', a] = [c', b'] = 1\rangle$$

Ejercicio 5. Primero definimos qué es un p-grupo.

Definición 0.1 (p-grupo)**.** Si p es un número primo, un grupo G se dice que es un p-grupo si todo elemento de G distinto del neutro tiene orden una potencia de p. Si G es un grupo, diremos que $H < G$ es un p-subgrupo si H es un p-grupo.

Necesitaremos el siguiente lema para la demostración:

Lema 0.1 (Relación Entre los Conjuntos Notables Orb y Stab de un G-conjunto)**.** *Sea G un grupo finito que actúa sobre X, entonces para cada $x \in X$, $Orb(x)$ es un conjunto finito y:*

$$|Orb(x)| = [G : Stab_G(x)]$$

En particular, el cardinal de la órbita es un divisor del orden de G.

Ahora enunciamos y demostramos el Teorema de Cauchy.

Teorema 0.2 (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, y, por tanto, tendrá un p-subgrupo de orden p.*

Demostración. Consideramos:

$$X = \{(a_1, \ldots, a_p) \in G^p : a_1 \cdots a_p = 1\}$$

Si $|G| = n$, entonces $X = n^{p-1}$, ya que elegimos libremente las $p - 1$ primeras coordenadas (variación con repetición):

$$a_1, \ldots, a_{p-1} \in G \quad \text{arbitrarios}$$

Y la última viene condicionada por:

$$a_p = (a_1, \ldots, a_{p-1})^{-1}$$

Sea ahora $\sigma = (1\ 2\ \cdots\ p) \in S_p$. Consideramos $H = \langle\sigma\rangle = \{1, \sigma, \ldots, \sigma^{p-1}\} \subseteq S_p$. Consideramos también la acción $ac : H \times X \to X$:

$$ac(\sigma^k, (a_1, \ldots, a_p)) = (a_{\sigma^k(1)}, \ldots, a_{\sigma^k(p)}) \quad \forall (a_1, \ldots, a_p) \in X, \quad \forall \sigma^k \in H$$

En efecto, es una acción, pues:

- Tomando como neutro $1 = \sigma^0$, tenemos que, para $x = (a_1, \ldots, a_p) \in X$ arbitrario:

$$ac(\sigma^0, (a_1, \ldots, a_p)) = (a_{\sigma^0(1)}, \ldots, a_{\sigma^0(p)}) = (a_1, \ldots, a_p)$$

  que es la identidad de X.

- Si tenemos $\sigma^k, \sigma^l \in H$, es decir, $k, l \in \{0, \dots, p-1\}$ arbitrarios, y $x = (a_1, \dots, a_p) \in X$, entonces:

$$ac(\sigma^k \sigma^l, x) = ac(\sigma^{k+l}, x) = (a_{\sigma^{k+l}(1)}, \dots, a_{\sigma^{k+l}(p)}) = (a_{\sigma^k(\sigma^l(1))}, \dots, a_{\sigma^k(\sigma^l(p))}) =$$

$$= ac(\sigma^k, (a_{\sigma^l(1)}, \dots, a_{\sigma^l(p)})) = ac(\sigma^k, ac(\sigma^l, x))$$

Por el Lema 0.1, tenemos que:

$$|\mathrm{Orb}(z)| = [H : \mathrm{Stab}_H(z)] = \frac{|H|}{|\mathrm{Stab}_H(z)|} \quad \forall z \in X$$

De donde tenemos que $|\mathrm{Orb}(a_1, \dots, a_p)|$ es un divisor de $H \quad \forall (a_1, \dots, a_p) \in X$. En dicho caso, $|\mathrm{Orb}(a_1, \dots, a_p)| \in \{1, p\}$, por ser $|H| = p$ (y ser p primo). Por tanto, las órbitas de un elemento serán unitarias o bien tendrán cardinal p.

Así, sean r el número de órbitas con un elemento, y s el número de órbitas con p elementos, entonces (con $|\Gamma| = s$):

$$n^{p-1} = |X| = |\mathrm{Fix}(X)| + \sum_{y \in \Gamma} |\mathrm{Orb}(y)| = r + \sum_{y \in \Gamma} p = r + sp$$

Veamos ahora cómo son los elementos de $\mathrm{Orb}(a_1, \dots, a_p)$:

$$\mathrm{Orb}(a_1, \dots, a_p) = \{{}^{\sigma^k}(a_1, \dots, a_p) : k \in \{0, \dots, p-1\}\} =$$

$$\{(a_1, \dots, a_p), (a_2, \dots, a_p, a_1), \dots, (a_p, a_1, \dots, a_{p-1})\}$$

Por tanto, la órbita será unitaria si, y sólo si, $a_1 = \dots = a_p$. Además, sabemos de la existencia de órbitas con un elemento ($r \geqslant 1$), como $\mathrm{Orb}(1, \dots, 1)$. Busquemos más: por hipótesis, $p|n$, y además $r = n^{p-1} - sp$, de donde $p|r$, luego $r \geqslant 2$, ya que lo divide un primo.

En conclusión, $\exists a \in G \setminus \{1\}$ de forma que $\mathrm{Orb}(a, \dots, a)$ es unitaria, de donde $a^p = 1$, luego $O(a)|p$, y sabemos que $O(a) \neq 1$ (porque $O(a) = 1 \iff a = 1$, y $a \in G \setminus \{1\}$). Así pues, debe ser $O(a) = p$.

Finalmente, sea $x \in \langle a \rangle \setminus \{1\}$, tenemos entonces que $1 \neq O(x)|p$, por lo que $O(x) = p$, y tenemos consecuentemente que todo elemento del subgrupo $\langle a \rangle$ es de orden p. En definitiva, $\langle a \rangle$ es un p-subgrupo de G de orden p, como queríamos probar. □

Ahora, concluimos que, si G es finito, entonces G es un p-grupo si y sólo si su orden es una potencia de p. Lo enunciamos como corolario:

Corolario 0.2.1 (Corolario del Teorema de Cauchy)**.** *Sea G un grupo finito y p un número primo:*

$$G \text{ es un } p\text{-subgrupo} \iff \exists n \in \mathbb{N} : |G| = p^n$$

Demostración. Lo probaremos por doble implicación:

$\Longleftarrow$) Si $|G| = p^n$ para cierto $n \in \mathbb{N}$, entonces tendremos que $O(x)|p^n$ para todo $x \in G$, de donde $O(x) = p^k$ para cierto $k \in \mathbb{N}$, luego G es un p-subgrupo por definición.

$\Longrightarrow$) Suponemos que q es un primo que divide al orden de $|G|$ (por el Teorema Fundamental de la Aritmética, todo número entero mayor que 1, en este caso, $|G| > 1$, tiene al menos un factor primo). Por el Teorema de Cauchy (Teorema 0.2), debe existir $x \in G$ de forma que $O(x) = q$. En tal caso, como G es un p-grupo (por hipótesis), $q = p^r$ para cierto $r \in \mathbb{N}$, de donde (dado que q y p son primos), $r = 1$ y $q = p$. De esta manera, el único primo que divide a $|G|$ es p, por lo que será $|G| = p^n$ para algún $n \in \mathbb{N}$, como queríamos probar.

$\square$