



# LISTA DE EJERCICIOS - ÁLGEBRA

## GEM - 2021

---

### Caleb - Michael

**Pregunta 1.** Sea  $p$  un número primo, pruebe que  $(\mathbb{Z}_p - \{\bar{0}\}, \cdot)$  es un grupo.

**Solución:** Consideremos  $\bar{a} \neq \bar{0}$  cualquiera, salvo representantes podemos considerar que  $a \in \{1, \dots, p-1\}$  y como  $p$  es primo entonces  $(a, p) = 1$ . Así existen  $x, y \in \mathbb{Z}$  tales que  $ax + py = 1$ . Esto implica que  $\bar{a}\bar{x} = \bar{1}$ , por lo que todo elemento no nulo tiene inverso, probando lo pedido.

**Pregunta 2.** Pruebe que:

$$D_{2n} = \langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle$$

donde  $a = s$  y  $b = sr$ .

**Solución.** Basta probar que las relaciones en cuestión son equivalentes a las vistas en la teoría.

- Si  $r^n = s^2 = 1$  y  $rs = sr^{-1}$  entonces se tiene que:

$$a^2 = s^2 = 1 \quad b^2 = (sr)^2 = sr sr = s^2 = 1 \quad (ab)^n = (s^2 r)^n = r^n = 1$$

- Si  $a^2 = b^2 = (ab)^n = 1$  entonces se tiene que:

$$s^2 = a^2 = 1 \quad r^n = (s^2 r)^n = (ab)^n = 1 \quad sr sr = 1 \implies rs = sr^{-1}$$

**Pregunta 3.** Pruebe que el grupo  $\text{GL}_2(\mathbb{Z}_2)$  no es abeliano y que tiene orden 6.

**Solución.** Los elementos de  $\mathbb{Z}_2$  son  $\{0, 1\}$ , haciendo cuentas se llega a que:

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

Para ver que no es un grupo abeliano resta ver que:

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

# Daniel - Cristopher

**Pregunta 1.** Consideremos  $\mathbb{Q}$  el conjunto de números racionales.

a) Considere la relación en  $\mathbb{Q}$  definida por:

$$a \sim b \Leftrightarrow a - b \in \mathbb{Z}$$

Pruebe que  $\sim$  es una relación de equivalencia.

b) Pruebe que  $\left(\frac{\mathbb{Q}}{\sim}, +\right)$  es un grupo abeliano con la operación:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right]$$

¿Es finito?

c) Considere  $p$  primo, pruebe que el conjunto:

$$\mathbb{Z}(p^\infty) = \left\{ \left[\frac{a}{b}\right] \in \frac{\mathbb{Q}}{\sim} : b = p^i, i \geq 0 \right\}$$

es un subgrupo de  $\frac{\mathbb{Q}}{\sim}$ .

**Solución.**

a) Es inmediato del hecho que  $0 \in \mathbb{Z}$  y que  $\mathbb{Z}$  es cerrado bajo la suma y producto.

b) Para ver que es un grupo abeliano resta ver que la operación está bien definido, pues las demás propiedades se heredan de la suma en  $\mathbb{Q}$ . Consideremos:

$$\frac{a}{b} \sim \frac{a'}{b'} \text{ y } \frac{c}{d} \sim \frac{c'}{d'}$$

Entonces se tiene que:

$$\frac{a}{b} + \frac{c}{d} - \left(\frac{a'}{b'} + \frac{c'}{d'}\right) \in \mathbb{Z} \implies \left[\frac{a}{b} + \frac{c}{d}\right] = \left[\frac{a'}{b'} + \frac{c'}{d'}\right]$$

c) Sean  $\left[\frac{a}{b}\right], \left[\frac{c}{d}\right] \in \mathbb{Z}(p^\infty)$ , se tiene entonces que  $b = p^i$  y  $d = p^j$  con  $i, j \geq 0$ . Luego:

$$\left[\frac{a}{b}\right] - \left[\frac{c}{d}\right] = \left[\frac{ad - bc}{bd}\right]$$

Como  $bd = p^{i+j}$  se tiene que la resta de estos elementos está en  $\mathbb{Z}(p^\infty)$  con lo que es un subgrupo. Note que es no vacío pues  $[a]$  es un elemento para cualquier  $a \in \mathbb{Z}$ .

**Pregunta 2.** Dado  $m \leq n$  pruebe que el número de ciclos de longitud  $m$  es:

$$\frac{n(n-1) \dots (n-m+1)}{m}$$

**Solución.** El número de posibilidades para escoger  $m$  números y definir la permutación  $(a_1 \dots a_m)$  es  $n(n-1)(n-2) \dots (n-m+1)$ . Sin embargo se sabe que:

$$(a_1 \dots a_m) = (a_2 a_3 \dots a_m a_1) = \dots = (a_m a_1 \dots a_{m-1})$$

Así para  $a_1, \dots, a_m$  escogidos, habrán  $m$  ciclos de longitud  $m$  que serán lo mismo. En otras palabras hemos contado  $m$  veces el número total de  $m$ -ciclos, osea:

$$(\text{número de m-ciclos})m = n(n-1)(n-2) \dots (n-m+1)$$

Así hemos obtenido lo pedido.

**Pregunta 3.** Para cada  $n$  definimos el conjunto:

$$U_n = \{z \in \mathbb{C}^* : z^n = 1\}$$

- a)  $U_n \subseteq U_m$  si y solo si  $n|m$ .
- b)  $U_n \cap U_m = U_d$  donde  $d = (m, n)$ .
- c) Sea  $H$  un subgrupo finito de  $(\mathbb{C}^*, \cdot)$ , pruebe que existen tal que  $H = U_n$ .

**Solución.**

- a) Supongamos que  $U_n \subseteq U_m$ , dado  $k \in \{0, 1, \dots, n-1\}$  se tiene que el número complejo  $e^{\frac{2\pi ki}{n}} \in U_n$ . Luego por hipótesis tenemos:

$$\left(e^{\frac{2\pi ki}{n}}\right)^m = \cos\left(\frac{2\pi km}{n}\right) + i \sin\left(\frac{2\pi km}{n}\right) = 1$$

Esto implica que  $\cos\left(2\pi k \frac{m}{n}\right) = 1$ , por lo que necesariamente  $m/n$  es un número entero. Recíprocamente, pongamos que  $m = nk$  con  $k$  un número entero. Si  $z \in U_n$  entonces:

$$z^m = (z^n)^k = 1$$

Por lo que  $z \in U_m$  y se tiene lo pedido.

b) Procederemos por doble inclusión:

( $\subseteq$ ) Sea  $z \in U_n \cap U_m$ , como  $d = (m, n)$  existen  $x, y$  enteros tal que  $d = mx + ny$ . Así tenemos que:  $z^d = z^{mx+ny} = (z^m)^x (z^n)^y = 1$ .

( $\supseteq$ ) Sea  $z \in U_d$ , como  $d$  divide a  $m$  y  $n$  se sigue que  $z^n = 1 = z^m$ .

c) Sea  $H$  un subgrupo finito díganos que tiene  $k$  elementos. Afirmamos que  $H = U_k$ , en efecto, veamos que  $H \subseteq U_k$  para esto primero probemos un resultado auxiliar.

**Lema:** Si  $G$  es abeliano y de orden  $n$ , para todo  $a \in G$  se tiene que  $a^n = 1$ .

En efecto, si  $a = 1$  lo que se pide es evidente. Supongamos que  $a \neq 1$  y que  $G = \{a_1, \dots, a_n\}$ . Los productos  $aa_i$  nos tiene que dar algún  $a_j$  con  $j \neq i$ , por lo que podremos reescribir  $G = \{aa_1, aa_2, \dots, aa_n\}$ . Realizando el producto de todos los elementos de  $G$  de ambas formas tenemos:

$$(a_1 \cdots a_n) = (aa_1)(aa_2) \cdots (aa_n) = a^n(a_1 \cdots a_n)$$

Cancelando se tiene que  $a^n = 1$ .

En nuestro caso  $H$  es un grupo finito de  $k$  elementos, por lo que cualquier  $h \in H$  cumple que  $h^k = 1$  y así  $h \in U_k$ . Finalmente como  $|U_k| = k$  entonces se sigue que  $H = U_k$ .

# Guido - Jhonatan

**Pregunta 1.** Sea  $G$  un grupo, pruebe lo siguiente:

- a) Si  $x^2 = 1$  para todo  $x \in G$ , entonces  $G$  es abeliano.
- b) Si  $G$  es abeliano pruebe que  $(ab)^n = a^n b^n$  para cualquier  $n \in \mathbb{Z}$  y  $a, b \in G$ . De un ejemplo de grupo no abeliano que no satisfaga lo anterior.

**Solución.**

- a) Sean  $x, y \in G$ , se tiene que:

$$y^{-1}xyx^{-1} = y^{-1}(\textcolor{red}{y}^2)xy(\textcolor{red}{x}^2)x^{-1} = yxyx = (yx)^2 = 1$$

Así  $y^{-1}xyx^{-1} = 1$  lo que implica que  $xy = yx$  y así  $G$  es abeliano.

- b) Primero veamos cuando  $n \in \mathbb{N}$ . Procederemos por inducción sobre  $n$ , el caso  $n = 1$  es evidente. Supongamos válido para  $n$ , tenemos:

$$(ab)^{n+1} = (ab)^n(ab) = a^n b^n(ab) = a^{n+1} b^{n+1}$$

Si  $n = 0$  se cumple de manera trivial y si  $n = -m$  con  $m \in \mathbb{N}$  tenemos:

$$(ab)^n = ((ab)^{-1})^m = (a^{-1}b^{-1})^m = a^{-m}b^{-m} = a^n b^n$$

Consideremos  $D_{2n}$ , basta ver que:

$$(\textcolor{red}{rs})^2 = \textcolor{red}{rsrs} = \textcolor{red}{sr}^{-1}rs = s^2 = 1 \quad \text{y} \quad \textcolor{red}{r}^2 s^2 = \textcolor{red}{r}^2 \neq 1$$

**Pregunta 2.** Sea  $n \geq 2$  y  $m \in \{1, \dots, n\}$ , pruebe que:

$$H = \{\sigma \in S_n : \sigma(m) = m\}$$

es un subgrupo de  $S_n$ .

**Solución.**  $H$  es no vacío pues la identidad está en  $H$ . Ahora, sean  $\sigma, \psi \in H$ , entonces:

$$(\sigma\psi^{-1})(m) = \sigma(m) = m$$

pues  $\psi^{-1}(m) = m$ . Así  $\sigma\psi^{-1} \in H$  demostrando lo pedido.

**Pregunta 3.** Un grupo  $H$  es finitamente generado si existe un conjunto finito  $S$  tal que  $H = \langle S \rangle$ . Pruebe que:

- a) Todo grupo finito es finitamente generado.
- b)  $\mathbb{Z}$  es finitamente generado.
- c) Todo subgrupo de  $(\mathbb{Q}, +)$  que es finitamente generado es cíclico.

### Solución.

- a) Resta ver que  $H = \langle H \rangle$ .
- b) Evidente pues  $\mathbb{Z} = \langle 1 \rangle$ .
- c) Sea  $H$  un subgrupo de  $\mathbb{Q}$  que es finitamente generado, digamos  $H = \langle q_1, \dots, q_n \rangle$ , donde los  $q_i$  son distintos. Siendo más específicos pongamos que:

$$q_i = \frac{a_i}{b_i}$$

Definamos dos números enteros como sigue:

$$a = \left( a_1 \left( \prod_{i \neq 1} b_i \right), a_2 \left( \prod_{i \neq 2} b_i \right), \dots, a_n \left( \prod_{i \neq n} b_i \right) \right) \quad \text{y} \quad b = \prod_{i=1}^n b_i$$

**Afirmación:**  $H = \left\langle \frac{a}{b} \right\rangle$ . En efecto, si  $h \in H$  entonces:

$$h = m_1 \left( \frac{a_1}{b_1} \right) + m_2 \left( \frac{a_2}{b_2} \right) + \dots + m_n \left( \frac{a_n}{b_n} \right)$$

donde  $m_i \in \mathbb{Z}$ . Operando estas fracciones tenemos que:

$$h = \frac{a_1 \left( \prod_{i \neq 1} b_i \right) m_1 + \dots + a_n \left( \prod_{i \neq n} b_i \right) m_n}{b_1 \dots b_n} = \frac{a(m_1 k_1 + \dots + m_n k_n)}{b_1 \dots b_n} = k \left( \frac{a}{b} \right)$$

donde los  $k_i$  son enteros. Esto prueba que  $H \subseteq \left\langle \frac{a}{b} \right\rangle$ . Para la otra inclusión, por la definición de  $a$  existen  $x_1, \dots, x_n$  enteros tales que:

$$a_1 \left( \prod_{i \neq 1} b_i \right) x_1 + \dots + a_n \left( \prod_{i \neq n} b_i \right) x_n = a$$

Esto implica que:

$$\frac{a}{b} = \frac{a_1 \left( \prod_{i \neq 1} b_i \right) x_1 + \dots + a_n \left( \prod_{i \neq n} b_i \right) x_n}{b_1 \dots b_n} = \frac{a_1 x_1}{b_1} + \dots + \frac{a_n x_n}{b_n} \in H$$

Así  $\left\langle \frac{a}{b} \right\rangle \subseteq H$  y esto prueba lo pedido.

# Juan Paucar - Marco

**Pregunta 1.** Consideremos  $G$  un grupo:

- a) Sea  $x \in G$  con  $|x| = n$ , pruebe que  $\{1, x, \dots, x^{n-1}\}$  son diferentes.
- b) Considere  $D_{2n}$ , halle el orden de  $\langle r \rangle$ .

**Solución.**

- a) Si existieran  $i, j$  con  $0 \leq i < j \leq n-1$  (por ejemplo) tales que  $x^i = x^j$ . Entonces  $x^{j-i} = 1$ , sin embargo  $j-i < n$  algo imposible. Esto prueba lo pedido.
- b) Por lo anterior el orden del subgrupo sería  $n$  pues  $|r| = n$ .

**Pregunta 2.** Considere el grupo  $S_5$ :

- a) Exprese

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

como producto de ciclos disjuntos. Indique la longitud de cada uno de estos.

- b) Halle el orden de  $\sigma$ .

**Solución.**

- a) Se tiene que  $\sigma = (135)(24)$  es la descomposición en ciclos disjuntos. La longitud de estos son 3 y 2.
- b) El orden de  $(135)$  es 3 y el orden de  $(24)$  es 2. Por esta razón el orden de  $\sigma$  es 6.

**Pregunta 3.** Pruebe que:

$$H(\mathbb{R}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

es un grupo llamado el grupo de Heisenberg.

**Solución.**  $H(\mathbb{R})$  es no vacío pues  $\text{Id} \in H(\mathbb{R})$ . Consideremos:

$$\begin{pmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix} \in H(\mathbb{R})$$

Un cálculo directo muestra que:

$$\begin{pmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a_2 & a_2 c_2 - b_2 \\ 0 & 1 & -c_2 \\ 0 & 0 & 1 \end{pmatrix}$$

Operando concluimos lo pedido:

$$\begin{pmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a_1 - a_2 & a_2 c_2 - b_2 - a_1 c_2 + b_1 \\ 0 & 1 & c_1 - c_2 \\ 0 & 0 & 1 \end{pmatrix} \in H(\mathbb{R})$$

# Miller

**Pregunta 1.** Sea  $G$  un grupo, pruebe lo siguiente:

- a) Si  $(ab)^2 = a^2b^2$  para todo  $a, b \in G$  pruebe que  $G$  es abeliano.
- b) Si  $(ab)^i = a^ib^i$  para todo  $a, b \in G$  y tres enteros consecutivos  $i$ , pruebe que  $G$  es abeliano.

**Solución.**

- a) Sean  $x, y \in G$  cualesquiera, basta usar la hipótesis y la propiedad cancelativa para probar lo pedido:

$$xyxy = (xy)^2 = x^2y^2 = xxyy \implies xy = yx$$

- b) Sean  $a, b \in G$  cualesquiera, entonces:

$$a^{i+1}b^{i+1} = (ab)^{i+1} = (ab)^i(ab) = a^ib^iab$$

$$a^{i+2}b^{i+2} = (ab)^{i+2} = (ab)^{i+1}(ab) = a^{i+1}b^{i+1}ab$$

En la primera ecuación multiplicamos por  $a$  (a la izquierda) y  $b$  (a la derecha) e igualando con la segunda ecuación obtenemos:

$$a^{i+1}b^{i+1}ab = a^{i+1}b^iab^2 \implies ba = ab$$

Esto prueba lo pedido.

**Pregunta 2.** Numere los vértices de un polígono regular de  $n$  lados ( $P_n$ ) por  $\{1, \dots, n\}$  (mantenga fija esta numeración). Para una simetría de  $P_n$  asocie una permutación  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  definida por:

$$\sigma(i) = j \Leftrightarrow s \text{ pone el vértice } i \text{ en el lugar del vértice } j$$

Denotamos por  $D_{2n}$  el conjunto de las permutaciones asociadas a cada simetría.

- a)  $D_{2n}$  es un grupo con la composición usual de funciones, además tiene orden  $2n$ . (Sugerencia: para encontrar el número total de simetrías debe hallar el número de formas que tiene de asignar los vértices 1 y 2 mediante estas. Para esto, dado  $i$  encuentre una simetría que envíe 1 a  $i$ , utilice la posición de los vértices para verificar que fijando este valor  $i$  existen dos simetrías más.)



- b) Sea  $r$  la permutación asociada a la rotación de  $2\pi/n$  y  $s$  la reflexión que deja el vértice 1 fijo. Pruebe que:

$$D_{2n} = \{1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$$

(Sugerencia: pruebe que  $r^n = s^2 = 1$ ,  $s \neq r^i$  y que  $sr^i \neq sr^j$ ).

- c) Del ítem a) concluya que  $D_{2n}$  es un subgrupo de  $S_n$ .

### Solución.

- a) El hecho que  $D_{2n}$  sea un grupo es evidente, la composición de funciones es cerrada y asociativa, el elemento neutro sería la identidad y el inverso la función inversa de la permutación.

Veamos ahora que el orden es  $2n$ , para esto procederemos como sigue.

- **Paso 1:** *Encontrar todas las maneras posibles en las que se puede mapear el par  $(1, 2)$  vía una simetría.* Veamos primero el caso del 1, este vértice se puede enviar a cualquier  $i \in \{1, \dots, n\}$  pues simplemente debemos hacer una rotación de  $2\pi(i-1)/n$ . Así 1 tiene  $n$  posibles imágenes vía simetrías. Ahora fijemos un  $i$ , el vértice 2 solo tiene dos posibilidades o bien es  $i-1$  o bien es  $i+1$  (recordar que una simetría es una isometría que mapea el polígono en si mismo, así debe llevar vértices en vértices y estos deben dejar la distancia entre ellos constante). En resumidas cuentas el par  $(1, 2)$  tiene  $2n$  posibilidades.
- **Paso 2:** *Para una elección de las imágenes del par  $(1, 2)$  existe una sola simetría.* En efecto, consideremos por ejemplo que  $\sigma(1) = i$  y  $\sigma(2) = i+1$  con  $n = i+j$ . Entonces como  $\sigma$  es una simetría necesariamente  $\sigma(3) = i+2$  así hasta llegar a  $\sigma(j+1) = n$ . Nuevamente como  $\sigma$  es simetría tenemos que  $\sigma(j+2) = 1, \sigma(j+3) = 2, \dots, \sigma(j+i) = i-1$ . Esta simetría está determinada por  $i$ , así es única.
- **Paso 3.** De los pasos anteriores tenemos que hay  $2n$  formas de asignar 1 y 2, cada asignación determina una única simetría por lo que exactamente hay  $2n$  simetrías, es decir  $|D_{2n}| = 2n$ . (**Observación:** cuando nos referimos a simetrías es a la permutación asociada)

- b) Las permutaciones vienen dadas de la siguiente manera:

$$r = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix} = (1 \ 2 \ \cdots \ n-1 \ n)$$

Si  $n = 2k$  es par (la línea de simetría pasa por 1 y  $k+1$  que son vértices opuestos):

$$s = \begin{pmatrix} 1 & 2 & 3 & \cdots & k+1 & \cdots & n \\ 1 & n & n-1 & \cdots & k+1 & \cdots & 2 \end{pmatrix} = (2 \ n)(3 \ n-1) \cdots (k \ k+2)$$

Si  $n = 2k + 1$  es impar (la línea de simetría pasa por 1 y el punto medio del lado opuesto):

$$s = \begin{pmatrix} 1 & 2 & 3 & \cdots & \cdots & n \\ 1 & n & n-1 & \cdots & \cdots & 2 \end{pmatrix} = (2 \ n)(3 \ n-1) \cdots (k \ k+3)(k+1 \ k+2)$$

La permutación  $r$  es un  $n$ -ciclo por lo que no es complicado probar que  $|r| = n$ . La permutación  $s$  es un producto de 2-ciclos, por lo que  $|s| = 2$ . Así, tenemos que:

$$\langle r \rangle = \{1, r, \dots, r^{n-1}\} \quad \text{y} \quad \langle s \rangle = \{1, s\}$$

Para probar lo pedido, vamos a encontrar  $2n$  simetrías distintas, como ya vimos que el orden de  $D_{2n}$  es  $2n$  estas simetrías conformarán todo el grupo. Ya hemos encontrado  $n$ , las potencias de  $r$  y una más que sería  $s$  ( $r \neq s$ ). Encontremos las demás.

**Afirmación:**  $s \neq r^i$  para todo  $i$ . El caso  $i = n$  es evidente pues  $r^n = 1 \neq 2$  veamos el caso en que  $i \neq n$ . Supongamos lo contrario, entonces existe algún  $i \in \{1, \dots, n-1\}$  tal que  $s = r^i$ . Como  $s(2) = n$  entonces  $r^i(2) = n$ , el único caso posible es que  $i = n - 2$  pues:

$$r^i(2) = \begin{cases} i+2 & \text{si } i \neq n-1 \\ 1 & \text{si } i = n-1 \end{cases}$$

Como  $s(n) = 2$  entonces  $r^i(n) = 2$  pero  $r^{n-2}(n) = n-2$  así el único caso en el que se da esto es cuando  $n = 4$ . En el caso del cuadrado tenemos:

$$s = (2 \ 4) \quad \text{y} \quad r = (1 \ 2 \ 3 \ 4)$$

y un cálculo directo muestra que  $s \neq r^2$  y  $s \neq r^3$ . Entonces no existe ese tal  $i$  por lo que  $s \neq r^i$ .

**Afirmación:**  $sr^i \neq sr^j$  para todo  $i \neq j$ . En efecto supongamos que existan  $i \neq j$  tal que  $sr^i = sr^j$ . Así  $sr^i(1) = sr^j(1)$ . Luego operando:

$$sr^i(1) = s(i+1) = n+1-i \quad \text{y} \quad sr^j(1) = s(j+1) = n+1-j$$

Si igualamos tendríamos  $j = i$  algo imposible.

De las dos afirmaciones obtenemos  $n$  elementos más que serían:

$$sr, sr^2, \dots, sr^{n-1}$$

Así hemos encontrado  $2n$  elementos distintos, probando lo pedido.

c) Es evidente pues  $D_{2n}$  está formado por permutaciones.

**Pregunta 3.** Pruebe que:

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$$

es un subgrupo de  $\text{GL}_2(\mathbb{R})$ .

**Solución.** Claramente  $G \subseteq \text{GL}_2(\mathbb{R})$  pues el determinante de cada matriz es no nulo, ya que  $a, c \neq 0$ . Además  $\text{Id} \in G$  por lo que  $G$  es no vacío.

Sean dos matrices:

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} \in G$$

Entonces:

- El producto:

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix} \in G$$

- El inverso:

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}^{-1} = \begin{pmatrix} 1/a_1 & -b_1/a_1 c_1 \\ 0 & 1/c_1 \end{pmatrix} \in G$$

Esto prueba lo pedido.