1.2. Generadores. Grupos cíclicos, diédricos y cuaterniones

Sistemas de generadores

Sean $(G,*)$ un grupo y $R \subsetneq G$ 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 $R \subsetneq G$ 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: $|g^k| = \frac{n}{\text{mcd}(k,n)}$.

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 $ba = a^{-1}b$.

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

$$\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

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

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

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

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

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

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

Diagrama de Cayley de un grupo

Sea $(G, *)$ un grupo finito con elementos $G = \{a_1, \dots, a_n\}$ y sea $B \subset G$ ...

1.3. Grupos de permutaciones

Sea X un conjunto no vacío, se llama **grupo simétrico** $(S_X, \circ)$ al grupo formado por las aplicaciones biyectivas en X, con la operación composición de aplicaciones. En particular si $X = \{1, 2, 3, \cdots, n\}$ el grupo se nota por $(S_n, \circ)$ y se denomina **grupo de permutaciones**.
Todo elemento del grupo $(S_n, \circ)$ recibe el nombre de **permutación**.
Sea $\sigma \in S_n$, se dice que σ es un **ciclo** de longitud r si existen $a_0, \cdots, a_{r-1} \in \{1, \cdots, n\}$ tales que $\sigma(a_0) = a_1$, $\sigma(a_1) = a_2$, $\cdots, \sigma(a_{r-2}) = a_{r-1}$, $\sigma(a_{r-1}) = a_0$, y para todo $k \in \{1, \cdots, n\}$ tal que $k \notin \{a_0, \cdots, a_{r-1}\}$ se verifica que $\sigma(k) = k$. La notación de dicho ciclo es $\sigma = (a_0, a_2, \cdots, a_{r-1})$.

Dos ciclos $\sigma \in S_n$ y $\tau \in S_n$ se dice que son **disjuntos** si ninguno de los elementos del conjunto $\{1, 2, ..., n\}$ aparece en la notación de ambos. Los ciclos de longitud 2 se denominan **transposiciones**.

Propiedades

1. Los ciclos disjuntos conmutan: Si $\sigma, \tau \in S_n$ son dos ciclos disjuntos entonces $\sigma\tau = \tau\sigma$.
2. El orden de un ciclo es su longitud

Formas de expresar una permutación

1. Toda permutación $\sigma \in S_n$ se puede expresar como **producto de ciclos disjuntos**.
2. Toda permutación $\sigma \in S_n$, con $n \geq 2$, se puede expresar como **producto de transposiciones**.

Lema 1. Reordenación de componentes en transposiciones

Dado un producto de $r > 0$ transposiciones: $\tau_1\tau_2...\tau_r$, siempre existe otro producto de transposiciones $\sigma_1\sigma_2...\sigma_s$ con $s \equiv r \mod 2$, $\tau_1\tau_2...\tau_r = \sigma_1\sigma_2...\sigma_s$, y verificando una de las siguientes condiciones:

- $s < r$ y la componente a de $\tau_r = (a, b)$ no aparece en ninguna transposición σ_i para $i \in \{1, ..., s\}$
- $s \leq r$ y la componente a de $\tau_r = (a, b)$ sólo aparece en la transposición σ_1.

Lema 2. La identidad como producto de transposiciones

La identidad de S_n, para $n \geq 2$, sólo puede descomponerse como producto de un número par de transposiciones.

Teorema. Paridad de una permutación

Si $\sigma \in S_n$ se puede expresar como producto de r transposiciones y como producto de s transposiciones entonces $r + s$ es par.

Definición. Permutaciones pares e impares

Una **permutación** de S_n es **par** o **impar** según pueda ser expresada como el producto de un número par o de un número impar de transposiciones respectivamente.

1.4. Isomorfismos en grupos

Dos grupos $(G, *_1)$ y $(G', *_2)$ son **isomorfos**, y se escribe $G \approx G'$, si existe una aplicación biyectiva $\phi : G \to G'$ tal que para todos $x, y \in G$ se verifica que

$$\phi(x *_1 y) = \phi(x) *_2 \phi(y)$$

La aplicación ϕ se denomina **isomorfismo de grupos**

Isomorfismos en grupos cíclicos

1. Todo grupo cíclico $(G, *)$ de orden infinito, es isomorfo a $(\mathbb{Z}, +)$
2. Todo grupo cíclico $(G, *)$ de orden n, es isomorfo a $(\mathbb{Z}_n, +_n)$

Producto de grupos cíclicos

El grupo $(\mathbb{Z}_m \times \mathbb{Z}_n, +_m \times +_n)$ es isomorfo a $(\mathbb{Z}_{mn}, +_{mn})$ si y sólo si $\mathrm{mcd}(m, n) = 1$

Definición de producto directo interno

Sea $(G, *)$ un grupo y sean $H \leq G$ y $K \leq G$.
Se dice que el grupo G es **producto directo interno de los subgrupos** H y K si se verifica que:

1. $H \cap K = \{e\}$
2. $G = HK = \{h * k : h \in H, k \in K\}$
3. Los elementos de H y de K conmutan: $\forall\, h \in H, k \in K$ es $h * k = k * h$

Relación entre producto directo interno y producto directo

Si $(G, *)$ es producto directo interno de los subgrupos H y K entonces $G \approx H \times K$

Teorema de Cayley

Todo grupo de orden $n \in \mathbb{N}$ es isomorfo a un grupo de permutaciones.