2 ej
12

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

Facultad de Ciencias

"ALGUNAS APLICACIONES DE LA TEORIA DE GRAFICAS A LA TEORIA DE GRUPOS."

T E S I S

Que para obtener el título de:

M A T E M A T I C O

P r e s e n t a :

Armando Moisés Martínez Cruz

México, D. F. 1987

INDICE.

Introducción.

INTRODUCCION

"NO TE ENORGULLEZCAS DEL FRUTO DE TU INTELIGENCIA. RECUERDA QUE SOLO ERES DUEÑO DEL ESFUERZO QUE PUSISTE EN SU CULTIVO; DE LO QUE LOGRAS, APENAS ERES UN SIMPLE ESPECTADOR".

Jacinto Canek.

Habiendo estudiado por una parte la Teoría de Gráficas y por otra la Teoría de Grupos, se buscaron aplicaciones que reunieran a ambas teorías. Se encontraron varios artículos y en base a ellos se desarrolló el presente trabajo.

En los dos primeros Capítulos se mencionan conceptos, resultados ejemplos, Teoremas y Corolarios tanto de la Teoría de Grupos Finitos , Cap. I., como de la Teoría de Gráficas Finitas. Cap. II.

Se consideró también la conveniencia de mencionar al menos varios nexos entre ambas Teorías. Algunos resultados importantes como el Teorema de Frucht y las Gráficas dirigidas de Cayley se mencionan en el Capítulo III.

En el último Capítulo se tratan tres aplicaciones de la Teoría de Gráficas a la Teoría de Grupos. En las dos primeras secciones no hay restricción alguna para la conmutatividad de la operación en el grupo Γ, la tercera sección se dedica a grupos abelianos.

El primer resultado se refiere a una cota superior para la cardinalidad de los subgrupos abelianos de un grupo finito. en base a la cardinalidad de las clases de conjugación de Γ. En este caso se asocia una gráfica de *conmutación* (dos vértices son adyacentes si y sólo si conmutan) y se utiliza un resultado sobre la coloración de vértices de una gráfica. El segundo resultado se refiere a cubiertas de un grupo mediante subgrupos abelianos, en este caso se utiliza también la gráfica de *conmutación* y un Teorema (Wei) que relaciona el número de independencia de una gráfica con la suma de los grados de los vértices. Para la última sección se usa una gráfica distinta y un Corolario del Teorema de Wei para demostrar un resultado sobre la cardinalidad de un conjunto libre de sumas.

Para la mejor comprensión de los resultados incluidos, se ilustran los conceptos con ejemplos esperando que los lectores no familiarizados con estas Teorías, puedan comprender el material. Ellos motivaron en buena parte la estructura del trabajo. Si este además despierta su inquietud, habré obtenido mi objetivo con éxito.

Sobre la localización de los Teoremas, Corolarios y Ejemplos. Todos están numerados en orden creciente mediante un número arábigo. Cuando se hace referencia a alguno de ellos, se usa además un número romano para indicar el Capítulo. Por ejemplo Tma. II, 3. se refiere al Teorema 3 del Capítulo II. En caso de que el Teorema, Corolario, Lema o Ejemplo pertenezca al mismo capítulo, se omite el número romano.

Las referencias bibliográficas se citan usando parentésis cuadrados, por ejemplo *ver* [8, pag. 25] indica la octava referencia, página 25.

Estoy en deuda con los Dres. Hortensia Galeana Sánchez y Hugo Alberto Rincón Mejía por sugerir, dirigir, revisar y corregir el trabajo. En particular, muchas gracias por su paciencia, comprensión, apoyo y disposición durante el desarrollo del mismo.

Gracias también a Vicky Urrutia, compañera y amiga, a Vicky Abrin y a Zeferino Parada por aceptar ser miembros del jurado.

Agradezco la paciencia y comprensión de todas las personas a mi alrededor, quienes se mostraron interesados e incluso preocupados por ver al fin listo este trabajo. Para no olvidar nombres, a todos ellos gracias.

Gracias también a todos mis profesores de la Facultad de Ciencias de la UNAM, a quienes debo mi formación en Matemáticas y a mis compañeros que con su dedicación y ejemplo me enseñaron que no todo se aprende en la escuela.

CAPITULO I. TEORIA DE GRUPOS FINITOS.

"CUANDO KLEIN NOS HACE VER QUE LA TEORIA ALGEBRAICA DE ECUACIONES DE 5o. GRADO SE SIMPLIFICA NOTABLEMENTE CON UN ESTUDIO PREVIO DE LAS PROPIEDADES DEL ICOSAEDRO REGULAR Y QUE ESTA COMPARACION TAMBIEN PERMITE UN ESTUDIO FRUCTIFERO DE CIERTAS ECUACIONES DIFERENCIALES DE 2o. ORDEN, NOS ADMIRAMOS DE COMO ESTA OBSERVACION ILUMINA MUCHOS DETALLES."

Emile Borel.

Básicamente, las operaciones que uno realiza son reglas aprendidas, que permiten asociar a un par de números dispuestos en un cierto orden, un tercer número como respuesta. La suma, el producto, la división, son reglas, pero distintas reglas. Y estas reglas se definen solamente para pares de objetos de un conjunto específico.

Def. Una operación binaria $*$ en un conjunto S es una regla que asigna a cada par ordenado de elementos del conjunto, algún elemento del conjunto.

$$* : S \times S \to S$$
$$(a, b) \to a*b$$

Def. Una operación binaria $*$ en un conjunto S es conmutativa si $a*b = b*a$, para todo a, $b \in$ S. La operación es asociativa si $(a*b)*c = a*(b*c)$ para todo a, b, $c \in$ S.

Muchas situaciones conducen a ecuaciones que involucran un número x, cuyo valor debe determinarse. Las ecuaciones más simples son las de la forma $a + x = b$ para la suma y $ax = b$ para el producto. Ambas tienen solución dependiendo del conjunto en el que se esté trabajando y en el caso del producto, añadiendo la suposición $a \neq 0$. De cualquier forma la solución de la ecuación lineal aditiva $10 + x = 2$ es una excelente motivación para los números negativos, de igual forma, la necesidad de los números racionales se manifiesta en la ecuación $3x = 4$, la necesidad de los números complejos se muestra en la ecuación $x^2 = -1$.

Es por tanto, deseable que podamos resolver ecuaciones lineales que involucren operaciones binarias. Sin embargo, esta situación no siempre es posible. Como ejemplo consideremos la ecuación $a*x = a$ definida en el conjunto $S = \{a, b, c\}$, de acuerdo con la siguiente tabla:

$*$	a	b	c
a	b	b	b
b	a	c	b
c	c	b	a

En este caso no hay solucion para la ecuación.

Examinemos las propiedades en $\mathbb{Z}$, que nos permiten resolver la ecuación $10 + x = 2$ en $\mathbb{Z}$.

Los pasos para encontrar la solución son:

$10 + x = 2$	propuesta
$-10 + (10 + x) = 2 - 10$	sumando -10
$(-10 + 10) + x = 2 - 10$	asociatividad
$0 + x = 2 - 10$	sumando $-10 + 10$
$x = 2 - 10$	propiedad de 0
$x = -8$	sumando $2 - 10$

Una descripción similar para la ecuación $3x = 4$ se hace:

$3x = 4$	propuesta
$(\frac{1}{3})3x = 4(\frac{1}{3})$	multiplicando por $\frac{1}{3}$
$(\frac{1}{3}3)x = 4(\frac{1}{3})$	asociatividad
$1x = 4\ \frac{1}{3}$	multiplicando $\frac{1}{3}\ 3$
$x = 4\ \frac{1}{3}$	propiedad del 1

$x = \frac{4}{3}$ multiplicando $4 \frac{1}{3}$

Veamos ahora las propiedades que un conjunto S y una operación binaria $*$ en S deben tener, que nos permitan reproducir este procedimiento para la ecuación $a*x = b$ en S. Básicamente necesitamos la existencia de un elemento e con la propiedad de que $a*e = e*a = a$, para todo elemento $a \in S$. 0 y 1 hacen este papel respectivamente en las ecuaciones arriba. Después necesitamos la existencia, de un elemento a', tal que $a'*a = a*a' = e$. Arriba -10 y $\frac{1}{3}$ hacen este papel, respectivamente.

Por último necesitamos la ley asociativa, el resto son meros cálculos.

Uno se puede convencer de que estas propiedades de $*$ en S, nos permiten resolver la ecuación $a*x = b$ en S. Estas propiedades son las de un grupo, precisamente.

Def. Un grupo $\langle \Gamma, * \rangle$ es un conjunto, junto con una operación binaria $*$ en Γ, denominada producto, tal que los siguientes axiomas se satisfacen:

i). $*$ es asociativa.

ii). $\exists\, e \in \Gamma$, tal que $\forall\, x \in \Gamma$, $x*e = e*x = x$.
e es un elemento identidad para $*$ en Γ.

iii). $\forall\, a \in \Gamma$, $\exists\, a' \in \Gamma$ tal que $a*a' = a'*a = e$.
a' es el inverso de a con respecto a $*$.

Es costumbre denotar a a' como $-a$ en el caso de la notación aditiva y a^{-1} en el caso de la notación multiplicativa. Salvo aclaración nosotros usaremos a^{-1}.

Algunos autores redundan, pidiendo que $*$ sea cerrada, de nuestra definición, $*$ resulta serlo.

Debe tenerse presente, que un grupo no sólo es un conjunto, sino que está constituido de dos identidades: el conjunto Γ y la operación binaria $*$ en Γ. De ahora en adelante y cuando no haya posibilidad de confusión, sólo usaremos la letra Γ para denotar $\langle \Gamma, * \rangle$ y ab se referirá a la expresión $a*b$.

Def. Un grupo Γ es abeliano, si su operación binaria es conmutativa.

Si S es un conjunto finito, se puede definir una operación binaria en el por medio de una tabla. Enunciaremos condiciones necesarias en esta tabla, para que defina un grupo:

Debe haber un elemento e que actúe como identidad. La condición $a*e = e*a = a$, $\forall\ a \in S$, significa que la primera columna es igual a la columna que contiene a los elementos a operar, en el mismo orden. De la misma manera , el primer renglón coincide en orden y elementos con el renglón que contiene los elementos a operar.

Como $\forall\ a \in S$, $\exists\ a^{-1}$, e debe aparecer en cada renglón y en cada columna.

Como la operación es cerrada, cada renglón y cada columna contiene una sola vez los elementos de Γ, en distinto orden.

Si estas condiciones se satisfacen, la tabla define un grupo si y sólo si la operación es asociativa.

Def. Si Γ es un grupo finito, el orden $|\Gamma|$ de Γ es el número de elementos de Γ. En general, $\forall$ A, conjunto finito, $|A|$ es el número de elementos de A.

Def. Sea Γ un grupo y sea A un subconjunto de Γ.
Si $\forall\ a, b \in A$ se tiene que el producto ab calculado en Γ también pertenece a A, entonces A es cerrado bajo la operación de grupo de Γ. La operación binaria en A así definida es la operación inducida de Γ en A.

Def. Si H es un subconjunto de un grupo Γ, cerrado bajo la operación de grupo de Γ, y si H es un grupo con esta operación inducida, entonces H es un subgrupo de Γ.

Def. Si Γ es un grupo, entonces Γ es el subgrupo impropio de Γ. Cualquier otro subgrupo es propio. $\{e\}$ es el subgrupo trivial de Γ. Cualquier otro subgrupo es no trivial.

Tma. 1. Sea Γ un grupo y sea $a \in \Gamma$. Entonces $H = \{a^n \ / \ n \in \mathbb{Z}\}$ es un subgrupo de Γ y es el subgrupo más chico de Γ que contiene a a, esto es, todo subgrupo que contiene a a contiene a H.
El grupo H es el subgrupo cíclico generado por a y se denotará por $\langle a \rangle$.

Def. Un elemento a de un grupo Γ genera a Γ y es un generador de Γ si $\langle a\rangle = \Gamma$. Un grupo es cíclico si existe algún elemento a en Γ que genere a Γ.

Ejemplos:

2. Sea $S = \mathbb{R} - \{-1\}$.
Definimos $*$ en S como $a*b = a + b + ab$.
Entonces S es un grupo abeliano de orden infinito.

3. Sea $S = \mathbb{Z}$ con la suma. Entonces S es un grupo infinito, abeliano, cíclico. Los elementos 1 y -1 son generadores del grupo.

4. Considérense las siguientes tablas de multiplicación:

$\mathbb{Z}_4$:

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

V:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Afirmamos que estas tablas definen una estructura de grupo en cada caso. El primero, $\mathbb{Z}_4$ es la suma en los enteros módulo 4 y el segundo es el 4-grupo de Klein.
Ambos grupos son abelianos de orden 4.
El único subgrupo propio no trivial de $\mathbb{Z}_4$ es $\{0, 2\}$.
Obsérvese que $\{0, 1\}$ no es un subgrupo de $\mathbb{Z}_4$, pues no es cerrado con $+$. Por ejemplo $1 + 1 = 2$ y $2 \notin \{0, 1\}$. Es cíclico y cualquier elemento distinto de la identidad es un generador.

V en cambio no es cíclico, de hecho contiene tres subgrupos propios no triviales, $\{e, a\}$, $\{e, b\}$ y $\{e, c\}$. En este caso $H = \{e, a, b\}$ no es un subgrupo, ya que $ab = c \notin H$, lo cual prueba que la operación no es cerrada en este subconjunto.

5. $n\mathbb{Z}$, el conjunto de los múltiplos de n, con la suma es un grupo abeliano, cíclico y de orden infinito. Si m es un entero divisible por n, $m\mathbb{Z}$ es un subgrupo de $n\mathbb{Z}$.

6. Si Γ es un grupo abeliano con identidad e, entonces:

$$H = \{x \in \Gamma \ / \ x^2 = e\} \text{ es un subgrupo de } \Gamma.$$

7. Todo subgrupo de un grupo cíclico es cíclico.

8. Todo grupo cíclico es abeliano, mientras que el recíproco es falso.

9. Si K es un subgrupo de H y H es un subgrupo de Γ, entonces K es un subgrupo de Γ.

Def. Sea Γ un grupo y $a \in \Gamma$. El conjunto $C(a) = \{ x \in \Gamma \mid xa = ax\}$ es un grupo y se conoce como el grupo centralizador de a.

La definición anterior se puede generalizar a cualquier subconjunto S de Γ.

Def. *a*). Sean Γ un grupo y S un subconjunto de Γ.
$C(S) = \{x \in \Gamma \mid xs = sx, \ \forall s \in S\}$. C(S) es un subgrupo de Γ.

b). Si $S = \Gamma$ en *a*), $C(\Gamma)$ es un subgrupo abeliano de Γ y se conoce como el centro de Γ. En adelante a este grupo lo denotaremos por $Z(\Gamma)$.

Nos referiremos a los elementos del centro como centrales.

Se puede demostrar que $Z(\Gamma) = \bigcap_{a \in \Gamma} C(a)$.

El siguiente teorema da condiciones necesarias y suficientes para que un subconjunto no vacío de un grupo, sea grupo.

Tma. 10. Un subconjunto no vacío H de un grupo Γ, es un subgrupo de Γ si y sólo si:

a). $\forall a, b \in H \Rightarrow ab \in H$.
b). $\forall a \in H \Rightarrow a^{-1} \in H$

Si $|\Gamma|$ es finito, el teorema anterior tiene una expresión más sencilla.

Tma. 11. Sea Γ un grupo de orden finito. Si H es un subconjunto no vacío de Γ, cerrado bajo la operación inducida de Γ en H, entonces H es un subgrupo de Γ.

Def. Una función o mapeo Φ de un conjunto A en un conjunto B es una regla que asigna a cada elemento $a \in A$, exactamente un elemento $b \in B$. Diremos que Φ mapea a en b y que Φ mapea A en B.
El elemento b es la imagen de a bajo Φ.
El hecho de que Φ mapea A en B se expresa simbólicamente como:

$$\Phi: A \rightarrow B.$$

Def. Si Φ y ψ son funciones con Φ: A $\to$ B y Ψ: B $\to$ C, existe un mapeo natural de A en C, usando las funciones Φ y Ψ.

Esta función mapeo de A en C es la función composición Φ seguida de Ψ. Si $\Phi(a) = b$ y $\Psi(b) = c$, $\Psi(\Phi(a)) = c$ es la composición de las funciones Φ y Ψ.

Def. Una función Φ de un conjunto A en un conjunto B es "uno a uno" o inyectiva, si para cualesquiera dos elementos $x \neq y$ en A, tenemos $\Phi(x) \neq \Phi(y)$.

Def. Una función Φ de un conjunto A en un conjunto B es suprayectiva o sobre, si $\forall\, b \in B$, $\exists\, a \in A$, tal que $\Phi(a) = b$.

Def. Una función Φ de un conjunto A en un conjunto B es biyectiva si es inyectiva y suprayectiva.

Def. Una permutación de un conjunto A es una función biyectiva de A en A.

En el conjunto de todas las permutaciones de un conjunto A se puede definir, en forma natural, una operación binaria.

Sea A un conjunto y sean Φ y Ψ dos permutaciones de A. La composición de funciones $\Phi(\Psi)$ es una función de A en A que es biyectiva.

El siguiente teorema muestra que el conjunto de todas las permutaciones de un conjunto no vacío A, forma un grupo con la composición de funciones.

Tma. 12. Sea A un conjunto no vacío. Sea S_A el conjunto de todas las permutaciones de A. Entonces S_A es un grupo con la composición de funciones.

Def. Si A es un conjunto finito, $\{1, 2, \ldots, n\}$, el grupo de todas las permutaciones de A se conoce como el grupo simétrico en n elementos y se denota por S_n y $|S_n| = n!$.

Ejemplo:

13. Consideremos S_3. Sea $A = \{1, 2, 3\}$. $|S| = 3! = 6$.

Los elementos de S_3 son:

$$ro = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad mo = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad m_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad m_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

El producto de los elementos está contenido en la siguiente tabla:

*	ro	r1	r2	mo	m1	m2
ro	ro	r1	r2	mo	m1	m2
r1	r1	r2	ro	m2	mo	m1
r2	r2	ro	r1	m1	m2	mo
mo	mo	m1	m2	ro	r1	r2
m1	m1	m2	mo	r2	ro	r1
m2	m2	mo	m1	r1	r2	ro

Este es el grupo de orden más chico que no es abeliano.

Existe una correspondencia natural entre los elementos de S_3 y las formas en que dos copias de un triángulo equilátero con vértices 1, 2 y 3 pueden ponerse, de tal manera que uno cubra al otro. Las r_i denotan rotaciones y las m_i reflexiones respecto a las bisectrices de los ángulos. Este grupo se conoce como el grupo diédrico de orden 3 y se denota como D_3.

Def. Si $x, y \in \Gamma$, diremos que x y y son conjugados si $\exists\ a \in \Gamma$ tal que $axa^{-1} = y$. axa^{-1} es el conjugado de x por a.

La relación "*ser conjugado de*" es de equivalencia. Es decir, reflexiva, simétrica y transitiva e induce una partición del conjunto en clases ajenas cuya unión es el total.

La clase de conjugados que contiene a x es $[x] = \{axa^{-1} / a \in \Gamma\}$.

Se dice que x es autoconjugado si su clase de conjugados sólo consiste de él mismo, y x es central si $axa^{-1} = x$, $\forall\ a \in \Gamma$. Este comentario permite dar otra caracterización del centro $Z(\Gamma)$ del grupo Γ, como el conjunto de elementos autoconjugados de Γ.

Def. Sea Γ un grupo y H un subgrupo de Γ. El conjugado de H por x se define como:

$$x^{-1}Hx = \{x^{-1}hx \ / \ h \in H\}$$

Def. Sea Γ un grupo, H un subgrupo de Γ. Si $x, y \in \Gamma$ diremos que x es congruente con y, módulo H ($x \equiv y \bmod H$) si $xy^{-1} \in H$.

Tma. 14. $x \equiv y \bmod H$ es una relación de equivalencia.

Esta relación de equivalencia induce una partición de los elementos de Γ en clases de equivalencia que denotaremos por $\lfloor a \rfloor$.

$$\lfloor a \rfloor = \{x \in \Gamma \ / \ a \equiv x \bmod H\}.$$

Def. Si H es un subgrupo de Γ y $a \in \Gamma$, entonces $Ha = \{ha \ / \ h \in H\}$. Ha se conoce como la clase lateral derecha de H inducida por a. De manera análoga se define la clase lateral izquierda aH.

Tma. 15. Sea Γ un grupo y H un subgrupo de Γ, entonces las siguientes condiciones son equivalentes.

i). $x \equiv y \bmod H$ es una relación de equivalencia.
ii). $x^{-1}Hx \subset H$, $\forall\ x \in \Gamma$.
iii). $x^{-1}Hx = H$, $\forall\ x \in \Gamma$.
iv). $Hx = xH$, $\forall\ x \in \Gamma$.

Obsérvese que *iii)*. dice que todo conjugado de H es igual a H. *iv)* dice que toda clase lateral derecha también es una clase lateral izquierda y viceversa. Estas condiciones no se cumplen para todos los subgrupos de Γ, sino que el Teorema garantiza que todas son falsas o todas son verdaderas.
Un subgrupo H de Γ que satisface alguna (y de aquí todas) condición se conoce como subgrupo normal (o subgrupo autoconjugado) de Γ y se denota por $H \triangleleft \Gamma$.

Def. Un grupo es simple si sus únicos subgrupos normales son él y la identidad.

Las clases laterales derechas están relacionadas con las clases de equivalencia inducidas por "$x \equiv y$ mod H".

$$\lfloor a \rfloor = \{ x \in \Gamma \mid x \equiv a \text{ mod } H\} = \{x \in \Gamma \mid xa^{-1} \in H\}$$
$$= \{x \in \Gamma \mid xa^{-1} = h \in H\} = \{x \in \Gamma \mid x = ha \text{ p. a. } h \in H\}$$
$$= Ha.$$

Por lo tanto las clases de equivalencia mod **H** son precisamente las clases laterales derechas de **H** en Γ.
La descomposición inducida por esta relación de equivalencia tiene también la siguiente propiedad.

Tma. 16. Si Ha y Hb son dos clases de equivalencia no vacías de H en Γ, existe una biyección τ: $Ha \to Hb$.

Dem. Definimos τ: $Ha \to Hb$
$ha \to hb$.

Al trabajar con grupos finitos, este Teorema nos permite determinar cuántos elementos tiene cada clase de equivalencia. De hecho el Teorema dice que todas tienen la misma cardinalidad y para determinarla usaremos la cardinalidad del subgrupo **H**.
Como $He = H$, también **H** es una clase lateral derecha y es tal que tiene $|H|$ elementos. Así que todas las clases tienen $|H|$ elementos.

Denotemos por ξ el número de clases de equivalencia distintas de **H** en Γ, inducidas por $x \equiv y$ mod **H**.

Como $x \equiv y$ mod **H** es de equivalencia, sabemos que:

$$i). \bigcup_{a \in \Gamma} Ha = \Gamma$$

$$ii). \ Ha = Hb \text{ o } Ha \cap Hb = \emptyset.$$

Por lo tanto $|\Gamma| = \xi |H|$.

ξ se conoce como el índice de **H** en Γ y se denota como $i_\Gamma(H)$ o bien como $[\Gamma : H]$. En los sucesivo utilizaremos esta última notación.

Esta relación entre el orden de Γ y el orden de un subgrupo **H** de Γ se conoce como **Tma. de Lagrange** para subgrupos.

Tma. (Lagrange). 17. Sea Γ un grupo de orden finito n y H un subgrupo de Γ. Entonces $|H|$ divide a $|\Gamma|$, $|\Gamma| = \xi|H|$.

Sabemos que el centralizador de cada elemento $x \in \Gamma$, $C(x)$ es un subgrupo de Γ, en este caso el Tma. de Lagrange adopta una forma muy interesante que usaremos constantemente.

Tma. 18. $|\Gamma| = |C(x)||[x]|$. $[x]$ la clase de conjugación de x.

Este teorema asegura que el índice del centralizador de cualquier elemento $x \in \Gamma$ es igual a la cardinalidad de la clase de conjugados de x.

Dem. Sabemos que la clase de conjugados de $x \in \Gamma$, $[x]$, consiste de todos los elementos axa^{-1} con $a \in \Gamma$. $|[x]|$ mide el número de distintos axa^{-1}. La demostración hará ver que dos elementos en la misma clase lateral derecha de $C(x)$ en Γ da el mismo conjugado de x, mientras que dos elementos en distintas clases laterales derechas de $C(x)$ en Γ producen distintos conjugados de x.
De esta manera tenemos una correspondencia uno a uno entre conjugados de x y clases laterales derechas de $C(x)$.

Supongamos que y, $z \in \Gamma$, y, z en la misma clase lateral derecha de $C(x)$ en Γ.

$$\therefore\ y = nz \text{ donde } n \in C(x) \text{ y } nx = xn.$$

$$\therefore \text{ como } y^{-1} = (nz)^{-1} = z^{-1}n^{-1};\ y^{-1}xy = z^{-1}n^{-1}xnz = z^{-1}xz.$$

$\therefore$ y, z están en la misma clase de conjugación.

Si y, $z \in \Gamma$, pertenecen a distintas clases laterales de $C(x)$ en Γ, afirmamos que $y^{-1}xy \neq z^{-1}xz$.

Si no fuese éste el caso, de $y^{-1}xy = z^{-1}xz$, deduciríamos que $zy^{-1}x = xzy^{-1}$; lo que a su vez implicaría que $zy^{-1} \in C(x)$. Lo que afirma que y, z están en la misma clase lateral derecha de $C(x)$ en Γ.

!!! CONTRADICCION !!!

Def. Un elemento a de un grupo Γ con elemento identidad e tiene orden $r > 0$ si r es el mínimo entero tal que $a^r = e$.

Corolario. 19. Todo grupo de orden primo es cíclico.

Def. El orden de un elemento $\alpha \in \Gamma$ es el mínimo entero positivo tal que $\alpha^n = e$.

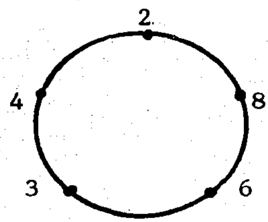
Corolario. 20. El orden de un elemento divide el orden del grupo.

Tma. 21. Si H y K son subgrupos de un grupo Γ tal que K es subgrupo de H y supongamos que $[H:K]$ y $[\Gamma:H]$ son finitos. Entonces $[\Gamma:K]$ es finito y $[\Gamma:K] = [\Gamma:H][H:K]$.

El papel que desempeñan las permutaciones es muy importante. Por ello ampliaremos un poco más sobre ellas.
Primero sobre la notación que usaremos para las permutaciones de un conjunto A.

Tomemos como ejemplo $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Supongamos que los cinco números 2, 4, 3, 6 y 8 se distribuyen sobre un círculo, como se muestra a continuación.



Supongamos ahora que el círculo se rota $2\pi/5$ radianes en sentido contrario a las manecillas del reloj. Así que 2 es movido a la posición que antes ocupaba el 4, el 4 a la que antes ocupaba el 3 y así sucesivamente. Sea τ la permutación en S_A que deja fijos al 1, al 5 y al 7 y que en los demás elementos hace justo lo descrito al rotar el círculo arriba.

Representemos las imágenes de esta función:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 6 & 3 & 5 & 8 & 7 & 2 \end{pmatrix}$$

Introducimos una notación más compacta para esta permutación:

$$\tau = (2,\ 4,\ 3,\ 6,\ 8)$$

Esta notación es la notación cíclica y significa, se puede empezar en cualquier elemento, que el 2 va al 4, el 4 al 3, el 3 al 6 el 6 al 8 y el 8 al 2, para cerrar el ciclo.
Los elementos que no aparecen en la permutación permanecen fijos.

Def. Una permutación τ de un conjunto **A** es un ciclo de longitud n, si existen $a_1, a_2, \dots, a_n \in$ **A** tales que:
$\tau(a_1) = a_2$, $\tau(a_2) = a_3, \dots, \tau(a_{n-1}) = a_n$ y $\tau(a_n) = a_1$, y $\tau(x) = x$ $\forall\ x \in$ **A**, pero $x \neq a_1, a_2, \dots, a_n$.

En el círculo arriba, τ es un ciclo de longitud 5.

Los ciclos son un tipo especial de permutaciones y pueden multiplicarse como ellas, pero su producto no necesariamente es un ciclo.

Una colección de ciclos se dice ajena, si ningún elemento de **A** es movido por dos ciclos distintos de la colección. Acordamos que cualquier ciclo de longitud uno es la identidad.

Tma. 22. Toda permutación es el producto de ciclos ajenos. Además esta representación es única salvo el orden de los factores.

Def. Un ciclo de longitud 2 es una transposición.

El número de transposiciones necesarias para representar una permutación dada siempre es par o impar.

Def. Una permutación de un conjunto finito es par (o impar) si el número necesario de transposiciones para expresarla como un producto de éstas es par (o impar).

Tma. 23. Si $n \geq 2$, el conjunto de todas las permutaciones pares de $\{1, 2, \ldots, n\}$ forma un subgrupo del grupo simétrico S_n. A este grupo se le conoce como el grupo alternante A_n en n elementos.

$$|A_n| = \frac{n!}{2}.$$

Ejemplos.

24. Ya hemos hablado de D_3, el grupo diédrico en 3 elementos. Examinaremos ahora el caso general. El grupo diédrico en n elementos se puede visualizar de la siguiente forma: Tomemos 2 n-ágonos regulares y fijémonos en las formas como se pueden poner los vértices de tal manera que un n-ágono cubra al otro.
El grupo diédrico de orden n, D_n, es el grupo de simetrías de un n-ágono regular.

Para $n \geq 3$, consideremos un n-ágono. ρ representa una rotación de $2\Pi/n$ radianes en sentido contrario a las manecillas del reloj alrededor de su centro. Las n rotaciones son:

$$\rho,\ \rho^2,\ \ldots,\ \rho^n = e \text{ (identidad).}$$

Si n es impar, hay n ejes de simetría que pasan cada uno por un vértice y por el punto medio del lado opuesto. Si pensamos en el n-ágono en un espacio tridimensional, podemos rotarlo (reflexión) Π radianes alrededor de cada uno de estos ejes. Así que las figuras inicial y final son idénticas.

Obsérvese que ninguna reflexión puede obtenerse por medio de una rotación, pues una reflexión invierte el orden de los vértices, mientras que una rotación no.

Si n es par, hay n ejes de simetría que pasan por pares de vértices opuestos y n ejes de simetría que pasan por pares de puntos medios situados en lados opuestos.

En cualquier caso, el grupo D_n de simetrías del n-ágono tiene orden $2n$. El conjunto $\langle\rho\rangle = \{e, \rho, \rho^2, \ldots, \rho^{n-1}\}$ de las rotaciones es un subgrupo de orden n, normal en D_n. Todos los otros n elementos de D_n tienen orden 2. Sea m uno de ellos. Si $m\rho \in \langle\rho\rangle$, digamos $m\rho = \rho^i$, entonces $m = \rho^{i-1} \in \langle\rho\rangle$, lo cual es una contradicción. Por lo tanto $m\rho \in D_n - \langle\rho\rangle$, lo que forza a $m\rho$ a tener orden 2. La ecuación $(m\rho)^2 = e$ implica $e = m\rho m\rho$, $\rho^{-1} = m\rho m$. Como $m = m^{-1}$, podemos escribir esta última como $\rho^{-1} = m\rho m^{-1}$.

Como el subgrupo $\langle\rho\rangle$ tiene índice 2, sólo tiene dos clases laterales, $\langle\rho\rangle$ y $m\langle\rho\rangle$ en D_n; por lo tanto:

$$D_n = \{e, \rho, \rho^2, \ldots, \rho^{n-1}, m, m\rho, \ldots, m\rho^{n-1}\}$$

Las ecuaciones:

$$\rho^n = e, \; m^2 = e, \; m^{-1}\rho m = \rho^{-1}$$

se conocen como relaciones del grupo D_n, ya que cualquier multiplicación en D_n puede efectuarse utilizando estas ecuaciones, por ejemplo:

$m^{-1}\rho m = \rho^{-1}$ implica $\rho m = m\rho^{-1}$, así que podemos multiplicar fácilmente, por ejemplo:

$$(m\rho)(m\rho^2) = m(\rho m)\rho^2 = m(m\rho^{-1})\rho^2 = m^2\rho = \rho.$$

O bien, $(m\rho^3)m = (m\rho^2)(\rho m) = (m\rho^2)(m\rho^{-1}) = (m\rho)(\rho m)\rho^{-1} =$
$(m\rho)(m\rho^{-1})\rho^{-1} = m(\rho m)\rho^{-2} = m(m\rho^{-1})\rho^{-2} = m^2\rho^{-3} = \rho^{-3}.$

El número de clases de conjugación es:

Si n es impar, $\dfrac{n+3}{2}$ y si n es par, $\dfrac{n}{2} + 3$.

Estas clases son:

Para n impar, $n = 2k - 1$: $D_n = [e] \cup [\rho] \cup [\rho^2] \cup \ldots \cup [\rho^{k-1}] \cup [m]$

y para n par, $n = 2k$: $D_n = [e] \cup [\rho] \cup \ldots \cup [\rho^k] \cup [m] \cup [m\rho]$.

25. Consideremos $A = \{1, -1, i, -i\}$ con el producto en los números complejos.

Este es un grupo cíclico de orden 4. Si calculamos las clases de conjugación de cada elemento, obtenemos que cada uno es autoconjugado, esto es todos los elementos son centrales.
Por lo tanto el grupo es abeliano. Y todos sus subgrupos son normales.
Este grupo contiene un subgrupo de orden 2, $\langle -1\rangle$.

Este grupo nos permitirá introducir un concepto al comparar su tabla con Z_4, ver Ejemplo 4.

$\ast$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

La idea del concepto es que son estructuralmente idénticos salvo el "*nombre*" de los elementos y de las operaciones. Así que debiéramos poder obtener **A** de $\mathbb{Z}_4$ al "*cambiar de nombre*" un elemento x de **A** por el nombre de un elemento x' de $\mathbb{Z}_4$. Esto es, a cada $x \in$ **A** se le asigna un elemento de $\mathbb{Z}_4$, lo cual no es sino una función Φ: **A** $\rightarrow \mathbb{Z}_4$.
Claramente dos elementos distintos x, y en **A** deben tener imágenes distintas en $\mathbb{Z}_4$, esto significa que Φ debe ser inyectiva.

También todo elemento de $\mathbb{Z}_4$ debe ser la imagen de algún elemento de A, esto es Φ debe ser suprayectiva. Esto cambia los nombres de los elementos.

Ahora, si los grupos deben ser idénticos estructuralmente y si por el momento denotamos la operación de grupo de **A** por $*$ y la de $\mathbb{Z}_4$ por $\ast$, entonces la imagen de $x*y$ debe ser $x' \ast y'$, o $\Phi(x*y)$ debe ser $\Phi(x) \ast \Phi(y)$. En general eliminamos los símbolos $*$ y $\ast$ para las operaciones, obteniendo:

$$\Phi(xy) = \Phi(x)\Phi(y).$$

Nótese que la operación en el lado izquierdo es en **A**, mientras que la del lado derecho es en $\mathbb{Z}_4$.

Resumimos todas estas ideas:

Def. Un isomorfismo de un grupo Γ con un grupo Δ es una función biyectiva $\Phi: \Gamma \rightarrow \Delta$, tal que $\forall\ x, y \in \Gamma$, $\Phi(xy) = \Phi(x)\Phi(y)$.

Def. Si existe un isomorfismo entre dos grupos Γ y Δ, decimos que son isomorfos y lo denotamos como $\Gamma \cong \Delta$.

Tma. 28. Si $\Phi: \Gamma \rightarrow \Delta$ es un isomorfismo de grupos y e es la identidad de Γ, entonces $\Phi(e)$ es la identidad en Δ, también: $\Phi(a^{-1}) = (\Phi(a))^{-1}$, $\forall\ a \in \Gamma$.

El Teorema indica que todo isomorfismo mapea la identidad en la identidad e inversos en inversos.

Son claros los pasos que hay que seguir para mostrar que dos grupos son isomorfos, sin embargo comentaremos brevemente cómo demostrar que dos grupos Γ y Δ no son isomorfos, si es el caso.

Que dos grupos Γ y Δ no sean isomorfos significa que no existe ninguna función biyectiva Φ: $\Gamma \to \Delta$ con la propiedad:

$$\Phi(xy) = \Phi(x)\Phi(y).$$

En general, probar esto es *inaccesible*, excepto en el caso cuando no hay funciones biyectivas. Este es el caso, si por *ejemplo*. Γ y Δ tienen distinta cardinalidad.

Ejemplos:

27. $\mathbb{Z}_5$ y $\mathbb{Z}_{19}$ no son isomorfos, pues no existe ninguna biyección de $\mathbb{Z}_5$ en $\mathbb{Z}_{19}$.

28. $\mathbb{Z}$ con la suma no es isomorfo a $\mathbb{R}$ con la suma, pues no existe ninguna biyección de $\mathbb{Z}$ en $\mathbb{R}$.

Suponiendo que se tengan biyecciones entre los dos grupos, uno demuestra *que* no son isomorfos (si es el caso), exhibiendo una propiedad estructural que un grupo tiene y el otro no. Una propiedad estructural de un grupo es una propiedad que debe tener todo grupo isomorfo y que no depende del "*nombre*" de los elementos o de alguna otra característica no estructural de ellos.

A continuación se *mencionan* algunas propiedades estructurales y algunas no estructurales de grupos.

Estructurales

1. Γ es cíclico.
2. Γ es abeliano.
3. $|\Gamma| = 10$.
4. Γ es finito.
5. Γ tiene exactamente dos elementos de orden 5.
6. $x^4 = a$ tiene una unica solución para cada $a \in \Gamma$.

No estructurales.

1. Γ contiene al 5.
2. Los elementos de Γ son números.
3. La operación de Γ es la suma.
4. Los elementos de Γ son permutaciones.
5. La operación en Γ es yuxtaponer los elementos.
6. Γ es un subgrupo de $(\mathbb{R}, +)$.

Desde luego hay muchas más propiedades que se pueden mencionar.

Ejemplos:

29. $\mathbb{Z}$ y $\mathbb{Q}$ ambos con la suma no son isomorfos, porque $\mathbb{Z}$ es cíclico y $\mathbb{Q}$, no.

30. $\mathbb{R} - \{0\}$ con la multiplicación no es isomorfo al grupo $\mathbb{C} - \{0\}$ con la multiplicación ya que la ecuación $x^2 = a$ tiene una solución $x \in \mathbb{C} - \{0\}$ $\forall\ a \in \mathbb{C} - \{0\}$, mientras que $x^2 = -1$ no tiene solución en $\mathbb{R} - \{0\}$.

31. $\mathbb{R} - \{0\}$ con la multiplicación no es isomorfo a $\mathbb{R}$ con la suma pues la ecuación $x + x = a$ siempre tiene solución en $\mathbb{R}$, $\forall\ a \in \mathbb{R}$, pero la correspondiente ecuación $x\ x = a$ no siempre tiene solucion en $\mathbb{R} - \{0\}$, por ejemplo si $a = -3$.

Producto directo externo de grupos.

Def. Sean $\Gamma_1, \Gamma_2, \ldots, \Gamma_n$ grupos. Si $(a_1, a_2, \ldots, a_n)$ y $(b_1, b_2, \ldots b_n)$ pertenecen a $\prod_{i=1}^{n} \Gamma_i$, definimos

$$(a_1, a_2, \ldots a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

Tma. 32. $\prod_{i=1}^{n} \Gamma_i$ es un grupo, el producto directo de los grupos Γ_i, con la operación definida arriba.

En caso de que cada Γ_i sea abeliano, se usa la notación aditiva en $\prod_{i=1}^{n} \Gamma_i$ y nos referimos a éste como la suma externa directa de los grupos Γ_i. En este caso se usa la notación $\bigoplus_{i=1}^{n} \Gamma_i$.

La suma directa de grupos abelianos puede escribirse como:

$$\Gamma_1 \oplus \Gamma_2 \oplus \ldots \oplus \Gamma_n.$$

Ejemplos:

33. El grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ tiene 6 elementos:
$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$. Es cíclico y $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$.

34. $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ no es isomorfo a $\mathbb{Z}_9$, pues el primero no es cíclico. Lo mismo ocurre con $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ y $\mathbb{Z}_4$. Así que del ejemplo **4**: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong V$.

CAPITULO II. TEORIA DE GRAFICAS.

"LO QUE MAS NOS SORPRENDE A TODOS, CUANDO COMPARAMOS LA MATEMATICA DE NUESTRO TIEMPO CON LA DE LAS EPOCAS ANTERIORES, ES LA EXTRAORDINARIA DIVERSIDAD Y LO INESPERADO DE LA TRAYECTORIA QUE HA TOMADO; EL APARENTE DESORDEN CON QUE EJECUTA SU MARCHA, SUS MANIOBRAS Y CONSTANTES CAMBIOS DE DIRECCION".

Pierre Boutrox.

Una gráfica es un concepto simple ejemplificado en muchas formas familiares; la telaraña de una araña, el mapa de carreteras de un país, las rutas de una compañía aérea, las conexiones en un sistema de telecomunicaciones.

La teoría de gráficas ha sido de gran interés para los matemáticos por las propiedades intrínsecas de las gráficas por una parte y por otra debido a su importancia en las aplicaciones a problemas prácticos en la industria, la administración y en las ciencias sociales. A esta rama de aplicación se le conoce como investigación de operaciones.

La teoría de gráficas en sí misma es elegante y una amplia variedad de problemas prácticos puede formularse en términos de una gráfica para las cuales las técnicas están bien estructuradas para cálculos computacionales. Es en suma una herramienta matemática muy atractiva que ha demostrado ser muy útil.

Def. Una gráfica G consiste de un conjunto no vacío V = V(G) de puntos junto con un subconjunto E = E(G) del conjunto de pares no ordenados de V(G).

Def. Los elementos de V(G) son los vértices de la gráfica G y los elementos de E(G) son las aristas de la gráfica G. La gráfica es finita si V(G) y E(G) son conjuntos finitos y es infinita en cualquier otro caso. En el presente trabajo sólo trataremos con gráficas finitas. De ahora en adelante, la palabra "gráfica" significa siempre una gráfica finita.

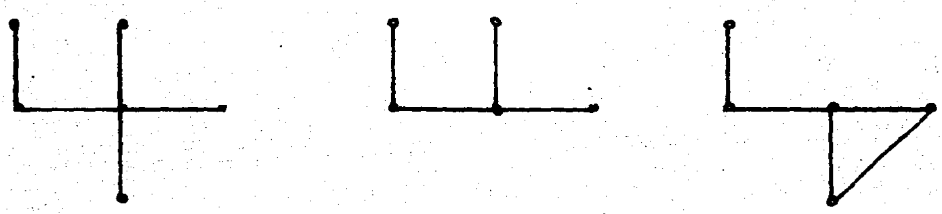
Def. Si $E_1 = \{u, v\}$ es un elemento de E(G), diremos que u y v son vértices adyacentes de G, que E_1 une u y v, y que u (o v) y la arista E_1 son incidentes.

Si las aristas E_1 y E_2 inciden en un vértice común, nos referiremos a ellas como aristas adyacentes.

Se acostumbra representar una gráfica G mediante un diagrama en el que cada vértice se muestra como un pequeño circulito y a cada arista como una línea que une los dos circulitos que representan sus extremos.

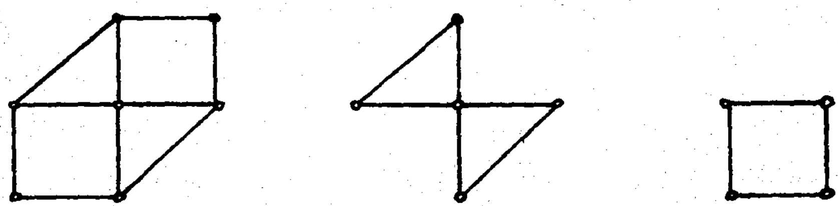
Según nuestra definición de gráfica, no es posible que en una gráfica, dos o más aristas unan un mismo par de vértices (es decir que tenga aristas múltiples), ni que una arista una un vértice consigo mismo (es decir que tenga lazos). Algunos autores las llaman simples.

Def. Una subgráfica H de una gráfica G es una gráfica en la que $V(H) \subseteq V(G)$ y $E(H) \subseteq E(G)$.



Una grafica y dos de sus subgraficas.

Def. Para cualquier conjunto $S \subseteq V(G)$, la subgráfica inducida $\langle S \rangle$ es la subgráfica maximal H de G tal que $V(H) = S$. Así que dos punpuntos de S son adyacentes en $\langle S \rangle$ si y sólo si son adyacentes en G.



Una grafica y dos subgraficas inducidas.

Def. Si de una gráfica G, eliminamos un vértice v_i, se obtiene una subgráfica $G - \{v_i\}$ que consiste de todos los vértices en $G - \{v_i\}$ y todas las aristas que no inciden en v_i. Así que $G - \{v_i\}$ es una subgráfica maximal de G que no contiene a v_i.

Una gráfica puede tener distintas propiedades. Una de ellas es la de ser conexa. Para introducir este concepto necesitaremos de algunas definiciones más.

Def. Un camino de una gráfica G es una sucesión alternada de vértices y aristas v_0, E_0, v_1, $E_1, \ldots, E_{n-1}$, v_n con vértices inicial v_0 y final v_n. El camino es cerrado si $v_0 = v_n$ y abierto en caso contrario.

Es un paseo si las aristas son distintas y una trayectoria si los vértices son distintos (y de aquí las aristas). Si el paseo es cerrado, entonces es un ciclo si sus n vértices son distintos y $n \geq 3$. n es la longitud del ciclo.
Denotamos por C_n la gráfica que consiste de un ciclo con n vértices. C_3 se conoce como un triángulo.

Def. Una gráfica es conexa si para todo par de vértices de G, existe una trayectoria que los une. La relación definida por $u \mathcal{R} v$ si y sólo si $\exists$ una trayectoria en G que los une es de equivalencia e induce una partición de G en clases ajenas. A cada clase se le conoce como componente conexa de G o simplemente una componente de G.
Por lo tanto, una gráfica disconexa tiene al menos dos componentes.

Def. La valencia (o grado) de un vértice $v \in G$, denotado como $\mathrm{val}(v)$ es el número de aristas incidentes en él.

Ya que toda arista incide en dos vértices, contribuye en 2 a la suma de los grados de los vértices. Este primer resultado, se debe a Euler, y fue el primer teorema de la teoría de gráficas.

Tma.1. La suma de los grados de los vértices de una gráfica G es dos veces el número de las aristas.

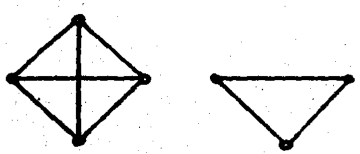
$$\sum_{v \in G} \mathrm{val}\ v = 2|E(G)|.$$

Corolario 2. En cualquier gráfica G, el número de vértices de grado impar es par.

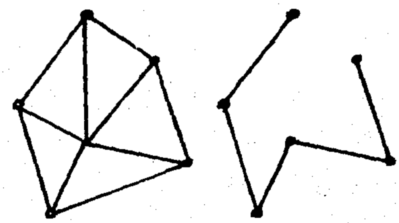
Def. Si en la gráfica G todos los vértices tienen la misma valencia, digamos r, G se conoce como regular de grado r.
Una gráfica regular de grado 0 no tiene aristas. Si G es regular de grado 1, cada componente tiene exactamente una arista. Si es regular de grado 2, toda componente es un ciclo y recíprocamente.

Las primeras gráficas regulares interesantes son las de grado 3. Tales gráficas se conocen como cúbicas.

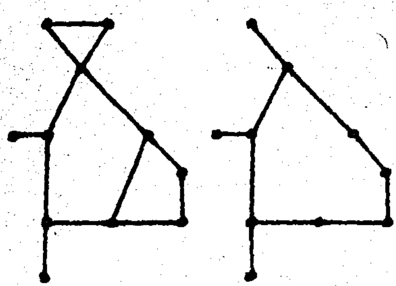
Corolario 3. Toda gráfica cúbica tiene un número par de vértices.



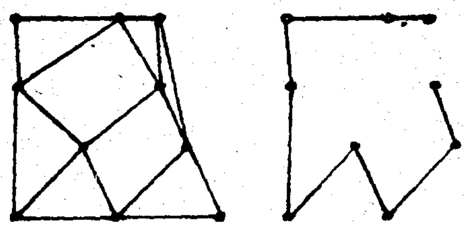
Una grafica y un ciclo.



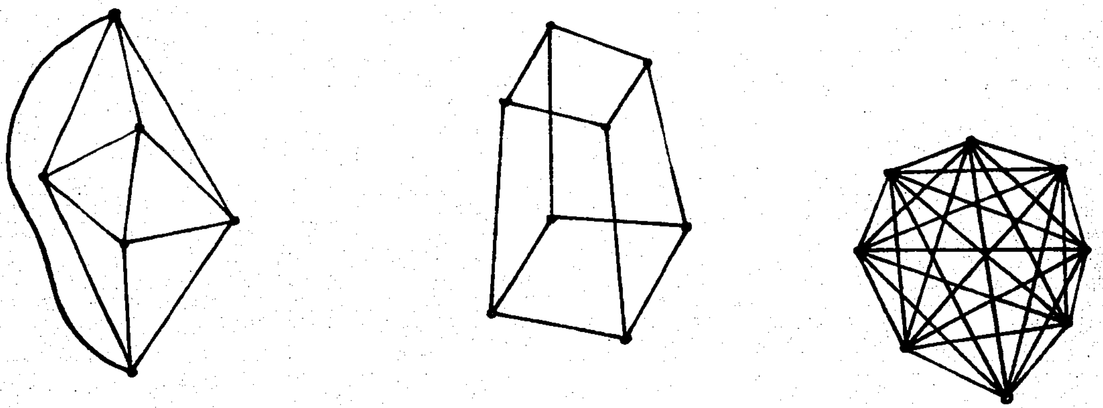
Una grafica y una trayectoria.



Una grafica y un camino.



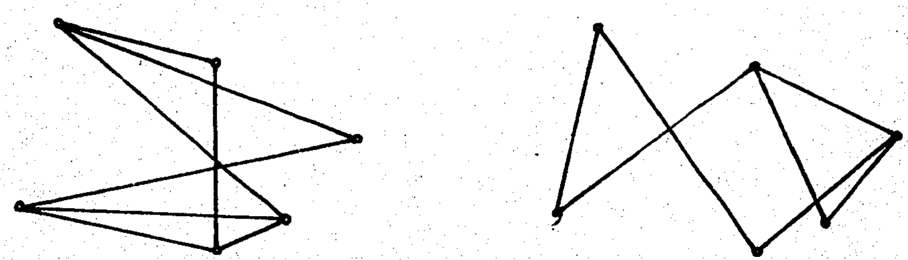
Una grafica y un paseo.



Algunas graficas regulares.

Def. El complemento G^c de una gráfica G tiene vértices V(G) y en la que dos vértices son adyacentes si y sólo si no son adyacentes en G.

Def. La gráfica completa K_n tiene n vértices y $\frac{n(n-1)}{2}$ aristas y es regular de grado (n - 1). K_3 es el triángulo (C_3). Las gráficas K_n^c son totalmente disconexas y 0 - regulares.

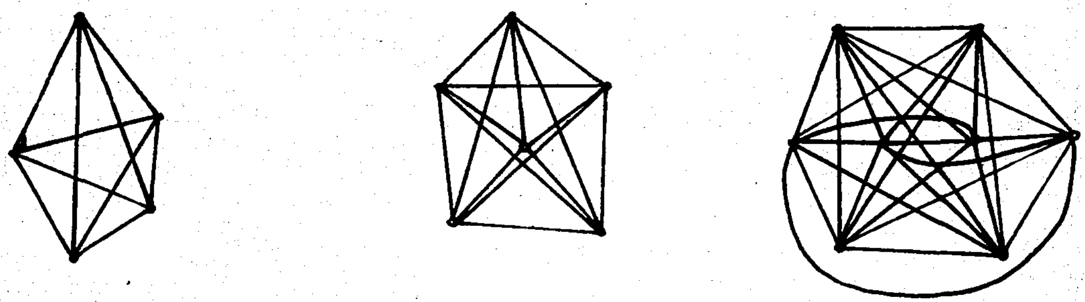


Una grafica G y su complemento G^c

Def. Una gráfica bipartita G es una gráfica cuyo conjunto de vértices V(G) puede partirse en 2 subconjuntos V_1 y V_2 tal que toda arista de G une V_1 con V_2.

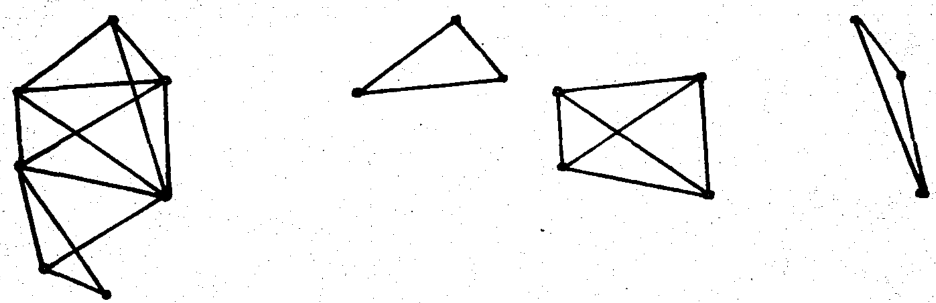
Def, Si G contiene todas las aristas que unen V_1 y V_2, entonces G es una gráfica completa. Si V_1 y V_2 tienen m y n vértices respectivamente, escribimos $G = K_{m,n} = K(m, n)$. $K_{m,n}$ tiene mn aristas.

Una estrella es una gráfica completa $K_{1,n}$.



Algunas graficas completas.

Def. Un clan de una gráfica es una subgráfica maximal completa.



Una grafica y algunos de sus clanes.

Def. Un conjunto de vértices de G es independiente si ningun par de ellos es adyacente. La cardinalidad máxima de uno de estos conjuntos es el número de independencia de G y se denota como $\alpha(G)$.

S es un clan de G si y sólo si S es un conjunto independiente de G^c.

El Teorema de Ramsey.

Si G no tiene clanes "grandes", uno pudiera esperar que tuviera un conjunto independiente "grande". Este resultado es cierto y fué demostrado por Ramsey en *1930*.

Ramsey demostró que dados cualesquiera dos enteros positivos k y l, $\exists$ un entero mínimo positivo $R(k, l)$ tal que toda gráfica con $R(k, l)$ vértices contiene un clan de k vértices o un conjunto independiente de l vértices. Por ejemplo, $R(1, l) = R(k, 1) = 1$ y $R(2, l) = l$, $R(k, 2) = k$.

Los números $R(k, l)$ se conocen como números de Ramsey. El siguiente Teorema sobre los números de Ramsey se debe a Erdös y Szekeres (*1935*) y a Greenwood y Gleason (*1955*).

Tma. 4. Para cualesquiera dos enteros $k \geq 2$ y $l \geq 2$:

$$R(k, l) \leq R(k, l - 1) + R(k - 1, l).$$

Además, si $R(k, l - 1)$ y $R(k - 1, l)$ son pares, entonces se satisface la desigualdad estricta.

Dem. Sea G un gráfica con $R(k, l - 1) + R(k - 1, l)$ vértices. Sea $v \in V(G)$.

1er. *caso*. v no es adyacente a un conjunto S con al menos $R(k, l - 1)$ vértices o,

2o. *caso*. v es adyacente a un conjunto T con al menos $R(k - 1, l)$ vértices.

Alguno de estos casos se debe cumplir ya que el número de vértices no adyacentes a v más el número de vértices adyacentes a v es $R(k, l - 1) + R(k - 1, l) - 1$.

En el primer caso, la subgráfica inducida por $G - \{S\}$ contiene o un clan de k vértices o un conjunto independiente de $l - 1$ vértices y por lo tanto la subgráfica inducida por $G - \{S \cup \{v\}\}$

contiene o un clan de k vértices o un conjunto independiente de l vértices.

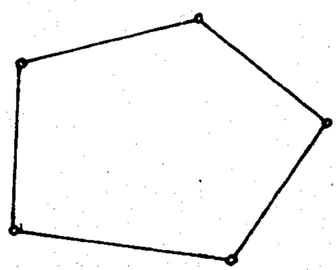
Si ocurre el caso 2, la subgráfica inducida por $G - \{T \cup \{v\}\}$ contiene o un clan de k vértices o un conjunto independiente de l vértices. Como alguno de los dos casos ocurre, G contiene o un clan de k vértices o un conjunto independiente de l vértices, lo cual prueba la primera parte del Teorema.

Supongamos ahora que $R(k, l - 1)$ y $R(k - 1, l)$ son pares y sea G una gráfica con $R(k, l - 1) + R(k - 1, l) - 1$ vértices. Como G tiene un número impar de vértices, del Corolario 2, G tiene algún vértice v de grado par. En particular v no puede ser adyacente justamente a $R(k - 1, l) - 1$ vértices. Por lo tanto, el primer caso o el segundo caso se cumple y consecuentemente G contiene o un ciclo de k vértices o un conjunto independiente de l vértices.

Por lo tanto $R(k, l) \leq R(k, l - 1) + R(k - 1, l) - 1$.

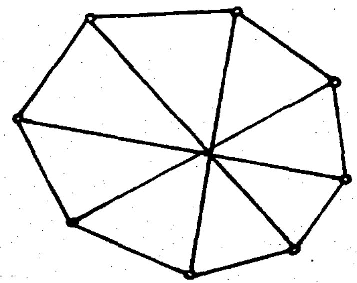
Determinar los números de Ramsey en general es un problema bastante difícil. Cotas inferiores pueden obtenerse al construir ciertas gráficas adecuadas.

Consideremos el ciclo de longitud 5. C_5 no contiene clanes de 3 vértices, ni conjuntos independientes de 3 vértices. Esto demuestra que $R(3, 3) \geq 6$.

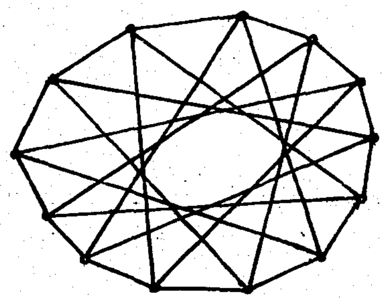


C_5 DEMUESTRA QUE $R(3, 3) > 5$.

La siguiente gráfica no contiene clanes de 3 vértices, ni conjuntos independentes de 4 vértices, por lo tanto $R(3, 4) \geq 9$.



La siguiente gráfica muestra que $R(3, 5) \geq 14$.



Mediante el Tma. 4 y las igualdades $R(2, l) = l$, $R(k, 2) = k$ se puede demostrar que la igualdad ocurre en los tres ejemplos anteriores.

Combinando el Tma. 4 y las dos igualdades se tiene:

$$6 \leq R(3, 3) \leq R(3, 2) + R(2, 3) = 6$$

$$\therefore \quad R(3, 3) = 6.$$

Como $R(3, 3)$ y $R(2, 4)$ son pares, aplicamos el Tma. 4 y obtenemos

$$9 \leq R(3, 4) \leq R(3, 3) + R(2, 4) - 1 = 9.$$

De nuevo del Tma. 4, $14 \leq R(3, 5) \leq R(3, 4) + R(2, 5) = 14$.

Def. Una coloración de una gráfica es una asignación de colores a sus vértices de tal manera que ningun par de vértices adyacentes tiene el mismo color. Una n - coloración de una gráfica G usa n colores; es decir parte $V(G)$ en n subconjuntos ajenos. El número cromático $\chi(G)$ se define como el mínimo n para el cual G tiene una n - coloración. Una gráfica es n - coloreable si $\chi(G) \leq n$.

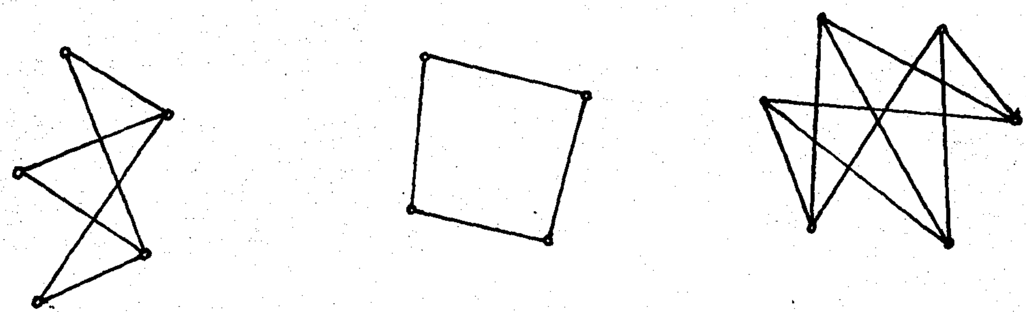
Corolario 5. Si G es n - coloreable entonces todo clan de G tiene cardinalidad $\leq n$.

Los números cromáticos de algunas gráficas ya mencionadas se pueden determinar fácilmente, por ejemplo:

$$\chi(K_n) = n; \quad \chi(K_n^c) = 1; \quad \chi(K_{m,n}) = 2; \quad \chi(C_{2n}) = 2; \quad \chi(C_{2n+1}) = 3.$$

Tma. 6. Una gráfica es bicoloreable si y sólo si no tiene ciclos impares.

Corolario 7. Una gráfica es bipartita si y sólo si todos sus ciclos son pares.



Algunas graficas bipartitas.

Tma. 8. Sea $(S_1, S_2, \ldots, S_q)$ una q-coloración (no necesariamente mínima de una gráfica simple G, y sea $d_k = \max_{v \in S_k} \{\mathrm{val}(v)\}$.

Entonces $\chi(G) \leq \max_{k \leq q} \min \{k, d_k + 1\}$.

Dem. 1. Si S_1 no es un conjunto independiente máximo, añadimos vértices a S_1 para obtener un conjunto independiente máximo S_1'. Si $S_2 - S_1'$ no es un conjunto independiente máximo en $V(G) - S_1'$, entonces añadimos vértices para formar un conjunto independiente máximo S_2' en $V(G) - S_1'$, etc. Este proceso define una nueva coloración $(S_1', S_2', \ldots, S_r')$ con

$$\bigcup_{i=1}^{\min(k,r)} S_i' \supset S_k \quad (k = 1, 2, \ldots, q)$$

2. Sea $i(v)$ el índice i tal que $v \in S_i'$. Sea v_0 un vértice con $i(v_0) = k$; como v_0 es adyacente a cada S_j' con $j \leq k - 1$ (por la maximalidad de S_j'), entonces:

$$\mathrm{val}(v_0) \geq k - 1.$$

$$\therefore \forall\, v \in V(G),\ i(v) \leq \mathrm{val}(v) + 1.$$

3. Sea $v_0 \in S_k$. De la parte 1, tenemos $i(v_0) \leq k$, y consecuentemente, $i(v_0) \leq \max\limits_{v \in S_k} i(v) \leq \max\limits_{v \in S_k} \{\mathrm{val}(v) + 1\} = d_k + 1$.

$$\therefore \quad \chi(G) \leq \max_{v_0} i(v_0) \leq \max_{k \leq q} \min\{k, d_k + 1\}.$$

Corolario 9. Sea G una gráfica simple. Si para algún entero q, el número de vértices de grado $\geq q$ es $\leq q$, entonces G es q-coloreable.

Dem. Supongamos que los vértices v_i están indicados con grados decrecientes.

Consideremos la n-coloración:

$$\left[\{v_1\},\ \{v_2\}, \ldots, \{v_n\}\right].$$

Entonces $d_k = \mathrm{val}(v_k)$.

Si $k \leq q$ tenemos $\min\{d_k + 1, k\} \leq q$.

Si $k \geq q + 1$, tenemos:

$$\min\{dk + 1,\ k\} \leq \min\{dq + 1,\ k\} \leq \min\ \{q,\ k\} \leq q.$$

Entonces del Tma. 8, $\chi(G) \leq q$.

El siguiente Teorema relaciona el número de independencia de una gráfica y el grado de sus vértices. Este Teorema fué demostrado por V. K. Wei en *1980* [*22*]. La técnica consiste en quitar un vértice v_0 de grado mínimo, los vértices adyacentes a v_0 y las aristas incidentes con alguno de estos vértices. La siguiente demostración que consiste en quitar un vértice de grado máximo y las aristas incidentes en él aparece en [*3*].

Tma. 10. Sea G una gráfica, $\alpha(G)$ el número de independencia de G.

Entonces

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{1 + \mathrm{val}(v)}.$$

La igualdad se cumple si y sólo si G es unión de clanes ajenos.

Dem. Sea v_0 un vértice de grado máximo en G, es decir,

$$\mathrm{val}(v_0) \geq \mathrm{val}(v),\ \forall\ v \in G.$$

Sea $G^{=}$ la subgráfica $G - \{v_0\}$.

La desigualdad se cumple si G no tiene aristas o bien si sólo tiene dos vértices, pues en el primer caso $|V(G)| = n$, $\mathrm{val}(v) = 0$, $\forall\ v \in V(G)$ y $\alpha(G) = n$.

$$\sum_{v \in V(G)} \frac{1}{1 + \mathrm{val}(v)} = n = \alpha(G).$$

Si G tiene dos vértices u, v, podemos suponer que $\exists$ E $\in$ (G) tal que E es incidente en u y v.

Por lo tanto $|V(G)| = 2$, $\mathrm{val}(v) = 1$, $\forall\ v \in G$ y $\alpha(G) = 1$.

$$\sum_{v \in V(G)} \frac{1}{1 + \mathrm{val}(v)} = 2\,\frac{1}{2} = 1 = \alpha(G).$$

Denotemos por $\mathrm{val}^{-}(v)$ el grado de $v \in V(G^{-})$.

Si $v \in G$, $\mathrm{val}(v) = \mathrm{val}^{-}(v)$ si v y v_0 no son adyacentes en G, mientras que $\mathrm{val}(v) = \mathrm{val}^{-}(v) + 1$ si v y v_0 son adyacentes en G.

Observación. $\alpha(G^{-}) \leq \alpha(G) \leq \alpha(G^{-}) + 1$.

Dem. Sea $X \subseteq V(G)$ un conjunto independiente máximo. Supongamos $|X| = \alpha(G)$.

Nota. Siempre tenemos $\forall\ v \in V(G - X)$ $\exists\ x_i \in V(G)$ tal que $\{v, x_i\} \in E(G)$. Si no fuera el caso: $\exists\ v_i \in V(G - X)\ \forall\ x \in X$ tal que $\{v_i, x\} \notin E(G)$ y por tanto $X \cup \{v_i\}$ sería independiente y $X \subset X \cup \{v_i\}$, $\therefore$ X no sería máximo, lo cual es una contradicción.

a). Si $v_0 \in X$, entonces $X - \{v_0\}$ es independiente en G^{-}.

$$\therefore\ \alpha(G^{-}) \geq |X - \{v_0\}| = |X| - 1 = \alpha(G) - 1.$$

$$\therefore\ \alpha(G^{-}) + 1 \geq \alpha(G).$$

b). Si $v_0 \notin X$, por la nota precedente, X también es independiente máximo en G^{-}, por lo tanto:

$$\alpha(G^{-}) \leq |X| = \alpha(G).$$

De a) y b), $\alpha(G^{-}) \leq \alpha(G) \leq \alpha(G^{-}) + 1$.

En el caso de que $\alpha(G) = \alpha(G^{-}) + 1$, se demuestra por inducción sobre $\alpha(G^{-})$ y usando el hecho de que

$$1 > \frac{1}{1 + \mathrm{val}(v_0)}$$

que $\alpha(G) > \displaystyle\sum_{v \in V(G)} \frac{1}{1 + \mathrm{val}(v)}$.

Para obtener el caso de la igualdad se necesita el siguiente hecho que siempre sucede:

$$\sum_{v \in V(G^{-})} \frac{1}{1 + \mathrm{val}^{-}(v)} \geq \sum_{v \in V(G)} \frac{1}{1 + \mathrm{val}(v)} .$$

Para aclarar este punto, nótese que,

$$\mathrm{val}^{-}(v) \leq \mathrm{val}(v) \Leftrightarrow 1 + \mathrm{val}^{-}(v) \leq 1 + \mathrm{val}(v)$$

$$\Leftrightarrow \frac{1}{1 + \mathrm{val}^{-}(v)} \geq \frac{1}{1 + \mathrm{val}(v)} \Leftrightarrow \sum_{v \in V(G^{-})} \frac{1}{1 + \mathrm{val}^{-}(v)} \geq \sum_{v \in V(G)} \frac{1}{1 + \mathrm{val}(v)}$$

Esta desigualdad, junto con inducción produce la desigualdad para $\alpha(G)$. Así que se mostrará que

$$\sum_{v \in V(G^{-})} \left[\frac{1}{1 + \mathrm{val}^{-}(v)} - \frac{1}{1 + \mathrm{val}(v)} \right] \geq \frac{1}{1 + \mathrm{val}(v_0)} .$$

Como $\mathrm{val}^{-}(v) = \mathrm{val}(v)$ si v y v_0 no son adyacentes en G, mientras que $\mathrm{val}^{-}(v) = \mathrm{val}(v) - 1$ si v y v_0 son adyacentes en G, la última desigualdad se reduce a:

$$\sum_{\substack{v \in V(G^{-}) \\ \{v, v_0\} \in E(G)}} \left[\frac{1}{1 + \mathrm{val}^{-}(v)} - \frac{1}{1 + \mathrm{val}(v)} \right] = \sum_{\substack{v \in V(G^{-}) \\ \{v, v_0\} \in E(G)}} \left[\frac{1}{\mathrm{val}(v)} - \frac{1}{1 + \mathrm{val}(v)} \right]$$

$$= \sum_{\substack{v \in V(G) \\ \{v, v_0\} \in E(G)}} \frac{\mathrm{val}(v) + 1 - \mathrm{val}(v)}{\mathrm{val}(v)\,[\mathrm{val}(v) + 1]} = \sum_{\substack{v \in V(G) \\ \{v, v_0\} \in E(G)}} \frac{1}{\mathrm{val}(v)\,[\mathrm{val}(v) + 1]} .$$

$$\therefore \sum_{\substack{v \in V(G^{-}) \\ \{v, vo\} \in E(G)}} \left[\frac{1}{val(v)[val(v) + 1]} \right] \geq \frac{1}{1 + val(vo)}$$

Ya que hay val(vo) términos, cada uno mayor o igual que:

$$\frac{1}{val(vo)[1 + val(vo)]} \quad \text{así que:}$$

$$\frac{1}{val(vo)[val(vO) + 1)} \leq \frac{1}{val(v)[val(v) + 1]} .$$

Por lo tanto la desigualdad se cumple y la primera parte del Teorema está probada.

Demostraremos ahora que la igualdad se cumple si y sólo si G es unión de clanes ajenos.

⇐) Si G es unión de clanes ajenos; $K_{n(1)}, K_{n(2)}, \ldots, K_{n(s)}$.
$\alpha(G) = s$.

$$\sum_{v \in V(K_{n(i)})} \frac{1}{1 + val(v)} = n(i) \frac{1}{(n(i) - 1) + 1} = 1.$$

Como hay s clanes ajenos, $\displaystyle\sum_{v \in V(G)} \frac{1}{1 + val(v)} = s.$

$\therefore$ la igualdad se cumple.

⇒) Si $\alpha(G) = \displaystyle\sum_{v \in V(G)} \frac{1}{1 + val(v)}$, como siempre se tiene,

$\alpha(G) \geq \alpha(G^{-}) \geq \displaystyle\sum_{v \in V(G^{-})} \frac{1}{1 + val^{-}(v)} \geq \sum_{v \in V(G)} \frac{1}{1 + val(v)}$ la igualdad implica:

$$\alpha(G^-) = \sum_{v \in V(G^-)} \frac{1}{1 + \text{val}^-(v)} = \sum_{v \in V(G)} \frac{1}{1 + \text{val}(v)}.$$

Ahora por inducción se puede suponer que G^- es unión de clanes ajenos.

Para $\alpha(G^-) = 1 \Rightarrow G^-$ es una gráfica completa.

Entonces $G = G^- \cup \{v_0\}$ también es completa, puesto que val(v_0) es máximo, así que v_0 debe ser adyacente a todo $v \in G^-$, $\therefore$ G es una gráfica completa.

Supongamos ahora que G es unión de r clanes ajenos, digamos K_1, $K_2, \ldots, K_r$, con $r = \alpha(G^-) = \alpha(G)$.

Por lo tanto v_0 debe ser adyacente a todos los vértices de algún K_j, j máximo, o bien existe un conjunto independiente en G de cardinalidad $(r + 1)$, (v_0 y un vértice de cada K_i, $1 \le i \le r$). Si v_0 es adyacente a todo vértice en K_i y no tiene otros vértices adyacentes, entonces G es unión de clanes ajenos. Si v_0 es adyacente a un vértice que no esté en K_i, entonces:

$$\text{val}(v_0) \ge |K_i| + 1 \text{ y } \text{val}(v) = |K_i|, \ \forall\, v \in V(K_i).$$

Pero ahora $\displaystyle\sum_{\substack{v \in V(G^-) \\ \{v, v_0\} \in E(G^-)}} \frac{1}{\text{val}(v)[1 + \text{val}(v)]} > \frac{1}{1 + \text{val}(v_0)}$, lo que contradice la igualdad entre $\displaystyle\sum_{v \in V(G)} \frac{1}{1 + \text{val}^-(v)}$ y $\displaystyle\sum_{v \in V(G)} \frac{1}{1 + \text{val}(v)}$.

Por lo tanto la demostración está completa.

Recordemos la desigualdad de Chebiychev:

$\displaystyle\sum_{i=1}^{n} a_i \sum_{i=1}^{n} b_i \ge n \sum_{i=1}^{n} a_i b_i$ con $\{a_i\}_1^n$ y $\{b_i\}_1^n$ sucesiones de números reales positivos, con igualdad si y sólo si o todos los a_i son iguales, o todos los b_i son iguales.

Y de esta desigualdad se obtiene:

$$\left[\sum_{v \in V(G)} \frac{1}{1 + \mathrm{val}(v)}\right]\left[\sum_{v \in V(G)} (1 + \mathrm{val}(v))\right] \geq |V(G)| \sum_{i=1}^{n} 1 = |V(G)|^2.$$

Del Tma. 1 se obtiene:

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{1 + \mathrm{val}(v)} \geq \frac{|V(G)|^2}{|V(G)| + 2|E(G)|}.$$

Con igualdad si y sólo si G es una gráfica regular.

Esto con el Tma. 10 (Wei) da:

Corolario 11. $\alpha(G) \geq \frac{|V(G)|^2}{|V(G)| + 2|E(G)|}$ con igualdad si y sólo si G es unión de clanes ajenos de la misma cardinalidad.

CAPITULO III. GRAFICAS Y GRUPOS.

"ES DIFICIL DAR UNA IDEA DEL AMPLIO ALCANCE DE LAS MATEMATICAS MODERNAS. LA PALABRA "ALCANCE" NO ES LA MEJOR; TENGO EN MIMENTE UN PULULAR DE IDEAS CON HERMOSOS DETALLES, NO LA ENVERGADURA UNIFORME DE UNA LLANURA SIN ATRACTIVO, SINO LA REGION DE UN HERMOSO PAIS, PRIMERO VISTO DESDE LA DISTANCIA, DIGNO DE SER RECORRIDO DE UN EXTREMO A OTRO Y DE SER ESTUDIADO EN SUS DETALLES MAS PEQUEÑOS; SUS VALLES, ARROYOS, ROCAS, BOSQUES Y FLORES."

Arthur Cayley.

SECCION A. UNA GRAFICA ASOCIADA A UN GRUPO.

En las gráficas como en todo conjunto en el que se ha definido una relación, existe un grupo de permutaciones que preserva esta relación. Así, es natural pensar en los vértices o en las aristas de una gráfica y en las relaciones de adyacencia e incidencia y analizar su grupo de permutaciones.

Def.

ϕ: G $\to$ H es un morfismo de gráficas si:

i). V(G) $\to$ V(H), y
ii). u ady_G v $\Rightarrow$ $\phi(u)$ ady_H $\phi(v)$.

Def.

ϕ: G $\to$ H es un isomorfismo si:

i). ϕ es morfismo y
ii). $\exists$ ϕ^{-1}: H $\to$ G, que también es morfismo.

Observación.

ϕ: G $\to$ H es isomorfismo si:

i). ϕ: V(G) $\to$ V(H) es una biyección y
ii). u ady_G v $\Leftrightarrow$ $\phi(u)$ ady_H $\phi(v)$.

De las anteriores definiciones obtenemos que si ϕ es un automorfismo de G, $v \in V(G)$, y $val(v) = k$, entonces $\phi(v)$ es adyacente a $\phi(v_i)$, con v_i, $i = 1, 2, \ldots, k$, los vértices adyacentes a v. Si existiera $u \in G$ tal que $u \neq v_i$, $\forall\, i$ y u adyacente a $\phi(v)$, entonces $\phi^{-1}(u)$ sería adyacente a v, lo cual contradice el hecho de que la valencia de v es k. Así obtenemos el siguiente:

Tma. 1. Si G es una gráfica y ϕ es un automorfismo de G, entonces $val(v) = val(\phi(v))$, $\forall\, v \in V(G)$.

El conjunto de los automorfismos de una gráfica forma un grupo, que en adelante denotaremos por $\mathfrak{U}(G)$. Este grupo se denomina el grupo de automorfismos de G o sencillamente el grupo de G.

Ejemplos.

2. Consideremos C_n el ciclo con n vértices. Entonces $\mathfrak{U}(C_n)$ es el grupo, diédrico de orden 2n.

3. Consideremos K_5.
   En este caso $\mathfrak{U}(K_5)$ es el grupo simétrico S_5 de orden 5!, y en general para K_n, $\mathfrak{U}(K_n) \cong S_n$, el grupo simétrico de orden n!.

4. Consideremos C_3, sabemos que $\mathfrak{U}(C_3) \cong D_3$ y por lo anterior $\mathfrak{U}(C_3) \cong S_3$ de orden 6. Por otra parte, se comprueba fácilmente que el complemento de C_3, C_3^c, también tiene un grupo que resulta isomorfo a S_3.

Esta situación es en general para una gráfica G y su complemento G^c y se contempla en el siguiente

Tma. 5. Si G es una gráfica y G^c su complemento, entonces: $\mathfrak{U}(G) \cong \mathfrak{U}(G^c)$.

Dem.

Sea $\phi \in \mathfrak{U}(G)$. Por lo tanto ϕ es una permutación de V(G) que preserva adyacencias, así de la definición se tiene:

$$u \text{ adya } v \Leftrightarrow \phi(u) \text{ adya } \phi(v)$$

$$\text{no } (u \text{ adya } v) \Leftrightarrow \text{no } (\phi(u) \text{ adya } \phi(v))$$

$$\therefore \quad \phi \text{ preserva no adyacencia}$$

$$\therefore \quad \phi \in \mathfrak{U}(G^c).$$

Como ya vimos arriba, cuando $G \cong K_n$, entonces $\mathfrak{U}(G) \cong S_n$. En caso de que G tenga n vértices, pero no sea K_n ni K_n^c resulta $\mathfrak{U}(G) \cong U$, con U un subgrupo propio de S_n.

Combinando esta nota, el Tma. 5 y el Tma. I. 17, obtenemos el siguiente

Corolario 6. Sea G una gráfica con p vértices. El orden $|\mathfrak{U}(G)|$ es un divisor de $p!$ y es igual a $p!$ si y sólo si $G \cong K_p$ o $G^c \cong K_p$.

El grupo $\mathfrak{U}(G)$ no es el único grupo que podemos asociar a G, también de sus aristas podemos obtener otro grupo asociado a G. Este se conoce como el grupo de isomorfismos de aristas.

Def. Sean G y H dos gráficas no vacías de aristas. Diremos que G y H son isomorfas en aristas si existe:

$$\phi: E(G) \to E(H), \text{ biyectiva}$$

tal que $E_1, E_2 \in E(G)$ son adyacentes en G si y sólo si:

$$\phi(E_1) \text{ es adyacente a } \phi(E_2) \text{ en } H.$$

ϕ se conoce como isomorfismo de aristas de G a H.

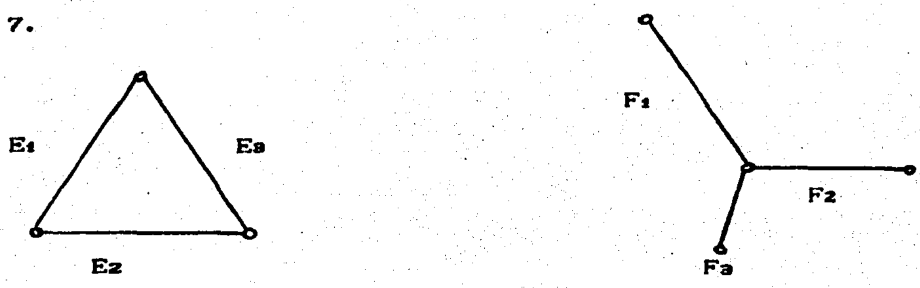
Si ϕ es un isomorfismo de vértices de una gráfica G no vacía de aristas en una gráfica H, entonces $\{u_1, u_2\} \in E(G)$ si y sólo si $\{\phi(u_1), \phi(u_2)\} \in E(H)$. Más aún, las aristas $\{u_1, u_2\}$ y $\{v_1, v_2\}$ son adyacentes en G si y sólo si las aristas $\{\phi(u_1), \phi(u_2)\}$ y $\{\phi(v_1), \phi(v_2)\}$ son adyacentes en H. Por lo tanto, dos gráficas no vacías isomorfas, son isomorfas en aristas.

De aquí que todo isomorfismo de G a H induce un isomorfismo de aristas de G a H.

Si un isomorfismo de aristas se obtiene de esta manera de un isomorfismo de vértices, lo llamaremos inducido.

El siguiente ejemplo muestra dos gráficas isomorfas en aristas, pero que no son isomorfas.

Ejemplo 7.



G_1 G_2

$\phi(E_i) = F_i$, $i = 1, 2, 3$ es un isomorfismo de aristas, pero sabemos que $val(v) = val(\phi(v))$. En G_1 los tres vértices son de grado 2, mientras que G_2 no contiene ningún vértice de grado 2.

Def. Sean G y H dos gráficas no vacías de aristas.

ϕ: G → H es morfismo de aristas si:

$\phi: E(G) \to E(H)$ y

$\{u, v\}$ ady_G $\{u_1, v_1\} \Rightarrow \phi(\{u, v\})$ ady_H $\phi(\{u_1, v_1\})$.

Def.

ϕ: G → H es un isomorfismo de aristas si:

$i)$ ϕ es morfismo y

$ii)$ $\exists\ \phi^{-1}$: H → G que también es morfismo.

Observación.

ϕ: G → H es isomorfismo de aristas si y sólo si:

$i)$ $\phi: E(G) \to E(H)$ es una biyección y

$ii)$ $\{u, v\}$ ady_G $\{u_1, v_1\} \Leftrightarrow \phi(\{u, v\})$ ady_H $\phi(\{u_1, v_1\})$.

Def. ϕ es automorfismo de aristas si:

$i)$ ϕ: $G \to G$ y

$ii)$ ϕ es isomorfismo de aristas.

El conjunto de todos los automorfismos de aristas de G (con la composición) forma un grupo, llamado **el grupo de aristas de G**, que denotaremos por $\mathfrak{A}_1(G)$.

Como cada isomorfismo de G en G' induce un isomorfismo de aristas de G en G', cuando elegimos $G' = G$, de manera natural hablamos de automorfismos de aristas inducidos. El conjunto de éstos, también forma un grupo con la composición, y se conoce como el grupo inducido de aristas de G. Este grupo se denota como $\mathfrak{A}^*(G)$.

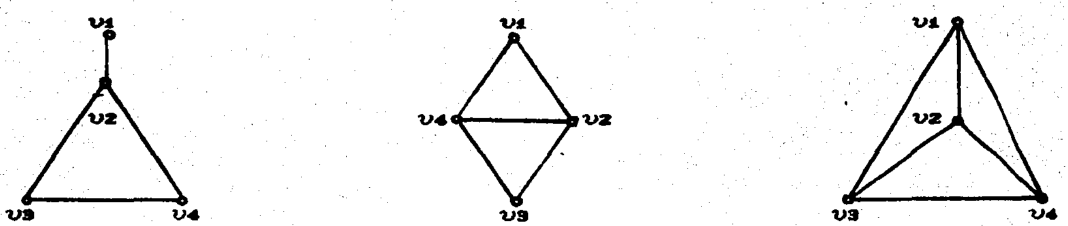
Es claro el hecho de que $\mathfrak{A}^*(G) \leq \mathfrak{A}_1(G)$.

Ejemplos

8. Sea $G = K_{(1,n)}$. Entonces $\mathfrak{A}_1(K_{(1,n)}) \cong S_n$.
   Mientras que si $G = C_p$, $\mathfrak{A}_1(C_p) \cong D_p$.

El siguiente ejemplo muestra que $\mathfrak{A}^*$ puede ser un subgrupo propio de $\mathfrak{A}_1(G)$.

9. Consideremos las gráficas G_1, G_2, G_3 como:



De acuerdo con estas etiquetaciones, definimos:

$$\Phi_1 = \begin{pmatrix} \{v_1, v_2\}, & \{v_2, v_3\}, & \{v_2, v_4\}, & \{v_3, v_4\} \\ \{v_3, v_4\}, & \{v_2, v_3\}, & \{v_2, v_4\}, & \{v_1, v_2\} \end{pmatrix}$$

$$\Phi_2 = \begin{bmatrix} \{v_1, v_2\}, & \{v_2, v_3\}, & \{v_2, v_4\}, & \{v_3, v_4\}, & \{v_1, v_4\} \\ \{v_2, v_3\}, & \{v_3, v_4\}, & \{v_2, v_4\}, & \{v_1, v_4\}, & \{v_1, v_2\} \end{bmatrix}$$

$$\Phi_3 = \begin{bmatrix} \{v_1, v_2\}, & \{v_2, v_3\}, & \{v_2, v_4\}, & \{v_3, v_4\}, & \{v_1, v_4\}, & \{v_1, v_3\} \\ \{v_3, v_4\}, & \{v_2, v_3\}, & \{v_2, v_4\}, & \{v_1, v_2\}, & \{v_1, v_4\}, & \{v_1, v_3\} \end{bmatrix}$$

Probaremos por ejemplo, que Φ_1 es un automorfismo de aristas, pero que no es inducido. Esta situación también se presenta para Φ_2 y Φ_3.

Por definición, $\Phi_1(E_1) = E_4$; $\Phi_1(E_2) = E_2$; $\Phi_1(E_3) = E_3$; $\Phi_1(E_4) = E_1$. Φ_1 intercambia las aristas E_1 y E_4.

Φ_1 por definición, es una biyección de $E(G_1)$ en sí mismo.

Probaremos ahora que es un morfismo.

Los pares de aristas adyacentes son: E_1E_2, E_1E_3, E_2E_4 y E_3E_4.

$\Phi_1(E_1) = E_4$ es adyacente a E_3 y a E_2, E_2 y E_3 quedan fijos bajo Φ. Por lo tanto $\Phi_1(E_1)\Phi_1(E_2)$ y $\Phi_1(E_1)\Phi_1(E_3)$ son adyacentes.

Por otra parte, $\Phi_1(E_4) = E_1$ es adyacente a E_2 y E_3, que quedan fijos bajo Φ_1. Por lo tanto $\Phi_1(E_2)\Phi_1(E_4)$ y $\Phi_1(E_3)\Phi_1(E_4)$ son adyacentes.

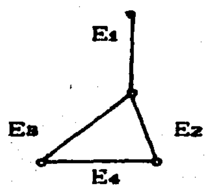
Por lo tanto, Φ_1 es un automorfismo de aristas.

Es claro que el grupo de automorfismos de G_1 es cíclico y de orden 2. Este grupo está compuesto por las permutaciones de vértices:

$$\mathfrak{A}(G_1) = \{\, id,\ (3,4)\}.$$

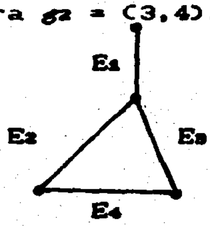
Por lo tanto el grupo de automorfismos de aristas inducidos es:

Para $g_1 = id$:



$g_1(E_1) = E_1$.
$g_1(E_2) = E_2$.
$g_1(E_3) = E_3$.
$g_1(E_4) = E_4$.

y para $g_2 = (3,4)$:



$g_2(E_1) = E_1.$
$g_2(E_2) = E_3.$
$g_2(E_3) = E_2.$
$g_2(E_4) = E_4.$

$$g_1(E_1) = g_2(E_1) \neq \bar{g}_1(E_1).$$

$\therefore$ $\bar{g}_1$ no es un automorfismo de aristas inducido.

De manera análoga se hace la demostración para $\bar{g}_2$ y $\bar{g}_3$.

Continuando con la consideración de estas tres gráficas, notamos que: $|\mathfrak{A}(G_i)| = 2|\mathfrak{A}'(G_i)|$ para $i = 1, 2, 3.$

$|\mathfrak{A}'(G_1)| = 2,$ $|\mathfrak{A}'(G_2)| = 4$ y $|\mathfrak{A}(G_3)| = 24.$

El siguiente teorema proporciona una relación interesante entre el grupo y el grupo de aristas inducido de una gráfica G

Tma. 10. Sea G una gráfica conexa no trivial.
Entonces $\mathfrak{A}(G) \cong \mathfrak{A}'(G)$ si y sólo si $G \ncong K_2$.

Dem.

$\Rightarrow$) (contrapuesta).

Supongamos $G \cong K_2$. Como $\mathfrak{A}(K_2) = S_2$, mientras que $\mathfrak{A}'(K_2) = S_1$, se tiene $\mathfrak{A}(G) \ncong \mathfrak{A}'(G)$.

$\Leftarrow$) Supongamos que G es una gráfica conexa no trivial, $\therefore$ $|V(G)| \neq 1$ así que $|V(G)| \geq 2$. Como $G \ncong K_2$ se tiene $|V(G)| \geq 3$, y por ser conexa $|E(G)| \geq 2$.

Para demostrar $\mathfrak{A}(G) \cong \mathfrak{A}'(G)$ definimos el siguiente mapeo:

ϕ: $\mathfrak{A}(G) \to \mathfrak{A}'(G)$ como $\phi(\omega) = \omega^*$, donde ω^* es el automorfismo de aristas de G inducido por ω.

Probaremos que ϕ es un isomorfismo de grupos.

i). "ϕ es una biyección".

a). Por construcción, ϕ es suprayectivo.

b). Para mostrar que ϕ es inyectivo, sean $\varphi \neq \lambda \in \mathfrak{A}(G)$.
Por demostrar: $\varphi^* \neq \lambda^*$ (*i. e.* $\exists$ E $\in$ E(G) tal que $\varphi^*(E) \neq \lambda^*(E)$).

Dem. Como $\varphi \neq \lambda$ podemos elegir $v \in V(G)$ tal que $\varphi(v) \neq \lambda(v)$. Como G es conexa y $|V(G)| \geq 3$, $\exists$ $u \in V(G)$ tal que u es adyacente a v. Si $\varphi(u) \neq \lambda(v)$ o $\lambda(u) \neq \varphi(v)$, entonces para la arista E = $\{u, v\}$, tenemos $\varphi^*(\{u, v\}) \neq \lambda^*(\{u, v\})$. Por lo tanto podemos suponer $\varphi(u) = \lambda(v)$ y $\lambda(u) = \varphi(v)$.
De nuevo como G es conexa y $|V(G)| \geq 3$, $\exists$ $w \in V(G)$ tal que $\{u, w\}$ o $\{v, w\} \in E(G)$ y $w \notin \{u, v\}$.

Si $\{u, w\} \in E(G)$ entonces $\varphi^*(\{u, w\}) \neq \lambda^*(\{u, w\})$.

Si $\{v, w\} \in E(G)$ entonces $\varphi^*(\{v, w\}) \neq \lambda^*(\{v, w\})$.

Por lo tanto en cualquier caso, ϕ es inyectiva.

Por a) y b), ϕ es biyectiva.

ii). Mostraremos ahora que ϕ respeta la operación, *i. e.*:
$\forall$ E $\in$ E(G), $\phi(\varphi\lambda)(E) = (\phi\varphi)(\phi\lambda)(E)$.

Dem. Sea E $\in$ E(G), E = $\{u, v\}$. Supongamos $\lambda(u) = u'$, $\lambda(v) = v'$, $\varphi(u') = u''$, $\varphi(v') = v''$.

$\phi(\varphi\lambda)(E) = \phi(\varphi\lambda)(\{u, v\}) = (\varphi\lambda)(u)(\varphi\lambda)(v) = \varphi(u')\varphi(v') = u''v''$,

y $\qquad (\phi\varphi)(\phi\lambda)(E) = (\phi\varphi)(\phi\lambda)(\{u, v\}) = (\phi\varphi)(\{\lambda(u), \lambda(v)\}) =$

$\qquad (\phi\varphi)(u'v') = \; = \varphi(u')\varphi(v') = u''v''$.

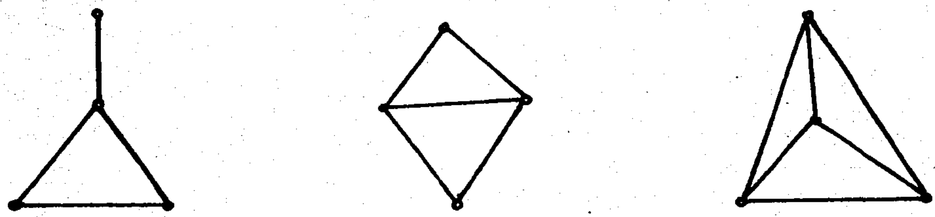
Como $\phi(\varphi\lambda)(\{u, v\}) = (\phi\varphi)(\phi\lambda)(\{u, v\})$, tenemos que ϕ respeta la operación.

Por i) y ii), ϕ es un isomorfismo entre los grupos $\mathfrak{A}(G)$ y $\mathfrak{A}^*(G)$.

Este teorema tiene una generalización para gráficas arbitrarias.

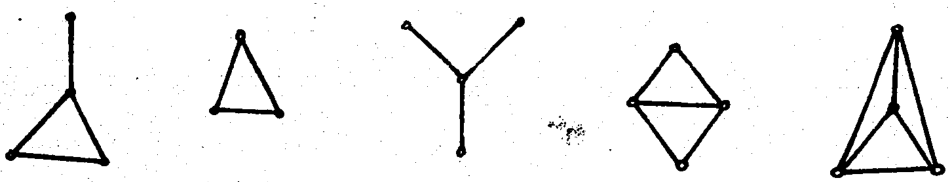
Corolario 11. Sea G una gráfica no trivial. Entonces $\mathfrak{A}(G) \cong \mathfrak{A}^*(G)$ si y sólo si G no incluye a K_2 como una componente y G tiene a lo más un vértice aislado.

Algunas gráficas poseen la propiedad de que $\mathfrak{A}_1(G) \cong \mathfrak{A}'(G)$. Sin embargo, para las tres siguientes gráficas, esta afirmación es falsa.



El siguiente resultado debido a Whitney, es útil para obtener una caracterización de las gráficas con $\mathfrak{A}_1(G) \cong \mathfrak{A}'(G)$. La demostración aparece en [6].

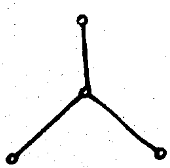
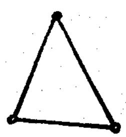
Tma. 12. Sup. que ϕ es un isomorfismo de aristas de una gráfica conexa H_1 a una gráfica conexa H_2, donde H_1 no es alguna de las gráficas:

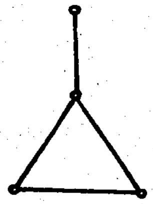
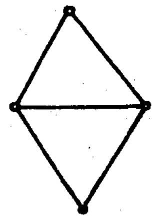
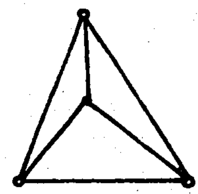


Entonces ϕ es inducido por algún isomorfismo de H_1 a H_2.

Así que usando este Tma. obtenemos:

Tma. 13. Sea G una gráfica no vacía de aristas.
Entonces $\mathfrak{A}_1(G) \cong \mathfrak{A}'(G)$ si y sólo si:

i). Ni  ni  son componentes de G.

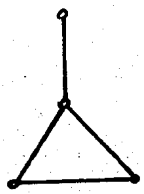
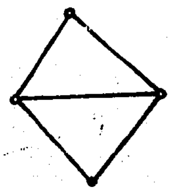
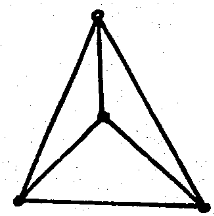
y ii). Ni  ni  ni 

es una componente de G

La demostración también aparece en [6].

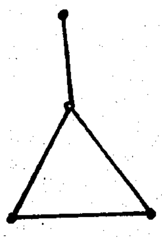
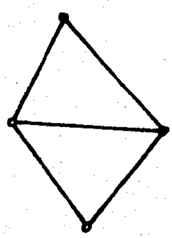
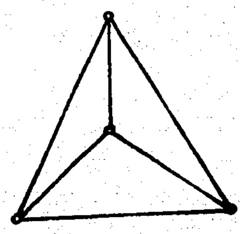
Se obtiene además el siguiente:

Corolario 14. Sea G una gráfica conexa no vacía.
Entonces $\mathfrak{A}_1(G) \cong \mathfrak{A}'(G)$ si y sólo si G es distinta de las gráficas:

Combinando este Corolario con el Tma. 10 se obtiene el siguiente:

Corolario 15. Sea G una gráfica conexa de orden $p \geq 3$.
Entonces los grupos $\mathfrak{A}(G)$, $\mathfrak{A}_1(G)$ y $\mathfrak{A}'(G)$ son isomorfos entre sí, si y sólo si G es distinta de las gráficas:

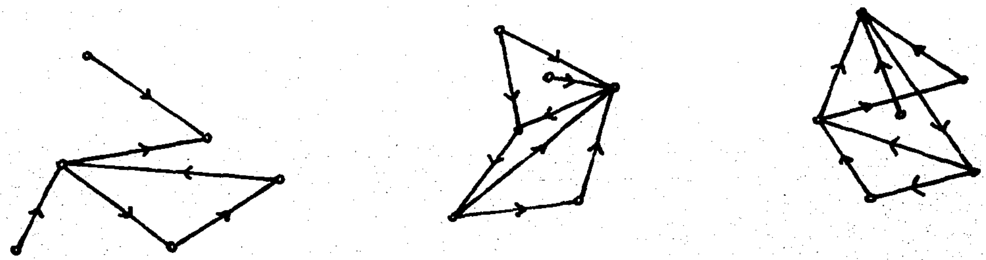
SECCION B. UNA GRAFICA ASOCIADA A UN GRUPO.

En la sección precedente ya vimos que a cada gráfica podemos asociar un grupo (de hecho son tres). A continuación consideraremos el problema inverso: asociar una gráfica a un grupo dado.

Sea Γ un grupo finito no trivial. Sea Δ un conjunto generador de Γ, es decir todo elemento del grupo es generado por la potencia de algún producto de éstos. $\Delta = \{\delta_1, \delta_2, \ldots, \delta_k\}$.

Introducimos el concepto de digráfica.

Def. Una digráfica (gráfica dirigida) es una gráfica en la que las aristas son un subconjunto de los pares ordenados del conjunto de vértices. En este caso, a las aristas las representamos mediante una flecha.

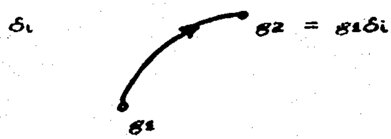


Algunas digraficas.

Asociaremos a Γ y Δ una digráfica (una gráfica dirigida), llamada la gráfica de color de Cayley de Γ con respecto a Δ y denotada por $D_\Delta(\Gamma)$.

Def. El conjunto de vértices de $D_\Delta(\Gamma)$, la gráfica de color de Cayley de Γ con respecto a Δ, es el conjunto de elementos del grupo Γ. Por lo tanto, $D_\Delta(\Gamma)$ tiene orden $|\Gamma|$. Todo generador δ_i es considerado como un color.

Si $g_1, g_2 \in \Gamma$, $\exists$ un arco (g_1, g_2) de color δ_i en $D_\Delta(\Gamma)$ si y sólo si $g_2 = g_1\delta_i$.



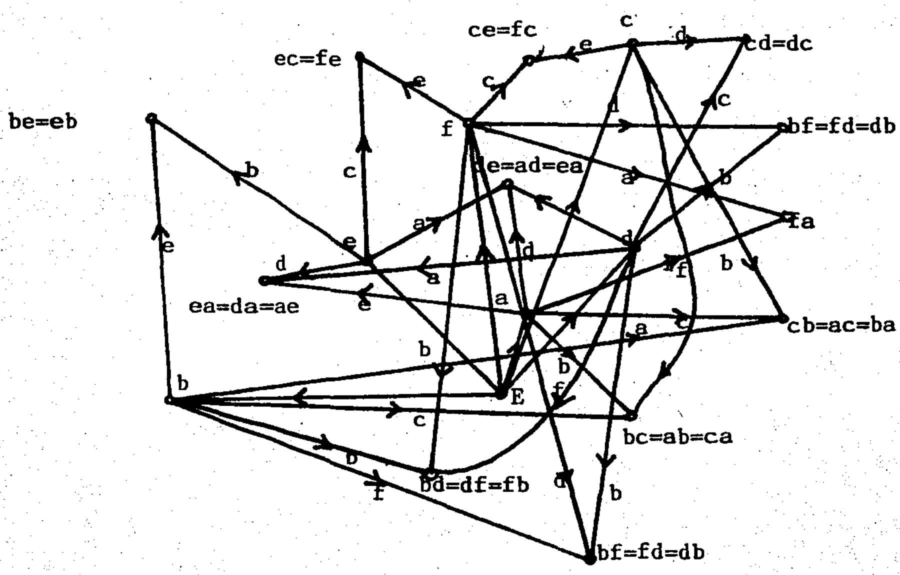
Si δ_i es un elemento de Γ de orden 2 (y por lo tanto auto-inverso) y $g_2 = g_1\delta_i$, necesariamente tenemos $g_1 = g_2\delta_i$, $(g_2 = g_1\delta_i \Leftrightarrow g_2\delta_i^{-1} = g_1 \Leftrightarrow g_2\delta_i = g_1)$.

Si la gráfica de color de Cayley $D_\Delta(\Gamma)$ contiene a los arcos (g_1, g_2) y (g_2, g_1) ambos de color δ_i, se acostumbra representar este par simétrico de arcos por la arista $\{g_1, g_2\}$.

A manera de ilustración, considérese:

Γ el grupo simétrico S_4.

Sea $\Delta = \{(3,4), (2,4), (2,3), (1,4), (1,3), (1,2)\}$. Denotemos cada elemento de Δ mediante una letra, $a = (3,4)$, $b = (2,4)$, $c = (2,3)$, $d = (1,4)$, $e = (1,3)$, $f = (1,2)$. Δ es un conjunto generador de Γ. La gráfica de color de Cayley $D_\Delta(S_4)$ resulta ser:



Def. Si el conjunto generador Δ de un grupo finito Γ no trivial, se elige como el conjunto de todos los elementos del grupo distintos de la identidad, entonces para cada 2 vértices $g_1, g_2 \in D_\Delta(\Gamma)$, los arcos (g_1, g_2) y (g_2, g_1) pertenecen a la gráfica (aún cuando no sean del mismo color). En este caso, $D_\Delta(\Gamma)$ es llamada una digráfica simétrica completa.

Def. Un automorfismo de una digráfica D es una permutación φ en $V(D)$ tal que (u, v) es un arco de D si y sólo si $(\varphi(u), \varphi(v))$ es un arco de D. Sabemos que el conjunto de todos los automorfismos de D forma un grupo bajo la composición y lo denotamos por $\mathfrak{U}(D)$.

Def. Si Γ es un grupo finito no trivial con un conjunto generador Δ, diremos que $\varphi \in \mathfrak{U}(D_\Delta(\Gamma))$ preserva colores si para todo arco (g_1, g_2) de $D_\Delta(\Gamma)$, los arcos (g_1, g_2) y $(\varphi(g_1), \varphi(g_2))$ tienen el mismo color.

Tma. 16. El conjunto de todos los automorfismos de $D_\Delta(\Gamma)$ que preservan colores es un subgrupo de $\mathfrak{U}(D_\Delta(\Gamma))$.

Por el **Tma. I, 11.** basta probar la cerradura.

Dem. Supongamos que φ y η preservan colores. Sea (g_1, g_2) un arco de $D_\Delta(\Gamma)$. Como η preserva colores, (g_1, g_2) y $(\eta(g_1), \eta(g_2))$ tienen el mismo color, $[(\eta(g_1), \eta(g_2))$ es un arco de $D_\Delta(\Gamma)]$ y como φ preserva colores $(\eta(g_1), \eta(g_2))$ tiene el mismo color que $(\varphi(\eta(g_1)), \varphi(\eta(g_2)))$.

$$\therefore (g_1, g_2) \text{ y } (\varphi(\eta(g_1)), \varphi(\eta(g_2))) \text{ tienen el mismo color.}$$

$\therefore$ el conjunto de todos los automorfismos de $D_\Delta(\Gamma)$ que preservan colores es un subgrupo de $\mathfrak{U}(D_\Delta(\Gamma))$.

Tma. 17. Sea Γ un grupo finito no trivial con un conjunto generador Δ. Sea φ una permutación de $V(D_\Delta(\Gamma))$. Entonces φ es un automorfismo de $D_\Delta(\Gamma)$ que preserva colores si y sólo si:

$$\varphi(g\delta) = (\varphi g)\delta, \ \forall\ g \in \Gamma,\ \delta \in \Delta.$$

Dem.
$\Rightarrow$) Supongamos que φ es un automorfismo de $D_\Delta(\Gamma)$ que preserva colores. Sean $g \in \Gamma$, $\delta \in \Delta$.
Consideremos el arco $(g, g\delta)$. De la definición, éste es un arco de $D_\Delta(\Gamma)$, de color δ.

Como φ preserva colores, $(\varphi g, \varphi(g\delta))$ también tiene color δ, es decir, $(\varphi g)\delta = \varphi(g\delta)$.

$\Leftarrow)$ Supongamos $\varphi(g\delta) = (\varphi g)\delta$, $\forall\ g \in \Gamma$, $\delta \in \Delta$.
$\therefore$ $(\varphi g, \varphi(g\delta))$ es un arco de $D_\Delta(\Gamma)$ de color δ.

Por demostrar, $(g, g\delta)$ tiene color δ.

Por definición, $g\delta = g\delta$ implica $(g, g\delta)$ tiene color δ.
$\therefore$ φ preserva colores.

El siguiente teorema aparece en [6] y lo mencionamos para mostrar la utilidad de las gráficas de color de Cayley.

Tma. 18. Sea Γ un grupo finito no trivial con conjunto generador Δ. Entonces el grupo de automorfismos de $D_\Delta(\Gamma)$ que preservan colores es isomorfo a Γ.

En *1936*, König autor del primer libro sobre teoría de gráficas, propuso el siguiente problema: "Determinar todos los grupos finitos Γ para los cuales existe una gráfica G tal que $\mathfrak{A}(G) \cong \Gamma$.

En *1938*, Frucht resolvió el problema, determinando que todo grupo finito tiene esta propiedad.

Con la teoría desarrollada hasta aquí, podemos ya dar una demostración de este resultado.

Si Γ es el grupo trivial, entonces $\mathfrak{A}(G) \cong \Gamma$ si $G \cong K_1$. Por lo tanto podemos suponer que Γ es no trivial. $\Gamma = \{g_1, \ldots, g_p\}$. Sea $\Delta = \{\delta_1, \ldots, \delta_n\}$ un conjunto generador para Γ.

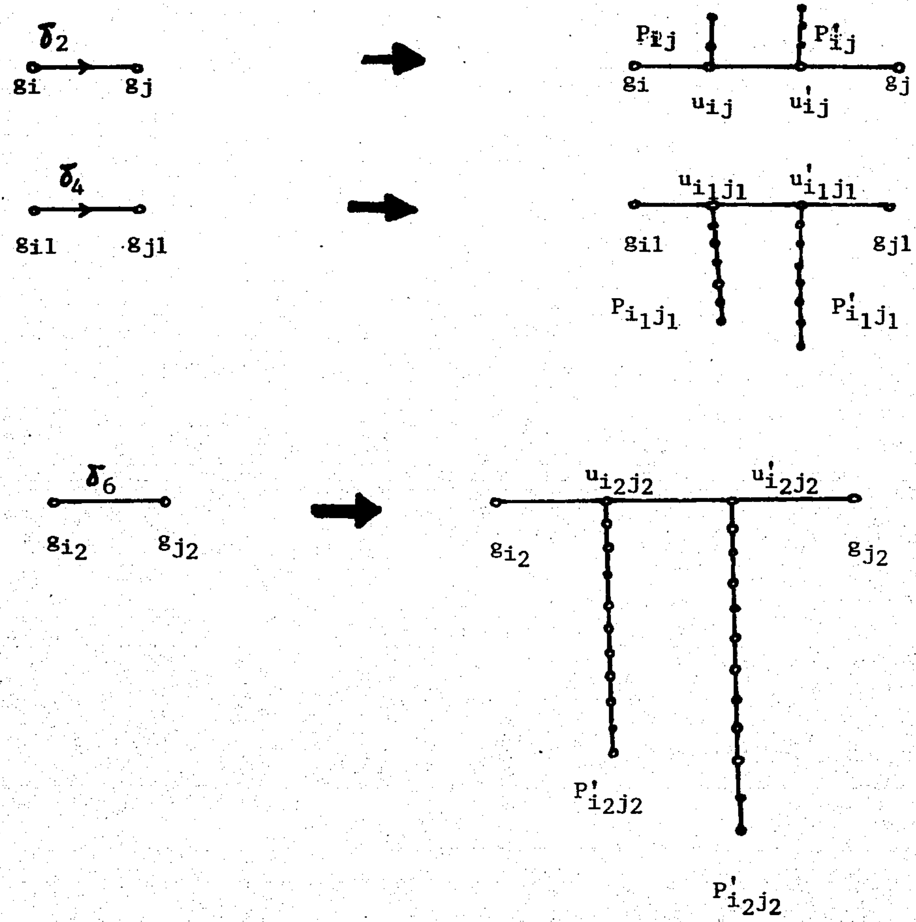
En primer lugar construimos la gráfica de color de Cayley, ésta resulta ser una digráfica. Sabemos del teorema precedente, que el grupo de automorfismos de $D_\Delta(\Gamma)$ que preservan colores es isomorfo a Γ.

Resta ahora, transformar la digráfica $D_\Delta(\Gamma)$ en una gráfica G.

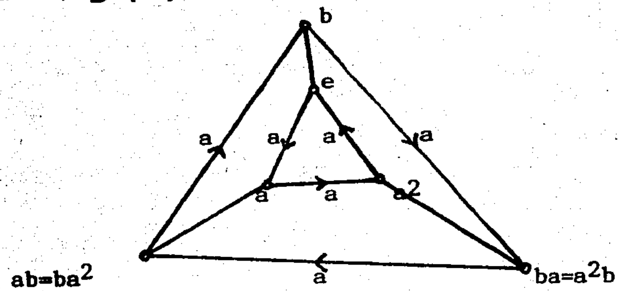
Lo haremos de acuerdo con la siguiente técnica.

Sea (g_i, g_j) un arco de $D_\Delta(\Gamma)$ de color δ_k. Quitemos este arco y sustituyámoslo por la trayectoria g_i, u_{ij}, u'_{ij}, g_j. En el vértice u_{ij} añadimos otra trayectoria P_{ij} de longitud $(2k - 2)$ y en el

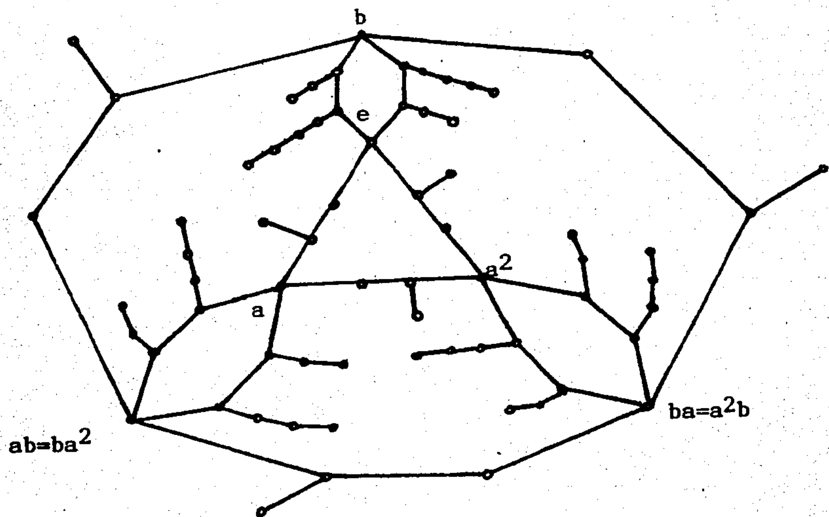
vértice u'_{ij} añadimos una trayectoria P'_{ij} de longitud $(2k - 1)$.
Esta construcción se hace en cada arco de $D_\Delta(\Gamma)$.
La siguiente figura muestra la construcción para δ_2, δ_4 y δ_6.



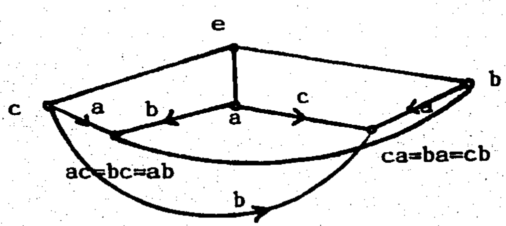
Para S_3, $D_\Delta\{S_3\}$ se tiene la digráfica:



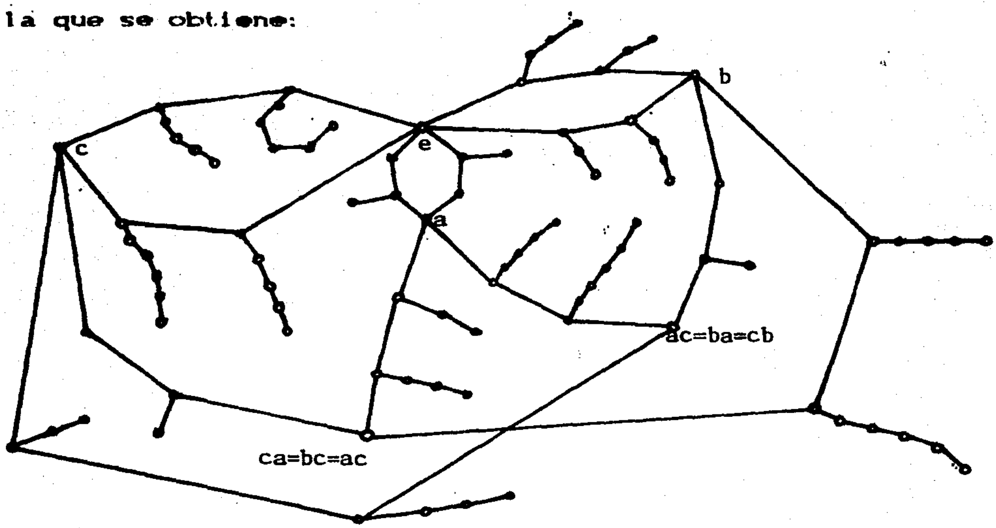
de la que se obtiene la gráfica:



Otro ejemplo



de la que se obtiene:



Resta ahora observar que todo automorfismo de $D_\Delta(\Gamma)$ que preserva colores, induce un automorfismo de G y recíprocamente. Enunciemos esto:

Tma. 19. (Frucht). $\forall\, \Gamma$, grupo finito, $\exists$ una gráfica G tal que

$$\mathfrak{A}(G) \cong \Gamma.$$

Construir una gráfica G con ciertas caraterísticas (grado de regularidad, conectividad, otros parámetros y combinación de éstos), de tal manera que $\mathfrak{A}(G) \cong \Gamma$, con Γ un grupo, es posible.

La ilustración en detalle de las técnicas involucradas en la construcción de una gráfica así, se hace en [6], al cual se refiere al lector.

CAPITULO IV. ALGUNAS APLICACIONES DE LA TEORIA DE GRAFICAS A GRUPOS FINITOS.

"SI QUEDE MARAVILLADO CON EL ALGEBRA, QUEDE EMBELESADO POR LAS APLICACIONES DEL ALGEBRA A LA GEOMETRIA. LA IDEA, LA POSIBILIDAD DE EXPRESAR UNA LINEA, UNA CURVA, EN TERMINOS ALGEBRAICOS, MEDIANTE UNA ECUACION, ME PARECIO TAN HERMOSO COMO LA ILIADA. CUANDO TUVE LA ECUACION DE UNA FUNCION Y LA RESOLVI, POR DECIRLO ASI, CON MIS MANOS Y LA PUDE TRADUCIR EN UNA INFINIDAD DE VERDADES, TODAS IGUALMENTE INDISPUTABLES, IGUALMENTE ETERNAS, IGUALMENTE RESPLANDECIENTES, CREI QUE ERA MIO EL TALISMAN QUE ABRIRIA LA PUERTA DE TODO MISTERIO".

Edgar Quinet.

SECCION A. Sobre la cardinalidad de los subgrupos abelianos de un grupo finito.

TMA 1. Sea Γ un grupo finito. Enumeremos las clases de conjugación de los elementos de Γ, de acuerdo con su cardinalidad:

$$1 \leq |[x_1]| \leq |[x_2]| \leq |[x_3]| \leq \ldots$$

Sea m el mínimo entero i tal que:

$$|[x_1]| + |[x_2]| + \ldots + |[x_i]| \geq |C(x_i)|$$

Entonces todo subgrupo abeliano A de Γ es tal que:

$$|A| \leq |[x_1]| + |[x_2]| + \ldots + |[x_m]|.$$

Dem.

1. Supongamos que Γ es abeliano.
   Entonces $\forall\ x \in \Gamma$, $|[x]| = 1$ y $C(x) = \Gamma$.
   Como Γ es finito, supongamos $|\Gamma| = n$ y se tiene $|C(x)| = n$.

Por lo tanto la m del teorema es n, ya que:

$$|[x_1]| + |[x_2]| + \ldots + |[x_i]| = |C(x_i)| = n.$$

$$1 \quad + \quad 1 \quad + \ldots + \quad 1 \quad = i.$$

Como Γ es abeliano, cualquier subgrupo A también es abeliano.

$$|A| \leq |\Gamma| = n = 1 + \ldots + 1 = |[x_1]| + |[x_2]| + \ldots + |[x_{m=n}]|.$$

2. Supongamos pues que Γ no es abeliano.

Sea $x_i \notin Z(\Gamma)$. Consideremos $C(x_i)$ el centralizador de x_i. Como Γ no es abeliano, $\exists$ $x_j \in \Gamma$ tal que $x_ix_j \neq x_jx_i$, para x_i.

$$\therefore C(x_j) \neq \Gamma.$$

De los elementos x_j con esta propiedad, tomemos uno que tenga el índice L mínimo en la siguiente sucesión.

$$|[x_1]| \leq |[x_2]| \leq |[x_3]| \leq \ldots$$

Sea x_L este elemento.

Como $C(x_L)$ es subgrupo de Γ y $C(x_L) \subset \Gamma$, tenemos $|C(x_L)| \leq |\Gamma|$.

Por lo tanto: $$1 < \frac{|\Gamma|}{|C(x_L)|} = |[x_L]|$$

Por lo tanto $|[x_L]| \geq 2$, y,

$$1 = |[x_1]| = |[x_2]| = \ldots = |[x_{L-1}]| < |[x_L]| \leq |[x_{L+1}]| \leq \ldots$$

de donde:

$$\frac{1}{|[x_L]|} \geq \frac{1}{|[x_{L+1}]|} \geq \frac{1}{|[x_{L+2}]|} \geq \ldots$$

y del hecho $|\Gamma| = |[x]|\,|C(x)|$, obtenemos al multiplicar por $|\Gamma|$:

$$|C(x_L)| \geq |C(x_{L+1})| \geq |C(x_{L+2})| \geq \dots \qquad (1)$$

Sea A un subgrupo abeliano de Γ.

Afirmación. Si A es máximo entre los subgrupos abelianos de Γ, entonces: " $Z(\Gamma) \leq A \cap C(x_L)$ ".

Dem.

1. "$Z(\Gamma) \leq C(x_L)$", obviamente.

2. "$Z(\Gamma) \subset A$".

Como $Z(\Gamma)$ es abeliano, $Z(\Gamma)A$ es un subgrupo abeliano de Γ tal que $A \leq Z(\Gamma)A$. Como A es máximo con la propiedad de ser abeliano tenemos que $A = Z(\Gamma)A$. Por lo tanto $Z(\Gamma) \leq Z(\Gamma)A = A$.

Así obtenemos la afirmación.

Mas aún, $|A| \leq |C(x_L)|$.

Para aclarar esto, observemos lo siguiente:

Si $A \leq C(x_L)$, obtenemos el resultado.

Si no es el caso, $\exists$ $\alpha \in A$ tal que $\alpha \notin C(x_L)$, por lo tanto

$$\alpha \notin \bigcap_{x \in \Gamma} C(x) = Z(\Gamma), \text{ i. e. } \alpha \notin Z(\Gamma)$$

Como $A \leq C(\alpha)$ y $\alpha \notin Z(\Gamma)$, $(|[\alpha]| > 1)$, tenemos:

$$|A| \leq |C(\alpha)| \leq |C(x_L)|, \qquad \text{por } (1).$$

Como las clases de conjugación inducen una partición de Γ, que no es abeliano, el entero m (en el enunciado del teorema), debe ser mayor o igual que L; L-1 es la cardinalidad de $Z(\Gamma)$.

Si $m = L$, entonces:

$|A| \leq |C(x_L)| \leq |[x_1]| + |[x_2]| + \dots + |[x_m]|$, y ya habríamos terminado.

Si $m > L$, entonces $m \geq L + 1$.

Consideremos la gráfica G_Γ definida sobre los elementos de Γ como sigue, x, $y \in \Gamma$ son adyacentes en G_Γ si y sólo si $xy = yx$.

G_Γ es la *gráfica de conmutación* asociada a Γ.

$G_{\Gamma - Z(\Gamma)}$ es la subgráfica inducida por $\Gamma - Z(\Gamma)$.

Afirmación

$$G_{\Gamma - Z(\Gamma)} \text{ es } \sum_{i=L}^{m} |[x_i]| \text{ - coloreable.}$$

Para demostrar esta afirmación, se mostrarán las hipótesis del Corolario II. 8 (*i. e.* el número de vértices de grado mayor o igual que:

$$\sum_{i=L}^{m} |[x_i]|, \text{ es menor o igual que } \sum_{i=L}^{m} |[x_i]|).$$

Sea $y \in V(G_{\Gamma - Z(\Gamma)})$, entonces $\mathrm{val}(y) = |C(y)| - |Z(\Gamma)| - 1$.

$C(y)$ contiene a los vértices que conmutan con y; $|C(y)| - 1$ es el grado de y en G.

$$\text{Si } \mathrm{val}(y) \geq \sum_{i=L}^{m} |[x_i]| \Rightarrow |C(y)| - |Z(\Gamma)| - 1 \geq \sum_{i=L}^{m} |[x_i]|$$

$$\text{O bien } |C(y)| - 1 \geq |Z(\Gamma)| + \sum_{i=L}^{m} |[x_i]|$$

$$= |[x_1]| + |[x_2]| + \ldots + |[x_{L-1}]| + \ldots + |[x_m]| \geq |C(x_m)|.$$

$\therefore$ $|C(y)| - 1 \geq |C(x_m)|$, y, $|C(y)| > |C(x_m)|$, de donde:

$$|C(y)| = \frac{|\Gamma|}{|[y]|} > |C(x_m)| = \frac{|\Gamma|}{|[x_m]|}.$$

Por lo tanto $|[x_m]| > |[y]|$.

Por consiguiente "y" ha sido considerado entre $\sum_{i=1}^{m-1} |[x_i]|$ y se ha mostrado que $\sum_{i=1}^{m-1} |[x_i]|$ es una cota superior para el número de vértices de grado mayor o igual que $\sum_{i=1}^{m} |[x_i]|$.

Aplicando ahora el Corolario II. 8, se obtiene:

Los vértices de $G_\Gamma - Z(\Gamma)$ pueden $\sum_{i=1}^{m} |[x_i]|$ - colorearse y por lo tanto los vértices de G pueden $(|Z(\Gamma)| + \sum_{i=1}^{m} |[x_i]|)$ - colorearse esto es $\sum_{i=1}^{m} |[x_i]|$ - colorearse.

De aquí se concluye que todo clan en G_Γ tiene cardinalidad menor o igual que $\sum_{i=1}^{m} |[x_i]|$.

Por otra parte sabemos que todo subgrupo abeliano de Γ está inmerso en algún clan de G_Γ, lo que junto con lo anterior nos da la conclusión del teorema.

El siguiente ejemplo muestra que la igualdad puede ocurrir:

Sea M un grupo abeliano de orden impar, $2k - 1$ con $k \geq 2$.

Si x tiene orden 2 y satisface $xyx = y^{-1}$, para todo $y \in M$, entonces el grupo generado por x y M es el grupo diédrico generalizado. En el Ejemplo I. 24, se comenta ampliamente sobre este grupo.

Para $y = e$, $|[e]| = 1$. Y $|C(x)| = 2$, $C(x) = \{e, x\}$.

Como $|\Gamma| = 4k - 2$; $4k - 2 = |[x]||C(x)| = 2|[x]|$.

$$\therefore \qquad |[x]| = \frac{4k - 2}{2} = 2k - 1$$

$$\begin{array}{ccccccccccc} |[x_1]| & < & |[x_2]| & = & |[x_3]| & = & \ldots & = & |[x_{k-1}]| & < & |[x]| \\ 1 & + & 2 & + & 2 & + & \ldots & + & 2 & & + (2k-1) = 4k - 2. \end{array}$$

Así hay $(k - 1)$ clases de conjugación de cardinalidad 2. En este caso, el entero m del teorema es igual a k y se obtiene:

$$1 + 2 + \ldots + 2 = 1 + 2(k - 1) = 2k - 1 = |M|.$$

Notas.

Ejemplificaremos el Teorema cuando se trata de un grupo abeliano. En este caso, la *gráfica de conmutación* asociada a Γ es completa, por ejemplo, pensemos en $\Gamma = \mathbb{Z}_7$, el grupo cíclico con 7 elementos.

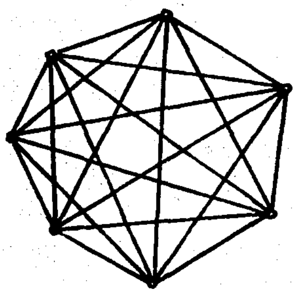
$$\Gamma = \{e, a, a^2, a^3, a^4, a^5, a^6\}.$$

$\forall\, x \in \Gamma$, $|[x]| = 1$, $C(x) = \Gamma$.

$$1 = |[e]| = |[a]| = \ldots = |[a^6]|.$$

$$|[e]| + |[a]| + \ldots + |[a^6]| \geq |C(a^6)| = |\Gamma| = 7.$$

$$\therefore \quad m = 7.$$



La grafica de conmutacion asociada a $\mathbb{Z}_7$.

Ahora ejemplificaremos el caso cuando Γ no sea abeliano. Consideremos $\Gamma = S_3$, el grupo de permutaciones en tres símbolos.

$S_3 = \{e, (2, 3), (1, 3), (1, 2), (1, 3, 2), (1, 3, 2)\}$. $|S_3| = 6$.

Las clases de conjugación son:

$[e] = \{e\}$.

$[(1, 2)] = \{(1, 2), (1, 3), (2, 3)\}$.

$[(1, 3, 2)] = \{(1, 2, 3), (1, 3, 2)\}$.

Los centralizadores en cada caso son:

$C(e) = S_3$. $C((1, 2)) = \{e, (1, 2)\}$.

$C((1, 3)) = \{e, (1, 3)\}$. $C((2, 3)) = \{e, (2, 3)\}$.

$C((1, 3, 2)) = \{e, (1, 3, 2), (1, 2, 3)\}$.

$C((1, 2, 3)) = \{e, (1, 2, 3), (1, 3, 2)\}$.

Indicamos sus clases de conjugación de acuerdo con su cardinalidad:

$$1 \leq |[e]| \leq |[(1,\ 3,\ 2)]| \leq |[(1,\ 2)]|.$$

$$2 \qquad \leq \qquad 3.$$

Calculamos *m*:

$$|[e]| + |[(1,\ 3,\ 2)]| \geq |C(1,\ 3,\ 2)|.$$

$$1 \quad + \quad 2 \quad \geq \quad 3.$$

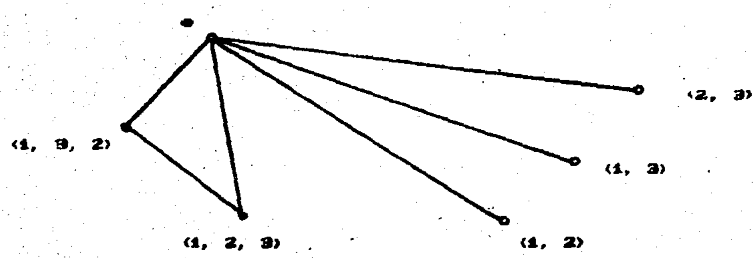
Por lo tanto *m* = 2.

Por lo tanto todo subgrupo abeliano de S_3 tiene cardinalidad menor o igual que 3: la suma de las cardinalidades de las dos primeras clases de conjugación.

Por el Tma. I. 17 sabemos que las posibles cardinalidades de los subgrupos de S_3 son 1, 2, 3 y 6. Pero S_3 no tiene ningún subgrupo abeliano de orden 6, pues sería él mismo, que no es abeliano.

S_3 también es un grupo diédrico D_3, y ejemplifica el refinamiento de la cota. Pues contiene un subgrupo abeliano de orden 3.

En este caso la *gráfica de conmutación* asociada a S_3 es:



SECCION B. CUBIERTAS DE GRUPOS MEDIANTE SUBGRUPOS ABELIANOS.

LEMA 1. Si el centro $Z(\Gamma)$ del grupo Γ es no trivial y $\Gamma = \bigcup x_i Z(\Gamma)$ es una descomposición en clases laterales de Γ, entonces $\Gamma = \bigcup \langle x_i Z(\Gamma)\rangle$ es una cubierta de Γ, donde $\langle x_i Z(\Gamma)\rangle$ son subgrupos abelianos.

Dem. $\langle x_i Z(\Gamma)\rangle \subseteq \Gamma$, $\forall\, x_i$, por lo tanto $\cup \langle x_i Z(\Gamma)\rangle \subseteq \Gamma$.

La otra inclusión: Sea $g \in \Gamma \Rightarrow g \in \langle gZ(\Gamma)\rangle$.
Por lo tanto $\Gamma \subseteq \cup \langle x_i Z(\Gamma)\rangle$.

Lo cual demuestra la igualdad.

Para mostrar que $\langle x_i Z(\Gamma)\rangle$ es abeliano, $\forall\, x_i \in \Gamma$:

Sea $x_i \in \Gamma$.
Consideremos $\langle x_i Z(\Gamma)\rangle$.
Sean $y_1, y_2 \in \langle x_i Z(\Gamma)\rangle$. P. d. $y_1 y_2 = y_2 y_1$.

$$y_1 = x_i^{j} z_1, \quad y_2 = x_i^{k} z_2, \text{ para alguna } z_1, z_2 \in Z(\Gamma);$$

$$j, k \in \{1, 2, 3, \ldots, |\Gamma|\}.$$

Entonces $y_1 y_2 = (x_i^{j} z_1)(x_i^{k} z_2) = x_i^{j}(x_i^{k} z_1) z_2 = x_i^{k} x_i^{j} z_1 z_2 =$

$$= (x_i^{k} z_2)(x_i^{j} z_1) = y_2 y_1.$$

Por lo tanto $\langle x_i Z(\Gamma)\rangle$ es abeliano.

En respuesta a una conjetura planteada por Erdös y Strauss en [5], Mason ha demostrado en [11] que aún cuando $|Z(\Gamma)| = 1$, Γ se puede cubrir con un número $\leq (\frac{1}{2}|\Gamma| + 1)$ de subgrupos abelianos de Γ.

Sea Γ un grupo y asociemos a él una "gráfica de conmutación" G_Γ como en la sección anterior.

$\alpha(G_\Gamma)$ denota el número de independencia.

Denotemos por $a(\Gamma)$ el mínimo número de subgrupos abelianos en cualquier colección, cuya unión sea igual a Γ.

El principio de las casillas (*Pigeonhole Principle. Ver:* [9], p. 110: *Si n objetos se distribuyen sobre m lugares y si n > m en-*

tonces algún lugar recibe al menos dos objetos, y nuestro comentario arriba implican:

$$\alpha(Gr) \leq a(\Gamma) \leq [\Gamma : Z(\Gamma)]$$

y por el resultado de Mason, $a(\Gamma) \leq \frac{1}{2}|\Gamma| + 1$.

Para la primera parte de la desigualdad, si x_1, $x_2 \in X$, con X conjunto independiente máximo en Gr, pertenecen entonces a subgrupos abelianos distintos en la cubierta de Γ.

Ahora $a(\Gamma) \leq [\Gamma : Z(\Gamma)]$, del hecho mencionado al inicio de la sección, explícitamente $\Gamma = \cup \langle x_i Z(\Gamma)$.

Si $k(\Gamma)$ denota el número de clases de conjugación de Γ y A es cualquier subgrupo abeliano de Γ, obtenemos el siguiente:

COROLARIO 2. a). $|\Gamma| \leq \alpha(Gr)\ k(\Gamma)$

b). $|A|^2 \leq k(\Gamma)\ |\Gamma|$

c). $|A|^2 \leq \alpha(Gr)\ k^2(\Gamma)$

En cada caso la igualdad se cumple si y sólo si Γ es abeliano y además $A = \Gamma$ en b) y c).

Dem. Si a) y b) son ciertas, tenemos:

$$|\Gamma| \leq \alpha(Gr)\ k(\Gamma) \quad \text{y} \quad |A|^2 \leq k(\Gamma)\ |\Gamma|.$$

Entonces $|A|^2 \leq k(\Gamma)\ k(\Gamma)\ \alpha(Gr) = k^2(\Gamma)\ \alpha(Gr)$ que es la afirmación en c).

Para demostrar a), usaremos el Corolario II. 10 y contaremos las aristas de Gr. En Gr, $x \in \Gamma$, val $= |C(x)| - 1$.

Así que $2|E(Gr)| = \sum_{v \in G} \text{val}\ (v) = \sum_{x \in \Gamma} (|C(x)| - 1) =$

$$= (|C(x_1)| - 1) + \ldots + (|C(x_n)| - 1) =$$

$$= |C(x_1)| + \ldots + |C(x_n)| - |\Gamma| = \sum_{\substack{\text{CLASES}\\ \text{DISTINTAS}}} (|[x]|\,|C(x)|) - |\Gamma|$$

Esta última igualdad se obtiene al usar de nuevo el Tma. I. 18, mediante la asociación de los elementos que pertenecen a la misma clase de conjugación, ya que la igualdad implica que sus centralizadores tienen la misma cardinalidad.

Usando la definición de $k(\Gamma)$, se puede escribir como:

$$\sum_{\substack{\text{CLASES}\\ \text{DISTINTAS}}} (|[x]|\,|C(x)|) - |\Gamma| = k(\Gamma)|\Gamma| - |\Gamma| = (k(\Gamma) - 1)|\Gamma|$$

Sabemos del Corolario I. 10 que:

$$\alpha(Gr) \geq \frac{|V(Gr)|^2}{|V(Gr)| + 2|E(Gr)|}$$

y que la igualdad se obtiene si y sólo si Gr es unión ajena de clanes de la misma cardinalidad.

Así obtenemos:

$$\alpha(Gr) \geq \frac{|V(Gr)|^2}{(|V(Gr)| + (k(\Gamma) - 1)|\Gamma|} = \frac{|\Gamma|^2}{|\Gamma| + k(\Gamma)|\Gamma| - |\Gamma|} =$$

$$= \frac{|\Gamma|^2}{k(\Gamma)|\Gamma|} = \frac{|\Gamma|}{k(\Gamma)}$$

Por lo tanto $|\Gamma| \leq k(\Gamma)\,\alpha(Gr)$ que es la afirmación en a).

El Corolario I. 10 garantiza que la igualdad se obtiene si y sólo si Gr es la unión ajena de clanes de la misma cardinalidad, por lo tanto la igualdad en a) se cumple si y sólo si Gr es una gráfica completa, en cuyo caso todos los elementos en Γ conmutan, lo que implica que Γ es abeliano.

Para demostrar b), podemos suponer que A es un subgrupo abeliano máximo. Si sumamos sobre las $k_\Gamma(A)$ clases $[a]$ en Γ, con $a \in A$, tenemos:

$$|A| \overset{(1)}{=} \sum |[a] \cap A| \overset{(2)}{\leq} \max_{a \in A} |[a]|kr(A)| \overset{(3)}{\leq} \frac{|\Gamma|k(\Gamma)}{\min\limits_{a \in A} |C(a)|} \overset{(4)}{\leq} \frac{|\Gamma|k(\Gamma)}{|A|}$$

Notas.

(1) resulta de contar los elementos de A que se encuentran en las distintas clases de conjugación, pues $A = \bigcup ([a] \cap A)$. Si hay $kr(A)$ distintas clases y de éstas, elegimos la de cardinalidad máxima, obtenemos una cota superior para $|A|$, así se obtiene (2). Como $|\Gamma| = |[x]||C(x)|$, $|[a]|$ será máxima, si $|C(a)|$ es mínima, así para (3), elegimos $a \in A$ tal que $|C(a)|$ sea mínima. Por último, como A es subgrupo abeliano, entonces:

$$A \subseteq C_\Gamma(a),\ \forall\ a \in A.$$

$$A \subseteq \min_{a \in A} C_\Gamma(a).$$

Por lo tanto $|A| \leq \min\limits_{a \in A} |C_\Gamma(a)| \Rightarrow \dfrac{1}{\min\limits_{a \in A} |C_\Gamma(a)|} \leq \dfrac{1}{|A|}$

$$\frac{|\Gamma|k(\Gamma)}{\min\limits_{a \in A} |C_\Gamma(a)|} \leq \frac{|\Gamma|k(\Gamma)}{|A|}.$$

Así de (1) y de (4), obtenemos:

$|A|^2 \leq |\Gamma|\ k(\Gamma)$, que es la afirmación en b).

Supongamos Γ abeliano y $A = \Gamma$, entonces $k(\Gamma) = |\Gamma|$. Por tanto $|A|^2 = |\Gamma|^2$ y se tiene la igualdad.

Supongamos ahora que tenemos la igualdad, es decir, $|A|^2 = |\Gamma|k(\Gamma)$.

Entonces $\forall\ a,\ b \in A$, $|[a]| = |[b]|$, de la sucesión de desigualdades anteriores.

En particular $|[e]| = 1$, pues $e \in A$.

$$\therefore\ |[a]| = |[e]|.$$

$$|[\alpha]| = 1 \Rightarrow \alpha \in Z(\Gamma).$$

$A \subseteq Z(\Gamma)$. Pero A es subgrupo abeliano máximo

$$\therefore Z(\Gamma) = A.$$

Por otra parte $\alpha \in A = Z(\Gamma)$ si y sólo si $C(\alpha) = |\Gamma|$.

Como estamos suponiendo la igualdad, se tiene:

$$|A| = \max_{\alpha \in A} |[\alpha]| \, k_\Gamma(A) = \frac{|\Gamma| \, k(\Gamma)}{\min_{\alpha \in A} |C_\Gamma(\alpha)|} = \frac{|\Gamma| k(\Gamma)}{|A|}$$

De lo anterior, se obtiene:

$$\max_{\alpha \in A} \left\{ |[\alpha]| \right\} = 1 \qquad \text{y} \qquad \min_{\alpha \in A} \left\{ |C_\Gamma(\alpha)| \right\} = |\Gamma|$$

$$\therefore \qquad |A| = k_\Gamma(A) = \frac{|\Gamma| k(\Gamma)}{|A|} = \frac{|\Gamma| k(\Gamma)}{|A|}$$

y de ésta $k(\Gamma) = \dfrac{|\Gamma| k(\Gamma)}{|A|}$ o bien $\dfrac{|\Gamma|}{|A|} = 1$.

$\therefore |\Gamma| = |A|$, $\therefore \Gamma$ es abeliano, lo cual demuestra b).

NOTAS.

Haciendo uso de a), podemos producir una cota inferior para $\alpha(\Gamma)$, y de aquí una para $a(\Gamma)$, si tenemos una cota superior para $k(\Gamma)$. Por ejemplo, si q es potencia de un primo, mayor o igual a 4, puede comprobarse que todo grupo simple $\Gamma \in \{PSL\ (2,q)\}$ ver [8] satisface:

$$c_1 |\Gamma|^{1/2} < k(\Gamma) \leq c_2 |\Gamma|^{1/2}, \text{ donde } c_1 = \left(\frac{1}{4}\right)^{1/2} \text{ y } c_2 = \left(\frac{25}{12}\right)^{1/2}.$$

GL(2, q) denota el grupo de matrices no singulares de 2 x 2 con entradas en un campo finito con q elementos. Este grupo es conoci-

do como el grupo lineal general (en dimensión 2). Al subgrupo que consta de las matrices con determinante 1 se le llama grupo especial lineal y se denota como SL(2, q). El centro de GL(2, q) consiste de matrices escalares y al grupo cociente correspondiente PGL(2, q) se le denomina el grupo lineal proyectivo.
Finalmente, la imagen PSL(2, q) de SL(2, q) en PGL(2, q) se conoce como el grupo lineal especial proyectivo.

Si Γ es simple, $\Gamma \in \{PSL(2, q)\}$ entonces

$$\left(\frac{1}{4}\right)^{1/2}|\Gamma|^{1/2} < k(\Gamma) \le \left(\frac{25}{12}\right)^{1/2}|\Gamma|^{1/2}$$

$\therefore$ $k(\Gamma) \le \left(\frac{25}{12}\right)^{1/2}|\Gamma|^{1/2}$ y usando el inciso $a)$ se tiene:

$$|\Gamma| \le \alpha(\Gamma) \left(\frac{25}{12}\right)^{1/2} |\Gamma|^{1/2}$$

$$\therefore \qquad \left(\frac{12}{25}\right)^{1/2}|\Gamma|^{1/2} \le \alpha(\Gamma)$$

Como $\alpha(\Gamma) \le \alpha(\Gamma)$ sabemos que Γ no puede cubrirse con la unión de menos de $\left(\frac{12}{25}\right)^{1/2}|\Gamma|^{1/2}$ subgrupos abelianos.

También $k(\Gamma) \le c2|\Gamma|^{1/2}$ y por lo tanto $\alpha(\Gamma) \ge \left(\frac{12}{25}\right)^{1/2}|\Gamma|$ para todos los grupos simples no abelianos finitos, $\Gamma \in \{PSL(2, q)\}$.

Por otra parte, Bertram en [2] ha demostrado que para cada $\varepsilon > 0$ fija, casi todos los enteros $n \le x$, cuando $x \to \infty$, tienen la propiedad de que $k(\Gamma) > |\Gamma|^{1-\varepsilon}$ para cada grupo Γ de orden n.

En el Tma. 4 se mostrará que si el grupo Γ contiene un subgrupo propio "*cerrado bajo centralizadores*", entonces $\alpha(\Gamma) \ge [\,|\Gamma|^{1/2}]$ (función máximo entero).

Respecto al inciso *b*), consideremos los grupos diédricos D_n.

Sabemos que $|D_n| = 2n$ y del Ejemplo I. 24, las clases de conjugación son:

i). Si n es impar, $n = 2t - 1$, $y \in Y = \langle y \rangle$, las clases de conjugación son:

$$[e],\ [y],\ [y^2],\ \ldots,\ [y^{t-1}] \text{ con } |[e]| = 1,\ |[y^j]| = 2,$$

$1 \leq j \leq t - 1$.

Como $C(x) = \{e, x\}$, $|C(x)| = 2$, y $|D_n| = 2n = |[x]|\,|C(x)|$ $\Rightarrow$ $|[x]| = n$.

$D_n = [e] \cup [y] \cup \ldots [y^{t-1}] \cup [x]$.

$\therefore$ hay $(t + 1)$ clases de conjugación.

Como $n = 2t - 1$, $t = \dfrac{n+1}{2}$.

$$k(D_n) = t + 1 = \frac{(n+1)}{2} + 1 = \frac{n+3}{2} = \frac{n}{2} + \frac{3}{2}.$$

En cada caso existe un subgrupo abeliano A de orden n, así que:

$$\therefore \lim_{n \to \infty} \frac{(n/2 + 3/2)2n}{n^2} = \lim_{n \to \infty} \frac{(n+3)n}{n^2} = 1.$$

Si la n es par, $k(D_n) = \dfrac{n}{2} + 3$.

$$\therefore \lim_{n \to \infty} \frac{(n/2 + 2)\, 2n}{n^2} = \lim_{n \to \infty} \frac{(n+4)n}{n^2} = 1$$

$$\therefore \lim \frac{k(D_n)\ |D_n|}{|A|^2} = 1.$$

Por último, los grupos D_n con n impar muestran que $\alpha(\Gamma) = a(\Gamma) = \frac{1}{2}|\Gamma| + 1$ puede ocurrir.

Sea $A \subset D_n$, $A = \{x, y, xy, \ldots, xy^{n-1}\}$; $|A| = n + 1$.

Los elementos de A no conmutan por parejas. Claramente A es un conjunto independiente máximo.

$$\therefore \alpha(D_n) = n + 1.$$

Como $\alpha(D_n) \leq \alpha(D_n) \leq \frac{1}{2}|D_n| + 1$ se obtiene:

$$n + 1 \leq \alpha(D_n) \leq \frac{1}{2}(2n) + 1 = n + 1.$$

$$\therefore \alpha(D_n) = \alpha(D_n) = \frac{1}{2}|D_n| + 1 = \frac{1}{2}|\Gamma| + 1$$

De hecho cualquier grupo no abeliano en el que todos los centralizadores (excepto Γ) son abelianos, satisfacen $\alpha(\Gamma) = \alpha(\Gamma)$.

Para aclarar esto, supongamos que Γ no es abeliano y tiene la propiedad de que todos sus subgrupos centralizadores (a excepción de él) son abelianos.

Supongamos $\alpha(\Gamma) = \delta$.

Sea $A = \{g_1, g_2, \ldots, g_\delta\}$un conjunto independiente máximo de elementos de Γ.

Como cada $x \in \Gamma$ es tal que $\exists\, g_i \in A$ y $xg_i = g_ix$, $x \in C(g_i)$. por lo tanto:

$|\Gamma| = \bigcup_{i=1}^{\delta} C(g_i)$ y así obtenemos una cubierta de Γ con subgrupos abelianos, $\therefore \alpha(\Gamma) \leq \alpha(\Gamma)$.

Como siempre se tiene $\alpha(\Gamma) \leq \alpha(\Gamma)$, obtenemos:

$$\alpha(\Gamma) = \alpha(\Gamma).$$

Sin embargo, la condición de que todos los centralizadores sean abelianos, no es necesaria. Consideremos S_4, el grupo simétrico en 4 símbolos, {1, 2, 3, 4}.

S_4 = { e, (34), (23), (234), (243), (24), (12), (12)(34),(1243), (124), (123), (1234), (132), (1342), (13), (134), (13)(24), (1324), (1432), (142), (14), (143), (1423), (14)(23)}.

$\alpha(S_4) = \alpha(S_4)$, pero el centralizador de la permutación (12)(34) no es abeliano.

C((12)(34)) = {e, (12), (34), (12)(34), (1324), (1423), (14)(23)}.

Se puede comprobar que x = (13)(24) y y = (12) no conmutan.

$\therefore$ C((12)(34)) no es abeliano.

Tomemos:

$A_1 = \langle(1234)\rangle$ $A_2 = \langle(1324)\rangle$ $A_3 = \langle(1243)\rangle$ $A_4 = \langle(123)\rangle$
$A_5 = \langle(124)\rangle$ $A_6 = \langle(134)\rangle$ $A_7 = \langle(234)\rangle$
A_8 = {(12), (34), (12)(34), e} A_9 = {(13), (24), (13)(24), e}
A_{10} = {(14), (23), (14)(23), e}.

$\bigcup A_i$ es una cubierta para S_4, donde los A_i son subgrupos abelianos que se intersectan por pares sólo en la identidad.

$A_1 = \langle(1234)\rangle$ = {(1234), (13)(24), (1432), e}.
$A_2 = \langle(1324)\rangle$ = {(1324), (12)(34), (1423), e}.
$A_3 = \langle(1243)\rangle$ = {(1243), (14)(23), (1342), e}.
$A_4 = \langle(123)\rangle$ = {(123), (132), e}.
$A_5 = \langle(124)\rangle$ = {(124), (142), e}.
$A_6 = \langle(134)\rangle$ = {(134), (143), e}.
$A_7 = \langle(234)\rangle$ = {(234), (243), e}.
A_8 = {(12), (34), (12)(34), e}.
A_9 = {(13), (24), (13)(24), e}.
A_{10} = {(14), (23), (14)(23), e}.

Todos son abelianos por ser a lo más de orden 4.

Por inspección obtenemos que $\bigcup A_i$ es una cubierta de S_4 y que sólo se intersectan por pares en la identidad.

$\therefore \quad \alpha(\Gamma) \leq 10.$

Consideremos ahora:

$$H = \{(1234), (1324), (1243), (123), (124), (134), (234), (12), (13), (14)\}.$$

Se puede comprobar que H es un conjunto independiente, *i. e.* estas permutaciones no conmutan por pares.

$$\therefore \quad 10 \leq \alpha(\Gamma)$$

$$\therefore \quad 10 \leq \alpha(\Gamma) \leq a(\Gamma) \leq 10.$$

$$\therefore \quad \alpha(S_4) = a(S_4) = 10.$$

$\therefore$ la condición de que todos los centralizadores sean abelianos no es necesaria.

LEMA 3. Sea Γ un grupo finito no abeliano tal que:

$$\alpha(\Gamma) \leq |\Gamma|^r - 1, \; 0 < r < 1, \text{ entonces:}$$

a) $\forall\, g \in \Gamma$, $|C(g)| \geq |\Gamma|^{(1-r)/2}$

b) $\exists\; g \in (\Gamma - Z(\Gamma))$ que satisface $|C(g)| > |\Gamma|^{1-r}$ y $|C(x) \cap C(g)| > |\Gamma|^{(1-3r)/2}$, $\forall\, x \in \Gamma$.

c) En todo grupo finito Γ, al menos $(k(\Gamma) - \alpha(\Gamma))$ de las distintas clases de conjugación en Γ satisfacen la condición:

$$|[x]| < |\Gamma|^{1/2}.$$

Dem.

a). En la gráfica G_Γ, el grado de cada vértice x es:

$$\text{val}(x) = |C(x)| - 1, \text{ de donde } |C(x)| = \text{val}(x) + 1.$$

Del Tma. I. 10:

$$\alpha(G_\Gamma) \geq \sum_{v \in \Gamma} \frac{1}{\text{val}(x) + 1} = \sum_{v \in \Gamma} \frac{1}{|C(x)|}$$

Como $|C(x)| = \dfrac{|\Gamma|}{|[x]|}$ es un invariante de clase:

$$\alpha(\Gamma) \geq \sum_{x \in \Gamma} \frac{1}{|C(x)|} = \sum_{x \in \Gamma} \frac{|[x]|}{|\Gamma|} = \frac{1}{|\Gamma|} \sum_{x \in \Gamma} |[x]| =$$

$$= \frac{1}{|\Gamma|} \sum_{x \in \Gamma} (|[x_1]| + \ldots + |[x_n]|) = \frac{1}{|\Gamma|} \sum_{\substack{\text{CLASES} \\ \text{DISTINTAS}}} |[x]|^2$$

La última igualdad se obtiene de asociar las clases de conjugación con la misma cardinalidad. En el caso de x_i, hay $|[x_i]|$ conjugados y sus clases tienen la cardinalidad $|[x_i]|$.

$$\frac{1}{|\Gamma|} \sum_{\substack{\text{CLASES} \\ \text{DISTINTAS}}} |[x]|^2 \leq \alpha(\Gamma) < |\Gamma|^r.$$

$$\therefore \quad \alpha(\Gamma) < |\Gamma|^r \text{ ya que } \alpha(\Gamma) \leq |\Gamma|^r - 1$$

$$\therefore \quad \sum_{\substack{\text{CLASES} \\ \text{DISTINTAS}}} |[x]|^2 < |\Gamma|^{r+1}$$

de donde cada sumando, $|[x]|^2 < |\Gamma|^{r+1}$, por lo tanto:

$$|[x]| < |\Gamma|^{(r+1)/2}$$

Como $|[x]| = \dfrac{|\Gamma|}{|C(x)|} < |\Gamma|^{(r+1)/2}$,

$$|C(x)| > \frac{|\Gamma|}{|\Gamma|^{(r+1)/2}} = |\Gamma|^{1-(r+1)/2} = |\Gamma|^{(1-r)/2}.$$

Por lo tanto $|C(x)| > |\Gamma|^{(1-r)/2}$.

Para demostrar *b*), tenemos que:

$$\alpha(\Gamma) \geq \sum_{x \in \Gamma} \frac{1}{|C(x)|} = \sum_{x \in \Gamma - Z(\Gamma)} \frac{1}{|C(x)|} + \sum_{x \in Z(\Gamma)} \frac{1}{|C(x)|} =$$

$$= \sum_{x \in \Gamma - Z(\Gamma)} \frac{1}{|C(x)|} + \sum_{x \in Z(\Gamma)} \frac{1}{|\Gamma|} =$$

$$= \sum_{x \in \Gamma - Z(\Gamma)} \frac{1}{|C(x)|} + \frac{1}{|\Gamma|} \sum_{x \in Z(\Gamma)} 1 = \frac{|Z(\Gamma)|}{|\Gamma|} + \sum_{x \in \Gamma - Z(\Gamma)} \frac{1}{|C(x)|}$$

Si la afirmación fuera falsa, tendríamos $|C(x)| \leq |\Gamma|^{1-r}$, para toda $x \in \Gamma - Z(\Gamma)$.

Como $\alpha(\Gamma) \geq \dfrac{|Z(\Gamma)|}{|\Gamma|} + \displaystyle\sum_{x \in \Gamma - Z(\Gamma)} \frac{1}{|C(x)|}$ y $\alpha(\Gamma) \leq |\Gamma|^{r} - 1$

por hipótesis, obtenemos:

$$\sum_{x \in \Gamma - Z(\Gamma)} \frac{1}{|C(x)|} \leq \alpha(\Gamma) - \frac{|Z(\Gamma)|}{|\Gamma|} \leq |\Gamma|^{r} - 1 - \frac{|Z(\Gamma)|}{|\Gamma|}$$

y $\displaystyle\sum_{x \in \Gamma - Z(\Gamma)} \frac{1}{|C(x)|} \geq \sum_{x \in \Gamma - Z(\Gamma)} \frac{1}{|\Gamma|^{1-r}} = \frac{|\Gamma| - |Z(\Gamma)|}{|\Gamma|^{1-r}}$

pues $|\Gamma - Z(\Gamma)| = |\Gamma| - |Z(\Gamma)|$.

$$\therefore \frac{|\Gamma| - |Z(\Gamma)|}{|\Gamma|^{1-r}} \leq |\Gamma|^{r} - 1 - \frac{|Z(\Gamma)|}{|\Gamma|}$$

de donde,

$$1 \leq |\Gamma|^{r} - \frac{|Z(\Gamma)|}{|\Gamma|} + \frac{|Z(\Gamma)| - |\Gamma|}{|\Gamma|^{1-r}} =$$

$$= |\Gamma|^r - \frac{|Z(\Gamma)|}{|\Gamma|} + \frac{|Z(\Gamma)|}{|\Gamma|^{1-r}} - \frac{|\Gamma|}{|\Gamma|^{1-r}} = |Z(\Gamma)|\left(\frac{1}{|\Gamma|^{1-r}} - \frac{1}{|\Gamma|}\right)$$

De nuestra suposición tenemos que $|C(x)| \leq |\Gamma|^{1-r}$ y del hecho $Z(\Gamma) = \bigcap_{x \in \Gamma} C(x)$, obtenemos $|Z(\Gamma)| \leq |C(x)| \leq |\Gamma|^{1-r}$

$$\therefore 1 \leq |Z(\Gamma)| \left(\frac{1}{|\Gamma|^{1-r}} - \frac{1}{|\Gamma|}\right) \leq |\Gamma|^{1-r}\left(\frac{1}{|\Gamma|^{1-r}} - \frac{1}{|\Gamma|}\right)$$

$$\therefore \quad 1 \leq 1 - \frac{1}{|\Gamma|^r} \quad \text{y} \quad \frac{1}{|\Gamma|^r} \leq 0$$

CONTRADICCION!!!

$$\therefore \exists\, g \in (\Gamma - Z(\Gamma)) \text{ tal que } |C(g)| > |\Gamma|^{1-r}$$

Como $C(g)$ y $C(x)$ son subgrupos de Γ, $\forall\, x \in \Gamma$, tenemos:

$|C(g) \cap C(x)| \geq \dfrac{|C(g)|\,|C(x)|}{|\Gamma|}$ y de la parte *a*) del Lema:

$$|C(x)| \geq |\Gamma|^{(1+r)/2}$$

$$\therefore |C(g) \cap C(x)| \geq \frac{|C(g)|}{|\Gamma|}|C(x)| \geq \frac{|C(g)|}{|\Gamma|}|\Gamma|^{(1+r)/2}$$

$$\frac{|\Gamma|^{1-r}|\Gamma|^{(1+r)/2}}{|\Gamma|} = |\Gamma|^{(1-3r)/2}$$

$\therefore$ $|C(g) \cap C(x)| > |\Gamma|^{(1-3r)/2}$, para alguna $g \in (\Gamma - Z(\Gamma))$ y $|C(g)| > |\Gamma|^{1-r}$

Para demostrar *c*), sea $L(\Gamma)$ el número de clases distintas de Γ que satisfacen $|[x]|^2 < |\Gamma|$.

Entonces $(k(\Gamma) - L(\Gamma))$ clases satisfacen $|[x]|^2 \geq |\Gamma|$.

$$\therefore \quad |\Gamma|(k(\Gamma) - \mathcal{L}(\Gamma)) \leq \sum_{\substack{\text{CLASES} \\ \text{DISTINTAS}}} |[x]|^2$$

Por lo tanto usando la demostración en $a)$, (pag. 71) se tiene:

$$|\Gamma|(k(\Gamma) - \mathcal{L}(\Gamma)) \leq \sum_{\substack{\text{CLASES} \\ \text{DISTINTAS}}} |[x]|^2 \leq |\Gamma|\ \alpha(\Gamma)$$

$\therefore\ k(\Gamma) - \mathcal{L}(\Gamma) \leq \alpha(\Gamma)$ $\qquad\qquad$ $\therefore k(\Gamma) - \alpha(\Gamma) \leq \mathcal{L}(\Gamma)$.

Del Lema 3b), tenemos que si $|[x]| \geq |\Gamma|^r$, para toda clase no central $[x]$, entonces $\alpha(\Gamma) \geq [\,|\Gamma|^r]$, esto es: $\alpha(\Gamma) \geq \min\limits_{x \in Z(\Gamma)} |[x]|$.

Para deducir esto, supóngase que: $|[x]| \geq |\Gamma|^r$, $\forall\ x \in \Gamma - Z(\Gamma)$.

Como $|\Gamma| = |[x]|\,|C(x)|$, se tiene: $|[x]| = \dfrac{|\Gamma|}{|C(x)|} \geq |\Gamma|^r$,

$\dfrac{1}{|C(x)|} \geq |\Gamma|^{r-1}$ $\quad \therefore |C(x)| \leq \dfrac{1}{|\Gamma|^{r-1}} = |\Gamma|^{1-r}$ lo cual muestra

incompatibilidad con $a)$, $\therefore$ no se cumple $\alpha(\Gamma) \leq |\Gamma|^r - 1$, sino $\alpha(\Gamma) > |\Gamma|^r - 1$, o bien $\alpha(\Gamma) \geq [\,|\Gamma|^r]$.

$$\therefore\ \alpha(\Gamma) \geq \min_{x \in Z(\Gamma)} |[x]|.$$

Si tomamos $r = \frac{1}{2}$ arriba, el **Lema** 3 c). da $\alpha(\Gamma) \geq k(\Gamma) - Z(\Gamma)$.

De este mismo Lema, sabemos que $\mathcal{L}(\Gamma) = k(\Gamma) - \alpha(\Gamma)$ de las distintas clases de conjugación satisfacen $|[x]| < |\Gamma|^{1/2}$, o bien $\mathcal{L}(\Gamma) \geq k(\Gamma) - \alpha(\Gamma)$ y $\alpha(\Gamma) \geq k(\Gamma) - \mathcal{L}(\Gamma)$, y como $\mathcal{L}(\Gamma)$ son los elementos centrales, $\mathcal{L}(\Gamma) = |Z(\Gamma)|$.

$$\therefore\ \alpha(\Gamma) \geq k(\Gamma) - |Z(\Gamma)|.$$

Pero en tales grupos, ver [9] $|\Gamma|^{1/2} \leq \dfrac{|\Gamma| - |Z(\Gamma)|}{k(\Gamma) - |Z(\Gamma)}$ así que:

$$k(\Gamma) - |Z(\Gamma)| < |\Gamma|^{1/2}.$$

Por lo tanto el **Lema 3c).** no proporciona una cota inferior para $\alpha(\Gamma)$, si $r = \frac{1}{2}$.

Trabajaremos ahora con "*grupos que contienen un subgrupo propio M cerrado bajo centralizadores*", esto es $\forall\ x \in M - \{e\}$, $C(x) \subseteq M$. Algunos ejemplos de esta situación son todos los grupos simples $PSL(2, p)$, $PSL(2, 2)$ y otros PSL. El grupo S_3 es un ejemplo de una situación así. En este caso, el centralizador de la permutación $(1,3,2)$ es un subgrupo cerrado bajo centralizadores.

Tma. 4. Sea Γ un grupo que contiene un subgrupo propio M tal que $\forall\ x \in M - \{e\}$, $C_\Gamma(x) \subseteq M$. Entonces $\alpha(\Gamma) \geq [\,|\Gamma|^{1/3}]$, donde $[r]$ denota la función máximo entero menor o igual que r.

Dem. (Por contradicción).

Supongamos $\alpha(\Gamma) < [\,|\Gamma|^{1/3}] \Rightarrow \alpha(\Gamma) \leq |\Gamma|^{1/3} - 1$.

Hagamos $r = \frac{1}{3}$ en el **Lema 3.**

De *b)* tenemos: $\exists\ g \in \Gamma - Z(\Gamma)$ tal que $|C(g)| > |\Gamma|^{1-1/3=2/3}$, y:

$$|C(x) \cap C(g)| > |\Gamma|^0 = 1,\ \forall\ x \in \Gamma.$$

Se mostrará que esto contradice nuestra hipótesis sobre el subgrupo M.

1. Sea $g \in M - \{e\}$, y, $x \notin M$.

   Si $y \in M - \{e\}$ obtenemos $y \notin C(x)$, pues si $y \in C(x) \Rightarrow yx = xy$. Por lo tanto $x \in C(y) \subseteq M$.

   $$\therefore\ x \in M.$$

   CONTRADICCION!!

   Si $y \in \Gamma - M$ entonces $y \notin C(g)$.

2. Supongamos $g \notin M$, y, $x \in M - \{e\}$.

   Si $y \in (\Gamma - M)$ obtenemos $y \notin C(x)$, pues si $y \in C(x)$, como $C(x) \subset M$, tendríamos $y \in M$.

   CONTRADICCION!!

Mientras que $y \in M - \{e\}$ implica $y \notin C(g)$.

$\therefore$ se tiene la conclusión del Teorema.

Corolario 5. Sea p un primo que divide el orden del grupo Γ, donde Γ no es abeliano. Si existe $x \in \Gamma$ tal que $|C(x)| = p$ entonces $\alpha(\Gamma) \geq [\,|\Gamma|^{1/2}]$.

Dem.

Sea Γ un grupo no abeliano. $|\Gamma| = np$.

Supongamos que $\exists\ x \in \Gamma$ tal que $|C(x)| = p$.

Entonces $C(x) = M$ es un subgrupo propio abeliano (pues su orden es primo).

Entonces $\forall\ y \in C(x) - \{e\}$, $C(y) \subseteq C(x)$.

Entonces $\alpha(\Gamma) \geq [\,|\Gamma|^{1/2}]$ por el **Tma. 4.**

Nota.

Isaacs en [13] ha demostrado que el Corolario 5 tiene una demostración directa de la Teoría de Grupos. A continuación se incluye la prueba.

Dem.

Sea $P = \langle x \rangle$, el subgrupo cíclico de orden p generado por x.

Como $P = C_\Gamma(P)$, P es un p-subgrupo de Sylow, *i. e.* $p^2 \nmid |\Gamma|$.

$P \leq P'$ con P' p-subgrupo de Sylow de Γ. Ahora para un p-subgrupo $Z(P') \neq e$.

$$\therefore Z(P') \subset N(x) = \langle x \rangle.$$

$\therefore x \in Z(P')$ $\qquad\qquad$ $\therefore P' \subset N(x)$, una contradicción.

$\therefore$ P es un p-subgrupo de Sylow de Γ.

También $N_\Gamma(P)/C_\Gamma(P)$ es isomorfo a un subgrupo del grupo de automorfismos de P, un grupo cíclico de orden $p - 1$.

Entonces $|\Gamma| = p[\Gamma:N][N:P] = pme$, donde $m = [\Gamma:N]$ y $e \mid p - 1$.

Como cualquier colección de m elementos distintos de la identidad, elegidos cada uno de los m conjugados de P, son parejas que no conmutan, tenemos $\alpha(\Gamma) \geqslant m$.

Si el Teorema fuera falso, entonces $\alpha^3(\Gamma) < |\Gamma|$, así que $m^3 < |\Gamma|$, $m^2 < pe < p^2$, y, $m < p$.

Por Sylow $m \equiv 1 \pmod p$, así que $m = 1$, y, $p < pe = |\Gamma| < p^2$.

También P es un subgrupo normal de Γ con $\Gamma/P = \mathrm{Nr}(P)/P$, un grupo cíclico.

Sea q un número primo, $q|e$, y supongamos que Q es un subgrupo de Γ con $|Q| = q$.

Si $x \in P$, y, $x^{-1}Qx = Q$ entonces $\forall$ $y \in Q$, $(x^{-1}y^{-1}x)y \in Q$, y $x^{-1}(y^{-1}xy) \in P$, ya que P es normal.

Por tanto $x^{-1}y^{-1}xy \in P \cap Q = \{e\}$ o $y \in C(x)$, lo que contradice que $C(P) = P$.

Por lo tanto $p \nmid |\mathrm{Nr}(Q)|$, así que $p \nmid [\Gamma:\mathrm{Nr}(Q)]$, y Q tiene al menos p conjugados, digamos $Q_1, Q_2, \ldots, Q_p$, con $Q_i = \langle x_i \rangle$. Si ningún par x_i, x_j conmuta, entonces $\alpha(\Gamma) \geq p > |\Gamma|^{1/2}$.

Si x_i y x_j conmutan, entonces:

$H = \langle x_i, x_j \rangle$ es abeliano, pero como $x_i \notin \langle x_j \rangle$, H no es cíclico de orden q^2.

Como $H \cap P = \{e\}$, $H \cong HP/P \leq \Gamma/P$, que es cíclico.

Lo cual es una contradicción.

En 1975 Erdös propuso el problema de encontrar una cota superior para $\alpha(\Gamma)$ en términos de $\alpha(\Gamma)$, donde el último es finito. Isaacs en [ ] demuestra el siguiente:

Tma. 6. Definimos una función $f(n)$ inductivamente como $f(1) = 1$ y $f(n) = n + \binom{n}{2} f(n-1)$. Si $\alpha(\Gamma) < \infty$, entonces $\alpha(\Gamma) \leq f(\alpha(\Gamma))$; en particular $\alpha(\Gamma) < \infty$.

Dem. Sea $\alpha(\Gamma) = \beta$.

Si x, $y \in \Gamma$, y. $xy \neq yx$, y $c_1, c_2, \ldots, c_\beta \in C(x) \cap C(y)$ entonces dos de los elementos: x, c_1y, $c_2y, \ldots, c_\beta y$ deben conmutar.

Pues aquí hay $(\beta + 1)$ elementos y no pueden formar un conjunto independiente.

Como x no conmuta con ninguno de los c_jy, ($xc_jy = c_jyx \Rightarrow c_jxy = c_jyx$!!), entonces dos de los últimos deben conmutar y por lo tanto dos de los c_i deben conmutar (pues se eligieron β elementos de $C(x) \cap C(y)$ que no forman un conjunto independiente).

De aquí $\alpha(C(x) \cap C(y)) < \alpha(\Gamma)$, si $xy \neq yx$.

Sean ahora $x_1, x_2, \ldots, x_\beta$ elementos que por parejas no conmutan y sea $B_{jk} = C(x_j) \cap C(x_k)$, con $j \neq k$.

Entonces $\alpha(B_{jk}) < \alpha(\Gamma)$, así que haciendo inducción sobre α (y usando el hecho de que f es monótona), concluimos que B_{jk} es la unión de a los más $f(\alpha - 1)$ subgrupos abelianos.

Sea ahora $A_j = C(x_j) - \bigcup_{k \neq j} B_{jk}$.

Como $\Gamma = \bigcup_{1\leq j\leq\beta} C(x_j) = \bigcup_{1\leq j\leq\beta} \langle A_j\rangle \cup \bigcup_{j,k} B_{jk}$, una vez que demostremos

que cada $\langle A_j\rangle$ es abeliano, habremos demostrado que:

$$\alpha(\Gamma) < \beta + \binom{\beta}{2} f(\beta - 1) = f(\alpha(\Gamma)).$$

Para demostrar que cada $\langle A_j\rangle$ es abeliano, sean u, $v \in A_j$. Entonces $x_1, x_2, \ldots, x_{j-1}, u, x_{j+1}, \ldots, x_\beta$ son β elementos que no conmutan por parejas, así que v debe conmutar con alguno de ellos. Por tanto v conmuta con u y $\langle A_j\rangle$ es abeliano.

Isaacs también deduce que $\alpha(\Gamma) = 2n + 1$ si Γ es extra especial de orden 2^{2n+1}, y $\alpha(\Gamma) \geq 2^n + 1$. Entonces, aún cuando el Teorema arriba muestra que: $\alpha(\Gamma) < f(\alpha(\Gamma)) < (\alpha(\Gamma)!)^2$, existe Γ para el cual

$\alpha(\Gamma) > c^{\alpha(\Gamma)}$, con $c > 1$, una constante.

SECCION C. Subconjuntos libres de sumas.

En esta sección, supondremos que Γ es un grupo abeliano finito. Un subconjunto $S \subset \Gamma$ es llamado "libre de sumas" si cada vez que $x, y \in S$, entonces $x + y \notin S$.

$S + S = \{ x + y : x, y \in S\}$.
$S - S$ se define de manera análoga.

Una definición equivalente a la de arriba es: S es libre de sumas si y sólo si la ecuación $x + y - z = 0$ no tiene solución con $x, y, z \in S$.

LEMA 1. S es libre de sumas si y sólo si

$$S \cap (S + S) = \emptyset = S \cap (S - S)$$

Dem.
$\Rightarrow$). Si $S \cap (S + S) \neq \emptyset$, sea $y \in S \cap (S + S)$.
$\Rightarrow y \in S$ y $y \in (S + S)$. $\therefore$ S no es libre de sumas.

$\Leftarrow$). Sean $x, y \in S$. Supongamos $x + y \in S$. $\therefore x + y \notin S + S$.
Entonces $x + y = s_1$. $\therefore x = s_1 - y$. $\therefore x \in S - S$,

CONTRADICCION $\blacksquare$

Un subconjunto $S \subset \Gamma$ libre de sumas es llamado localmente máximo o no extendible, si cada vez que T sea un subconjunto libre de sumas de Γ y $S \subseteq T$, entonces $S = T$. Un conjunto S con esta propiedad es llamado máximo si S también tiene la cardinalidad más grande entre todos los subconjuntos libres de sumas de Γ.

Los conjuntos libres de sumas localmente máximos han sido estudiados en distintos contextos, pero principalmente por su relación con los números de Ramsey $R_k(3, 2)$. En esta sección consideraremos a $R_k(3, 2)$ como el mínimo entero positivo tal que cualquier coloración (con k colores) de las aristas de una gráfica completa con $R_k(3, 2)$ vértices resulta tener al menos un triángulo monocromático.

A continuación se ejemplifica el uso de los subconjuntos libres de sumas para estimar algunos números de Ramsey. Todas las aplicaciones son similares a este ejemplo en el sentido de que dependen de partir un conjunto de enteros positivos en subconjuntos libres de sumas ajenos por pares.

Sea $\Gamma = \mathbb{Z}_5$ los enteros módulo 5. Supongamos que partimos los elementos no cero de Γ en dos conjuntos ajenos libres de sumas $S_1 = \{1, 4\}$ y $S_2 = \{2, 3\}$ y asignamos al conjunto S_n el color c_n para $n = 1, 2$. Sea ahora K_5 la gráfica completa con 5 vértices v_0, v_1, v_2, v_3, y v_4 y coloremos la arista de v_i a v_j de color c_n si $i-j \in S_n$. Como $S_n = -S_n$, esto induce una coloración bien definida de las aristas de la gráfica. Sean v_p, v_q y v_r tres vértices cualesquiera de K_5 y consideremos el triángulo con estos vértices. Supongamos que dos de sus aristas, digamos $\{v_p, v_q\}$ y $\{v_q, v_r\}$ tienen color c_n. Esto significa que $p-q$, $q-r \in S_n$. Pero como S_n es libre de sumas, tenemos que $p-r = (p-q) + (q-r) \notin S_n$ así que la arista $\{v_p, v_r\}$ tiene color distinto y no puede ser que K_5 tenga un triángulo monocromático.

Esto muestra que $R_2(3, 2) > 5$.

Ahora probaremos que $R_2(3, 2) = 6$.

Supongamos que coloreamos las aristas de K_6 con dos colores, digamos rojo y azul. Consideremos el vértice v_1.

Al menos tres de las aristas incidentes con v_1 deben estar coloreadas con el mismo color. Supongamos que las aristas $\{v_1, v_2\}$, $\{v_1, v_3\}$ y $\{v_1, v_4\}$ son rojas. Si cualquiera de las aristas que une dos de los vértices v_2, v_3, v_4 es roja, tenemos un triángulo rojo. Si ninguna de estas aristas es roja, todas deben ser azules y tenemos un triángulo azul. Así que $R_2(3, 2) = 6$.

En particular se sabe [11] que si el conjunto Γ^*, de los elementos no cero, pueden partirse en k conjuntos libres de sumas, entonces una k-coloración, libre de triángulos de la gráfica completa en $|\Gamma|$ vértices es posible, y todo conjunto libre de sumas tiene cardinalidad menor a R_{k-1}. Además, véase [9], toda partición libre de sumas de Γ^* puede sumergirse en al menos una cubierta de Γ^* por conjuntos libres de sumas localmente máximos, y de nuevo las cardinalidades de éstos menores que $\dot{R}_{k-1}$.

Por tanto es de gran interés encontrar la cardinalidad mínima de los conjuntos libres de sumas localmente máximos en un grupo Γ, así como también caracterizar todos los subconjuntos libres de sumas localmente máximos.

LEMA 2. Sean $A \subseteq \Gamma$, $B \subseteq \Gamma$ con Γ un grupo.
Entonces $\Gamma = A + B = \{a + b \,/\, a \in A,\ b \in B\}$ o $|\Gamma| \geq |A| + |B|$.

Dem. Si $\Gamma \neq A + B$, elegimos $g \in \Gamma - \{A + B\}$.

Sea $B' = \{g - b \,/\, b \in B\} = \{g\} - B$, así que $|B'| = |B|$. $B' \subseteq \Gamma$.

Supongamos que $A \cap B' \neq \emptyset$ entonces $\exists\, a \in A \cap B'$ y de aquí $a = g - b$ o $g = a + b$, lo cual es una contradicción. Así que $A \cap B' = \emptyset$, de donde:

$$|\Gamma| \geq |A| + |B'| = |A| + |B|.$$

Tma. 3. Sea Γ un grupo finito y sea S un conjunto máximo libre de sumas en Γ. Entonces $|S| \leq \frac{1}{2}|\Gamma|$.

Dem. Por el Lema anterior $\Gamma = S + S$ o $|\Gamma| \geq |S| + |S|$, como S es libre de sumas, $|\Gamma| \geq 2|S|$ y de aquí $|S| \leq \frac{1}{2}|\Gamma|$.

El siguiente teorema se refiere a cotas inferiores de la cardinalidad de cualquier conjunto libre de sumas localmente máximo, en términos de $|\Gamma|$.

LEMA 4. Denotemos por $\frac{1}{2}S = \{x \in \Gamma \,/\, 2x \in S\}$.

Si S es libre de sumas, entonces $\frac{1}{2}S$ es libre de sumas.

Dem.

Sean $x, y \in \frac{1}{2}S$. P. d. $x + y \notin \frac{1}{2}S$.

$x, y \in \frac{1}{2}S \Rightarrow 2x \in S,\ 2y \in S$

Como S es libre de sumas $2x + 2y \notin S$ y como Γ es abeliano

$2x + 2y = 2(x + y) \notin S$.

$\therefore\ (x + y) \notin \frac{1}{2}S$ $\qquad\qquad \therefore\ \frac{1}{2}S$ es libre de sumas.

Además, si $|\Gamma|$ es impar entonces $|\frac{1}{2}S| = |S|$, *ver* [24].

Si $|\Gamma|$ es par entonces $|\frac{1}{2}S| \leq \frac{1}{2}|\Gamma|$ ya que todo conjunto libre de sumas en cualquier grupo tiene cardinalidad menor o igual que $|\Gamma|$, como garantiza el **Tma. 3.** También $|\frac{1}{2}S| = \frac{1}{2}|\Gamma|$ ocurre por ejemplo cuando $S = \{2 + 4i\}_{i=0}^{n-1} \subset \mathbb{Z}_{4n}$

TEOREMA 5. Sea S un conjunto libre de sumas localmente máximo. Entonces

i) $\Gamma = S \cup (S + S) \cup (S - S) \cup \frac{1}{2}S$.

ii) Si $|\Gamma|$ es impar, entonces $|S| \geq \frac{1}{6}((24|\Gamma| - 15)^{1/2} - 3)$.

iii) Si $|\Gamma|$ es par, entonces $|S| \geq \frac{1}{6}((12|\Gamma| - 23)^{1/2} - 1)$.

iv) Si $|S + S| \leq c|S|$, entonces $|S| \geq |\Gamma|/(c^2 + c + 2)$ cuando $|\Gamma|$ es impar y $|S| \geq |\Gamma|/2(c^2 + c + 1)$ si $|\Gamma|$ es par.

Dem.

i). Supongamos $x \in \Gamma - \{S \cup (S + S) \cup (S - S)\}$. Entonces $S \cup \{x\}$ no es libre de sumas, pues si así fuera, como $S \subset S \cup \{x\}$, y S es localmente máximo, tenemos $S = S \cup \{x\}$, lo que implica $x \in S$.

Por lo tanto $2x \in S$, $x \in S + S$ ó $(x + S) \cap S \neq \emptyset$.

Como S es libre de sumas, la única posibilidad es $2x \in S$, es decir $x \in \frac{1}{2}S$.

Por lo tanto $\Gamma = S \cup (S + S) \cup (S - S) \cup \frac{1}{2}S$.

Para *ii)* y *iii)* utilizamos el hecho de que para todo subconjunto S:

$$|S + S| \le \binom{|S|}{2} + |S| \qquad \text{y} \qquad |S - S| \le 1 + 2\binom{|S|}{2}.$$

Para obtener ambas cotas, considérese la forma de los elementos en cada conjunto.

Esta estimación junto con *i)* y nuestra nota sobre $|\frac{1}{2}S|$, muestra que si $|\Gamma|$ es impar: $|\Gamma| \le \frac{3}{2}|S|^2 + \frac{3}{2}|S| + 1$, mientras que si $|\Gamma|$ es par tenemos $|\Gamma| < 3|S|^2 + |S| + 2$.

Para probar *iv)*, usamos un resultado de Ruzsa [*18*]. Para un conjunto arbitrario $A \subseteq \Gamma$, si $|A + A| \le c|A|$, entonces:

$$|A - A| \le c^2|A|.$$

Las cotas inferiores en $|S|$ se siguen en cada caso como arriba.

NOTAS.

En nuestro ejemplo, $S = \{2, 6, \ldots, 4n-2\} \subseteq \mathbb{Z}_{4n}$, el conjunto libre de sumas $\frac{1}{2}S$ también satisface $|\frac{1}{2}S| = 2|S|$.

Existe una amplia evidencia de que $|\frac{1}{2}S| \le 2|S|$ es cierto si S es un conjunto libre de sumas localmente máximo. Esta afirmación no es cierta para cualquier subconjunto libre de sumas, pues $S = \{(2, 0), (2, 2), (2, 3)\}$ en $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ así lo comprueba.

En este ejemplo, $S \cup \{(2, 1)\}$ es libre de sumas y $|\frac{1}{2}S| = 8$.

$|\frac{1}{2}S| = \{(1, 2), (1, 0), (1, 1), (1, 3), (3, 1), (3, 3), (3, 0), (3, 2)\}$ y $2|S| = 6$.

Si $\left|\frac{1}{2}S\right| \leq 2|S|$ es cierto, se puede modificar la cota inferior para $|S|$ en el teorema *iii)*.

Si $|\Gamma|$ es par, $|S| \geq \frac{1}{6}\left((24|\Gamma| + 1)^{1/2} - 5\right)$.

Dem.

$\Gamma = S \cup (S + S) \cup (S - S) \cup \frac{1}{2}S.$

$|\Gamma| \leq |S| + |S + S| + |S - S| + \left|\frac{1}{2}S\right|$ pero

$$|S + S| \leq \binom{|S|}{2} + |S| \qquad y \qquad |S - S| \leq 1 + 2\binom{|S|}{2}.$$

$$|\Gamma| \leq |S| + \binom{|S|}{2} + |S| + 1 + 2\binom{|S|}{2} + 2|S|$$

$$2|\Gamma| \leq 3|S|^2 + 5|S| + 2$$

$$\frac{2}{3}|\Gamma| + \frac{1}{36} \leq \left(|S| + 5/6\right)^2.$$

$$\frac{1}{6}\left[(24|\Gamma| + 1)^{1/2} - 5\right] \leq |S|.$$

Con la misma hipótesis de $|\Gamma|$ par, el teorema *iv)* queda:

$$|S| \geq \frac{|\Gamma|}{c^2 + c + 3}$$

Dem.

$$|S + S| < c|S| \quad y \quad |S - S| < c^2|S|$$

$$|\Gamma| \leq |S| + |S + S| + |S - S| + |\tfrac{1}{2} S| \leq$$

$$\leq |S| + c|S| + c^2|S| + 2|S| = |S|(c^2 + c + 3)$$

$$\therefore \frac{|\Gamma|}{c^2 + c + 3} \leq |S|$$

En [19, p. 226] se menciona que si $\frac{1}{5}(n + 2) \leq h \leq \frac{1}{3}(n + 2)$; existe entonces un conjunto libre de sumas localmente máximo en Z_n de cardinalidad h, justamente $\{h, h + 1, \ldots, 2h - 1\}$.

A este resultado, Bertram en [3] añade que en Z_{11k+2}, k impar, el conjunto $\{2k + 1, 2k + 2, \ldots, 3k, 4k + 1, 6k + 1\}$ es un conjunto libre de sumas localmente máximo de cardinalidad menor que: $\frac{1}{11}|\Gamma| + 2$.

Para motivar las aplicaciones del número de vértices independientes, consideremos un grupo abeliano Γ de orden divisible por 3, $|\Gamma| = 3k$, y H un subgrupo de índice 3 en Γ, $|H| = k$.

De lo anterior $\Gamma = H \cup (H + a) \cup (H + 2a)$, donde a y $2a \notin H$, pero $3a \in H$.

Entonces $S = H + a$ es un conjunto libre de sumas localmente máximo en Γ, ya que:

$$S \cap (S + S) = (H + a) \cap (H + 2a) = \emptyset.$$

$$S \cap (S - S) = (H + a) \cap H = \emptyset.$$

Además $|S - S| + |S \cup -S| - 3 = |H| + |(H + a) \cup (H + 2a)| - 3 =$

$$= |H| + 2|H| - 3 = 3|H| - 3 = |\Gamma| - \frac{|\Gamma|}{|H|} = |\Gamma|(1 - |S - S|^{-1}).$$

TEOREMA 6. Sea S un conjunto libre de sumas localmente máximo en un grupo abeliano Γ.

Entonces $|S - S| + |S \cup -S| - 3 \leq |\Gamma|(1 - |S - S|^{-1})$; y la igualdad se cumple si y sólo si $(S - S)$ es un subgrupo de Γ con índice 3 en Γ y S es una clase lateral de $S - S$.

Dem.

Con el ejemplo arriba, mostramos que si S es una clase lateral no trivial de un subgrupo de índice 3 en Γ, se da la igualdad.

Para demostrar la implicación, sea S un conjunto libre de sumas localmente máximo en Γ.

Si $x_1, x_2, \dots, x_r$ es cualquier conjunto de elementos distintos de Γ, con $x_i - x_j \notin S - S$, $i \neq j$, $1 \leq i$; $j \leq r$, en primer lugar tenemos la siguiente

AFIRMACION.

$$r \leq |\Gamma| - |S - S| - |S \cup -S| + 3.$$

Dem.

Consideremos el r-conjunto: $y_1 = 0$, $y_2 = x_2 - x_1$, $y_3 = x_3 - x_1$, $\dots$, $y_i = x_i - x_1, \dots$ Como $i \neq j$, tenemos $y_i - y_j = x_i - x_j$, solamente y_1 pertenece a $S - S$.

También a lo más una de las y_i, $i \geq 2$ pertenece a $-S$.

Como S es libre de sumas, $(S - S) \cap (S \cup -S) = 0$ y por lo tanto:

$$r + (|S - S| - 1) + (|S \cup -S| - 2) \leq |\Gamma|, \text{ de donde:}$$

$$r \leq |\Gamma| - |S - S| - |S \cup -S| + 3.$$

Sea ahora S cualquier subconjunto de un grupo abeliano Γ, $|\Gamma| = n$. $\Gamma = \langle g_1, g_2, \dots, g_n \rangle$. Definimos una gráfica G_Γ sobre los elementos de Γ en la que dos vértices g_i, g_j son adyacentes si y sólo si $g_i - g_j \in S - S$.

Para cada $g_i \in \Gamma$, hay $|S - S| - 1$ elementos $g_j \neq g_i$, tales que $g_i - g_j \in (S - S)$.

Por lo tanto Gr es una gráfica regular, pues $val(g_i) = |S - S| - 1$, para todo g_i, y Gr tiene $\frac{n}{2}(|S - S| - 1)$ aristas.

Del Corolario II. 11 sabemos que cualquier conjunto independiente de cardinalidad máxima $\alpha(Gr)$, satisface:

$$\alpha(Gr) \geq \frac{|Gr|^2}{|Gr| + 2|E|} = \frac{|Gr|}{|S - S|}$$

con igualdad si y sólo si Gr es una unión de clanes ajenos, cada uno de cardinalidad $|S - S|$, ya que Gr es regular.

Un conjunto independiente en Gr es un conjunto S de elementos distintos $g_1, g_2, \ldots, g_r$, que satisface $g_i - g_j \notin S - S$ si $i \neq j$.

Cuando S es libre de sumas, vimos en la primera parte que:

$$r \leq |\Gamma| - |S - S| - |S \cup -S| + 3.$$

Por lo tanto:

$$\frac{|\Gamma|}{|S - S|} \leq \alpha(Gr) \leq |\Gamma| - |S - S| - |S \cup -S| + 3.$$

$$|S - S| + |S \cup -S| - 3 \leq |\Gamma|(1 - |S - S|^{-1}) = |\Gamma| - \frac{|\Gamma|}{|S - S|}.$$

Y la desigualdad ha sido demostrada.

Además $|\Gamma| - |S - S| - |S \cup -S| + 3 = \frac{|\Gamma|}{|S - S|}$ si y sólo si:

Gr es la unión de clanes ajenos, cada uno de cardinalidad $|S - S|$.

Cuando tenemos la igualdad, los mismos elementos de $(S - S)$ forman un clan, ya que cada elemento de $(S - S) - \{0\}$ es adyacente a 0. Por lo tanto $S - S$ es un subgrupo, ya que el primero es cerrado bajo diferencias.

AFIRMACION.

S es un clan de Gr, de donde $|S| = |S - S|$ y S es una clase lateral (no trivial) de $S - S$.

Dem.

En primer lugar notemos que cada pareja de elementos de S es adyacente en Gr, ($x, y \in S \Rightarrow x - y \in S - S$ por definición).

Supongamos $a \notin S$ y a es adyacente a todo elemento de S, i. e.:

$$(a - S) \cup (S - a) \subseteq S - S. \text{ Entonces:}$$

i) $2a \notin S$, pues de otra manera, existiría $s \in S$ tal que $2a = s$ o $a = s - a \in S - S$, contradiciendo el hecho de que ningun elemento de $(S - S)$ es adyacente a algún elemento que no está en $S - S$.

ii) $a \notin S + S$. De no ser así, existirían $s_1, s_2 \in S$ tales que $s_1 = a - s_2 \in S - S$ lo que contradice la hipótesis sobre S referente a ser libre de sumas.

Ya que $a \notin S - S \Leftrightarrow (a + S) \cap S = \emptyset$, lo que junto con i) y ii) implican que $S \cup \{a\}$ también es libre de sumas, contradiciendo nuestra suposición de que S es localmente máximo. Por lo tanto S es un clan de Gr.

Claramente S es una clase lateral de $S - S$, ya que dos elementos de Γ están en la misma clase lateral módulo un subgrupo si y sólo si su diferencia está en ese subgrupo.

Por último, $-S$ también es una clase lateral de $S - S$.

$$\therefore S = -S \quad \text{o} \quad S \cap -S = \emptyset.$$

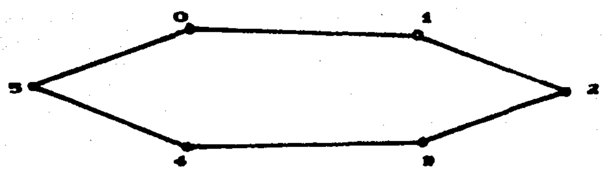
Si $S = -S$ y $|S - S| + |S \cup -S| - 3 = (|\Gamma|(1 - |S - S|^{-1})$, entonces $|S| = |S - S|$ implica $|S|(2|S| - 3) = |\Gamma|(|S| - 1)$.

Pero $|S| - 1$ es primo relativo con $|S|$ y $2|S| - 3$, así que $|S| = 2 = |\Gamma|$, una contradicción. Así que $S \cap (-S) = \emptyset$ y la igualdad implica:

$$3|S| - 3 = \frac{|\Gamma|}{|S - S|}(|S| - 1), \text{ es decir } S - S \text{ tiene índice 3 en } \Gamma.$$

NOTAS.

1 Por ejemplo en $\Gamma = Z_6$, y eligiendo S como $S = \{3, 2\}$, $S - S$ resulta ser $S - S = \{1, 0, 5\}$. En este caso la gráfica asociada Gr resulta ser:

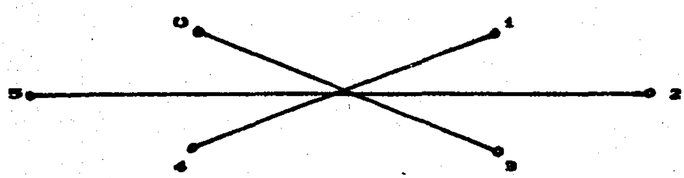


En este caso $(S - S)$ es un subgrupo de indice 2.

$$\therefore \text{ se tiene } |S - S| + |S \cup -S| - 3 \leq |\Gamma|(1 - |S - S|^{-1}).$$

$$\therefore 3 + 3 - 3 \leq 6(1 - 1/3) = 6(2/3) = 4$$

2. En este otro ejemplo con el mismo grupo, tomamos $S = \{3, 0\}$. En este caso $S - S = \{0, 3\}$. Así que la gráfica asociada es:



$$|S - S| + |S \cup -S| - 3 \leq |Z_6|(1 - |S - S|^{-1}).$$

$$2 + 2 - 3 \leq 6(1/2).$$

$$1 \leq 3.$$

$(S - S)$ es un subgrupo de indice 3 pero S no es una clase lateral de $(S - S)$.

Simbología.

$\emptyset$	Conjunto vacío.
$\forall$	Para todo
$\exists$	Existe
e	Elemento identidad de un grupo Γ
a^{-1}, $-a$	Inverso multiplicativo de a en el grupo Γ
$a \in A$	a pertenece a A, a es elemento de A
$\lvert A \rvert$	Cardinalidad de A
$\mathbb{R}$	El conjunto de números reales
$\mathbb{Z}_n$	$\{0, 1, \ldots, n - 1\}$ módulo n
$\mathbb{Q}$	El conjunto de números racionales
$\mathbb{C}$	El conjunto de números complejos
$n\mathbb{Z}$	El conjunto de los múltiplos de n
$C(a)$	El centralizador de a, $\{x \in \Gamma \,/\, xa = ax\}$
$Z(\Gamma)$	$\bigcap_{a \in \Gamma} C(a)$
$A \cap B$	$\{x \,/\, x \in A \text{ y } x \in B\}$
$A \cup B$	$\{x \,/\, x \in A \text{ o } x \in B\}$
S_A	Grupo de permutaciones de un conjunto A
D_n	Grupo diédrico de orden 2n
$[x]$	$\{axa^{-1} \,/\, a \in \Gamma\}$
$\lfloor a \rfloor$	Clase de equivalencia mod H (subgrupo de Γ). $\{b \in \Gamma \,/\, ab^{-1} \in H\}$
$A \equiv B$	A es equivalente a B
ξ	Número de clases de equivalencia mod un subgrupo en un grupo Γ
$[\Gamma : H]$	Indice del subgrupo H en el grupo Γ. Número de clases laterales del subgrupo H en Γ
$\langle a \rangle$	Subgrupo cíclico generado por $a \in \Gamma$, $\{a^n / n \in \mathbb{Z}\}$.
A_n	Grupo alternante en n símbolos. Permutaciones pares del grupo de permutaciones en n símbolos
$\prod_{i=1}^{n} \Gamma_i$	Producto directo de los grupos Γ_i
$\bigoplus_{i=1}^{n} \Gamma_i$	Suma directa de los grupos Γ_i
$V(G)$	El conjunto de vértices de la gráfica G
$E(G)$	El conjunto de aristas de la gráfica G
$\langle S \rangle$	La subgráfica inducida por S
C_n	El ciclo con n vértices
$val(v)$	El grado, valencia, del vértice v en la gráfica G
G^c	La gráfica complemento de G
K_n	La gráfica completa con n vertices
$K_{m,n}$	La gráfica bipartita con mn aristas
$\alpha(G)$	El número de independencia de la gráfica G
$R(k, l)$	El *número* de Ramsey
$\chi(G)$	El número cromático de la gráfica G

$val^{-}(v)$	El grado del vértice v en la gráfica $G - \{vo\}$
G^{-}	La gráfica inducida por $G - \{vo\}$
$(1) \Rightarrow (2)$	La propiedad 1 implica la propiedad (2)
$(1) \Leftrightarrow (2)$	La propiedad 1 es equivalente a la propiedad (2)
$\mathfrak{A}(G)$	El grupo de la gráfica G
$\Lambda \cong \Lambda$	Los grupos Δ y Λ son isomorfos
$p!$	$1 \cdot 2 \cdot 3 \cdots (p-1)p$. p factorial
$\mathfrak{A}_1(G)$	El grupo de aristas de G
$\mathfrak{A}'(G)$	El grupo inducido de aristas de G
$D_\Delta(\Gamma)$	La gráfica de color de Cayley asociada al grupo Γ y al conjunto generador Δ
$k(\Gamma)$	Número de clases de conjugación en el grupo Γ
$k_\Gamma(A)$	Número de clases $[a]$ en Γ, $a \in A$
$\{PSL(2, q)\}$	Grupo lineal especial proyectivo
$A - B$	$\{x / x \in A \text{ y } x \notin B\}$
$S + S$	$\{a + b / a \in S \text{ y } b \in S\}$
$S - S$	$\{a - b / a \in S \text{ y } b \in S\}$
$R_k(3, 2)$	Número de Ramsey
$\frac{1}{2}S$	$\{x / 2x \in S\}$
$\therefore$	Por lo tanto
$A \subseteq B$	A es subconjunto impropio de B
$A \subset B$	A es subconjunto propio de B
$\leq, \geq$	menor o igual que; mayor o igual que

BIBLIOGRAFIA.

1. **BERGE, C.** Graphs and Hypergraphs. North-Holland.

2. **BERTRAM, E. A.** On large cyclic subgroups of finite groups. Proceeding of American Mathematical Society 56. p. 63-66. 1976.

3. **BERTRAM, E. A.** Some applications of graph theory to finite groups. Discrete Mathematics 44. p. 31-43. North-Holland Publishing Co. 1983.

4. **BIRKHOFF, G. and McLANE, S.** Modern Algebra. Macmillan Publishing Company, Inc. 4th. ed. 1977. New York, USA.

5. **BONDY, J. A. and MURTY, U. S. R.** Graph Theory with applications. Elsevier North-Holland, Inc. 1980. New York, USA.

6. **CHARTRAND, G., BEHZAD, M. and LESNIAK-FOSTER, L.** Graphs and digraphs. Prindle, Weber and Schmidt. 1979. Boston, Mass. USA.

7. **DORNHOFF, L. L. and HOHN, F. E.** Applied Modern Algebra. Macmillan Publishing Co., Inc. 1978. USA.

8. **ERDOS, P. amd STRAUSS, E. G.** How abelian es a finite group? Linear and Multilinear Algebra 3, 1976. p. 307-312.

9. **FRALEIGH, J. B.** A first course in abstract algebra. Addison-Wesley Publishing Company. 3a. ed. 1982, USA.

10. **GORENSTEIN, D.** Finite groups. Chelsea Publishing Co., 2nd ed. 1980. New York, USA.

11. **GREENWOOD, R. E. and GLEASON, A. M.** Combinatorial relations and chromatic graphs. Canadian Journal Of Mathematics, 7. p. 1-7. 1955.

12. **HARARY, F.** Graph Theory. Addison-Wesley Publishing Co. 3rd. ed. 1972. USA.

13. **HERSTEIN, I. N.** Topics in Algebra. Xerox College Publishing. 2nd. ed. 1975. Lexington, Mass, USA.

14. **HERSTEIN, I. N.** Algebra Moderna. Edit. Trillas. 1a. ed. en español, 1970. 5a. reimpresión 1980. Trad. Federico Velasco Coba. México.

15. **ISAACS, I. M.** Comunicación personal con E. Bertram. Citada en [3].

16. **MASON, D. R.** On covering of finite groups by abelian subgroups. Mathematical Proceeding of Cambridge Phylosophical Society, 83. 1978. p. 205-209.

17. **NEWER USES OF MATHEMATICS.** James Lighthill ed. Penguin Books. 1st. reprint 1980. England.

18. **RUZSA, I. Z.** On the cardinality of A + A and A - A in: A. Hajnal and V. T. Sós, eds. Combinatorics; Colloquium of the Mathematical Society János Bolyai 18. North-Holland. 1976. p. 933 - 938. Amsterdam, Nederland.

19. **STREET, A. P.** and **WHITEHEAD, Jr. E. G.** Group Ramsey Theory. Journal of Combinatorial Theory, 17. p. 219-226. 1974.

20. **TORANZOS, F. A.** Introducción a la Teoria de Grafos. Programa Regional de Desarrollo Cientifico y Tecnológico. Depto. de Asuntos Cientificos. Sria. General de la OEA. 1976. USA.

21. **TUTTE, W. T.** Connectivity in graphs. University of Toronto Press. 1966. Canada.

22. **VARGAS, J. A.** Teoría de grupos. Centro de Investigación y de Estudios Avanzados del IPN. 1981. Oaxtepec, Morelos. México.

23. **WALLACE, D. A. R.** Grupos. Edit. Limusa. 1a. ed. 1978. México.

24. **WALLIS, W. D., STREET, A. P.** and **WALLIS, J. S.** Combinatorics: Rooms Squares, Sum-Free Sets, Hadamard Matrices. Lecture Notes in Mathematics 292. Springer Verlag. 1972. Berlin, Heidelberg, New York.

25. **WEI, V. K.** Coding for a multiple access channel. Ph. D. dissertation. Dept. of Electrical Engineering. University of Hawaii. 1980.