

UNIVERSIDAD AUTÓNOMA DE QUERÉTARO

FACULTAD DE INGENIERÍA

MAESTRÍA EN DOCENCIA DE LAS MATEMÁTICAS

UNA APLICACIÓN DE LA TEORÍA DE GRÁFICAS EN
TEORÍA DE GRUPOS

TESIS

QUE PARA OBTENER EL GRADO DE MAESTRO

PRESENTA

ADELINA SILVA MUSLERA

Querétaro. Qro., Junio de 1997

No. Adm. H56258
No. Título _____
Clas. 512.22
S586a

UNIVERSIDAD AUTÓNOMA DE QUERÉTARO
FACULTAD DE INGENIERÍA
MAESTRÍA EN DOCENCIA DE LAS MATEMÁTICAS

NOMBRE DE LA TESIS:
UNA APLICACIÓN DE LA TEORÍA DE GRÁFICAS EN TEORÍA DE GRUPOS

Que como parte de los requisitos para obtener el grado de
MAESTRO

Presenta:
Adelina Silva Muslera

Dirigida por:
Dr. Alejandro J. Díaz Barriga Casales

SINODALES

Dr. Alejandro J. Díaz Barriga Casales
Presidente


Firma

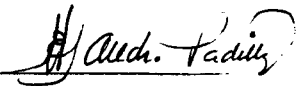
Dr. Emilio Lluís Riera
Secretario


Firma

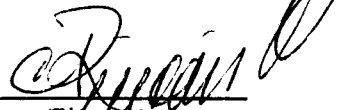
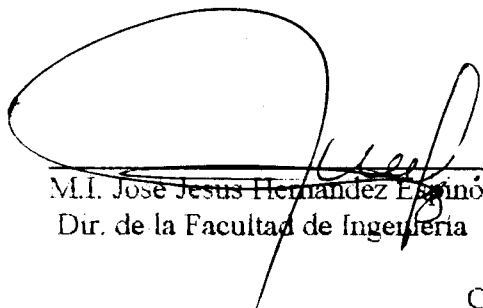
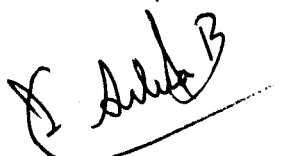
Dr. Rodolfo San Agustín Chi
Vocal


Firma

M. en C. Alejandro Padilla González
Suplente


Firma

M. en C. César Alejandro Rincón Orta
Suplente


Firma
M.I. José Jesús Hernández Espinó
Dir. de la Facultad de Ingeniería
M. C. Carlos Isaac Silva Barrón
Dir. de Estudios de Posgrado

Dedico esta tesis a
Beto
y a mis pequeños amores
Anabella y Adelina
por su apoyo y
comprensión

Agradecimientos:

Al Dr. Alejandro Díaz Barriga Casales
por sus enseñanzas, regaños y gritos

Al M.C. Alejandro Padilla González
por su apoyo y paciencia

Al Ing. Fernando Ochoa Salazar
por su confianza y solidaridad

A mis padres
por sus consejos

Y a Tere
por su amistad

Índice

	<i>Página</i>
Introducción	0
Capítulo I	1
<i>Teoría de Gráficas.</i>	
Problema de los puentes de Königsberg	1
Definición de gráfica	2
Gráfica dirigida	3
Subgráficas	4
Gráficas isomorfas	5
Gráfica completa	6
Gráfica bipartita	7
Gráfica de líneas	9
Operaciones con gráficas	10
Capítulo II	12
<i>Teoría de Grupos.</i>	
Funciones	12
Grupo simétrico de grado n	13
Grupos	14
Subgrupos	15
Clases laterales	17
Teorema de Lagrange	17
Isomorfismo	18
Subgrupo normal	19
Teorema de Cayley	20

Capítulo III	21
<i>Permutaciones.</i>	
Definición de permutación	21
Ciclo de orden k	23
Producto de ciclos ajenos	24
Producto de transposiciones	25
Permutaciones pares e impares	26
Grupo alternante de grado n	28
Capítulo IV	29
<i>Una aplicación de la Teoría de Gráficas en Teoría de Grupos.</i>	
Preliminares	29
Teorema	30
Bibliografía	36

Introducción

En años recientes, el interés por la teoría de gráficas se ha visto incrementado por varios motivos: uno de ellos es la aplicación que la teoría de gráficas tiene en algunas áreas como física, química, ciencias de la comunicación, tecnología computacional, ingeniería civil, ingeniería eléctrica, arquitectura, genética, sicología, sociología, economía, antropología y lingüística, entre otras; otro es que está altamente relacionada con ciertas ramas de la matemática como: teoría de grupos, teoría de matrices, análisis numérico, probabilidad, topología y combinatoria. Además, como un modelo matemático para los sistemas que involucran relaciones binarias.

Por todo lo anterior surgió la inquietud de realizar un trabajo que relacionara la teoría de gráficas con alguna de las ramas de las matemáticas antes mencionadas y qué mejor que un isomorfismo entre gráficas construidas con elementos de teoría de grupos. En esta tesis eso es lo que se hace.

El presente trabajo consta de cuatro capítulos, en el capítulo I se presentan conceptos generales de la teoría de gráficas como: definición de una gráfica, gráfica dirigida, gráfica bipartita, operaciones con gráficas, entre otros.

El Capítulo II está dedicado a la teoría de grupos; en él se incluyen los primeros resultados elementales, así como el teorema de Cayley que dice que todo grupo es isomorfo a algún subgrupo de S_n ; dando de esta forma significado al estudio de las permutaciones, que es lo que se hace en el capítulo III.

Finalmente, en el capítulo IV utilizamos todos los conceptos desarrollados en los tres capítulos anteriores para demostrar el isomorfismo entre dos gráficas que se obtienen a partir de S_6 .

I. Teoría de Gráficas.

En el siglo XVII la ciudad de Königsberg perteneciente a Prusia oriental, estaba dividida en cuatro zonas por el río Pregel. Dos zonas eran tierra firme y las otras dos eran islas, una de ellas, la isla de Kneiphof. Siete puentes comunicaban entre si las zonas. Las dos islas estaban unidas a tierra firme por seis puentes y uno las unía entre sí, como la ilustración de la figura I.1.

Se cuenta que los habitantes destinaban paseos dominicales a recorrer toda la ciudad, intentando cruzar exactamente una vez cada puente, pasando por cada una de las cuatro zonas, además empezando y concluyendo el recorrido en el mismo lugar; como nadie lo lograba surgió la inquietud sobre la factibilidad o imposibilidad de hacerlo.

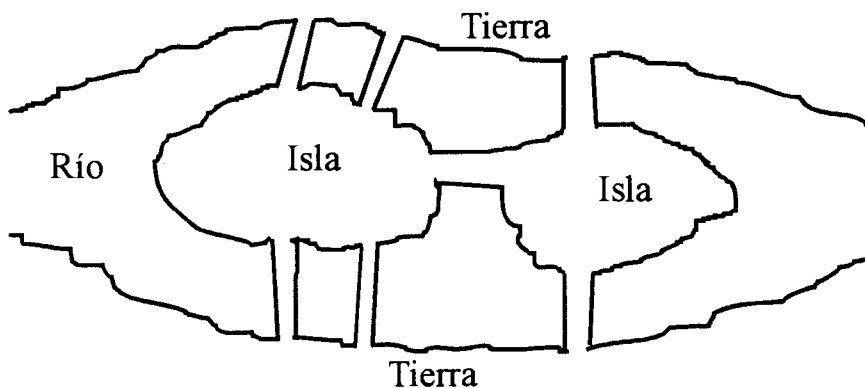


Fig. I.1.

En 1736 el matemático suizo Leonhard Euler (1707-1783) elaboró un modelo matemático de este problema en el cual reemplazó por un punto cada una de las zonas de tierra y por una recta cada uno de los puentes, dando lugar a una gráfica como la que mostramos en la figura I.2. Este modelo es considerado como el inicio de la Teoría de Gráficas.

Euler demostró ante la Academia Rusa de San Petersburgo que el recorrido no era posible. El razonamiento que presentó decía que cada vez que se pasa por un punto de la gráfica se entra por una línea y se sale por otra, el punto que es considerado el inicio del recorrido deberá tener una línea por la cual empezar y otra para concluir en ese punto el recorrido, por lo que el número de líneas que deberá tener cada punto será un número par.

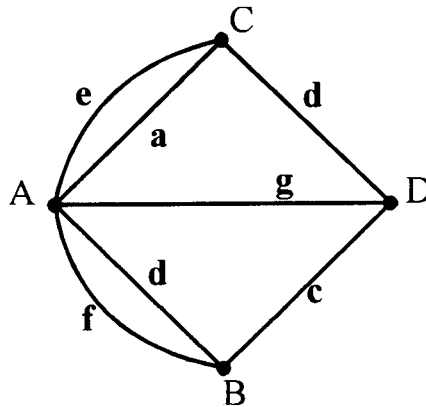


Fig. I.2.

Definimos una *gráfica* $G(V, X)$ como un conjunto finito V no vacío de puntos llamados *vértices* y una colección X de pares no ordenados de puntos de V llamados *aristas*; por lo tanto una arista queda determinada por sus vértices.

Si los puntos A y B forman una arista, como una manera de expresarlo, decimos que dicha arista une los puntos A y B .

A dos o más aristas que tengan los mismos vértices les llamamos *aristas múltiples*. Si los vértices de una arista son el mismo punto, la arista se llama *lazo*.

Decimos que dos vértices son *adyacentes* si forman una arista, dos aristas son *adyacentes* si tienen un vértice en común, y un vértice y una arista *inciden* si dicho vértice es uno de los que forman la arista.

A manera de ejemplo consideramos el conjunto de vértices cuyos elementos son A, B, C y D y la colección de pares no ordenados AC, AC, AB, AB, CD, AD y BD que forman una gráfica. En ella tenemos cuatro vértices y siete aristas, a una de las aristas AC la denotamos como **a**, a la otra arista AC la denotamos como **e**, a una de las aristas AB la denotamos como **d**, a la arista AD la denotamos como **g**, y a la arista BD como **c**.

La figura I.2 es una ilustración del ejemplo. En ella podemos ver que los vértices C y D son adyacentes, que **c** y **d** son aristas adyacentes y que la arista **c** y el vértice D inciden.

En el párrafo anterior hemos dicho que la figura I.2 es una ilustración de la gráfica. En adelante a las ilustraciones de las gráficas les llamaremos simplemente gráficas.

Cuando en una gráfica no aparecen lazos ni aristas múltiples la llamamos *gráfica simple*.

Para toda gráfica $G(V, X)$ y para todo $v \in V$, el *grado* del vértice v es el número de aristas que inciden en él; se denota por $gr_G(v)$. También al grado se le denomina *valencia*.

Por ejemplo, los grados de cada uno de los vértices de la gráfica que se obtiene del problema de los puentes de Königsberg, y que se ilustra en la figura I.2 son: $gr_G(\mathbf{A}) = 5$ y $gr_G(\mathbf{B}) = gr_G(\mathbf{C}) = gr_G(\mathbf{D}) = 3$.

Si en una gráfica las aristas se consideran como parejas ordenadas, decimos que la gráfica es *dirigida*. Así si una arista v se considera como la pareja (A,B) decimos que la arista esta dirigida de A a B; al vértice A le llamamos *origen* o *fuentes* y a B le llamamos *término* o *vértice final*. En la ilustración de la gráfica dirigida pondremos flechas para indicar cuales vértices son origen y cuales término. La figura I.3 ilustra una gráfica dirigida, en la que la arista v es la pareja (u,w), donde u es fuente y w término.

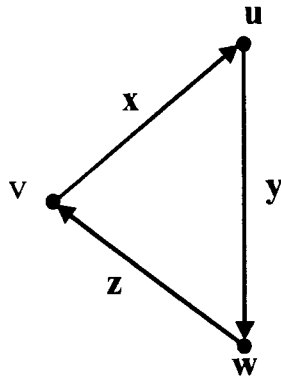


Fig. I.3.

Decimos que la gráfica $H(U, Y)$ es una subgráfica de $G(V, X)$ si $U \subseteq V$ y $Y \subseteq X$. Una gráfica puede tener más de una subgráfica.

Sean $G(V, X)$ una gráfica y $V' \subseteq V$. La *subgráfica de G inducida por V'* que denotamos $\langle V' \rangle$ es la subgráfica de G que resulta al quitar los vértices de V' y las aristas que tienen algún vértice en V' .

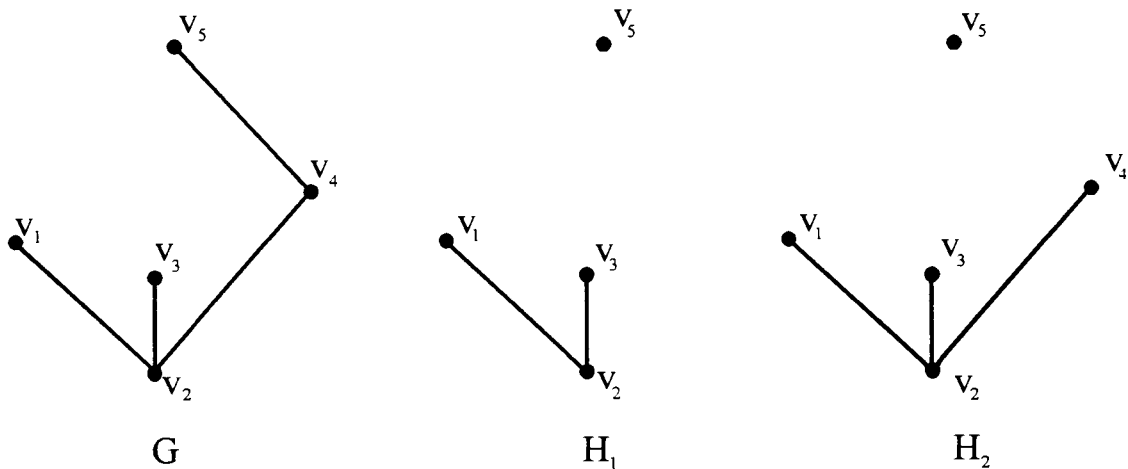


Fig. I.4.

De forma análoga si $G(V, X)$ es una gráfica y $X' \subseteq X$, la *subgráfica de G inducida por X'* que denotamos $\langle X' \rangle$ es la subgráfica de G que se obtiene quitando a G las aristas de X' pero no sus vértices.

En la figura I.4 H_1 es la subgráfica que resulta de quitar el vértice v_4 de la gráfica G y H_2 es la subgráfica que resulta de quitar la arista $v_4 v_5$ de la gráfica G.

Dos gráficas son *isomorfas*, si existe una correspondencia biyectiva* entre los conjuntos de vértices y al menos una correspondencia biyectiva entre los conjuntos de aristas, tales que, conserven las adyacencias. Para denotar que dos gráficas G y H son isomorfas escribimos $G \cong H$.

Es interesante poder establecer si dos gráficas son o no isomorfas. Inicialmente al pensarse en este problema puede suponerse que basta conocer el número de vértices de cada una de las gráficas y el número de aristas adyacentes a cada uno de los vértices, sin embargo esta información no es suficiente para determinar que las gráficas sean isomorfas. Por ejemplo, en las gráficas de la figura I.5, ambas tienen diez vértices y cada vértice tiene tres aristas adyacentes y no son isomorfas.

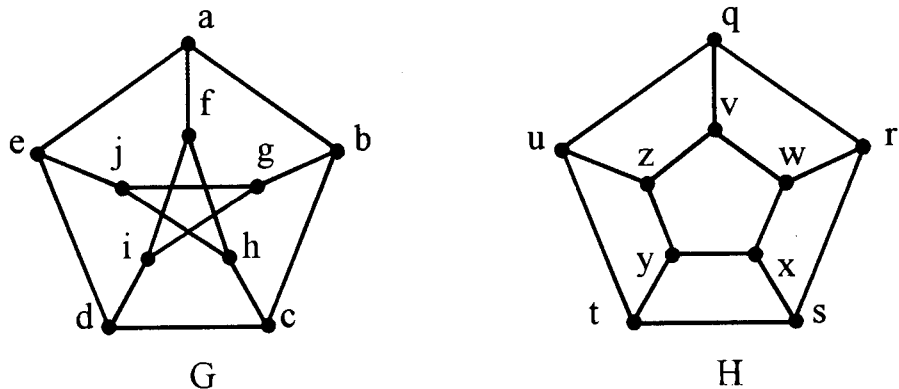


Fig. I.5

Un *invariante* de una gráfica G es un número que se le asocia a G y que permanece fijo bajo isomorfismos. Como ejemplo consideremos:

*Ver capítulo II

- i) el número de aristas de G .
- ii) el número de vértices de G .

Los invariantes de las gráficas nos ayudan a determinar cuando éstas no son isomorfas.

Un *camino* en una gráfica G es una secuencia alternante de vértices v_i y aristas x_i de la forma $v_0, x_1, v_1, \dots, v_{n-1}, x_n, v_n$, en la que cada arista incide con los vértices contiguos. La *longitud* de un camino es el número de aristas que lo forman. Un camino cerrado inicia y termina en el mismo vértice. Un *ciclo* es un camino cerrado de la forma $v_1, x_1, v_2, \dots, v_n, x_n, v_1$, donde $v_i \neq v_j$ para toda $i \neq j$. Cuando G es una gráfica simple, se puede definir un camino dando sólo una secuencia de vértices, por ejemplo en la gráfica G de la figura 1.5 a, b, g, i, d, c, b, g es un camino de longitud 7 y a, f, i, d, e, a es un ciclo de longitud 5.

Un *paseo* en una gráfica G es un camino en el que no se repiten aristas. Un paseo se llama *paseo cerrado* si el vértice inicial coincide con el vértice final. Por ejemplo, en la gráfica H de la figura 1.5 q, r, s, t, y es un paseo y q, r, s, t, u, q es un paseo cerrado.

Una *trayectoria*, en una gráfica G es un paseo en el que no se repiten vértices. Por ejemplo $q, v, w, r, s, x, y, z, u$ es una trayectoria en la gráfica H de la figura 1.5.

Una gráfica G es *completa* si todo par de vértices son adyacentes. A una gráfica completa K con n vértices, la denotamos K_n . Es fácil ver que todas las gráficas completas con n vértices son isomorfas.

En la figura 1.6 mostramos las gráficas $K_1, K_2, K_3, K_4, K_5, K_6$.

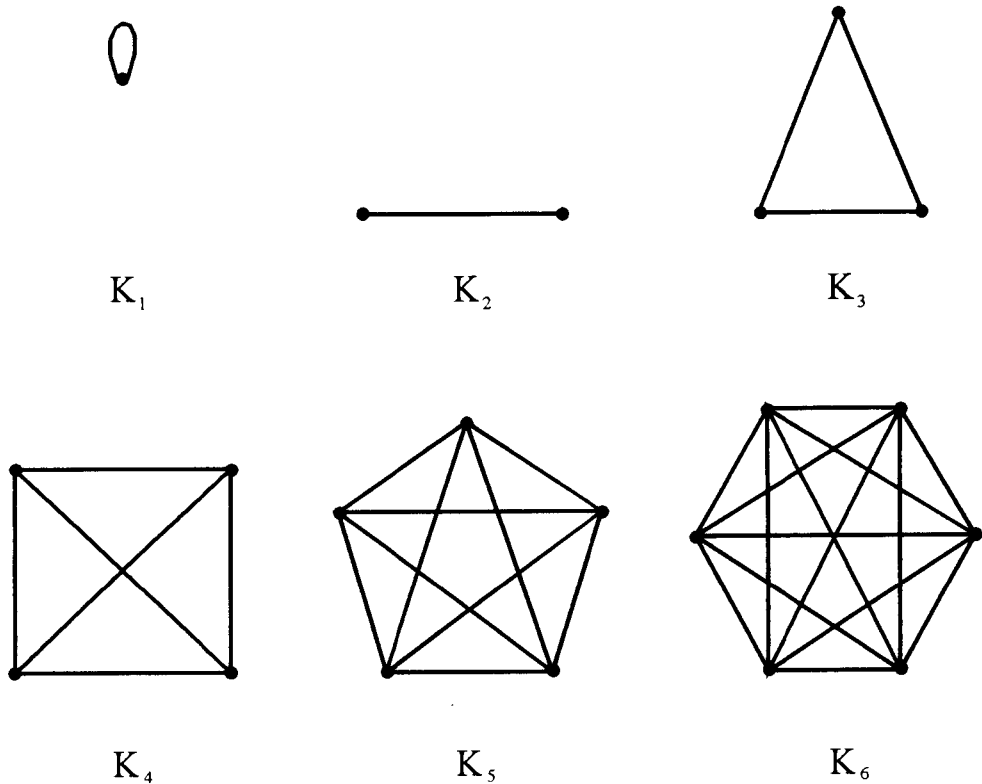


Fig. I.6.

Definimos el *grado mínimo* de una gráfica G , como el menor de los grados de sus vértices y lo denotamos por $\delta(G)$. De manera análoga, definimos el *grado máximo* de G que denotamos $\Delta(G)$ como el mayor de los grados de sus vértices. Una gráfica k -regular, o de *grado* k , es aquella en la que todos los vértices son de grado k .

Una gráfica $G(V, X)$ es *bipartita*, si existe una partición de V en dos conjuntos V_1 y V_2 , de forma que cada arista de G tenga un extremo en V_1 y el otro en V_2 . Por ejemplo la gráfica de la figura I.7, es bipartita y la partición esta formada por $V_1 = \{v_1, v_2, v_3\}$ y $V_2 = \{v_4, v_5, v_6\}$.

Una gráfica $G(X, V)$ es *bipartita completa*, si existe una partición $\{V_1, V_2\}$ de V , tal que, cada vértice de V_1 es adyacente a todos los vértices de V_2 . Estas gráficas las denotamos por $K_{n,m}$, donde n es la cardinalidad de V_1 y m es la cardinalidad de V_2 . Un ejemplo es la gráfica $K_{3,3}$ de la figura 1.7.

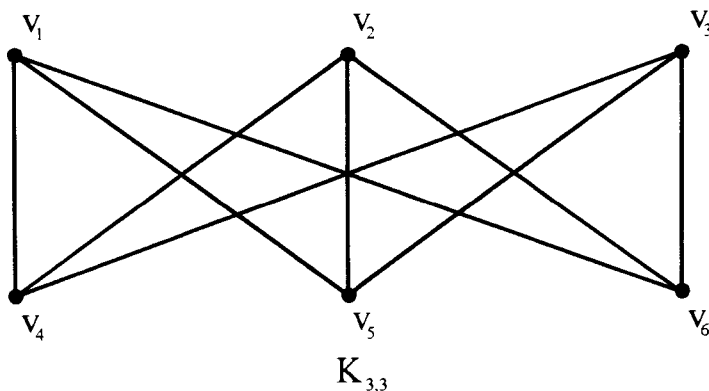


Fig. I.7.

Una gráfica G es *conexa* si y sólo si para cualquier par de vértices de G existe una trayectoria que los una. Una gráfica es *no conexa* si para al menos un par de vértices no existe una trayectoria que los una. En la figura I.8, la gráfica G es conexa, ya que existen trayectorias que unen a cada par de vértices; la gráfica H es no conexa, ya que no existe una trayectoria que una al vértice v_1 con el vértice v_4 .

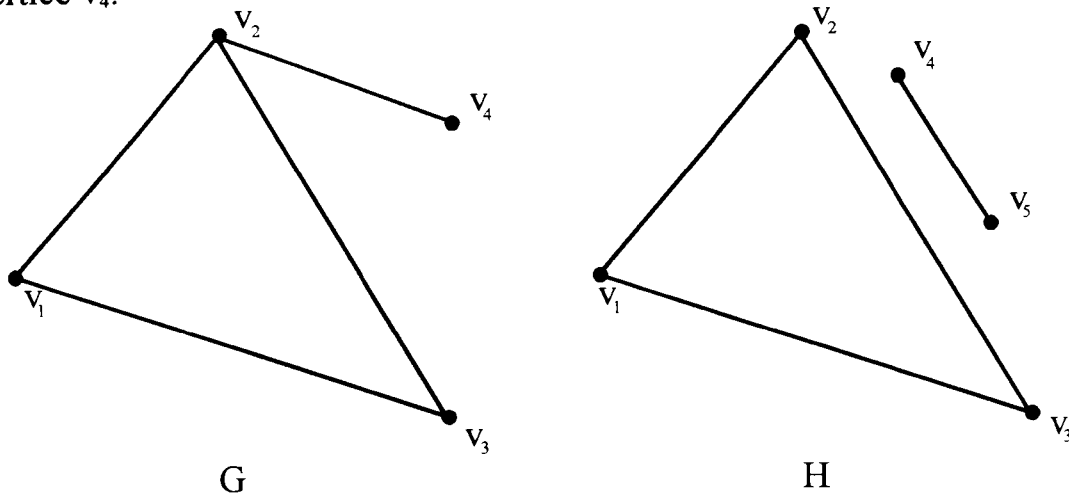


Fig. I.8.

Las *componentes conexas* de una gráfica G son las subgráficas conexas de G que no están contenidas en ninguna otra subgráfica conexa de G . El número de componentes conexas de una gráfica G lo denotamos por $c(G)$. Por ejemplo, en

las gráficas de la figura I.8, el número de componentes conexas de G es $c(G) = 1$ y de la gráfica H es $c(H) = 2$.

Si G es una gráfica simple, su *complemento*, que denotamos por G^c , es la gráfica que consta del mismo conjunto de vértices que G , en donde, dos de ellos son adyacentes si y sólo si no lo son en G . En la figura I.9 mostramos la gráfica G y su complemento.

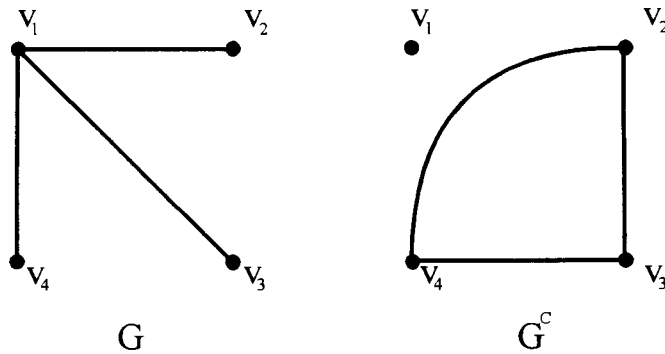


Fig. I.9.

Sea G una gráfica simple, la *gráfica de líneas de G* , que denotamos $L(G)$, es la gráfica que tiene como vértices las aristas de G y dos vértices son adyacentes en $L(G)$ si las aristas respectivas en G tienen un vértice en común. En la figura I.10 mostramos la gráfica K_4 y la gráfica $L(K_4)$.

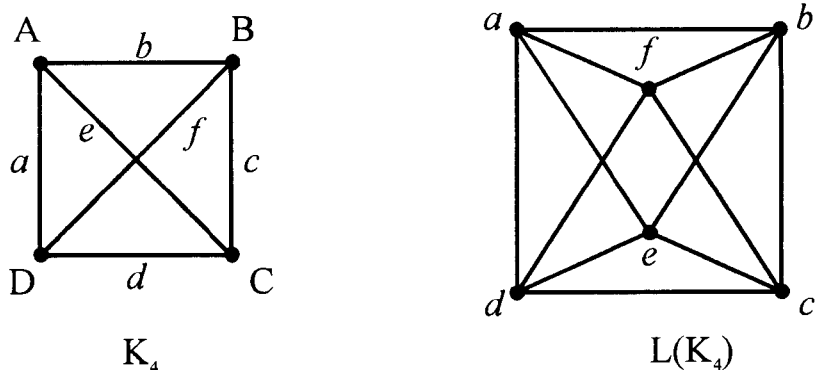


Fig. I.10.

Si dos gráficas simples $G_1(V_1, X_1)$ y $G_2(V_2, X_2)$ son tales que ningún vértice de V_1 está en V_2 les llamamos *gráficas ajenas*.

Sean $G_1(V_1, X_1)$ y $G_2(V_2, X_2)$ dos gráficas ajenas, entonces la *unión* de G_1 con G_2 que denotamos $G_1 \cup G_2$, es la gráfica simple que tiene como vértices a $V_1 \cup V_2$ y su colección de aristas tiene a todas las aristas que estén en X_1 y todas las que estén en X_2 , colección que denotamos $X_1 \cup X_2$.

Sean $G_1(V_1, X_1)$ y $G_2(V_2, X_2)$ dos gráficas ajenas, entonces la *suma* $G_1 + G_2$ es la gráfica simple que tiene a todos los vértices y a todas las aristas de $G_1 \cup G_2$ y además tiene a todas las aristas que se forman al unir cada vértice de V_1 con cada vértice de V_2 .

En la figura I.11 se ilustran las gráficas $G_1, G_2, G_1 \cup G_2$ y $G_1 + G_2$.

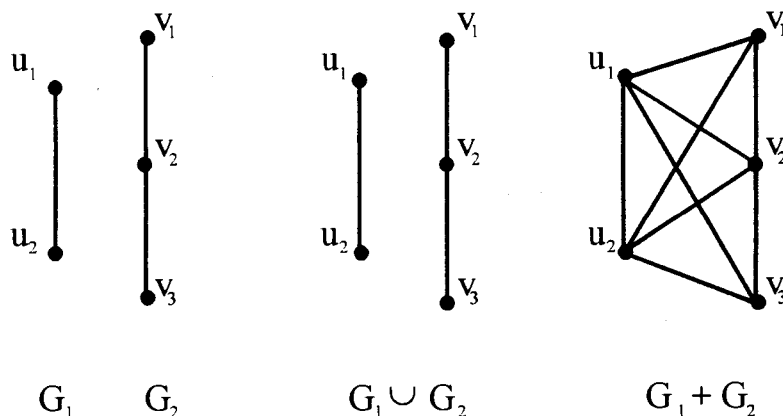


Fig. I.11.

Sean $G_1(V_1, X_1)$ y $G_2(V_2, X_2)$ dos gráficas ajenas. Entonces el *producto* de G_1 con G_2 que denotamos $G_1 \times G_2$ tiene como conjunto de vértices a $V_1 \times V_2$ y dos vértices $u = (u_1, u_2)$ y $v = (v_1, v_2)$ que pertenecen a $V_1 \times V_2$, son adyacentes en $G_1 \times G_2$ si $u_1 = v_1$ y u_2 ady v_2 ó $u_2 = v_2$ y u_1 ady v_1 . En la figura I.12 se ilustran las gráficas G_1, G_2 y el producto $G_1 \times G_2$.

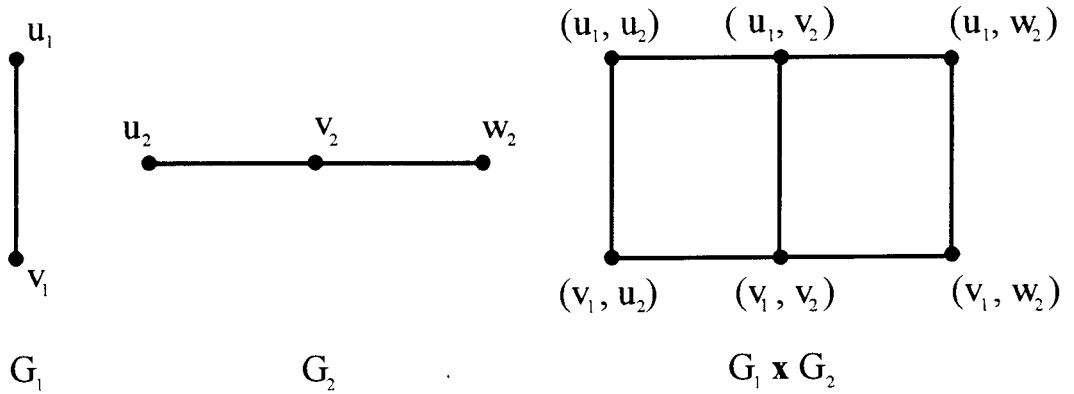


Fig. I.12.

La *composición* de dos gráficas ajenas $G_1(V_1, X_1)$ y $G_2(V_2, X_2)$, que denotamos $G_1[G_2]$ tiene como conjunto de vértices $V_1 \times V_2$ y (u_1, u_2) es adyacente con (v_1, v_2) , si u_1 ady v_1 ó $u_1 = v_1$ y u_2 ady v_2 . Consideramos las mismas gráficas G_1 y G_2 de la figura I.12 para ilustrar a $G_1[G_2]$ y a $G_2[G_1]$ en la figura I.13.

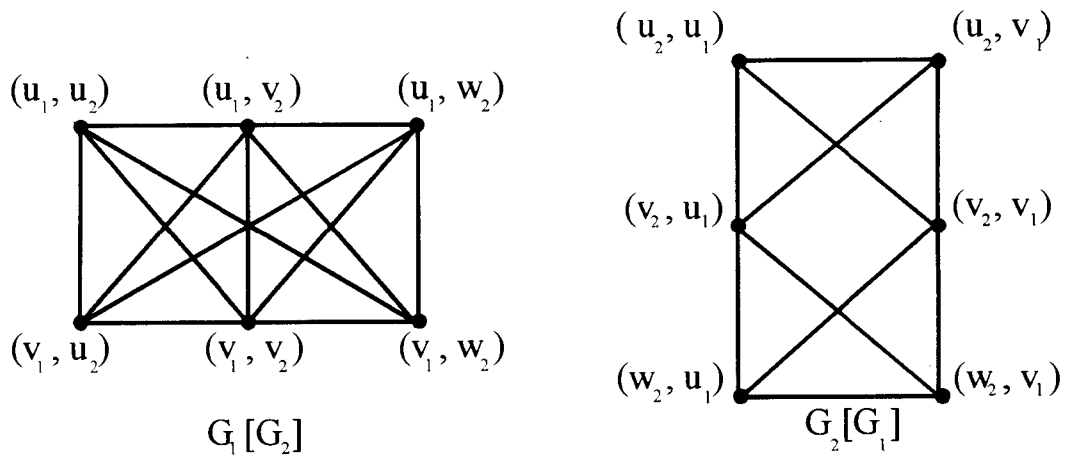


Fig. I.13.

II. Teoría de Grupos.

Recordaremos primero algunos conceptos relativos a conjuntos y a funciones. Sean S y T conjuntos, una *función* f de S en T es una regla que a cada elemento del conjunto S le asigna un único elemento del conjunto T . Al conjunto S se le llama *dominio* de la función y al conjunto T *contradominio*. Una función f con un dominio S y un contradominio T , se denota $f: S \rightarrow T$.

Sean $t \in T$ y $s \in S$, para indicar que t es el elemento asociado a s , mediante f , escribimos $f(s) = t$ y $f(s)$ le llamamos *imagen* de s bajo f .

Nos referiremos a continuación a algunas funciones especiales.

Si una función tiene el mismo conjunto como dominio y contradominio decimos que es una función definida en dicho conjunto. Así si $f: A \rightarrow A$, decimos que f está definida en A .

A la función que hace corresponder a cada elemento de S el mismo elemento le llamamos función *idéntica* sobre S y la denotamos I_S . Por lo que $I_S: S \rightarrow S$ es la función, para toda $x \in S$, $I_S(x) = x$.

Una función $f: S \rightarrow T$ se llama *inyectiva* o *uno a uno* si dados dos elementos cualesquiera distintos en S la regla f les asocia imágenes distintas en T . Esto es, para cualquier s_1 y s_2 en S , si $s_1 \neq s_2$ entonces $f(s_1) \neq f(s_2)$; en forma equivalente, si $f(s_1) = f(s_2)$ entonces $s_1 = s_2$.

Una función $f: S \rightarrow T$ es *suprayectiva* o *sobreyectiva* si todo elemento de T es imagen de por lo menos un elemento de S . Es decir, si para todo $t \in T$ existe $s \in S$ tal que $f(s) = t$.

Una función $f: S \rightarrow T$ es *biyectiva* si es a la vez inyectiva y sobreyectiva.

Sean $g: S \rightarrow T$ y $f: T \rightarrow U$ funciones, definimos la *composición* de g seguida de f como la función con dominio S y contradominio U que denotamos por $f \circ g$ tal que $f \circ g(s) = f(g(s))$. Se hace notar que hemos pedido que el contradominio de g , sea el dominio de f .

Una propiedad de la composición de funciones es que satisface: si $h: S \rightarrow T$, $g: T \rightarrow U$ y $f: U \rightarrow V$, entonces $f \circ (g \circ h) = (f \circ g) \circ h$, ya que:

$$(f \circ g) \circ h(s) = f \circ g(h(s)) = f(g(h(s)))$$

$$f \circ (g \circ h)(s) = f(g \circ h(s)) = f(g(h(s))).$$

Sea $f: S \rightarrow T$ una función. Si $h: T \rightarrow S$ es tal que $f \circ h = I_T$ y $h \circ f = I_S$, entonces h es la inversa de f ; a h también la denotamos f^{-1} y decimos que f es invertible.

Se puede probar fácilmente que una función f es invertible si y sólo si f es biyectiva.

Antes de abordar el concepto de grupo consideremos el conjunto de todas las funciones biyectivas definidas en un conjunto S , que denotamos $A(S)$, y la composición de funciones como operación definida en $A(S)$.

$A(S)$ con la composición satisface:

- a) Si $f, g \in A(S)$, entonces $f \circ g \in A(S)$.
- b) Para cualesquiera $f, g, h \in A(S)$, entonces $(f \circ g) \circ h = f \circ (g \circ h)$.
- c) Existe $I_S \in A(S)$, tal que $f \circ I_S = I_S \circ f$ para toda $f \in A(S)$.
- d) Dada $f \in A(S)$, existe $f^{-1} \in A(S)$, tal que $f \circ f^{-1} = f^{-1} \circ f = I_S$.

Si S es un conjunto finito con n elementos, $A(S)$ recibe el nombre de *grupo simétrico de grado n* y se denota S_n .

El número de elementos de $A(S)$ depende del número de elementos de S . Así, si S tiene n elementos $A(S)$ tiene $n!$ elementos. Para mostrarlo supongamos que $S = \{x_1, x_2, \dots, x_n\}$ y $f \in A(S)$; entonces f puede asignar n imágenes diferentes a x_1 y como f es inyectiva $f(x_1) \neq f(x_2)$; luego f puede asignar $n - 1$ imágenes diferentes a x_2 , por ser f inyectiva puede asignar $n - 2$ imágenes diferentes a x_3 y así sucesivamente; por lo tanto, el número de funciones biyectivas de S en S es: $n(n - 1)(n - 2) \dots 1 = n!$.

Ahora definimos lo que es un grupo: Un conjunto G con una operación $*$ es un *grupo*, si satisface:

i) Si $a, b \in G$, entonces $a * b \in G$.

Por esta propiedad decimos que G es *cerrado* respecto a la operación $*$.

ii) Para cualesquiera $a, b, c \in G$, tenemos que $a * (b * c) = (a * b) * c$.

A esta propiedad le llamamos la *ley asociativa* en G .

iii) Existe un elemento $e \in G$ tal que $a * e = e * a = a$, para toda $a \in G$.

Al elemento e le llamamos *elemento identidad*.

iv) Para todo $a \in G$ existe un elemento $b \in G$ tal que $a * b = b * a = e$.

Al elemento b le llamamos *inverso de a en G* y lo escribimos como a^{-1} .

Un grupo G es *abeliano* o *conmutativo* si $a * b = b * a$ para toda $a, b \in G$; es decir, si la operación $*$ es conmutativa.

Para facilitarnos la escritura de $a*b$, cuando no se preste a confusión, lo expresamos simplemente como ab , a $*$ le llamamos producto de G y al grupo $(G, *)$ lo denotamos por G .

Algunas de las propiedades de un grupo G son:

A) Su elemento identidad es único.

Mostramos que esto es cierto. Suponemos que e y k son elementos identidad de G , es decir, para toda $a \in G$, $ae = ea = a$ y $ak = ka = a$ y concluimos que $e = k$. Esto es porque $ek = e$ y $ek = k$ y por consiguiente $e = ek = k$.

- B) i) Si $a, b, c \in G$ y $ab = ac$ entonces $b = c$,
 ii) Si $a, b, c \in G$ y $ba = ca$ entonces $b = c$.

Probamos i), $b = eb = (\alpha^{-1} a) b = \alpha^{-1} (ab) = \alpha^{-1} (ac) = (\alpha^{-1} a)c = ec = c$. Análogamente se prueba ii).

- C) Cada $a \in G$ tiene un inverso único $a^{-1} \in G$.

Vemos que es cierto suponiendo $b, c \in G$ inversos de $a \in G$, entonces $ab = ac$, y por la propiedad anterior $b = c$ por lo que el inverso de a es único.

- D) Si $a \in G$, $(a^{-1})^{-1} = a$

Ya que si $a \in G$, existe $a^{-1} \in G$ tal que $a^{-1} a = e$ y $e = a a^{-1}$ además existe $(a^{-1})^{-1} \in G$ tal que $a^{-1} (a^{-1})^{-1} = e$ y $(a^{-1})^{-1} a^{-1} = e$, y por el inciso C, $(a^{-1})^{-1} = a$.

- E) Para cualesquiera $a, b \in G$, $(ab)^{-1} = b^{-1} a^{-1}$, ya que:

$$\begin{aligned} (ab)(b^{-1} a^{-1}) &= ((ab)a^{-1}) a^{-1} = (a(bb^{-1})) a^{-1} = (ae) a^{-1} = a a^{-1} = e. \\ (b^{-1} a^{-1})(ab) &= a^{-1} ((ab)b^{-1}) = a^{-1} (a(bb^{-1})) = a^{-1} a = a^{-1} (ae) = e. \end{aligned}$$

A un subconjunto no vacío H , de un grupo G , le llamamos *subgrupo* de G , si H mismo forma un grupo relativo al producto de G . Es decir, dado H un subconjunto de G no vacío es un subgrupo de G si y sólo si H es cerrado con respecto a la operación de G y, dado $a \in H$, entonces $a^{-1} \in H$.

Decimos que un grupo G es *finito* si consta de un número finito de elementos. A este número de elementos de G le llamamos *orden de G* y lo denotamos $|G|$ o $o(G)$. Si G consta de un número infinito de elementos, entonces decimos que es de *orden infinito*.

Recordemos rápidamente las siguientes definiciones y el siguiente resultado:

A una relación \sim en un conjunto S le llamamos *relación de equivalencia* si satisface:

- a) $a \sim a$ para toda $a \in S$ (*reflexividad*)
- b) Si $a \sim b$ entonces $b \sim a$ para todo $a, b \in S$ (*simetría*)
- c) Si $a \sim b$ y $b \sim c$ entonces $a \sim c$ para todo $a, b, c \in S$ (*transitividad*)

Si \sim es una relación de equivalencia en un conjunto S y $a \in S$, entonces definimos la clase de a como $\{ b \in S \mid b \sim a \}$, conjunto que denotamos $[a]$.

Si \sim es una relación de equivalencia en S , afirmamos que:

- i) $S = \cup_{a \in S} [a]$
- ii) Si $[a] \neq [b]$, entonces $[a] \cap [b] = \emptyset$.
- iii) $[a] \neq \emptyset$ para toda $a \in S$

Para ver que i) es cierto. Sea $a \in S$, como $a \sim a$ entonces $a \in [a]$ por lo que entonces $a \in \cup_{a \in S} [a]$; entonces $S \subset \cup_{a \in S} [a]$ la contención $\cup_{a \in S} [a] \subset S$ es clara.

Para mostrar que ii) es cierto suponemos $[a] \cap [b] \neq \emptyset$; sea $c \in [a] \cap [b]$; por la definición de clase, $c \sim a$ y $c \sim b$ y por ser \sim relación de equivalencia $a \sim b$, sea $d \in [a]$ entonces $a \sim d$ y $d \sim a$ y como $a \sim b$ se tiene que $d \sim b$ por lo que $b \sim d$ de donde $d \in [b]$ y entonces $[a] \subset [b]$, de forma análoga $[b] \subset [a]$, entonces $[a] = [b]$.

En el caso de iii), sea $a \in S$ entonces $a \sim a$ y por lo tanto $a \in [a]$ y $[a] \neq \emptyset$, para toda $a \in S$.

Continuamos con nuestro desarrollo de teoría de grupos:

Sean G un grupo y H un subgrupo de G , definimos una relación \sim en G tal que para cualesquiera $a, b \in G$ $a \sim b$ si $ab^{-1} \in H$. Afirmamos que dicha relación es una relación de equivalencia, ya que: es reflexiva por que si $a \in G$, entonces $a \sim a$ ya que $a a^{-1} = e$, y $e \in H$; es simétrica porque si $a \sim b$, entonces $ab^{-1} \in H$ entonces $(ab^{-1})^{-1} \in H$ y $(a b^{-1})^{-1} = (b^{-1})^{-1} a^{-1} = b a^{-1}$ por lo que $b \sim a$: y es transitiva por que $a \sim b$ y $b \sim c$ entonces $a b^{-1} \in H$ y $b c^{-1} \in H$, entonces $(a b^{-1})(b c^{-1}) = a c^{-1}$ por lo que $a c^{-1} \in H$, entonces $a \sim c$.

La clase de a es:

$$[a] = \{ b \in G \mid ab^{-1} \in H \}, \text{ lo que es lo mismo que}$$

$$[a] = \{ b \in G \mid ab^{-1} = h \in H \}, \text{ luego}$$

$$[a] = \{ b \in G \mid b = ha \text{ con } h \in H \} = Ha$$

y le llamamos *clase lateral derecha* de H en G .

De manera análoga tenemos que:

$$aH = \{ b \in G \mid b = ah \}$$

y le llamamos *clase lateral izquierda* de H en G .

TEOREMA DE LAGRANGE: Si G es un grupo finito y H es un subgrupo de G , entonces el orden de H divide al orden de G .

Por la relación de equivalencia que damos en párrafos anteriores tenemos que: $G = \cup_{a \in S} [a]$, como G es finito y $[a] = Ha = \{ha \mid h \in H\}$, entonces debe de tener un número finito de clases distintas. Sea k el número de clases distintas: Ha_1, Ha_2, \dots, Ha_k ; entonces $G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$ y $Ha_j \cap Ha_i = \emptyset$, si $i \neq j$. Para ver que Ha_i tiene el mismo número de elementos que H ; consideremos la aplicación $H \rightarrow Ha_i$ tal que $h \rightarrow ha_i$ ésta es

una biyección, por lo que H y $H\alpha_i$ tienen el mismo número de elementos. Por lo que cada $H\alpha_i$ tiene $\mathfrak{o}(H)$ elementos, luego tenemos que $\mathfrak{o}(G) = k\mathfrak{o}(H)$, entonces $\mathfrak{o}(H)$ divide a $\mathfrak{o}(G)$.

Si G es un grupo finito y $a \in G$, definimos el orden de a como el *mínimo entero positivo* n , tal que $a^n = e$ y lo denotamos $\mathfrak{o}(a)$.

Sea G es un grupo y $a \in G$, entonces $H = \{ a^m \mid m \in \mathbf{Z} \}$ es un subgrupo de G .

Mostramos que es cierto: si $a^s, a^t \in H$ donde $s, t \in \mathbf{Z}$; entonces $a^s a^t = a^{s+t}$, por lo que $a^{s+t} \in H$; como $a^m a^0 = a^{m+0} = a^{0+m} = a^0 a^m = a^m$ para toda $m \in \mathbf{Z}$ por lo tanto $a^0 = e$ y $e \in H$; si $a^s \in H$ entonces $s \in \mathbf{Z}$ y existe $-s \in \mathbf{Z}$, por lo tanto $a^{-s} \in H$ y como $a^s a^{-s} = a^{s+(-s)} = a^0 = e$ entonces a^{-s} es el inverso de a^s .

Llamamos al conjunto $\{ a^m \mid m \in \mathbf{Z} \}$ el *subgrupo cíclico de G generado por a* y lo denotamos $\langle a \rangle$; es fácil ver que si G es finito entonces $\mathfrak{o}(\langle a \rangle) = \mathfrak{o}(a)$.

Sean G y G' dos grupos; una función $\varphi : G \rightarrow G'$ es un *homomorfismo*, si $\varphi(ab) = \varphi(a)\varphi(b)$, para cualesquiera $a, b \in G$.

Si un homomorfismo $\varphi : G \rightarrow G'$ es uno a uno, decimos que φ es un *monomorfismo*.

Si un homomorfismo $\varphi : G \rightarrow G'$ es tal que φ es sobre; es decir, si $\varphi(G) = G'$, decimos que es un *epimorfismo*.

Si un homomorfismo $\varphi : G \rightarrow G'$ es tanto uno a uno como sobre decimos que φ es un *isomorfismo* y, así se dice que G es isomorfo a G' y se denota por $G \cong G'$.

Si φ es un homomorfismo de G en G' , entonces

- i) $\varphi(e) = e'$ donde e es el idéntico de G y e' el de G' .
 ii) $\varphi(a^{-1}) = \varphi(a)^{-1}$ para toda $a \in G$.

Probamos i) $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$ por lo que $e' = \varphi(e)$. Para ii) tenemos $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$ por lo que $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Definimos la *imagen* de φ como: $\varphi(G) = \{ \varphi(a) \mid a \in G \}$, y la denotamos como: $I_m \varphi$.

Afirmamos que la $I_m \varphi$ es un subgrupo de G' .

Es claro que $I_m \varphi \neq \emptyset$ ya que $e \in G$ lo que implica que $\varphi(e) = e' \in I_m \varphi$. Sea $y, z \in I_m \varphi$ entonces existen $a, b \in G$ tal que $\varphi(a) = y$ y $\varphi(b) = z$. Sea $y \in I_m \varphi$ entonces existe $a \in G$ tal que $\varphi(a) = y$, como G es grupo, existe $a^{-1} \in G$ y $\varphi(a^{-1}) = \varphi(a)^{-1} = y^{-1}$ por lo que $y^{-1} \in I_m \varphi$.

Si φ es un homomorfismo de G en G' , entonces el *Kernel* o *núcleo* de φ , que denotamos con $\mathbf{K}(\varphi)$, lo definimos como $\mathbf{K}(\varphi) = \{ a \in G \mid \varphi(a) = e' \}$.

Decimos que el Kernel es un subgrupo de G .

Veamos que es cierto. Sean $a, b \in \mathbf{K}(\varphi)$, entonces $\varphi(ab) = \varphi(a)\varphi(b) = e'e' = e'$ por lo que $ab \in \mathbf{K}(\varphi)$. Por otro lado si $a \in \mathbf{K}(\varphi)$, como $a \in G$ existe $a^{-1} \in G$ y $\varphi(a^{-1}) = \varphi(a)^{-1} = e'^{-1} = e'$ por lo que $a^{-1} \in \mathbf{K}(\varphi)$. Por último como $\varphi(e) = e'$ se tiene que $e \in \mathbf{K}(\varphi)$.

Un subgrupo N de G es un *subgrupo normal* de G , si $a^{-1}Na \subset N$, para todo $a \in G$ y lo denotamos $N \nabla G$.

Es fácil ver que si $a^{-1}Na \subset N$ para toda $a \in G$, entonces $a^{-1}Na = N$ para toda $a \in G$.

Afirmamos que $N \triangleleft G$ si y sólo si toda clase lateral izquierda de N en G es una clase lateral derecha de N en G .

Supongamos $N \triangleleft G$, entonces $a^{-1} N a = N$ para toda $a \in G$; la clase lateral derecha de N en G para $a \in G$ es Na y se tiene $Na = (a a^{-1})(Na) = a(a^{-1} Na) = aN$ para toda $a \in G$.

Supongamos que una clase lateral derecha es clase lateral izquierda, es decir, $Nb = aN$ como $a \in aN$ se tiene que $a \in Nb$, por lo que $Na \subset N(Nb) = (NN) b = N b$ entonces $a^{-1} Na \subset N$ para toda $a \in G$ por lo que N es normal en G .

Un teorema clásico en la teoría de grupos es el de Cayley. Aquí lo enunciamos y demostramos.

TEOREMA DE CAYLEY: *Todo grupo G es isomorfo a algún subgrupo de $A(S)$, para un S apropiado.*

Sea G un grupo y como S escogemos el conjunto subyacente a G que denotamos por G mismo. Sea $a \in G$, definimos $T_a: G \rightarrow G$ tal que $T_a(x) = ax$, es claro que T_a es biyectiva, además tenemos que: $(T_a T_b)(x) = T_a(T_b x) = T_a(bx) = (ab)x = T_{ab}(x)$ por lo que definimos $\varphi: G \rightarrow A(G)$ tal que $\varphi(a) = T_a$ para $a \in G$, como $\varphi(ab) = T_{ab} = T_a T_b = \varphi(a)\varphi(b)$, entonces φ es un homomorfismo de G en $A(G)$.

Supongamos que $\varphi(a) = \varphi(b)$, es decir $T_a = T_b$, entonces $ax = bx$ para toda $x \in G$, entonces $a = b$ por lo tanto φ es inyectiva.

La imagen de φ que es: $\varphi(G) = \{T_a \in A(G) \mid a \in G\}$ es un subgrupo de $A(G)$ de esta manera G es isomorfo a un subgrupo de $A(G)$.

III. Permutaciones.

En este capítulo nos ocuparemos de los grupos de permutaciones que, como vimos al final del capítulo anterior en el teorema de Cayley, son de suma importancia y además haremos uso de ellos posteriormente.

Sean $S = \{x_1, x_2, \dots, x_n\}$ y como establecimos anteriormente $S_n = A(S)$. A los elementos de S_n los llamamos *permutaciones de n elementos*, por lo que si σ es una permutación de n elementos $\sigma \in S_n$. Como $\sigma(x_k) \in S$ para $k = 1, 2, \dots, n$, entonces $\sigma(x_k) = x_{i_k}$ para algún $i_k, 1 \leq i_k \leq n$.

Como la permutación σ es inyectiva, si $j \neq k$, entonces $x_{i_j} = \sigma(x_j) \neq \sigma(x_k) = x_{i_k}$; por lo tanto, i_1, i_2, \dots, i_n son simplemente los números $1, 2, \dots, n$ acomodados en algún orden y la acción de σ en S queda determinada por la forma en que σ asocia el i_j correspondiente al subíndice j de x_j ; por lo que el símbolo x sale sobrando y para referirnos a S bastaría con referirnos únicamente a un conjunto de la forma $\{1, 2, \dots, n\}$ al que llamamos I_n .

Una forma clara para expresar una permutación es hacer una tabla que muestre como σ asocia a los elementos de I_n . Así, si $\sigma \in S_n$ es tal que $\sigma(1) = i_1, \sigma(2) = i_2, \dots, \sigma(n) = i_n$, entonces a σ la describimos como:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

El siguiente ejemplo nos permite observar que no es necesario escribir siempre el primer renglón de la tabla que representa una permutación en el orden $1\ 2\ \dots\ n$, sino que es posible escribirlo en cualquier orden.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

La permutación identidad es aquella en la que los dos renglones de la tabla que la representa son iguales, es decir, $\text{Id}_n(1) = 1, \text{Id}_n(2) = 2, \dots, \text{Id}_n(n) = n$.

Para $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ la permutación inversa de σ , que denotamos σ^{-1} es:

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

Si σ y τ son dos permutaciones de S_n , a $\sigma \circ \tau$ la denotamos $\sigma \tau$ y le llamamos producto, se realiza aplicando primero τ y a este resultado se le aplica σ . Para obtener la tabla $\sigma \tau$ primero se examina el número r del primer renglón de τ y se ve que i_r está abajo de r en el segundo renglón de τ , después se observa el lugar de i_r en el primer renglón de σ y se ve el número s que está abajo de i_r en el segundo renglón de σ y este último número s es la imagen de r respecto al producto $\sigma \tau$.

A manera de ejemplo consideramos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \text{y} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

de acuerdo a lo anterior

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Consideremos el siguiente ejemplo, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$; en él

observamos que 1 va al 2, 2 va al 3, 3 va al 1 y como 1 va al 2 se ha generado una situación cíclica; de igual manera 4 va al 5 y 5 va al 4 es otra situación cíclica, lo que nos motiva a definir el concepto de k -ciclo como sigue.

Al arreglo $(i_1 \ i_2 \ . \ . \ . \ i_k)$ le llamamos *ciclo de orden k o k -ciclo*. Determina la permutación σ $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ y $\sigma(j) = j$ para toda $j \in I_n, j \neq i_1, \dots, i_k$.

En el caso particular de que $k = 2$, al arreglo $(i_1 \ i_2)$ le llamamos *transposición*.

Dados un k -ciclo y un m -ciclo, decimos que son *ajenos* o *disjuntos* si no tienen ningún elemento en común. Por ejemplo, $(1 \ 2 \ 3)$ y $(4 \ 5)$ son dos ciclos ajenos.

Afirmamos que si la permutación $\sigma \in S_n$ es un k -ciclo, entonces el orden de σ es k .

Para mostrarlo suponemos que σ es el k -ciclo de S_n igual a $(i_1 \ i_2 \ . \ . \ . \ i_k)$, entonces $\sigma^k(i_1) = \sigma^{k-1}(i_2) = \sigma^{k-2}(i_3) = \dots = \sigma(i_k) = i_1$. Y así para todo i_j $\sigma^k(i_j) = i_j$, por lo que $\sigma^k = e$ y $\sigma^s \neq e$ para $0 < s < k$.

Para un k -ciclo $\sigma = (i_1 \ i_2 \ . \ . \ . \ i_k)$ tenemos que: $\sigma = (i_1 \ \sigma(i_1) \ \sigma^2(i_1) \ . \ . \ . \ \sigma^{k-1}(i_1))$ por lo que le llamamos el k -ciclo *determinado por i_1* .

Necesitamos de la siguiente proposición. Sean $\sigma_1, \sigma_2 \in S_n$, suponemos que se tiene $T_1 \subset I_n, T_2 \subset I_n$ con $T_1 \cap T_2 = \emptyset$, tales que σ_1 deja fijo a $I_n - T_1$, es decir, sólo actúa en T_1 y σ_2 deja fijo a $I_n - T_2$, es decir, sólo actúa en T_2 , entonces $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$.

Para probarla decimos que si $i_j \in T_1$, entonces $\sigma_1 \sigma_2(i_j) = \sigma_1(i_j)$ y $\sigma_2 \sigma_1(i_j) = \sigma_1(i_j)$ ya que $\sigma_1(i_j) \notin T_2$. Análogamente si $i_j \in T_2$, entonces $\sigma_1 \sigma_2(i_j) = \sigma_2(i_j)$ y $\sigma_2 \sigma_1(i_j) = \sigma_2(i_j)$ ya que $\sigma_2(i_j) \notin T_1$. Si $i_j \in I_n - (T_1 \cup T_2)$, entonces $\sigma_1 \sigma_2(i_j) = i_j$ y $\sigma_2 \sigma_1(i_j) = i_j$ y por lo tanto $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$.

Ahora afirmaremos que toda permutación en S_n es el producto de ciclos ajenos.

Para mostrarlo consideremos a $\sigma \in S_n$ y tomamos a τ_1 un k -ciclo determinado por i_1 y a τ_2 un l -ciclo determinado por i_2 , donde i_2 es el primer elemento de I_n que no aparece en τ_1 , por lo que τ_1 y τ_2 son ajenos; τ_3 es un m -ciclo determinado por algún elemento de I_n que no aparezca en τ_1 y en τ_2 , por lo que τ_1, τ_2 y τ_3 son ajenos y este proceso termina hasta llegar a una τ_p , determinada por el primer elemento que no aparezca en $\tau_1 \tau_2 \tau_3 \dots \tau_{p-1}$. Por lo que $\tau_1 \tau_2 \tau_3 \dots \tau_p$ es el producto de ciclos ajenos y $\sigma = \tau_1 \tau_2 \tau_3 \dots \tau_p$.

Por ejemplo, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 1 & 4 & 5 & 9 & 6 & 3 & 7 \end{pmatrix}$ es una

permutación de S_9 que tiene como ciclos a: $(1\ 2\ 8\ 3)$, (4) , (5) y $(6\ 9\ 7)$, luego σ se expresa como el producto $(1\ 2\ 8\ 3)(4)(5)(6\ 9\ 7)$.

Convenimos que al expresar una permutación como el producto de ciclos ajenos, se omiten todos los ciclos de orden uno, así, en el ejemplo anterior la permutación se expresa como: $\sigma = (1\ 2\ 8\ 3)(6\ 9\ 7)$.

Decimos que si $\sigma \in S_n$ es una permutación que tiene una descomposición en k -ciclos ajenos de longitudes m_1, m_2, \dots, m_k , entonces el orden de σ es el *mínimo común múltiplo* de m_1, m_2, \dots, m_k .

Lo mostramos para el caso en que $\sigma = \tau_1 \tau_2$, donde τ_1 y τ_2 son ajenos; suponemos a τ_1 un m_1 -ciclo y a τ_2 un m_2 -ciclo; entonces σ es el producto de ciclos ajenos de ordenes m_1 y m_2 ; si el orden de σ es k , entonces es fácil por los párrafos anteriores que $\sigma^k = (\tau_1 \tau_2)^k = \tau_1^k \tau_2^k = e$. Entonces $\tau_1^k = e = \tau_2^k$ y por el teorema de Lagrange $m_1 \mid k$ y $m_2 \mid k$; por lo tanto, si m es el mínimo común múltiplo de m_1, m_2 , entonces m divide a k por lo que $m \leq k$; además si m es el mínimo común múltiplo de m_1 y m_2 , entonces $\sigma^m = (\tau_1 \tau_2)^m = \tau_1^m \tau_2^m = e$ por lo que $m \geq k$; por lo tanto $m = k$.

Afirmamos que toda permutación en S_n es el producto de transposiciones.

En párrafos anteriores vimos que toda permutación es el producto de ciclos ajenos y si $(i_1 i_2 \dots i_k)$ es un k -ciclo, entonces $(i_1 i_2 \dots i_k) = (i_1 i_k)(i_1 i_{k-1}) \dots (i_1 i_2)$, por lo que todo k -ciclo es producto de k transposiciones, si $k > 1$.

En el siguiente ejemplo observamos que este producto se puede realizar de varias formas, no de forma única. $(1 2 3) = (1 3)(1 2)$ y $(1 2 3) = (3 2)(1 3)$.

Decimos que si τ_1, τ_2 son transposiciones en S_n para $n \geq 3$, entonces $\tau_1 \tau_2$ es un 3-ciclo o bien el producto de dos 3-ciclos.

Para mostrarlo es necesario separar en tres casos:

1º.Caso: Suponemos que $\tau_1 = \tau_2$, tal que $\tau_1 = (i_1 i_2) = \tau_2$, entonces $\tau_1 \tau_2 = (i_1 i_2)(i_1 i_2) = (i_1 i_2)^2 = e$ y e es el producto de dos 3-ciclos, por ejemplo $e = (1 2 3)(3 2 1)$

2º.Caso: Suponemos τ_1 y τ_2 , tales que $\tau_1 = (i_1 i_2)$ y $\tau_2 = (i_1 i_3)$ con $i_2 \neq i_3$, entonces $\tau_1 \tau_2 = (i_1 i_2)(i_1 i_3) = (i_1 i_3 i_2)$ es un 3-ciclo.

3º.Caso: Suponemos τ_1 y τ_2 , tales que $\tau_1 = (i_1 i_2)$ y $\tau_2 = (i_3 i_4)$ con $\{i_1, i_2\} \cap \{i_3, i_4\} = \emptyset$, entonces $\tau_1 \tau_2 = (i_1 i_2)(i_3 i_4) = (i_1 i_4 i_2)(i_1 i_4 i_3)$ es el producto de dos 3-ciclos.

Procedemos ahora a dar unas definiciones que nos servirán posteriormente.

Sea $\sigma \in S_n$ tal que, $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$, entonces

decimos que $\sigma(i), \sigma(j)$ forman una *inversión* si $i < j$ y $\sigma(i) > \sigma(j)$.

Una permutación $\sigma \in S_n$ es *par* si el número de inversiones en $\sigma(1), \sigma(2), \dots, \sigma(n)$ es *par*.

Una permutación $\sigma \in S_n$ es *impar* si el número de inversiones en $\sigma(1), \sigma(2), \dots, \sigma(n)$ es *impar*.

Por ejemplo, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$ es una permutación de S_5 en la

que:

$$\sigma(2) = 3 \text{ forma inversión con } \sigma(1) = 5$$

$$\sigma(3) = 4 \text{ forma inversión con } \sigma(1) = 5$$

$$\sigma(4) = 1 \text{ forma inversión con } \sigma(1) = 5$$

$$\sigma(5) = 2 \text{ forma inversión con } \sigma(1) = 5$$

$$\sigma(4) = 1 \text{ forma inversión con } \sigma(2) = 3$$

$$\sigma(5) = 2 \text{ forma inversión con } \sigma(2) = 3$$

$$\sigma(4) = 1 \text{ forma inversión con } \sigma(3) = 4$$

$$\sigma(5) = 2 \text{ forma inversión con } \sigma(3) = 4$$

lo que nos da un total de ocho inversiones y por lo tanto, la permutación σ es par.

Aseveramos que si τ es una permutación obtenida de la permutación σ mediante el intercambio de dos números, entonces σ y τ tienen distinta paridad.

Para mostrarlo separamos en dos casos:

1^{er}. Caso: Si los números que se intercambian son consecutivos.

Sean σ y τ dos permutaciones de S_n , tales que τ se obtuvo de intercambiar a σ dos números consecutivos, así:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(i) & \sigma(i+1) & \dots & \sigma(n) \end{pmatrix} \text{ y}$$

$$\tau = \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(i+1) & \sigma(i) & \dots & \sigma(n) \end{pmatrix}, \text{ entonces las parejas}$$

de números que forman inversión en σ , también la forman en τ , excepto $\sigma(i)$ y $\sigma(i+1)$. Si $\sigma(i)$, $\sigma(i+1)$ no forman inversión en σ , en τ si la forman e inversamente. Por esto, el número de inversiones en σ aumenta o disminuye en 1 al pasar a τ . Es decir, si σ tiene r inversiones, entonces τ tiene $r+1$ o $r-1$ inversiones y por lo tanto, la paridad de σ y de τ es distinta.

2o. Caso: Si los números que se intercambian están separados s lugares.

$$\text{Sea } \sigma = \begin{pmatrix} 1 & 2 & \dots & r & \dots & r+s & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(r) & \dots & \sigma(r+s) & \dots & \sigma(n) \end{pmatrix} \text{ una}$$

permutación en S_n , entonces podemos obtener σ' haciendo s intercambios de números consecutivos, cambiando $\sigma(r)$ por cada uno de su derecha hasta llegar

$$\text{a } \sigma' = \begin{pmatrix} 1 & 2 & \dots & r & \dots & r+s & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(r+1) & \dots & \sigma(r) & \dots & \sigma(n) \end{pmatrix} \text{ y después}$$

haciendo $s - 1$ intercambios de números consecutivos, cambiando $\sigma(r + s)$ que está a la izquierda de $\sigma(r)$, con cada uno de los anteriores hasta llegar a

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & r & \dots & r+s & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(r+s) & \dots & \sigma(r) & \dots & \sigma(n) \end{pmatrix}. \text{ Por lo que}$$

pasamos de σ a τ con $2s - 1$ intercambios de números consecutivos y la paridad cambia.

Es fácil ver por los párrafos anteriores que si σ es una permutación de S_n y τ una transposición en S_n , entonces σ y $\tau\sigma$ tienen distinta paridad.

El producto de m transposiciones es par si y sólo si m es par. Análogamente, el producto de m transposiciones es impar si y sólo si m es impar.

Obviamente, por todo lo anterior, la permutación identidad es par, pues hay cero inversiones; entonces τ_1 es impar; $\tau_2 \tau_1$ es par; $\tau_3 \tau_2 \tau_1$ es impar y así sucesivamente.

Entonces tenemos el siguiente resultado: una permutación es par si y se le puede escribir como el producto de un número par de transposiciones.

Al conjunto de todas las permutaciones pares, que denotamos A_n , le llamamos *grupo alternante de grado n* y es un subgrupo de S_n .

Afirmamos que A_n es un subgrupo normal de S_n .

Para mostrarlo sea $\sigma \in A_n$ y $\rho \in S_n$, entonces ρ y ρ^{-1} son de la misma paridad y como σ es una permutación par tenemos que $\rho^{-1}\sigma\rho$ es par y por lo tanto está en A_n .

IV. Una Aplicación de la Teoría de Gráficas en Teoría de Grupos.

En este capítulo mostraremos una aplicación interesante de la teoría de gráficas en teoría de grupos. Es el isomorfismo entre dos gráficas construidas con elementos de la teoría de grupos.

Sabemos, por el capítulo anterior, que S_6 es el grupo de permutaciones de $I_6 = \{1, 2, 3, 4, 5, 6\}$. Denominamos con T el conjunto de elementos de orden dos S_6 y definimos una gráfica, que denominamos T , como la que tiene por vértices los elementos del conjunto T y además dos vértices son adyacentes si su producto es de orden tres.

A partir de la gráfica T obtenemos tres subgráficas, que llamamos G_1 , G_2 y G_3 ; donde G_1 tiene como vértices al conjunto de transposiciones, G_2 tiene como vértices el producto de dos transposiciones ajenas y G_3 tiene como vértices al producto de tres transposiciones ajenas.

Diremos que $\{ (x, y) \mid x, y \in I_6 \}$ son los vértices de G_1 y dos vértices son adyacentes si son de la forma $(x y)$, $(x z)$, con $y \neq z$. Es fácil mostrarlo ya que su producto $(x y)(x z) = (x z y)$ es de orden tres y el producto de los vértices que no son de esta forma es de orden dos.

Afirmamos que $\{(w x)(y z) \mid w, x, y, z \in I_6\}$, con todos distintos entre sí, son los vértices de G_2 y dos vértices son adyacentes si tienen alguna de las siguientes formas:

- i) $(u v)(w x)$ y $(u v)(w y)$ con $x \neq y$ ó
- ii) $(u v)(w x)$ y $(u y)(w z)$ con $v \neq y$ y $x \neq z$

Evidentemente ambos productos son de orden tres y además el producto de vértices que no tienen estas formas no son de orden tres.

En G_3 $\{(u v)(w x)(y z) \mid u, v, w, x, y, z \in I_6\}$, con todos distintos entre sí, son sus vértices y dos vértices son adyacentes si son de la forma $(u v)(w x)(y z)$ y $(u w)(v y)(x z)$. Es fácil ver que su producto es de orden tres y que si no tienen esta forma, entonces su producto no es de orden tres.

Inmediatamente se ve que si tomamos un vértice de G_1 y uno de G_2 , entonces su producto no es de orden tres, lo mismo sucede si tomamos uno de G_2 y uno de G_3 ; también el producto de un vértice de G_1 con uno de G_3 no es de orden tres.

Por lo anterior, las gráficas G_1 , G_2 y G_3 son subgráficas ajenas y $T = G_1 \cup G_2 \cup G_3$.

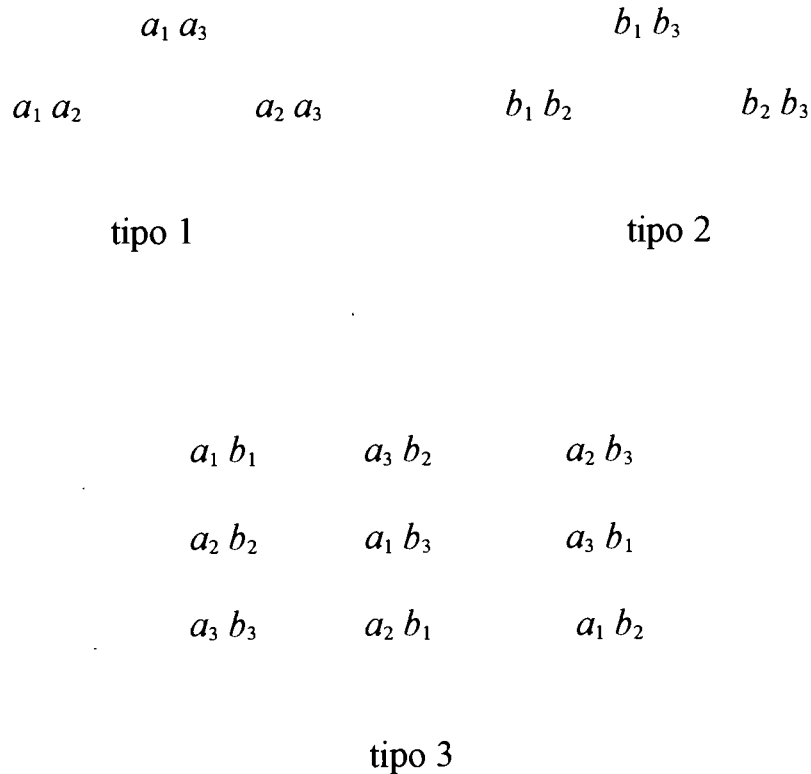
La idea central de este capítulo es probar que la gráfica G_1 es isomorfa a la gráfica G_3 , es decir, $G_1 \cong G_3$.

Para probarlo emplearemos la gráfica $L(K_6)$, que como vimos en el capítulo I es la gráfica de aristas de K_6 , donde dos vértices son adyacentes en $L(K_6)$ si las aristas de K_6 tienen un vértice en común.

Primero probaremos que $G_1 \cong L(K_6)$ y posteriormente probaremos que $G_3 \cong L(K_6)$ y por lo tanto $G_1 \cong G_3$.

Para probar que $G_1 \cong L(K_6)$ suponemos a K_6 la gráfica con vértices $\{a, b, c, d, e, f\}$ y con aristas $\{\{x, y\} \mid x, y \in \{a, b, c, d, e, f\} \text{ con } x \neq y\}$. Por párrafos anteriores los vértices de $L(K_6)$ son de la forma $\{x, y\}$ y dos de ellos son adyacentes si son de la forma $\{x, y\}, \{x, w\}$ con $y \neq w$. La correspondencia dada entre los vértices de $L(K_6)$ y los de G_1 , es decir, $\{x, y\} \rightarrow (x y)$ es biyectiva y preserva adyacencias; por lo tanto $G_1 \cong L(K_6)$.

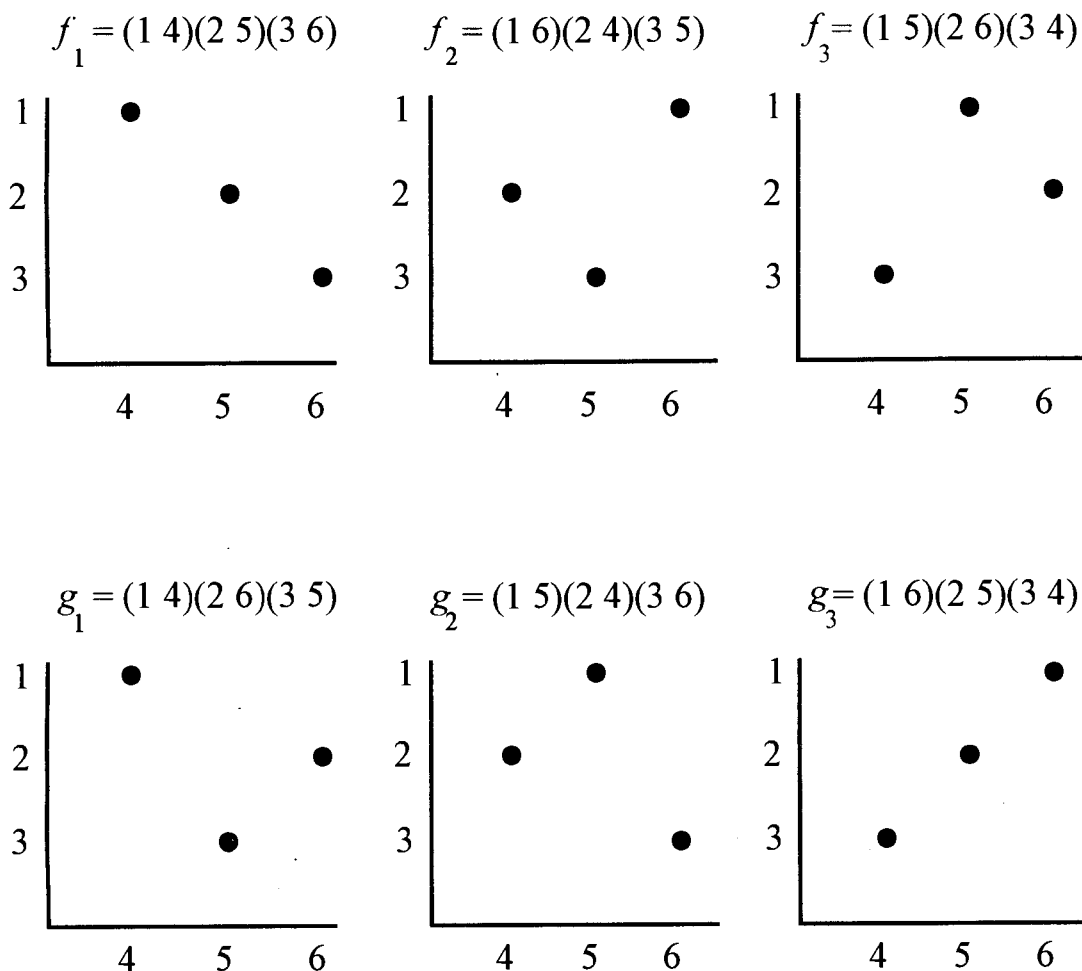
Para probar que $G_3 \cong L(K_6)$ consideremos a K_6 la gráfica con vértices $\{a_1, a_2, a_3, b_1, b_2, b_3\}$ y además a los quince vértices de la gráfica $L(K_6)$ los clasificamos en tres tipos.



En esta clasificación observamos lo siguiente: los tres vértices del tipo 1 son adyacentes, es decir tenemos a K_3 , al igual que los del tipo 2 y además entre los vértices del tipo 1 y los del tipo 2 no existen adyacencias. También observamos que cada vértice del tipo 3 es adyacente con cuatro vértices que no están en el mismo renglón y columna que él y además cada uno es adyacente con dos vértices del tipo 1 y con dos del tipo 2.

Describiremos a continuación la gráfica G_3 de tal manera que un isomorfismo entre ella y la gráfica $L (K_6)$ que acabamos de ilustrar resulte evidente.

Sean $C = \{1, 2, 3\}$ y $C' = \{4, 5, 6\}$, identificamos los seis siguientes vértices de G_3 con las seis funciones biyectivas de C en C' en la manera siguiente:



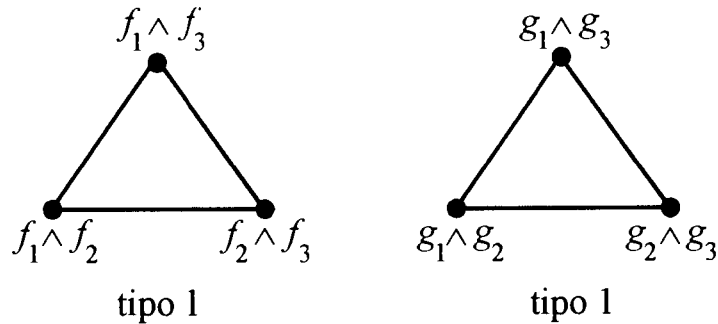
Los tres primeros vértices f_1, f_2 y f_3 , que llamamos *funciones pares*, serán los del tipo 1 y los vértices g_1, g_2 y g_3 que llamamos *funciones impares*, serán los del tipo 2. Observemos que:

$$\begin{aligned}
 f_1 f_2 f_1 = f_2 f_1 f_2 = f_3, & \quad f_1 f_3 f_1 = f_3 f_1 f_3 = f_2, & \quad f_2 f_3 f_2 = f_3 f_2 f_3 = f_1, \\
 g_1 g_2 g_1 = g_2 g_1 g_2 = g_3, & \quad g_1 g_3 g_1 = g_3 g_1 g_3 = g_2 & \quad \text{y } g_2 g_3 g_2 = g_3 g_2 g_3 = g_1.
 \end{aligned}$$

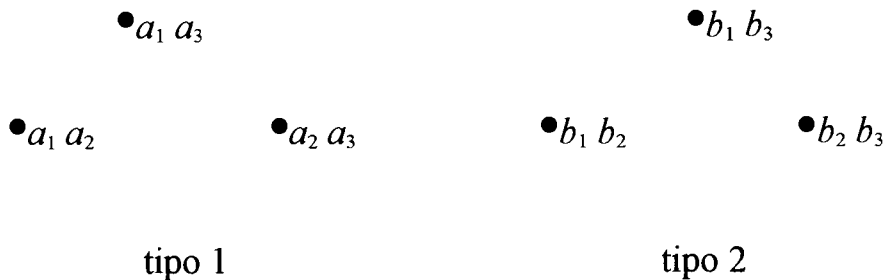
Así, adoptamos la notación

$$\begin{aligned}
 f_3 &= f_1 \wedge f_2, & f_2 &= f_1 \wedge f_3, & f_1 &= f_2 \wedge f_3, \\
 g_3 &= g_1 \wedge g_2, & g_2 &= g_1 \wedge g_3, & g_1 &= g_2 \wedge g_3.
 \end{aligned}$$

Tomando en cuenta que, por definición dos vértices de G_3 son adyacentes si no tienen una transposición común, la parte de la gráfica G_3 restringida a estos seis vértices es



y los tres vértices del tipo 1, al igual que los del tipo 2, son adyacentes dos a dos, mientras que los del tipo 1 no son adyacentes con los del tipo 2. Aquí vemos, por lo pronto parte del isomorfismo de G_3 con $L(K_6)$:



Pasemos ahora al análisis de los nueve restantes vértices de G_3 para compararlos con los de $L(K_6)$.

A cada punto (a,b) del producto cartesiano $C \times C'$ asociamos un vértice de G_3 como sigue: sea $C - \{a\} = \{c, d\}$ y $C' - \{b\} = \{e, f\}$, entonces a (a,b) le asociamos el vértice $(a\ b) (c\ d) (e\ f)$ de G_3 . Por ejemplo a $(1, 4)$ le asociamos $(1\ 4)(2\ 3)(5\ 6)$; a $(2, 6)$ le asociamos $(2\ 6)(1\ 3)(4\ 5)$; a $(3, 4)$ le asociamos $(3\ 4)(1\ 2)(5\ 6)$, etc.

Observamos ahora que cada punto de $C \times C'$ está exactamente en una f_i y exactamente en una g_j . Por ejemplo, $(1, 4)$ está en f_1 y en g_1 ; de hecho es

$f_1 \cap g_1$; es la transposición común (1 4). Por ejemplo también, (2, 6) es $f_3 \cap g_1$. De esta manera, los nueve vértices restantes de G_3 que llamaremos del tipo 3 los podemos escribir así:

$$\begin{array}{ccc} f_1 \cap g_1 & f_3 \cap g_2 & f_2 \cap g_3 \\ f_2 \cap g_2 & f_1 \cap g_3 & f_3 \cap g_1 \\ f_3 \cap g_3 & f_2 \cap g_1 & f_1 \cap g_2 \end{array}$$

tipo 3

Esto nos da la correspondencia con los nueve vértices del tipo 3 de $L(K_6)$.

$$\begin{array}{ccc} a_1 b_1 & a_3 b_2 & a_2 b_3 \\ a_2 b_2 & a_1 b_3 & a_3 b_1 \\ a_3 b_3 & a_2 b_1 & a_1 b_2 \end{array}$$

tipo 3

Finalmente, es directo comprobar que:

1.- Cada vértice del tipo 3 de G_3 , al igual de lo que ocurre en $L(K_6)$, es adyacente exactamente con los cuatro vértices que no están en el mismo renglón ni en la misma columna que él. Es decir $f_i \cap g_j$ es adyacente con los cuatro vértices $f_r \cap g_s$ con $r \neq i, s \neq j$.

2.- Todo vértice del tipo 3, $f_i \cap g_j$, como también ocurre en $L(K_6)$, es adyacente con los dos vértices $f_i \wedge f_r$ del primer tipo y con los dos vértices $g_s \wedge g_j$ del tipo 2.

Con esto queda demostrado el isomorfismo de G_3 y $L(K_6)$. Y, como ya sabemos G_1 es también isomorfo a la gráfica de aristas de $L(K_6)$. Por lo tanto las gráficas G_1 y G_3 son isomorfas.

Bibliografía

Behzad Mehdi, Chartrand Gary, Lesniak-Foster Linda.
Graphs & Digraphs.
Prindle, Weber & Schmidt International Series. 1979

Cárdenas H., Lluís E., Raggi F., Tomás F.
Álgebra Superior.
Editorial Trillas. 1985

Cárdenas Humberto y Lluís Emilio.
The outer automorphism of S_6 .
Aportaciones Matemáticas.
XXVI Congreso Nacional de la Sociedad Matemática Mexicana.
Sociedad Matemática Mexicana. 1994.

Curcó María del Carmen.
Una introducción a la teoría de gráficas.
Serie Vínculos Universitarios
Facultad de Ciencias UNAM. 1991

Fraleigh John B.
Algebra Abstracta.
Addison-Wesley Iberoamericana. 1987

Harary Frank.
Graph Theory
Addison-Wesley Publishing Co. 1969

Herstein I.N.
Algebra Abstracta.
Grupo Editorial Iberoamérica. 1989

Ross Kenneth A., Wright Charles R.B.
Matemáticas Discretas.
Prentice-Hall Hispanoamericana. 1994