UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

GRUPOS ASOCIADOS A CONFIGURACIONES Y GRAFICAS

T E S I S

Que para obtener el Título de

MATEMATICO

P r e s e n t a

DAVID REYES GASTELUM

DIRECTOR DE TESIS:

DR. ALBERTO GERARDO RAGGI CARDENAS

FACULTAD DE CIENCIAS
UNAM

2000

220919

UNIVERSIDAD NACIONAL
AVENMA DE
MEXICO

MAT. MARGARITA ELVIRA CHÁVEZ CANO
Jefa de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo de Tesis:

GRUPOS ASOCIADOS A CONFIGURACIONES Y GRAFICAS

realizado por REYES GASTELUM DAVID

con número de cuenta 9455891-5 , pasante de la carrera de MATEMATICAS

Dicho trabajo cuenta con nuestro voto aprobatorio

Atentamente

Director de Tesis
Propietario DR. ALBERTO GERARDO RAGGI CARDENAS

Propietario DR. FAUSTO HUMBERTO CARDENAS TRIGOS H. C

Propietario DR. EMILIO LLUIS RIERA

Suplente DRA. MARIA DE LA PAZ ALVAREZ SCHERER

Suplente M. en C. JOSE ANTONIO GOMEZ ORTEGA

Consejo Departamental de

MATEMATICAS

Héctor Méndez L.

DR. HECTOR MENDEZ LANGO

Dedico esta tesis a Lucie y a mis abuelitos: Quito y Tivita..

Agradecimientos

Quiero agradecer a Lucie a quien tanto amo por todo el apoyo y paciencia que me ha tenido.

Quiero agradecer a mis papás por todo el apoyo a lo largo de la carrera, y a mis hermanos. También quiero agradecer a Babette y Alejandro.

Quiero agradecer a Gerardo y a todos mis sinodales por todo su apoyo, así como a todos los maestros que a lo largo de la carrera me mostraron lo bonitas que son las matemáticas.

Indice

Introducción 1

Capítulo 1
Conocimentos preliminares 4

Capítulo 2
Definición de las permutaciones de los contadores en configuraciones y gráficas 23

Capítulo 3
$P_2(2)$ 26
Gráfica de Petersen 29
$P_2(3)$ 34

Bibliografia 62

Introducción

En esta tesis presento una forma de estudiar y conocer la estructura de ciertos grupos a partir de ver como actúan en contadores asociados a gráficas y configuraciones.

Una de las razones por lo que se hace esto es porque algunos de estos casos se presentan en juegos al ser interpretadas las reglas como acciones de grupos. Se vio que algunas de las propiedades de los grupos se perciben fácilmente desde el aspecto geométrico porque son fáciles de visualizar mentalmente. Algunos ejemplos son:

• El juego (o rompecabezas) que tiene una cuadrícula de 4×4, en cada cuadrito hay un número del 1 al 15 y uno de los cuadritos se encuentra vacío (este puede ser interpretado como el contador especial). Las permutaciones permitidas son las que se obtienen de intercambiar el cuadrito vacío con uno de los contadores que se encuentra a la derecha, izquierda, arriba o abajo del cuadrito vacío. Se puede ver que en este caso el grupo que actúa es A_{16}.

• Las permutaciones de los contadores asociados a los vértices de un polígono regular que se obtienen utilizando las simetrías del polígono. En el caso de un n-ágono se puede ver que el grupo que actúa es S_n.

En el primer capítulo defino, demuestro, y menciono los conocimientos básicos que utilizaré para identificar los grupos obtenidos y sus propiedades.

Las definiciones y conocimientos se encuentran en los libros $[CS]$, $[Hu]$, $[Ro]$, y $[VW]$.

Una de las finalidades de este capítulo es la de introducir el concepto de grupo, este concepto lo utilizaré para interpretar los movimientos de los contadores asociados a gráficas y configuraciones como actuaciones de grupos. Esta interpretación permite emplear los conocimentos y herramientas que se tienen en el álgebra, y además permite relacionar los conocimientos del álgebra con los de la geometría.

Algunos de los resultados demostrados en este capítulo los utilizo para identificar los grupos que actúan en los contadores.

En el segundo capítulo defino las permutaciones de los contadores a partir de unas permutaciones que denoto con el nombre de movimientos admisibles los cuales a su vez están definidos a partir de los movimientos admisibles simples.

Una de las razones por lo cual lo hago de esta forma es porque así se pueden interpretar las permutaciones como movimientos de un juego o rompecabezas, y a su vez nos permite interpretar los juegos o rompecabezas ya conocidos como permutaciones de contadores. Un ejemplo de esto sería un juego que consiste en desordenar los contadores, y cuyo objetivo es regresar los contadores a su lugar inicial Las permutaciones de los contadores permitidas son las que se obtienen con los movimientos admisibles; igual que en el caso del juego mencionado anteriormente de la cuadrícula de 4×4.

El tercer capítulo se encuentra dividido en tres ejemplos.

En el primer ejemplo tenemos los contadores asociados a los puntos de la configuración $P_2(2)$, denotada con el nombre de *Plano de Fano*; y los movimientos admisibles simples consisten en tomar una de las rectas que contienen al contador especial y rotar los contadores que se encuentran en dicha recta, i.e. aplicar $\{e, (123), (132)\} \leq A_3$ a los contadores que se encuentran en la recta.

En este caso obtenemos que los movimientos admisibles simples que dejan fijo al contador especial forman el grupo A_6; para la demostración de esto utilizo algunos de los resultados que se encuentran en el primer capítulo.

En el segundo ejemplo tenemos los contadores asociados a los vértices de la gráfica denotada con el nombre de *Gráfica de Petersen*; y los movimientos admisibles simples consisten en tomar los contadores adyacentes al contador especial y rotarlos, i.e. aplicar $\{e, (123), (132)\} \leq A_3$ a los contadores que se encuentran adyacentes al contador especial.

En este caso obtenemos que los movimientos admisibles que dejan fijos a los contadores especiales forman el grupo $PSL(2,7) \cong PGL(3,2)$. Para la demostración de esto observo que el grupo que deja fijos a los contadores especiales o los intercambia contiene al grupo $PSL(2,7)$, también observo que el grupo $PSL(2,7)$ se encuentra contenido en el grupo que deja fijos a los contadores especiales, y utilizo esto para demostrar lo que queremos.

En el tercer ejemplo tenemos los contadores asociados a los puntos de la configuración $P_2(3)$, denotada con el nombre de *Plano Proyectivo de Orden Tres*; y los movimientos admisibles simples consisten en tomar una de las rectas que contienen al contador especial y aplicar el de *Grupo de Klein* a los contadores de dicha recta.

Este ejemplo está basado en el artículo $[Co]$.

En este caso obtenemos que los movimientos admisibles que dejan fijo al contador especial forman el grupo de Mathieu M_{12}. Para la demostración de esto pruebo que el grupo es dos-transitivo en los contadores asociados a los puntos, y utilizo este resultado para concluir que si asignamos contadores a las rectas y definimos movimientos admisibles simples para los contadores de las rectas obtenemos que los contadores de las rectas también son dos-transitivos por la dualidad de la configuración. También defino unos objetos geométricos denotados con el nombre de *hexadas* que se encuentran contenidos en la configuración, y utilizo la dos-transitividad de los contadores de las rectas para demostrar la transitividad de las hexadas. Utilizando estos resultados demuestro que los movimientos admisibles que dejan fijo al contador especial forman el grupo de Mathieu M_{12}.

Al demostrar los resultados mencionados también demuestro que las hexadas forman un sistema de Steiner $S(5,6,12)$, con lo que obtenemos que el grupo de Mathieu M_{12} actúa transitivamente en el sistema de Steiner $S(5,6,12)$.

En general, no es fácil identificar un grupo que actúa en una gráfica o configuración dada.

Al interpretar grupos como permutaciones de contadores asociados a objetos geométricos a veces da la sensación de complicar la forma de ver al grupo, pero al *familiarizarnos con esto nos permite* aprovechar la intuición geométrica que tenemos. De esta manera se pueden observar propiedades del grupo que a veces pueden resultar difíciles sin la representación geométrica.

Capítulo 1

Conocimientos Preliminares

En esta sección de conocimientos preliminares daré la definición de los términos que utilizaré, y también demostraré varios de los resultados que se utilizarán.

El concepto más utilizado será el de grupo, el cual es un caso especial de semigrupo.

Definición 1 *Un* semigrupo $(G, *)$ *es un conjunto no vacío* G *junto con una operación binaria asociativa* $*$.

Un semigrupo $(G, *)$ junto con las condiciones de que contenga un elemento identidad , e, i.e. $e * a = a = a * e$, $\forall a \in G$; y que para todo elemento $a \in G$, exista $b \in G$ (El inverso de a. En general se denotará al inverso de a por a^{-1}, dependiendo de la operación binaria que se este utilizando.), tal que $ab = e = ba$, es un *grupo*.

Por lo general denotaré a un grupo $(G, *)$ por G.

Ejemplo: $(\mathbb{Z}, +)$; $(\{\text{los enteros divisibles por dos}\}, +) = (\{0, \pm 2, \pm 4, \dots\}, +) = (\{\text{números pares}\}, +) = (P, +)$.

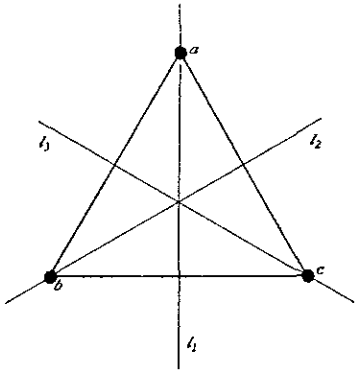
De los ejemplos anteriores podemos ver que el primer grupo $(\mathbb{Z}, +)$ contiene al segundo $(P, +)$, lo cual nos lleva a la siguiente definición.

Definición 2 *Sea* G *un grupo. Un* subgrupo H *de* G *denotado por* $H \leq G$, *es un subconjunto* H *de* G $(H \subseteq G)$ *tal que* H *es un grupo con la misma operación binaria de* G.

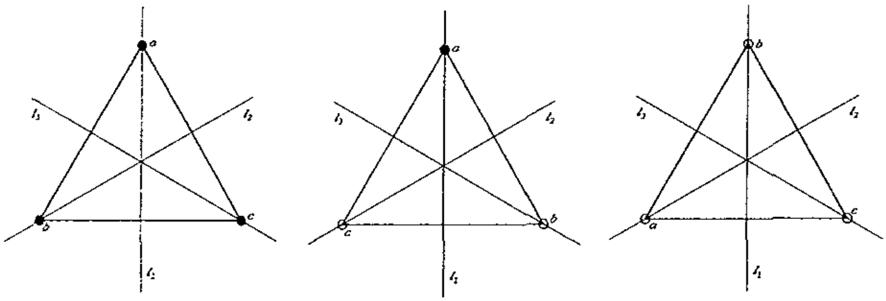
Los ejemplos mencionados anteriormente son ejemplos de grupos conmutativos.

Definición 3 *Un grupo* G *es* conmutativo (abeliano), *si para todo par de elementos* $a, b \in G$, $ab = ba$.

Un ejemplo de un grupo no conmutativo es: $\{\text{simetrías de un tríangulo}\} = \{\text{rotar } 120°, 240°; \text{ reflejar con respecto a } l_1, l_2, l_3; \text{ identidad}\}$.

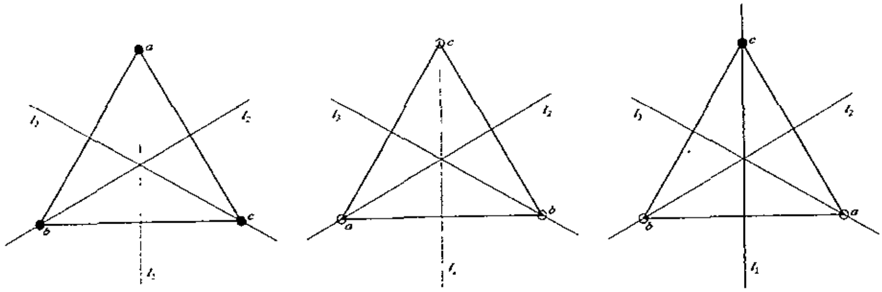


Podemos ver que reflejar con respecto a l_1 y despues rotar 120°, no es lo mismo que rotar 120° y despues reflejar con respecto a l_1. Porque con la primera transformación obtenemos



reflexión respecto a l_1 rotación de 120°

Y con la segunda transformación obtenemos



rotación de 120° reflexión respecto a l_1

Los grupos que utilizaré son grupos finitos, i.e. el grupo contiene un número finito de elementos.

Definición 4 *Sea G un grupo finito. El orden de G, denotado por $|G|$, es el número de elementos que contiene el grupo.*

El orden de un elemento $g \in G$, es el orden del subgrupo generado por el elemento g; i.e. el orden de g es $|\langle g \rangle|$.

Además, si $g \in G$ y $H \leq G$, entonces:

- $|\langle g \rangle| \mid |G|$,
- $|H| \mid |G|$.

Un tipo especial de subgrupos son los son los subrupos normales.

Definición 5 *Sea G un grupo. Un subgrupo $K \leq G$ es* normal, *denotado por $K \lhd G$, si para todo $k \in K$ tenemos que $gkg^{-1} \in K$ para todo $g \in G$.*

Se puede ver de la definición de subgrupo que:

- $e \in K$,
- si $k \in K$ entonces $k^{-1} \in K$.

Observación 6 *Todo subgrupo K de un grupo conmutativo G es normal ($K \lhd G$).*

Algunas partes importantes de un grupo son.

Definición 7 *El* centro *de un grupo G denotado por $Z(G)$, es el conjunto de todos los elementos $a \in G$, tal que a conmuta con todos los elementos de G, ($a \in Z(G) \iff \forall b \in G, ab = ba$).*

De la definición de centro se puede observar que el centro es no vacío ($Z(G) \neq \varnothing$) porque $e \in Z(G)$; y el centro de un grupo conmutativo G es G mismo.

Observación 8 *$Z(G) = G \iff G$ es un grupo conmutativo.*

En general tenemos el siguiente lemma.

Lema 9 *Sea G un grupo, entonces $Z(G) \leq G$.*

Demostración. Es suficiente con demostrar que $e \in Z(G)$, y si $a \in Z(G)$ entonces $a^{-1} \in Z(G)$.
• $ea = a = ae, \forall a \in G, \therefore e \in Z(G)$
• Si $a \in Z(G)$, sea $b \in G$.
$a^{-1}b = a^{-1}be = a^{-1}baa^{-1} = a^{-1}aba^{-1} = eba^{-1} = ba^{-1}, \therefore a^{-1} \in Z(G)$. ■

Observación 10 *Sea G un grupo, entonces $Z(G) \lhd G$.*

Definición 11 *Sea G un grupo, si $a, b \in G$, el* conmutador *de a y b, denotado por $[a, b]$, es $[a, b] = aba^{-1}b^{-1}$.*

Observación 12 *Si a y b conmutan, entonces $[a, b] = aba^{-1}b^{-1} = baa^{-1}b^{-1} = beb^{-1} = bb^{-1} = e$.*

Definición 13 *Sea G un grupo. El* subgrupo conmutador *de G denotado por G', es el subgrupo de G generado por todos los conmutadores, $G' = \langle\{aba^{-1}b^{-1} \mid a, b \in G\}\rangle$.*

Observación 14 *Es fácil ver que $G' = \{e\}$ si y solo si G es abeliano. Por lo tanto, G' de alguna forma nos indica que tan conmutativo es el grupo G.*

Cuando $G' = G$ se dice que el grupo G es *perfecto*.

Una manera de estudiar los grupos (para clasificarlos y para ver las semejanzas entre ellos) es viendo las funciones (transformaciones) entre ellos. Hay varios tipos de transformaciones que nos sirven porque preservan ciertas propiedades, por ejemplo: homomorfismos, epimorfismos, monomorfismos, isomorfismos.

Nota: El término transformación lo estaré utlizando como sinónimo de función.

Definición 15 *Una transformación* ϕ *de un grupo* G *en un grupo* H $(\phi : G \longrightarrow H)$ *es un* homomorfismo (morfismo) *si*

$$\phi(ab) = \phi(a)\,\phi(b)$$

para todos los elementos $a, b \in G$.

Observación 16 *Un morfismo tiene las siguientes propiedades:*
• $\phi(e_G) = e_H$
• $\phi(a^{-1}) = (\phi(a))^{-1}$
• $\phi(a^n) = (\phi(a))^n$, $\forall n \in \mathbb{N}$.

Si los grupos G y H son iguales $(G = H)$ se dice que es un *endomorfismo* de G y se denota por $End(G)$.

Definición 17 *Un* isomorfismo *es un morfismo biyectivo (i.e. inyectivo y suprayectivo) entre un grupo* G *y un grupo* H.

Si existe un ismorfismo entre los grupos G y H entonces son isomorfos y se denota por $G \cong H$.
Si los grupos G y H son iguales $(G = H)$ se dice que la función es un *automorfismo* de G y se denota por $Aut(G)$.

Más adelante estaré utilizando varios grupos, los cuales menciono a continuación; pero antes de dar las definiciones de los grupos, definiré lo que es un anillo y un espacio vectorial.

Definición 18 *Un* anillo *es un conjunto no vacío* R *junto con dos operaciones binarias asociativas* $+, *$; *donde* $(R, +)$ *es un grupo abeliano con elemento identidad* 0, $(R, *)$ *es un semigrupo con elemento identidad* 1, *y ademas se tienen las siguientes propiedades:*
• $(a + b) * c = ac + bc$,
• $a * (b + c) = ab + bc$, $\forall a, b, c \in R$
(i.e cumple la ley distributiva).

Si en un anillo la operación binaria $*$ (multiplicación) es conmutativa entonces se dice que el anillo es conmutativo o que es un anillo conmutativo.
Un ejemplo de un anillo son los números enteros junto con las operaciones binarias de suma y multiplicación, $(\mathbb{Z}, +, *)$; otros ejemplos son los números

racionales, $(\mathbb{Q}, +, *)$, y los números reales, $(\mathbb{R}, +, *)$. Todos estos son ejemplos de anillos infinitos (que contienen un número infinito de elementos), no todos los anillos son de esta forma. También existen anillos con un número finito de elementos, por ejemplo: los enteros módulo n, $(\mathbb{Z}_n, +, *)$.

Definición 19 *Los* enteros modulo n, *denotados por* $(\mathbb{Z}_n, +, *)$. *Es el conjunto* $\{0, 1, 2, 3, \ldots, (n-1)\}$, *con las operaciones binarias de suma y multiplicación, donde:*
- *Sean* $i, j \in \{0, 1, 2, 3, \ldots, (n-1)\}$.
Entonces $i + j \equiv \left\{ \begin{array}{ll} i+j & si,\ 0 \leq i+j \leq n-1 \\ i+j-n & si,\ n \leq i+j \leq 2n-2 \end{array} \right\}$.
- *Sean* $i, j \in \{0, 1, 2, 3, \ldots, (n-1)\}$.
Entonces $i * j \equiv r$, *donde* $n \mid i*j-r$ *(i.e.* n *divide a* $i*j-r$*) y* $0 \leq r \leq n-1$.

Otra forma de definir a $(\mathbb{Z}_n, +, *)$ es utilizando relaciones de equivalencia: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, o como lo denotaremos más adelante, $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$, ya que los dos anillos no son realmente iguales pero si son equivalentes (isomorfos).

De los ejemplos de anillos mencionados tenemos que los anillos: $(\mathbb{Q}, +, *)$, $(\mathbb{R}, +, *)$, y $(\mathbb{Z}_p, +, *)$ donde p es un número primo; son ejemplos de campos, los cuales se definen de la siguiente manera:

Definición 20 *Un* campo *es un anillo* $(K, +, *)$, *donde* $(K, +, 0)$ *y* $(K \backslash \{0\}, *, 1)$ *son grupos abelianos.*

Los ejemplos de anillos mencionados anteriormente son ejemplos de anillos conmutativos, pero no todos los anillos son conmutativos. Un ejemplo de un anillo no conmutativo es: el anillo de las matrices de $n \times n$ con entradas en un campo F, denotadas por $M_{n \times n}(F)$ o $M_n(F)$.

Otra de las transformaciones que utilizaré son las transformaciones lineales, las cuales serán utilizadas para definir transformaciones de un espacio vectorial a otro.

Definición 21 *Un conjunto no vacío* V *se dice que es un* espacio vectorial *sobre un campo* K *si* V *es un grupo abeliano respecto a una operación que denotamos por* $+$, *y si para todo* $\alpha \in K$, $v \in V$ *está definido un elemento, escrito como* αv, *de* V, *con las siguientes propiedades:*
- $\alpha(v + w) = \alpha v + \alpha w$
- $(\alpha + \beta) v = \alpha v + \beta v$

• $\alpha(\beta v) = (\alpha\beta) v$
•$1_K v = v$
para cualesquiea $\alpha, \beta \in K$ *y* $v, w \in V$.

Definición 22 *Sea* K *un campo. Sea* V *y* V' *dos espacios vectoriales sobre el campo* K. *Una* transformación lineal φ *es una función* $\varphi : V \longrightarrow V'$ *tal que:*
• $\varphi(\alpha v) = \alpha\varphi(v)$, $\forall \alpha \in K$ *y* $\forall v \in V$
• $\varphi(v + w) = \varphi(v) + \varphi(w)$, $\forall v \in V$ *y* $\forall w \in V$

Los siguientes son ejemplos de espacios vectoriales y transformaciones lineales.

Si tomamos el campo de los reales $\mathbb{R}$, tenemos que $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$, $\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{R}, \forall\, 1 \leq i \leq n\}$ con $n \in \mathbb{N}$, serían ejemplos de espacios vectoriales.

Sea $M_{m,n}$ una matriz de m renglones y n columnas con entradas en los números reales, entonces

$$M_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} = (a_{i,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = (a_{i,j}), \text{ donde } a_{i,j} \in \mathbb{R}.$$

Sea $\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ tal que

$$\varphi((x_1, x_2, \ldots, x_n)) = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Entonces φ sería una transformación lineal del espacio vectorial $\mathbb{R}^n$ al espacio vectorial $\mathbb{R}^m$.

Definición 23 *Una transformación lineal es* no singular *si la transformación (función) es inyectiva.*

Definición 24 *Si* V *es un espacio vectorial de dimensión* m *sobre el campo* K, *entonces el* grupo general lineal *denotado por* $GL(V)$ *es el grupo de todas las transformaciones lineales no singulares* $\varphi : V \longrightarrow V$. *Cuando el campo* K *es finito de orden* q *lo denotaremos con* $GL(m, q)$.

Sea $n \in \mathbb{N}$. Si tomamos $V = \mathbb{R}^n$ como nuestro espacio vectorial de dimensión n sobre el campo de los reales, $\mathbb{R}$; entonces tenemos que nuestro grupo general lineal, $GL(\mathbb{R}^n)$, se puede interpretar como el conjunto de matrices con determinante distinto de cero, de la misma forma que fueron identificadas las funciones lineales con las matrices de dimensión $n \times n$ con entradas en los reales anteriormente.

Observación 25 *Sea V un espacio vectorial de dimensión n. Siempre es posible identificar las transformaciones lineales $\varphi : V \longrightarrow V$ con el espacio de matrices de dimension $n \times n$, esto se se puede hacer tomando una base del espacio vectorial V, y despues ver que les paso a los elementos de la base bajo la transformación.*

Ejemplo 26 *Sea $\mathbb{R}^2$ el espacio vectorial de dimensión 2 sobre el campo de los reales, como sabemos, $\{(1,0),(0,1)\}$ forman una base de $\mathbb{R}^2$. Entonces identificamos la matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, donde $a, b, c, d \in \mathbb{R}$, y la transformación lineal $\varphi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ tal que:*
- $\varphi((1,0)) = (a,b)$
- $\varphi((0,1)) = (c,d)$.

Definición 27 *Una matriz (o transformación lineal) de determinante 1 es llamada* unimodular.

Definición 28 *Si V es un espacio vectorial de dimensión m sobre el campo K, entonces el* grupo especial lineal *denotado por $SL(V)$ es el subgrupo de $GL(V)$ que consiste de todas las transformaciones unimodulares.*

Dos grupos importantes que se obtienen utilizando los grupos definidos anteriormente son los siguientes:

Definición 29 *Sea $Z(m,q)$ el centro de $GL(m,q)$, entonces el* grupo proyectivo general lineal *es:* $PGL(m,q) \cong \frac{GL(m,q)}{Z(m,q)}$.

Definición 30 *Sea $SZ(m,q)$ el centro de $SL(m,q)$, entonces el* grupo proyectivo especial *lineal es:* $PSL(m,q) \cong \frac{SL(m,q)}{SZ(m,q)}$.

Algunos de los conceptos (o definiciones) y resultados que utilizaré más adelante para hablar de las familias de transformaciones de las etiquetas (o índices) asociados a los vértices de las gráficas (o puntos de las configuraciones), i.e. de las funciones que intercambian las etiquetas (o índices) asociados a los vértices, son los siguientes:

Definición 31 *Una* categoría *es una familia de objetos* $\mathbb{X}$, *y para todo par de objetos* $A, B \in \mathbb{X}$ *tenemos* $Hom_{\mathbb{X}}(A, B) = \{\varphi \mid \varphi : A \longrightarrow B$ *es un morfismo*$\}$, *con composición como operación entre los morfismos:*
$Hom_{\mathbb{X}}(A, B) \times Hom_{\mathbb{X}}(B, C) \longrightarrow Hom_{\mathbb{X}}(A, C) \qquad (f, g) \longmapsto gf$
y un elemento identidad $1_A \in Hom_{\mathbb{X}}(A, A)$ *para cada objeto* A *tal que:*
- *La composición es asociativa, i.e.* $h(gf) = (hg)f$ *cuando las operaciones están bien definidas.*
- $f1_A = f$ *y* $1_A g = g$ *cuando las operaciones estan bien definidas.*

Definición 32 *Un* Grupoide *es una categoría en la cual todos los morfismos son isomorfismos.*

Este concepto lo utilizaré para describir la familia de permutaciones de etiquetas (o índices) asociados a vértices de gráficas (o puntos de configuraciones), ya que no siempre va a ser posible componer dos permutaciones, pero siempre que se pueda se tiene que la composición es asociativa. Todo esto será explicado con mayor detalle más adelante.

Definición 33 *Una* extensión central *de un grupo* G *es una pareja* (H, π) *donde* H *es un grupo y* $\pi : H \longrightarrow G$ *es un morfismo suprayectivo con* $\text{núcleo}(\pi) \leq Z(H)$.

Definición 34 *Una extensión central* $\left(\widetilde{G}, \pi\right)$ *de* G *es* universal *si para toda extensión central* (H, σ) *de* G *existe un único morfismo*
$\alpha : \left(\widetilde{G}, \pi\right) \longrightarrow (H, \sigma)$.

Definición 35 *Si* G *es un grupo perfecto y* $\left(\widetilde{G}, \pi\right)$ *su extensión central universal, entonces el* $\text{núcleo}(\pi)$ *se llama el* multiplicador de Schur *de* G.

Las permutaciones de índices en las gráficas serán vistas como acciones de ciertos grupos sobre el conjunto de índices en las gráficas. Y esta acción está definida de la siguiente forma:

Definición 36 *Sea* X *un conjunto y* G *un grupo. Entonces* X *es un* G-conjunto *si existe una función* $\alpha : G \times X \longrightarrow X$ *(a la cual llamaremos una acción), denotada por* $\alpha : (g, x) \longmapsto gx$ *tal que :*
- $1x = x$ *para todo* $x \in X$,
- $g(hx) = (gh)x$ *para todo* $g, h \in G$ *y* $x \in X$.

Definición 37 *Un G-conjunto X es n-*transitivo *$(n \leq |X|)$ si para todo $x_1, \ldots, x_n \in X$ e $y_1, \ldots, y_n \in X$, donde $x_i \neq x_j$ si $i \neq j$ e $y_i \neq y_j$ si $i \neq j$, existe $g \in G$ tal que $gx_i = y_i$ $\forall 1 \leq i \leq n$.*

Definición 38 *El* grupo simétrico sobre X *denotado por S_X es el grupo que actúa en el G-conjunto X permutando sus elementos. Si $X = \{1, 2, \ldots, n\}$ lo denotaremos con S_n y lo llamaremos* grupo simétrico sobre n elementos.

En el grupo simétrico S_n podemos representar sus elementos como producto de ciclos ajenos de la forma: $(i_1, i_2, \ldots, i_j)$ o $(i_1 i_2 \ldots i_j)$ con $i_l \neq i_m$ si $l \neq m$ donde el ciclo quiere decir que mandamos el elemento i_l al elemento i_{l+1} si $l = 1, 2, \ldots, (j-1)$ y mandamos el elemento i_j al elemento i_1, o productos de ciclos en donde actuaremos los ciclos de izquierda a derecha. Si el ciclo es de longitud dos ((ij)) lo llamaremos *transposición*.

Observación 39 *Sean $\sigma \in S_n$ y $(i_1 i_2 \ldots i_j) \in S_n$ $(j \leq n)$ un ciclo de longitud j, entonces $\sigma^{-1}(i_1 i_2 \ldots i_j)\sigma = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_j))$ donde $\sigma(i)$ quiere decir que le aplicamos la permutación σ al elemento i. Esta propiedad es fácil de ver:*
- *si $\sigma^{-1}(i) \notin \{i_1, i_2, \ldots, i_j\}$, entonces $(\sigma^{-1}(i_1 i_2 \ldots i_j)\sigma)(i) = ((i_1 i_2 \ldots i_j)\sigma)\sigma^{-1}(i) = \sigma(\sigma^{-1}(i)) = i$,*
- *si $\sigma^{-1}(i) \in \{i_1, i_2, \ldots, i_j\}$ supongamos que $\sigma^{-1}(i) = i_l$ $(\sigma^{-1}(i) = i_l \Longrightarrow i = \sigma(\sigma^{-1}(i)) = \sigma(i_l))$, entonces, si $1 \leq l < j$ tenemos $(\sigma^{-1}(i_1 i_2 \ldots i_j)\sigma)(i) = ((i_1 i_2 \ldots i_j)\sigma)\sigma^{-1}(i) = \sigma((i_1 i_2 \ldots i_j)(\sigma^{-1}(i))) = \sigma(i_{l+1})$, donde tenemos que a $\sigma(i_l)$ lo mandamos a $\sigma(i_{l+1})$, y si $l = j$ tenemos $(\sigma^{-1}(i_1 i_2 \ldots i_j)\sigma)(i) = ((i_1 i_2 \ldots i_j)\sigma)\sigma^{-1}(i) = \sigma((i_1 i_2 \ldots i_j)(\sigma^{-1}(i))) = \sigma(i_1)$, donde tenemos que a $\sigma(i_j)$ lo mandamos a $\sigma(i_1)$.*

Teorema 40 *El grupo simétrico S_n es generado por el conjunto de transposiciones, $S_n = \langle\{(ij) \mid i \neq j \text{ y } i, j \in \{1, 2, \ldots, n\}\}\rangle$.*

Demostración. Para demostrar esto es suficiente con ver que cualquier ciclo lo podemos escribir como producto de transposiciones. El ciclo $(i_1 i_2 \ldots i_j)$ lo podemos escribir como $(i_j i_{j-1})(i_{j-1} i_{j-2})\ldots(i_3 i_2)(i_2 i_1)$, es fácil verificar que son equivalentes. ■

Corolario 41 *El grupo simétrico $S_n = \langle\{(i, i+1) \mid i = 1, 2, \ldots, n-1\} \cup \{(n, 1)\}\rangle$.*

Demostración. Para demostrar esto basta con demostrar que podemos generar cualquier transposición. Sea la transposición (ij), sin perdida de generalidad, suponemos $i < j$.
Como $i \neq j$, sea $k = j - i$, si $k = 1$ la transposición es una de nuestras generadoras, si $k \neq 1$ entonces:
$(ij) = (i+2, \ldots, i+(k-1), j, i+1)(i, i+1)(i+1, j, i+(k-1), \ldots, i+2)$
$(ij) = (i+1, i+2, \ldots, i+(k-1), j)(i, i+1)(j, i+(k-1), \ldots, i+2, i+1)$
$(ij) = (i+(k-1), j)\ldots(i+1, i+2)(i, i+1)(i+1, i+2)\ldots(i+(k-1), j)$.
∎

Corolario 42 *El grupo simétrico* $S_n = \langle (1,2), (1,2,\ldots,n) \rangle$.

Demostración. Sea $\sigma = (1,2,\ldots,n)$, entonces $\sigma^{-1}(1,2)\sigma = (2,3)$, $\sigma^{-1}(2,3)\sigma = (3,4)$,..., $\sigma^{-1}(n-1,n)\sigma = (n,1)$. Utilizando el *corolario 41* obtenemos lo que queremos. ∎

Los elementos de S_n $(n \geq 2)$ se dividen en permutaciones pares y permutaciones impares. Una *permutación par (impar)* es una permutación que al expresarla como producto de transposiciones se tiene un número par (impar) de transposiciones. Esta representación como producto de transposisiciones no es única, pero la paridad del número de transposiciones es independiente de la representación.

Sea $A_n = \{\text{permutaciones pares}\}$. Se puede ver facilmente que $A_n \leq S_n$, ya que $e \in A_n$ y el producto de dos permutaciones pares es una permutacion par.

El subrupo A_n lo llamaremos *grupo alternante sobre n elementos*; A_n es un subgrupo normal de S_n $(A_n \lhd S_n)$ y tenemos que el orden de A_n es: $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$.

Lema 43 *Sea* $n \in \mathbb{N}$, $n \geq 3$. *Sean* $r, s \in \{1, 2, \ldots, n\}$ *y* $r \neq s$. *Entonces* A_n *es generado por los 3-ciclos* $\{(rsk) \mid 1 \leq k \leq n \text{ y } k \neq r, s\}$.

Demostración. Si $n = 3$, entonces $A_3 = \{e, (123), (132)\}$, de donde se ve facilmente que el lema se cumple.
Si $n > 3$. Entonces todo elemento de A_n distinto de e es el producto de transpocisiones de la forma $(ab)(ac)$ o $(ab)(cd)$, donde $a, b, c, d \in \{1, 2, \ldots, n\}$ y son distintos entre sí. Tenemos que $(ab)(ac) = (cab)$ y
$(ab)(cd) = (ab)(ac)(ac)(cd) = (cab)(cad)$; de esto se tiene que A_n está generado por los 3-ciclos. Un 3-ciclo tiene una de las siguientes formas:

$(rsa)\,,(ras)\,,(rab)\,,(sab)\,,(cab)$, donde $a, b, c \in [\{1, 2, \ldots, n\} \setminus \{r, s\}]$ y son distintos entre sí. Y, como:

- $(ras) = (rsa)\,(rsa)$,
- $(rab) = (ras)\,(rsb) = (rsa)\,(rsa)\,(rsb)$,
- $(sab) = (rcs)\,(rab)\,(rsc) = (rsc)\,(rsc)\,(rsa)\,(rsa)\,(rsb)\,(rsc)$,
- $(cab) = (rcs)\,(sab)\,(rsc) = (rsc)\,(rsc)\,(rsc)\,(rsc)\,(rsa)\,(rsa)\,(rsb)\,(rsc)\,(rsc)$.

Por lo tanto, los 3-ciclos están generados por los elementos contenidos en $\{(rsk) \mid 1 \leq k \leq n \text{ y } k \neq r, s\}$ y esto implica que $A_n = \langle\{(rsk) \mid 1 \leq k \leq n \text{ y } k \neq r, s\}\rangle$.
■

Lema 44 *Sea $n \in \mathbb{N}$, $n \geq 3$. Sean $N \trianglelefteq A_n$ tal que N contiene un 3-ciclo entonces $N = A_n$.*

Demostración. Sea (rsk) el 3-ciclo contenido en N. Sea $1 \leq a \leq n$ y $a \neq r, s, k$, tenemos que
$(rsa) = (rs)\,(ka)\,(rsk)\,(rsk)\,(ka)\,(rs) = [(rs)\,(ka)]^{-1}\,(rsk)\,(rsk)\,[(ka)\,(rs)]$, por lo que $(rsa) \in N$ porque N es normal y $(ka)\,(rs) \in A_n$. Por lo tanto, utilizando el *Lema 43* tenemos que $N = A_n$. ■

Todos los conceptos y resultados mencionados anteriormente se usarán en relación con los de configuraciones y gráficas los cuales están definidos de la siguiente forma:

Definición 45 *Sean $v, k, t, \lambda \in \mathbb{Z}$ donde $v \geq k \geq t \geq 0$ y $\lambda \geq 1$. Un* $t-(v.k, \lambda)$ diseño *o* $S_\lambda(t, k, v)$ diseño *es una estructura de v elementos donde cada bloque contiene k elementos y para todo conjunto T de elementos ($|T| = t$) existen exactamente λ bloques que contienen al conjunto T.*

En la definición de un $S_\lambda(t, k, v)$ diseño mencioné que es una estructura de v elementos y que cada bloque contiene k elementos, la aplicación que utilizaré no es tan general, el caso particular es: una estuctura de v puntos y que cada recta contiene k puntos Esto realmente es un caso particular ya que nuestros elementos en otros casos pueden ser rectas y nuestros bloques pueden ser espacios, por lo que un diseño tiene realmente muchas formas de ser interpretado pero la interpretación que le daré es la de puntos y rectas.

Un caso particular de un diseño es el sistema de Steiner.

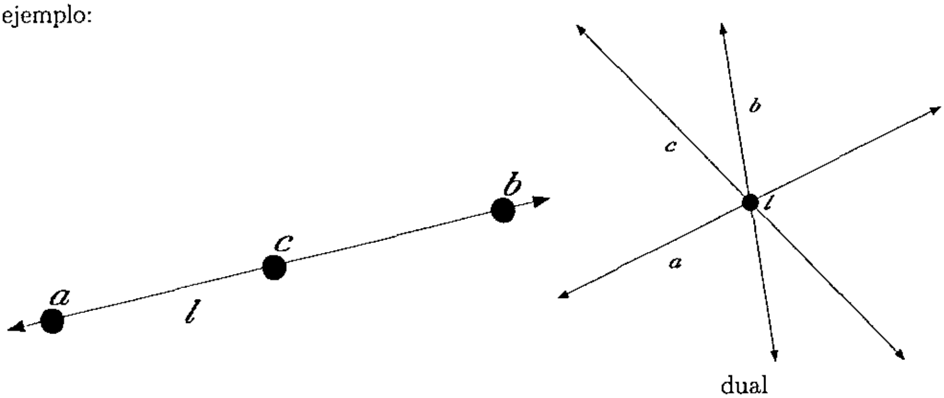
Definición 46 *Un* sistema de Steiner $S(t, k, v)$ *es un* $S_\lambda(t, k, v)$ *diseño con* $\lambda = 1$.

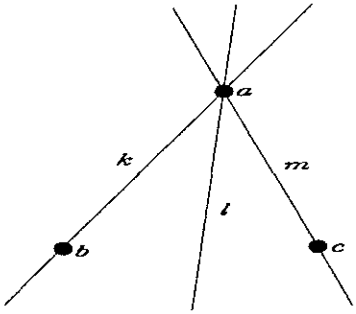
Los sistemas de Steiner son importantes, un caso particular es: $S(2, k, v)$, el cual es una estructura de v puntos, donde cada recta contiene k puntos y que además tiene la condición de que cada dos puntos están contenidos en exactamente una recta.

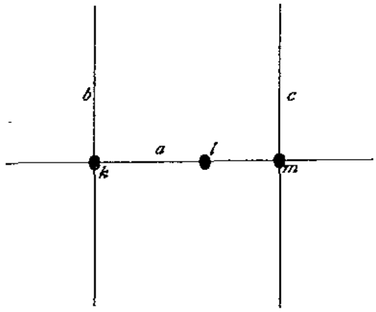
Definición 47 *Una* configuración *es un conjunto de puntos y rectas donde: dos puntos están a lo más en una recta, dos rectas a lo más se intersectan en un punto y todas las rectas tienen el mismo número de puntos.*

Como se puede ver de la definición, una configuración está contenida en un sistema de Steiner, i.e. una configuración se puede ver como una subestructura de un sistema de Steiner, por subestructura quiero decir que si para algún sistema de Steiner se toma un subconjunto de rectas del sistema de Steiner se obtiene la configuración.

Un concepto que voy a utilizar a continuación es el de *dualizar* una configuración (o tomar el dual de una configuración). Con lo cual quiero decir que la estructura se transforma de tal forma que las rectas son puntos y que los puntos son rectas. Y además se transforman las propiedades de incidencia, i.e. si dos rectas se intersectan estas se van a transformar en dos puntos que se encuentran en una misma recta y si dos puntos se encuentran en una misma recta estas se van a transformar en dos rectas que se intersectan. Por ejemplo:







dual

Un caso particular de un sistema de Steiner es el plano proyectivo finito, i.e. que contiene un número finito de puntos.

Definición 48 *Un* plano proyectivo *de orden q, donde $q = p^k$ para algun p primo y $k \in \mathbb{N}$, denotado por $P_2(q)$, es un sistema de Steiner $S(2, q+1, q^2+q+1)$.*

Lema 49 *Los planos proyectivos tienen las siguientes propiedades:*
a) dos rectas cualesquiera siempre se intersectan,
b) dos puntos cualesquiera siempre se encuentran en una única recta,
c) cada punto está contenido exactamente en $q+1$ rectas,
d) el dual de $P_2(q)$ es él mismo.

Demostración. *a*) Supongamos que existen dos rectas, l_1 y l_2, que no se intersectan. Entonces los puntos de l_1 son distintos de los puntos de l_2. Sean $p_1, p_2, \ldots, p_{q+1}$ los puntos contenidos en l_1 y $p'_1, p'_2, \ldots, p'_{q+1}$ los puntos contenidos en l_2, como cada dos puntos determinan una única recta entonces p_1 y p'_1 determinan una recta la cual contiene $q-1$ puntos distintos de $p_1, p_2, \ldots, p_{q+1}, p'_1, p'_2, \ldots, p'_{q+1}$, p_1 y p'_2 determinan una recta la cual contiene $q-1$ puntos distintos de todos los mencionados anteriormente,$\cdots$. Por lo tanto, tenemos $(q-1)(q+1)$ distintos de $p_1, p_2, \ldots, p_{q+1}, p'_1, p'_2, \ldots, p'_{q+1}$, por lo que al menos hay $(q-1)(q+1) + 2(q+1) = q^2 + 2q + 1$, con lo cual se obtiene una contradicción ya que sólo hay $q^2 + q + 1$ puntos.
Por lo tanto, dos rectas cualesquiera siempre se intersectan.
b) Esta propiedad se cumple por definición.
c) Sea p un punto. Como cada dos puntos se encuentran en una única recta

y cada recta contiene $q+1$ puntos. Entonces, dado cualquier otro punto tenemos que p se encuentra en una recta con ese punto, cada recta por el punto p contiene q puntos distintos de p, y hay $q^2+q=q(q+1)$ puntos distintos de p. Por lo tanto p se encuentra contenido en $q+1$ rectas.
d) Esta propiedad se cumple ya que:
• cada recta contiene $q+1$ puntos y por cada punto pasan $q+1$ rectas,
• dos puntos se encuentran en una única recta y dos rectas siempre se intersectan,
• hay q^2+q+1 puntos y tambien q^2+q+1 rectas. Porque si contamos las rectas tenemos:

$$\frac{\binom{q^2+q+1}{2}}{\binom{q+1}{2}} = \frac{\frac{(q^2+q+1)!}{(q^2+q-1)!\,(2)!}}{\frac{(q+1)!}{(q-1)!\,(2)!}} = \frac{(q^2+q+1)\,(q^2+q)}{(q+1)\,(q)} = q^2+q+1. \blacksquare$$

Otra forma de definir un plano proyectivo de orden q es:

Definición 50 *Sea $\mathbb{F}^3(q)$ el espacio vectorial sobre el campo finito de orden q, donde $q=p^k$ para algún p primo y $k\in\mathbb{N}$. El* plano proyectivo $P_2(q)$ *es el $\frac{\mathbb{F}^3(q)\setminus\{0\}}{\sim}$, donde $\sim$ es la relación de equivalencia que dice que dos elementos son equivalentes si uno es múltiplo escalar del otro.*

Observación 51 *Se tiene con la definición anterior que el plano proyectivo siempre existe para q de la forma mencionada.*

Definición 52 *Una* gráfica Γ *es un conjunto de vértices denotado por $V(\Gamma)$ y un conjunto de aristas denotado por $A(\Gamma)$. Tal que el conjunto de aristas $(A(\Gamma))$ cumple con:*
• $A(\Gamma)\subseteq\{(u,v)\mid u,v\in V(\Gamma)\}$,
• *si* $(u,v)\in A(\Gamma)\Longrightarrow(v,u)\in A(\Gamma)$,
• $(v,v)\notin A(\Gamma)$ *para todo* $v\in V(\Gamma)$.

Definición 53 *Dos vértices $u,v\in V(\Gamma)$ se dicen que son* adyacentes *si $(u,v)\in A(\Gamma)$.*

Sea $v\in V(\Gamma)$, el conjunto de vértices adyacentes a v lo denotaré con: $\Omega(v)=\{u\in V(\Gamma)\mid(u,v)\in A(\Gamma)\}$. A este conjunto le asocio un nombre especial ya que lo utilizaré más adelante.

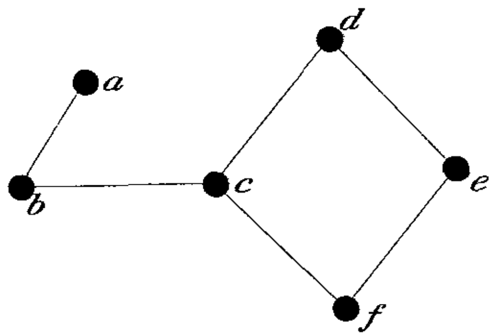
El *grado* de un vértice $v\in V(\Gamma)$ lo denotaré con δ_v, donde
$\delta_v=|\{(u,v)\in A(\Gamma)\mid u\in V(\Gamma)\}|=|\Omega(v)|$.

Definición 54 *Una gráfica* Γ *es* regular *si* $\delta_u = \delta_v$ *para todo* $u, v \in V(\Gamma)$, *en este caso denotaremos con* δ *el grado de cualquier vértice.*

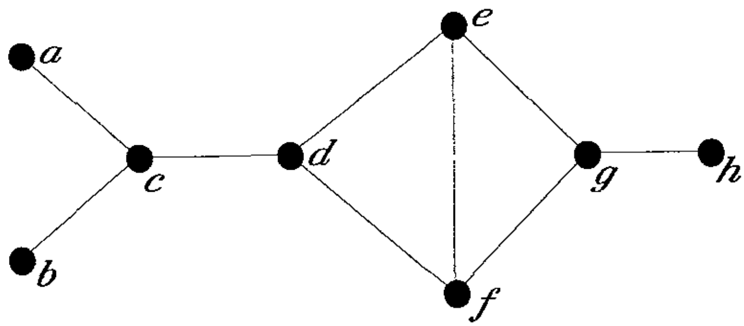
Definición 55 *Sea* Γ *una gráfica. Un* automorfismo de la gráfica Γ *es una función biyectiva* $\varphi : V(\Gamma) \longrightarrow V(\Gamma)$, *tal que* $\forall u, v \in V(\Gamma)$ *tenemos que* $(u, v) \in A(\Gamma) \Longleftrightarrow (\varphi(u), \varphi(v)) \in A(\Gamma)$.

Definición 56 *Dos puntos en una gráfica son* equivalentes *si existe un automorfismo de la gráfica tal que mande un punto al otro.*

Por ejemplo:



En esta gráfica tenemos que los únicos puntos equivalentes son: d y f.



En esta gráfica tenemos que los puntos a y b son equivalentes, tambien los puntos e y f son equivalentes. Y estos son los únicos puntos equivalentes.

Definición 57 *Una* matriz de Hadamard, *es una matriz cuadrada* H *(*$H \in M_{n\times n}$*) con entradas en* $\{\pm 1\}$ *y tal que* $H^T H = nI$.

Sea $H = (a_{i,j}) = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$.

Entonces, $H^T H = \begin{pmatrix} a_{1,1} & a_{2,1} & \cdots & a_{n,1} \\ a_{1,2} & a_{2,2} & \cdots & a_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,n} & a_{2,n} & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} =$

$$= \begin{pmatrix} \sum\limits_{k=1}^{n} a_{k,1}a_{k,1} & \sum\limits_{k=1}^{n} a_{k,1}a_{k,2} & \cdots & \sum\limits_{k=1}^{n} a_{k,1}a_{k,n} \\ \sum\limits_{k=1}^{n} a_{k,2}a_{k,1} & \sum\limits_{k=1}^{n} a_{k,2}a_{k,2} & \cdots & \sum\limits_{k=1}^{n} a_{k,2}a_{k,n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum\limits_{k=1}^{n} a_{k,n}a_{k,1} & \sum\limits_{k=1}^{n} a_{k,n}a_{k,2} & \cdots & \sum\limits_{k=1}^{n} a_{k,n}a_{k,n} \end{pmatrix}$$

Por lo que, $\sum\limits_{k=1}^{n} a_{k,i}a_{k,j} = \begin{Bmatrix} 0 \text{ si } i \neq j \\ n \text{ si } i = j \end{Bmatrix}$.

Lema 58 *Una matriz de Hadamard tiene la propiedad que al intercambiar renglones o columnas sigue cumpliendo con ser de Hadamard.*

Demostración. Sea R un anillo. Sea $H \in M_{n\times n}(R)$ una matriz de Hadamard. Sean $e_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$, $\cdot$, $e_n = \begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix} \in M_{1\times n}(R)$ y $f_i = e_i^T \in M_{n\times 1}(R)$ para $1 \leq i \leq n$.

Tenemos que $\begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_n} \end{pmatrix} H$, donde $1 \leq i_k \leq n$ y $i_k \neq i_l$ $(\forall 1 \leq k, l \leq n)$, es la matriz H pero con renglones intercambiados. Y $H \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix}$, *donde* $1 \leq i_k \leq n$ *y* $i_k \neq i_l$ $(\forall 1 \leq k, l \leq n)$, es la matriz H pero con columnas intercambiadas.

Entonces,

$$\left(\begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_n} \end{pmatrix} H\right)^T \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_n} \end{pmatrix} H = H^T \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_n} \end{pmatrix}^T \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_n} \end{pmatrix} H = H^T I H = H^T H =$$
nI,

y

$(H \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix})^T H \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix} =$

$= \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix}^T H^T H \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix} =$

$= \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix}^T nI \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix} =$

$= nI \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix}^T \begin{pmatrix} f_{i_1} & f_{i_2} & \cdots & f_{i_n} \end{pmatrix} = nII = nI.$ ■

Lema 59 *Si $H = (a_{i,j})$ es una matriz de Hadamard, entonces $H \in M_{n\times n}$, donde $n = 2$ o $n = 4k$ $(k \in \mathbb{N})$.*

Demostración. Tenemos que dos columnas distintas sólo coinciden en $\frac{n}{2}$ entradas, porque $\sum_{k=1}^{n} a_{k,i}a_{k,j} = 0$ si $i \neq j$. $\therefore n$ tiene que ser par.

Bajo estas condiciones sí existen matrices de Hadamard de 2×2, ejemplo: $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Si $n > 2$. Sin perdida de generalidad puedo asumir que todas las entradas en la primera columna son $1's$.

$$\begin{pmatrix} 1 & \\ 1 & \\ \vdots & * \\ 1 & \end{pmatrix}$$

La segunda columna tiene $\frac{n}{2}$ $1's$ y $\frac{n}{2}$ $(-1)'s$, porque $\sum_{k=1}^{n} a_{k,1}a_{k,2} = 0$. Sin perdida de generalidad podemos asumir que estan de la siguiente forma: $\begin{pmatrix} 1 & 1 & \\ \vdots & \vdots & \\ 1 & 1 & \\ 1 & -1 & * \\ \vdots & \vdots & \\ 1 & -1 & \end{pmatrix}$.

La tercera columna tiene tambien $\frac{n}{2}$ $1's$ y $\frac{n}{2}$ $(-1)'s$, porque $\sum_{k=1}^{n} a_{k,1}a_{k,3} = 0$. Y como $\sum_{k=1}^{n} a_{k,2}a_{k,3} = 0$, entonces los $1's$ de la tercera columna solo pueden coincidir con $\frac{n}{4}$ $1's$ de la segunda columna. Por lo tanto, n es múltiplo de 4.
$\blacksquare$

Capítulo 2

Definición de las permutaciones de los contadores (o etiquetas) en configuraciones y gráficas. (Definiciones en general.)

Utilizando una función inyectiva de los vértices (o puntos) a un conjunto de etiquetas le podemos asociar a cada vértice una etiqueta; por lo general las etiquetas que utilizaré serán números.

En otras palabras asociándole a cada vértice (o punto en el caso de una configuración) un contador (o etiqueta), como contadores utilizaré números; i.e. numerando los vértices (o puntos).

Al hacer esto es posible definir grupos conocidos (e interesantes) a partir de ciertas permutaciones de los contadores en las gráficas o en las configuraciones. Una forma de pensar en esto es como un juego en el cual se mueven los contadores y el objetivo del juego es el de regresar los contadores a su lugar inicial.

Nota: Para simplificar la notación escribiré que los contadores se encuentran en una recta o en conjunto de vértices para querer decir que los contadores se encuentran asociados con puntos contenidos en la recta o con vértices contenidos en el conjunto de vértices.

Definición 60 *Sea C una configuración y l una recta de dicha configuración. Sea $\sigma \in S_k$, llamamos* movimiento admisible simple de la configuración *a la permutación (de los contadores) que se obtiene de aplicarle σ a los contadores que se encuentran en l denotado por $\sigma(l)$. Un* movimiento admisible de la configuración *es una sucesión finita de movimientos admisibles simples de la configuración.*

En la definición anterior es posible ponerle restricciones, por ejemplo, que la recta l siempre contenga a un contador al cual designaremos como contador especial o que únicamente podamos utilizar ciertos subgrupos de S_k.

Definición 61 *Sea Γ una gráfica regular y $v \in V(\Gamma)$. Sea $\sigma \in S_\delta$, llamamos* movimiento admisible simple de la gráfica *a la permutación (de los contadores) que se obtiene de aplicarle σ a los contadores que se encuentran asociados con los vértices contenidos en Ω_v denotado por $\sigma(\Omega_v)$. Un* movimiento admisible de la gráfica *es una sucesión finita de movimientos simples de la gráfica.*

En la definición anterior también es posible agregarle restricciones, por ejemplo, que tomemos dos vértices adyacentes y que a sus contadores los designemos como contadores especiales, que el vértice v (mencionado en la definición anterior) siempre sea uno de los vértices en el cual se encuentra uno de los contadores especiales o que únicamente podamos utilizar ciertos subgrupos de S_6.

Observación 62 *Una sucesión (o composición) de movimientos admisibles es un movimiento admisible.*

En general se obtiene que el conjunto de movimientos admisibles nos genera un grupoide, esto se debe a que no siempre va a ser posible actuar un elemento del conjunto de movimientos admisibles después de otro.

Lema 63 *El conjunto de movimientos admisibles genera un grupoide.*

Demostración. Sea A la asociación (inicial) de contadores con los vértices (o puntos), i.e. sea una función inyectiva $f : \{\text{vértices}\} \longrightarrow \{\text{contadores}\}$, $A = \{(v, f(v)) \mid v \text{ es un vértice}\}$. Sea $\mathbb{X}$ la familia de objetos B tal que $B = \varphi(A) = \{(v, \varphi(f(v))) \mid v \text{ es un vértice}\}$, donde φ es un movimiento admisible.
El elemento identidad $1_B \in Hom_{\mathbb{X}}(B, B)$ es el movimiento admisible que no mueve ningún contador.
La composición es asociativa ya que la composición de movimientos admisibles es asociativa.
Con esto se obtiene que tenemos un grupoide. ■

El estabilizador del contador especial (o los contadores especiales), el cual denotaré con E, i.e. los movimientos admisibles que regresan al contador especial (o contadores especiales) a su vértice (o punto) inicial nos determina un grupo.

Es un grupo en el cual:

- La operación definida en el grupo es la composición.
- Existe un elemento identidad, el que no mueve los contadores de la configuración
- Dada una permutación existe su inverso, la cual se obtiene realizando la sucesión de movimientos que se utilizaron para obtener la permutación pero en orden inverso.
- La operación es asociativa, esto se tiene por estar contenido en el grupoide y tener la misma operación .

En las configuraciones con las propiedades:

• al tomar dos puntos siempre existe una recta que los contenga,

• dos rectas siempre se intersectan en un punto de la configuración,

por ejemplo planos proyectivos, se tiene que el grupo que se obtiene (el estabilizador del contador especial) se encuentra generado por permutaciones triangulares, ya que son las mínimas sucesiones de movimietos que se puede tener y cualquier sucesión de movimientos se puede escribir como composición de estas.

Una permutación triangular es la que se obtiene con la siguiente sucesión de movimientos admisibles:

• tomamos uno de los contadores y lo llamamos (o designamos) contador especial,

• tomamos el contador especial y una recta que lo contenga y le aplicamos un movimiento admisible (simple),

• nos fijamos donde quedo nuestro contador especial y tomamos una recta que contenga al contador especial y le aplicamos otro movimiento admisible (simple),

• si el contador especial aún no se encuentra en su lugar inicial nos fijamos donde está nuestro contador especial y tomamos la recta que contenga al contador especial y al contador que se encuentra en el punto donde se encontraba el contador especial al inicio y le aplicamos un movimiento admisible de forma que el contador especial regrese a su lugar inicial.

Estas permutaciones son las mínimas permutaciones no triviales que se encuentran en el estabilizador del contador especial.

Nota: Para poder generar todas las posibles permutaciones triangulares es necesario que los subgrupos (o grupos), S_k, utilizados sean 1-transitivos.

Capítulo 3

Ejemplos.

Ejemplo, $P_2(2)$.

Tomamos el plano proyectivo de orden dos ($P_2(2)$, figura 1). Tenemos siete puntos y cada uno con su respectivo contador de los cuales designamos a uno de ellos como el contador especial. Sean los números del cero al cinco y ∞ los contadores, ∞ es el contador especial.

Tomamos las permutaciones generadas por los movimientos en la configuración tal que toman al contador especial y una recta l de las tres rectas que lo contienen y rotamos los tres contadores que se encuentran en la recta (tomamos $\sigma \in \{(\infty ij), (\infty ji), e \mid i,j \in l\}$), y cualquier sucesión de estos movimientos (y después tomar el estabilizador del punto especial). En otras palabras tomar el subgrupo $\{(\infty ij), (\infty ji), e\}$ ($\cong A_3$) de S_3, donde ∞, i, j se encuentran en una misma recta.

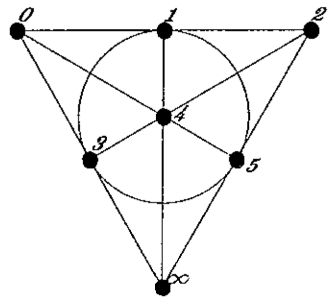
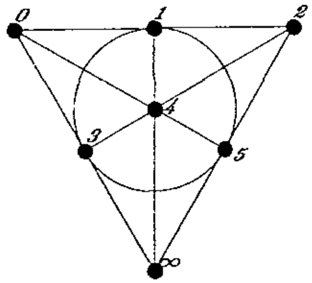
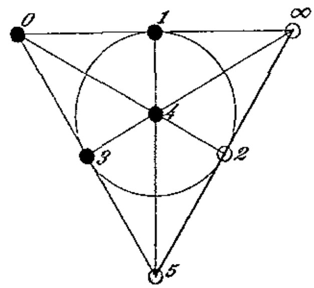


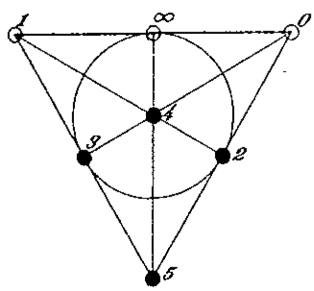
figura 1

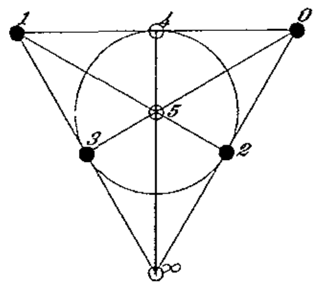
Ejemplo 64 *Al observar la siguiente permutación triangular, tenemos:*





$(\infty, 2, 5)$





$(\infty, 1, 0)$ $(\infty, 5, 4)$

Como se puede ver, la permutación que obtenemos es: $(\infty 54)(\infty 10)(\infty 25)$.
Como se puede ver se obtiene la permutación pero en sentido contrario, i.e. no se obtiene la permtuación: $(\infty 25)(\infty 10)(\infty 54)$. *Esto se debe a que la permutación que se obtuvo es:*

$$(\infty, 2, 5)(\alpha(\infty), 1, 0)(\beta(\infty), \beta(5), 4) = (\infty, 2, 5)\alpha^{-1}(\infty, 1, 0)\alpha(\beta(\infty), \beta(5), 4) =$$
$$= (\infty, 1, 0)(\infty, 2, 5)(\beta(\infty), \beta(5), 4) = (\infty, 1, 0)(\infty, 2, 5)\beta^{-1}(\infty, 5, 4)\beta =$$
$$= (\infty, 5, 4)(\infty, 1, 0)(\infty, 2, 5)$$

y otra forma de escribirlo es:

$$(\infty, 2, 5)(\alpha(\infty), 1, 0)(\beta(\infty), \beta(5), 4) = (\infty 25)(210)(1\infty 4).$$

Sabemos que el grupo que se obtiene al tomar el estabilizador del punto especial es un subgrupo de A_6, $E \leq A_6$, esto es porque lo que obtenemos son permutaciones de seis elementos, y todas las permutaciones son pares porque se obtienen como producto de permutaciones pares.

Lema 65 $E = A_6$.

Demostración. Para demostrar que E es normal en A_6, $E \lhd A_6$; tenemos que:

• Las permutaciones triangulares son elementos de orden cinco, por ejemplo: $(\infty 52)(540)(4\infty 1) = (05214)$.

• Con las permutaciones triangulares $(05214), (05243), (02513), (03145)$ se pueden generar los elementos:

$(213) = (05214)(05243)(02513)(03145)$

$(013) = (02513)(03145)(05214)(05243)$

con los cuales se genera un subrupo de orden doce,

$$\langle (213), (013) \rangle = \left\{ \begin{array}{c} e, (213), (231), (013), (031), (032), (023), \\ (021), (012), (01)(23), (02)(13), (03)(12) \end{array} \right\}.$$

• Con las permutaciones triangulares $(03152), (03145)$ se puede generar el elemento: $(01)(2345) = (03152)(03145)$.

Con este último elemento y uno de los elementos obtenidos en el el subgrupo de orden doce obtenemos: $(345) = (01)(2345)(01)(23)$.

Utilizando este último y con uno de los elementos del subgrupo de orden doce se genera un subgrupo de orden nueve,

$$\langle (345), (012) \rangle = \left\{ \begin{array}{c} e, (345), (354), (012), (021), (345)(012), \\ (345)(021), (354)(012), (354)(021) \end{array} \right\}.$$

Con estas tres cosas obtenemos que el orden del grupo E es divisible por $5, 12$ y 9. Por lo tanto, el orden de E es divisible por $180 =$ mínimo común múltiplo $(5, 12, 9)$. Y como el orden de A_6 es 360, entonces el orden de E es: 180 o 360; y en cualquiera de los dos casos obtenemos que E es normal en A_6

Utilizando el *lema 43*, porque $E \lhd A_6$ y E contiene un 3-ciclo, entonces $E = A_6$. ■

Ejemplo, Gráfica de Petersen.

Tomamos la gráfica de Petersen (figura 2). La gráfica contiene diez vértices a los cuales le asociamos diez contadores, uno a cada uno.
Designamos a dos de los contadores como contadores especiales, los tomamos de tal manera que sean adyacentes. Los contadores especiales estarán designados con ∞ y ∞';y los ocho contadores restantes estarán designados con los números del cero al siete. La asignación de los contadores que usaré es la que se muestra en la figura:

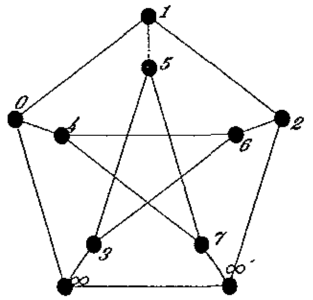
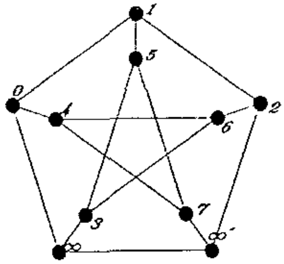


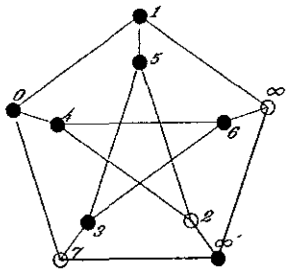
figura 2

Los movimientos que se utilizan en este caso consisten en tomar uno de los contadores especiales; tomamos los tres contadores adyacentes al contador especial seleccionado, y los rotamos cíclicamente. Por ejemplo tomamos al contador ∞', el conjunto de contadores adyacentes es $\Omega(\infty')$, y tomamos $\sigma \in \{(\infty, i, j), (\infty, j, i) \mid i, j \in \Omega(\infty')\}$. En otras palabras tomamos
$S_\xi \cong \{e, (abc), (acb)\} \leq S_{\{a,b,c\}} \cong S_3$.

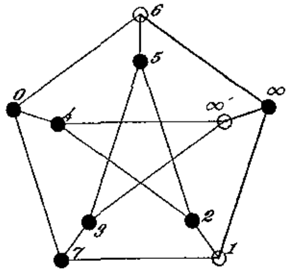
Observación 66 *Siempre tenemos que* $\infty \in \Omega(\infty')$ *y que* $\infty' \in \Omega(\infty)$.

Un ejemplo de un movimiento simple que deja fijos a los dos contadores especiales es:

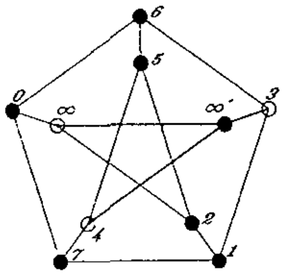




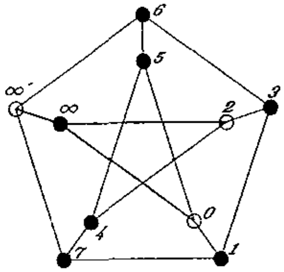
$(\infty, 2, 7)$



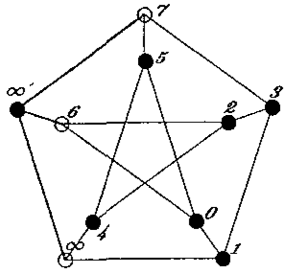
$(\infty', 6, 1)$



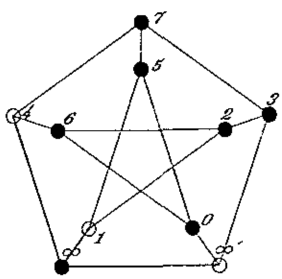
$(\infty, 4, 3)$



$(\infty', 0, 2)$



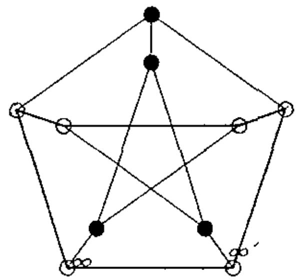
$(\infty, 7, 6)$



$(\infty', 1, 4)$

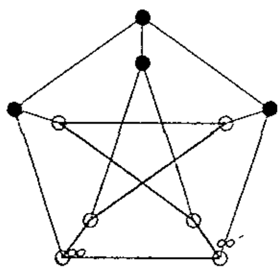
Con lo cual obtenemos la permutación:
$(0. 7, 1, 3, 2. 6, 4) = (\infty', 1. 4)\,(\infty, 7, 6)\,(\infty', 0, 2)\,(\infty, 4, 3)\,(\infty', 6, 1)\,(\infty, 3, 8) =$
$= (\infty, 3, 8)\,(\infty', 6, 1)\,(2, 4, 3)\,(0, 7, 6)\,(\infty, 1, 4)\,(\infty', 3, 0).$

A este movimiento lo denotaré con el nombre de *movimiento básico de longitud seis*, lo denoto con este nombre porque los puntos especiales se mueven a lo largo de una trayectoria de longitud seis.

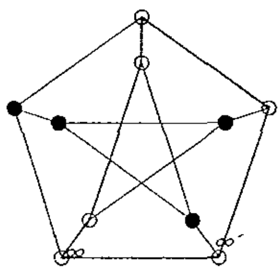


$(0,7,1,3,2,6,4)$

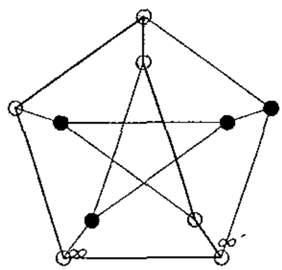
Esta permutación es uno de los movimentos básicos de longitud seis que dejan fijos a los contadores especiales, los otros tres movimentos básicos de longitud seis que dejan fijos a los contadores especiales son: $(0,7,4,6,3,2,5)$, $(0,2,1,5,3,7,6)$, y $(0,2,4,3,7,5,1)$.



$(0,7,4,6,3,2,5)$



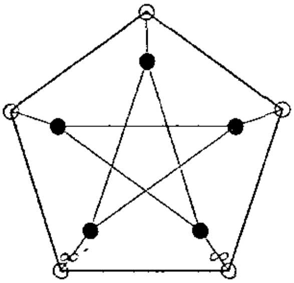
$(0,2,1,5,3,7,6)$



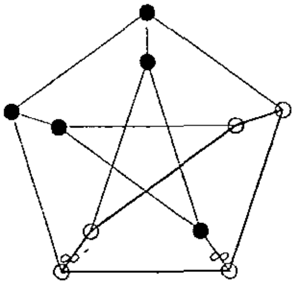
$(0,2,4,3,7,5,1)$

Los movimientos básicos de longitud cinco y seis que no dejan fijos a los contadores especiales pero que los intercambian entre sí son:

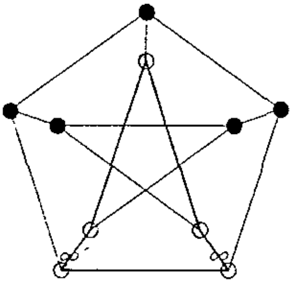
- longitud cinco



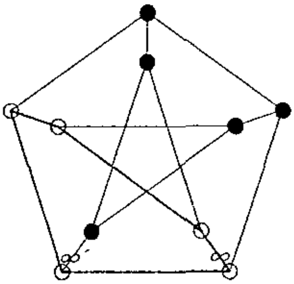
$(\infty, \infty')\,(0,5,2,7,4,1,6,3)$



$(\infty, \infty')\,(0,3,4,2,7,5,6,1)$

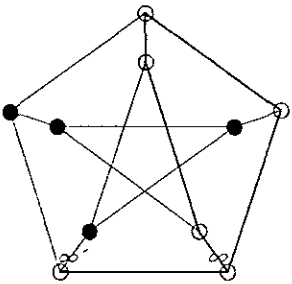


$(\infty, \infty')\,(0,3,1,7,2,6,5,4)$

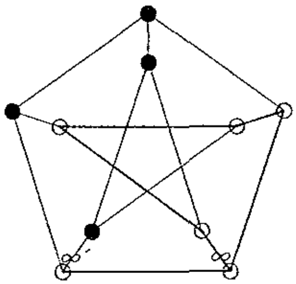


$(\infty, \infty')\,(0,6,7,2,1,4,5,3)$

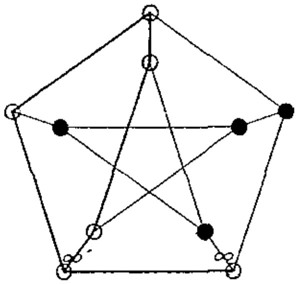
- longitud seis

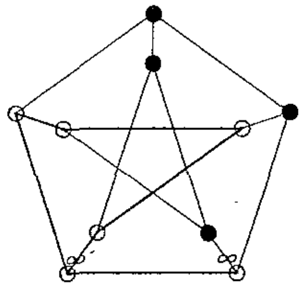


$(\infty, \infty')\,(0,7,2,3,1,6,4,5)$



$(\infty, \infty')\,(0,6,1,5,4,3,7,2)$





$(\infty,\infty')\,(0,3,2,5,6,4,1,7)$ $\qquad$ $(\infty,\infty')\,(0,3,7,6,5,1,4,2)$

Estos movimientos básicos de longitud cinco y seis que intercambian los contadores especiales son muy importantes porque son los mínimos movimientos admisibles que intercambian a los contadores especiales, y generan todos los movimientos admisibles que dejan fijos a los contadores especiales o los intercambian.

Utilizando el programa para computadora llamado GAP obtenemos:

$$\left|\left\langle \begin{array}{c} (\infty,\infty')\,(0,5,2,7,4,1,6,3)\,,(\infty,\infty')\,(0,3,4,2,7,5,6,1)\,, \\ (\infty,\infty')\,(0,3,1,7,2,6,5,4)\,,(\infty,\infty')\,(0,6,7,2,1,4,5,3)\,, \\ (\infty,\infty')\,(0,7,2,3,1,6,4,5)\,,(\infty,\infty')\,(0,6,1,5,4,3,7,2)\,, \\ (\infty,\infty')\,(0,3,2,5,6,4,1,7)\,,(\infty,\infty')\,(0,3,7,6,5,1,4,2) \end{array}\right\rangle\right| = 336$$

También obtenemos que:

$|\langle(0,7,1,3,2,6,4)\,,(0,7,4,6,3,2,5)\,,(0,2,1,5,3,7,6)\,,(0,2,4,3,7,5,1)\rangle| = 168$

Y además:

$\langle(0,7,1,3,2,6,4)\,,(0,7,4,6,3,2,5)\,,(0,2,1,5,3,7,6)\,,(0,2,4,3,7,5,1)\rangle$ es simple.

Con lo que obtenemos $E = \left\langle \begin{array}{c} (0,7,1,3,2,6,4)\,,(0,7,4,6,3,2,5)\,, \\ (0,2,1,5,3,7,6)\,,(0,2,4,3,7,5,1) \end{array}\right\rangle.$

Por lo tanto $E \cong PSL\,(2,7) \cong PGL\,(3,2)$.

Ejemplo, $P_2(3)$

Sea el plano proyectivo de orden 3 ($P_2(3)$). Tomamos la siguiente representación, en la cual designaremos un contador como contador especial utilizando el contador ∞ y a los contadores restantes con números del cero al once (figura 1) o con letras de la a a la l (figura 2) según nos convenga, es indiferente a cual punto le asociemos el contador especial porque todos los puntos son equivalentes.

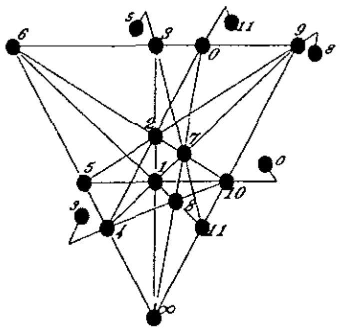


figura 1

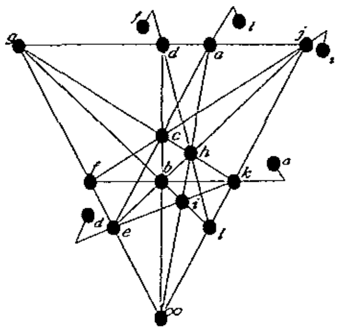
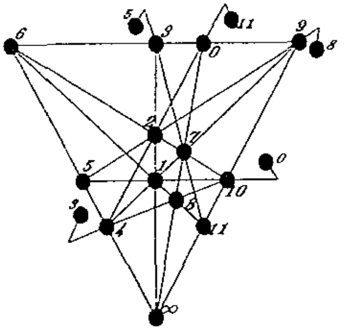
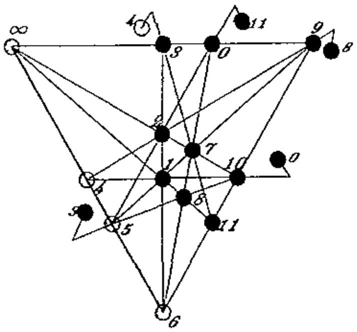


figura 2

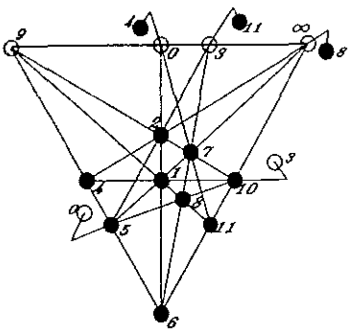
Tomaremos las permutaciones de los contadores de la configuración que se obtienen por los siguientes movimientos admisibles de los contadores de la configuración: sea l una recta que contiene al contador especial, nos fijamos en los 4 contadores que contiene dicha recta e intercambiamos el contador especial con alguno de los contadores de la recta e intercambiamos los otros dos contadores que contiene la recta
($\sigma \in \{(\infty, i)(j,k), (\infty, j)(i,k), (\infty, k)(i,j) \mid i,j,k \in l\} \cong$ (Grupo de Klein)). El conjunto de permutaciones de los contadores de la configuración es independiente de la representación y asignación de los contadores que se tome, y del punto que se designe como punto especial ya que los puntos son equivalentes.

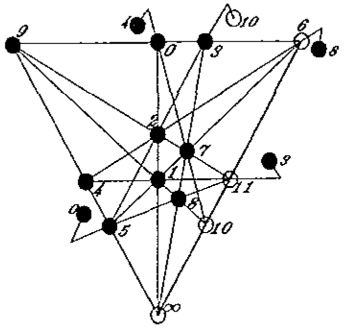
Las permutaciones de los contadores que se obtienen al mover el contador especial por los vértices de un triángulo formado por tres rectas de la configuración de las cuales dos de ellas se intersectan en el vértice donde se encuentra el contador especial inicialmente es una permutación triangular. El ejemplo que doy es la permutación $(4,5)(6,9)(0,3)(10,11)$ que se obtiene de la siguiente manera:





$(\infty, 6)\,(4, 5)$





$(\infty, 9)\,(0, 3)$ $\qquad$ $(\infty, 6)\,(10, 11)$

Con lo que obtenemos:

$(4,5)(6,9)(0,3)(10,11) = (\infty,6)\,(10,11)\,(\infty,9)\,(0,3)\,(\infty,6)\,(4,5) =$
$= (\infty,6)\,(4,5)\,(6,9)\,(0,3)\,(\infty,9)\,(10,11)$

El conjunto de permutaciones triangulares genera a E, porque son las mínimas permutaciones no triviales que se encuentran en E (el estabilizador del contador especial).

En la demostración de este ejemplo denotaré con G al estabilizador del contador especial.

Lema 67 *El G-conjunto $X = \{0, ..., 11\}$ es 2 transitivo. El grupo G es dos veces transitivo (en la configuración).*

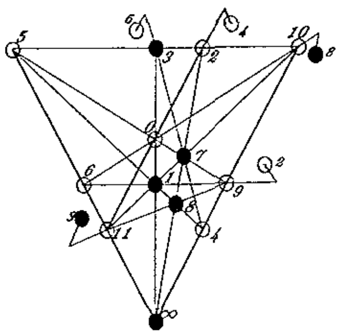
Demostración. Para ver que es uno transitivo, basta con demostrar que cualquier contador de nuestra configuración lo podemos mandar al contador seis. Nota: cuando escribo que queremos mandar a un contador al contador seis (por ejemplo) quiero decir que quiero mandarlo al vértice donde se encontraba el contador seis inicialmente. Para demostrar esto lo podemos hacer por casos, dependiendo de que si el contador que queremos mover se encuentra o no se encuentra en la misma recta vertical que el contador hacia donde lo queremos mover:

<u>Caso 1</u>

El contador que queremos mover y el contador seis se encuentran en la misma recta vertical.

En general, lo que se hace es aplicar la permutación triangular que tiene como vértices al contador especial, al contador que se encuentra en la misma recta vertical que el contador especial pero distinto del contador seis y el contador que se quiere mover, y como tercer vértice se puede tomar cualquier contador que se encuentre en una recta vertical que no contenga al contador seis.

Un ejemplo de este caso es si el contador que queremos mover es el cinco entonces podemos aplicar la permutación triangular que se muestra en la figura:



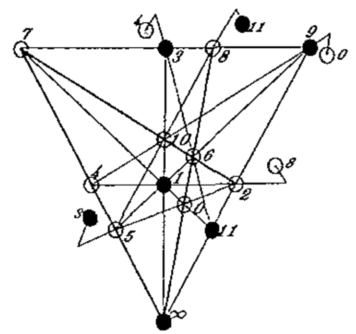
$$(5,6)(4,11)(0,2)(9,10)$$

<u>Caso 2</u>

El contador que queremos mover y el contador seis se encuentran en diferentes rectas verticales.

En general, lo que se hace es aplicar la permutación triangular que tiene como vértices al contador especial, al contador seis, y al contador que se

quiere mover.
Un ejemplo de este caso es si el contador que queremos mover es el siete entonces podemos aplicar la permutación triangular que se muestra en la figura:

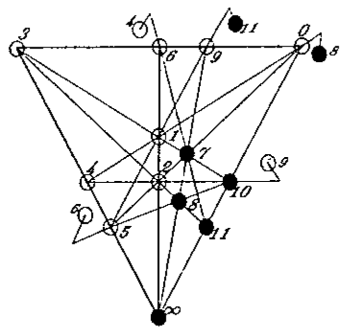


$$(4,5)(6,7)(2,10)(0,8)$$

Basta con demostrar esto para que G sea uno transitivo porque lo que acabamos de ver es que el contador seis lo podemos intercambiar con cualquier otro contador, entonces lo que podemos hacer cuando queremos mover el contador i al j es mover el i al contador seis y luego mandarlo a donde se encontraba el contador j originalmente utilizando el inverso de la permutación que manda al contador j al contador seis.

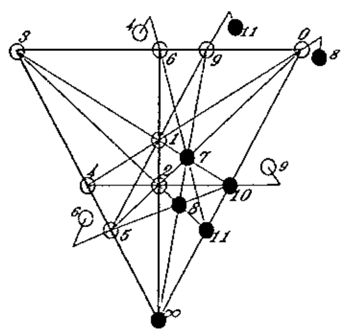
Para ver que es dos transitivo es suficiente con ver que podemos mandar cualquiera dos contadores a los dos contadores de arriba de la línea vertical de la izquierda, i.e. al contador seis y al contador cinco.
Utilizando el procedimiento anterior podemos mandar cualquier contador al contador de arriba de la línea vertical de la izquierda, i.e. al contador seis, y después fijarnos donde quedo el contador que queremos mandar al segundo contador de la línea vertical de la izquierda, i.e. al contador cinco, y mandarlo ahí mediante dos permutaciones triangulares.
En general, sea l la recta (vertical) que contiene a los contadores seis y cinco, y al contador especial en su posición inicial. Despues de mover el contador que se desea al contador seis se tienen los siguientes casos:
• El contador que se desea mover al contador cinco se encuentra ahí.
Un ejemplo de este caso es si queremos mandar el contador 3 al contador 6

y el contador 4 al contador 5.



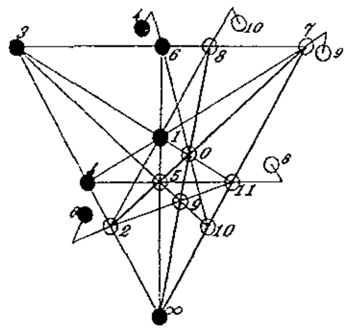
$(4,5)(3,6)(0,9)(1,2)$

• El contador que se desea mover al contador cinco se encuentra en la recta l pero no en el vértice correcto.
Un ejemplo de este caso es si queremos mandar el contador 3 al contador 6 y el contador 5 al contador 5 (i.e. dejar fijo al contador 5).

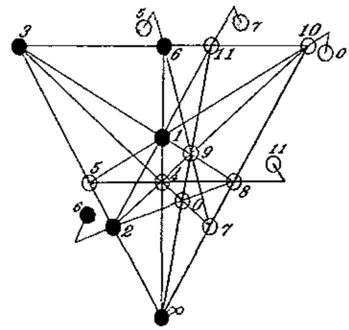


$(4,5)(3,6)(0,9)(1,2)$

Entonces, después se pueden aplicar las permutaciones triangulares que se muestran en las figuras·



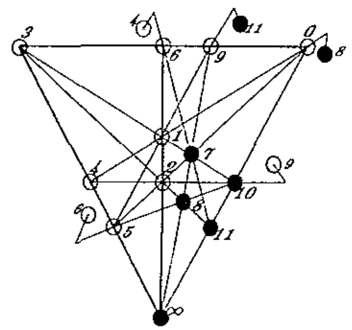
$(8,9)\,(0,7)\,(2,5)\,(10,11)$



$(0,9)\,(8,11)\,(4,5)\,(7,10)$

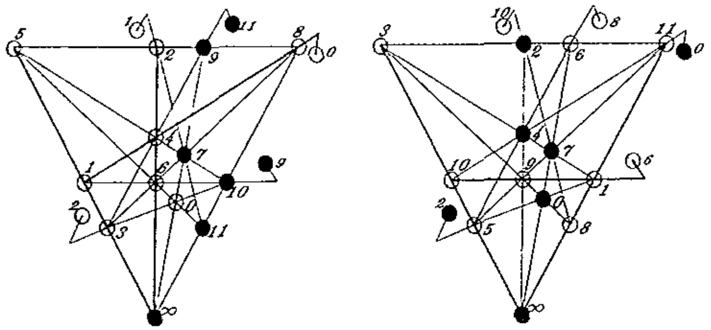
- el contador que se desea mover al contador cinco no se encuentra en la recta l.

Un ejemplo de este caso es si queremos mandar el contador 3 al contador 6 y el contador 10 al contador 5



$(4,5)(3,6)(0,9)(1,2)$

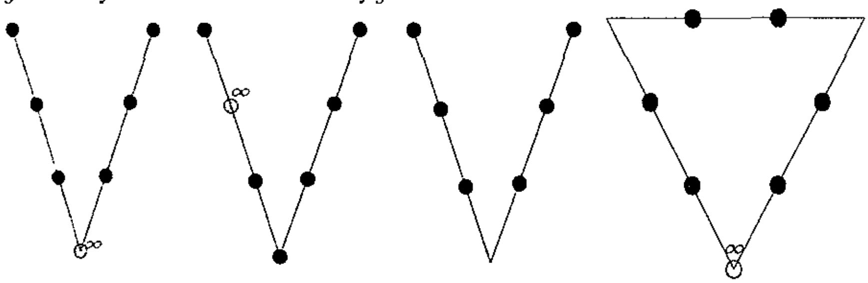
Entonces, después se pueden aplicar las permutaciones triangulares que se muestran en las figuras:



(3, 5)(1, 4)(0, 8)(2, 6)   (3, 5)(1, 10)(6, 9)(8, 11)

Con esto se demuestra que el grupo G es dos veces transitivo. ■

Definición 68 *Las hexadas son conjuntos de 6 contadores que tienen las siguientes formas dentro de la configuración:*



Tipo 1   *Tipo* 2   *Tipo* 3   *Tipo* 4

La tipo 1 está conformada por dos rectas que se intersectan en el punto especial, la tipo 2 está conformada por dos rectas en donde una de ellas contiene el punto especial y el punto especial no es punto de intersección, la tipo 3 está conformada por dos rectas de las cuales ninguna de las dos contiene al punto especial y la tipo 4 está conformada por tres rectas de las cuales dos de ellas se intersectan en el punto especial.

Los diferentes tipos de hexadas se pueden contar de la siguiente forma:

Tipo 1, tomando dos de las cuatro rectas que contienen al punto especial, $\binom{4}{2} = 6$;

Tipo 2, tomando una de las cuatro rectas que contienen al punto especial después uno de los tres contadores que contiene dicha recta y por último tomando una de las tres rectas restantes que contienen al contador elegido, $4 \cdot 3 \cdot 3 = 36$;

Tipo 3, tomando cualquiera de los doce contadores y después eligiendo dos de las tres rectas que contienen al contador elegido y que no contienen al punto especial, $12 \cdot \binom{3}{2} = 36$;

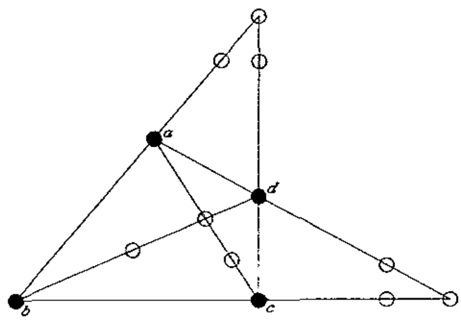
Tipo 4, tomando dos de las cuatro rectas que contienen al punto especial después eligiendo un contador de cada una de las rectas elegidas con los cuales determinamos la tercer recta de la hexada, $\binom{4}{2} \cdot 3^2 = 54$;

Con lo cual obtenemos un total de 132 hexadas.

Lema 69 *Dados 5 contadores existe una única hexada que los contiene.*

Demostración. Sean a, b, c, d, e los cinco contadores dados.
La demostración esta dividida en casos y para eliminar uno de los casos tenemos la siguiente afirmación.

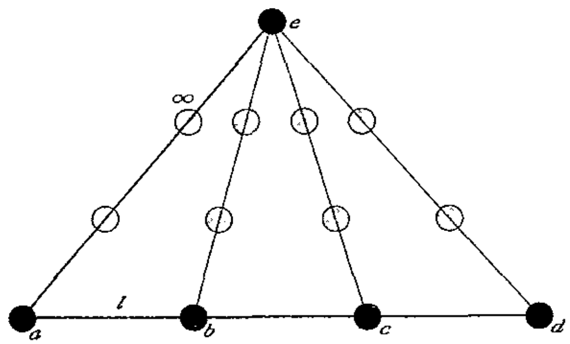
Afirmación. Dados cinco contadores existe una recta l tal que l contiene al menos tres de los contadores dados.
Demostración de la afirmación. Supongamos que en el conjunto de contadores a, b, c, d no hay tres colineales, porque de no ser cierta la suposición demostramos la afirmación.
Entonces, al tomar las rectas determinadas por estos contadores obtenemos la siguiente subconfiguración:



Al observar la subconfiguración tenemos que las seis rectas determinadas por los contadores a, b, c, d contienen a los trece contadores de la configuración $P_2(3)$. Por lo tanto, el contador e se encuentra contenido en una de las rectas de la configuración y dicha recta contiene tres de los contadores. Por lo que queda demostrada la afirmación.

Sea l la recta (o una de las rectas) que más contadores contiene de los cinco contadores dados.

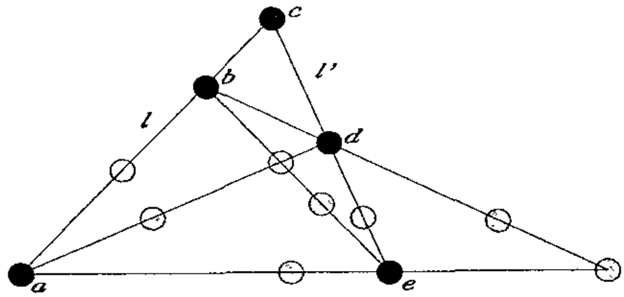
Caso 1. La recta l contiene cuatro de los contadores dados. Sin pérdida de generalidad, $a, b, c, d \in l$. Al tomar las rectas determinadas por estos contadores obtenemos la siguiente configuración:



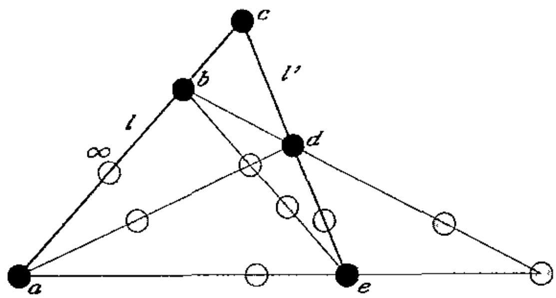
Podemos observar que la única hexada determinada por los cinco contadores a, b, c, d, e es la de tipo 2 que se encuentra señalada.

Caso 2. La recta l contiene tres de los contadores dados. Sin pérdida de generalidad, $a, b, c \in l$. Y existe la recta l', $l \neq l'$, tal que l' también contiene tres de los contadores dados. Por la estructura de la configuración $P_2(3)$, la única posibilidad es que l' contenga a d, e y a uno de los contadores contenidos en l. Sin pérdida de generalidad, supongamos que $c, d, e \in l'$.

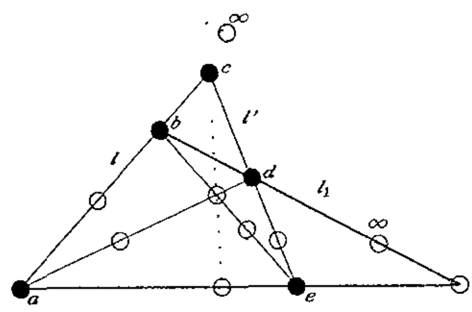
Al tomar las rectas determinadas por estos contadores obtenemos la siguiente configuración:



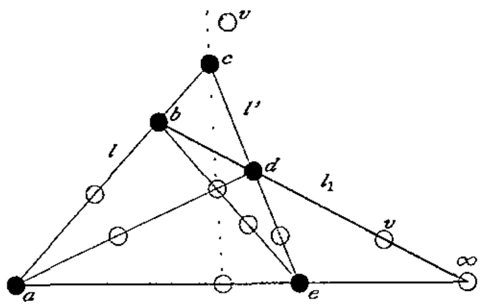
Donde obtenemos los siguientes subcasos:
Subcaso 2.1. El contador especial está contenido en la recta l (o en la recta l'). Como se muestra en la figura:



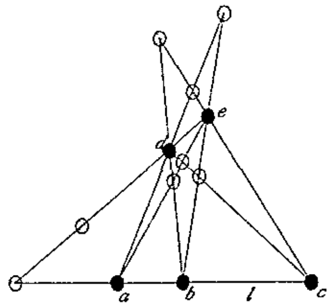
Podemos observar que la única hexada determinada por los cinco contadores a, b, c, d, e es la de tipo 2 que se encuentra señalada.
Subcaso 2.2. El contador especial está contenido en exactamente una de las rectas que contienen exactamente dos de los contadores dados. Sin pérdida de generalidad, supongamos que el contador especial se encuentra en la recta l_1. Como se muestra en la figura:



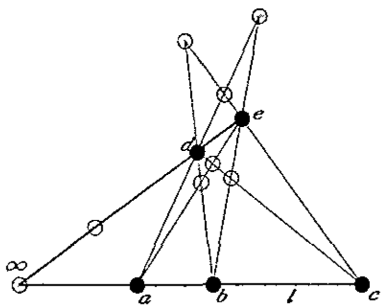
Podemos observar que la única hexada determinada por los cinco contadores a, b, c, d, e es la de tipo 4 que se encuentra señalada.
<u>Subcaso 2.3.</u> El contador especial está contenido en exactamente dos de las rectas que contienen exactamente dos de los contadores dados. Sin pérdida de generalidad, supongamos que el contador especial se encuentra en la recta l_1. Como se muestra en la figura:



Podemos observar que la única hexada determinada por los cinco contadores a, b, c, d, e es la de tipo 4 que se encuentra señalada.
<u>Caso 3.</u> La recta l contiene tres de los contadores dados. Sin pérdida de generalidad, $a, b, c \in l$. Y no existe recta l', $l \neq l'$, tal que l' también contiene tres de los contadores dados. Como se muestra en la figura:



De donde obtenemos los siguientes subcasos:
Subcaso 3.1. El contador especial está contenido en la recta l. Como se muestra en la figura:

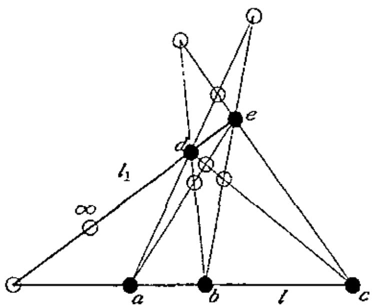


Podemos observar que la única hexada determinada por los cinco contadores a, b, c, d, e es la de tipo 1 que se encuentra señalada.
Subcaso 3.2. El contador especial está contenido en exactamente una de las rectas que contienen exactamente dos de los contadores dados. Por lo tanto el punto especial se encuentra en la recta l_1, así como se muestra en la figura:

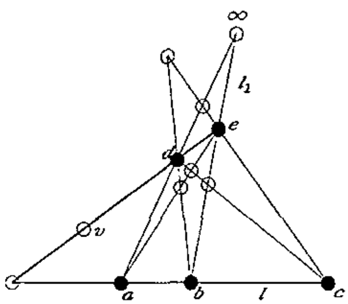
determinar en cuánto es necesario incrementar la productividad para recuperar los costos.

Por otra parte, los directivos tampoco reconocen como su función la de formar o capacitar recursos humanos para el trabajo y mantienen opiniones tradicionales al respecto, considerándolas como un gasto que están en incapacidad de realizar. Es por eso que muchas empresas sólo tienden a cumplir con lo establecido en la ley, únicamente como un trámite sin tomar en cuenta que el capacitar efectivamente al personal les redituaría beneficios tanto para aumentar la productividad como para que el personal tenga un mejor desempeño encaminado a brindar formación tecnológica sólidamente enraizada en las necesidades y recursos de dicha empresa.

Analizando la situación actual, se puede observar que todos los puntos anteriores se cumplen generalmente sólo de manera formal; es decir, que los patrones se limitan a cumplir ante la ley con los planes de capacitación y adiestramiento, sin buscar incrementar la productividad de los trabajadores (en beneficio tanto de la empresa como de los trabajadores mismos, que es la finalidad de la capacitación y el adiestramiento). En México esto sucede principalmente en la pequeña y mediana empresa, ya que se observa que en las filiales de las grandes compañías extranjeras sí se le da un gran énfasis a la educación de sus trabajadores.



Podemos observar que la única hexada determinada por los cinco contadores a, b, c, d, e es la de tipo 1 que se encuentra señalada.
<u>Subcaso 3.3.</u> El contador especial está contenido en exactamente dos de las rectas que contienen exactamente dos de los contadores dados. Sin pérdida de generalidad, supongamos que el contador especial se encuentra en la recta l_1. Como se muestra en la figura:



Podemos observar que la única hexada determinada por los cinco contadores a, b, c, d, e es la de tipo 3 que se encuentra señalada.
<u>Caso 4.</u> La recta l contiene dos de los contadores dados. Este caso no es posible por lo que se demostró en la afirmación.

Por lo tanto, dados cinco contadores existe una única hexada que los contiene.
■

Lema 70 *Al realizar algún movimiento admisible en nuestra configuración ($P_2(3)$), hexadas van a dar a hexadas aunque posiblemente de distinto tipo; i.e. el conjunto de hexadas es un invariante ante los movimientos admisibles.*

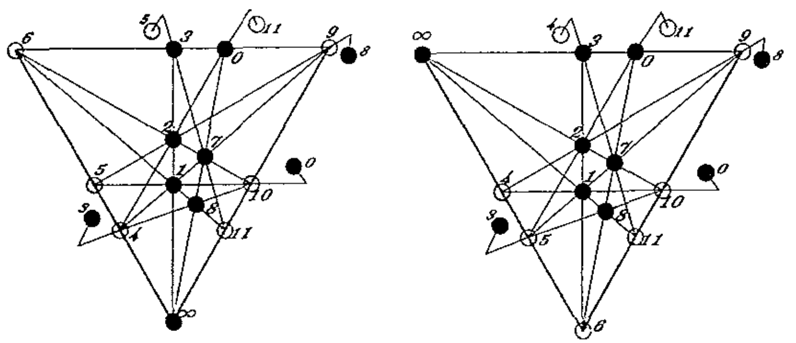
Demostración.

<u>Caso 1.</u>

Tomemos una hexada del tipo 1, en donde tenemos dos tipos esencialmente distintos de movimientos: que tomemos una de las rectas de la hexada para realizar nuestro movimiento y que tomemos una de las otras dos rectas que contienen al contador especial y no contienen contadores de la hexada.

<u>Subcaso 1.1.</u>

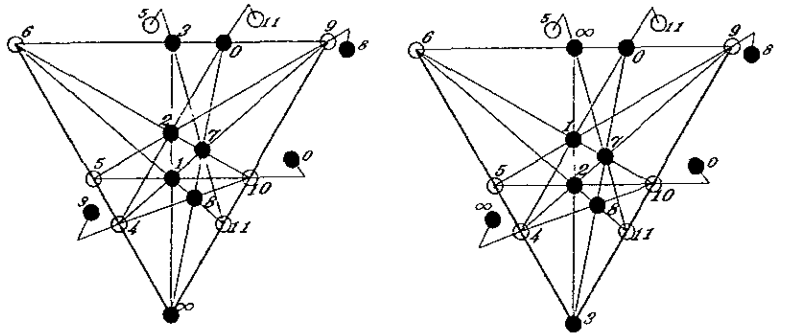
Si tomamos una de las rectas de la hexada para realizar nuestro movimiento, esencialmente lo que pasa es que mandamos una hexada del tipo 1 a una del tipo 2, por ejemplo:



$(\infty, 6)\,(4, 5)$

<u>Subcaso 1.2.</u>

Si tomamos una de las otras dos rectas que contienen al contador especial y no contienen contadores de la hexada, esencialmente lo que pasa es que mandamos una hexada del tipo 1 a una del tipo 3, por ejemplo:



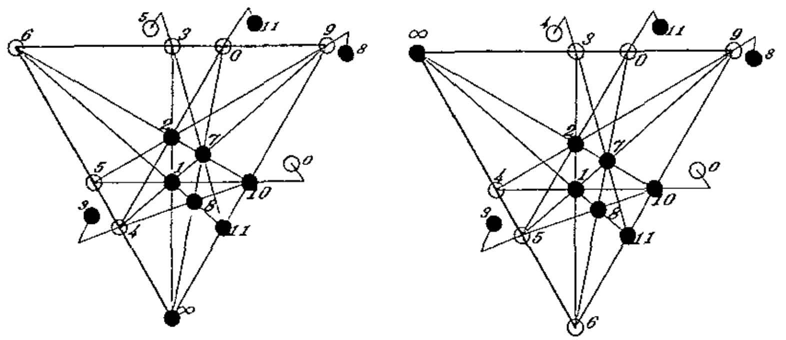
$(\infty, 3)\,(1, 2)$

Caso 2

Tomemos una hexada del tipo 2. En donde tenemos tres tipos esencialmente distintos de movimientos. El primero que es tomar la recta que contiene 3 contadores de la hexada y al contador especial y los otros dos que es tomar una de las tres rectas restantes que contienen al contador especial.

Subcaso 2.1.

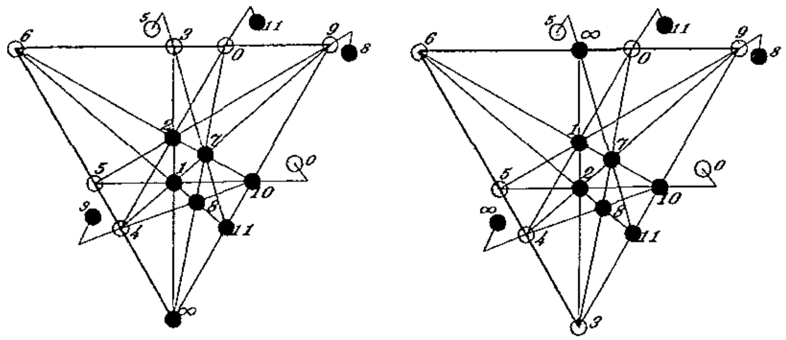
Si tomamos la recta que contiene 3 contadores de la hexada y al contador especial, esencialmente lo que pasa es que mandamos una hexada del tipo 2 a una del tipo 1, por ejemplo:



$(\infty, 6)\,(4, 5)$

Subcaso 2.2.

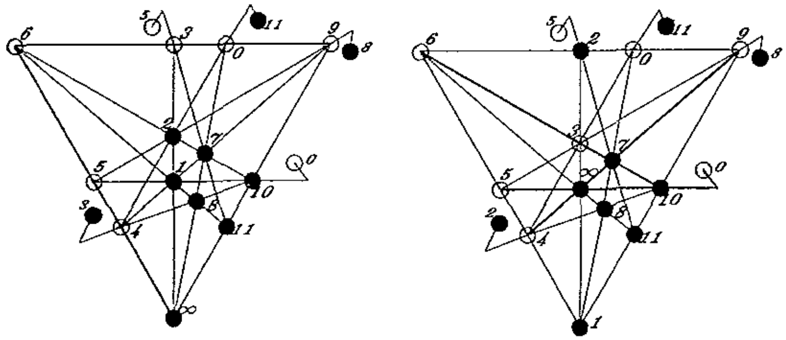
Si tomamos una de las rectas restantes que contienen al contador especial, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 2 a una del tipo 2, por ejemplo:



$(\infty, 3)\,(1, 2)$

Subcaso 2.3.

Si tomamos una de las rectas restantes que contienen al contador especial, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 2 a una del tipo 4, por ejemplo:



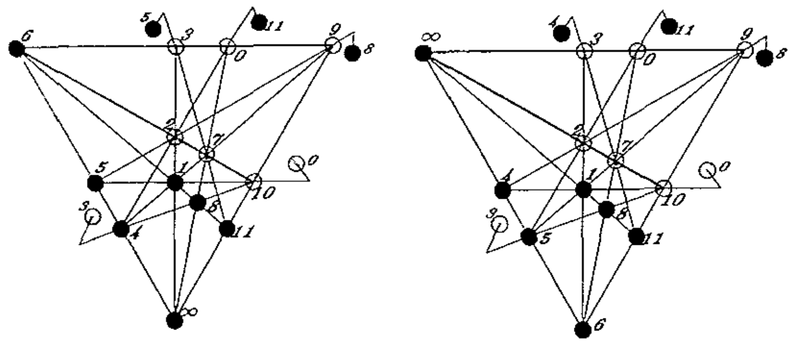
$(\infty, 1)\,(2, 3)$

Caso 3.

Tomemos una hexada del tipo 3, en donde tenemos cuatro tipos esencialmente distintos de movimientos. Los primeros dos que es tomar la recta que contiene al contador especial y que no contiene contadores de la hexada y los otros dos que es tomar una de las tres rectas restantes que contienen al contador especial y a dos contadores de la hexada.

Subcaso 3.1.

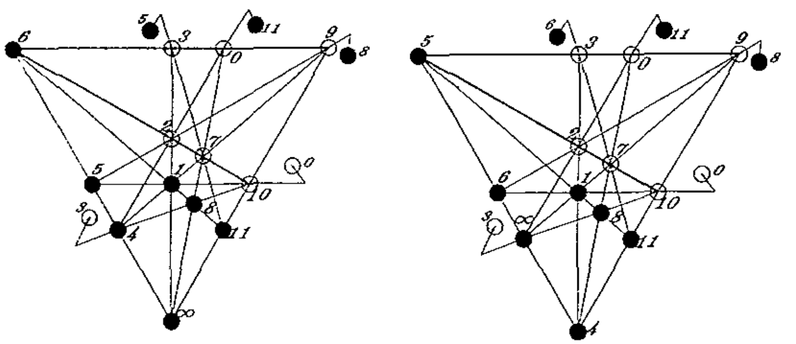
Si tomamos la recta que contiene al contador especial y que no contiene contadores de la hexada, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 3 a una del tipo 1, por ejemplo:



$(\infty, 6)\,(4, 5)$

Subcaso 3.2.

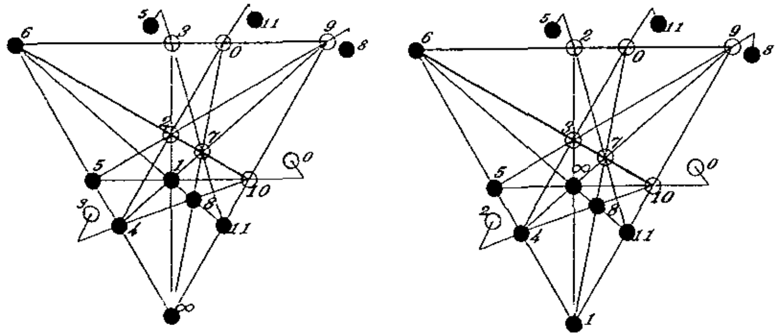
Si tomamos la recta que contiene al contador especial y que no contiene contadores de la hexada, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 3 a una del tipo 3, por ejemplo:



$(\infty, 4)\,(5, 6)$

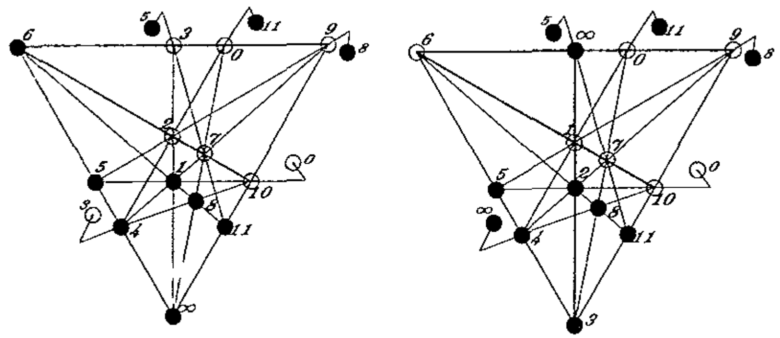
Subcaso 3.3.

Si tomamos una de las tres rectas restantes que contienen al contador especial y a dos contadores de la hexada, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 3 a una del tipo 3, por ejemplo:



$(\infty,1)\,(2,3)$

Subcaso 3.4.
Si tomamos una de las tres rectas restantes que contienen al contador especial y a dos contadores de la hexada, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 3 a una del tipo 2, por ejemplo:



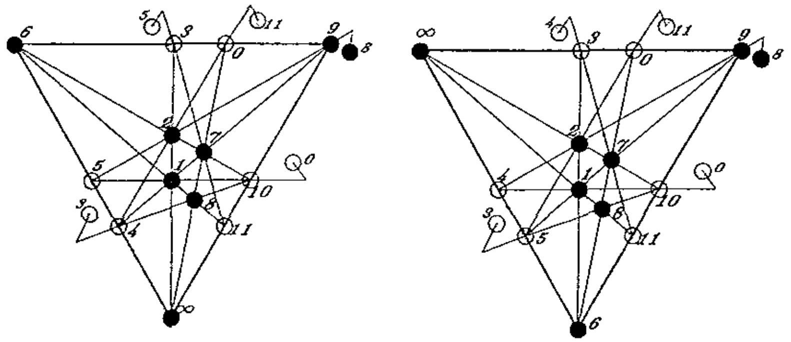
$(\infty,3)\,(1,2)$

Caso 4
Tomemos una hexada del tipo 4, en donde tenemos cuatro tipos esencialmente distintos de movimientos. Los primeros dos que es tomar una de las rectas que contiene al contador especial y a dos contadores de la hexada y los otros dos que es tomar una de las dos rectas que contiene al contador

especial y a un contador de la hexada.

Subcaso 4.1.

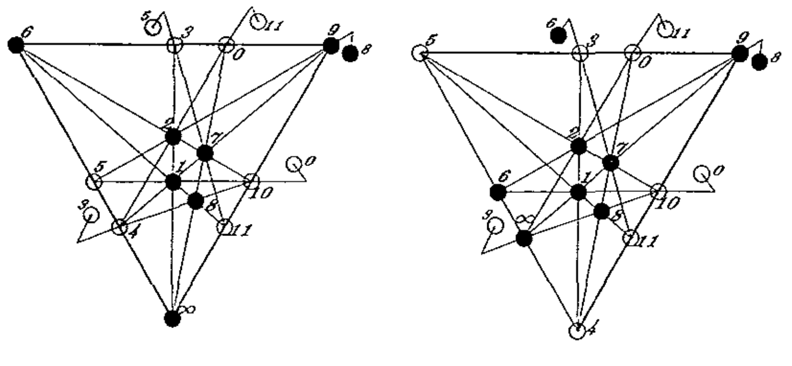
Si tomamos una de las rectas que contiene al contador especial y a dos contadores de la hexada, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 4 a una del tipo 4, por ejemplo:



$(\infty, 6)\,(4, 5)$

Subcaso 4.2.

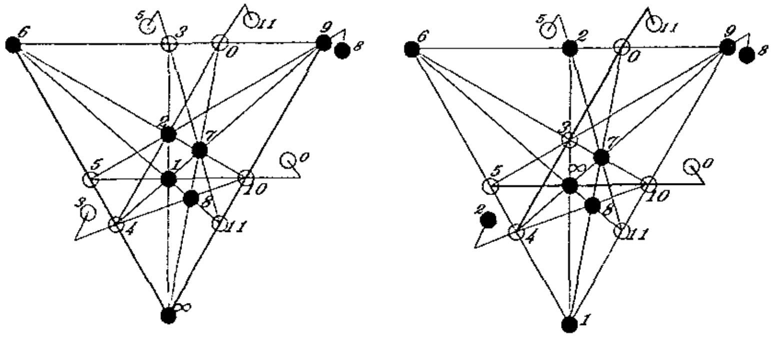
Si tomamos una de las rectas que contiene al contador especial y a dos contadores de la hexada, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 4 a una del tipo 3, por ejemplo:



$(\infty, 4)\,(5, 6)$

Subcaso 4.3.

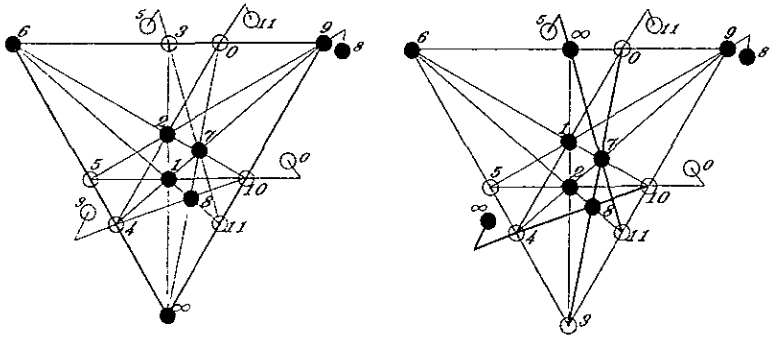
Si tomamos una de las dos rectas que contiene al contador especial y a un contador de la hexada, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 4 a una del tipo 2, por ejemplo:



$(\infty, 1)\,(2, 3)$

Subcaso 4.4.

Si tomamos una de las dos rectas que contiene al contador especial y a un contador de la hexada, en uno de los movimientos admisibles esencialmente lo que pasa es que mandamos una hexada del tipo 4 a una del tipo 4, por ejemplo:



■

$(\infty, 3)\,(1, 2)$

Observación 71 *Con el* lema 69 *y* lema 70 *demostramos que el conjunto de contadores (como elementos) y el conjunto de hexadas (como bloques) determinan el sistema de Steiner* $S(5, 6, 12)$*, y que los movimientos admisibles* *actúan como automorfismos del sistema de Steiner* $S(5,6,12)$.

Sabemos que el grupo M_{12} tiene multiplicador de Schur de orden dos. Y el grupo G lo muestra con la existencia del grupo $2G$ que tiene un homomorfismo a G con núcleo de orden dos. Esto puede construirse como la permutación de 24 símbolos:

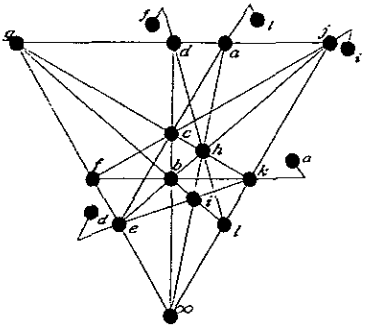
$$\pm a, \pm b, \pm c, ..., \pm k, \pm l$$

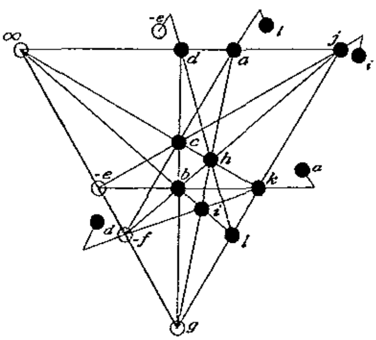
de tal forma que si ignoramos los signos obtenemos permutaciones las cuales son elementos de G. También se podrían usar $\pm 0, \pm 1, \pm 2, ..., \pm 10, \pm 11$ como símbolos, pero utilizaré $\pm a, \pm b, \pm c, ..., \pm k, \pm l$ para evitar confusiones más adelante.

Lo que tenemos ahora es un contador especial y 24 etiquetas para los 12 contadores. Y tomamos las transformaciones que se encuentran definidas de manera similar a las anteriores (las de G), lo que hacen ahora los movimientos admisibles es intercambiar al contador especial con cualquier otro contador que se encuentre en la misma recta e intercambiar los dos contadores restantes y cambiarles de signo.

Por ejemplo:

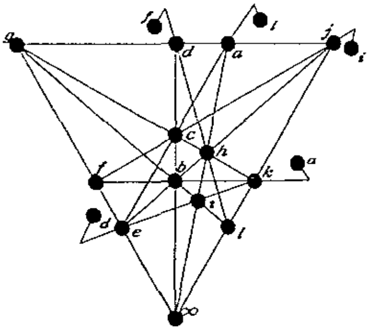
- Un movimiento admisible simple:

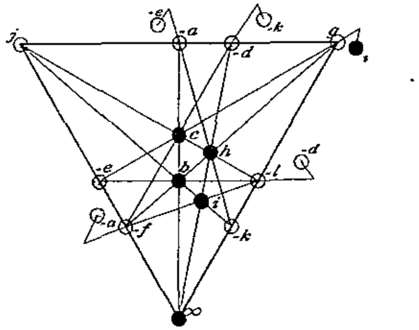




$\infty \longleftrightarrow g \; ; \; e \longleftrightarrow f$

- Una permutación triangular:





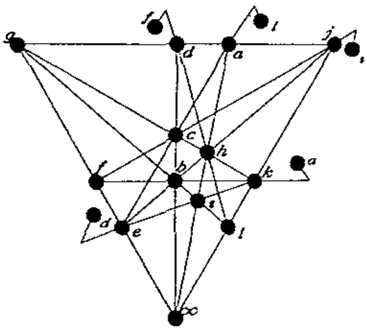
$$\infty \longleftrightarrow g \ ; \ e \longleftrightarrow f$$
$$\infty \longleftrightarrow j \ ; \ a \longleftrightarrow d$$
$$\infty \longleftrightarrow g \ ; \ k \longleftrightarrow l$$

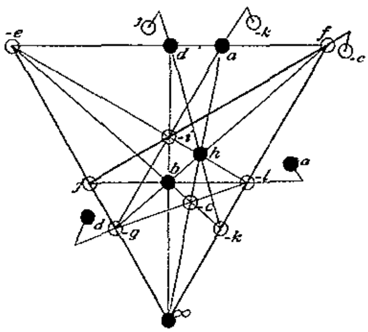
Lema 72 *2G es dos veces transitivo.*

Demostración. Como ya demostramos 2-transitividad en G es suficiente con demostrar que existe una transformación que fija a uno de los contadores involucrados en la 2-transitividad y le cambia de signo al otro.

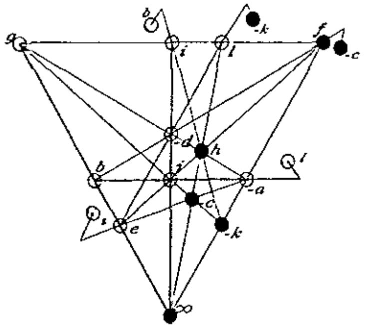
Caso 1

Los dos contadores se encuentran en la misma recta vertical. Por ejemplo, fijar al contador g y cambiarle de signo al contador f.





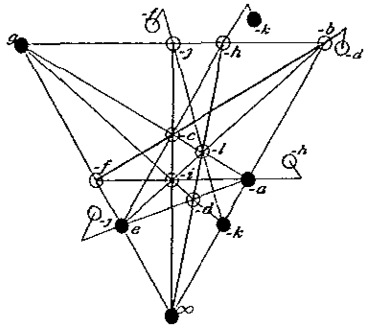
$$\infty \longleftrightarrow f \ ; \ e \longleftrightarrow g$$
$$\infty \longleftrightarrow j \ ; \ c \longleftrightarrow i$$
$$\infty \longleftrightarrow f \ ; \ k \longleftrightarrow l$$



$\infty \longleftrightarrow j\ ;\ \ -e \longleftrightarrow -g$

$\infty \longleftrightarrow b\ ;\ a \longleftrightarrow -l$

$\infty \longleftrightarrow j\ ;\ d \longleftrightarrow -i$



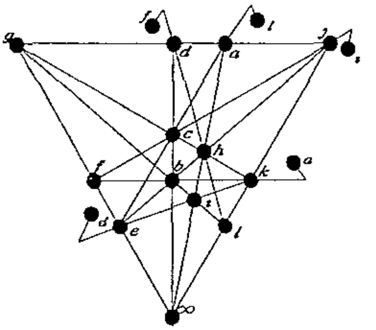
$\infty \longleftrightarrow -d\ ;\ i \longleftrightarrow j$

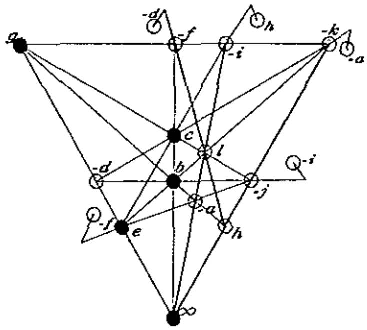
$\infty \longleftrightarrow -c\ ;\ b \longleftrightarrow f$

$\infty \longleftrightarrow -d\ ;\ h \longleftrightarrow l$

Caso 2

Los dos contadores se encuentran en distintas rectas verticales. Por ejemplo, fijar al contador g y cambiarle de signo al contador d.

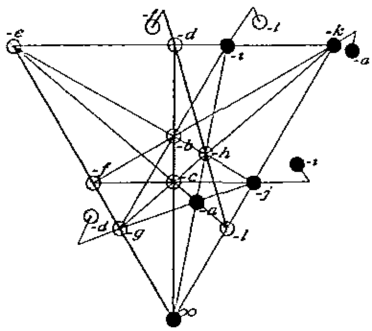




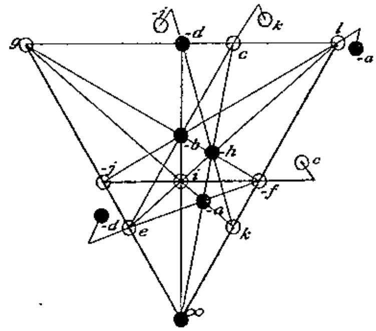
$\infty \longleftrightarrow h\ ;\ a \longleftrightarrow i$

$\infty \longleftrightarrow l\ ;\ d \longleftrightarrow f$

$\infty \longleftrightarrow h\ ;\ j \longleftrightarrow k$



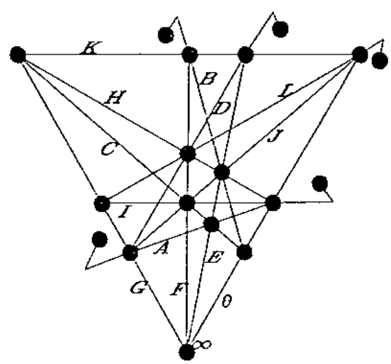
$\infty \longleftrightarrow -d \ ; \ e \longleftrightarrow g$
$\infty \longleftrightarrow -f \ ; \ h \longleftrightarrow l$
$\infty \longleftrightarrow -d \ ; \ b \longleftrightarrow c$



■

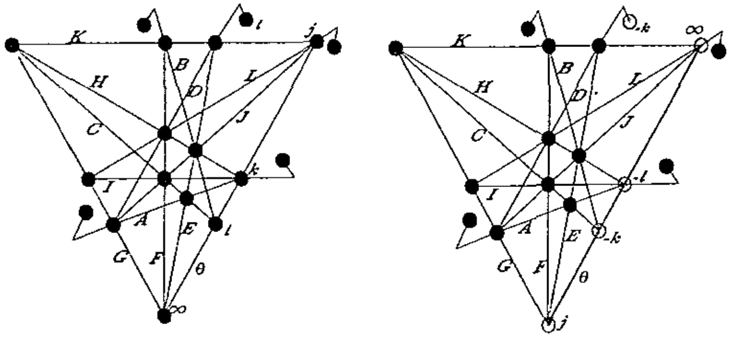
$\infty \longleftrightarrow -f \ ; \ -e \longleftrightarrow -g$
$\infty \longleftrightarrow -j \ ; \ -c \longleftrightarrow -i$
$\infty \longleftrightarrow -f \ ; \ -k \longleftrightarrow -l$

Designamos a cada recta con las etiquetas $A, B, ..., L, \theta$, llamaré a cada una de estas etiquetas con el nombre de *recta-contador* para diferenciarlos de los contadores asignados a los puntos Llamaré al contador θ con el nombre de *recta-contador especial*. La única condición para la asignación de los recta-contadores es que el contador y el recta-contador especial sean incidentes. La asignación que usaré es la que se muestra en la figura.



Ahora nuestros movimientos lo que hacen es intercambiar al contador especial con cualquier contador que se encuentre en el recta-contador especial

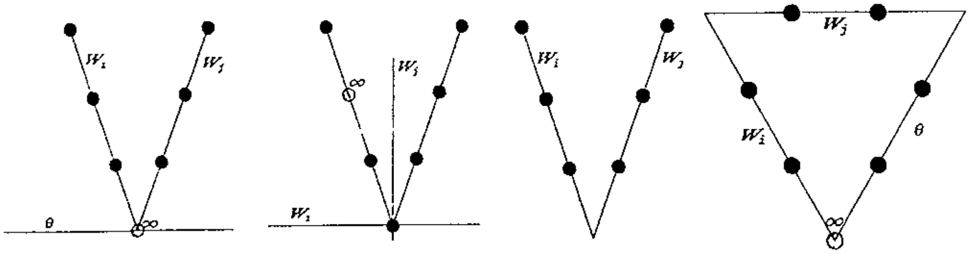
En la demostración es suficiente con ver que pasa con los contadores que se estan moviendo y los recta-contadores que los contienen. Tenemos que al realizar un movimiento admisible simple de los contadores, por ejemplo al aplicar el movimiento admisible $[\infty \longleftrightarrow j\ ;\ k \longleftrightarrow l]$ las contenciones de los contadores en los recta-contadores variaron de la siguiente forma:



$$\infty \longleftrightarrow j\ ;\ k \longleftrightarrow l$$

Al observar los valores que se obtienen con la función f, podemos ver que son los mismos; i.e. antes del movimiento admisible $f(k, A) = 1$ y después del movimiento admisible $f(-k, A) = -1 = -f(k, A)$. ∎

Observación 74 *Utilizando esta función podemos dar una definición distinta de las hexadas de la siguiente forma: Si tomamos dos recta-contadores* w_i *y* w_j *con* $i \neq j$*, tenemos que existen seis contadores tal que* $f(\_, w_i) = f(\_, w_j)$ *los cuales forman una hexada la cual es denotada con* $[W_i, W_j]$ *y existen seis contadores tal que* $f(\_, w_i) = -f(\_, w_j)$ *los cuales forman otra hexada la cual es denotada con* $[W_i, -W_j]$*. Al ir variando los recta-contadores obtenemos todas las hexadas posibles. Es muy fácil ver esto con la nueva definición de las hexadas, así como se muestra en las figuras siguientes:*



$[W_i, W_j]$ $\quad$ $[W_i, W_j]$ $\quad$ $[W_i, -W_j]$ $\quad$ $[W_i, -W_j]$

Con esta función también podemos construir una matriz de 12×12 tal que su entrada ij se obtiene con $f(v_i, w_j)$, la cual resulta ser una matriz de Hadamard.

La matriz que se obtiene es:

$$H = \begin{bmatrix} 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Es fácil verificar que esta matriz es de Hadamard.

De lo anterior tenemos que el lema 73 implica el lema 70. Esto se debe a la forma en que están definidas las hexadas y a que la función f se mantiene invariante ante los movimientos admisibles de la configuración $P_2(3)$.

Lema 75 *G actúa transitivamente en las hexadas.*

Demostración. En el lema 72 se demostró que $2G$ es 2 transitivo, como tenemos que si dualizamos el $P_2(3)$ volvemos a obtener el $P_2(3)$ tenemos que el dual de el lema 72 se cumple, esto es que el conjunto $\{\pm A, \pm B, .., \pm L\}$ es 2 transitivo bajo la acción de $2G'$.

Por lo que la hexada $[W_1, W_2]$ la podemos mandar a la hexada $[W_3, \pm W_4]$ para todo $W_1, W_2, W_3, W_4 \in W$. ∎

Lema 76 *Las transposiciones inducidas por las permutaciones triangulares de G en la hexada $\{0,1,2,3,7,8\}$ genera a S_6.*

Demostración. Tenemos que la permutación triangular $(4,5)(6,9)(0,3)(10,11)$ nos induce la transposición $(0,3)$ en la hexada. Análogamente podemos inducir las transposiciones $(0,2),(2,7),(7,1),(1,8)$, con las cuales podemos generar el elemento $(3,0,2,7,1,8) = (1,8)(7,1)(2,7)(0,2)(3,0)$.
Por el corolario 42 obtenemos que $\langle (0,3),(3,0,2,7,1,8) \rangle \cong S_6$. ∎

Hemos demostrado que el grupo G actúa transitivamente en las hexadas (lema 75) y junto con el lema 76 y el lema 69 concluimos que G es exactamente 5 transitivo (i.e. no es 6 transitivo).

Por lo tanto G es el grupo de Mathieu M_{12}.

Bibliografía

[*Co*] Conway, J.H. 1997. M_{13}. Surveys in Combinatorics, 1997. Cambridge University Press. 1-11.

[*CS*] Conway, J.H. y N.J.A. Sloane. 1988. *Sphere Packings, Lattices and Groups.* New York: Springer-Verlag.

[*Hu*] Hungerford, T.W. 1974. *Algebra.* New York: Springer-Verlag.

[*Ro*] Rotman, J.L. 1995. *An Introduction to the Theory of Groups.* 4th ed. Graduate Texts in Math. no.148. New York: Springer-Verlag.

[*VW*] Van Lint, J. H. y R. M. Wilson. 1992. *A course in combinatorics.* Cambridge University Press.