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:

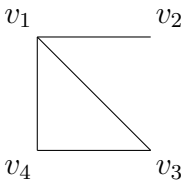
$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

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

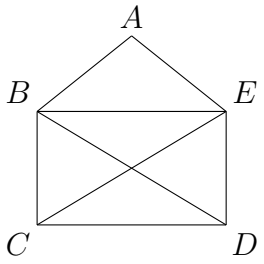
$$\sum_i gr(v_i) = 2 \cdot l$$

  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 $Xa = b \Rightarrow d = ba^{-1}$.

□