Universidad de Granada

Doble Grado en Ingeniería Informática y Matemáticas

Álgebra II

Autor:
Jesús Muñoz Velasco

Curso 2024-2025

Índice general

1. Tema 1: Combinatoria y Teoría Elemental de Grafos

1.1. Definiciones

Definición 1.1. Una **permutación** de un conjunto X es una aplicación biyectiva $f : X \to X$.

El conjunto de todas las permutaciones de un conjunto X se denota $Perm(X)$. En particular, si $X = \{1, 2, \ldots, n\}$ el conjunto de permutaciones se representa por S_n y su cardinal es $n!$. (importa el orden)

Definición 1.2. Se llaman **variaciones sin repetición** de n elementos, tomados de m en m a cada una de las posibles elecciones ordenadas de m elementos distintos, dentro de un conjunto de n elementos. (también importa el orden)

$$V_n^m = \frac{n!}{(n-m)!}$$

Definición 1.3. Se llaman variaciones con repetición de n elementos, tomados de m en m ...

En ambos casos, dos posibles elecciones se diferencian, bien en la naturaleza de los elementos elegidos, bien en el orden en el que se han elegido.

Definición 1.4. Una combinación sin repetición de n elementos tomados de m en m, con $1 \leqslant m \leqslant n$, es cada uno de los posibles subjconjuntos de m elementos distintos dentro de un conjunto de n elementos. (no importa el orden).

El número de combinaciones sin repetición de n elementos tomados de m a m,

Definición 1.5. Una combinación con repetición de n elementos tomados de m a m, $1 \leqslant m \leqslant n$, es cada una de las posibles agrupaciones de m elementos (no necesariamente distintos).

En ambos casos se tiene por tanto que dos combinaciones son iguales si y solo si tienen los mismos elementos sin importar el orden.

Proposición 1.1.

Definición 1.6. Dado $\{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$, un ciclo de longitud m es una permutación $\sigma \in S_n$ tal que

$$\begin{cases} \sigma(a_i) = a_{i+1} & i = 1, \ldots, a_{m-1} \\ \sigma(a_m) = a_1 & \\ \sigma(a_j) = a_j & \forall a_j \notin \{a_1, a_2, \ldots, a_m\} \end{cases}$$

y lo representamos $\sigma = (a_1, a_2, \ldots, a_m)$, pero también por $(a_2, \ldots, a_m, a_1) = (a_3, \ldots, a_1, a_2) = \cdots = (a_m, a_1, \ldots, a_{m-1})$. Hay m formas distintas de representar un ciclo de longitud m.

Ejemplo. En S_3, los ciclos de longitud 2 son $(12), (13), (23)$ y los de longitud 3 son $(123), (231), (312); (132), (321), (213)$. El número de ciclos de longitud 3, como importa el orden, hay $V_3^3 = P_3$, pero cada ciclo de longitud 3 se expresa de 3 maneras distintas, el número de ciclos es $\dfrac{V_3^3}{3} = 2$.

En general, el número de ciclos de longitud m en $S_n = \dfrac{V_n^m}{m}$

1.2. Grafos. Introducción

Definición 1.7. Un grafo G es un par (V, E), donde V y E son dos conjuntos, junto con una aplicación $\gamma_G : E \to \{\{u, v\} : u, v \in V\}$. V es el conjunto de vértices, E el conjunto de lados o aristas y γ_G aplicación de incidencia.

Ejemplo. Puentes de Konigsberg

Definición 1.8. Un grafo dirigido u orientado es un par (V, E), donde V y E son conjuntos, junto con dos aplicaciones $s, t : E \to V$.

Definición 1.9. Sea $G = (V, E)$ un grafo con aplicación de incidencia γ_G. Un subgrafo de G es un nuevo grafo $G' = (V', E')$ donde $V' \subseteq V$, $E' \subseteq E$ y se verifica que $\gamma_{G'}(e) = \gamma_G(e)$ para cualquier $e \in E'$.

Definición 1.10. Un subgrafo G' se dice pleno si se verifica que $e \in E$ es tal que $\gamma(e) \subseteq (V')$ entonces $e \in E'$, es decir, si tiene todas las aristas de G que unen vértices de V'.

Definición 1.11. Un camino es una sucesión finita de lados con la propiedad de que cada lado acaba donde empieza el siguiente.

Un camino de longitud n es una sucesión de lados $e_1, e_2, \ldots, e_n$, junto con una sucesión de vértices $v_0, v_1, \ldots, v_n$ tales que $\gamma_G(e_i) = \{v_{i-1}, v_i\}$.

Un camino puede ser:

- •) **Cerrado:** camino que empieza y acaba en el mismo vértice.
- •) **Recorrido:** camino sin lados repetidos.
- •) **Simple:**

Sea G un grafo, si existe un camino de u a v, entonces existe un camino simple de u a v.

Sea G un frafo y sean u y v dos vértices distintos. Si existen dos caminos simples distintos de u a v, entonces hay un ciclo en G.

En el conjunto de vértices de un frafo G se puede establecer la siguiente relación binaria R (que es de equivalencia)

$$u, v \in V, uRv \iff \text{existe un camino de } u \text{ a } v$$

Definición 1.12. Un grafo se dice conexo si todo par de vértices están relacionados por la relación anterior, es decir, están conectados por un camino. El conjunto cociente V/R es unitario.

Definición 1.13. Sea G un grafo cuyo conjunto de vértices es $V = \{v_1, v_2, \ldots, v_n\}$. Se define su matriz de adyacencia como la matriz $A \in M_n(\mathbb{N})$ cuyo coeficiente a_{ij} es el número de aristas que unen v_i con v_j.

Propiedades. Para un grafo sin lazos y no dirigido se verifica que:

- •) los elementos de la diagonal principal son todos 0
- •) es simétrica
- •) la matriz de adyacencia no es única, depende de la ordenación de los vértices (se pasa de una a otra mediante una permutación, matriz invertuble con un 1 por fila y los demás ceros)
- •) toda matriz cuadrada con coeficientes en $\mathbb{N}$ es la matriz de adyacencia de algún grafo
- •)

Teorema 1.2. Sea G un grafo y A su matriz de adyacencia. En la posición ij de la matriz A^k aparece el número de caminos de longitud k que unen v_i y v_j.

Se demuestra por inducción sobre n.

Definición 1.14. Sea G un grafo cuyo conjunto de vértices es $V = \{v_1, v_2, \ldots, v_n\}$. Se define su **matriz de incidencia** como la matriz $A \in M_{n\times m}(\mathbb{N})$ cuyo coeficiente a_{ij} vale 1 si $v_i \in \gamma_G(e_j)$ y 0 en otro caso.

Propiedades.

- •) La matriz de incidencia no es única, depende de la ordenación de los vértices.
- •) Si un grafo tiene lados paralelos

Ejemplo. Supongamos que tenemos la siguiente matriz de adyacencia:

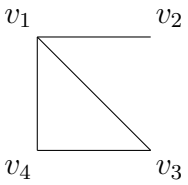
$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Entonces el grafo asociado será:

Ejemplo. Supongamos que tenemos la siguiente matriz de adyacencia:

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

Entonces el grafo asociado será:



Definición 1.15. Dos grafos G y G' se dice que son isomorfos si existen dos biyecciones $h_V : V \to V'$, $h_E : E \to E'$ tales que para cada lado $e \in E$ se verifica que $\gamma'_G(h_E(e)) = \{\}$

Definición 1.16. Una propiedad se dice invariante por isomorfismo si dados dos grafos isomorfos G y G', uno satisface la propiedad si y solo si lo satisface el otro. Los dos primeros invariantes son el número de vértices y el número de lados.

Definición 1.17. Sea G un grafo y v un vértice de G se define el grado de v, y lo denotaremos por $gr(v)$, como el número de lados que son incidentes en v. Denotaremos mediante $D_k(G)$ al número de vértices de V de grado k. A la sucesión $D_0(G), D_1(G), \ldots, D_k(G), \ldots$ la llamaremos sucesión de grados del grafo.

Observación. El grado de un vértice es un invariante por isomorfismos, esto es, $gr(v) = gr(h_V(v))$.

Observación. Las sucesiones de grados de dos grafos isomorfos son iguales.

Propiedades.

- **•)** La relación entre grados y lados la podemos expresar como

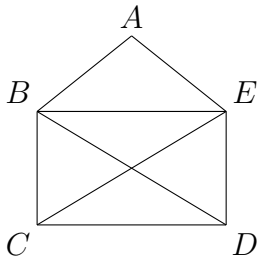
$$\sum_i gr(v_i) = 2 \cdot l$$

  con $l = |E|$ el número de lados.

- **•)** En un grafo, el número de vértices de grado impar es par.

Definición 1.18. Un grafo se dice que es regular si todos los vértices tienen el mismo grado.

Ejercicio 1.2.1. (Ejercicio 5 de la relación)



Definición 1.19. Se llama grafo completo de n vértices y se denota K_n al grafo (con n vértices) que no tiene lados paralelos, y dados dos vértices hay un lado que los une. $|V| = n$; $|E| = \frac{1}{2}(n-1) \cdot n$.

Su matriz de adyacencia vale 0 en la diagonal principal y 1 en el resto (de forma que haya $n-1$ unos en cada fila).

Definición 1.20. Sea $G = (V, E)$ un grafo. Se dice que G es bipartido si podemos descomponer V en dos subconjuntos disjuntos V_1 y $V2$ de manera que todo lado incide en un vértice de V_1 y en un vértice de V_2. $|V| = |V_1| + |V_2|$.

Definición 1.21. Un grafo $G = (V, E)$ se dice bipartido completo si es bipartido y para cada $v_1 \in V_1$ y $v_2 \in V_2$ existe un único lado $e \in E$ tal que $\gamma(e) = \{v_1, v_2\}$. Se denotan mediante $K_{n,m}$, donde $n = |V_1|$ y $m = |V_2|$. En este cado, $|V| = m + n$ y $|E| = m \cdot n$.

Definición 1.22. Un grafo $G = (V, E)$ se dice ciclo con n vértices si cada vértice es incidente únicamente con los vértices anterior y posterior. $|V| = n$ y $|E| = n$. Se denota mediante C_n.

Definición 1.23. Un grafo $G = (V, E)$ se dice rueda con n vértices si cada vértice es incidente únicamente con los vértices anterior y posterior y con un tercer vértice central. $|V| = n + 1$ y $|E| = 2n$. Se denota mediante W_n.

Definición 1.24. Sean $d_1, d_2, \ldots, d_n \in \mathbb{N}$. Decimos que la sucesión $d_1, d_2, \ldots, d_n$ es una sucesión gráfica si existe un grafo G sin lazos, ni lados paralelos con n vértices $\{v_1, v_2, \ldots, v_n\}$ y tal que $gr(v_i) = d_i$. Diremos que G es una realización de la sucesión $d_1, d_2, \ldots, d_n$.

Teorema 1.3. (Havel-Hakini)
Sea $d_1, d_2, \ldots, d_n$ una sucesión de números naturales ordenada ($d_1 \geqslant d_2 \geqslant \ldots \geqslant d_n$) y con $d_1 < n$. Entonces $d_1, d_2, \ldots, d_n$ es una sucesión gráfica si y solo si $d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, \ldots, d_n$ es una sucesión gráfica.

Definición 1.25. Un camino de Euler en un grafo G es un recorrido en el que aparecen todos los lados.

Definición 1.26. Un circuito de Euler es un camino de Euler cerrado .

Definición 1.27. Un grafo G es un grafo de Euler si es conexo y tiene un circuito de Euler.

Teorema 1.4. Un grafo conexo es de Euler si y solo si todos sus vértices son de grado par.

Demostración.

⇒) Supongamos que G es conexo y es de Euler. Sea α un circuito de Euler y para cada vez que pasamos por un vértice le estamos añadiendo un grado 2 al vértice. Como cada lado aparece una sola vez, entonces el grado es múltiplo de 2.

⇐) Se hace por inducción. Veamos qué ocurre para el caso $n = 4$. Hagamos la siguiente partición:

$$\begin{aligned}\sigma_1 &= v_1e_1v_2e_2v_3e_6v_1\\ \sigma_2 &= v_3e_3v_4e_4v_5e_1v_3\\ \sigma_3 &= v_2e_9v_4e_{10}v_1e_3v_3v_2\end{aligned}$$

y hacemos el siguiente circuito, conectando los anteriores por v_3 y v_4:

$$\sigma = v_3e_6v_1e_1v_2e_2v_3e_3v_4e_{10}v_1e_5v_5e_8v_2e_9v_4e_4v_5e_7v_3$$

□

2. Tema 2: Grupos. Definición, generalidades y ejemplos

Definición 2.1. Sea G un conjunto, una **operación binaria** en G es una aplicación

$$\begin{aligned} * : G \times G &\to G \\ (a, b) &\mapsto a * b = a \cdot b = ab \end{aligned}$$

Ejemplo.

1. Suma y producto en $\mathbb{N}, \mathbb{Z}, \mathbb{R}$
2. Dado X un conjunto, $\mathcal{P}(X)$, $\cup, \cap$ son operaciones binarias.

Definición 2.2. Un **monoide** es un conjunto no vacío junto con una operación binaria verificando:

i) La propiedad asociativa: $(x * y) * z = x * (y * z)$

ii) Existencia de elemento neutro: $\exists e \in G$ tal que $e * x = x \quad \forall x \in G$

Lema 2.1. En un monoide el neutro es único.

Ejemplo.

1. $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \times, 1)$
2. $(\mathcal{P}(X), \cap, X)$, $(\mathcal{P}(X), \cup, \emptyset)$

Definición 2.3. Un **grupo** es un conjunto no vacío junto con una operación binaria verificando:

i) La propiedad asociativa: $(x * y) * z = x * (y * z)$

ii) Existencia de elemento neutro: $\exists e \in G$ tal que $e * x = x \quad \forall x \in G$

iii) Existencia de elemento simétrico: $\forall x \in G \;\; \exists x' \in G$ tal que $x * x' = e$

y si además se cumple que

iv) Propiedad conmutativa: $x * y = y * x \;\; \forall x, y \in G$

Entonces G es un **grupo abeliano**.

Observación.

1. $(G, *, e) \rightsquigarrow G$
2. Notación multiplicativa:
   - •) $x * y = xy$
   - •) Neutro $\rightsquigarrow 1$
   - •) simétrico $\rightsquigarrow$ inverso x^{-1}
3. Notación aditiva:
   - •) $x + y$
   - •) Neutro $\rightsquigarrow 0$
   - •) simétrico $\rightsquigarrow$ opuesto $-x$

Ejemplo.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la suma son grupos abelianos.
2. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con el producto son grupos abelianos.
3. $\{1, -1, i, -i\} \subset \mathbb{C}$ con el producto es un grupo abeliano.
4. $(\mathcal{M}_2(\mathbb{R}), +)$ es un grupo abeliano
5. $GL_2(\mathbb{R})$ el grupo lineal de orden 2 con el producto es un grupo (pero no abeliano, ya que el producto de matrices no es conmutativo).
$$GL_2(\mathbb{R}) = \{A \in \mathcal{M}_2(\mathbb{R}) \text{ tal que } \det(A) \neq 0\}$$
6. $\mathbb{Z}_n$ con la suma es un grupo abeliano.
7. $U(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n \text{ tal que } m.c.d(a, n) = 1\}$ con la multiplicación (multiplicación de clases) es un grupo abeliano. Por ejemplo:
$$U(\mathbb{Z}_4) = \{1, 3\} \qquad 1 \cdot 1 = 1,\ 3 \cdot 3 = 1$$
8. $n \geqslant 1$, $\mu_n = \{\text{raíces complejas de } x^n - 1\} = \{\xi_k = \cos\frac{2k\pi}{n} + i\,\text{sen}\,\frac{2k\pi}{n},\ k = 0, \ldots, n-1\} = \{1, \xi, \xi^2, \ldots, \xi^{n-1} \text{ tal que } \xi = \cos\frac{2\pi}{n} + i\,\text{sen}\,\frac{2\pi}{n}\}$ es un grupo abeliano con el producto.
9. $SL_2(\mathbb{K}) = \{\text{matrices con det} = 1\}$ con $\mathbb{K}$ un cuerpo con el producto de matrices es un grupo.
10. G y H grupos, $G \times H$ es un grupo con $(x, y) * (x', y') = (xx', yy')$ y se llama **producto directo** de G y H.
11. Sea X un conjunto no vacío. Consideramos
$$S(X) = \{f : X \to X \text{ biyectivas}\}$$
el conjunto de las permutaciones de X. Con la composición es un grupo. Llamaremos a este grupo S_n donde n será el número de elementos de X, $X = \{1, 2, \ldots, n\}$.

12. Sean G un grupo, X un conjunto. Consideramos

$$Apl(X,G) = G^X = \{f : X \to G \text{ aplicaciones}\}$$

podemos definir $(f * g)(x) = f(x)g(x)$. Si $f \in G^X$, tendremos que $f'(x) = (f(x))'$.

Si $X = \emptyset$, entonces $G^X = \{\emptyset\}$ y si $X = \{1, 2\}$, entonces G^X es isomorfo a $G \times G$.

Lema 2.2. Sea G un grupo, entonces

i) $xx^{-1} = e \ \ \forall x \in G$.

ii) $xe = x \ \ \forall x \in G$.

Demostración.

i) $x^{-1}(xx^{-1}) = (x^{-1}x)x^{-1} = ex^{-1} = x^{-1}$

ii) $xe = x(x^{-1}x) = (xx^{-1})x = ex = x$

□

Lema 2.3. En un grupo G, el neutro del grupo y el simétrico de cada elemento son únicos.

Lema 2.4. (Propiedad cancelativa).

$$\forall x, y, z \in G \begin{cases} xy = xz \Rightarrow y = z \\ xy = zy \Rightarrow x = z \end{cases}$$

Demostración. Para el primer caso tenemos $y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$. El segundo caso es análogo □

Lema 2.5. Sea G un grupo, entonces

i) $e^{-1} = e$

ii) $(x^{-1})^{-1} = x \ \ \forall x \in G$.

iii) $(xy)^{-1} = y^{-1}x^{-1} \ \ \forall x, y \in G$.

Demostración.

i) $ee = e$

ii) $xx^{-1=e} \Rightarrow (x^{-1})^{-1} = x$.

iii) $(y^{-1}x^{-1})(xy) = y^{-1}x^{-1}xy = y^{-1}ey = y^{-1}y = e$

□

Lema 2.6. Sea G un conjunto no vacío con una operación binaria asociativa. Entonces son equivalentes:

i) G es un grupo.

ii) Para cada par de elementos $a, b \in G$, las ecuaciones $aX = b$, $Xa = b$ tienen solución en G, es decir, que $\exists c, d \in G$ de forma que $ac = b$ y $da = b$, en cuyo caso c y d son las soluciones de la ecuación.

Demostración.

i) $\Rightarrow$ ii)) $aX = b \Rightarrow c = a^{-1}b$ y $Xa = b \Rightarrow d = ba^{-1}$.

ii) $\Rightarrow$ i)) Sabemos que $aX = b$ tiene solución y la notamos por e_a. Consideramos también $\forall b \in G$, $Xa = b$ y tomamos x tal que $xa = b$. Entonces $be_a = xae_a = xa = b \Rightarrow e_a \rightsquigarrow e$ es un neutro por la derecha. Por tanto tenemos que $aX = e \rightsquigarrow \exists a^{-1} \Rightarrow G$ es un grupo.

□

Lema 2.7. (Ley asociativa general)
Sea G un grupo, $\forall x \in G$, $\forall m, n > 0$ con $n > m > 0$, entonces se tiene

$$\left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{n} x_i\right) = \prod_{i=1}^{n} x_i$$

Definición 2.4. Potencia

$$x^n = \begin{cases} x^n & n > 0 \\ e & n = 0 \\ (x^{-1})^{-n} & n < 0 \end{cases} \qquad x^{n+m} = x^n \cdot x^m$$

Definición 2.5. Sea G un grupo, si G tiene un número finito de elementos, entonces se llama **grupo finito** y a ese número de elementos se le llama orden del grupo y lo notaremos por $|G|$.

Definición 2.6. (Tabla de Cayley)
En un grupo finito $G = \{x_1 = 1, x_2, \ldots, x_n\}$ se llama **tabla de Cayley** (o tabla de multiplicar) a la matriz $n \times n$ cuya entrada (i, j) es $x_i x_j$.

Ejemplo.

•) $G = \{0, 1\}$

$*_1$	0	1
0	0	1
1	1	0

$*_2$	0	1
0	1	0
1	0	1

•) $G = \{0, 1, 2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

- **)** $G = \{0, 1, 2, 3\}$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Propiedades.

- **)** Todas las tablas son simétricas (en el caso de grupo abeliano).
- **)** Todos los elementos aparecen en todas las filas y todas las columnas (sino las ecuaciones del lema anterior no tendrían solución).
- **)** Tiene que haber una fila igual que el encabezado (actúa de neutro).

Definición 2.7. En un grupo G, el **orden** de un elemento x es el menor entero positivo n si existe, tal que $x^n = 1$. Lo notaremos por $O(x)$ o por $ord(x)$

Si no existe dicho n, se dice que el orden es infinito.

Observación.

$$x^m = 1 \Rightarrow n|m$$
$$m = nq + r \quad 0 \leqslant r \leqslant n$$
$$1 = x^m = x^{nq} \cdot x^r = x^r \Rightarrow r = 0$$

Ejemplo.

1. $O(x) = 1 \iff x = 1$
2. $O(x) = O(x^{-1}) \quad \forall x \in G$
3. $\forall x \neq 0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ se tiene que $O(x) = +\infty$
4. $\mathbb{C}^*$, $O(i) = 4$
5. $\mathbb{Z}_9$, $O(\overline{6}) = 3$

Ejercicio 1. Consideramos $(\mathbb{Z}, *)$ donde $*$ es la operación binaria definida por

$$a * b = a + b + 1$$

Probar que esto es un grupo abeliano.

Demostración. Para verlo tendremos que ver que verifica las propiedades de un grupo abeliano:

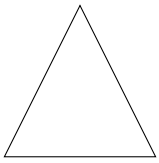
- •) Asociativa: $(a * b) * c = (a + b + 1) * c = a + b + c + 2 = a * (b * c)$
- •) Neutro: $a * x = a$, $a + x + 1 = a$, por lo que $x = -1$.
- •) Inverso: $a * a^{-1} = -1$, $a^{-1} = -a - 2$.

Además se verifica la conmutativa por ser una suma en $\mathbb{Z}$ (que es conmutativa). □

2.1. Grupos Diédricos (D_n)

Estos grupos vienen de las isometrías de un polígono regular que dejan fija la figura (en el plano).

2.1.1. Triángulo



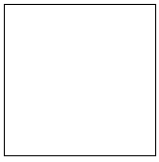
Rotaciones:

- •) Identidad
- •) Rotación de ángulo $\frac{2\pi}{3}$, r_1 $1-2-3-1$ $(1\ 2\ 3)$ (r)
- •) Rotación de ángulo $\frac{4\pi}{3}$, r_2 $1-3-2-1$ $(1\ 3\ 2)$ (r^2)

Simetrías:

- •) s_1 $(1\ 2)$ s
- •) s_2 $(1\ 3)$ $sr = s_2$
- •) s_3 $(2\ 3)$ $sr^2 = s_3$

2.1.2. Cuadrado



Rotaciones:

- •) Identidad
- •) Rotación de ángulo $\frac{\pi}{2}$ $(1\ 2\ 3\ 4)$ (r)

- •) Rotación de ángulo π (1 3)(2 4) (r^2)
- •) Rotación de ángulo $\frac{3\pi}{3}$ (1 4 3 2) (r^3)

Simetrías:

- •) s_1: (1 2)(3 4)
- •) s_2: (1 4)(2 3)
- •) s_3: (2 4)
- •) s_4: (1 3)

Observación.

- •) Se tiene que $sr \neq rs$
- •) Además, $sr = r^3 s$ y $r = sr^3$

La tabla de D_4 será:

	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

$$
\begin{aligned}
rs &= sr^{-1} \\
rsr &= sr^{-1}r = s \\
rsr^2 &= sr^{-1}r^2 = sr \\
rsr^3 &= sr^{-1}r^3 = sr^2
\end{aligned}
$$

2.1.3. En general, D_n

D_n son las isometrías que dejan fijo un polígono regular de n lados. Tendremos $2n$ elementos:

- •) n rotaciones $\frac{2k\pi}{n} = r_k$, $k = 0, \ldots, n-1$.
- •) n simetrías, $s_1, \ldots, s_n$

Si n es par tendremos $\frac{n}{2}$ diagonales y $\frac{n}{2}$ mediatrices. Si n es impar tendremos n radios que irán desde un vértice hasta el punto medio del lado opuesto.

Notación.

$r \equiv$ rotación de ángulo $\dfrac{2\pi}{n}$

$s \equiv$ simetría que pasa por el origen de coordenadas y el vértice 1 ($s = s_1$)

Lema 2.8.

1. $1, r, r^2, \ldots, r^{n-1}$ son todos distintos y $r^n = 1$ ($(O(r) = n)$)
2. $s^2 = 1$, $O(s) = 2$
3. $s \neq r^i \ \ \forall\, 0 \leqslant i \leqslant n-1$ (s fija el 1 pero las rotaciones no).
4. sr^i, $0 \leqslant i \leqslant n-1$ son simetrías en los ejes de simetrías $(s_2, s_3, \ldots, s_n)$ y $sr^i \neq sr^j$ para $i \neq j$.
5. $sr = r^{-1}s$ y en general $sr^i = r^{-i}s$

Ejemplo. En D_2 tenemos que $sr^9sr^6 = r^9$

Definición 2.8. Un conjunto de generadores de un grupo G es un subconjunto $S \subset G$ tal que todo elemento de G puede escribirse como producto finito de elementos de S y sus inversos. Lo notaremos como $G =< S >$ o, en el caso de $S = \{x_1, \ldots, x_n\}$ podremos escribir $G =< x_1, \ldots, x_n >$ y diremos que G está generado por S.

Cualquier elemento $x \in G$ podremos escribirlo como

$$x = x_1^{\gamma_1} x_2^{\gamma_2} \ldots x_n^{\gamma_n} \quad x_i \in S, \quad \gamma_i = \pm 1$$

Ejemplo.

1. $G =< x >$, $S =< x >$ es un grupo cíclico. $\mathbb{Z} =< 1 >$
2. $D_n =< r, s >$

Definición 2.9. Si $G =< S >$ y existe un conjunto de relaciones $R_1, R_2, \ldots, R_m$ (igualdades entre elementos de $S \cup \{1\}$) tal que cualquier relación entre los elementos de S puede deducirse de estas, entonces decimos que estos generadores y relaciones constituyen una **presentación de** G y lo escribimos como

$$G =< S/R_1, R_2, \ldots, R_m >$$

Ejemplo.

1. $D_n =< r, s/rs = sr^{-1} >$ (presentación abstracta de D_n).
   Podemos considerar $D_1 =< s/s^2 = 1 >$ y $D_2 =< r, s/r^2 = s^2 = 1, sr = rs >$ que no tienen sentido geométrico pero sí abstracto.
2. $C_n =< x/x^n = 1 >= \{1, x, x^2, \ldots, x^{n-1}\}$ es el grupo cíclico de orden n.
3. $V^{abs} =< x, y/x^2 = 1,\ y^2,\ (xy)^2 = 1 >=< 1, x, y, xy >$ es el grupo de Klein abstracto

4. $Q_2^{abs} =< x, y / x^4 = 1,\ y^2 = x^2,\ yxy^{-1} = x^{-1} >$ es el grupo de cuaternios abstracto. Tenemos que $Q_2^{abs} = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$, $O(x) = 4$, $|Q_2^{abs}| = 8$, $O(x^2) = 2$, los demás tienen orden 4.

   Podemos identificar este grupo con $SL_2(\mathbb{C})$ de la siguiente forma:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad x = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad x^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$x^3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \qquad xy = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \qquad x^2y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad x^3y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

   y tenemos los Cuaternios $Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ y se tiene que $i^2 = j^2 = k^2 = -1$ y además se verifica

$$\begin{array}{ccc} ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j \end{array}$$

   y podemos hacer la siguiente identificación:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv 1 \qquad x = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \equiv i \qquad y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \equiv j$$

$$x^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \equiv -1 \qquad x^3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \equiv -i \qquad xy = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \equiv k$$

$$x^2y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \equiv -j \qquad x^3y = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \equiv -k$$

   de esta forma hemos identificado el grupo Q_2^{abs} con Q_2 (la presentación con el grupo descrito por sus elementos).

2.2. Grupos Simétricos (S_n)

Este grupo lo construiremos a partir de las permutaciones. Dado un conjunto X, podemos definir el conjunto de aplicaciones biyectivas

$$S(X) = \{f : X \to X \text{ biyectivas}\}$$

que ya se ha trabajado como el conjunto de permutaciones. Dado $X = \{1, \ldots, n\}$ finito podemos considerar el n-ésimo grupo simétrico $S(X) = S_n$ (con la composición). Se va a verificar que $|S_n| = n!$.

Una forma de representar los elementos $\sigma \in S_n$ es con la **representación matricial**

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

Ejemplo. S_5 podemos describirlo matricialmente de la siguiente forma:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \rightsquigarrow (1\ 2\ 3\ 4\ 5) \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \rightsquigarrow (1\ 3)(2\ 4\ 5)$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \rightsquigarrow (1\ 4)(2\ 5\ 3) \qquad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix} \rightsquigarrow (1\ 4\ 2)(3\ 5)$$

Esta segunda representación (la que aparece a continuación de la matricial) es la representación en ciclos disjuntos. No siempre tienen que variar los elementos

Definición 2.10. Sea $\sigma \in S_n$ tal que desplaza circularmente al conjunto $\{a_1, a_2, \ldots, a_m\} \subseteq X$ y al resto de elementos los deja fijos (no se desplazan). Esto será un **ciclo de longitud** m.

Es indiferente el primer elemento de estos ciclos de forma que

$$\sigma = (a_1, a_2, \ldots, a_m) = (a_2, a_3, \ldots, a_m, a_1) = \cdots = (a_m, a_1, \ldots, a_{m-1})$$

Tendremos $\dfrac{V_m^n}{m}$ ciclos de longitud m.

Ejemplo. En S_5 tendremos $\dfrac{V_5^2}{2}$ ciclos de longitud 2 y $\dfrac{V_5^3}{3}$ ciclos de longitud 3.

Lema 2.9.

- **)** El orden de un ciclo de longitud m es m.
- **)** Dado $\sigma = (a_1, a_2, \ldots, a_m) \rightsquigarrow \sigma^{-1} = (a_m, a_{m-1}, \ldots, a_2, a_1)$.

Definición 2.11. Los 2-ciclos los llamaremos **trasposiciones**

Definición 2.12. Podemos descomponer cualquier ciclo en ciclos disjuntos de distinta longitud de la forma

$$\sigma = (a_1, a_2, \ldots, a_{m_1})(a_{m_1+1}, a_{m_1+2}, \ldots, a_{m_2}) \ldots (a_{m_k+1}, a_{m_k+2}, \ldots, a_{m_{k+1}})$$

y lo llamaremos **descomposición en ciclos disjuntos**.

De esta forma tendremos que $\sigma(a_k) = a_{k+1}$ para cualquier elemento de un ciclo que no sea el último, $\sigma(a_n) = a_1$ para el último elemento del ciclo y $\sigma(a_j) = a_j$ para todo elemento que no esté en el ciclo.

Ejemplo. Consideramos S_{13} la siguiente representación matricial:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$$

Tendremos que la descomposición en ciclos disjuntos será

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(3)(5\ 11\ 7)(6\ 9)$$

Tenemos que el inverso por tanto será

$$\sigma = (4\ 10\ 8\ 12\ 1)(2\ 13)(7\ 11\ 5)(6\ 9)$$

Por ejemplo, tenemos que $\sigma(7) = 5$

Observación.

- •) Si $\sigma \in S_n$, entonces $\sigma \in S_m$ para todo $m \geqslant n$.
- •) En general, S_n no es abeliano para $n \geqslant 3$

Ejercicio 2.2.1. (Ejercicio 14 de la Relación)
Sean $s_1, s_2 \in S_7$ dados por

$$s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 2 & 1 & 4 & 3 \end{pmatrix} \qquad s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 1 & 7 & 6 \end{pmatrix}$$

Calculamos los siguientes elementos:

$$s_1 s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 7 & 2 & 3 & 5 & 4 \end{pmatrix} \qquad s_2 s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

$$s_2^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 7 & 5 & 2 & 6 \end{pmatrix}$$

Los podemos expresar en ciclos disjuntos como

$$s_1 s_2 = (2\ 6\ 5\ 3\ 7\ 4) \qquad s_2 s_1 = (1\ 6\ 3\ 2\ 7\ 4)$$

$$s_2^2 = (2\ 3\ 4\ 7\ 6)$$

Teorema 2.10. Toda permutación $\sigma \in S_n$ con $\sigma \neq 1$ se expresa en la forma $\sigma = \gamma_1 \gamma_2 \dots \gamma_k$ donde γ_i, $i = 1, \dots, k$ son ciclos disjuntos de longitud mayor o igual que 2. Además, esta descomposición es única salvo el orden de los factores.

Demostración. Vamos a definir una relación de equivalencia en X. Para ello suponemos $X = \{1, 2, \dots, n\}$ y $\sigma \in S_n$ con $\sigma \neq 1$ (no es la identidad). Además, consideramos la relación R dada por

$$xRy \iff \exists m \in \mathbb{Z} \text{ tal que } y = \sigma^m(x)$$

Es fácil ver que R así definida es una relación de equivalencia en X. Consideramos entonces la clase de equivalencia para $x \in S$

$$C = \{\sigma^m(x) / m \in \mathbb{Z}\}$$

Donde C tiene un número finito de elementos (ya que X es finito). Por tanto tenemos que $x, \sigma(x), \sigma^2(x), \dots, \sigma^{m+1}(x) = x$ son elementos de la misma clase C.

Podemos considerar la permutación $\gamma \in S_n$ dada por

$$\gamma = (x\ \sigma(x)\ \sigma^2(x)\ \dots\ \sigma^m(x))$$

De esta forma tenemos

$$\gamma(y) = \begin{cases} \sigma(y) & y \in C \\ y & y \neq C \end{cases}$$

y tenemos una partición de X en clases de equivalencia C_i, con γ_i dada por

$$\gamma_i(y) = \begin{cases} \sigma(y) & y \in C_i \\ y & y \neq C_i \end{cases}$$

Tenemos que los ciclos son disjuntos porque la partición es disjunta ya que si $y \in \gamma_i$, entonces $\gamma_i(y) = \sigma(y)$. Si $y \in \gamma_j$ con $j \neq i$, entonces $\gamma_j(y) = y$ y por tanto no puede estar en C_i y en C_j simultáneamente.

Tendremos que $\sigma = \gamma_1\gamma_2 \dots \gamma_k$. Veamos ahora cuál es la imagen de un cierto $y \in C_i$. Para ello tenemos

$$\sigma(y) = \gamma_1\gamma_2 \dots \gamma_i(y) = \gamma_1\gamma_2 \dots \gamma_{i-1}(\sigma(y)) = \sigma(y)$$

y se verifica la igualdad (trivialmente).

Para ver que es única se supone que existe otra y por tanto la única posibilidad es reordenar los elementos pero el resto se queda igual. □

Corolario 2.10.1. El orden de cualquier permutación es el *m.c.m.* de las longitudes de los ciclos disjuntos en los que se descompone.

Demostración. Supongamos $\sigma = \gamma_1\gamma_2 \dots \gamma_k$. Sabemos que los ciclos conmutan, es decir que $\gamma_i\gamma_j = \gamma_j\gamma_i$. Podemos escribir entonces

$$\sigma^m = \gamma_1^m\gamma_2^m ... \gamma_k^m$$

Por tanto tenemos que

$$\sigma^m = 1 \iff \gamma_i^m = 1 \quad \forall i = 1, \dots, m$$

y en dicho caso $O(\sigma) = m$. Por tanto $O(\sigma_i)|m$ (divide a m) para todo $i = 1, \dots, m$. Por tanto $O(\sigma_i)$ es *m.c.m.* de las longitudes. □

Ejemplo.

- **)** S_2: $X = \{1, 2\}$ y tenemos $S_2 = \{id, (1\ 2)\}$
- **)** S_3: $X = \{1, 2, 3\}$ y tenemos $S_3 = \{id, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\} \cong D_3$
- **)** S_4: $X = \{1, 2, 3, 4\}$ y tenemos $S_4 = \{id, (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4),$ $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3),$ $(1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(2\ 4), (1\ 4)(2\ 3)\}$