1.2. Generadores. Grupos cíclicos, diédricos y cuaterniones

Sistemas de generadores

Sean $(G, *)$ un grupo y $R \subseteq G$ un subconjunto no vacío de G.
El menor subgrupo de $(G, *)$ que contiene a R se denomina el **subgrupo generado por** R:

$$\langle R \rangle = \{a_1^{r_1} * \cdots * a_n^{r_n} : \text{ donde } a_i \in R, r_i \in \mathbb{Z}, \text{ y } n \in \mathbb{N}\}$$

- Un conjunto $R \subseteq G$ es un **sistema de generadores** del grupo $(G, *)$ si verifica que $G = \langle R \rangle$.
- El grupo $(G, *)$ es **cíclico** si tiene un sistema de generadores con un único elemento:

$$\exists\, g \in G \quad \text{tal que} \quad G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

Orden de un elemento

Sean $(G, *)$ un grupo y $a \in G$.
Se llama **orden de** a al menor entero positivo $r \in \mathbb{Z}^+$ tal que $a^r = e_G$. Se escribe $|a| = r$.
Si para todo $n \in \mathbb{Z}^+$ se verifica que $a^n \neq e_G$, se dice que el orden de a es infinito y se escribe $|a| = \infty$.

Orden de un elementos y orden del subgrupo que genera

Sean $(G, *)$ un grupo y $a \in G$. El orden de a coincide con el orden del subgrupo cíclico que genera:

$$|a| = |\langle a \rangle|$$

Orden de elementos de un grupo cíclico

Sea $(G, *)$ un grupo cíclico de orden n, y sea $g \in G$ un generador de G

1. Para todo $k \in \mathbb{Z}$, se verifica que $g^k = e_G \Leftrightarrow n$ divide a k
2. El orden de $g^k \in G$ es: $|g^k| = \frac{n}{\mathrm{mcd}(k,n)}$.

Propiedades de grupos cíclicos

1. Todo grupo cíclico es abeliano.
2. Todo subgrupo de un grupo cíclico es cíclico.

Grupo de cuaterniones y grupos diédricos

- Se llama **grupo de cuaterniones** Q_8 al grupo generado por dos elementos de orden 4, $a, b \in Q_8$ tales que $ba = a^{-1}b$ y $b^2 = a^2$.

$$Q_8 = \langle a, b : |a| = 4, b^2 = a^2, ba = a^{-1}b \rangle$$

- Para todo $n > 2$, se llama **grupo diédrico** D_n al grupo de las simetrías de un polígono regular de n lados. Su orden es $2n$ y está generado por un elemento $a \in D_n$ de orden n y un elemento $b \in D_n$ de orden 2 tales que $ba = a^{-1}b$.

$$D_n = \langle a, b : |a| = n, |b| = 2, ba = a^{-1}b \rangle$$

  Por analogía se define $D_2 = \langle a, b : |a| = 2, |b| = 2, ba = a^{-1}b \rangle$, que también recibe el nombre de **grupo cuatro de Klein**

Grupo cuatro de Klein $D_2 = \langle a, b : a^2 = e, b^2 = e, ba = ab \rangle$

$*$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$$

Grupo $D_4 = \langle a, b : a^4 = e, b^2 = e, ba = a^{-1}b \rangle$

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

$$\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$$

Grupo $Q_8 = \langle a, b : a^4 = e, b^2 = a^2, ba = a^{-1}b \rangle$

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

$$\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \rangle$$

Grupo $W_8 = \langle a, b : a^4 = e, b^2 = e, ba = ab \rangle$

$*$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	ab	a^2b	a^3b	e	a	a^2	a^3
ab	ab	a^2b	a^3b	b	a	a^2	a^3	e
a^2b	a^2b	a^3b	b	ab	a^2	a^3	e	a
a^3b	a^3b	b	ab	a^2b	a^3	e	a	a^2

$$\langle \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$$

Diagrama de Cayley de un grupo

Sea $(G, *)$ un grupo finito con elementos $G = \{a_1, \cdots, a_n\}$ y sea $R \subset G$ un conjunto generador del grupo. El digrafo $\mathrm{Cay}(G, R)$ con conjunto de vértices $\{a_1, \cdots, a_n\}$ y conjunto de aristas $\{(a, a * r) \in G \times G : a \in G, r \in R\}$, se denomina digrafo de Cayley del grupo.

1.2. Problemas

1. Dado un grupo $(G, *)$, demostrar que para todos $a, b, g \in G$ se verifica:

   a) $|a| = |a^{-1}|$
   b) $|a| = |g^{-1}ag|$
   c) $|ab| = |ba|$

2. Qué orden puede tener el elemento $a \in G$ si $a^{24} = e$.

3. Sea $(G, *)$ un grupo y sean $a, b \in G$ tales que $b \neq e$. Si $|a| = 2$ y $b^2 = aba$ ¿qué puede decirse sobre el orden de b?

4. Sea $(G, *)$ un grupo y sean $a, b \in G$ tales que $b \neq e$

   a) Demostrar que si $aba^{-1} = b^k$ entonces $a^r ba^{-r} = b^{k^r}$
   b) Si $|a| = 5$ y $b^2 = aba^{-1}$ ¿qué puede decirse sobre el orden de b?

5. Escribir al menos 5 elementos de cada uno de los siguientes subgrupos cíclicos:

   a) $\langle 25 \rangle \ \leq (\mathbb{Z}, +)$
   b) $\langle \frac{1}{2} \rangle \ \leq (\mathbb{Q}^*, \cdot)$
   c) $\langle \pi \rangle \ \leq (\mathbb{R}^*, \cdot)$

6. Indicar cuáles de los siguientes grupos son cíclicos y obtener sus generadores.
   $(H_1, *_1) = (\mathbb{Z}, +)$ $\quad$ $(H_2, *_2) = (\mathbb{Q}, +)$ $\quad$ $(H_3, *_3) = (\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot)$ $\quad$ $(H_4, *_4) = (6\mathbb{Z}, +)$
   $(H_5, *_5) = (\{6^n : n \in \mathbb{Z}\}, \cdot)$

7. Encontrar un generador de cada uno de los siguientes subgrupos de $(\mathbb{Z}_{12}, +_{12})$:
   a) $\langle 2, 3 \rangle$ $\quad$ *b*) $\langle 4, 6 \rangle$ $\quad$ *c*) $\langle 6, 8, 10 \rangle$

8. Se considera el grupo $G = \langle g \rangle = \{e = g^6, a_1 = g, a_2 = g^2, a_3 = g^3, a_4 = g^4, a_5 = g^5\}$. Calcular los subgrupos $\langle a_2 \rangle$, $\langle a_3 \rangle$, $\langle a_4 \rangle$, $\langle a_5 \rangle$. ¿Cuáles son los generadores de G?

9. Obtener el orden de cada uno de los elementos del grupo $(\mathbb{Z}_2 \times \mathbb{Z}_4, +)$ y encontrar un generador en caso de que fuera cíclico o un conjunto generador en caso de no ser cíclico.

10. Encontrar el número de generadores de los grupos cíclicos de órdenes 6, 8, 12 y 60.

11. Demostrar que si $(G, *)$ es un grupo que no tiene subgrupos propios no triviales, entonces es cíclico.

12. Demostrar que si $(G, *)$ es un grupo que no tiene subgrupos propios no triviales, entonces su orden es primo.

13. Encontrar el número de elementos de cada uno de los subgrupos cíclicos indicados:

    a) $H_a = \langle 25 \rangle \leq \mathbb{Z}_{30}$
    b) $H_b = \langle 30 \rangle \leq \mathbb{Z}_{42}$
    c) $H_c = \langle i \rangle \leq \mathbb{C}^* = \mathbb{C} - \{0\}$
    d) $H_d = \langle \frac{1+i}{\sqrt{2}} \rangle \leq \mathbb{C}^* = \mathbb{C} - \{0\}$
    e) $H_e = \langle i+1 \rangle \leq \mathbb{C}^* = \mathbb{C} - \{0\}$

14. Sea $n \in \mathbb{N}$, demostrar que para todo k divisor n, el grupo $(\mathbb{Z}_n, +_n)$ tiene un único subgrupo de orden k, que es $H_k = \langle \frac{n}{k} \rangle$.

15. Sea H un subgrupo propio de $(\mathbb{Z}, +)$. Estudiar si puede determinarse el subgrupo H en cada uno de los siguientes casos:

    a) Si $18, 30, 40 \in H$
    b) Si $12, 30, 54 \in H$

16. Dibujar el diagrama de Cayley de los grupos D_2, D_4, Q_8 y W_8.

17. Demostrar que se cumple que $Y^2 = J^2 = K^2 = -q_0$, $YJ = K$, $JK = Y$, $KY = J$, $JY = -K$, $KJ = -Y$, y $YK = -J$. Obtener el orden de cada elemento y un conjunto generador del grupo $(\mathcal{Q}, \cdot)$. $\mathcal{Q} = \{q_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$
$-q_0 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, -Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, -J = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, -K = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\}$.

18. Describir el grupo de simetrías de un rectángulo y encontrar un conjunto generador.

19. Describir el grupo de simetrías de un rombo y encontrar un conjunto generador.

20. Se considera el grupo diédrico $(D_n, \circ)$, $D_n = \langle a, b : |a| = n, b^2 = e, ba = a^{-1}b \rangle$.

    a) Demostrar que $ba^r = a^{-r}b$ para todo $0 \leq r < n$
    b) Demostrar que todo elemento de la forma $a^r b$ tiene orden 2
    c) Encontrar el centro de D_n

21. Encontrar en cada caso, un grupo con las condiciones requeridas:

    a) G contiene elementos a y b tales que $|a| = |b| = 2$ y $|ab| = 3$
    b) G contiene elementos a y b tales que $|a| = |b| = 2$ y $|ab| = 4$
    c) G contiene elementos a y b tales que $|a| = |b| = 2$ y $|ab| = 5$

22. Demostrar que D_6 tiene un subgrupo de orden 4

23. Demostrar que D_3 no tiene un subgrupo de orden 4