9
2 9

UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CIENCIAS

DESCOMPOSICIONES MINIMAS EN LOS GRUPOS SIMETRICOS

T E S I S

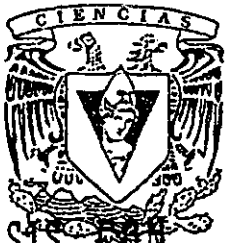
QUE PARA OBTENER EL TITULO DE:

MATEMATICO

P R E S E N T A:

GERARDO JUAREZ FLORES

27150



DIRECTOR DE TESIS: DR. EMILIO LLUIS RIERA

1999

TESIS CON
FALLA DE ORIGEN

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CIENCIAS

DESCOMPOSICIONES MINIMAS EN LOS GRUPOS SIMETRICOS

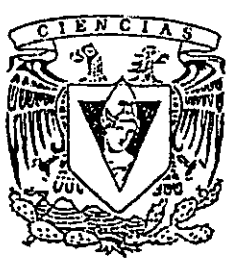
T E S I S

QUE PARA OBTENER EL TITULO DE:

MATEMATICO

P R E S E N T A:

GERARDO JUAREZ FLORES



DIVISION DE ESTUDIOS PROFESIONALES
FACULTAD DE CIENCIAS

DIRECTOR DE TESIS: DR. EMILIO LLUIS RIERA

1999

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

M. en C. Virginia Abrín Batule
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
P r e s e n t e

Comunicamos a usted que hemos revisado el trabajo de Tesis:

DESCOMPOSICIONES MINIMAS EN LOS GRUPOS SIMETRICOS

realizado por GERARDO JUAREZ FLORES

con número de cuenta 8838714-5 , pasante de la carrera de MATEMATICAS

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dr. EMILIO LLUIS RIERA
Propietario	Dr. FRANCISCO FEDERICO RAGGI CARDENAS
Propietario	Dr. JUAN MORALES RODRIGUEZ
Suplente	Dr. JOSE RIOS MONTES
Suplente	Dr. RODOLFO SAN AGUSTIN CHI

Consejo Departamental de Matemáticas

MAT. JULIO CESAR GUEVARA BRAVO

A mi familia: Juvencio,

Dominga

y Adela.

Agradecimientos

Con este trabajo quiero agradecer a todas aquellas personas que de un modo u otro han estado cerca de mí y me han apoyado en algún sentido.

Primeramente quiero agradecer a mis padres, Juvencio Juárez Parra y Dominga Flores Olaya, el haber estado cerca de mí y de mi desempeño para lograr hacer realidad algo que parecía muy lejano. Gracias por su apoyo y los quiero mucho. Espero con esto haber correspondido a su confianza.

También quiero agradecer a mi hermana Adela Juárez Flores el haber pasado muchos momentos agradables y el de compartir nuestras experiencias académicas y personales.

Quiero agradecer en forma muy general al interés mostrado por mi familia que radica en Chilapa, Edo. de Puebla.

Quiero agradecer de una manera muy especial a todos mis profesores que han participado de mi desarrollo académico, pero en particular a dos personas fundamentales para realizarme, ellos son, el Dr. Emilio Lluis Riera y el Dr. Juan Morales Rodríguez.

El Dr. Emilio Lluis fué una pieza importante en mi formación académica, pues los diferentes cursos impartidos por él, me permitieron tener un conocimiento general del álgebra y de hecho fué el imán que me atrajo a esta área.

El Dr. Juan Morales ha sido un apoyo invaluable en mi formación profesional al permitirme compartir con él experiencias docentes. Ha sido una importante fuente de ideas para lograr observar situaciones que usualmente no se aprenden cursando materias en el aula. También agradezco a Juan el tiempo invertido para comentar y corregir éste trabajo así como por sus útiles observaciones.

También quiero agradecer los comentarios y correciones hechas al trabajo a los Dres. Francisco Raggi, José Ríos y Rodolfo San Agustín.

Quiero agradecer a Jaime Salazar su invaluable amistad, así como la confianza que me tuvo para que yo concluyera este trabajo. Gracias por la paciencia que me has tenido y perdona el abandono en que te he dejado. También agradezco tus aportaciones para las gráficas de éste trabajo.

Quiero agradecer el apoyo dado por los compañeros de carrera y ahora mis amigos, Berta Zavala y el "Dr." Julio César. Con ellos compartí múltiples experiencias a través de varios años de trabajo conjunto, pues con ellos he logré hacer un buen equipo de trabajo, lástima que se dediquen a otras áreas de la matemática.

Es una tarea difícil mencionar aquí a todas aquellas personas que han seguido el desempeño de este trabajo y que me han estado apoyando durante todo este tiempo. Espero me perdonen la omisión pero quiero agradecer en forma general a todas aquellas personas que son mis amigos, ya sea porque alguna vez fuimos compañeros de estudio en las aulas o bien porque alguna vez fueron mis alumnos.

También quiero agradecer a la UNAM, por conducto de la Facultad de Ciencias, la formación obtenida en sus aulas. Y de manera especial al Instituto de Matemáticas por las facilidades dadas para la realización de este trabajo.

Índice General

Introducción

En este trabajo daremos algunas demostraciones de un teorema sobre grupos simétricos que afirma lo siguiente:

Toda permutación π de n letras se puede descomponer como un producto de $n - r$ transposiciones, donde r es el número de ciclos ajenos de π, y cualquier otra descomposición de π como producto de transposiciones tiene al menos $n - r$ factores.

En esta tesis daremos tres demostraciones para el teorema citado anteriormente.

El primer capítulo está dedicado a conceptos preliminares.

En el segundo capítulo damos una demostración de este teorema utilizando la teoría de grupos.

En el tercer capítulo que es la parte central de este trabajo, presentamos una demostración basada en un artículo de George Mackiw. En esta demostración se hace uso del álgebra lineal.

El cuarto capítulo está relacionado con la teoría de gráficas. Se manejan conceptos relacionados con las gráficas, gráficas conexas, árboles y se da una tercera demostración del teorema citado.

La descomposición de una permutación como un producto mínimo de transposiciones no es única, así que en el quinto capítulo, como curiosidad matemática y por estar relacionado con las descomposiciones mínimas de una permutación, contamos el número de formas distintas en que un ciclo de longitud n se descompone como producto mínimo de transposiciones.

Capítulo 1

Resultados preliminares

Algunos resultados necesarios sobre la teoría de grupos.

A manera de reseña histórica, fueron tres las áreas de la matemática que implicitamente usaron la noción de grupo antes de que ésta existiera plenamente.

En la teoría de ecuaciones, Lagrange consideró las raíces de un polinomio y sus permutaciones como herramienta para resolver ecuaciones.

Por otra parte Euler consideró las propiedades que presentaban los residuos obtenidos al dividir un número a^n entre un primo p, y operarlos con la multiplicación. También Gauss notó que la composición de formas cuadráticas daba origen a otras formas cuadráticas.

En el siglo XIX, el estudio de invariantes bajo ciertas transformaciones, dió origen al grupo lineal general.

Fué a finales del siglo XIX cuando se dió una noción clara del concepto de grupo, debido a los trabajos de Walter Von Dick y Heinrich Weber.

Es importante hacer notar que las permutaciones fueron una de las áreas en que se comenzó a formar la noción de grupo.

Por otro lado, las permutaciones en si mismas tienen un pasado mucho mas lejano. En el Libro de la Creación (Sefer Yetsirah en hebreo) existe un problema en que se intenta contar el número diferente de arreglos o sucesiones que pueden formarse con cierto número de letras del alfabeto. Esto ocurría alrededor del siglo VIII A. C.

Ya para el siglo XIII la noción de permutaciones toma mas sentido y forma de tal modo que el matemático y filósofo francés Levi Ben Gerson da una prueba rigurosa de que el número de

permutaciones de un conjunto con n letras es exactamente $n!$.

Fué el francés Agustín Louis-Cauchy quien sienta las bases para el estudio de permutaciones. El le llamó "cálculo de substituciones". También a él se debe la mayoría de la notación de permutaciones utilizada en nuestros días. Algunos de sus trabajos fueron sobre los ciclos de una permutación, sobre las transposiciones, definió el producto de permutaciones, así como la distinción entre permutaciones pares e impares. Probó la existencia del grupo alternante.[5][14]

Ahora enunciaremos las definiciones necesarias para el presente trabajo.

Definición 1 *Sea* $\mathbf{G}$ *un conjunto y* $*$ *una operación binaria en* $\mathbf{G}$. $(\mathbf{G}, *)$ *es un grupo si se tiene que para todo* $a, b, c \in \mathbf{G}$

-$a * (b * c) = (a * b) * c$.

-Existe $e \in \mathbf{G}$ *tal que* $e * a = a * e = a$ *para toda* $a \in \mathbf{G}$.

-Para cada $a \in \mathbf{G}$ *existe* $y \in \mathbf{G}$ *tal que* $a * y = y * a = e$.

Si además la operación $*$ resulta ser conmutativa, esto es que $a*b = b*a$, para todo $a, b \in \mathbf{G}$ entonces diremos que $(\mathbf{G}, *)$ es *grupo abeliano.*

Si $(\mathbf{G}, *)$ es un grupo, también se puede decir que $\mathbf{G}$ es un grupo con la operación $*$ y por abuso de notación $(\mathbf{G}, *)$ se escribe simplemente como $\mathbf{G}$.

Definición 2 *Sea* $\mathbf{G}$ *un grupo y* $H \subset \mathbf{G}$, $H \neq \varnothing$, H *es subgrupo de* $\mathbf{G}$ *si* H *forma un grupo con la operación en* $\mathbf{G}$.

Ejemplo 3 *El conjunto de números enteros* $\mathbf{Z}$ *con la suma usual* $+$ *es un grupo abeliano.*

Ejemplo 4 *El conjunto de números racionales diferentes de cero* $\mathbf{Q} - \{0\}$ *con el producto usual* $\times$ *es un grupo abeliano.*

Ejemplo 5 *El conjunto de matrices invertibles de* 2×2 *con elementos racionales con el producto usual de matrices es un grupo no abeliano. Si consideramos*

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

se tiene que

$$AB = \begin{pmatrix} -1 & -3 \\ -2 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 4 \\ -1 & 0 \end{pmatrix} = BA.$$

Ejemplo 6 *Sea Ω un conjunto no vacío y definimos $S_\Omega = \{f : \Omega \to \Omega \mid f$ es biyectiva$\}$*

El conjunto S_Ω con la operación composición de funciones forma un grupo llamado el grupo simétrico de Ω.

Definición 7 *Sea X un conjunto. La cardinalidad de X es el número de elementos de X y se denota por $|X|$.*

Proposición 8 *Si Ω es un conjunto y $|\Omega| \geq 3$ entonces S_Ω no es abeliano.*

Demostración. Como $|\Omega| \geq 3$ elegimos $a, b, c \in \Omega$ distintos.

Consideremos $f, g : \Omega \to \Omega$ definidas por:

$$f(x) = \begin{cases} b & \text{si } x = a \\ c & \text{si } x = b \\ a & \text{si } x = c \\ x & \text{si } x \neq a, b, c \end{cases} \quad , g(x) = \begin{cases} b & \text{si } x = a \\ a & \text{si } x = b \\ c & \text{si } x = c \\ x & \text{si } x \neq a, b, c \end{cases}$$

Claramente $f, g \in S_\Omega$ pero

$g \circ f(a) = g(b) = a$

$f \circ g(a) = f(b) = c$

Por lo tanto $g \circ f \neq f \circ g$. Así S_Ω no es conmutativo. ■

Definición 9 *Si Ω es un conjunto con n elementos, a S_Ω lo denotamos por S_n y se le llama el grupo simétrico de grado n.*

Si $|\Omega| = n$ entonces $|S_\Omega| = n!$. Para probar este resultado haremos uso de algunos resultados de la teoría de grupos.

Definición 10 *Si $\mathbf{G}$ es un grupo, H es un subgrupo de $\mathbf{G}$ y $a \in \mathbf{G}$ entonces el conjunto*

$$aH = \{ah \mid h \in H\}$$

es una clase lateral izquierda de $\mathbf{G}$.

Teorema 11 *Si* G *es un grupo finito y* H *es un subgrupo de* G *entonces*

$$|\mathrm{G}| = |H| \cdot A$$

donde A *es el número de clases laterales izquierdas de* H.

Una demostración de este resultado puede hallarse en [5] y en [8].

Proposición 12 *Sea* Ω *un conjunto y* $x \in \Omega$. *El conjunto* $H = \{f \in S_\Omega \mid f(x) = x\}$ *es subgrupo de* S_Ω.

Demostración. La composición de funciones es asociativa.

Sea $e \in S_\Omega$ tal que $e(y) = y$ para todo $y \in \Omega$. En particular $e(x) = x$, por lo tanto $e \in H$.

Si $f \in H$ entonces $f(x) = x$. Por ser f biyectiva existe $f^{-1} \in S_\Omega$ tal que $f^{-1}f = e$, pero $x = e(x) = f^{-1}f(x) = f^{-1}(f(x)) = f^{-1}(x)$.

Si $f, g \in H$ entonces $fg \in H$ ya que $(fg)(x) = f(g(x)) = f(x) = x$.

Por lo tanto H es subgrupo de S_Ω. ■

Proposición 13 *Sea* Ω *un conjunto,* $x \in \Omega$, $H = \{f \in S_\Omega \mid f(x) = x\}$, $g \in S_\Omega$, $g(x) = y$. *Si* $g' \in S_\Omega$ *entonces* $g'(x) = y$ *si y sólo si* $g^{-1}g' \in H$.

Demostración. Como $g(x) = y$ y $g'(x) = y$ entonces $g'(x) = g(x)$ de donde $g^{-1}g'(x) = x$ y así $g^{-1}g' \in H$.

Inversamente si $g^{-1}g' \in H$ entonces $g^{-1}g'(x) = x$ de donde $g'(x) = g(x)$. ■

Corolario 14 *Sea* Ω *un conjunto,* $x \in \Omega$, $H = \{f \in S_\Omega \mid f(x) = x\}$. $g_2, g_1 \in S_\Omega$ *entonces* $g_1(x) = g_2(x)$ *si y sólo si* $g_1 H = g_2 H$.

Demostración. $g_1(x) = g_2(x)$ si sólo si $g_2^{-1}g_1 \in H$ si y sólo si $g_2(g_2^{-1}g_1) \in g_2 H$ de donde $g_1 \in g_2 H$ y entonces $g_1 H \subset g_2 H$. Análogamente se obtiene $g_2 H \subset g_1 H$. ■

Proposición 15 *Sea* $x \in \Omega$, $g \in S_\Omega$ *tal que* $g(x) = y$ *si* $H = \{f \in S_\Omega \mid f(x) = x\}$ *entonces* $g'(x) = y$ *si y solo si* $g' \in gH = \{gf \mid f \in H\}$.

Demostración. Si $g'(x) = y$ entonces $g^{-1}g'(x) = g^{-1}(y) = x$ de donde $g^{-1}g' \in H$. Sea $g^{-1}g' = h$ entonces se tiene que $g' = gh \in gH$.

Inversamente sea $g' \in gH$ entonces $g' = gh$ para alguna $h \in H$ y se tiene que

$$\begin{aligned} g'(x) = \; & gh(x) = \\ & g(h(x)) = \\ & g(x) = y \blacksquare \end{aligned}$$

Sea $x \in \Omega$, $H = \{f \in S_\Omega \mid f(x) = x\}$. Sea $S_\Omega/H = \{gH \mid g \in S_\Omega\}$, definamos

$$\varphi : \Omega \rightarrowtail S_\Omega/H$$

tal que para cada $y \in \Omega$, $\varphi(y) = gH$ con $g \in S_\Omega$ tal que $g(x) = y$.

Por el corolario anterior se tiene que φ es función.

φ es biyección.

Claramente φ es sobre porque si $gH \in S_\Omega/H$ tal que $g(x) = y$ entonces por definición $\varphi(y) = gH$.

φ es inyectiva porque si $\varphi(y_1) = \varphi(y_2)$ sean $g_1(x) = y_1$ y $g_2(x) = y_2$ y entonces $g_1H = g_2H$ pero por la proposición 13 $g_2^{-1}g_1 \in H$ y entonces $g_2^{-1}g_1(x) = x$ de donde $g_1(x) = g_2(x)$ y por lo tanto $y_1 = y_2$.

Observación 1 *Si $A = |S_\Omega/H|$ entonces por lo visto anteriormente $A = |\Omega|$.*

Con lo anterior estamos en condiciones para demostrar el siguiente teorema:

Teorema 16 *Si $|\Omega| = n$ entonces $|S_\Omega| = n!$.*

Demostración. Por inducción sobre $|\Omega|$.

Si $|\Omega| = 1$, $\Omega = \{a\}$, la única función biyectiva posible es $e : \Omega \to \Omega$ definida por $e(a) = a$. Por lo tanto $|S_\Omega| = 1 = 1!$

Supongamos que Ω es un conjunto con k elementos y $|S_\Omega| = k!$.

Sea ahora Ω' un conjunto con $k+1$ elementos, $x \in \Omega'$.

Sea $H = \{f \in S_{\Omega'} \mid f(x) = x\}$. H es subgrupo de $S_{\Omega'}$.

Consideremos el conjunto $\Omega = \Omega' - \{x\}$, por hipótesis $|S_\Omega| = k!$. En forma natural se puede construir una biyección de H en S_Ω, la biyección es la restricción de cada $\alpha \in S_{\Omega'}$ a S_Ω.

Por lo tanto $|H| = k!$

Por el teorema 11 $|S_\Omega| = |H| A$.

Por la proposición anterior el número de clases laterales izquierdas de H en Ω' es el número de elementos de Ω', es decir, $A = k + 1$.

Por lo tanto $|S_{\Omega'}| = k!\,(k+1) = (k+1)!$ ■

Definición 17 *Sea* $\mathbf{G}$ *un grupo y* Ω *un conjunto. Una acción del grupo* $\mathbf{G}$ *en el conjunto* Ω *es una función* $\varphi : \mathbf{G} \times \Omega \to \Omega$ *tal que si se denota* $\varphi(g, x) = g(x)$, *entonces*

i) $e(x) = x$ *para todo* $x \in \Omega$.

ii) $(g_2 g_1)(x) = g_2(g_1(x))$ *para todo* $x \in \Omega$, $g_1, g_2 \in \mathbf{G}$.

En este caso decimos que Ω *es un* $\mathbf{G}-$*conjunto.*

Ejemplo 18 *Sea* $\mathbf{G}$ *un grupo y* $\Omega = \mathbf{G}$. *La acción* $\varphi : \mathbf{G} \times \mathbf{G} \to \mathbf{G}$ *definda como* $\varphi(h, g) = h^{-1}gh$ *se llama conjugación.*

Definición 19 *Sea* $\mathbf{G}$ *un grupo y* Ω *un conjunto.* $\mathbf{G}$ *actúa transitivamente sobre* Ω *si para cada* $x, y \in \Omega$, *existe* $g \in \mathbf{G}$ *tal que* $g(x) = y$.

Algunos resultados necesarios del álgebra lineal.

Definición 20 *Sea* V *un espacio vectorial sobre el campo* K *y* $T : V \to V$ *una función lineal. Un valor propio* λ *de* T *es un escalar tal que existe* $v \in V$ *con* $v \neq 0$, *tal que* $T(v) = \lambda v$. *El vector* v *es un vector propio de* T.

Definición 21 *Sea* $\mathbf{R}$ *el campo de los números reales y* V *un espacio vectorial sobre* $\mathbf{R}$. *Un producto escalar sobre* V *es una función* $\langle , \rangle : V \times V \to \mathbf{R}$, *tal que si* $u, v, w \in V$ *y* $\alpha \in \mathbf{R}$ *se tienen las siguientes propiedades:*

i) $\langle u + w, v \rangle = \langle u, v \rangle + \langle w, v \rangle$

ii) $\langle \alpha u, v \rangle = \alpha \langle u, v \rangle$

iii) $\langle u, v \rangle = \langle v, u \rangle$

iv) $\langle u, u \rangle \geq 0$ *y* $\langle u, u \rangle = 0$ *solo si* $u = 0$.

Ejemplo 22 *Sean* $u = (x_1, x_2, \cdots, x_n)$, $v = (y_1, y_2, \cdots, y_n) \in \mathbf{R}^n$. *La función*

$$\langle u, v \rangle = \sum_{i=1}^{n} x_i y_i$$

define un producto escalar, llamado el producto escalar canónico de R^n.

Definición 23 *Sea* V *un espacio vectorial sobre* K, V *con producto escalar* $\langle , \rangle$. $u, v \in V$ *son ortogonales si* $\langle u, v \rangle = 0$.

Algunos resultados de la teoría de gráficas.

Definición 24 *Sea* X *un conjunto no vacío. Una gráfica de* X *es una pareja ordenada* $\mathcal{G} = (V, A)$ *con* $V \subset X$, $V \neq \varnothing$ *y* $A = \varnothing$ *ó* A *un conjunto de parejas desordenadas de elementos distintos de* V. *Los elementos de* V *se llaman los vértices de la gráfica* $\mathcal{G}$ *y los elementos de* A *se llaman las aristas de la gráfica* $\mathcal{G}$.

Cada gráfica $\mathcal{G} = (V, A)$ de X se puede representar en $\mathbf{R}^2$ (el plano) de la forma siguiente:

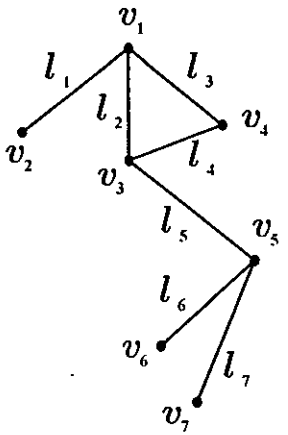
Cada vértice $v \in V$ se representa como un punto p de $\mathbf{R}^2$. Vértices $v_1, v_2 \in V$ con $v_1 \neq v_2$ se representan por puntos p_1, p_2 diferentes.

Si $l \in A$, es decir, si $l = \{v_1, v_2\} \in A$, l se representa como el segmento de recta $L \subset \mathbf{R}^2$ que une a p_1 y p_2, con p_i el punto que representa a v_i, $i = 1, 2$.

Ejemplo 25 *Si* $\mathcal{G} = (V, A)$ *es una gráfica con*

$$V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}, A = \{l_1, l_2, l_3, l_4, l_5, l_6, l_7\}$$

y $l_1 = \{v_1, v_2\}$, $l_2 = \{v_1, v_3\}$, $l_3 = \{v_1, v_4\}$, $l_4 = \{v_3, v_4\}$, $l_5 = \{v_3, v_5\}$, $l_6 = \{v_5, v_6\}$, $l_7 = \{v_5, v_7\}$, $\mathcal{G}$ *se puede representar de la siguiente forma.*



Representación de una gráfica

Definición 26 *Una subgráfica de una gráfica $\mathcal{G} = (V, A)$ de X, es una gráfica $\mathcal{G}' = (V', A')$ de X tal que $V' \subset V$, y $A' \subset A$.*

Si $\mathcal{G} = (V, A)$ es una gráfica de X y $l = \{v_1, v_2\} \in A$ se dice que la arista l une a v_1 con v_2 y denotamos $l = \overline{v_1 v_2}$

Definición 27 *Dos vértices $v_1, v_2 \in V$ son adyacentes si existe una arista l en $\mathcal{G}$ que une v_1 con v_2.*

Observación 2 *Si $\mathcal{G} = (V, A)$ es una gráfica y $v_1, v_2 \in V$ diferentes entonces v_1 y v_2 pueden estar unidos a lo más por una arista.*

Definición 28 *Un camino en una gráfica $\mathcal{G}$ es una sucesión de alguna de las siguientes formas $C_1 = \{v_1\}$ ó $C_2 = \{v_1, \overline{v_1 v_2}, v_2, ..., \overline{v_{k-1} v_k}, v_k\}$ $k \geq 2$ y $\{v_1, v_2, \cdots, v_k\}$ vértices de $\mathcal{G}$. Diremos que el camino c une v_1 con v_k.*

Definición 29 *Un vértice v_1 en una gráfica $\mathcal{G} = (V, A)$ es vértice terminal si existe uno y sólo un vértice $v_i \in V$ adyacente a v_1.*

Definición 30 *Un camino de una gráfica $\mathcal{G}$ es cerrado si es de la forma $C_1 = \{v_1\}$ ó $C_2 = \{v_1, \overline{v_1 v_2}, v_2, ..., \overline{v_{n-1} v_n}, v_n\}$ con $n \geq 3$ y $v_n = v_1$.*

Definición 31 *Una gráfica es conexa si para cada par de vértices $v_1, v_2 \in V$, existe un camino C que une v_1 con v_2.*

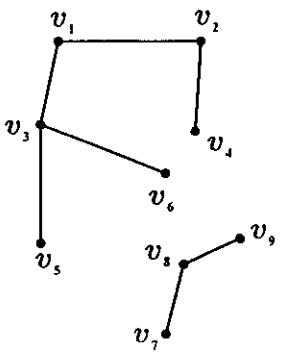
Definición 32 *Una gráfica es disconexa si no es conexa.*

En el ejemplo 25 se tiene una gráfica conexa.

Definición 33 *Un ciclo en una gráfica es un camino cerrado C con tres o más vértices distintos.*

En el ejemplo 25 se tiene un ciclo formado por los vértices v_1, v_3, v_4 y las aristas correspondientes.

Ejemplo 34 *Si $\mathcal{G} = (V, A)$ es una gráfica con $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9\}$ y $A = \{l_1, l_2, l_3, l_4, l_5, l_6, l_7\}$ con $l_1 = \overline{v_1v_2}$, $l_2 = \overline{v_2v_4}$, $l_3 = \overline{v_1v_3}$, $l_4 = \overline{v_3v_5}$, $l_5 = \overline{v_3v_6}$, $l_6 = \overline{v_7v_8}$, $l_7 = \overline{v_8v_9}$, entonces es disconexa pues no existe un camino que une v_6 con v_8.*

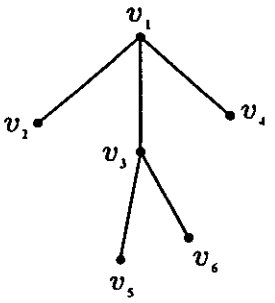


Gráfica disconexa

Con lo visto anteriormente, estamos en condiciones de definir una estructura importante en la teoría de gráficas.

Definición 35 *Un árbol es una gráfica conexa sin ciclos.*

Ejemplo 36 *$\mathcal{G} = (V, A)$ con $V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$ y $A = \{l_1, l_2, l_3, l_4, l_5\}$ con $l_1 = \overline{v_1v_2}$, $l_2 = \overline{v_1v_3}$, $l_3 = \overline{v_1v_4}$, $l_4 = \overline{v_3v_5}$, $l_5 = \overline{v_3v_6}$, es un árbol.*



Teorema 37 *Si $\mathcal{G} = (V, A)$ es una gráfica con n vértices, las siguientes afirmaciones son equivalentes:*

i) $\mathcal{G}$ es un árbol.

ii) $\mathcal{G}$ conexa con $n-1$ aristas.

iii) $\mathcal{G}$ no posee una subgráfica propia conexa y que contenga los mismos vértices que $\mathcal{G}$.

iv) $\mathcal{G}$ es conexa y para toda arista $l \in A$, la subgráfica $\mathcal{G}' = (V, A')$, con $A' = A - \{l\}$ es disconexa.

Demostración. *i)* $\rightarrow$ *ii)* $\mathcal{G}$ es conexa por ser árbol. Como $\mathcal{G}$ es conexa y con n vértices entonces $\mathcal{G}$ tiene al menos $n-1$ aristas. Como en $\mathcal{G}$ no hay ciclos, el número mínimo de aristas es $n-1$.

ii) $\rightarrow$ *iii)* Sea $\mathcal{G}'$ una subgráfica propia de $\mathcal{G}$ con los mismos vértices que $\mathcal{G}$, entonces el número de aristas de $\mathcal{G}'$ es menor que el número de aristas de $\mathcal{G}$, es decir, $\mathcal{G}'$ tiene n vértices y menos de $n-1$ aristas, por lo tanto $\mathcal{G}'$ no es conexa.

iii) $\rightarrow$ *iv)* Sea $l \in A$, consideremos la subgráfica $\mathcal{G}' = (V, A')$ con $A' = A - \{l\}$.

Por hipótesis $\mathcal{G}$ no contiene subgráficas conexas con n vértices y por lo tanto la subgráfica $\mathcal{G}'$ es disconexa.

iv) $\rightarrow$ *i)* Por hipótesis $\mathcal{G}$ es conexa, por lo tanto resta probar que $\mathcal{G}$ no tiene ciclos.

Supongamos que existe un ciclo C en $\mathcal{G}$ con $C = \{v_1, \overline{v_1v_2}, v_2, ..., \overline{v_{k-1}v_k}, v_k\}$ el camino correspondiente. Por ser C un ciclo entonces los vértices son diferentes y $k-1 \geq 3$. La gráfica $\mathcal{G}'$ que se obtiene de $\mathcal{G}$ al eleiminar cualquiera de las aristas $\overline{v_iv_{i+1}}$ es conexa, lo que es una

Capítulo 2

Descomposición de permutaciones como producto de transposiciones I.

En este capítulo se da una demostración del teorema que afirma que el número mínimo necesario de transposiciones para descomponer una permutación $\pi \in S_n$, $\pi \neq e$, es $n-r$ con r el número de ciclos ajenos de π incluyendo los posibles ciclos triviales. En la demostración se hace uso de algunos resultados sobre grupos de permutaciones.

En la proposición 8 se probó que si Ω es un conjunto con más de tres elementos, el grupo simétrico S_Ω no es abeliano. Fácilmente se puede probar el siguiente resultado.

Proposición 38 *Si* $|\Omega| = 1$ *ó* 2 *entonces el grupo* S_Ω *es abeliano.*

Demostración. Sea $\Omega = \{a\}, |\Omega| = 1$ entonces $S_\Omega = \{e\}$. Donde $e(a) = a$.

Sea $\Omega = \{a, b\}, |\Omega| = 2$ entonces $S_\Omega = \{e, f\}$. Donde

$e(a) = a, e(b) = b$ y $f(a) = b, f(b) = a$.

Observamos que $ef(a) = e(b) = b$ y por otro lado $fe(a) = f(a) = b$, entonces $ef(a) = fe(a)$.

Verificando para b tenemos: $ef(b) = e(a) = a$ y $fe(b) = f(b) = a$, entonces $ef(b) = fe(b)$.

Por lo tanto $ef = fe$ y S_Ω es abeliano. ■

De las proposiciones 8 y 38 se tiene que el grupo simétrico S_Ω no es grupo abeliano excepto para los casos $|\Omega| = 1$ o 2.

La notación usual para una permutación $\pi \in S_n$ es la siguiente:

$$\pi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \pi(a_1) & \pi(a_2) & \cdots & \pi(a_n) \end{pmatrix}$$

donde en el primer renglón se colocan los diferentes elementos de Ω y en el segundo renglón se colocan las imágenes de a_i bajo π.

Ejemplo 39 *Si* $\Omega = \{1,2,3\}$ *entonces los elementos de* $S_\Omega = S_3$ *son:*

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Donde π_1 *es la identidad en* S_3.

Definición 40 *Sean* $\pi \in S_\Omega$ *y* $a \in \Omega$, *definimos la órbita de* a *bajo* π *como el conjunto*

$$\theta(a) = \{\pi^n(a) \mid n \in \mathbf{Z}\}$$

Observación 3 *Si* $a \in \Omega$, Ω *finito,* $\pi \in S_\Omega$ *entonces existe un entero* l, *que depende de* a, *tal que* $\pi^l(a) = a$.

Si k *es el entero positivo mínimo tal que* $\pi^k(a) = a$ *entonces la órbita de* a *bajo* π, *es el conjunto* $\theta(a) = \{a, \pi(a), \pi^2(a), \cdots, \pi^{k-1}(a)\}$. *Notamos que si* $i \neq j$, $i < k$, $j < k$ *entonces* $\pi^i(a) \neq \pi^j(a)$.

Observación 4 *Si* $a, b \in \Omega$, $|\Omega| = n$, $\pi \in S_\Omega$ *y* b *no está en la órbita de* a *bajo* π, *entonces la órbita de* a *y la órbita de* b *bajo* π *son ajenas.*

Observación 5 $\{\theta(a) \mid a \in \Omega\}$ *es una partición de* Ω.

Definición 41 *Un ciclo* σ *de* π *es la restricción de* π *a una órbita* $\theta(a)$ *de algún elemento* $a \in \Omega$.

Si $\theta(a) = \{a, \pi(a), \pi^2(a), \cdots, \pi^{k-1}(a)\}$ σ *se denota como*

$$\sigma = \left(a, \sigma(a), \sigma^2(a), \cdots, \sigma^{k-1}(a)\right)$$

y se dice que $\theta(a)$ es la órbita de σ.

Observación 6 *Si $a_1, a_2, \cdots, a_k \in \Omega$ diferentes, el arreglo ordenado*

$$\beta = (a_1, a_2, \cdots, a_k)$$

denota a la permutación $\pi \in S_\Omega$ tal que $\pi(a_1) = a_2$, $\pi(a_2) = a_3$, ..., $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$, y $\pi(x) = x$ para toda $x \in \Omega - \{a_1, a_2, \cdots, a_k\}$. Es inmediato que β es un ciclo de π.

Observación 7 *Si $\sigma = (a, \pi(a), \pi^2(a), \cdots, \pi^{k-1}(a))$ es un ciclo de $\pi \in S_\Omega$, se puede pensar como una permutación $\sigma \in S_\Omega$ tal que*

$$\sigma(x) = \begin{cases} \sigma_i(x) & si \quad x \in \{a, \pi(a), \pi^2(a), \cdots, \pi^{k-1}(a)\} \\ x & si \quad x \notin \{a, \pi(a), \pi^2(a), \cdots, \pi^{k-1}(a)\} \end{cases}$$

Definición 42 *Sean $\pi \in S_\Omega$, σ_1 y σ_2 dos ciclos de π. $\sigma_1 = (a_1, a_2, \cdots, a_r)$ y $\sigma_2 = (b_1, b_2, \cdots, b_s)$ son ajenos si $\{a_1, a_2, \cdots, a_r\} \cap \{b_1, b_2, \cdots, b_s\} = \varnothing$.*

Observación 8 *Si los ciclos $\sigma_1, \sigma_2 \in S_\Omega$ son ajenos, entonces $\sigma_1\sigma_2 = \sigma_2\sigma_1$.*

Teorema 43 *Sea Ω un conjunto con n elementos. Todo $\pi \in S_\Omega$ se puede escribir como producto de ciclos ajenos en forma única, excepto por el orden en que aparecen los ciclos.*

Demostración. Inducción sobre el número de órbitas de π.

Si $\pi \in S_\Omega$ tiene sólo una órbita, sea $a_1 \in \Omega$, entonces $\Omega = \theta(a_1)$ sea σ_1 el ciclo obtenido a partir de $\theta(a_1)$ y entonces $\pi = \sigma_1$.

Supóngase que el resultado es cierto para π con k órbitas.

Sean $\pi \in S_\Omega$ una permutación con $k+1$ órbitas, $a_1 \in \Omega$, entonces consideremos $\overline{\pi} \in S_{\Omega - \theta(a_1)}$ definido por $\overline{\pi}(a) = \pi(a)$, entonces $\overline{\pi}$ es una permutación con k órbitas y por hipótesis de inducción $\overline{\pi} = \rho_1\rho_2\cdots\rho_k$ es producto de k ciclos.

Nótese que $\pi = \overline{\pi}\sigma_1 = \rho_1\rho_2\cdots\rho_k\sigma_1$ con σ_1 el ciclo obtenido a partir de $\theta(a_1)$.

Por lo tanto π es producto de $k+1$ ciclos.

Como $\{\theta(a) \mid a \in \Omega\}$ es una partición de Ω, cada $\theta(a_i)$ da origen a un único ciclo σ_i.

Como Ω es finito existe un número finito de órbitas ajenas de π. De aquí se tiene la descomposición única en ciclos, salvo por el orden de los factores. ■

Ejemplo 44 *Sea* $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *en* S_3. *La órbita de* 1 *es el conjunto*

$$\theta(1) = \{1, \sigma(1), \sigma^2(1)\} = \{1, 3, 2\}$$

$\Omega = \theta(1)$ *y así podemos escribir* σ *como el ciclo* $(1, 3, 2)$.

Ejemplo 45 *Sea* $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ *en* S_3. *La órbita de* 1 *es el conjunto*

$$\theta(1) = \{1\}$$

La órbita de 2 *es el conjunto*

$$\theta(2) = \{2, \sigma(2)\} = \{2, 3\}$$

En este caso $\Omega = (\theta 1) \cup \theta(2)$ *y podemos escribir* π *como el producto de ciclos* $(1)(2, 3)$.

Definición 46 *Definimos la longitud de un ciclo* $\sigma = (a_1, a_2, a_3, \cdots, a_{k-1}, a_k) \in S_\Omega$ *como el número de elementos en la órbita de* σ.

$$l(a_1, a_2, a_3, \cdots, a_{k-1}, a_k) = k$$

En los ejemplos anteriores, el ciclo $(1, 3, 2)$ es de longitud 3. Los ciclos (1) y $(2, 3)$ son de longitud 1 y 2 respectivamente.

Si un ciclo es de longitud k, lo llamaremos un $k-$ciclo.

Definición 47 *Sean* $\pi, \rho \in S_n$. π *y* ρ *son conjugados si existe* $\tau \in S_n$ *tal que* $\pi = \tau^{-1}\rho\tau$.

Teorema 48 *Sean* $\pi, \rho \in S_n$. π *y* ρ *son conjugados, si y solo si* π *y* ρ *tienen la misma estructura cíclica, es decir, si* π *y* ρ *se descomponen como producto de ciclos ajenos,* π *y* ρ *tienen el mismo número de ciclos ajenos y además los ciclos de* π *tienen la misma longitud que los ciclos de* ρ.

No se dará la prueba de este teorema. Para una demostración de este teorema consultar [8].

Observación 9 *Si una permutación* $\pi \in S_\Omega$ *tiene ciclos de longitud* 1, *se conviene en omitir estos de la descomposición de* π *como producto de ciclos ajenos.*

Observación 10 *Sea* $(a_1, a_2, \cdots, a_{n-1}, a_n) \in S_\Omega$ *un ciclo de longitud* n. *Observamos que los* $n-$*ciclos:*

$$\begin{aligned}
\sigma_1 &= (a_1, a_2, \cdots, a_{n-1}, a_n) \\
\sigma_2 &= (a_2, a_3, \cdots, a_n, a_1) \\
&\vdots \\
\sigma_{n-1} &= (a_{n-1}, a_n, \cdots, a_{n-3}, a_{n-2}) \\
\sigma_n &= (a_n, a_1, \cdots, a_{n-2}, a_{n-1})
\end{aligned}$$

son iguales, lo que implica que cada $n-$*ciclo se puede escribir de* n *formas distintas.*

La observación anterior nos sirve para contar los ciclos de longitud n.

Proposición 49 *En* S_n *existen* $(n-1)!$ *ciclos de longitud* n.

Demostración. Como Ω es un conjunto con n elementos, entonces se tienen $n!$ ordenaciones de Ω, cada ordenación $\{a_1, a_2, \cdots, a_n\}$ determina al ciclo $(a_1, a_2, \cdots, a_n)$, pero hay n diferentes ordenaciones que determinan al mismo ciclo, por lo tanto el número de n ciclos en S_Ω es $\frac{n!}{n} = (n-1)!$. ■

Definición 50 *Definimos una transposición como un* $2-$*ciclo.*

Teorema 51 *Sea* Ω *un conjunto finito con* $|\Omega| = n \geq 2$. *Sea* $\pi \in S_\Omega$ *un* $k-$*ciclo,* π *se puede descomponer como producto de transposiciones.*

Demostración. Si $\pi = (a)$, sea $b \in \Omega - \{a\}$, entonces $\pi = (a) = (a, b)(a, b)$.

Si $\pi = (a_1, a_2, a_3, \cdots, a_{k-1}, a_k)$ con $k \geq 2$

$$\pi = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2). \blacksquare$$

Es fácil ver que esta descomposición no es única. En el capítulo 5 contaremos las diferentes formas en que un $n-$ciclo se puede descomponer como producto mínimo de transposiciones.

Definición 52 *La descomposición anterior se conoce como descomposición canónica de* π.

De los teoremas 43 y 51 tenemos el siguiente resultado:

Teorema 53 *Si $\pi = \pi_1\pi_2\cdots\pi_r \neq e$ es un producto de ciclos ajenos, y π_i es un k_i-ciclo, entonces π se puede descomponer como un producto de $n-r$ transposiciones.*

Demostración. Hemos visto que cada π_i es un producto de $k_i - 1$ transposiciones, por lo tanto π se descompone como un producto de

$$t = (k_1 - 1) + (k_2 - 1) + \cdots + (k_r - 1)$$

transposiciones, pero $t = (k_1 + k_2 + \cdots + k_r) - r = n - r$. ■

Ejemplo 54 *Sea $\Omega = \{1,2,3,4,5,6\}$. Expresar π como producto de ciclos y también como producto de transposiciones donde*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 5 & 2 \end{pmatrix}$$

Los ciclos de π son $(1,3)$, $(2,4,6)$, (5).

Entonces $\pi = (1,3)(2,4,6)(5) = (1,3)(2,4,6)$

Como $(2,4,6) = (2,6)(2,4)$, entonces $\pi = (1,3)(2,6)(2,4)$.

Nuestro objetivo es calcular el número mínimo de transposiciones necesarias para descomponer una permutación $\pi \in S_n$.

Observación 11 *Sea e la identidad en S_Ω con $|\Omega| \geq 2$ entonces se descompone como un producto de dos trasposiciones.*

Nótese que $e = (a) = (ab)(ab)$ con $a, b \in \Omega$ y $a \neq b$.

La demostración del teorema 51 garantiza que π un $k-$ciclo, con $k \geq 2$, π se descompone como producto de $k - 1$ transposiciones. Resta probar que el producto de un número menor a $k - 1$ transposiciones, no da lugar a un $k-$ciclo.

Definición 55 *Sea Ω un conjunto y H un subgrupo de S_Ω. Decimos que H es subgrupo transitivo sobre Ω si para cada $a, b \in \Omega$ existe $\pi \in H$ tal que $\pi(a) = b$.*

Lema 56 *Sea Ω un conjunto con n elementos. Las siguientes afirmaciones son equivalentes:*

i) Para $n \geq 2$, $n-2$ transposiciones no pueden generar un grupo con un subgrupo cíclico transitivo sobre Ω.

ii) Sea $\mathbf{G}$ subgrupo de S_Ω generado por $n-2$ transposiciones entonces $\mathbf{G}$ no tiene un $n-$ciclo.

Demostración. *i)* $\Rightarrow$ *ii)* Supongamos que existe un grupo de permutaciones $\mathbf{G}$ generado por $n-2$ transposiciones y $\sigma \in \mathbf{G}$ un $n-$ciclo entonces $H = \langle \sigma \rangle$ es subgrupo de $\mathbf{G}$ transitivo sobre Ω, lo cual es una contradicción.

ii) $\Rightarrow$ *i)* Supongamos que $n-2$ transposiciones generan un grupo $\mathbf{G}'$ con un subgrupo ciclico $K = \langle \rho \rangle$ transitivo sobre Ω, entonces la órbita de ρ es Ω y por lo tanto ρ es un ciclo de longitud n, esto contradice *ii)*. ■

El siguiente teorema garantiza que para σ un $n-$ciclo $n \neq 1$, se necesitan exactamente $n-1$ transposiciones como mínimo para descomponerlo.

Teorema 57 *Ningún grupo de permutaciones $\mathbf{G} \subset S_\Omega$ generado por $n-2$ transposiciones tiene un $n-$ciclo.*

Demostración. Inducción sobre n.

Para $n = 2$ sea $\Omega = \{a_1, a_2\}$ un conjunto con 2 elementos entonces T es un conjunto con $2-2=0$ transposiciones, es decir, $T = \varnothing$ de ahí que $\langle T \rangle = \{e\} = \mathbf{G}$ no puede tener ciclos de longitud 2.

Supongamos que el teorema es cierto para $n = k$. Si $\Omega = \{a_1, a_2, \cdots, a_{k-1}, a_k\}$ es un conjunto con k elementos, $T = \{\sigma_1, \sigma_2, \cdots, \sigma_{k-2}\}$ es un conjunto con $k-2$ transposiciones y $\mathbf{G} = \langle T \rangle$ y entonces $\mathbf{G}$ no tiene $k-$ciclos.

Consideremos el caso $n = k+1$, $\Omega = \{a_1, a_2, \cdots, a_{k-1}, a_k, a_{k+1}\}$ es un conjunto con $k+1$ elementos, $T = \{\sigma_1, \sigma_2, \cdots, \sigma_{k-1}\}$ es un conjunto con $k-1$ transposiciones y sea $\mathbf{G} = \langle T \rangle$.

Como T es un conjunto con $k-1$ transposiciones, entonces existe $y \in \Omega$ tal que $\sigma(y) = y$ para todo $\sigma \in T$ o existe sólo un $\sigma \in T$ tal que $\sigma = (x, y) \in T$ para algun $x \in T$.

Consideremos $\Omega' = \Omega - \{y\}$ y $T' = T - \{\sigma\}$ entonces Ω' es un conjunto con k elementos y T' es un conjunto con $k-2$ transposiciones, por hipótesis de inducción $\langle T' \rangle$ no tiene $k-$ciclos que pertenezcan a $S_{\Omega'}$.

El subgrupo generado por T mueve a lo más un elemento más de Ω de los que mueve el subgrupo generado por T', por lo tanto el subgrupo generado por T no puede tener un $(k+1)$ −ciclo. ■

Como consecuencia del teorema 57 tenemos la siguiente proposición:

Proposición 58 *El número necesario mínimo de transposiciones para descomponer un ciclo de longitud* n, $n \geq 2$ *es* $n-1$.

La proposición anterior y el teorema 43 permiten obtener el siguiente teorema:

Teorema 59 *Sea* $\pi \in S_n$, π *diferente de la identidad en* S_n. $\pi = \sigma_1\sigma_2\cdots\sigma_r$ *un producto de ciclos ajenos, entonces* $n-r$ *es el número mínimo de transposiciones necesario para descomponer* π *como producto de transposiciones.*

Capítulo 3

Descomposición de permutaciones como producto de transposiciones II.

En este capítulo probaremos usando técnicas de álgebra lineal que si $n \geq 2$, el número mínimo de transposiciones necesarias para descomponer una permutación $\pi \in S_n$, π diferente de la identidad, es $n - r$, con r el número de ciclos ajenos diferentes de π incluyendo los posibles ciclos triviales.

Para este fin hacemos actuar el grupo S_n sobre $\mathbf{R}^n$.

Sea $\beta = \{e_1, e_2, \cdots, e_n\}$ la base canónica de $\mathbf{R}^n$. Para $\pi \in S_n$ y $v = \sum_{i=1}^{n} a_i e_i \in \mathbf{R}^n$ definamos $\varphi : S_n \times \mathbf{R}^n \to \mathbf{R}^n$ tal que

$$\varphi\left(\pi, \sum_{i=1}^{n} a_i e_i\right) = \pi\left(\sum_{i=1}^{n} a_i e_i\right) = \sum_{i=1}^{n} a_i e_{\pi(i)}$$

φ es una acción de S_n sobre $\mathbf{R}^n$.

Veamos que φ es en efecto una acción, para esto verificamos que se cumplen las condiciones de la definición 17.

Sea $e \in S_n$ la identidad entonces $e\left(\sum_{i=1}^{n} a_i e_i\right) = \sum_{i=1}^{n} a_i e_{e(i)} = \sum_{i=1}^{n} a_i e_i$.

Sean $\sigma, \rho \in S_n$ entonces por definición

$$(\sigma\rho)\left(\sum_{i=1}^{n} a_i e_i\right) = \sum_{i=1}^{n} a_i e_{\sigma\rho(i)}$$

por otro lado

$$\sigma\left(\rho\left(\sum_{i=1}^{n} a_i e_i\right)\right) = \sigma\left(\sum_{i=1}^{n} a_i e_{\rho(i)}\right) = \sum_{i=1}^{n} a_i e_{\sigma\rho(i)}.$$

Por lo tanto φ define una acción de de S_n sobre $\mathbf{R}^n$.

Nótese que esta acción se puede ver desde el punto de vista del álgebra lineal como la función lineal $T_\pi : \mathbf{R}^n \to \mathbf{R}^n$ definida por:

$$T_\pi\left(\sum_{1=1}^{n} a_i e_i\right) = \sum_{1=1}^{n} a_i e_{\pi(i)}$$

Esta transformación permuta coordenadas de elementos de $\mathbf{R}^n$.

La matriz asociada a T_π con respecto a β la base canónica de $\mathbf{R}^n$ pertenece a una clase particular de matrices llamadas matrices permutación.

Definición 60 *Una matriz permutación es aquella obtenida de la identidad mediante intercambio de renglones (columnas).*

Ejemplo 61 *Si $\pi = (1,3) \in S_3$ y $\beta = \{e_1, e_2, e_3\}$ es la base canónica de $\mathbf{R}^3$, T_π es la función lineal $T_\pi : \mathbf{R}^3 \to \mathbf{R}^3$ definida por*

$$T_\pi(e_1) = e_{\pi(1)} = e_3$$
$$T_\pi(e_2) = e_{\pi(2)} = e_2$$
$$T_\pi(e_3) = e_{\pi(3)} = e_1$$

Obsérvese que si $\overline{x} = (x_1, x_2, x_3)$, entonces $T_\pi(\overline{x}) = (x_3, x_2, x_1)$.

Esta función lineal tiene la siguente matriz asociada respecto a β:

$$[T]_\beta = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = A_\pi$$

Esta matriz se obtiene de la identidad al intercambiar el primer renglón con el tercero. (o bien primera columna con la tercera).

Proposición 62 *Sean $\pi, \sigma \in S_n$ entonces $T_\sigma \circ T_\pi = T_{\sigma\pi}$*

Demostración. Es inmediata del hecho de que φ es una acción de S_n sobre $\mathbf{R}^n$. ■

En particular si $\pi = \sigma_1\sigma_2\cdots\sigma_r$ es un producto de r ciclos ajenos tenemos la siguiente igualdad:

$$T_\pi = T_{\sigma_1}T_{\sigma_2}\cdots T_{\sigma_r}$$

Proposición 63 *Si $\pi \in S_n$, $1 \in \mathbf{R}$ es valor propio de T_π.*

Demostración. Descompóngase π como producto de ciclos ajenos, y sea $\sigma = (a_1, a_2, \cdots, a_k)$ un ciclo de π, entonces el vector

$$u_\sigma = e_{a_1} + e_{a_2} + \cdots + e_{a_k} \in \mathbf{R}^n$$

es un vector propio asociado al valor propio $\lambda = 1$.

En efecto

$$\begin{aligned} T_\pi(u) &= T_\pi\left(e_{a_1} + e_{a_2} + \cdots + e_{a_{k-1}} + e_{a_k}\right) \\ &= e_{\pi(a_1)} + e_{\pi(a_2)} + \cdots + e_{\pi(a_{k-1})} + e_{\pi(a_k)} \\ &= e_{\sigma(a_1)} + e_{\sigma(a_2)} + \cdots + e_{\sigma(a_{k-1})} + e_{\sigma(a_k)} \\ &= e_{a_2} + e_{a_3} + \cdots + e_{a_k} + e_{a_1} \\ &= u \end{aligned}$$

Esto es, u es un vector propio de T_π asociado al valor propio $\lambda = 1$. ■

Observación 12 *Si $\pi \in S_n$, se descompone como un producto de r ciclos ajenos $\sigma_1, \sigma_2, \cdots, \sigma_r$, por cada ciclo σ_i $i = 1, 2, \cdots, r$ podemos construir un vector propio u_{σ_i} asociado al valor propio $\lambda = 1$. La contrucción es la hecha en la demostración de la proposición anterior.*

Definición 64 *Si $\pi \in S_n$, al conjunto $\{v \in \mathbf{R}^n \mid T_\pi(v) = v\}$ lo llamamos el espacio propio de T_π asociado al valor $\lambda = 1$ y lo denotamos por V_π.*

Ejemplo 65 *Sea $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$, $\pi = (1,3)(2)$. La función lineal T_π es la dada en el ejemplo 61. $u_1 = e_1 + e_3$ y $u_2 = e_2$ son vectores propios de T_π asociados al valor propio $\lambda = 1$. Los vectores u_1 y u_2 forman una base para el espacio propio V_π.*

Claramente el conjunto $\{u_1, u_2\}$ es linealmente independiente, por lo que es suficiente probar que si $\overline{x} \in \mathbf{R}^3$ tal que $\overline{x} \in V_\pi$ entonces es combinación lineal de u_1 y u_2.

Sea $\overline{x} = (x_1, x_2, x_3) \in V_\pi$ *entonces* $T_\pi(x_1, x_2, x_3) = (x_1, x_2, x_3)$ *pero también*

$$\begin{aligned} T_\pi(x_1, x_2, x_3) &= T_\pi(x_1 e_1 + x_2 e_2 + x_3 e_3) \\ &= x_1 T_\pi(e_1) + x_2 T_\pi(e_2) + x_3 T_\pi(e_3) \\ &= x_1 e_{\pi(1)} + x_2 e_{\pi(2)} + x_3 e_{\pi(3)} \\ &= x_1 e_{[(1,3)(2)](1)} + x_2 e_{[(1,3)(2)](2)} + x_3 e_{[(1,3)(2)](3)} \\ &= x_1 e_3 + x_2 e_2 + x_3 e_1 \\ &= (x_3, x_2, x_1) \end{aligned}$$

de lo anterior tenemos que $(x_1, x_2, x_3) = (x_3, x_2, x_1)$ *así que* $x_1 = x_3$ *y entonces*

$$\begin{aligned} (x_1, x_2, x_3) &= (x_3, x_2, x_3) \\ &= x_3(e_1 + e_3) + x_2 e_2 \\ &= x_3 u_1 + x_2 u_2 \end{aligned}$$

Por lo tanto $\{u_1, u_2\}$ *genera al espacio propio* V_π. *y concluimos que* $\{u_1, u_2\}$ *es base de* V_π.

Ejemplo 66 *Para* $\pi = (1,3)(2,5)(4) \in S_5$. $u_1 = e_1 + e_3$, $u_2 = e_2 + e_5$, *y* $u_3 = e_4$ *son vectores propios de* T_π *correspondientes al valor* $\lambda = 1$. *El conjunto de vectores* $\{u_1, u_2, u_3\}$ *es base para el espacio propio* V_π.

El conjunto $\{u_1, u_2, u_3\}$ *es linealmente independiente pues si*

$$\mu_1 u_1 + \mu_2 u_2 + \mu_3 u_3 = 0$$

entonces

$$\mu_1(e_1 + e_3) + \mu_2(e_2 + e_5) + \mu_3 e_3 = 0$$

la cual es una combinación lineal de elementos de la base canónica de $\mathbf{R}^5$ *y por lo tanto* $\mu_i = 0$, *con* $i = 1, 2, 3$. *Por lo tanto* $\{u_1, u_2, u_3\}$ *es linealmente independiente.*

Se puede probar que el conjunto $\{u_1, u_2, u_3\}$ *genera el espacio propio asociado a* V_π *con el mismo argumento al empleado en el ejemplo 65.*

Ejemplo 67 *Sea* $\pi = (2,3,5)(1,6)(4)(7) \in S_7$. $u_1 = e_2 + e_3 + e_5$, $u_2 = e_1 + e_6$, $u_3 = e_4$ *y* $u_4 = e_7$ *son vectores propios asociados al valor* $\lambda = 1$. *Estos vectores forman una base para* V_π.

Los ejemplos anteriores sugieren la siguiente proposición:

Proposición 68 *Sea $\pi = \sigma_1\sigma_2\cdots\sigma_r \in S_n$ con $\sigma_1, \sigma_2, \cdots, \sigma_r$ los ciclos ajenos de π, incluyendo los posibles ciclos triviales. Si $u_1, u_2, \cdots, u_r$, son los r vectores propios obtenidos según la observación 12 entonces $\{u_1, u_2, \cdots, u_r\}$ es base del espacio propio V_π y por consiguiente* $\dim V_\pi = r$.

Demostración. Escribamos los ciclos σ_i como $\sigma_i = (a_{i,1}, a_{i,2}, \cdots, a_{i,s_i})$, es decir,

$$\begin{aligned}
\sigma_1 &= (a_{1,1}, a_{1,2}, \cdots, a_{1,s_1}) \\
\sigma_2 &= (a_{2,1}, a_{2,2}, \cdots, a_{2,s_2}) \\
&\vdots \\
\sigma_r &= (a_{r,1}, a_{r,2}, \cdots, a_{r,s_r}).
\end{aligned}$$

Según la observación 12 el vector u_i correspondiente al ciclo σ_i es:

$$u_i = e_{a_{i,1}} + e_{a_{i,2}} + \cdots + e_{a_{i,s_i}} = \sum_{j=1}^{s_i} e_{a_{i,j}}$$

Si $\mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_r u_r = 0$ entonces

$$\begin{aligned}
\mu_1 u_1 + \mu_2 u_2 + \cdots + \mu_r u_r &= \mu_1 \left(\textstyle\sum_{j=1}^{s_i} e_{a_{1,j}}\right) + \\
&+\mu_2 \left(\textstyle\sum_{j=1}^{s_i} e_{a_{2,j}}\right) + \cdots + \mu_r \left(\textstyle\sum_{j=1}^{s_i} e_{a_{r,j}}\right) \\
&= \textstyle\sum_{i=1}^{r} \sum_{j=1}^{s_i} \mu_i e_{a_{i,j}} = 0
\end{aligned}$$

Esto es una combinación lineal de los elementos de la base canónica de $\mathbf{R}^n$ igualada a 0 y entonces $\mu_i = 0$ para toda $i = 1, \cdots, r$.

Por lo tanto $\{u_1, u_2, \cdots, u_r\}$ es linealmente independiente.

Falta probar que $\{u_1, u_2, \cdots, u_r\}$ genera al espacio propio V_π.

Si $\beta = \{e_1, e_2, \cdots, e_n\}$ es la base canónica de $\mathbf{R}^n$ cambiemos el orden de β de tal forma que aparezcan primero todas las e_k con k en la órbita de σ_1; después todas las e_k con k en la órbita de σ_2 y así sucesivamente hasta obtener la base ordenada

$$\gamma = \left\{e_{a_{1,1}}, e_{a_{1,2}}, \cdots, e_{a_{1,s_1}}, e_{a_{2,1}}, e_{a_{2,2}}, \cdots, e_{a_{2,s_2}}, \cdots, e_{a_{r,1}}, e_{a_{r,2}}, \cdots, e_{a_{r,s_r}}, \right\}$$

Sea $v = \sum_{i=1}^{n} b_i e_i \in \mathbf{R}^n$ tal que $T_\pi(v) = v$. Con respecto a la base γ, v se expresa como:

$$\begin{aligned} v = \; & b_{a_{1,1}} e_{a_{1,1}} + b_{a_{1,2}} e_{a_{1,2}} + \cdots + b_{a_{1,s_1-1}} e_{a_{1,s_1-1}} + b_{a_{1,s_1}} e_{a_{1,s_1}} + \\ & b_{a_{2,1}} e_{a_{2,1}} + b_{a_{2,2}} e_{a_{2,2}} + \cdots + b_{a_{2,s_2-1}} e_{a_{2,s_2-1}} + b_{a_{2,s_2}} e_{a_{2,s_2}} + \cdots + \\ & b_{a_{r,1}} e_{a_{r,1}} + b_{a_{r,2}} e_{a_{r,2}} + \cdots + b_{a_{r,s_r-1}} e_{a_{r,s_r-1}} + b_{a_{r,s_r}} e_{a_{r,s_r}} \end{aligned} \qquad (I)$$

Aplicando T_π a v tenemos:

$$\begin{aligned} T_\pi(v) \; = \; & T_\pi\left(b_{a_{1,1}} e_{a_{1,1}} + b_{a_{1,2}} e_{a_{1,2}} + \cdots + b_{a_{1,s_1-1}} e_{a_{1,s_1-1}} + b_{a_{1,s_1}} e_{a_{1,s_1}}\right) + \\ & T_\pi\left(b_{a_{2,1}} e_{a_{2,1}} + b_{a_{2,2}} e_{a_{2,2}} + \cdots + b_{a_{2,s_2-1}} e_{a_{2,s_2-1}} + b_{a_{2,s_2}} e_{a_{2,s_2}}\right) + \cdots + \\ & T_\pi\left(b_{a_{r,1}} e_{a_{r,1}} + b_{a_{r,2}} e_{a_{r,2}} + \cdots + b_{a_{r,s_r-1}} e_{a_{r,s_r-1}} + b_{a_{r,s_r}} e_{a_{r,s_r}}\right) = \\ & b_{a_{1,1}} e_{\pi(a_{1,1})} + b_{a_{1,2}} e_{\pi(a_{1,2})} + \cdots + b_{a_{1,s_1-1}} e_{\pi\left(a_{1,s_1-1}\right)} + b_{a_{1,s_1}} e_{\pi\left(a_{1,s_1}\right)} + \\ & b_{a_{2,1}} e_{\pi(a_{2,1})} + b_{a_{2,2}} e_{\pi(a_{2,2})} + \cdots + b_{a_{2,s_2-1}} e_{\pi\left(a_{2,s_2-1}\right)} + b_{a_{2,s_2}} e_{\pi\left(a_{2,s_2}\right)} + \cdots + \\ & b_{a_{r,1}} e_{\pi(a_{r,1})} + b_{a_{r,2}} e_{\pi(a_{r,2})} + \cdots + b_{a_{r,s_r-1}} e_{\pi(a_{r,s_r-1})} + b_{a_{r,s_r}} e_{\pi(a_{r,s_r})} = \\ & b_{a_{1,1}} e_{\sigma_1(a_{1,1})} + b_{a_{1,2}} e_{\sigma_1(a_{1,2})} + \cdots + b_{a_{1,s_1-1}} e_{\sigma_1\left(a_{1,s_1-1}\right)} + b_{a_{1,s_1}} e_{\sigma_1\left(a_{1,s_1}\right)} + \\ & b_{a_{2,1}} e_{\sigma_2(a_{2,1})} + b_{a_{2,2}} e_{\sigma_2(a_{2,2})} + \cdots + b_{a_{2,s_2-1}} e_{\sigma_2\left(a_{2,s_2-1}\right)} + b_{a_{2,s_2}} e_{\sigma_2\left(a_{2,s_2}\right)} + \cdots + \\ & b_{a_{r,1}} e_{\sigma_r(a_{r,1})} + b_{a_{r,2}} e_{\sigma_r(a_{r,2})} + \cdots + b_{a_{r,s_r-1}} e_{\sigma_r(a_{r,s_r-1})} + b_{a_{r,s_r}} e_{\sigma_r(a_{r,s_r})} = \\ & = b_{a_{1,1}} e_{a_{1,2}} + b_{a_{1,2}} e_{a_{1,3}} + \cdots + b_{a_{1,s_1-1}} e_{a_{1,s_1}} + b_{a_{1,s_1}} e_{a_{1,1}} + \\ & b_{a_{2,1}} e_{a_{2,2}} + b_{a_{2,2}} e_{a_{2,3}} + \cdots + b_{a_{2,s_2-1}} e_{a_{2,s_2}} + b_{a_{2,s_2}} e_{a_{2,1}} + \cdots + \\ & b_{a_{r,1}} e_{a_{r,2}} + b_{a_{r,2}} e_{a_{r,3}} + \cdots + b_{a_{r,s_r-1}} e_{a_{r,s_r}} + b_{a_{r,s_r}} e_{a_{r,1}} \end{aligned} \qquad (II)$$

Como $T_\pi(v) = v$ comparando la expresión obtenida para $T_\pi(v)$ en (II) con la expresión de v obtenida en (I) obtenemos las siguientes igualdades:

$$\begin{aligned} b_{a_{1,1}} = b_{a_{1,2}}, b_{a_{1,2}} = b_{a_{1,3}}, \cdots, b_{a_{1,s_1}} = b_{a_{1,1}} \\ b_{a_{2,1}} = b_{a_{2,2}}, b_{a_{2,2}} = b_{a_{2,3}}, \cdots, b_{a_{2,s_2}} = b_{a_{2,1}} \\ \vdots \\ b_{a_{r,1}} = b_{a_{r,2}}, b_{a_{r,2}} = b_{a_{r,3}}, \cdots, b_{a_{r,s_r}} = b_{a_{r,1}} \end{aligned}$$

de lo que se sigue que:

$$\begin{aligned} v = \; & b_{a_{1,1}}\left(e_{a_{1,1}} + e_{a_{1,2}} + \cdots + e_{a_{1,s_1}}\right) + \\ & b_{a_{2,1}}\left(e_{a_{2,1}} + e_{a_{2,2}} + \cdots + e_{a_{2,s_2}}\right) + \\ & \vdots \\ & +b_{a_{r,1}}\left(e_{a_{r,1}} + e_{a_{r,2}} + \cdots + e_{a_{r,s_r}}\right) \\ = \; & b_{a_{1,1}}u_1 + b_{a_{2,1}}u_2 + + b_{a_{r,1}}u_r \end{aligned}$$

Por lo tanto $\{u_1, u_2, \cdots, u_r\}$ es base de V_π. ■

La proposición 68 nos permite concluir el siguiente corolario:

Corolario 69 *La dimensión de V_π es r, con r es el número de ciclos ajenos de π, incluyendo los posibles ciclos triviales.*

Observación 13 *En el caso de una transposición $\sigma = (i,j) \in S_n$, $i < j$, hay exactamente $n-1$ vectores propios de T_σ linelamente independientes asociados al valor propio $\lambda = 1$.*

Los vectores $e_1, e_2, \cdots, e_{i-1}, e_{i+1}, \cdots, e_{j-1}, e_{j+1}, \cdots, e_n, e_i + e_j$ forman una base para V_σ. Por lo tanto $\dim(V_\sigma) = n - 1$.

Definición 70 *Sea $\sigma = (i,j) \in S_n$ con $i < j$. Al vector $v = e_i - e_j$ le llamaremos el* vector asociado *a σ.*

Proposición 71 *Sea $\sigma = (i,j) \in S_n$ con $i < j$. $-1 \in \mathbf{R}$ es valor propio de T_σ correspondiente al vector asociado a σ.*

Demostración. $T_\sigma(e_i - e_j) = e_j - e_i = -(e_i - e_j)$ ■

Observación 14 *Si $\sigma = (i,j) \in S_n$ con $i < j$ y $v = e_i - e_j$ el vector asociado a σ, entonces*

$$\dim(\mathbf{R}^n) = n = 1 + (n-1) = \dim\langle v\rangle + \dim V_\sigma.$$

Proposición 72 *Si $\sigma = (i,j) \in S_n$ con $i < j$ y v es el vector asociado a σ, entonces el complemento ortogonal de v es V_σ, es decir, $\langle v\rangle^\perp = V_\sigma$ donde $\langle v\rangle^\perp$ denota al complemento ortogonal de v.*

Demostración. Por la observación 13 V_σ, está generado por $e_1, e_2, \cdots, e_{i-1}, e_{i+1}, \cdots, e_{j-1}, e_{j+1}, \cdots, e_n, e_i + e_j$. De la definición de v es inmediato que con el producto escalar usual de $\mathbf{R}^n$, $\langle v, u \rangle = 0$ para todo $u \in V_\sigma$. ■

Con lo anterior estamos en condiciones de probar el siguiente resultado.

Teorema 73 *Sea $\pi \in S_n$ si $\pi = \tau_1 \tau_2 \cdots \tau_r$ con $\tau_1, \tau_2, \cdots, \tau_r$ los ciclos ajenos de incluyendo los posibles ciclos triviales, entonces π no puede escribirse como producto de menos de $n - r$ transposiciones, donde r es el número de ciclos ajenos de π incluyendo los posibles ciclos triviales.*

Demostración. Supongamos que $\pi = \sigma_1 \sigma_2 \cdots \sigma_k$ con cada σ_i una transposición. Demostraremos que $k \geq n - r$.

A cada σ_i le hacemos corresponder su vector asociado v_i.

Por la proposición 72 cada v_i es ortogonal al subespacio V_{σ_i}.

Sea $V = \langle \{v_1, v_2, \cdots, v_k\} \rangle$ el subespacio de $\mathbf{R}^n$ generado por los vectores asociados a $\sigma_1, \sigma_2, \cdots, \sigma_k$.

Es inmediato que $\dim V \leq k$, de donde se sigue

$$n - \dim V \geq n - k. \qquad (I)$$

Por otro lado $\mathbf{R}^n = V \oplus V^\perp$, de donde se sigue $n = \dim V + \dim V^\perp$ y entonces

$$\dim V^\perp = n - \dim V \qquad (II)$$

De las expresiones (I) y (II) se tiene la desigualdad

$$\dim V^\perp \geq n - k \qquad (III)$$

Sea $\gamma = \{w_1, w_2, \cdots, w_{n-k}\}$ un subconjunto de $V^\perp$, $\langle w_s, v_i \rangle = 0$, entonces por la proposición 72 se tiene que $w_s \in V_{\sigma_i}$ lo que implica que w_s es dejado fijo por T_{σ_i} para toda $i = 1, 2, \cdots, k$ y entonces $T_\pi(w_s) = w_s$, es decir, $w_s \in V_\pi$.

Por lo tanto $V^\perp \subset V_\pi$ y entonces $\dim V^\perp \leq \dim V_\pi$.

Por (III) $n-k \leq \dim V^{\perp}$ y por el corolario 69 $\dim V_{\pi} = r$.

Por lo tanto $n-k \leq r$, de donde

$$n-r \leq k \blacksquare$$

Usando la notación anterior se sabe que $\pi \in S_n$ se puede descomponer como producto de $n-r$ transposiciones, (teorema 53) y usando el teorema anterior encontramos nuevamente el mismo resultado enunciado en el teorema 59.

Observación 15 *Para* $v = (a_1 a_2, \ldots, a_n) \in \mathbf{R}^n$,

$$\langle v \rangle^{\perp} = \{\overline{x} \in \mathbf{R}^n \mid \langle v, \overline{x} \rangle = 0\}$$

Si $\overline{x} \in \langle v \rangle^{\perp}$, *entonces* $0 = \langle v, \overline{x} \rangle = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$, *en particular si* v *es un vector asociado a una transposición* $\sigma = (i,j) \in S_n$, $n \geq 2$, $i < j$, *el subespacio* $\langle v \rangle^{\perp} = V_{\sigma}$ *se puede caracterizar como el conjunto de soluciones de una ecuación lineal homogenea*

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0$$

Definición 74 *Sea* $\pi \in S_n$ *y* $\sigma_1 \sigma_2 \cdots \sigma_k$ *una descomposición para* π *como producto de transposiciones. Diremos que el producto* $\sigma_1 \sigma_2 \cdots \sigma_k$ *es una representación mínima de* π *si* k *es el número mínimo de transposiciones necesarias para descomponer* π *como producto de transposiciones.*

Teorema 75 *Si* $\pi = \sigma_1 \sigma_2 \cdots \sigma_k$ *es una representación mínima de* π *y* v_i *es el vector asociado a* σ_i *para* $i = 1, 2, \ldots, k$ *entonces el conjunto* $\{v_1, v_2, \cdots, v_k\}$ *es linealmente independiente.*

Demostración. Para cada σ_i consideremos el subespacio V_{σ_i} y por la observación 15 los elementos de cada subespacio V_{σ_i} se pueden caracterizar como las soluciones de una ecuación lineal homogenea en n indeterminadas.

Con las k ecuaciones lineales obtenidas a partir de las V_{σ_i} formamos un sistema de k ecuaciones lineales homogeneas con n indeterminadas.

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ &\vdots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &= 0 \end{aligned} \qquad (*)$$

o bien en forma matricial $A\overline{x} = 0$, con A la matriz asociada al sistema $(*)$.

Notamos que el subespacio $\cap_{i=1}^{k} V_{\sigma_i}$ es el conjunto de soluciones del sistema $(*)$. Como $\pi = \sigma_1\sigma_2\cdots\sigma_k$ es una representación mínima, entonces $k = n - r$ con r el número de ciclos ajenos de π y entonces el sistema $(*)$ tiene soluciones no triviales.

El espacio de soluciones para $(*)$ es el espacio nulo de A. Si $Nul\,(A)$ denota la dimensión del espacio nulo de A entonces $Nul\,(A) = \dim\left(\cap_{i=1}^{k} V_{\sigma_i}\right)$ porque el espacio nulo de A es igual a $\cap_{i=1}^{k} V_{\sigma_i}$.

Por otra parte A es una matriz de k renglores y n columnas por lo tanto el rango de A denotado por $Ran\,(A)$ cumple que

$$Ran\,(A) \leq k \qquad (I)$$

Por el teorema de la dimensión en álgebra lineal se tiene la igualdad

$$n = Nul\,(A) + Ran\,(A) \qquad (II)$$

De (I) y (II) se tiene $n \leq Nul\,(A) + k$ y entonces $n - k \leq Nul\,(A)$.

Por lo tanto se tiene

$$n - k \leq \dim\left(\cap_{i=1}^{k} V_{\sigma_i}\right) \qquad (III)$$

Por otro lado

$$\mathrm{R}^n = V_\pi \oplus V_\pi^{\perp}$$

como $\cap_{i=1}^{k} V_{\sigma_i} \subset V_\pi$, entonces $\dim\left(\cap_{i=1}^{k} V_{\sigma_i}\right) \leq \dim V_\pi$ y como $\pi = \sigma_1\sigma_2\cdots\sigma_k$ es una represen-

tación mínima de π, entonces $\dim V_\pi = r = n - k$, de donde

$$\dim\left(\cap_{i=1}^{k} V_{\sigma_i}\right) \leq n - k \qquad (IV)$$

De (III) y (IV) se tiene $\dim\left(\cap_{i=1}^{k} V_{\sigma_i}\right) = \dim V_\pi$ y por consiguiente

$$\left(\cap_{i=1}^{k} V_{\sigma_i}\right) = V_\pi$$

Como $Nul\,(A) = \dim\left(\cap_{i=1}^{k} V_{\sigma_i}\right) = \dim V_\pi = n - k$ entonces en (II) se tiene

$$n = n - k + Ran\,(A)$$

de donde $Ran\,(A) = k$.

Por lo tanto los renglones de A son linealmente independientes y por lo tanto los vectores $v_1, v_2, \cdots, v_k$ son linealmente independientes. ■

Corolario 76 *Si $\pi = \sigma_1\sigma_2\cdots\sigma_k$ es una representación mínima, entonces el conjunto de vectores $\{v_1, v_2, \cdots, v_k\}$, ($v_i$ asociados a σ_i) es base del subespacio $V_\pi^\perp$.*

Demostración. Para $\pi \in S_n$ se cumple $\mathrm{R}^n = V_\pi \oplus V_\pi^\perp$.

En la demostración del teorema anterior se tienen dos resultados:

$$V_\pi = \cap_{i=1}^{k} (V_{\sigma_i}) = \cap_{i=1}^{k} \langle v_i\rangle^\perp \qquad (I)$$

y

$$\dim V_\pi = n - k \qquad (II)$$

Si $v \in V_\pi$ entonces $v \in \cap_{i=1}^{k} \langle v_i\rangle^\perp$. De lo anterior $v \in \langle v_i\rangle^\perp$ para toda $i = 1, 2, \cdots, k$. Por lo cual $\langle v, v_i\rangle = 0$ para toda i. De aquí que $v_i \in V_\pi^\perp$ para toda $i = 1, 2, \cdots, k$.

De lo anterior $\{v_1, v_2, \cdots, v_k\}$, es un conjunto linealmente independiente contenido en $V_\pi^\perp$.

Como $\mathrm{R}^n = V_\pi \oplus V_\pi^\perp$ y por (II) tenemos $\dim V_\pi^\perp = k$.

Por lo tanto $\{v_1, v_2, \cdots, v_k\}$ es base de $V_\pi^\perp$. ■

Proposición 77 *Sea $\pi = \tau_1\tau_2\cdots\tau_r \in S_n$ un producto de ciclos ajenos. Si $\pi = \sigma_1\sigma_2\cdots\sigma_k$ es*

una representación mínima, entonces para cada $\sigma_i = (a_i, b_i)$ se tiene que a_i y b_i corresponden a un mismo ciclo de π.

Demostración. Sean $\tau_c, \tau_d \in S_n$ dos ciclos ajenos de π.

Supongamos que existe una transposición $\sigma_i = (a, b) \in S_n$ para alguna $i = 1, 2, \cdots, k$, con $a < b$, a y b en órbitas distintas bajo π. (ciclos ajenos). Sea el v_i vector aosciado a σ_i.

Como $\sigma_1\sigma_2\cdots\sigma_k$ es una representación mínima, $\{v_1, v_2, \cdots, v_k\}$ el conjunto de vectores asociados es base de $V_\pi^\perp$.

Consideremos el vector

$$u = \sum_{a_j \in \theta(\tau_c)} e_{a_j}$$

Con $\theta(\tau_c)$ la órbita de a bajo π. Entonces $u_1 \in V_\pi$.

El producto

$$\begin{aligned} \langle v, u\rangle = \; & \langle e_a - e_b, e_{a_1} + e_{a_2} + \cdots + e_{a_t}\rangle = \\ & \langle e_a, e_{a_1} + e_{a_2} + \cdots + e_{a_t}\rangle - \langle e_b, e_{a_1} + e_{a_2} + \cdots + e_{a_t}\rangle = \\ & 1 - 0 = 1 \neq 0 \end{aligned}$$

Lo cual contradice el hecho de que $u \in V_\pi$.

Por lo tanto a y b pertenecen al mismo ciclo. ■

En la proposición anterior la condición de ser descomposición mínima es fundamental.

Ejemplo 78 *Consideremos $\pi = (1,6)(3,4)(4,6)(1,3) \in S_6$. El conjunto de vectores asociados $\{e_1 - e_6, e_3 - e_4, e_4 - e_6, e_1 - e_3\}$ no es linealmente independiente, pues*

$$e_1 - e_6 = (e_3 - e_4) + (e_4 - e_6) + (e_1 - e_3)$$

Nótese que $\pi = (1,4)(3,6)$.

Capítulo 4

Descomposición de permutaciones como producto de transposiciones III.

En este capítulo daremos una prueba para calcular el número mínimo de transposiciones necesarias para descomponer una permutación $\pi \in S_n$ como producto de transposiciones. La prueba hace uso de la teoría de gráficas. Además podremos definir la función índice ($ind(\pi)$) con $\pi \in S_n$ y probar un teorema debido a Ree.

Sea Ω un conjunto con n elementos y sea $\mathbf{T} \subset S_\Omega$ un conjunto de transposiciones. A partir de Ω y $\mathbf{T}$ construimos una gráfica denotada por $\mathcal{G}_\mathbf{T}$ considerando al conjunto Ω como conjunto de vértices y al conjunto $\mathbf{T}$ como conjunto de aristas. Inversamente, si $\mathcal{G} = (A, V)$ es una gráfica, asociamos a $\mathcal{G}$ un conjunto $\mathbf{T}_V \subset S_A$ de transposiciones.

Observación 16 *La construcción anterior es una biyección.*

Ejemplo 79 *En S_4 sea $\mathbf{T} = \{(1,2),(1,3),(2,4)\} \subset S_4$. Una representación de la gráfica $\mathcal{G}_\mathbf{T}$ asociada a $\mathbf{T}$ es la de la figura 4.1.*

Aprovechando los conceptos de la teoría de gráficas, calcular el número mínimo de transposiciones necesarias para descomponer un ciclo se reduce al siguiente lema:

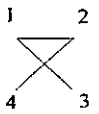


Figura 4-1:

Lema 80 *Sea* $\mathbf{T}$ *un conjunto mínimo de transposiciones que generan un subgrupo transitivo* H *sobre* Ω, *con* Ω *un conjunto con* n *elementos,* $n \geq 2$, *entonces:*

i) el número de elementos de $\mathbf{T}$ *es* $n-1$.

ii) El producto de los elementos de $\mathbf{T}$, *(en cualquier orden) es un* $n-$*ciclo.*

Demostración. *i)* A partir del conjunto $\mathbf{T}$, contruimos la gráfica asociada $\mathcal{G}_{\mathbf{T}}$.

Como $\mathbf{T}$ genera un grupo transitivo, para cada par $a_i, a_j \in \Omega$ existen transposiciones $\sigma_1, \sigma_2, \cdots, \sigma_k \in \mathbf{T}$ tal que $\sigma_1\sigma_2\cdots\sigma_k(a_i) = a_j$ y por tanto existe en $\mathcal{G}_{\mathbf{T}}$ un camino que une a_i con a_j, para todo $a_i, a_j \in \Omega$. De aquí que $\mathcal{G}_{\mathbf{T}}$ es conexa.

Se afirma que $\mathcal{G}_{\mathbf{T}}$ es un árbol.

Como $\mathcal{G}_{\mathbf{T}}$ es conexa resta probar que $\mathcal{G}_{\mathbf{T}}$ no tiene ciclos.

Supóngamos que $\mathcal{G}_{\mathbf{T}}$ no es un árbol, entonces en $\mathcal{G}_{\mathbf{T}}$ existe un ciclo formado por aristas l_1, l_2, $\cdots$, l_k, sean σ_1, σ_2, $\cdots$, σ_k las transposiciones correspondientes, entonces el conjunto $A = \{\sigma_1, \sigma_2, \cdots, \sigma_k\} \subseteq \mathbf{T}$ tal que $\sigma_1\sigma_2\cdots\sigma_k = e \in S_\Omega$ con e la identidad en S_Ω entonces $\sigma_1\sigma_2\cdots\sigma_{k-1} = \sigma_k$ lo que implica que $\mathbf{T} - \{\sigma_k\}$ genera a H. Esto es una contradicción pues $\mathbf{T}$ es un conjunto mínimo de transposiciones que genera un subgrupo transitivo H sobre Ω.

Por lo tanto $\mathcal{G}_{\mathbf{T}}$ no tiene ciclos y $\mathcal{G}_{\mathbf{T}}$ es un árbol.

Como $\mathcal{G}_{\mathbf{T}}$ es un árbol y Ω es un conjunto con n elementos entonces $\mathcal{G}_{\mathbf{T}}$ tiene n vértices y por lo tanto $n-1$ aristas. De ahí que $n-1$ es el número de elementos de $\mathbf{T}$. Por lo tanto el número mínimo de transposiciones necesario para generar un subgrupo transitivo H sobre Ω es $n-1$.

ii) Sean $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$ los elementos de $\mathbf{T}$. El producto de los elementos de $\mathbf{T}$ es un $n-$ciclo.

La demostración se hara por inducción sobre $m = n-1$ el número de elementos de $\mathbf{T}$.

Si $m = 1$, $n = 2$, $\mathbf{T} = \{(a_1, a_2)\}$ y el producto de los elementos de $\mathbf{T}$ es (a_1, a_2) que es un $2-$ciclo.

Supongamos que el resultado se cumple para un conjunto Ω con $m+1$ elementos y $\mathbf{T}$ un conjunto con m transposiciones.

Sea Ω un conjunto con $m+2$ elementos y $\mathbf{T} = \{\sigma_1, \sigma_2, \cdots, \sigma_m, \sigma_{m+1}\}$ un conjunto mínimo de transposiciones que genera un subgrupo transitivo sobre Ω.

La gráfica $\mathcal{G}_{\mathbf{T}}$ asociada a $\mathbf{T}$ es un árbol, entonces existe al menos un vértice terminal de $\mathcal{G}_{\mathbf{T}}$. Sea a_i un vértice terminal de $\mathcal{G}_{\mathbf{T}}$ entonces existe un único $a_j \in \Omega$, tal que $(a_i, a_j) \in \mathbf{T}$, o bien $\overline{a_i, a_j} \in \mathcal{G}_{\mathbf{T}}$. Supongamos que $\sigma_1 = (a_i, a_j)$.

Sean $\mathbf{T}' = \mathbf{T} - \{\sigma_1\}$ y $\Omega' = \Omega - \{a_j\}$.

La gráfica $\mathcal{G}_{\mathbf{T}'}$ es conexa y entonces $\mathbf{T}'$ genera un subgrupo transitivo sobre Ω'. Nótese que $\mathcal{G}_{\mathbf{T}'}$ es una subgráfica conexa de $\mathcal{G}_{\mathbf{T}}$. $\mathcal{G}_{\mathbf{T}'}$ es árbol.

Como $|\mathbf{T}'| = m$, entonces por hipótesis de inducción el producto de los elementos de $\mathbf{T}'$ es un $(m+1)-$ciclo. Sea $(a_j, a_l, \cdots, a_r)$ el $(m+1)-$ciclo obtenido del producto $\sigma_2\sigma_3\cdots\sigma_m\sigma_{m+1}$.

El producto del $(m+1)-$ciclo con σ_1 es:

$$\begin{aligned}\tau = \sigma_1(\sigma_2\sigma_3\cdots\sigma_m\sigma_{m+1}) = \quad & (a_i, a_j)(a_j, a_l, \cdots, a_r) = \\ & (a_j, a_l, \cdots, a_r, a_i)\end{aligned}$$

el cual resulta ser $((m+1)+1) = m+2$ un $m+2-$ciclo.

Por lo tanto si $|\mathbf{T}| = m$ el producto de los elementos de $\mathbf{T}$ es un $(m+1)-$ciclo.

Obérvese que en el producto $\tau = \sigma_1\sigma_2\cdots\sigma_m\sigma_{m+1}$ en σ_1 aparece un vértice terminal de la gráfica $\mathcal{G}_{\mathbf{T}}$.

Si al considerar el producto $\tau = \sigma_1\sigma_2\sigma_3\cdots\sigma_{m+1}$ se tiene que en σ_1 no hay vértices terminales de $\mathcal{G}_{\mathbf{T}}$, en $\tau = \sigma_1\sigma_2\sigma_3\cdots\sigma_{m+1}$ hallamos σ_i con un vértice terminal de $\mathcal{G}_{\mathbf{T}}$, sea $\rho = \sigma_{i-1}\cdots\sigma_2\sigma_1$ y por conjugación se obtiene una permutación $\tau' = \rho\tau\rho^{-1}$. Por el teorema 48 τ y τ' tienen la misma estructura cíclica y

$$\begin{aligned}\rho\tau\rho^{-1} = \quad & (\sigma_{i-1}\cdots\sigma_2\sigma_1)(\sigma_1\sigma_2\cdots\sigma_{i-1}\sigma_i\cdots\sigma_k)(\sigma_1\sigma_2\cdots\sigma_{i-1}) = \\ & \sigma_i\sigma_{i+1}\cdots\sigma_{n-1}\sigma_1\sigma_2\cdots\sigma_{i-1} = \\ & \tau'\end{aligned}$$

En τ' se tiene el producto de todos los elementos de T con un vértice terminal en σ_i, y entonces estamos en las condiciones del caso anterior, entonces τ' es un $n-$ciclo y en consecuencia τ también es un $n-$ciclo. ■

Los subconjuntos de permutaciones X que generan un grupo transitivo sobre Ω no son únicos.

Ejemplo 81 *Sea* $\Omega = \{1,2,3,4\}$ $S_\Omega = S_4$.

Sea X= $\{(1,2),(1,3),(1,4)\}$ entonces X genera un grupo transitivo sobre Ω,ya que $\langle X \rangle = S_4$. $|X| = 3$.

El conjunto X'= $\{(1,2),(2,3),(3,4)\}$ también genera un grupo transitivo sobre Ω.

El lema 80 proporciona otra forma de calcular el número mínimo de transposiciones necesarias para descomponer un $n-$ciclo.

Teorema 82 *El número mínimo de transposiciones necesarias para descomponer un* $n-$*ciclo es* $n-1$.

Demostración. Sea Ω un conjunto con n elementos. Sea $\pi \in S_\Omega$ un $n-$ciclo, el subgrupo generado por π es transitivo sobre Ω.

Sea $T \subset S_\Omega$ un subconjunto de transposiciones que genere π.

Por el lema 80, el número mínimo de transposiciones para generar π es $n-1$.

Por lo tanto el número mínimo de transposiciones necesarias para descomponer un $n-$ciclo es $n-1$. ■

Considerando que toda permutación π se descompone como producto de ciclos ajenos en forma única, aplicando el lema a cada uno de los ciclos de la permutación π se obtiene otra demostración del teorema:

Teorema 83 *Dada una permutación* $\pi \in S_n$, *producto de* r *ciclos ajenos, se requiere un mínimo de* $n-r$ *transposiciones para descomponer* π *como producto de transposiciones.*

Definición 84 *Para* π *un ciclo de longitud* k, *definimos la función índice de* π *como:*

$$\upsilon(\pi) = k - 1$$

Definición 85 *Sea Ω un conjunto con n elementos y supóngase que $\pi = \pi_1\pi_2\cdots\pi_k \in S_\Omega$ es un producto de ciclos disjuntos, entonces definimos el índice de π como*

$$\upsilon(\pi) = \sum_{i=1}^{k} \upsilon(\pi_i)$$

Observación 17 *La función índice de está bien definida por la unicidad de la descomposición de π en ciclos ajenos.*

Ejemplo 86 *Consideremos* $\Omega = \{1,2,3,4\}$.

Sea $\pi_1 = (1,2,3) \in S_\Omega = S_4$, *entonces* $\upsilon(\pi_1) = 3-1 = 2$.

Sea $\pi_2 = (1,2)$ *entonces* $\upsilon(\pi_2) = 2-1 = 1$.

Sea $\pi_3 = (1,2)(3,4)$ *entonces* $\upsilon(\pi_3) = \upsilon(1,2) + \upsilon(3,4) = (2-1)+(2-1) = 2$.

Observación 18 *Si $\pi \in S_n$ es un $n-$ciclo entonces por definición $\upsilon(\pi) = n-1$, pero $n-1$ es el número mínimo de transposiciones necesarias para descomponer π, de aquí que si $t(\pi)$ es el número mínimo de transposiciones necesarias para descomponer π entonces $\upsilon(\pi) = n-1 = t(\pi)$.*

El teorema siguiente es un adelanto hacia el teorema de Ree.

Teorema 87 *Sea Ω un conjunto con n elementos y $\mathrm{T} = \{\pi_1, \pi_2, \cdots, \pi_m\}$ un conjunto de permutaciones que genera un subgrupo transitivo sobre Ω entonces*

$$\upsilon(\pi_1) + \upsilon(\pi_2) + \cdots + \upsilon(\pi_m) \geq n-1$$

Demostración. En virtud de la observación 18 podemos suponer que cada π_i es una transposición entonces

$$\upsilon(\pi_1) + \upsilon(\pi_2) + \cdots + \upsilon(\pi_m) = m$$

Como el grupo generado por T es transitivo, la gráfica asociada $\mathcal{G}_\mathrm{T}$ es conexa y con n vértices, entonces al menos hay $n-1$ aristas y en consecuencia $n-1$ transposiciones.

$$\upsilon(\pi_1) + \upsilon(\pi_2) + \cdots + \upsilon(\pi_m) = m \geq n-1 \ \blacksquare$$

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

Podemos enunciar el siguiente corolario a partir del teorema ant

Corolario 88 *Si* $\mathbf{T} = \{\pi_1, \pi_2, \cdots, \pi_m\}$ *genera un subgrupo transitivo sobre* Ω, Ω *un conjunto con* n *elementos y*

$$v(\pi_1) + v(\pi_2) + \cdots + v(\pi_m) = n - 1$$

entonces $\pi_1\pi_2\cdots\pi_m$ *es un ciclo de longitud* n, *independientemente del orden en que se efectúe el producto.*

Demostración. Igual que en el corolario anterior podemos suponer que cada π_i es una transposición.

Como $v(\pi_1) + v(\pi_2) + \cdots + v(\pi_m) = n - 1$ entonces $m = n - 1$ y como $\mathbf{T}$ genera un subgrupo transitivo sobre Ω entonces por el lema 80 se tiene el resultado.

Ahora estamos en condiciones de probar el teorema de Ree.

Teorema 89 *Sea* Ω *un conjunto con* n *elementos. Sea* $\mathbf{T} = \{\pi_1, \pi_2, \cdots, \pi_m\}$ *permutaciones que actúan sobre un conjunto* Ω, *tal que*

$\pi_1\pi_2\cdots\pi_m = e$ *entonces*

$$v(\pi_1) + v(\pi_2) + \cdots + v(\pi_m) \geq 2(n - s)$$

donde s *es el número de componentes transitivos generado por* $\{\pi_1, \pi_2, \cdots, \pi_m\}$.

Demostración. Caso 1) $s = 1$.

Sea Ω un conjunto con n elementos. Nos interesa calcular el valor de v sobre las permutaciones de $\mathbf{T}$. Por la observación 18 podemos suponer que $\mathbf{T}$ es un conjunto de transposiciones.

Como $\mathbf{T}$ genera un subgrupo con una órbita entonces $\mathbf{T}$ es transitivo sobre Ω. Por el teorema 87, $m \geq n - 1$.

Por el lema 80, si $\mathbf{T}' \subset \mathbf{T}$ es un subconjunto mínimo de transposiciones que genere un subgrupo transitivo sobre Ω entonces el número de elementos de $\mathbf{T}'$ es $r = n - 1$.

Sea $\mathbf{T}' = \{\pi_{i_1}, \pi_{i_2}, \cdots, \pi_{i_r}\} \subset \mathbf{T}$ un subconjunto mínimo de transposiciones que genere un subgrupo transitivo sobre Ω. Por la segunda parte del lema 80, el producto de los elementos de $\mathbf{T}'$ es un $n-$ciclo, con lo cual si $\pi_{i_k} \in \mathbf{T}'$ $k = 1, 2, \cdots, r$, entonces $(\pi_{i_k})^{-1} \notin \mathbf{T}'$.

Como $\pi_1\pi_2\cdots\pi_m = e$, si $\pi_{i_k} \in \mathbf{T}'$, $(\pi_{i_k})^{-1} \in \mathbf{T} - \mathbf{T}'$, con lo cual si $|\mathbf{T}'| = n-1$ entonces $|\mathbf{T} - \mathbf{T}'| \geq n-1$ y así

$$|\mathbf{T}| = |\mathbf{T}'| + |\mathbf{T} - \mathbf{T}'| \geq 2(n-1)$$

Como cada elemento de $\mathbf{T}$ es una transposición se tiene que $v(\pi_i) = 1$ para toda $i = 1, 2, \cdots, m$.

Por lo tanto

$$v(\pi_1) + v(\pi_2) + \cdots + v(\pi_m) = m \geq 2(n-1)$$

con lo cual queda demostrado el teorema en el caso $s = 1$.

Caso 2) Supóngase que tenemos k órbitas.

Sean θ_i las diferentes órbitas, para cada órbita se tiene el correspondiente conjunto de permutaciones $\mathbf{T}_i'$ que actúa transitivamente sobre los elementos de θ_i.

Aplicando el caso anterior para los conjuntos tenemos:

$|\theta_i| = n_i$, $\sum_{i=1}^{k} n_i = n$, $|\mathbf{T}_i'| = m_i$, $\sum_{i=1}^{k} m_i = m$.

Para cada i se cumple el primer caso. Por lo tanto

$$v(\pi_{1_i}) + v(\pi_{2_i}) + \cdots + v(\pi_{m_i}) = m_i \geq 2(n_i - 1)$$

Sumando los correspondientes resultados, tenemos que:

$$\sum_{i=1}^{k} m_i \geq \sum_{i=1}^{k} 2(n_i - 1) = 2\sum_{i=1}^{k} (n_i - 1) = 2(n-k)$$

Por lo tanto

$$m = \sum_{i=1}^{k} m_i \geq 2(n-k)$$

Estamos suponiendo que cada permutación es una transposición, entonces

$$\sum_{\pi \in \mathbf{T}} v(\pi) = m \geq 2(n-k) \ \blacksquare$$

El teorema de Ree, teorema 89, así como la función v han sido empleados en el estudio de

superficies de Riemann. En cierto momento Ree expone dentro de su artículo [4] que la prueba directa para su teorema parecía complicada. Ree para probar su teorema, empleó cubiertas para la esfera de Riemann, requirió de una orientación y finalmente calculó el genero de la superficie por el método de Hurwitz. No es mi propósito entrar en detalles de esa demostración.

Otra caracterización para la función v.

Dada $\pi \in S_n$ podemos pensar en la función lineal T_π de $\mathbf{R}^n$ en $\mathbf{R}^n$, dada en el capítulo tres, que permuta coordenadas. La matriz asociada a esta función lineal es una matriz permutación. De ella hablamos en el capítulo tres. Una matriz permutación siempre tiene a 1 como valor propio.

Notación.- Sea $m(\pi)$ la multiplicidad de 1 pensado como valor propio de la matriz permutación.

Proposición 90 *Sea $m(\pi)$ la multiplicidad de 1 como valor propio de la matriz permutación, (función lineal T_π) entonces $v(\pi) = n - m(\pi)$.*

Demostración. En el capítulo tres se probó que el número de vectores propios asociado a la función lineal T_π es r.

El número de vectores asociados a la matriz permutación es el mismo que el de vectores propios asociados a la función lineal T_π.

Por lo tanto la multiplicidad de 1 como valor propio de la matriz permutación, es exactamente el número de ciclos ajenos en que se descompone π. De tal manera si π es producto de r ciclos ajenos, entonces $m(\pi) = r$.

Nótese que $v(\pi) = \sum_{i=1}^{r} (l(\pi_i) - 1) = n - r = n - m(\pi)$. ■

Capítulo 5

Descomposiciones diferentes de un n-ciclo.

En los capítulos anteriores se probó que el número mínimo de transposiciones necesario para descomponer una permutación $\pi \in S_n$ de n letras y r ciclos ajenos es $n - r$. En particular un $n-$ciclo se descompone como producto de $n - 1$ transposiciones. La descomposición de π como producto de transposiciones no es única, asi que en este capítulo contaremos el número de formas distintas en que se puede descomponer una permutación.

Para este fin necesitamos contar el número de árboles con n vértices etiquetados distintos.

Definición 91 *Una etiquetación para una gráfica $\mathcal{G} = (V, A)$ de n vértices será una función $f : V \to I_n$, donde $I_n = \{1, 2, \cdots, n\}$ y f es biyectiva.*

A los enteros, $1, 2, 3, \cdots, n$, se les llama etiquetas de $\mathcal{G}$.

Definición 92 *Una gráfica etiquetada es una pareja $(\mathcal{G}, f)$ con $\mathcal{G}$ una gráfica y f una etiquetación de $\mathcal{G}$.*

Nótese que esto es una etiquetación para el conjunto de vértices de $\mathcal{G}$.

Ejemplo 93 *Sea $\mathcal{G} = (V, A)$ con $V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$ y $A = \{l_1, l_2, l_3, l_4, l_5\}$ con $l_1 = \overline{v_1v_2}$, $l_2 = \overline{v_1v_3}$, $l_3 = \overline{v_1v_4}$, $l_4 = \overline{v_3v_5}$, $l_5 = \overline{v_3v_6}$, $\mathcal{G}$ es una gráfica etiquetada, más aún $\mathcal{G}$ es un árbol etiquetado.*

La figura 5.1 es una representación de $\mathcal{G}$ y corresponde a una gráfica etiquetada.

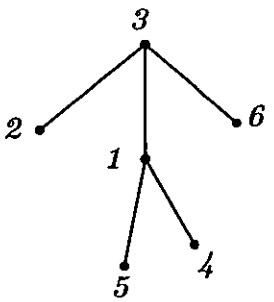


Figura 5-1: Representación de una gráfica etiquetada.

El siguiente teorema auxiliar debido a Cayley, 1889, calcula el número de arboles etiquetados distintos, que pueden ser formados con n vértices.

Teorema 94 *El número de árboles etiquetados distintos es* n^{n-2}.

Hay varias demostraciones de este teorema, en particular H. Prüfer (1918) probó que hay una correspondencia biyectiva entre los árboles etiquetados con n vértices y las sucesiones finitas distintas de $n-2$ etiquetas tomadas del conjunto con n etiquetas. En este trabajo no daremos una demostración de este teorema. Para una demostración de este teorema consultar [13].

Si $\mathcal{G}$ es un árbol entonces $\mathcal{G}$ tiene $n-1$ aristas, podemos pensar en una etiquetación para las aristas definiendo una función $\varphi : A \to J$, J un conjunto con $n-1$ elementos y φ una función biyectiva.

Una gráfica etiquetada por los vértices y las aristas será entonces una terna $(\mathcal{G}, f, \varphi)$, donde $\mathcal{G}$ es una gráfica, f es una etiquetación para los vértices de $\mathcal{G}$ y φ es una etiquetación para las aristas de $\mathcal{G}$.

Proposición 95 *El número de árboles etiquetados por vértices y aristas distintos es*

$$n^{n-2}(n-1)!.$$

Demostración. Por el teorema 94 se tiene que el número de árboles etiquetados por vértices distintos es n^{n-2}.

Para cada árbol etiquetado por sus vérices se tiene que el número de etiquetaciones posibles para las aristas es igual a las permutaciones de las $n-1$ etiquetas y por lo tanto cada árbol etiquetado por sus vértices se puede etiquetar por sus aristas de $(n-1)!$.

Por lo tanto el número total de árboles etiquetados por vértices y aristas es $n^{n-2}(n-1)!$. ■

El teorema siguiente calcula el número de formas diferentes en que un $n-$ciclo se puede descomponer como producto de transposiciones.

Teorema 96 *Sea $\rho \in S_n$ un $n-$ciclo entonces ρ se puede escribir como producto de transposiciones de n^{n-2} formas diferentes.*

Demostración. Mostraremos por inducción sobre n el número de vértices de $\mathcal{G}$ que a cada árbol etiquetado por vértices y aristas le podemos hacer corresponder un $n-$ciclo.

Claramente para $n = 2$ se cumple el resultado.

Según la expresión citada en el teorema anterior para $n = 2$ se tiene

$$n^{n-2}(n-1)! = 2^{2-2}(2-1)! = 2^0(1) = 1$$

Para $n = 2$ nuestra gráfica se reduce a dos vértices y una arista, de ahí que hay solo un árbol etiquetado y sólo hay una forma de escribir un $2-$ciclo como producto de transposiciones. Por lo tanto el teorema es válido en este caso.

Sea $n > 2$ fija y supongamos que $\forall k$ con $2 \leq k < n$, el teorema es válido, es decir, todo árbol etiquetado con k vértices y $k-1$ aristas corresponde a un $k-$ciclo. Hay que probar que todo árbol con n vértices y $n-1$ aristas etiquetadas corresponde a un $n-$ciclo.

Sea $\mathcal{G}$ un árbol etiquetado por vértices y aristas, con n vértices. Para cada arista l_i de la gráfica etiquetada $\mathcal{G}$ sea σ_i la transposición obtenida según la correspondencia dada en la observación 16, con esto obtenemos un conjunto T con $n-1$ transposiciones.

Lo anterior se da en virtud del teorema 37. Sea $\mathcal{G}$ un árbol con n vértices entonces $\mathcal{G}$ tiene $n-1$ aristas, de aquí que tengamos $n-1$ transposiciones en el conjunto T.

Sea $\mathbf{T} = \{\sigma_1, \sigma_2, \cdots, \sigma_{n-1}\}$ el conjunto de las transposiciones obtenidas de $\mathcal{G}$.

En la gráfica $\mathcal{G}$ eliminemos la arista correspondiente a $\sigma_k = (i,j)$ pero sin eliminar los vértices i,j.

Como $\mathcal{T}$ es un árbol, al eliminar una arista obtenemos dos subgráficas disconexas $\mathcal{G}'$ y $\mathcal{G}''$. Nótese que $\mathcal{G}'$ y $\mathcal{G}''$ también son árboles.

i) Sea k_1 el número de vértices de $\mathcal{G}'$ y k_2 el número de vértices de $\mathcal{G}''$ entonces $k_1 + k_2 = n$.

ii) Si $\mathcal{G}' = (A', V')$ y $\mathcal{G}'' = (A'', V'')$ entonces $A' \cap A'' = \varnothing$.

Aplicando la hipótesis inductiva a los árboles $\mathcal{G}'$ y $\mathcal{G}''$ obtenemos que el árbol $\mathcal{G}'$ corresponde a un k_1-ciclo y el árbol $\mathcal{G}''$ corresponde a un k_2-ciclo.

Supongamos que $\rho_1 = (ia_1a_2\cdots a_{k_1-1})$ es el k_1-ciclo correspondiente a $\mathcal{G}'$ y que $\rho_2 = (jb_1b_2\cdots b_{k_2-1})$ es el k_2-ciclo correspondiente a $\mathcal{G}''$.

Como $A' \cap A'' = \varnothing$ entonces los ciclos ρ_1 y ρ_2 no tienen elementos en común y por lo tanto conmutan, es decir, $\rho_1\rho_2 = \rho_2\rho_1$.

El producto $\rho_1\rho_2\sigma_1$

$$\begin{aligned}\rho_1\rho_2\sigma_1 = \quad & (ia_1a_2\cdots a_{k_1-1})(jb_1b_2\cdots b_{k_2-1})(i,j) = \\ & (ib_1b_2\cdots b_{k_2-1}ja_1a_2\cdots a_{k_1-1})\end{aligned}$$

es un $n-$ciclo.

Por lo tanto cada árbol etiquetado con n vértices y $n-1$ aristas corresponde a un $n-$ciclo.

En la proposición 49 mostramos que en S_n existen $(n-1)!$ diferentes $n-$ciclos, asi que cada ciclo se puede representar como producto de

$$\frac{n^{n-2}(n-1)!}{(n-1)!} = n^{n-2}$$

formas diferentes ■

Ejemplo 97 *Consideremos* $(1234) \in S_4$. *Según lo anterior, existen* $4^{4-2} = 4^2 = 16$ *formas diferentes para descomponer* $(1234) \in S_4$ *como producto de transposiciones. Esencialmente hay 16 gráficas distintas, cada una de ellas dá origen a un* $4-$*ciclo, pero sólo algunas dan origen al* $4-$*ciclo* (1234).

Gráfica	*Transposiciones*	*Soluciones*	*Total de soluciones*
5.2.a	$\{(12),(23),(34)\}$	$(12)(23)(34) = (1234)$	*1*
5.2.b	$\{(14),(23),(34)\}$	$(23)(34)(14) = (1234)$	*1*
5.2.c	$\{(12),(14),(34)\}$	$(34)(14)(12) = (1234)$	*1*
5.2.d	$\{(12),(14),(23)\}$	$(14)(12)(23) = (1234)$	*1*

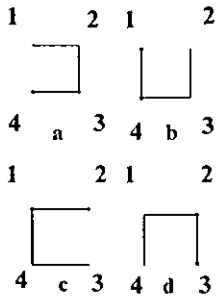


Figura 5-2: Ciclos

Gráfica	Transposiciones	Soluciones	Total de soluciones
5.3.*a*	$\{(14),(24),(23)\}$	$(24)(14)(23) = (1234) = (24)(23)(14)$	2
5.3.*b*	$\{(12),(13),(34)\}$	$(13)(12)(34) = (1234) = (13)(34)(12)$	2
5.3.*c*	$\{(14),(13),(23)\}$	$(14)(23)(13) = (1234) = (23)(14)(13)$	2
5.3.*d*	$\{(12),(24),(34)\}$	$(12)(34)(24) = (1234) = (34)(12)(24)$	2

Gráfica	Transposiciones	Soluciones	Total de soluciones
5.4.*a*	$\{(14),(24),(34)\}$	$(34)(24)(14) = (1234)$	1
5.4.*b*	$\{(13),(23),(34)\}$	$(23)(13)(34) = (1234)$	1
5.4.*c*	$\{(12),(24),(23)\}$	$(12)(24)(23) = (1234)$	1
5.4.*d*	$\{(12),(13),(14)\}$	$(14)(13)(12) = (1234)$	1

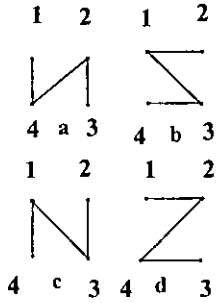


Figura 5-3: Zetas

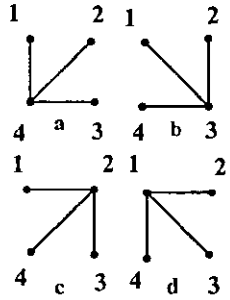


Figura 5-4: Canónicos

Gráfica	Transposiciones	Soluciones	Total de soluciones
5.5.*a*	$\{(13),(23),(24)\}$	no hay	0
5.5.*b*	$\{(12),(24),(13)\}$	no hay	0
5.5.*c*	$\{(13),(34),(24)\}$	no hay	0
5.5.*d*	$\{(13),(14),(24)\}$	no hay	0

El teorema anterior nos sirve para calcular el número total en que un ciclo puede escribirse como un producto mínimo de transposiciones. El ejemplo 97 muestra un caso particular y manejable de la aplicación del teorema. Para probar el teorema se utilizó como herramienta auxiliar la teoría de gráficas. Se mostró que cada árbol de n vértices da lugar a un $n-$ciclo.

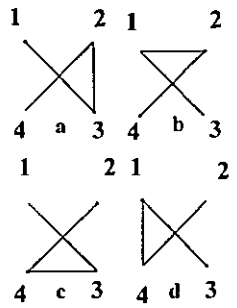


Figura 5-5: Cruzados

Una pregunta interesante es la siguiente:

Dado un $n-$ciclo, ¿Es posible saber cuáles árboles corresponden a ese $n-$ciclo?

La respuesta parece ser muy complicada.

En nuestro ejemplo existen simetrías y también puede verse que los isomorfismos de gráficas respetan la descomposición cíclica. Notamos que todas las graficas de la figura 5.4 son isomorfas entre si, pero que no representan al ciclo $(1,2,3,4)$, mientras que las gráficas de la figura 5.2 son isomorfas y cada una de ellas da origen a dos descomposiciones distintas para el ciclo $(1,2,3,4)$.

Definición 98 *Dos gráficas $\mathcal{G} = (A,V)$ y $\mathcal{G}' = (A',V')$ son isomorfas si existe una función biyectiva f entre A y A' tal que si los vértices $a_1, a_2 \in A$ son adyacentes, entonces los vértices $f(a_1), f(a_2) \in A'$ también son adyacentes.*

Otra pregunta interesante es tratar de generalizar el resultado anterior para que, en lugar de contar las diferentes formas para descomponer un ciclo, lo intentáramos hacer para permutaciones en general.

La pregunta es una curiosidad matemática interesante. La solución es un problema de cálculo combinatorio y el número buscado depende de la longitud de los ciclos y del número de ciclos ajenos que intervienen en la descomposición. Es complicado dar una expresión que calcule este número.

Bibliografía

[1] George Mackiw. Permutations as Products of Transpositions. American Mathematical Monthly. May 1995. 438, 439, 440.

[2] Walter Feit, Roger Lyndonn and Leonard Scott. A remark about permutations. Journal of Combinatorial Theory. (A) 18. 1975. 234-235.

[3] O. P. Lossers. Solution to problem E3058. American Mathematical Monthly. 93. 1986, 820, 821.

[4] R. Ree. A theorem on permutations. Journal of combinatorial Theory 10 (1971), 174-175.

[5] John B. Fraleigh. A first course in abstract algebra. Addison-Wesley Pub. 5ª Ed. 1994.

[6] Joseph J. Rotman. An introduction to the theory of groups. Springer-Verlag. 4ª Ed. 1995.

[7] John Dixon. Problems in group theory. Dover Publications Inc. 1973.

[8] I. N. Herstein. Topics in algebra. John Wiley & Sons, Inc. 2ª Ed. 1975.

[9] Walter Ledermann. Introduction to the theory of finite groups. Interscience Publishers, Inc. 5ª Ed. 1964.

[10] J.A. Bondy and U. S. Murty. Graph theory with aplications. American Elsevier publishing Co. 1976.

[11] Robin J. Wilson. Introduction to graph theory. Academic Press. 2ª ed. 1979.

[12] L. R. Foulds. Graph theory applications. Springer-Verlag. 1992.

[13] Frank Harary. Graphical enumeration. Academic Press. 1973.