UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

Construcción y Propiedades del Grupo M_{12}

T E S I S

Que para Obtener el Título de

M A T E M A T I C O

P r e s e n t a

ARTURO MAGIDIN VISO

México, D. F. 1993

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INDICE

I. Introducción

> "La Teoría de Grupos es la rama de las Matemáticas en la que uno le hace algo a algo y después compara el resultado con el resultado obtenido de hacerle lo mismo a algo distinto, o de hacerle algo distinto a lo mismo."

Así describe James R. Newman a la Teoría de Grupos, que llama el ejemplo supremo del Arte de la Abstracción en las Matemáticas. Es, nos afirma, el instrumento más poderoso que ha sido inventado para iluminar y estudiar el concepto de estructura. Los grupos aparecen en todas las áreas de las Matemáticas, y además aparecen en el estudio de la estructura de los cristales, en el diseño de códigos de corrección de errores, en las ecuaciones relativistas de Lorentz, y en muchos otros lugares, la mayoría insospechados.

La Teoría de Grupos nace oficialmente en la víspera de la muerte de Évariste Galois en 1830, cuando se utiliza por primera vez el término de "grupo" en la carta que escribiera éste antes del duelo que le costara la vida. El concepto ya había sido manejado, aunque bajo el nombre de *transformaciones*, y sin mucha herramienta poderosa a la disposición de los matemáticos.

Treinta años después, en 1861, aparece en el prestigiado *Journal de Mathématiques Pures et Appliquée* una memoria con el título de *"Mémoire sur l'étude des fonctions de plusieurs quantités"*, por Émile Léonard Mathieu, matemático francés. En él, el autor describe cinco grupos que había construido, y que tenían propiedades interesantes.

En 1872 aparece en el mismo lugar un artículo de Camille Jordan, Ingeniero de Minas y una de las luminarias de las Teoría de Grupos. En el manuscrito, titulado *"Recherches sur les substitutions"*, Jordan prueba que dos de los grupos de Mathieu, que actúan en 11 y 12 letras (denotados usualmente por M_{11} y M_{12} respectivamente), son únicos en cuanto al concepto de transitividad exacta. Jordan prueba que M_{11} es el único grupo exactamente 4– transitivo no trivial, M_{12} el único grupo exactamente 5– transtivo no trivial, y que no existen grupos exactamente k– transitivos no triviales con $k \geq 6$.

Un año después publica Mathieu su segunda memoria sobre sus grupos, titulada *"Sur la fonction cinq fois transitive de 24 quantités"*, en la que busca presentar un algoritmo para la construcción de grupos multiplemente transitivos. En la memoria aparecen algunas

afirmaciones que carecen de justificación, e incluso utiliza un resultado del que nos dice "...nunca he dudado de la exactitud de este teorema, pero la demostración no me ha parecido plenamente satisfactoria y no la he publicado."

En 1938, Ernst Witt publica dos artículos en el Abh. Mat. Sem. von Hamburg, titulados *"Die 5-fach transitiven Gruppen von Mathieu"* y *"Über Steinersche Systeme"*. En ellos, Witt construye los cinco grupos de Mathieu de manera sistemática, demuestra sus propiedades más importantes, y establece su relación con los Sistemas de Steiner.

Otra propiedad importante de los cinco grupos de Mathieu es su propiedad de ser simples. La simplicidad de M_{11} fue establecida en 1896 por F. Cole; la de M_{12} por G.A. Miller en 1899, y la de los otros tres, M_{22}, M_{23}, y M_{24} por el mismo Miller en 1900. Curiosamente, Miller había publicado un artículo en el *"Messenger of Mathematics"* en 1898, "demostrando" que M_{24} no existía. Dicho artículo, sobra decir, no aparece en la colección de obras completas de Miller.

Los grupos simples finitos, que juegan un papel fundamental en la Teoría de Grupos, se pueden clasificar en 19 familias. Dieciocho de ellas son infinitas, y se conocen algoritmos para construír cualquier miembro de ellas.

La última familia contiene veintiseis miembros, que se conocen como los grupos simples *"esporádicos"*, pues son grupos que no se conforman a ningún patrón ni regla, y evaden todo tipo de clasificación general.

La búsqueda de los grupos simples esporádicos comenzó en 1860, con la publicación de la memoria de Mathieu, pues sus cinco grupos eran más excepcionales de lo que él mismo imaginaba: eran grupos que habrían de pertenecer a la familia de los esporádicos.

El problema fue que durante más de cien años, todos los grupos simples que se encontraban no eran esporádicos, lo que llevó a muchos a la conclusión de que los únicos esporádicos eran los cinco grupos de Mathieu. Pero el problema de la búsqueda cambió radicalmente en 1964, cuando Walter Feit de Yale y John Thompson de Cambridge publican la prueba de la conjetura de Burnside que todo grupo finito simple que no sea cíclico es de orden par. Los métodos desarrollados en la larga demostración de este hecho (más de 250 páginas) ayudaron en mucho a clasificar los grupos simples finitos.

Así, en 1965, Zvonimir Janko, de la Universidad de Heidelberg, anunció su descubrimiento de un grupo simple de orden 175560, que es uno de los esporádicos. Tres años después John Horton Conway de Cambridge sorprendió al mundo al encontrar tres más.

Para 1979 se tenían construidos 24 grupos esporádicos, incluyendo los cinco de Mathieu, y se sospechaba la existencia de dos más. En enero de 1980 se anunció la construcción de uno de ellos, J_4, y el segundo se construyó en febrero de 1980, F_1, conocido como *"el monstruo"* debido a su gran tamaño.

El descubrimiento del monstruo por parte de Griess fue seguido en el verano de 1980 por el trabajo de Michael Aschbacher de CalTech y de Daniel Gorenstein de Rutgers University, quienes rápidamente ataron los cabos sueltos en la clasificación de grupos simples finitos, probando entre otras cosas que la lista de 26 grupos simples esporádicos estaba completa, más de 120 años después de comenzarse.

Los grupos de Mathieu, que comenzaron el problema, mantuvieron el interés y atención de los matemáticos, en particular debido a las otras propiedades que tienen, como la transitividad múltiple y su relación con los Sistemas de Steiner y el Código de Golay, que se utiliza para construir rutinas de corrección de errores. Artículos sobre los grupos (en especial M_{24} que contiene copias isomorfas de los otros cuatro) continuan apareciendo en las páginas de las revistas de investigación.

Uno de estos artículos se publica en 1989. Titulado *"Natural Constructions of the Mathieu Groups"*, por R.T. Curtis, aparece en el Mathematical Procedures of the Cambridge Philosophical Society. En él, el autor presenta un algoritmo para construir los grupos de Mathieu en 12 y 24 letras, M_{12} y M_{24}. El artículo esboza tambien pruebas sobre algunas de las propiedades de estos grupos.

El grupo de Mathieu de grado 12, o como se denota usualmente M_{12}, es el objeto de estudio del presente trabajo.

En el presente trabajo se demostrará que el algoritmo de Curtis es válido, i.e. que los diversos grados de libertad que aparecen en la construcción son irrelevantes, y que se

puede elegir cualquiera de los caminos que se presentan, pues nos llevaran siempre al mismo grupo (o a copias isomorfas de él). Se probará además que dicho grupo es el grupo de Mathieu de grado 12, M_{12}.

También se dará un algoritmo, mucho más sencillo que el de Curtis, para construir generadores del grupo de Mathieu. Este algoritmo fue descubierto por el Dr. Humberto Cárdenas Trigos y el Dr. Emilio Lluis Riera, y se demostrará que da lugar efectivamente al grupo de Mathieu. Para terminar también se probarán algunas propiedades de M_{12}: el que sea un subgrupo máximo de A_{12}, el que sea su propio normalizador en S_{12}, y otros resultados más.

Veremos además dos maneras más de construir a M_{12}, cada una de las cuales nos otorgará una nueva visión de la estructura del grupo y de sus propiedades.

En el Capítulo II y el Capítulo III se desarrollará la base teórica y los resultados preliminares necesarios para el resto del trabajo. La construcción dada por Marshall Hall, Jr. en su libro "The Theory of Groups" se discute en el Capítulo IV. Esta construcción permite demostrar que M_{12} es el único grupo exactamente 5- transitivo no trivial, caracterizandolo. El Capítulo V presenta la construcción dada por Joseph J. Rotman en "An Introduction to the Theory of Groups", que se basa fuertemente en el trabajo de Ernst Witt y su artículo de 1938.

La íntima relación de M_{12} con el Sistema de Steiner de tipo $S(5,6,12)$ motiva la detallada discusión de este último que se lleva a cabo en el Capítulo VI. Esta discusión se basa en el trabajo del Dr. Humberto Cárdenas y del Dr. Emilio Lluis. Esta relación se utiliza en el Capítulo VII para presentar nuevas propiedades de M_{12}, y presentar una nueva construcción por generadores. Además se caracteriza a M_{12} como el grupo de automorfismos del Sistema de Steiner de tipo $S(5,6,12)$.

La última construcción que se da es la de R.T. Curtis, que se explora en el Capítulo VIII. Para terminar, el Capítulo IX presenta algunas de las propiedades de M_{12}, y menciona algunos otros hechos interesantes relacionados con él y el resto de los grupos de Mathieu. El Capítulo X contiene la bibliografía utilizada en el desarrollo de este trabajo.

El Apéndice A incluye un pequeño poema anónimo sobre grupos simples, que apareció por primera vez en el American Mathematical Monthly en noviembre de 1973, y posteriormente

en la columna de Mathematical Games de Martin Gardner, en el Scientific American de Junio de 1980.

El Apéndice B contiene una tabla con los nombres y ordenes de los veintiseis grupos simples esporádicos que se conocen, así como una tabla que indica cómo están estos grupos involucrados unos en otros.

II. Conceptos Preliminares

En este capítulo definiremos los conceptos de *Acción de Grupos*, *Estabilizador*, *Transitividad*, *Orbitas*, *Transitividad Nítida*, *Bloques* y *Primitividad*. También se demostrarán algunas de las propiedades elementales de los grupos transitivos, que se requerirán más adelante.

DEFINICIÓN

Si X es un conjunto y G un grupo, entonces X es un G-conjunto sii existe una función $G \times X \to X$, denotada por $(g,x) \mapsto gx$, tal que:

(i) $1x = x$

(ii) $g(hx) = (gh)x$

para toda $x \in X$, y todas $g, h \in G$. Se dice entonces que G actúa en X. Si $|X| = n$, entonces n es el grado de X.

PROPOSICIÓN 2.1

Todo G-conjunto define un homomorfismo $\varphi: G \to S_X$ dado por $\varphi(g): x \mapsto gx$ (su acción). Recíprocamente, todo homomorfismo $\psi: G \to S_X$ da a X una estructura de G-conjunto.

Demostración: Sea X un G-conjunto. Si $g \in G$, entonces $\varphi(g)$ es una permutación de X, pues $g^{-1}(gx) = (g^{-1}g)(x) = (1)x = x$, y además $g(g^{-1}x) = x$ de manera análoga. Es morfismo por el inciso *(ii)* de la definición de G-conjunto. Para el recíproco, definamos $gx = \psi(g)(x)$. Como ψ es morfismo, $\psi(1) = 1$, y por lo tanto $1x = x \ \ \forall x \in X$. También por ser morfismo, tenemos que

$$g(hx) = \psi(g)(hx) = \psi(g)(\psi(h)(x)) = \psi(g) \circ \psi(h)(x) = \psi(gh)(x) = (gh)(x),$$

de manera que el segundo inciso se satisface.

□

DEFINICIÓN

Un G-conjunto es fiel sii la acción asociada $\varphi: G \to S_X$ es inyectiva.

Cuando la acción del grupo es fiel, por conveniencia identificaremos el grupo con su imágen en S_X, de manera que cualquier acción fiel de grupo dará lugar a un grupo de permutaciones. En ese caso, diremos simplemente que G es un grupo de permutaciones.

DEFINICIÓN

Si X es un G-conjunto, la órbita (en G) de un punto $x \in X$ es el subconjunto de X

$$Gx = \{gx \mid g \in G\}.$$

DEFINICIÓN

Si X es un G-conjunto y $x_1, \ldots, x_k \in X$, el estabilizador $G_{x_1,\ldots,x_k}$ es el subgrupo de G

$$G_{x_1,\ldots,x_k} = \left\{ g \in G \;\middle|\; gx_i = x_i, \forall i \in \{1,\ldots,k\} \right\}$$

Claramente X es un $G_{x_1,\ldots,x_k}$-conjunto, siempre que sea un G-conjunto. Además, si $x, y \in X$, tenemos que

$$(G_x)_y = G_{x,y} = (G_y)_x.$$

DEFINICIÓN

Un G-conjunto X es transitivo sii $\forall x, y \in X \; \exists g \in G$ tal que $gx = y$.

Claramente, un G-conjunto es transitivo si y sólo si tiene únicamente una órbita.

Como en teoría de grupos elemental, se verifica fácilmente que $i_G(G_x)$ es el cardinal de la órbita Gx. De esto se obtiene la siguiente proposición:

PROPOSICIÓN 2.2

Si X es un G-conjunto transitivo de grado n, y $x \in X$, entonces

$$|G| = n|G_x|$$

Si además las acción es fiel, entonces $|G_x|$ es un divisor de $(n-1)!$.

Demostración: Tenemos que $|G| = i_G(G_x)|G_x|$. Ya que $i_G(G_x)$ es el número de elementos en la órbita Gx, y por ser transitivo se sigue que $Gx = X$, tenemos que $i_G(G_x) = n$. Si además la acción es fiel, entonces G se identifica con un subgrupo de S_n. Entonces G_x se identifica con uno de S_{n-1}, y el resultado se sigue por Teorema de Lagrange.

□

PROPOSICIÓN 2.3

Sea X un G-conjunto transitivo, y sean $x, y \in X$.

(i) Si $tx = y$ para alguna $t \in G$, entonces $G_y = tG_xt^{-1}$.

(ii) X tiene el mismo número de G_x-órbitas que de G_y-órbitas.

Demostración: (i) Sea $g \in G_x$. Por lo tanto, $tgt^{-1}(y) = tg(x) = t(x) = y$. Por lo tanto $tG_xt^{-1} \subset G_y$. Análogamente se obtiene que $t^{-1}G_yt \subset G_x$, y el resultado se sigue.

(ii) Ya que la acción de G es transitiva, existe $t \in G$ tal que $tx = y$. Consideremos la partición de X en sus G_x-órbitas, $\{G_xa_i \mid i \in I\}$, con $a_i \in X$. Definimos $b_i = ta_i \in X$. Entonces los conjuntos $\{G_yb_i \mid i \in I\}$ son las G_y-órbitas de X, pues $G_yb_i = tG_xt^{-1}b_i = tG_xa_i$. Puesto que t es una permutación de X, manda particiones en particiones, de manera que los subconjuntos G_yb_i forman una partición, y G_y actúa transitivamente en cada uno de ellos, de manera que se trata de las G_y-órbitas.

□

DEFINICIÓN

Si X es un G-conjunto transitivo, el rango de X es el número de G_x-órbitas de X, visto como G_x- conjunto.

Gracias a la Proposición 2.3, la definición tiene sentido y no depende de la $x \in X$ particular que tomemos.

PROPOSICIÓN 2.4

Sea X un G-conjunto transitivo, y sea $x \in X$. El rango de X es el número de clases laterales dobles $G_x - G_x$ en G.

Demostración: Definimos $\pi: \{G_x\text{-órbitas de } X\} \to \{G_x - G_x \text{ clases laterales dobles}\}$ dado por $\pi(G_x y) = G_x g G_x$, donde $gx = y$.

π está bien definida, pues si $hx = y$, entonces $gx = hx$, y por lo tanto $g^{-1}hx = x$. De ahí que $g^{-1}h \in G_x$, $gG_x = hG_x$, y por lo tanto $G_x g G_x = G_x h G_x$.

Además, π es inyectiva, pues si $\pi(G_x y) = \pi(G_x z)$, entonces $G_x g G_x = G_x h G_x$ (con $gx = y$, y $hx = z$). Entonces $g = t_1 h t_2$ para $t_1, t_2 \in G_x$, y $y = t_1 z$. Por lo tanto, $G_x y = G_x z$.

Por último, π es suprayectiva, pues si $g \in G$, y $gx = y$, entonces $\pi(G_x y) = G_x g G_x$. De manera que la biyectividad de π termina la prueba.

□

DEFINICIÓN

Sea X un G-conjunto de grado n y sea $k \leq n$ un entero positivo. Se dice que X es k-transitivo sii para todo par de k-adas $(x_1, \ldots, x_k)$ y $(y_1, \ldots, y_k)$, con entradas diferentes entre sí en X, existe $g \in G$ tal que $gx_i = y_i \; \forall i \in \{1, \ldots, k\}$

Si $k > 1$, entonces k-transitividad implica trivialmente $(k-1)$- transitividad. Si $k = 2$ se dice que X es doblemente transitivo, triplemente transitivo si $k = 3$. En general, si $k > 1$ se dice que X es múltiplemente transitivo.

PROPOSICIÓN 2.5

Sea X un G-conjunto. X es k-transitivo ($k \geq 2$) si y sólo si $\forall x \in X$, $X - \{x\}$ es un G_x-conjunto $(k-1)$-transitivo.

Demostración: Sea $x \in X$. Sean $x_1, \ldots, x_{k-1}, y_1, \ldots, y_{k-1} \in X - \{x\}$, con las x_i distintas entre sí, lo mismo que las y_i. Por lo tanto $\exists g \in G$ tal que $gx_i = y_i \;\; i = 1, \ldots, k-1$, y además $gx = x$ (i.e., $g \in G_x$). Esto demuestra la suficiencia. Para la necesidad, sean $x_1, \ldots, x_k, y_1, \ldots, y_k \in X$ con las x_i distintas entre sí, lo mismo que las y_i. Existe $g \in G_{x_1}$ tal que $gx_i = y_i \;\; i = 2, \ldots, k$, y existe $h \in G_{y_k}$ tal que $hx_1 = y_1$ y además $hy_j = y_j \;\; j = 2, \ldots, k-1$. hg es el elemento de G buscado.

□

TEOREMA 2.6

Todo G-conjunto X múltiplemente transitivo tiene rango 2, y si $x \in X$ y $g \notin G_x$, entonces $G = G_x \cup G_x g G_x$.

Demostración: Como G actúa k-transitivamente en X, con $k > 1$, G_x actúa transitivamente en $X - \{x\}$. De manera que $X - \{x\}$ tiene sólo una G_x-órbita. De ahí que X tenga dos G_x-órbitas, a saber $X - \{x\}$ y $\{x\}$. Por lo tanto el rango de X es 2.

Por la Proposición 2.4, tenemos que sólo hay 2 clases laterales dobles $G_x - G_x$ de G, a saber G_x y $G_x g G_x$ para $g \notin G_x$. De ahí que $G = G_x \cup G_x g G_x$.

□

TEOREMA 2.7

Si X es un G-conjunto k-transitivo y de grado n, entonces

$$|G| = n(n-1)\cdots(n-k+1)|G_{x_1,\ldots,x_k}|$$

para toda elección de k elementos distintos $x_1, \ldots, x_k \in X$. Si la acción de G es fiel, entonces $|G_{x_1,\ldots,x_k}|$ es un divisor de $(n-k)!$.

Demostración: Sea $x_1 \in X$. Tenemos que $|G| = n|G_{x_1}|$. Puesto que además G_{x_1} actúa $(k-1)$-transitivo en $X - \{x_1\}$, y ya que $x_2, \ldots, x_k$ son elementos distintos de $X - \{x_1\}$, por inducción tenemos que

$$|G_{x_1}| = (n-1)\cdots(n-k+1)|G_{x_1,x_2,\ldots,x_k}|.$$

Si G actúa de manera fiel, entonces G es un subgrupo de S_n, y por lo tanto $G_{x_1,\ldots,x_k}$ corresponde a un subgrupo de S_{n-k}, y el resultado se sigue por Teorema de Lagrange.

□

DEFINICIÓN

Un G-conjunto X k-transitivo es nítidamente (o exactamente) k-transitivo sii sólo la identidad de G fija k elementos distintos de X.

COROLARIO 2.8

Para un G–conjunto fiel X de grado n y k–transitivo, son equivalentes:

(i) X es nítidamente k– transitivo.

(ii) Si $(x_1,\ldots,x_k)$ y $(y_1,\ldots,y_k)$ son k-cadas con entradas diferentes entre sí en X, existe una única $g \in G$ tal que $gx_i = y_i$ para $i = 1,\ldots,k$.

(iii) $|G| = n(n-1)\cdots(n-k+1)$.

(iv) El estabilizador de k elementos distintos de X es $\{1\}$.

Si además $k \geq 2$, estas condiciones son equivalentes a:

(v) Para cada $x \in X$, el G_x-conjunto $X - \{x\}$ es nítidamente $(k-1)$-transitivo.

Demostración: (i) $\Rightarrow$ *(ii)*. Sean $g, h \in G$ tales que $gx_i = hx_i = y_i$ para cada $i = 1,\ldots,k$. (Existen pues el conjunto es k-transitivo). Entonces $gh^{-1}(y_i) = gx_i = y_i$ para cada $i = 1,\ldots,k$. Por ser nítidamente k-transitivo, $gh^{-1} = 1$, y por lo tanto $g = h$.

(ii) $\Rightarrow$ *(iii)*. Tenemos que $|G| = n(n-1)\cdots(n-k+1)|G_{x_1,\ldots,x_k}|$. Claramente la identidad manda cada x_i en sí misma, y como es la única, tenemos que $G_{x_1,\ldots,x_k} = \{1\}$.

(iii) $\Rightarrow$ *(iv)*. Sean $x_1,\ldots,x_k \in X$ elementos distintos entre sí. Tenemos que

$$n(n-1)\cdots(n-k+1) = |G| = n(n-1)\cdots(n-k+1)|G_{x_1,\ldots,x_k}|.$$

Por lo tanto, $|G_{x_1,\ldots,x_k}| = 1$, y se trata del subgrupo trivial $\{1\}$.

(iv) $\Rightarrow$ *(i)*. Inmediato por definición.

Si además $k \geq 2$, probaremos que *(v)* es equivalente a *(i)*. Si X es nítidamente k–transitivo, en particular es k– transitivo, y por lo tanto $X - \{x\}$ es $(k-1)$-transitivo en G_x. Si un elemento de G_x fija $k-1$ elementos de $X - \{x\}$, como también fija a x, es la identidad. Así que la acción es nítida. Inversamente, sea $g \in G$ que fije a k elementos distintos de X. Si x_1 es uno de ellos, tenemos $g \in G_{x_1}$, y fija a $k-1$ elementos de $X - \{x_1\}$. Por lo tanto $g = 1$, y la acción original es nítida.

□

Cuando consideramos a la acción de grupo simplemente como un subgrupo del grupo de permutaciones, es muy cómodo abusar del lenguaje y decir simplemente que el grupo es transitivo. Como el interés del presente trabajo es en grupos de permutaciones, usaremos esta convención de ahora en adelante.

TEOREMA 2.9

Para cada n, los grupos simétricos S_n y S_{n+1} son nítidamente n-transitivos. Para cada $n \geq 3$, el grupo alternante A_n es nítidamente $(n-2)$-transitivo.

Demostración: Claramente S_n es n transitivo, pues contiene todas las permutaciones de los n elementos. S_{n+1} también es n transitivo, pues de hecho es $n+1$ transitivo por la misma razón.

$|S_n| = n!$ y actúa sobre un conjunto de n elementos, así que el resultado se sigue por el inciso *(iii)* del Corolario 2.8. $|S_{n+1}| = (n+1)! = (n+1)(n)\cdots 2$, y actúa sobre un conjunto de $n+1$ elementos, y el resultado se sigue nuevamente del inciso *(iii)*.

La segunda afirmación se prueba por inducción sobre n. Cuando $n = 3$, $A_3 = \langle (1,2,3) \rangle$, y es transitivo en $X = \{1,2,3\}$. Si $n > 3$, notemos que el estabilizador de un punto en A_n es precisamente A_{n-1} en los restantes, que actúa $n-3$ transitivamente por hipótesis de inducción. De manera que A_n es $(n-2)$-transitivo. Para ver la nitidez, notemos que $|A_n| = n(n-1)\cdots 3 = n(n-1)\cdots(n-(n-2)+1)$, y tenemos el resultado por el inciso *(iii)* del Corolario 2.8.

□

Los S_n y A_n se consideran ejemplos "triviales" de grupos múltiplemente transitivos.

Hablaremos ahora un poco sobre el concepto de bloques de un grupo de permutaciones, para dar algunos resultados sobre grupos transitivos.

DEFINICIÓN

Un bloque de un G-conjunto X es un subconjunto $B \subset X$ tal que, para cada $g \in G$, tenemos que $gB = B$ o bien $gB \cap B = \emptyset$.

Claramente $B = \emptyset$, $B = X$, y los subconjuntos de X con un elemento son bloques. Estos son llamados los bloques triviales, y cualquier otro bloque es no trivial.

DEFINICIÓN

Un G-conjunto transitivo X es primitivo sii no contiene bloques no triviales. Un G-conjunto X que contiene bloques no triviales se llama no primitivo.

PROPOSICIÓN 2.10

Sea B un bloque no trivial del G-conjunto transitivo X de grado n. Entonces:

(i) Si $g \in G$, entonces gB es un bloque.

(ii) Hay elementos $g_1, g_2, \ldots, g_m$ de G tales que

$$Y = \{B, g_1B, g_2B, \ldots, g_mB\}$$

es una partición de X.

(iii) $|B|$ divide a $|X|$.

(iv) El conjunto Y es un G-conjunto transitivo de grado $\frac{n}{|B|}$.

Demostración: (i) Supongamos que $gB \cap hgB \neq \emptyset$ para algunos $h \in G$. Entonces $B \cap g^{-1}hgB \neq \emptyset$, y por lo tanto son iguales, y tenemos que $gB = hgB$.

(ii) Sea $b \in B$, y $x_1 \notin B$. Como G actúa transitivamente, existe $g_1 \in G$ con $g_1(b) = x$. Como B es bloque, g_1B es un bloque disjunto de B. Si $X = B \cup g_1B$, terminamos. Si no es todo, elegimos $x_2 \in X - (B \cup g_1B)$, y $g_2 \in G$ tal que $g_2(x_1) = x_2$, y continuamos el proceso hasta terminar.

(iii) Si $g \in G$, entonces $|B| = |gB|$, y el resultado se sigue de *(ii)*.

(iv) Para cualquier $g \in G$, tenemos que gg_iB corta a algún g_jB, y por lo tanto $gg_iB = g_jB$. Entonces existe $\varphi: G \to S_Y$ definida por $\varphi(g): g_iB \mapsto gg_iB$, que hace a Y un G-conjunto. Claramente transitivo, y de grado $|Y| = \frac{n}{|B|}$.

□

TEOREMA 2.11

Todo G-conjunto X múltiplemente transitivo es primitivo.

Demostración: Supongamos que X tiene un bloque no trivial B. Sean $x, y \in B$ elementos distintos, y $z \notin B$. Existe $g \in G$ tal que $gx = x$, y $gy = z$, de manera que B y gB son distintos y con intersección no vacía, una contradicción.

□

TEOREMA 2.12

Supongamos que X es un G-conjunto transitivo. Entonces X es primitivo si y sólo si, para cada $x \in X$, el estabilizador G_x es un subgrupo máximo de G.

Demostración: $\Rightarrow$) Supongamos que X es primitivo y que existe un subgrupo H con $G_x \subsetneq H \subsetneq G$. Definimos $B = Hx$; entonces B es un bloque: Si $g \in G$ y $B \cap gB \neq \emptyset$, entonces $hx = gh'x$ para algunas $h, h' \in H$. Por lo tanto $h^{-1}gh' = k \in G_x \subset H$, y $g \in H$; de manera que $gB = gHx = Hx = B$.

Basta ahora ver que B es no trivial para llegar a una contradicción. Claramente $B = Hx \neq \emptyset$. Si $Hx = X$, entonces sea $g \in G$, $g \notin H$; tenemos que $gx = hx$ para alguna $h \in H$, y por lo tanto $h^{-1}g \in G_x \subset H$, contradiciendo que $H \neq G$. Por último, puesto que $G_x \subsetneq H$, tenemos que Hx no puede ser sólo un punto.

$\Leftarrow$) Supongamos que G_x es un subgrupo máximo, pero que existe un bloque no trivial B en X. Definimos un subgrupo $H < G$ dado por

$$H = \{g \in G \mid gB = B\}.$$

Sea $x \in B$. Como B es un bloque, $G_x \subset H$. Como B es no trivial, existe $y \in B$ con $y \neq x$. Puesto que la acción es transitiva, existe $g \in G$ con $gx = y$. Claramente $g \notin G_x$, pero $g \in H$, pues $B \cap gB \neq \emptyset$; de manera que $G_x \subsetneq H$. Por último, tenemos por la Proposición 2.10*(ii)* que $H \neq G$, pues de lo contrario $B = X$. Por lo tanto B no puede existir.

□

LEMA 2.13

Sea X un G-conjunto. Si $H \triangleleft G$, entonces los subconjunto Hx son bloques de X (con $x \in X$).

Demostración: Sea $g \in G$, y supongamos que $Hx \cap gHx \neq \emptyset$. Puesto que H es normal en G, tenemos que

$$g(Hx) = (gH)x = (Hg)x = H(gx)$$

y si dos órbitas no son ajenas, son la misma, de manera que $Hx = gHx$, y Hx es un bloque.

□

TEOREMA 2.14

Si X es un G-conjunto fiel y primitivo, y $H \lhd G$, con $H \neq \{1\}$, entonces X es H-transitivo.

Demostración: Tenemos que Hx es un bloque con $x \in X$. Como G actúa de manera primitiva, tenemos que para cada x, $Hx = X$ ó $Hx = \{x\}$. Pero si pasa lo segundo, tenemos una contradicción con la fidelidad del conjunto y que $H \neq \{1\}$. De manera que el conjunto es H transitivo.

□

TEOREMA 2.15

Supongamos que X es un G-conjunto fiel y primitivo, con un estabilizadores G_x simples. Entonces G es simple, o bien X es una H-conjunto regular (i.e. nítidamente 1-transitivo) para todo subgrupo normal $H \neq \{1\}$.

Demostración: Supongamos $H \neq \{1\}$ es un subgrupo normal en G. Por teorema anterior tenemos que X es H-transitivo. Por lo tanto, H actúa de manera regular, o bien $H \cap G_x \neq \{1\}$ para alguna $x \in X$. Pero $H \cap G_x \lhd G_x$, de manera que $H \cap G_x = G_x$, i.e. $G_x \subset H$. Pero por Teorema 2.12 tenemos que $H = G_x$ o bien $H = G$, y el primer caso no puede ocurrir pues H actúa transitivamente. De manera que G es simple.

□

DEFINICIÓN

Un subgrupo normal H de G para el cuál un G-conjunto X es un H-conjunto regular se llama un subgrupo normal regular de G.

LEMA 2.16

Sea X un G-conjunto transitivo y sea H un subgrupo normal regular de G. Fijemos $x \in X$, y hagamos actuar a G_x en H^* por conjugación. Entonces los G_x-conjuntos H^* y $X - \{x\}$ son isomorfos.

Demostración: Sea $\theta: H^* \to X - \{x\}$ dado por $\theta(h) = hx$. Si $\theta(h) = \theta(k)$, entonces $h^{-1}k \in H_x = \{1\}$, pues H actúa regular. De manera que θ es inyectiva. La regularidad de la acción también nos da que $|H| = |X|$, y por lo tanto $|H^*| = |X - \{x\}|$, de manera que θ debe ser suprayectiva.

Por último demostraremos que θ respeta la acción de H. Si $g \in G_x$ y $h \in H^*$, denotamos la acción de g en h por $g * h = ghg^{-1}$. Entonces tenemos que

$$\theta(g * h) = \theta(ghg^{-1}) = ghg^{-1}x = ghx$$

pues $g^{-1} \in G_x$; además,

$$g\theta(h) = gh(x)$$

de manera que

$$\theta(g * h) = g\theta(h)$$

y θ respeta la acción, y por lo tanto es un isomorfismo de G-conjuntos.

□

TEOREMA 2.17

Sea X un G-conjunto k-transitivo ($k \geq 2$) de grado n, y supongamos que G tiene un subgrupo normal regular H. Entonces $k \leq 4$. Además:

(i) Si $k = 2$, entonces H es un p-grupo elemental abeliano para algún primo p, y $n = p^m$.

(ii) Si $k = 3$, entonces $H \cong \mathbb{Z}_3$ y $n = 3$, o bien H es un 2-grupo elemental abeliano y $n = 2^m$.

(iii) Si $k = 4$, entonces $H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ y $n = 4$.

Demostración: Si X es un G-conjunto k-transitivo con $k \geq 2$, entonces para una $x \in X$ fija tenemos que $X - \{x\}$ es un G_x- conjunto $(k-1)$-transitivo. Por el Lema 2.16, tenemos que H^* es un G_x-conjunto $(k-1)$-transitivo, con G_x actuando en H^* por conjugación.

(i) Supongamos que $k = 2$. Puesto que la conjugación es un automorfismo (interior), tenemos que todos los elementos de H^* tienen el mismo orden, que debe ser un primo p. De manera que H es un p-grupo; puesto que el centro de H es un subgrupo característico no trivial, H debe ser abeliano. Por último, $|H| = n$, pues su acción es regular.

(ii) Supongamos que $k = 3$. Entonces H^* es un G_x-conjunto múltiplemente transitivo, y por lo tanto primitivo. Si $h \in H^*$, tenemos que $\{h, h^{-1}\}$ es un bloque, pues la acción es por conjugación. Puesto que es primitivo, tenemos que $\{h, h^{-1}\} = H^*$, que tiene dos elementos, y por lo tanto $H = \mathbb{Z}_3$ y $n = 3$, o bien $h = h^{-1}$, y todo elemento tiene orden 2. Puesto que 3-transitividad implica 2-transitividad, el resultado del inciso *(i)* vale, y H es un 2-grupo elemental abeliano, y $n = |H| = 2^m$.

(iii) Supongamos que $k = 4$. En este caso $k - 1 = 3$, y $|H^*| \geq 3$, de manera que H no es $\mathbb{Z}_3$ ni $\mathbb{Z}_2$. Puesto que 4-transitividad implica 3-transitividad, tenemos que el grupo es elemental abeliano de orden 2^m, y debe contener una copia del grupo de Klein, digamos $\{1, h, k, hk\}$. Pero $G_{x,h}$ actúa 2- transitivo, y por lo tanto de manera primitiva, en $H^* - \{h\}$. Pero $\{k, hk\}$ es un bloque en este nuevo conjunto, y por lo tanto

$$H^* - \{h\} = \{k, hk\}$$

de lo que concluimos que H es el Grupo de Klein, y $n = |H| = 4$.

Por último, no podemos tener $k \geq 5$, pues implicaría 4- transitividad, y $n = 4$, pero el grado no puede ser menor que la transitividad.

□

COROLARIO 2.18

Sea X un G-conjunto fiel, k-transitivo, con $k \geq 4$, y supongamos que G_x es simple para alguna $x \in X$. Entonces G es simple.

Demostración: Por Teorema 2.15 tenemos que G es simple o contiene un subgrupo normal regular H. Si H existe, tenemos por el Teorema de arriba que $k \leq 4$, y por lo tanto $k = 4$. Tenemos entonces que H es isomorfo al Grupo de Klein, y $|X| = 4$. Pero el único subgrupo 4-transitivo de S_4 es S_4 mismo, y el estabilizador de un punto es S_3 que no es simple, lo cual es una contradicción. Tenemos pues que G es simple.

□

III. Extensión Transitiva de Grupos

En este capítulo introducimos el concepto de *Extensión Transitiva de un Grupo*, y obtenemos condiciones necesarias y suficientes para que exista. Además, se da un método de extensión, que permite acotar el número de posibles extensiones sucesivas de un grupo.

Todos los G–conjuntos serán de ahora en adelante fieles, y llamaremos a G un grupo de permutaciones, identificándolo con su imágen en el grupo de permutaciones del conjunto X. Diremos que un grupo G es múltiplemente transitivo de grado n cuando exista un conjunto $X = \{x_1, \ldots, x_n\}$, que es un G–conjunto múltiplemente transitivo.

DEFINICIÓN

Sea G un grupo de permutaciones sobre X, y sea $\overline{X} = X \cup \{\infty\}$ (donde $\infty \notin X$). Un grupo $\overline{G}$ transitivo de permutaciones sobre $\overline{X}$ es una extensión transitiva de G sii el estabilizador $\overline{G}_\infty$ es G.

TEOREMA 3.1

(Witt, 1938) Sea G un grupo múltiplemente transitivo de permutaciones que actúa sobre un conjunto X. Supongamos que existe $\infty \notin X$, una permutación h de $\overline{X} = X \cup \{\infty\}$, un elemento $x \in X$, y un elemento $g \in G$ tales que:

(i) $g \notin G_x$.

(ii) $h(\infty) \in X$.

(iii) $h^2 \in G$ y $(gh)^3 \in G$.

(iv) $hG_xh = G_x$.

Entonces $\overline{G} = \langle G, h \rangle$ es una extensión transitiva de G.

Demostración: $\overline{G}$ actúa transitivamente en $\overline{X}$, pues contiene a G, y como $h(\infty) \in X$, si $x \in X$, $\exists g \in G$ tal que $g(x) = h(\infty)$, y el elemento $h^{-1}g$ manda x en ∞, de manera que la acción es transitiva.

Supongamos que $G \cup GhG$ es un grupo. Entonces tendríamos que $\overline{G} = \langle G, h \rangle = G \cup GhG$. Además, $\overline{G}_\infty = G$, pues todo elemento de G fija a ∞ y todo elemento de GhG lo mueve. Así que basta probar que $G \cup GhG$ es un grupo. Para ello, basta ver que es cerrado bajo

multiplicaciones. Tenemos que $G \cdot G = G$, $G \cdot GhG = GhG$, y $GhG \cdot G = GhG$. De manera que basta ver que $(GhG) \cdot (GhG) \subset G \cup GhG$.

Como $(GhG) \cdot (GhG) = GhGhG$, basta ver que $hGh \subset G \cup GhG$, pues entonces $GhGhG \subset G(G \cup GhG)G = (G \cup GhG)G = G \cup GhG$.

Como G es múltiplemente transitivo en X, tenemos que $G = G_x \cup G_x g G_x$ pues $g \notin G_x$. Notemos además que $h^2 = \gamma_1 \in G$, y por lo tanto $h\gamma_1^{-1} = h^{-1} = \gamma_1^{-1}h$; y como $(gh)^3 = \gamma_2 \in G$, $ghghgh = \gamma_2$, y por lo tanto $hgh = g^{-1}h^{-1}g^{-1}\gamma_2$. Por lo tanto:

$$\begin{aligned}
hGh &= h(G_x \cup G_x g G_x)h \\
&= hG_xh \cup hG_xgG_xh \\
&= hG_xh \cup (hG_xh)h^{-1}gh^{-1}(hG_xh) \\
\text{(condición } \textit{(in)}) \quad &= G_x \cup G_xh^{-1}gh^{-1}G_x \\
&= G_x \cup G_x(\gamma_1^{-1}h)g(h\gamma_1^{-1})G_x \\
&= G_x \cup G_x\gamma_1^{-1}(hgh)\gamma_1^{-1}G_x \\
&= G_x \cup G_x\gamma_1^{-1}(g^{-1}h^{-1}g^{-1}\gamma_2)\gamma_1^{-1}G_x \\
&= G_x \cup (G_x\gamma_1^{-1}g^{-1})h^{-1}(g^{-1}\gamma_2\gamma_1^{-1}G_x) \\
\text{(pues } G_x \subset G) \quad &\subset G \cup Gh^{-1}G \\
&= G \cup G\gamma_1^{-1}hG \\
&= G \cup GhG
\end{aligned}$$

Por lo tanto, $hGh \subset G \cup GhG$, y tenemos que $G \cup GhG$ es un grupo, y el resultado queda establecido.

□

El Teorema de Witt nos permitirá construir el grupo de Mathieu M_{12} más adelante. Además, establece condiciones suficientes para la construcción de extensiones de grupos.

Trabajaremos ahora con un grupo múltiplemente transitivo, y daremos un algoritmo para extenderlo transitivamente. Esto nos permitirá establecer condiciones necesarias y suficientes para que se pueda extender dicho grupo.

Sea $k > 1$. G_k representará un grupo k-transitivo en las letras $X \cup \{0, 1, \ldots, k-1\}$, que no contiene un elemento que es un ciclo de orden 2 o uno de orden 3.

Para $i = 0, 1, \ldots, k-1$, sea G_i el estabilizador de la letra i en G_{i+1} (i.e., G_i es el estabilizador de las letras $i, i+1, \ldots, k-1$ en G_k).

La letra que agregaremos al buscar una extensión transitiva de G_k se denotará por k. Sean $G_k^{(\rho)}$ con índice ρ variable, las extensiones transitivas de G_{k-1} distintas de G_k.

PROPOSICIÓN 3.2

En G_i $(i = 2, \ldots, k)$ existe un elemento a_i que intercambia $i-1$ con $i-2$, manda X en sí mismo, y fija el resto de las letras.

Demostración: G_i es i-transitivo en las letras $X \cup \{0, 1, \ldots, i-1\}$. Elegimos un elemento que mande $0, 1, 2, \ldots, i-3$ en sí mismos, $i-2$ en $i-1$, e $i-1$ en $i-2$. Claramente debe mandar X en sí mismo.

□

Los elementos análogos a a_k en $G_k^{(\rho)}$ serán denotados por $a_k^{(\rho)}$. Tenemos que $a_i G_0 = G_0 a_i$ para $i = 0, 1, \ldots, k$, y además $a_k^{(\rho)} G_0 = G_0 a_k^{(\rho)}$, pues las clases laterales de G_0 quedan determinadas por la acción del elemento en el conjunto $\{0, 1, \ldots, k-1\}$. Además, $a_i^2 \in G_0$, para $i = 0, 1, \ldots, k$, y $\left(a_i^{(\rho)}\right)^2 \in G_0$.

Vale la pena mencionar que cualquier elemento de $G_k^{(\rho)}$ que fije a $k-1$ será también un elemento de G_k, por ser el primero una extensión transitiva de G_{k-1}.

DEFINICIÓN

Definimos

$$a_{k+1}^{(\rho)} = (k, k-1, k-2) a_k a_k^{(\rho)} a_k^{-1}.$$

Tenemos que entonces $a_{k+1}^{(\rho)}$ actúa en $\{0, 1, \ldots, k\}$ como la permutación $(k, k-1)$.

PROPOSICIÓN 3.3

Si adjuntar $a_{k+1}^{(\rho)}$ a G_k produce una extensión transitiva de G_k, entonces estas extensiones son distintas entre sí.

Demostración: Si $a_{k+1}^{(\rho)}$ y $a_{k+1}^{(\rho')}$ dan las mismas extensiones transitivas, puesto que actúan en $\{0,1,\ldots,k\}$ de la misma manera, tenemos que

$$a_{k+1}^{(\rho)} \in a_{k+1}^{(\rho')} G_0$$

por lo tanto, $a_k^{(\rho)} a_k^{-1} \in a_k^{(\rho')} a_k^{-1} G_0$. De ahí que $a_k^{(\rho)} a_k^{-1} a_k a_k^{(\rho')^{-1}} = a_k^{(\rho)} a_k^{(\rho')^{-1}} \in G_0$. Esto nos resulta en $a_k^{(\rho)} \in a_k^{(\rho')} G_0$, y de ahí que $a_k^{(\rho)} \in G_k^{(\rho')}$, y viceversa. Por lo tanto, $G_k^{(\rho)} = G_k^{(\rho')}$, y entonces $\rho = \rho'$.

□

TEOREMA 3.4

Para que una $a_{k+1}^{(\rho)}$ particular dé lugar a una extensión transitiva de G_k, es necesario y suficiente que $(a_k^{(\rho)} a_k)^3 \in G_0$ y $a_{k+1}^{(\rho)} G_{k-1} a_{k+1}^{(\rho)} = G_{k-1}$.

Demostración: Notemos que

$$a_{k+1}^{(\rho)} a_k = (k, k-1, k-2) a_k a_k^{(\rho)}$$

y que $a_k a_k^{(\rho)}$ fija $\{0,1,\ldots,k\}$. Por lo tanto $(k,k-1,k-2)$ conmuta con $a_k a_k^{(\rho)}$. De ahí que

$$(a_{k+1}^{(\rho)} a_k)^3 = \left((k,k-1,k-2) a_k a_k^{(\rho)}\right)^3 = (k,k-1,k-2)^3 \left(a_k a_k^{(\rho)}\right)^3 = \left(a_k a_k^{(\rho)}\right)^3$$

De manera que haciendo $g = a_k$ y $h = a_{k+1}^{(\rho)}$, se satisfacen las hipótesis del Teorema de Witt, dando la suficiencia. La necesidad se sigue de un Teorema de Jordan, publicado en 1870 en su *Traité de Substitutions et des Équations Algébriques.*

□

TEOREMA 3.5

(Holyoke, 1952) Cada extensión transitiva de G_k se obtiene adjuntándole alguna de las $a_{k+1}^{(\rho)}$, en cuyo caso la $G_k^{(\rho)}$ correspondiente es isomorfa a G_k por conjugación, con el elemento $(k,k-1)a_{k+1}^{(\rho)}$ transformando G_{k-1} en sí mismo, y a_k en algún elemento de $a_k^{(\rho)} G_0$.

Demostración: Sea G_{k+1} una extensión transitiva de G_k, y a_{k+1} un elemento de G_{k+1} que intercambia k y $k-1$, y fija a $0,1,\ldots,k-2$.

Sea $a'_k = (k,k-1,k-2)a_{k+1}a_k a_{k+1}^{-1}$. Si $a'_k \in G_k$, entonces

$$a'_k(a_{k+1}a_k^{-1}a_{k+1}^{-1}) = (k,k-1,k-2)a_{k+1}a_k a_{k+1}^{-1}a_{k+1}a_k^{-1}a_{k+1}^{-1} = (k,k-1,k-2) \in G_{k+1},$$

y por ser al menos 3 transitivo, G_k contendría un ciclo de longitud tres, lo cual era imposible por hipótesis. De manera de $a'_k \notin G_k$.

G_k y $\langle G_{k-1}, a'_k\rangle$ son isomorfos, pues conjugando con $(k,k-1)a_{k+1}$, transformamos G_{k-1} en sí mismo, y a_k en a'_k: La primera afirmación es inmediata, pues $(k,k-1)a_{k+1}$ no mueve las letra $0,1,\ldots,k-2$. La segunda, pues tenemos que

$$(k,k-1)a_{k+1}\Big|_{\{0,1,\ldots,k\}} = (k,k-1)(k,k-1) = 1_{\{0,1,\ldots,k\}}$$
$$(k,k-1)a_{k+1}\Big|_X = a_{k+1}\Big|_X$$

De manera que tenemos:

$$(k,k-1)a_{k+1}a_k a_{k+1}^{-1}(k,k-1)\Big|_{\{0,1,\ldots,k\}} = (k-1,k-2)$$
$$a'_k\Big|_{\{0,1,\ldots,k\}} = (k,k-1,k-2)a_{k+1}a_k a_{k+1}^{-1}\Big|_{\{0,1,\ldots,k\}} = (k-1,k-2)$$
$$(k,k-1)a_{k+1}a_k a_{k+1}^{-1}(k,k-1)\Big|_X = a_{k+1}a_k a_{k+1}^{-1}\Big|_X$$
$$a'_k\Big|_X = a_{k+1}a_k a_{k+1}^{-1}\Big|_X$$

Por lo tanto, $(k,k-1)a_{k+1}a_k a_{k+1}^{-1}(k,k-1) = a'_k$.

$\langle G_{k-1}, a'_k\rangle$ es una extensión transitiva de G_{k-1}, pues el estabilizador de $k-1$ es G_{k-1}, y por ser isomorfo a G_k que es k-transitivo. Puesto que $a'_k \notin G_k$, $\langle G_{k-1}, a'_k\rangle \neq G_k$, y $\langle G_{k-1}, a'_k\rangle = G_k^{(\rho)}$ para alguna ρ.

Ya que $a_k^{(\rho)}$ actúa en $\{0,1,\ldots,k\}$ igual que a'_k, tenemos que $a_k^{(\rho)} = a'_k f$ para alguna $f \in G_0$. Por lo tanto:

$$\begin{aligned} a_{k+1}^{(\rho)} &= (k,k-1,k-2)a_k a_k^{(\rho)} a_k^{-1} \\ &= (k,k-1,k-2)a_k a'_k f a_k^{-1} \\ &= (k,k-1,k-2)a_k(k,k-1,k-2)a_{k+1}a_k a_{k+1}^{-1} f a_k^{-1} \end{aligned}$$

Este elemento actúa en $\{0,1,\ldots,k\}$ como

$$(k,k-1,k-2)(k-1,k-2)(k,k-1,k-2)(k,k-1)(k-1,k-2)(k,k-1)(k-1,k-2) = (k,k-1),$$

y en X actúa como $a_k a_{k+1} a_k a_{k+1}^{-1} f a_k^{-1}|_X$. Por otro lado, $a_k a_{k+1} a_k a_{k+1}^{-1} f a_k^{-1}$ actúa en X de la misma manera, y en $\{0,1,\ldots,k\}$ como

$$(k-1,k-2)(k,k-1)(k-1,k-2)(k,k-1)(k-1,k-2) = (k,k-1),$$

de manera que son el mismo. Por lo tanto:

$$a_{k+1}^{(\rho)} = a_k a_{k+1} a_k a_{k+1}^{-1} f a_k^{-1} \in G_{k+1}.$$

De ahí que $\langle G_k, a_{k+1}^{(\rho)} \rangle = G_{k+1}$, y la extensión se obtuvo adjuntando $a_{k+1}^{(\rho)}$.

Por último, $a_{k+1}^{(\rho)}$ y a_{k+1} actúan igual en $\{0,1,\ldots,k\}$, de manera que $a_{k+1}^{(\rho)} \in a_{k+1} G_0$. Por lo tanto $\exists f \in G_0$ tal que $a_{k+1}^{(\rho)} = a_{k+1} f$.

$(k,k-1)a_{k+1}^{(\rho)}$ manda a G_{k-1} en sí mismo bajo conjugación, pues el primero fija a $\{0,1,\ldots,k\}$, y manda a a_k en algún elemento de $a_k^{(\rho)} G_0$,

$$(k,k-1)a_{k+1}^{(\rho)} a_k a_{k+1}^{(\rho)\,-1}(k,k-1)\Big|_{\{0,\ldots,k\}} = (k-1,k-2)$$

i.e. la misma acción de $a_k^{(\rho)}$ y por lo tanto está en su misma clase lateral según G_0; de manera que $G_k \cong G_k^{(\rho)}$, terminando la demostración.

□

Aplicando este Teorema sucesivamente, obtenemos el siguiente resultado, que establece una cota al número de posibles extensiones sucesivas de un grupo dado.

COROLARIO 3.6

Si el número de distintas extensiones de G_{k-1} que son isomorfas bajo conjugación a G_k es un número finito l, entonces el número de extensiones de G_k es menor que l; en particular, si un grupo finito transitivo de grado $n > 3$ tiene a lo más l extensiones, isomorfas entre sí, entonces G no se puede extender a un grupo $(l+1)$-transitivo de grado $(n+l+1)$.

IV. Construcción de Hall

En este capítulo demostraremos un teorema de Jordan que enumera los grupos nítidamente 4-transitivos. En la demostración, que se llevará a cabo siguiendo el trabajo de Marshall Hall, Jr., se construirá el grupo M_{11}, y la construcción nos permitirá además enumerar los grupos nítidamente 5-transitivos, estableciendo así que M_{12} es el único grupo nítidamente 5- transitivo no trivial.

Primero, se demostrarán dos lemas sobre grupos que se utilizarán posteriormente.

LEMA 4.1

Sea $\overline{G}$ el producto subdirecto de los grupos G_i y G_j, y sean H_{ij} y H_{ji} los subgrupos de G_i y G_j respectivamente, de elementos que ocurren en un factor de $\overline{G}$ con la identidad del otro lado. Entonces

$$H_{ij} \triangleleft G_i, \qquad H_{ji} \triangleleft G_j$$

y además

$$\frac{G_i}{H_{ij}} \cong \frac{G_j}{H_{ji}}.$$

Demostración: Si $h \in H_{ij}$, $g \in G_i$, $\exists z \in G$ tal que $(g,z) \in \overline{G}$. Por lo tanto

$$(g,z)\cdot(h,1)\cdot(g^{-1},z^{-1}) = (ghg^{-1},1) \in \overline{G}$$

Por lo tanto, $ghg^{-1} \in H_{ij}$, y este último es normal. Por lo tanto $H_{ij} \triangleleft G_i$, y análogamente $H_{ji} \triangleleft G_j$.

Si $g_1 \in G_i$ es un elemento fijo, los elementos de G_j que aparecen con g_1 en $\overline{G}$ forman una clase lateral respecto de H_{ji}, pues $(g_1,r)\cdot(g_1^{-1},s^{-1}) = (1,rs^{-1})$, y $r \equiv s \pmod{H_{ji}}$. Análogo con H_{ij}.

Además, si $(g_1,g_2) \in \overline{G}$, todo elemento de la forma $(h_{ij}g_1, h_{ji}g_2) \in \overline{G}$ $\forall h_{ij} \in H_{ij}$ y $h_{ji} \in H_{ji}$, y ningún otro (g_1', g_2') los involucra como elementos. Por lo tanto, hay una correspondencia biyectiva entre $H_{ij}g_1$ y $H_{ji}g_2$ donde (g_1,g_2) es un elemento de $\overline{G}$. Por lo tanto

$$\frac{G_i}{H_{ij}} \cong \frac{G_j}{H_{ji}}$$

pues el producto es coordenada a coordenada.

□

LEMA 4.2

Sea G un grupo t–transitivo en n letras. Sea H un subgrupo que fija t letras, y P un p-subgrupo de Sylow de H, donde P fija $\omega \geq t$ letras. Entonces el normalizador de P en G es t–transitivo en las ω letras que fija P.

Demostración: Sean $a_1, a_2, \ldots, a_t$ y $b_1, b_2, \ldots, b_t$ dos conjuntos ordenados de t letras, ambos de entre las ω letras que fija P. Ya que G es t–transitivo, $\exists x \in G$ tal que $x(a_i) = b_i$, para $i = 1, \ldots, t$.

Por lo tanto xPx^{-1} fija a $b_1, \ldots, b_t$, y tanto P como xPx^{-1} son p-subgrupos de Sylow que fijan $b_1, \ldots, b_t$, de manera que son conjugados en $G_{b_1,\ldots,b_t}$.

Así, $\exists y \in G_{b_1,\ldots,b_t}$ tal que $y(xPx^{-1})y^{-1} = P$. Si $z = yx$, entonces z manda $a_1, \ldots, a_t$ en $b_1, \ldots, b_t$, y $zPz^{-1} = P$. Por lo tanto hay un elemento en el normalizador de P en G que manda $a_1, \ldots, a_t$ en $b_1, \ldots, b_t$, y de ahí que dicho normalizador sea t– transitivo en las ω letras fijadas por P.

□

Enumeraremos primero a los grupos nítidamente 4–transitivos, para pasar de ahí a los nítidamente 5–transitivos, extendiendolos transitivamente. Analicemos ahora el caso de grupos que actúan en menos de 8 letras:

TEOREMA 4.3

Un grupo nítidamente 4–transitivo de grado a lo más 7 debe ser S_4, S_5 o A_6.

Demostración: Si G es 4–transitivo en 4 letras debe tratarse de S_4. Si es 4–transitivo en 5 letras debe ser S_5. Si es nítidamente 4– transitivo en 6 letras, es de orden $6 \cdot 5 \cdot 4 \cdot 3$, y por lo tanto es A_6.

Si G fuera nítidamente 4–transitivo en 7 letras, sería de orden $7 \cdot 6 \cdot 5 \cdot 4$, y su índice en A_7 sería el menor primo que divide al orden de A_7, y por lo tanto sería normal en A_7, lo cual es imposible. Además, S_7 no tiene subgrupos de índice 6. De manera que tal grupo no existe.

□

Para analizar el caso de grupos que actúan en 8 o más letras, se requieren de algunos resultados que obtendremos a continuación.

LEMA 4.4

Elementos a y b en un grupo que satisfacen las relaciones

$$a^2 = b^2 = 1; \qquad (ab)^s = 1$$

generan el grupo dihédrico de orden $2s$. Si $s = 2t-1$ es impar entonces hay una potencia de (ab) que transforma a en b bajo conjugación. Si $s = 2r$ es par entonces a y b conmutan con $(ab)^r$.

Demostración: Sea $y = ab$. Entonces $a^2 = 1$, $y^s = 1$, $b = aab = ay = baa = y^{-1}a$. Por lo tanto, $b = ay = y^{-1}a$.

Ya que $ay = y^{-1}a$, tenemos que $\forall t(y^{-t}a = ay^t)$.

Si $s = 2t-1$, entonces $y^{-t}ay^t = ay^ty^t = ay^{2t} = (ay)y^{2t-1} = ay = b$, de manera que a y b son conjugados bajo una potencia de ab.

Si $s = 2r$, entonces $ay^r = y^{-r}a = y^ra$ pues $y^r = y^{-r}$. Análogamente, ya que $b = ay = y^{-1}a$, tenemos que $a = by^{-1} = yb$, y por lo tanto $y^rb = by^{-r} = by^r$, de manera que a y b conmutan con $(ab)^r$.

□

En lo que resta del capítulo G representará un grupo nítidamente 4-transitivo en al menos 8 letras.

LEMA 4.5

El grupo G contiene elementos de orden 2, y todos son conjugados. Además pasa una de:

(i) Todo elemento de orden 2 fija dos letras.

(ii) Todo elemento de orden 2 fija tres letras.

Demostración: Por 4-transitividad, G tiene un elemento

$$g = (1,2)(3,4)\cdots$$

Ya que g^2 fija 4 elementos, debe ser la identidad, y como $g^2 = 1$, entonces g es un elemento de orden 2.

Sea

$$u = (a, b)(c, d)\cdots$$

un elemento de orden 2. Por lo tanto hay un conjugado de u

$$g = wuw^{-1} = (1, 2)(3, 4)\cdots$$

eligiendo a w que actúa $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 3$, $d \mapsto 4$. Por lo tanto todo elemento de orden 2 es conjugado.

Por último, hay un elemento en G, $z = (1)(2)(3, 4)\cdots$, y como z^2 fija al menos cuatro elementos, es de orden 2. Por lo tanto, todo elemento de orden 2 fija al menos dos elementos, y como no puede fijar a cuatro, fija al menos dos y a lo más tres. De manera que todo elemento de orden 2 fija dos letras, o todo elemento de orden 2 fija tres letras.

□

Estudiemos ahora la estructura de nuestro hipotético grupo G.

Sean $a_1 = (1)(2)(3, 4)\cdots$ y $b = (1, 2)(3, 4)\cdots$ dos elementos de orden 2 de G. Sea $a_3 = a_1 b = (1, 2)(3)(4)\cdots$. Es de orden 2, y por Lema 4.4 conmuta con a_1 y con b, pues es de orden par. Sea $a_2 = a_1 a_3 = a_1 a_1 b = b$. Entonces:

$$a_2 a_1 = a_1 a_3 a_1 = a_1^2 a_3 = a_3$$

$$a_1 a_2 = a_1 a_1 a_3 = a_1^2 a_3 = a_3$$

$$a_2 a_3 = a_1 a_3 a_3 = a_1 a_3^2 = a_1$$

$$a_3 a_2 = a_3 a_1 a_3 = a_1 a_3^2 = a_1$$

Por lo tanto a_1, a_2 y a_3 conmutan entre sí, con a_1, a_2, a_3 igual a:

$$a_1 = (1)(2)(3, 4)\cdots$$

$$a_2 = (1, 2)(3, 4)\cdots$$

$$a_3 = (1, 2)(3)(4)\cdots$$

Como a_2 es de orden 2, fija dos letras (digamos 5 y 6) o tres letras (digamos 5, 6, y 7). Ya que conmuta con a_1, a_1 debe mandar estas letras en sí mismas, pues si por ejemplo $a_1(5) = 8$, entonces $a_1 a_2(5) = a_1(5) = 8$ y $a_2 a_1(5) = a_2(8) \neq 8$. Pero a_1 fija al 1 y al

2, y por lo tanto a lo más a otra letra. El mismo argumento vale para a_3 que también conmuta con a_2. Tenemos entonces que

$$a_1 = (1)(2)(3,4)(5,6)\cdots$$
$$a_2 = (1,2)(3,4)(5)(6)\cdots$$
$$a_3 = (1,2)(3)(4)(5,6)\cdots$$

en el primer caso (si a_2 fija dos letras), o bien

$$a_1 = (1)(2)(3,4)(5,6)(7)\cdots$$
$$a_2 = (1,2)(3,4)(5)(6)(7)\cdots$$
$$a_3 = (1,2)(3)(4)(5,6)(7)\cdots$$

en el otro (si a_2 fija tres letras).

Tenemos pues que los elementos $1_G, a_1, a_2, a_3$ forman un grupo V de orden 4, isomorfo al Grupo de Klein. Las demás letras deben ocurrir en grupos de 4, que son bloques de transitividad para V:

$$a_1 = (1)(2)(3,4)(5,6)(7)(h,i)(j,k)\cdots$$
$$a_2 = (1,2)(3,4)(5)(6)(7)(h,j)(i,k)\cdots$$
$$a_3 = (1,2)(3)(4)(5,6)(7)(h,k)(i,j)\cdots$$

(con la convención de que el 7 está en el segundo caso, y no está en el primero) pues, por conmutar con a_1, a_2 debe mandar $\{h,i,j,k\}$ en sí mismo, y no puede mandar a h en i también, pues $a_1 a_2$ fijaría cuatro letras sin ser la identidad. Análogo argumento permite completar a_3.

Consideremos ahora a K, el subgrupo de G que manda a h,i,j,k en sí mismos. K debe ser de orden 24 (un elemento por cada posible manera de mandarlos, y hay $4! = 24$ maneras). K tiene un subgrupo U en los cuales h,i,j,k son permutados de cada una de las siguientes maneras:

$$(h)(i)(j)(k) = 1_G$$
$$(h,i)(j,k)$$

$$(h,j)(i,k)$$
$$(h,k)(i,j)$$
$$(h,j,i,k)$$
$$(h,k,i,j)$$
$$(h,i)(j)(k)$$
$$(h)(i)(j,k)$$

Entonces U es de orden 8; V estará contenido en U (de hecho corresponde a los primeros 4 elementos en la descripción de arriba).

Llamemos u al elemento que manda $h \mapsto j$, $i \mapsto k$, $j \mapsto i$, y $k \mapsto h$. Entonces a_1u manda $h \mapsto k$, $i \mapsto j$, $j \mapsto h$, y $k \mapsto i$. a_2u manda $h \mapsto i$, $i \mapsto h$, $j \mapsto j$, y $k \mapsto k$. Por último, a_3u manda $h \mapsto h$, $i \mapsto i$, $j \mapsto k$, y $k \mapsto j$. De manera que

$$U = \{1_G, a_1, a_2, a_3, u, a_1u, a_2u, a_3u\}$$

La acción sobre el resto de las letras queda determinada de la siguiente manera: Ya que a_1u^2 actúa en h,i,j,k como la identidad, se trata de la identidad, así que $u^2 = a_1^{-1} = a_1$. Por lo tanto u fija al 1 y al 2, y al 7 en caso necesario, y u^2 manda 3 en 4 y 5 en 6. Por lo tanto ocurre una de

$$u = (1)(2)(3,5,4,6)(7)(h,j,i,k)\cdots$$
$$u = (1)(2)(3,6,4,5)(7)(h,j,i,k)\cdots$$

con el 7 presente sólo en caso necesario.

Por otro lado $u^{-1}a_2u$ actúa en $\{h,i,j,k\}$ como la permutación $(h,k)(i,j)$, i.e. como a_3, de manera que $u^{-1}a_2u = a_3$. Y a_2u actúa en el mismo conjunto como $(h,i)(j)(k)$, y por lo tanto es de orden 2. De manera que

$$u^2 = a_1; \qquad u^{-1}a_2u = a_3; \qquad (a_2u)^2 = 1_G$$

Además, u manda, bajo conjugación, a a_1 en sí mismo, a_2 en a_3, y a_3 en a_2. Por lo tanto, u normaliza a V. También concluimos que manda las fijas por a_2 en las fijas por a_3, de manera que manda 5 en 4 y 6 en 3, o bien 5 en 3 y 6 en 4. Todo esto sigue

correspondiendo bien con la estructura de u que se obtuvo analizando su producto con a_1.

Eligiendo la primer opción para u, tendríamos entonces a U descrito de la siguiente manera:

$$U = \left\{ \begin{array}{l} 1_G \\ a_1 = (1)(2)(3,4)(5,6)(7)(h,i)(j,k)\cdots \\ a_2 = (1,2)(3,4)(5)(6)(7)(h,j)(i,k)\cdots \\ a_3 = (1,2)(3)(4)(5,6)(7)(h,k)(i,j)\cdots \\ u = (1)(2)(3,5,4,6)(7)(h,j,i,k)\cdots \\ a_1u = (1)(2)(3,6,4,5)(7)(h,k,i,j)\cdots \\ a_2u = (1,2)(3,5)(4,6)(7)(h)(i)(j,k)\cdots \\ a_3u = (1,2)(3,6)(4.5)(7)(h,i)(j)(k)\cdots \end{array} \right\}$$

con o sin el 7 (dependiendo de cuántos fijan los elementos de orden 2). Si el u corresponde a la segunda descripción, tendríamos entonces el 5 y el 6 intercambiados en la descripción de arriba.

Cada componente de 4 letras en el cual V es transitivo, como h,i,j,k de arriba, da lugar a un grupo S similar a U.

Los elementos $(1,2)(3,5)(4,6)\cdots$ y $(1,2)(3,6)(4,5)\cdots$ como en la descripción de U arriba fijan dos letras cada uno del bloque $\{h,i,j,k\}$. Como un elemento no puede fijar cuatro letras distintas sin ser la unidad, a cada bloque de 4 letras le corresponden elementos distintos de los descritos, pero que deben permutar las primeras seis letras de las maneras $(1,2)(3,5)(4,6)$ y $(1,2)(3,6)(4,5)$ respectivamente. Pero si se portan igual en 4 letras deben ser el mismo elemento, pues la acción es nítida. De manera que sólo hay un posible elemento de este tipo.

Concluimos que hay a lo más un bloque de cuatro letras. Si denotamos por t el número de dichos bloques, tenemos que $t = 0, 1$, y además $n = 4t+6$ o bien $n = 4t+7$, dependiendo de si los elementos de orden dos fijan 2 ó 3 letras. Si $t = 0$, tenemos que $n = 6$ ó $n = 7$ y se trata del grupo alternante A_6 como ya se analizó arriba. Entonces, considerando el caso de $t = 1$, tenemos el siguiente resultado.

PROPOSICIÓN 4.6

Un grupo nítidamente 4-transitivo en al menos ocho letras es de grado 10 o grado 11.

Analicemos el caso de $n = 10$. Un grupo nítidamente 4-transitivo en 10 letras tiene orden $10 \cdot 9 \cdot 8 \cdot 7$, y por lo tanto tiene un elemento de orden 7, que será necesariamente un 7-ciclo. El subgrupo cíclico generado por él será un 7-subgrupo de Sylow de G, que denotaremos por P. Como el grupo es en particular 3 transitivo, por el Lema 4.2 tenemos que el normalizador de P en G es 3 transitivo en las letras que fija P. Como P fija tres letras, la acción del normalizador de P en las tres letras es la misma que la de S_3. Además, $N_G(P)$ es un producto subdirecto de su acción en las siete letras involucradas en el ciclo, y de S_3 (su acción en las tres letras fijadas por P).

Consideremos el $H < S_3$ que queda aparecido con la unidad en el producto subdirecto. Por Lema 4.1, tenemos que $H \lhd S_3$, y por lo tanto $H = \{1_{S_3}\}$, $H = A_3$, o $H = S_3$. En cualquiera de los últimos dos casos, tendríamos un 3-ciclo como elemento de H, y por lo tanto del normalizador de P en G. Esto nos llevaría a que G contiene un 3-ciclo. Como es 4-transitivo, contendría a todos, y sería al menos A_{10}, lo cual es imposible, pues A_{10} no es nítidamente 4-transitivo. De manera que concluimos que $H = \{1_G\}$.

Si llamamos M a la acción de $N_G(P)$ en las letras que mueve el ciclo, tenemos, haciendo una reasignación de los nombres de las letras, que $M < S_7$. Como P es el cíclico de orden 7, tendrámos que necesariamente

$$\frac{M}{P} \cong S_3$$

de lo que se sigue que el orden de M debe ser 42.

De hecho, haciendo una reasignación correcta de los nombres de las letras,

$$M < N_{S_7}\Big(\langle (1,2,3,4,5,6,7) \rangle\Big)$$

¿Quién es dicho normalizador? Notemos que el normalizador debe mandar al ciclo $(1,2,3,4,5,6,7)$ en una potencia de sí mismo que no sea la identidad, y que hay 6 potencias. Además por cada potencia, podemos elegir a cual de las 7 letras involucradas

mandamos al 1, de manera que el normalizador tendrá $6 \cdot 7 = 42$ elementos. Puesto que ese era el orden que debía tener M, tenemos que

$$M = N_{S_7}(\langle(1,2,3,4,5,6,7)\rangle)$$

Utilizando el paquete CAYLEY para el estudio de grupos, se puede verificar fácilmente que $M = \langle(1,2,3,4,5,6,7),(2,4,3,7,5,6)\rangle$, y que además el cociente de M módulo P da un grupo isomorfo al cíclico de orden 6, y no a S_3.

En conclusión, el subgrupo H de los que aparecen apareados con la identidad debe ser S_3 o A_3, y en cualquier caso, el grupo G contendrá a todos los 3-ciclos, y por lo tanto a A_{10}.

COROLARIO 4.7

No existen grupos nítidamente 4-transitivos en 10 letras.

Analicemos ahora la estructura que tendría un grupo nítidamente 4- transitivo en 11 letras (y que por lo tanto no puede ser A_{11} ni S_{11}).

Sea $W < G$ el subgrupo que fija 3 letras, digamos $1, 10, 11$. W es regular (i.e. nítidamente 1-transitivo) en las ocho letras restantes, y es de orden 8, de manera que es la representación regular de alguno de los 5 grupos de orden 8: $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, el dihédrico de orden 8 D_4, o el grupo multiplicativo de los cuaternios Q.

PROPOSICIÓN 4.8

W es isomorfo al grupo de los cuaternios.

Demostración: No importa cuál de los cinco casos se trate, W tiene un elemento de orden 2, digamos $x = (9,2)(3,4)(5,6)(7,8)(1)(10)(11)$. En el subgrupo $H < G$ que fija al 10 y al 11, hay nueve conjugados de W, uno por cada letra que fija entre $\{1,2,3,\ldots,9\}$.

Si dos elementos de orden 2 contienen a la misma transposición, digamos (i,j), su producto sería un elemento distinto de la identidad que fija al menos cuatro elementos, y eso es imposible. Ya que cada elemento de orden 2 contiene cuatro transposiciones, y hay $\binom{9}{2} = 36$ transposiciones de $1,2,\ldots,9$, sólo hay nueve elementos de orden 2, y estará uno en cada conjugado de W en H. De manera que W tiene sólo un elemento de orden 2, y por lo tanto debe ser $\mathbb{Z}_8$ Q.

Si $W = Z_8$, tenemos sin perder generalidad que $W = \langle(9,3,5,7,2,4,6,8)\rangle$.

El normalizador de W es 3-transitivo en las 3 letras que fija W por Lema 4.2, y por lo tanto contiene una imágen homomorfa a S_3, basándonos en cómo actúa en esas letras. Así que 3 divide al órden del normalizador, que tendrá elementos de orden 3. Pero Z_8 no tiene automorfismos de orden 3, de manera que dicho elemento actúa como la identidad en las 8 letras del ciclo. Pero entonces es la identidad, pues el grupo es nítidamente 4--transitivo, y sería de orden 1 y no de orden 3, lo cual nos da una contradicción. Con lo cual concluimos que $W \cong Q$ los cuaternios.

□

Consideremos ahora el subgrupo $H < G$ que fija al 10 y al 11. Es de orden $8 \cdot 9 = 72$, nítidamente 2-transitivo, y contiene a 8 copias isomorfas de Q, cada una fijando a otro elemento de $\{1,2,\ldots,9\}$. Cualesquiera dos de estas copias tienen en común sólo a la identidad, pues están determinadas por su elemento de órden 2, y cualquier elemento distinto de la identidad es de orden 2 o su cuadrado es de orden 2. Esto cubre a $9 \cdot 7 + 1 = 64$ elementos, de manera que faltan ocho.

H tiene un subgrupo de orden 9 (su 3-subgrupo de Sylow), y no puede tocar ninguna de las copias de Q que contiene; así que esos 8 elementos que faltan y la identidad forman un grupo, cuyos elementos son la identidad, y los demás de orden 3 ó 9. Claramente es el único 3-subgrupo de Sylow, de manera que es normal en H. Denotemoslo por U.

PROPOSICIÓN 4.9

U es elemental abeliano de orden 9, y sus ocho elementos distintos de la identidad son conjugados bajo Q uno del otro.

Demostración: U es de orden 9, y por ser su orden el cuadrado de un número primo, el grupo es necesariamente abeliano.

Los elementos de U no fijan ningún elemento, de manera que cada uno de ellos envía al 1 a otro elemento del $\{1,2,\ldots,9\}$. (Si dos elementos, $x, y \in U$ mandaran al 1 en la misma letra x, entonces xy^{-1} fijaría a x y sería elemento de alguna de las copias de Q contenidas en H). Puesto que Q es regular, es claro que si conjugo el que manda el 1 a y con el elemento de Q que manda y en x, obtengo el elemento que manda el 1 en x.

De manera que todos los elementos de U son conjugados uno del otro bajo Q, y por lo tanto U no puede ser el cíclico de orden 9, y debe ser elemental abeliano.

□

De esta información podemos construír a H, único salvo isomorfismos. U está generado por

$$u = (1,2,3)(4,5,6)(7,8,9)(10)(11)$$

$$v = (1,4,7)(2,5,8)(3,6,9)(10)(11)$$

Y $H = Q \cdot U$, con Q el grupo de cuaternios dado por

$$a = (1)(2,4,3,7)(5,6,9,8)(10)(11)$$

$$b = (1)(2,5,3,9)(4,8,7,6)(10)(11)$$

con $a^2 = b^2 = (2,3)(4,7)(5,9)(6,8)(1)(10)(11)$.

Es fácil verificar que el grupo H en efecto es nítidamente 2-transitivo. Utilizando los Teoremas de Holyoke y Witt, podemos ahora construir extensiónes transitivas de H hasta llegar al grupo G.

Identificando a las letras $2, 1, 10, 11$ con las $0, 1, 2, 3$ de la notación de Holyoke, tenemos que $G_0 = \{1_G\}$, $G_1 = Q$, y $G_2 = H$, que es el que queremos extender.

El subgrupo K que fija al 11 estará generado, por el Teorema de Holyoke, por H y un elemento $a_i^{(\sigma)}$ que fija al 2 y al 11, e intercambia 1 y 10. Por lo tanto será un elemento de orden 2, y ya que todo elemento de orden 2 es conjugado, se trata de un conjugado de a^2.

Llamemos x a dicho elemento. Para que produzca una extensión transitiva es necesario y suficiente que normalice a Q (el enunciado del teorema pide que $xQx = Q$, pero por ser x de orden dos esto equivale a normalizarlo), y que multiplicado por el elemento de H que intercambia 1 y 2, elevado al cubo sea elemento de G_0 (i.e., sea de orden 3). El elemento de H que intercambia 1 y 2 es $y = (1,2)(6,9)(4,8)(5,7)$, lo cual se puede verificar construyendo H.

Ya que $Q = \langle a, b \rangle$, con

$$a = (1)(2,4,3,7)(5,6,9,8)(10)(11)$$

$$b = (1)(2,5,3,9)(4,8,7,6)(10)(11)$$

x debe fijar al 3, pues debe mandar x^2 en sí mismo y debe fijar al 2. De manera que

$$x = (2)(3)(11)(1,10)\cdots$$

Las únicas posibilidades para x serán pues:

$$x_1 = (2)(3)(11)(1,10)(4,5)(7,9)(6,8)$$
$$x_2 = (2)(3)(11)(1,10)(4,6)(7,8)(5,9)$$
$$x_3 = (2)(3)(11)(1,10)(4,7)(5,6)(9,8)$$
$$x_4 = (2)(3)(11)(1,10)(4,8)(7,6)(5,9)$$
$$x_5 = (2)(3)(11)(1,10)(4,9)(5,7)(6,8)$$

Además, adjuntar x a H no debe producir un elemento que fije a 4 o más letras y no sea la identidad.

Tenemos que $ux_4 = (1,10,2,3)(4,9,6,8,5,7)$, y por lo tanto $(ux_4)^1$ fija a 4 letras sin ser la identidad, de manera que x_4 queda fuera. Análogamente, $ux_5 = (1,10,2,3)(4,7,6,9,5,8)$, lo cual deja fuera también a x_5 de las consideraciones.

El elemento $(4,5,6)(7,9,8)$ manda bajo conjugación a H en sí mismo, y manda a x_1 en x_3, x_3 en x_2, y x_2 en x_1; de manera que agregar cualquiera de ellos daría lugar a extensiones transitivas isomorfas. Veamos que en efecto agregar x_1 da lugar a una extensión isomorfa.

TEOREMA 4.10

$K = \langle H, x_1 \rangle$ es una extensión transitiva de H.

Demostración: Por construcción tenemos que $x_1 Q x_1 = Q$. De manera que el primer requisito se satisface. Además, tomando $x_1 y$ tenemos que

$$\begin{aligned}(x_1 y)^3 &= \Big((1,10)(4,5)(7,9)(6,8)(1,2)(6,9)(4,8)(5,7)\Big)^3 \\ &= \Big((1,2,10)(3)(4,6,7)(5,9,8)\Big)^3 \\ &= 1_G\end{aligned}$$

de manera que las dos condiciones del Teorema 3.4 se satisfacen y $K = \langle H, x_1 \rangle$ es una extensión transitiva de H.

□

COROLARIO 4.11

Habrá a lo más dos extensiones transitivas de K a un grupo 4– transitivo, y a lo más una a un grupo 5–transitivo.

Demostración: Se sigue del Corolario 3.6, i.e. de aplicaciones sucesivas del Teorema de Holyoke.

□

Consideremos ahora a K, la extensión de H por x_1, como el subgrupo de G que fija al 11. K es un grupo nítidamente 3– transitivo, y G se obtendrá como una extensión de K agregando un elemento de orden 2 (y por lo tanto conjugado de a^2) adecuado.

Nuevamente renumeremos a $2, 10, 1, 11$ como $0, 1, 2, 3$ en la notación de Holyoke, identificando $G_0 = \{1_G\}$, $G_1 = Q$ (el subgrupo que fija al $1, 10, 11$), y G_2 el subgrupo de K que fija 1 y 11 (y por lo tanto el conjugado de H por un elemento que mande 10 en 1, por ejemplo x_1) y por último $G_3 = K$.

La extensión de K a G estará dada por un elemento de orden dos que normalice a $x_1 H x_1$, intercambie 1 y 11, y fije a 2 y 10. Además, debe normalizar a Q, pues Q fija el $1, 10, 11$, y este elemento manda estos en sí mismos. De manera que tenemos únicamente 5 posibilidades de elemento, que son

$$y_1 = (2)(3)(10)(1,11)(4,5)(6,8)(7,9)$$
$$y_2 = (2)(3)(10)(1,11)(4,6)(5,9)(7,8)$$
$$y_3 = (2)(3)(10)(1,11)(4,7)(5,6)(8,9)$$
$$y_4 = (2)(3)(10)(1,11)(4,8)(5,9)(7,6)$$
$$y_5 = (2)(3)(10)(1,11)(4,9)(5,7)(6,8)$$

Agregar una tal y a K no debe producir un elemento distinto de la identidad que fije al menos a cuatro letras. Pero tenemos que $uy_4 = (1,11,2,3)(4,9,6,8,5,7)$, que a la cuarta da lugar a un elemento que fija a cuatro letras y no es la identidad. De esta manera desechamos a y_4. Análogamente, y ya que $uy_5 = (1,11,2,3)(4,7,6,9,5,8)$, podemos desechar a y_5. Por último, ya que $x_1 y_1 = (1,11,10)$, podemos desechar también a y_1. Esto nos deja únicamente a y_2 y a y_3.

El elemento $(4,9)(5,7)(6,8)$ normaliza a K y manda y_2 en y_3, de manera que adjuntar cualquiera de ellos me daría una extensión isomorfa.

TEOREMA 4.12

$G = \langle K, y_2 \rangle$ es una extensión transitiva de K.

Demostración: Se requiere que y_2 normalice a $x_1 H x_1$, y multiplicado por el elemento de orden 2 que intercambia 1 y 10 dé un elemento de orden 3.

Tenemos que $x_1 H x_1 = \langle x_1 a x_1, x_1 b x_1, x_1 u x_1, x_1 v x_1 \rangle$. Puesto que x_1 normaliza a Q, $x_1 a x_1 = a$ y $x_1 b x_1 = b$. Además,

$$x_1 u x_1 = (10,2,3)(5,4,8)(9,6,7)$$

$$x_1 v x_1 = (10,5,9)(2,4,6)(3,8,7)$$

Bastará checar que $y_2 x_1 u x_1 y_2 = x_1 u x_1$ y $y_2 x_1 v x_1 y_2 = x_1 v x_1$, pues por contrucción y_2 normaliza a Q. Y tenemos que en efecto

$$y_2(10,2,3)(5,4,8)(9,6,7)y_2 = (10,2,3)(5,4,8)(9,6,7)$$

$$y_2(10,5,9)(2,4,6)(3,8,7)y_2 = (10,5,9)(2,4,6)(3,8,7)$$

de manera que y_2 satisface la primera condición del Teorema 3.4.

Por último, tenemos que

$$y_2 x_1 = (1,11)(4,6)(5,9)(7,8)(1,10)(4,5)(7,9)(6,8) = (1,10,11)(2)(3)(4,9,8)(5,6,7)$$

un elemento de orden 3, y por lo tanto se satisface la segunda condición del Teorema 3.4, verificando que agregar y_2 produce una extensión transitiva G de K.

□

COROLARIO 4.13

Cualquier grupo nítidamente 4-transitivo en 11 letras será isomorfo a G.

Demostración: La construcción que hemos realizado determinó salvo isomorfismos a Q y a H. Además, las observaciones que se han hecho, y el Teorema de Holyoke, nos garantizan la unicidad hasta isomorfismo de G, demostrandose el resultado.

□

COROLARIO 4.14

Existe a lo más una posible extensión de G a un grupo nítidamente 5-transitivo en 12 letras.

El grupo G que hemos construído se llama el **Grupo de Mathieu de grado 11**, y se suele denotar por M_{11}.

TEOREMA 4.15

Un grupo nítidamente 4-transitivo debe ser S_4, S_5, A_6, o isomorfo a M_{11}.

Pensemos ahora en M_{11} como un subgrupo de S_{12}, donde todo elemento fija al 12, y buscaremos dar la extensión transitiva a un grupo nítidamente 5-transitivo. Identificando ahora a $2, 10, 11, 1, 12$ con $0, 1, 2, 3, 4$ en la notación de Holyoke, tenemos que $G_0 = \{1_{M_{11}}\}$, $G_1 = Q$, $G_2 = x_1 H x_1$, $G_3 = y_2 K y_2$, y $G_4 = M_{11}$. La extensión transitiva la dará un elemento de orden dos que intercambie 1 con 12, y fije a $2, 10, 11$. Además, debe normalizar a $y_2 K y_2 = (y_2 H y_2, y_2 x_1 y_2)$, y al multiplicarlo por un elemento que intercambie 1 con 11 (por ejemplo y_2) debe dar un elemento de orden 3. Puesto que además manda el $\{1, 10, 11, 12\}$ en sí mismo, debe normalizar a Q. Tenemos pues únicamente 5 posiblidades:

$$z_1 = (2)(3)(10)(11)(1,12)(4,5)(6,8)(7,9)$$
$$z_2 = (2)(3)(10)(11)(1,12)(4,6)(6,8)(7,9)$$
$$z_3 = (2)(3)(10)(11)(1,12)(4,7)(5,6)(8,9)$$
$$z_4 = (2)(3)(10)(11)(1,12)(4,8)(5,9)(7,6)$$
$$z_5 = (2)(3)(10)(11)(1,12)(4,9)(5,7)(6,8)$$

Adjuntar la z adecuada no debe producir elementos distintos de la identidad que fijen a 5 o más letras.

Tenemos que $z_1 x_1 = (1,12)(1,10) = (1,10,12)$ que fija más de cinco letras, de manera que podemos desechar z_1. Análogamente, y ya que $z_2 y_2 = (1,12)(1,11) = (1,11,12)$,

podemos hacer a un lado z_2. Tenemos además que

$$\begin{aligned} uz_4 &= (1,2,3)(4,5,6)(7,8,9)(1,12)(4,8)(5,9)(7,6) \\ &= (1,12,2,3)(4,9,6,8,5,7)(10)(11) \end{aligned}$$

$$\begin{aligned} uz_5 &= (1,2,3)(4,5,6)(7,8,9)(1,12)(4,9)(5,7)(6,8) \\ &= (1,12,2,3)(4,7,6,9,5,8)(10)(11) \end{aligned}$$

y ambos elevados a la cuarta potencia fijan más de 5 elementos sin ser la identidad. De manera que la única posibilidad de extensión la dá z_3.

TEOREMA 4.16

$M_{12} = \langle M_{11}, z_3 \rangle$ es una extensión transitiva de M_{11}.

Demostración: Tenemos que debe normalizar a y_2Ky_2, y multiplicado por y_2 debe dar un elemento de orden tres.

Puesto que y_2 y z_3 ambos normalizan a Q, basta verificar que $z_3y_2uy_2z_3 \in y_2Ky_2$ y $z_3y_2vy_2z_3 \in y_2Ky_2$. Notemos primero que

$$y_2uy_2 = (11,2,3)(6,9,4)(8,7,5)$$

$$y_2vy_2 = (11,6,8)(2,9,7)(3,4,5)$$

y que $y_2uvy_2 = (11,9,5)(2,4,8)(3,6,7)$. Tenemos ahora que

$$\begin{aligned} z_3y_2uy_2z_3 &= (11,2,3)(5,8,7)(9,4,6) \\ &= y_2uy_2 \end{aligned}$$

$$\begin{aligned} z_3y_2vy_2z_3 &= (11,5,9)(2,8,4)(3,7,6) \\ &= (y_2uvy_2)^{-1} \end{aligned}$$

por lo que z_3 normaliza a y_2Ky_2, verificandose la primera condición del Teorema 3.4.

Para terminar, tenemos que

$$\begin{aligned} y_2z_3 &= (1,11)(4,6)(5,9)(7,8)(1,12)(4,7)(5,6)(8,9) \\ &= (1,12,11)(2)(3)(4,8,5)(6,9,7) \end{aligned}$$

de orden tres, terminando la demostración.

□

El grupo M_{12} que acabamos de construir recibe el nombre de **Grupo de Mathieu de grado 12**. Tenemos, con esto y la clasificación de los grupo nítidamente 4-transitivos, el siguiente resultado:

TEOREMA 4.17

Los únicos grupos nítidamente 5-transitivos son S_5, S_6, A_7, y M_{12}.

Demostración: El estabilizador de una letra en un grupo nítidamente 5 transitivo es un grupo nítidamente 4 transitivo, que debe ser S_4, S_5, A_6, o M_{11}. Por lo que el grupo dado debe actuar en 5, 6, 7, ó 12 letras. En los tres primeros casos, el orden del grupo nos da la igualdad con S_5, S_6, y A_7 respectivamente. En el último caso, tenemos que queda determinado de manera única por cuál copia isomorfa de M_{11} se trate. La extensión tendrá que ser por una permutación isomorfa a z_3, con el mismo isomorfismo que determina la copia, y será por lo tanto isomorfa a M_{12}.

□

COROLARIO 4.18

El único grupo nítidamente 5-transitivo no trivial es M_{12}, salvo isomorfismos. El único grupo nítidamente 4-transitivo no trivial es M_{11}, salvo isomorfismos.

COROLARIO 4.19

Los únicos grupos nítidamente k-transitivos, con $k \geq 6$ son los triviales, esto es, los simétricos y alternante correspondientes.

Demostración: Un grupo nítidamente k-transitivo que no sea alternante ni simétrico dará lugar a un grupo isomorfo a M_{12} al bajarle la transitividad considerando subgrupos que fijan diversas letras. Sin embargo, ya tenemos que M_{12} no se puede extender como consecuencia del Teorema de Holyoke, pues la extensión de M_{11} a M_{12} es única. De manera que dicho grupo no puede existir, pues sería una extensión transitiva de M_{12}.

□

Además, hemos obtenido la siguiente información sobre M_{12}.

TEOREMA 4.20

M_{12} es un subgrupo del grupo alternante A_{12}.

Demostración: M_{12} se obtuvo como extensiones sucesivas del grupo H. H fue dado explícitamente por generadores, todos ellos permutaciones pares. De manera que $H < A_{12}$. Tenemos pues que $M_{12} = (H, x_1, y_2, z_3)$, las tres permutaciones x_1, y_2, z_3 son pares. De manera que M_{12} es un grupo generado por permutaciones pares, y por lo tanto es un subgrupo del alternante correspondiente. En este caso, de A_{12}.

□

TEOREMA 4.21

Si $a \in M_{12}$ es de orden 2 y fija al menos una letra, entonces fija a cuatro letras.

Demostración: Sea $a \in M_{12}$. Supongamos que fija a la letra i. Entonces a está en el estabilizador de i en M_{12}. Dicho estabilizador es isomorfo a M_{11}, pues es nítidamente 4-transitivo en 11 letras. Pero en M_{11} todo elemento de orden 2 fija tres letras. De manera que a fija a tres letras (además de i). Entonces a fija a cuatro letras.

□

TEOREMA 4.22

Si $a \in M_{12}$ fija exactamente tres letras, entonces es de orden tres.

Demostración: Sea $a \in M_{12}$ que fije tres letras, digamos i, j, k. Entonces está contenido en el estabilizador de i en M_{12}, que es una copia isomorfa de M_{11}, y estará en el estabilizador de 2 letras en ese M_{11}. Ese grupo es de orden 72, y es isomorfo al grupo H que se construyó arriba (i.e. el grupo de cuaternios por un elemental abeliano de orden 9). Por lo tanto a es de orden 2, 4 ó 3. No puede ser de orden 2, pues un elemento de orden dos que fija al menos una letra en M_{12} fija a cuatro. No puede ser de orden 4, pues entonces su cuadrado sería de orden 2 y debería fija cuatro letras. (Su estructura como elemento de orden cuatro tendría que ser un producto de dos 4-ciclos, por pertenecer a la copia de Q en H). Concluímos que pertenece al elemental abeliano de orden 9, y por lo tanto es de orden 3.

□

V. Construcción de Rotman–Witt

En este capítulo realizaremos la construcción de Rotman del grupo M_{12}, que hemos ya caracterizado como el único grupo nítidamente 5-transitivo no trivial. La construcción se hace como extensiones transitivas sucesivas del grupo lineal $Sh(9)$. El proceso realizado por Rotman es análogo al dado por Witt en su artículo *Die 5-fach transitiven Gruppen von Mathieu*, publicado en 1938.

Primero daremos algunas definiciones y proposiciones necesarias para la definiciones del grupo $Sh(9)$.

$CG(q)$ representará el campo de Galois de orden q, donde q es una potencia de un número primo.

$Aut(q)$ representa el grupo de automorfismos de campo de $CG(q)$, con la composición.

Sea V un espacio vectorial sobre un campo K. Definimos una relación de equivalencia en $V^* = V - \{\overline{0}\}$, dado por $x \sim y \iff \exists \lambda \in K$ tal que $x = \lambda y$. Si $x \in V^*$, denotaremos la clase de x por $[x]$.

DEFINICIÓN

Sea V un espacio vectorial sobre K de dimensión $n+1$. El conjunto cociente

$$P(V) = \{[x] \mid x \in V^*\}$$

se llama el espacio proyectivo n- dimensional (sobre K) y se dice que tiene dimensión (proyectiva) n.

Si V es de dimensión $n+1$, se escribirá simplemente $P^n(K)$. Si $K = CG(q)$, se escribirá simplemente $P^n(q)$.

El espacio proyectivo 1-dimensional sobre el campo K se puede representar como el campo K adjuntándole un nuevo punto ∞, que es la imágen de la recta $(0, x)$ bajo la proyección canónica. Todas las demás, al representarlas en la forma $(1, y)$ van a dar al elemento $y \in K$.

DEFINICIÓN

Sea K un campo y $\sigma \in Aut(K)$. Una transformación semilineal fraccionaria es una función $f: K \cup \{\infty\} \to K \cup \{\infty\}$ de la forma

$$f(\lambda) = \frac{a\sigma(\lambda) + b}{c\sigma(\lambda) + d},$$

con $ad - bc \neq 0$; si $c = 0$, entonces $f(\infty) = \infty$. Si $c \neq 0$, entonces se define $f(\infty) = ac^{-1}$. Si σ es la identidad, f se llama una transformación lineal fraccionaria.

DEFINICIÓN

Todas las transformaciones semilineales fraccionarias forman un grupo con la composición, que se denota por $\Gamma LF(K)$; todas las transformaciones lineales fraccionarias forman un subgrupo de $\Gamma LF(K)$, denotado por $LF(K)$. Si $K = CG(q)$, se escribirá $\Gamma LF(q)$ en vez de $\Gamma LF(K)$, y $LF(q)$ en vez de $LF(K)$.

Si $h \in \Gamma LF(q)$, entonces $h(\lambda) = (a\sigma(\lambda) + b) / (c\sigma(\lambda) + d)$ con $\sigma \in Aut(CG(q))$, y con $ad - bc \neq 0$. Multiplicar el numerador y el denominador por $\mu \in CG(q)^*$ no afecta h, pero cambia el "determinante" a $\mu^2(ad - bc)$. Si q es potencia de 2, todo elemento en $CG(q)$ es un cuadrado; pero si q es potencia de un primo impar, y denotamos por α un elemento primitivo de $CG(q)$, entonces los cuadrados no cero forman un subgrupo de índice dos en $CG(q)^*$, a saber $\langle \alpha^2 \rangle$. En este caso, tiene sentido preguntarse si $det(h)$ es o no es un cuadrado.

El segundo ingrediente en la definición de $Sh(q)$ es un automorfismo de $CG(q)$ de orden 2. Es fácil ver que dicha σ existe y es única cuando $q = p^{2n}$, y en ese caso $\sigma(\lambda) = \lambda^{p^n}$.

DEFINICIÓN

Sea $q = p^{2n}$, con p un primo impar, y sea $\sigma \in Aut(CG(q))$ de orden 2 (i.e., $\sigma(\lambda) = \lambda^{p^n}$). Definimos $Sh(q)$ como el subconjunto $A \cup B$ de $\Gamma LF(q)$, donde

$$A = \left\{ h: \lambda \mapsto \frac{a\lambda + b}{c\lambda + d} \;\middle|\; ad - bc \text{ es un cuadrado} \right\}$$

y

$$B = \left\{ h: \lambda \mapsto \frac{a\sigma(\lambda) + b}{c\sigma(\lambda) + d} \;\middle|\; ad - bc \text{ no es un cuadrado} \right\}.$$

PROPOSICIÓN 5.1

$Sh(q)$ es un subgrupo de $\Gamma LF(q)$.

Demostración: La composición en A es cerrada, pues si

$$g = \frac{a\lambda + b}{c\lambda + d}$$
$$h = \frac{\alpha\lambda + \beta}{\gamma\lambda + \delta}$$

con $ad - bc$ y $\alpha\delta - \gamma\beta$ cuadrados, entonces

$$\begin{aligned} h \circ g(\lambda) &= h\left(\frac{a\lambda + b}{c\lambda + d}\right) \\ &= \frac{\alpha\left(\frac{a\lambda+b}{c\lambda+d}\right) + \beta}{\gamma\left(\frac{a\lambda+b}{c\lambda+d}\right) + \delta} \\ &= \frac{(\alpha a + \beta c)\lambda + (\alpha b + \beta d)}{(\gamma a + \delta c)\delta + (b\gamma + \delta d)} \end{aligned}$$

y además

$$\begin{aligned} (\alpha a + \beta c)(b\gamma + \delta d) - (\alpha b + \beta d)(\gamma a + \delta c) &= \alpha a b\gamma + \alpha a\delta d + \beta c b\gamma + \beta c\delta d + \\ &\quad - (\alpha b\gamma a + \alpha b\delta c + \beta d\gamma a + \beta d\delta c) \\ &= \alpha a\delta d + bc\beta\gamma - bc\alpha\delta - ad\beta\gamma \\ &= (ad - bc)(\alpha\delta - \beta\gamma). \end{aligned}$$

que es producto de cuadrados, y por lo tanto cuadrado. De manera que $A \circ A \subset A$.

Análogamente tenemos que la composición de elementos de B da un elemento de A, pues si $g, h \in B$, tenemos que

$$g = \frac{a\sigma(\lambda) + b}{c\sigma(\lambda) + d}$$
$$h = \frac{\alpha\sigma(\lambda) + \beta}{\gamma\sigma(\lambda) + \delta}$$

con $ad - bc$ y $\alpha\delta - \gamma\delta$ ambos no cuadrados, tenemos que

$$\begin{aligned} h \circ g(\lambda) &= h\left(\frac{a\sigma(\lambda)+b}{c\sigma(\lambda)+d}\right) \\ &= \frac{\alpha\sigma\left(\frac{a\sigma(\lambda)+b}{c\sigma(\lambda)+d}\right)+\beta}{\gamma\sigma\left(\frac{a\sigma(\lambda)+b}{c\sigma(\lambda)+d}\right)+\delta} \\ &= \frac{\alpha\left(\frac{a(a)\lambda+\sigma(b)}{\sigma(c)\lambda+\sigma(d)}\right)+\beta}{\gamma\left(\frac{a(a)\lambda+\sigma(b)}{\sigma(c)\lambda+\sigma(d)}\right)+\delta} \\ &= \frac{\alpha\sigma(a)\lambda+\alpha\sigma(b)+\beta\sigma(c)\lambda+\beta\sigma(d)}{\gamma\sigma(a)\lambda+\gamma\sigma(b)+\sigma(c)\delta\lambda+\sigma(d)\delta} \\ &= \frac{(\alpha\sigma(a)+\beta\sigma(c))\lambda+(\alpha\sigma(b)+\beta\sigma(d))}{(\gamma\sigma(a)+\delta\sigma(c))\lambda+(\gamma\sigma(b)+\delta\sigma(d))}. \end{aligned}$$

Basta ver que el determinante es un cuadrado. Pero lo es, pues

$$\begin{aligned} &(\alpha\sigma(a)+\beta\sigma(c))(\gamma\sigma(b)+\delta\sigma(d)) - (\alpha\sigma(b)+\beta\sigma(d))(\gamma\sigma(a)+\delta\sigma(c)) = \\ &\quad = \alpha\sigma(a)\gamma\sigma(b) + \alpha\sigma(a)\delta\sigma(d) + \beta\sigma(c)\gamma\sigma(b) + \beta\delta\sigma(c)\sigma(d) + \\ &\quad - (\alpha\sigma(a)\gamma\sigma(b) + \alpha\sigma(b)\delta\sigma(c) + \beta\sigma(d)\gamma\sigma(a) + \beta\sigma(c)\delta\sigma(c)) = \\ &= \alpha\sigma(a)\delta\sigma(d) + \beta\sigma(c)\gamma\sigma(b) - (\alpha\sigma(b)\delta\sigma(c) + \beta\sigma(d)\gamma\sigma(a)) = (\alpha\delta - \beta\gamma)\sigma(ad - bc). \end{aligned}$$

Como σ es un automorfismo, manda cuadrados en cuadrados (pues el subgrupo de los cuadrados es normal y de índice dos), y por lo tanto manda no cuadrados en no cuadrados. De manera que lo de arriba es un producto de elementos de $\{\sigma, \sigma^3, \ldots, \sigma^9\}$, y es por lo tanto un cuadrado. De manera que $B \circ B \subset A$.

Si $g \in B$ y $h \in A$, entonces tenemos que

$$\begin{aligned} g &= \frac{a\sigma(\lambda)-b}{c\sigma(\lambda)-d} \\ h &= \frac{\alpha\lambda-\beta}{\gamma\lambda-\delta} \end{aligned}$$

con $ad - bc$ no un cuadrado, y $\alpha\delta - \beta\gamma$ un cuadrado. Haciendo los cálculos, se obtiene que

$$h \circ g(\lambda) = \frac{(\alpha a + \beta c)\sigma(\lambda) + (\alpha b + \beta d)}{(\gamma a + \delta c)\sigma(\lambda) + (\gamma b + \delta d)}$$

y que el determinante es igual a $(ad-bc)(\alpha\delta-\beta\gamma)$, que no es un cuadrado. De manera que $A \circ B \subset B$.

Por último, se obtiene que, con la misma notación de arriba,

$$g \circ h(\lambda) = \frac{(a\sigma(\alpha)+b\sigma(\gamma))\sigma(\lambda)+(a\sigma(\beta)+b\sigma(\delta))}{(c\sigma(\alpha)+d\sigma(\gamma))\sigma(\lambda)+(c\sigma(\beta)+d\sigma(\delta))}$$

y que el determinante vale $(ad-bc)\cdot\sigma(\alpha\delta-\gamma\beta)$, que es el producto de un no cuadrado por un cuadrado, y por lo tanto no un cuadrado. De manera que $B \circ A \subset B$, y tenemos que es cerrado bajo la operación.

Se verifica fácilmente que el inverso de $g=(a\lambda+b)/(c\lambda+d) \in A$ es $(\alpha\lambda+\beta)/(\gamma\lambda+\delta)$ con

$$\alpha=\frac{d}{ad-bc}; \quad \beta=\frac{-b}{ad-bc}; \quad \gamma=\frac{-c}{ad-bc}; \quad \delta=\frac{a}{ad-bc}$$

y $\alpha\delta-\beta\gamma=1$ que es un cuadrado. Y un inverso de un elemento de B es igual, pero con $\sigma(\alpha),\sigma(\beta),\sigma(\gamma),\sigma(\delta)$. De manera que $Sh(q)$ es un grupo.

□

PROPOSICIÓN 5.2

A es un subgrupo de $Sh(q)$, de índice 2, y B es la otra clase lateral en $Sh(q)$ respecto de A.

Demostración: Como se vió en la demostración del anterior, $A \circ A \subset A$, de manera que A es un subgrupo de $Sh(q)$. La otra clase lateral respecto de A es B, pues nuevamente hemos visto que $B \circ B \subset A$, y por lo tanto dos elementos de B siempre están en la misma clase lateral (y puesto que $B \circ A, A \circ B \subset B$ los elementos de A y los de B no están en la misma clase lateral). Puesto que esto cubre todo $Sh(q)$, el índice de A debe ser dos.

□

Las letras "Sh" abrevian "*sharp*", nítido. Esto se aprecia en el siguiente teorema:

TEOREMA 5.3

Si p es un primo impar, y $q=p^{2n}$, entonces $P^1(q)$ es un $Sh(q)$-conjunto fiel y nítidamente 3-transitivo.

Demostración: Sea $K = CG(q)$, e identifiquemos nuevamente a $P^1(q)$ con $K \cup \{\infty\}$. En primer lugar, la acción es claramente nítida, pues dos elementos de $Sh(q)$ que actúan idéntico en $K \cup \{\infty\}$ deben ser el mismo (la acción en ∞ determina el valor de ac^{-1}, y la acción en 0 el valor de bd^{-1}, etc.).

Tenemos que $Sh(q)_\infty = A_\infty \cup B_\infty$, donde

$$A_\infty = \{h: \lambda \mapsto a\lambda + b \mid a \in (K^*)^2\}$$
$$B_\infty = \{h: \lambda \mapsto a\sigma(\lambda) + b \mid a \notin (K^*)^2\}$$

Si a y b son dos elementos distintos de K, con $a \neq 0$, entonces un pequeño cálculo permite exhibir $h \in Sh(q)_\infty$ con $h(0) = b$ y $h(1) = a$. A saber $h = (a-b)\lambda + b$ si $(a-b)$ es un cuadrado, y $h = (a-b)\sigma(\lambda) + b$ si $(a-b)$ no es un cuadrado. De manera que G_∞ actúa doblemente transitivo en K. Pero en cada uno de A_∞ y B_∞ hay q opciones para b y $\frac{1}{2}(q-1)$ opciones para a, de manera que $|Sh(q)_\infty| = q(q-1)$, y la acción de G_∞ en K es nítidamente 2-transitiva.

Por último, $Sh(q)$ actúa transitivamente en $K \cup \{\infty\}$, pues $\lambda \mapsto -\frac{1}{\lambda}$ es elemento de G e intercambia 0 con ∞. Puesto que la acción es transitiva, y el estabilizador de un punto es nítidamente 2-transitivo en el conjunto que queda, tenemos que la acción de $Sh(q)$ es nítidamente 3-transitiva en $K \cup \{\infty\}$, como consecuencia del Corolario 2.8*(v)*.

□

DEFINICIÓN

$Sh(9)$ se suele denotar por M_{10}, y se llama el Grupo de Mathieu de grado 10.

Veremos ahora un poco sobre la estructura de M_{10}, antes de pasar a extenderlo transitivamente. Identificaremos a $CG(9)$ con el campo

$$\{0, 1, -1, i, -i, 1+i, 1-i, -1+i, -1-i\}$$

con la suma módulo 3, y conveniendo que $i^2 = -1$. Además, el elemento primitivo α será identificado con $(1+i)$.

Introduciremos ahora un poco de notación.

$GL(n,q)$ denota el grupo multiplicativo de las matrices no singulares de $n \times n$ con coeficientes en $CG(q)$.

$Sc(n,q)$ denota el grupo de todas las matrices de $n \times n$, escalares e invertibles (i.e. la identidad por $\lambda \in CG(q)^*$).

$PGL(n,q)$ denota el grupo cociente $\frac{GL(n,q)}{Sc(n,q)}$.

Se puede probar que en general, $P^1(q)$ es un $PGL(2,q)$-conjunto fiel y nítidamente 3-transitivo (ver Rotman, pp. 216). De hecho se puede demostrar que el grupo $PGL(2,q)$ es isomorfo al grupo $LF(q)$ de las trasformaciones lineales fraccionarias.

TEOREMA 5.4

$PGL(2,9)$ y M_{10} son dos grupos no isomorfos de orden 720, cada uno de los cuales actúa nítidamente 3-transitivo en $P^1(9)$.

Demostración: Con los resultados anteriores, ya tenemos que cada uno de los grupos actúa en la manera descrita en $P^1(9) = K \cup \{\infty\}$. Es fácil ver que

$$PGL(2,9)_{0,\infty} = \{h : \lambda \mapsto a\lambda \text{ con } a \neq 0\}$$

teniendo en cuenta el isomorfismo con $LF(9)$. Este grupo es claramente isomorfo a $CG(9)^*$, que es a su vez isomorfo a Z_8; de hecho, un generador de $PGL(2,9)_{0,\infty}$ es $g : \lambda \mapsto \alpha\lambda$, con α un elemento primitivo de $CG(9)$. Si $\tau(\lambda) = \lambda^{-1}$, entonces τ es un elemento de orden 2 de $PGL(2,9)$, y tenemos que $\tau g \tau = g^{-1}$. Se sigue que $\langle G_{0,\infty}, \tau \rangle$ es el grupo dihédico de orden 16 y que es un 2-Subgrupo de Sylow de $PGL(2,9)$.

Consideremos ahora a M_{10}. Puesto que $q = 3^2$, el automorfismo σ es simplemente $\sigma(\lambda) = \lambda^3$. Entonces $(M_{10})_{0,\infty} = A_{0,\infty} \cup B_{0,\infty}$. Tenemos además que

$$A_{0,\infty} = \{h : \lambda \mapsto a^2\lambda \text{ con } a \neq 0\}$$

y que

$$B_{0,\infty} = \{h : \lambda \mapsto a\lambda^3 \text{ con } a \text{ no un cuadrado}\}.$$

Tenemos pues que éste es un grupo no abeliano de orden 8 que sólo tiene un elemento de orden 2 (a saber $\lambda \mapsto \alpha^4\lambda \in A_{0,\infty}$) y que por lo tanto $(M_{10})_{\infty,9} \cong Q$ los cuaternios.

Ya que el grupo dihédrico no tiene subgrupos isomorfos a los cuaternios, se sigue que los 2-subgrupos de Sylow de $PGL(2,9)$ y de M_{10} no son isomorfos, y por fuerza $PGL(2,9)$ no es isomorfo a M_{10}.

□

PROPOSICIÓN 5.5

Un 3-subgrupo de Sylow de M_{10} es elemental abeliano de orden 9.

Demostración: Puesto que $|M_{10}| = 10 \cdot 9 \cdot 8 = 720$, un 3-subgrupo de Sylow será de orden 9. Puesto que el orden es el cuadrado de un primo, necesariamente será abeliano. Construiremos un 3-subgrupo de Sylow de M_{10}, demostrando así la proposición.

Sea $S = \{\lambda \mapsto \lambda + b \mid b \in CG(9)\}$. Si $g(\lambda) = \lambda + a$ y $h(\lambda) = \lambda + b$ son elementos de S, entonces $gh^{-1}(\lambda) = g(\lambda - b) = \lambda - b + a = \lambda + (a - b) \in S$, de manera que S es un subgrupo de M_{10}. Por tener orden 9, será un 3-subgrupo de Sylow de M_{10}.

Por último, recordando que la característica de $CG(9)$ es 3, tenemos que $\forall g \in S$, si $g(\lambda) = \lambda + b$, $g^3(\lambda) = \lambda + 3b = \lambda$, de manera que $g^3 = 1_{GF(9)\cup\{\infty\}}$, y S es elemental abeliano.

□

PROPOSICIÓN 5.6

$(M_{10})_\infty$ es un grupo de orden 72, con un 3-subgrupo de Sylow que es normal. De hecho, $(M_{10})_\infty$ es un producto semidirecto de $Z_3 \times Z_3$ por Q (los cuaternios).

Demostración: Los elementos de $(M_{10})_\infty$ tienen la forma $f(\lambda) = \frac{a\lambda+b}{d}$, o $g(\lambda) = \frac{a\lambda^3+b}{d}$. De hecho, multiplicando por d^{-1} arriba y abajo, podemos suponer sin pérdida de generalidad, que los elementos son simplemente de la forma $f(\lambda) = a\lambda + b$, o $g(\lambda) = a\lambda^3 + b$.

Para el primer caso, hay 4 maneras de elegir a a (los 4 cuadrados de $CG(9)$), y 9 de elegir a la b. Lo mismo para el segundo caso, de manera que $|(M_{10})_\infty| = 36 + 36 = 72$. (Otra manera: puesto que M_{10} es nítidamente 3 transitivo en 10 símbolos, el estabilizador de uno de ellos es nítidamente 2 transitivo en 9, y por lo tanto de orden $9 \cdot 8 = 72$).

Puesto que el subgrupo S definido en la Proposición 5.5 es un subgrupo de M_{10}, será también un 3-subgrupo de Sylow de $(M_{10})_\infty$. Así que basta verificar que es normal. Para

ello, notemos primero que el inverso de $\lambda \mapsto \alpha^{2i}\lambda + b$ es $\lambda \mapsto \alpha^{6i}\lambda - \alpha^{6i}b$, y que el inverso de $\lambda \mapsto \alpha^{2i+1}\lambda^3 + b$ es $\lambda \mapsto \alpha^{2i+5}\lambda^3 - a^{2i+5}b^3$. En efecto, identificando con g el primero y h el supuesto inverso en cada caso, tenemos que

$$\begin{aligned} h \circ g(\lambda) &= h(\alpha^{2i}\lambda + b) \\ &= \alpha^{6i}(\alpha^{2i}\lambda + b) - \alpha^{6i}b \\ &= \alpha^{8i}\lambda + \alpha^{6i}b - \alpha^{6i}b \\ &= \lambda \end{aligned}$$

en el primer caso, y

$$\begin{aligned} h \circ g(\lambda) &= h(\alpha^{2i+1}\lambda^3 + b) \\ &= \alpha^{2i+5}(\alpha^{2i+1}\lambda^3 + b)^3 - \alpha^{2i+5}b^3 \\ &= \alpha^{2i+5}(\alpha^{6i+3}\lambda^9 + 3\alpha^{4i+2}\lambda^6 b + 3\alpha^{2i+1}b^3 + b^3) - \alpha^{2i+5}b^3 \\ \text{(ya que } car(CG(9)) = 3) \quad &= \alpha^{2i+5}(\alpha^{6i+3}\lambda + b^3) - \alpha^{2i+5}b^3 \\ &= \alpha^{8i+8}\lambda + \alpha^{2i+5}b^3 - \alpha^{2i+5}b^3 \\ &= \lambda \end{aligned}$$

en el segundo.

Tenemos pues que si $g(\lambda) = \lambda + \beta \in S$ y $h(\lambda) = \alpha^{2i}\lambda + b \in (M_{10})_\infty$, entonces

$$\begin{aligned} h \circ g \circ h^{-1}(\lambda) &= h(g(\alpha^{6i}\lambda - \alpha^{6i}b)) \\ &= h(\alpha^{6i}\lambda + \beta - \alpha^{6i}b) \\ &= \alpha^{8i}\lambda - \alpha^{8i}b + \alpha^{2i}\beta + b \\ &= \lambda - b + \alpha^{2i}\beta + b \\ &= \lambda + \alpha^{2i}\beta \in S \end{aligned}$$

Y si $h = \alpha^{2i+1}\lambda^3 + b$, mediante cálculos semejantes obtenemos que

$$h \circ g \circ h^{-1}(\lambda) = \lambda + \alpha^{2i+1}\beta^3 \in S$$

de manera que S es normal en $(M_{10})_\infty$.

Por otro lado, ya que $CG(9) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, entonces $S \cong CG(9) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ (con el isomorfismo natural $(\lambda + b) \mapsto b$), basta ver que el complemento es los cuaternios.

Los demás elementos de $(M_{10})_\infty$ son de la forma $\alpha^{2i}\lambda + b$ y $\alpha^{2i+1}\lambda^3 + b$. Tomamos $P < (M_{10})_\infty$ dado por

$$P = \{\lambda, -\lambda, i\lambda, -i\lambda, (i+1)\lambda^3, (1-i)\lambda^3, (-1+i)\lambda^3, (-1-i)\lambda^3\}$$

que es claramente un subgrupo, y establecemos un isomorfismo con

$$Q = \{1, -1, i, -i, j, -j, k, -k\}$$

mediante la siguiente correspondencia:

$$\begin{array}{ll} 1 \mapsto \lambda & j \mapsto (1+i)\lambda^3 \\ -1 \mapsto -\lambda & -j \mapsto (-1-i)\lambda^3 \\ i \mapsto i\lambda & k \mapsto (-1+i)\lambda^3 \\ -i \mapsto -i\lambda & -k \mapsto (1-i)\lambda^3 \end{array}$$

que es un isomorfismo. Puesto que todo elemento de $(M_{10})_\infty$ se puede ver como la composición de un elemento de P con uno de S, y $P \cap S = \{1\}$, tenemos que $(M_{10})_\infty$ es un producto semidirecto de S por P. Los isomorfismos ya dados dan el resultado deseado.

□

Para la Proposición 5.8 utilizaremos el Lema que aparece a continuación, que no se probará en este trabajo.

LEMA 5.7

Si $f(\lambda)$ y $g(\lambda)$ son polinomios en $K[x]$ con $K = CG(q)$, y $\partial f, \partial g < q$, entonces las funciones polinomiales correspondientes a f y g son iguales si y sólo si $f = g$.

PROPOSICIÓN 5.8

Hay exactamente 8 elementos de orden 3 en $(M_{10})_\infty$, y son conjugados uno de otro en $(M_{10})_\infty$.

Demostración: Supongamos que $(\alpha^{2i}\lambda + b)^3 = \lambda$. Entonces $\alpha^{6i}\lambda^3 + b^3 = \lambda$. Por el Lema 5.7, tenemos que $\alpha^{6i} = 1$ y por lo tanto $\alpha^{2i} = 1$.

Si $(\alpha^{2i+1}\lambda^3 + b)^3 = \lambda$, entonces tenemos nuevamente que $\alpha^{6i+3}\lambda + b^3 = \lambda$, y por lo tanto $\alpha^{2i+1} = 1$ lo cual es una contradicción. Concluimos que los únicos elementos de orden 3 son de la forma $\lambda + b$ con $b \in CG(9)^*$. Así que sólo hay ocho elementos de orden 3.

Conjugando con elementos de la forma $\alpha^{2k}\lambda + \gamma$, tenemos la fórmula

$$\alpha^{2k}\left((\alpha^{6k}\lambda - \alpha^{6k}\gamma) + b\right) + \gamma$$

que es igual a $\lambda + \alpha^{2k}b$. Conjugando con elementos de la forma $\alpha^{2k+1}\lambda + \gamma$, obtenemos $\gamma + \alpha^{2k+1}b^3$. Eligiendo $b = 1$, la primera fórmula cubre todos los elementos con término constante un cuadrado de $CG(9)$, y la segunda cubre aquellos con término constante un no cuadrado de $CG(9)$, de manera que todo elemento es conjugado de $\lambda + 1$, y por lo tanto uno del otro.

□

PROPOSICIÓN 5.9

M_{10} no es el producto semidirecto de A por $\mathbb{Z}_2$.

Demostración: Notemos primero que B no tiene elementos de orden 2. Esto se debe a que si $f \in B$, el determinante de f puede ser uno de $\{1+i, 1-i, -1+i, -1-i\}$. Además, es fácil verificar que $det(f^2) = det^4(f)$, y $(\pm 1 \pm i)^4 = -1 \neq 1$. De manera que B no tiene elementos de orden 2.

Sin embargo, si M_{10} fuera un producto semidirecto de A por $\mathbb{Z}_2$, la imágen del -1, que sería un elemento de B, sería de orden 2. Como esto es imposible, concluimos que M_{10} no es dicho producto semidirecto.

□

Notemos que hasta ahora hemos verificado algunas de las propiedades que tenía el subgrupo H de M_{12} en la construcción de Hall del capítulo anterior, y hemos obtenido algunas más, debido a la presentación de M_{10} dada en este capítulo.

Por último, extenderemos M_{10} a grupos nítidamente 4 y 5- transitivos. Utilizaremos el Teorema de Witt para garantizar que en efecto obtenemos extensiones transitivas de M_{10}.

TEOREMA 5.10

Existe un grupo nítidamente 4-transitivo de grado 11, y de orden $7920 = 11 \cdot 10 \cdot 9 \cdot 8$, tal que el estabilizador de un punto es M_{10}.

Demostración: Sabemos ya que M_{10} actúa nítidamente 3-transitivo en $CG(9) \cup \{\infty\}$. Construiremos una extensión transitiva de M_{10}.

En la notación del Teorema de Witt, identificamos $G = M_{10}$, $X = CG(9) \cup \{\infty\}$, $\overline{X} = X \cup \{\omega\}$. Definimos a

$$x = \infty$$

$$g = (0, \infty)(\alpha, \alpha^7)(\alpha^2, \alpha^6)(\alpha^3, \alpha^5)$$

$$h = (\omega, \infty)(\alpha, \alpha^2)(\alpha^3, \alpha^7)(\alpha^5, \alpha^6)$$

Notemos que g corresponde al elemento de M_{10} que manda $\lambda \mapsto \lambda^{-1}$ (cuyo determinante es -1, un cuadrado). También tenemos que $(\alpha, \alpha^2)(\alpha^3, \alpha^7)(\alpha^5, \alpha^6)$ corresponde a la permutación de $CG(9)$ dada por $\lambda \mapsto \alpha^2\lambda + \alpha\lambda^3$.

Claramente $g \notin (M_{10})_\infty$. Además, $h(\omega) = \infty \in X$, $h^2 = 1$, y

$$gh = (\omega, 0, \infty)(\alpha, \alpha^6, \alpha^3)(\alpha^2, \alpha^7, \alpha^5)$$

de orden 3. De manera que para satisfacer las condiciones del Teorema de Witt, basta ver que si $f \in (M_{10})_\infty$ entonces

$$hfh(\infty) = hf(\omega) = h(\omega) = \infty.$$

Por lo tanto $h(M_{10})_\infty h = (M_{10})_\infty$ si cada $hfh \in (M_{10})_\infty$.

Escribiendo $(M_{10})_\infty = A_\infty \cup B_\infty$, tenemos que $f = \alpha^{2i}\lambda + b$, o bien $f = \alpha^{2i+1}\lambda^3 + b$, con $i \geq 0$ y $b \in CG(9)$. Componiendo con $(\alpha^2\lambda + \alpha\lambda^3)$, tenemos que

$$\begin{aligned} hfh(\lambda) &= hf(\alpha^2\lambda + \alpha\lambda^3) \\ &= h(\alpha^{2i+2}\lambda + \alpha^{2i+1}\lambda^3 + b) \\ &= \alpha^2(\alpha^{2i+2}\lambda + \alpha^{2i+1}\lambda^3 + b) + \\ &\quad + \alpha(\alpha^{2i+1}\lambda + \alpha^{2i+1}\lambda^3 + b)^3 \\ &= \alpha^{2i+4}\lambda + \alpha^{2i+3}\lambda^3 + \alpha^2 b + \\ &\quad + \alpha^{6i+7}\lambda^3 + \alpha^{6i+4} + \alpha b^3 \\ &= (\alpha^{2i+3} + \alpha^{6i+7})\lambda^3 + (\alpha^{2i+4} + \alpha^{6i+4})\lambda + \alpha^2 b + \alpha b^3 \end{aligned}$$

Cuando i es par, el coeficiente de λ^3 es 0 y el de λ es $2\alpha^{2i+4}$. Puesto que $2 = -1 = \alpha^4$, tenemos que el coeficiente de λ es un cuadrado, y $hfh \in A_\infty$. Si i es impar, el coeficiente de λ es 0, y el de λ^3 es $2\alpha^{2i+3} = \alpha^{2i+7}$ que no es un cuadrado, y por lo tanto $hfh \in B_\infty$.

El segundo caso, i.e. $f(\lambda) = \alpha^{2i+1}\lambda^3 + b$ es similar, y calculando obtenemos que

$$hfh(\lambda) = \alpha^{2i+6}(1+\alpha^{4i})\lambda + \alpha^{2i+1}(1+\alpha^{4i+4})\lambda^3 + \alpha^2 b + \alpha b^3,$$

que se puede tratar de la misma forma que en el primer caso, dando como conclusión que $hfh \in (M_{10})_\infty$.

De manera que las hipótesis del Teorema de Witt se satisfacen, y $M_{11} = \langle M_{10}, h\rangle$ actúa nítidamente 4-transitivo en $\overline{X}$, y por lo tanto $|M_{11}| = 11\cdot 10\cdot 9\cdot 8 = 7920$.

□

El procedimiento se puede repetir una vez más, y obtenemos M_{12}.

TEOREMA 5.11

Existe un grupo nítidamente 5-transitivo M_{12}, de grado 12, y de orden $12\cdot 11\cdot 10\cdot 9\cdot 8 = 95040$, y tal que el estabilizador de un punto es M_{11}.

Demostración: Sabemos que M_{11} actúa nítidamente 4-transitivo en $Y = \{CG(9), \infty, \omega\}$; construiremos una extensión de M_{11} que actúe en $\overline{Y} = Y \cup \{\Omega\}$. Definimos, en la notación de Witt,

$$x = \omega$$
$$g = (\omega,\infty)(\alpha,\alpha^2)(\alpha^3,\alpha^7)(\alpha^5,\alpha^6)$$
$$h = (\omega,\Omega)(\alpha,\alpha^3)(\alpha^2,\alpha^6)(\alpha^5,\alpha^7).$$

(Nótese que la $g \in M_{11}$ es la h de la extensión pasada). Observemos que el factor $(\alpha,\alpha^3)(\alpha^2,\alpha^6)(\alpha^5,\alpha^7)$ de h se obtiene por la permutación de $CG(9)$ dada por $\lambda \mapsto \lambda^3$. Claramente $h(\Omega) = \omega \in Y$, y $g \notin (M_{11})_\omega = M_{10}$. Además $h^2 = 1$, y

$$gh = (\omega,\Omega,\infty)(\alpha,\alpha^7,\alpha^6)(\alpha^2,\alpha^5,\alpha^3)$$

de orden 3.

Para satisfacer la última condición del Teorema de Witt, notemos primero que si

$$f \in (M_{11})_\omega = M_{10} = A \cup B,$$

entonces hfh también fija ω. Por último, veamos que $hfh \in M_{11}$: Si

$$f(\lambda) = \frac{a\lambda + b}{c\lambda + d} \in A,$$

entonces

$$hfh(\lambda) = \frac{a^3\lambda + b^3}{c^3\lambda + d^3}$$

con determinante $a^3d^3 - b^3c^3 = (ad - bc)^3$, que es un cuadrado pues $ad - bc$ lo era. Un argumento similar prueba que $hfh \in B$ si $f \in B$. De manera que $hM_{10}h = M_{10}$, satisfaciendo las hipótesis de Witt.

Se sigue pues que $M_{12} = \langle M_{11}, h\rangle$ actúa nítidamente 5-transitivo en $\overline{Y}$, y por lo tanto tiene orden $|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040$.

□

VI. El Sistema de Steiner S(5,6,12)

En este capítulo introduciremos la noción de *Sistema de Steiner* y demostraremos algunas de las propiedades básicas de ellos. Posteriormente, llevaremos a cabo una discusión detallada del Sistema de Steiner $S(5,6,12)$, que guarda íntima relación con M_{12}, el grupo de Mathieu. La discusión del $S(5,6,12)$ está basada en el trabajo del Dr. Humberto Cárdenas Trigos y del Dr. Emilio Lluis Riera.

DEFINICIÓN

Sean $1 < t < k < v$ enteros. Un Sistema de Steiner de tipo $S(t,k,v)$ es un par ordenado (X, ST), donde X es un conjunto con v elementos, y ST es una familia de subconjuntos de X (llamados **bloques**), cada uno con k elementos, tales que cualesquiera t elementos de X están en uno y sólo un bloque.

Los bloques de los Sistemas de Steiner no tienen relación con los bloques de primitividad de un grupo. Se trata simplemente de una coincidencia en la terminología.

Dados los paramétros $1 < t < k < v$, el problema de determinar si existe un Sistema de Steiner $S(t,k,v)$ no está resuelto. Las desigualdades son estrictas para eliminar casos poco interesantes. Si $t = 1$, entonces todo punto está en un único bloque, y los bloques son una partición de X. Si $t = k$, todo subconjunto con t elementos es un bloque. Por último, si $k = v$, entonces hay sólo un bloque.

PROPOSICIÓN 6.1

Sea (X, ST) un Sistema de Steiner de tipo $S(t,k,v)$ con $t \geq 3$. Sea $x \in X$. Definimos $X' = X - \{x\}$, y ST' como la familia de todas las $\beta - \{x\}$ con $\beta \in ST$ que contiene a x. Entonces (X', ST') es un Sistema de Steiner de tipo $S(t-1, k-1, v-1)$.

Demostración: Claramente X' tiene $v-1$ elementos, los elementos de ST' tienen $k-1$ elementos cada uno. Por último, sean $\{x_1, \ldots, x_{t-1}\} \subset X'$. Por lo tanto existe un único $\beta \in ST$ tal que $\{x_1, \ldots, x_{t-1}, x\} \subset \beta$, y $\beta' = \beta - \{x\}$ dá el bloque deseado.

□

Al sistema (X', ST') de arriba se le llama una contracción de (X, ST).

Para abreviar, en vez de decir que (X, ST) es un Sistema de Steiner de tipo $S(t,v,k)$, diremos simplemente que (X, ST) es un $S(t,v,k)$.

Una manera común de contar elementos de un conjunto $S \subset A \times B$ es la siguiente. Para cada $a \in A$, se define

$$S(a,\ ) = \{b \in B \mid (a,b) \in S\};$$

y para cada $b \in B$

$$S(\ ,b) = \{a \in A \mid (a,b) \in S\}.$$

Claramente

$$\sum_{a \in A} |S(a,\ )| = \sum_{b \in B} |S(\ ,b)|,$$

pues ambos lados son iguales a $|S|$. Deducimos que si $\forall a \in A \quad |S(a,\ )| = m$ y si $\forall b \in B \ |S(\ ,b)| = n$, entonces

$$m|A| = n|B|.$$

TEOREMA 6.2

Sea (X, ST) un $S(t,k,v)$. Si b es el número de bloques, entonces

$$b = \frac{v(v-1)(v-2)\cdots(v-t+1)}{k(k-1)(k-2)\cdots(k-t+1)};$$

si r es el número de bloques que contienen a un punto $x \in X$, entonces r no depende de x y

$$r = \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}.$$

Demostración: Sea A la familia de todos los subconjuntos de t puntos (distintos) de X. Entonces $|A| = \binom{v}{t} = \frac{v(v-1)\cdots(v-t+1)}{t!}$. Sea ST el conjunto de bloques, y sea $S \subset A \times ST$ que consiste de todas las parejas $(\{x_1,\ldots,x_t\},\beta)$ con $\{x_1,\ldots,x_t\} \subset \beta$. Ya que cada conjunto de t elementos está en un único bloque, $|S(\{x_1,\ldots,x_t\},\ )| = 1$; ya que cada bloque β tiene k elementos, $|S(\ ,\beta)| = \binom{k}{t} = \frac{k(k-1)\cdots(k-t+1)}{t!}$. Tenemos entonces que

$$b\left(\frac{k!}{t!(k-t)!}\right) = \frac{v!}{t!(v-t)!}$$

de lo que obtenemos que

$$b = \frac{v!}{(v-t)!} \cdot \frac{(k-t)!}{k!} = \frac{v(v-1)(v-2)\cdots(v-t+1)}{k(k-1)(k-2)\cdots(k-t+1)}.$$

El número de bloques r que contienen a x es el número de bloques en la contracción (X', ST') al quitar a x. Vemos pues que r no depende de x, y como (X', ST') es de tipo $S(t-1, k-1, v-1)$, la fórmula se sigue de la primera.

□

¿Cuántos bloques del $S(t,k,v)$ contienen a un par de puntos x, y? El sistema contraído (X', ST') que se obtiene al quitar x es de tipo $S(t-1, k-1, v-1)$, y el número de bloques r' ahí que contienen a y es igual al número de bloques que contienen a $\{x, y\}$ en (X, ST). Podemos pues calcular r' como en el teorema anterior, y obtenemos:

$$r' = \frac{(v-2)(v-3)\cdots(v-t+1)}{(k-2)(k-3)\cdots(k-t+1)}.$$

De manera similar podemos contar el número de bloques de (X, ST) que contienen p puntos dados, con $1 \leq p < t$, y obtenemos que hay

$$\frac{(v-p)(v-p-1)\cdots(v-t+1)}{(k-p)(k-p-1)\cdots(k-t+1)}.$$

DEFINICIÓN

Sean (X, ST) y (X_1, ST_1) Sistemas de Steiner. Un isomorfismo de (X, ST) en (X_1, ST_1) es una biyección $f: X \to X_1$ tal que $\beta \in ST$ implica $f(\beta) \in ST_1$. Si $(X, ST) = (X_1, ST_1)$, un isomorfismo se llama un automorfismo.

PROPOSICIÓN 6.3

Todos los automorfismos de un Sistema de Steiner (X, ST) forman un subgrupo de S_X.

Demostración: El único detalle que falta es verificar si el inverso de un automorfismo h es un automorfismo. Pero S_X es finito, de manera que $h^{-1} = h^m$ para alguna $m > 0$, y es obvio que h^m es un automorfismo si h lo es.

□

TEOREMA 6.4

Si (X, ST) es un Sistema de Steiner, entonces su grupo de automorfismos actúa fielmente en ST.

Demostración: Sea ϕ un automorfismo de (X, ST) tal que $\phi(\beta) = \beta \ \forall \beta \in ST$. Debemos demostrar que $\phi = 1_X$.

Si $x \in X$, sea $s(x)$ la familia de bloques que contienen a x; de manera que $|s(x)| = r$. Ya que ϕ es un automorfismo, $\phi(s(x)) = s(\phi(x))$; puesto que ϕ fija todo bloque, $\phi(s(x)) = s(x)$. Por lo tanto $s(x) = s(\phi(x))$, y los bloques que contienen a x son los mismos bloques que contienen a $\phi(x)$. Si $x \neq \phi(x)$, los valores calculados arriba nos dan que

$$\frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)} = \frac{(v-2)\cdots(v-t+1)}{(k-2)\cdots(k-t+1)}$$

de manera que $v - 1 = k - 1$, lo cual es imposible pues $k < v$. De manera que $x = \phi(x)$, y $\phi = 1_X$.

□

Pasaremos ahora a la construcción de Sistemas de Steiner de tipo $S(5, 6, 12)$. Empezaremos definiendo algunas gráficas y dando sus propiedades, y posteriormente se establecerá la relación entre dichas gráficas y los $S(5, 6, 12)$.

Para un $S(5, 6, 12)$, el número de bloques debe ser 132. Esto se debe a que es igual al número de maneras de escoger 5 elementos de 12 dados, entre el número de maneras de elegir 5 de 6. Es decir,

$$\binom{12}{5} \Big/ \binom{6}{5} = \frac{12!}{6 \cdot 5!7!} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{6!} = \frac{95040}{720} = 132$$

Usando este mismo procedimiento, los siguientes resultados se establecen fácilmente:

PROPOSICIÓN 6.5

Sea A un subconjunto de X con $|A| = n$ Entonces el número q de bloques que contienen a A es

n:	5	4	3	2	1	0
q:	1	4	12	30	66	132

PROPOSICIÓN 6.6

Sea B un bloque fijo, y A un subconjunto de B con $|A| = n$. El número r de bloques B' tales que $B \cap B' = A$ es

n:	5	4	3	2	1	0
r:	1	3	2	3	0	1

PROPOSICIÓN 6.7

Si B es un bloque, entonces el número s de bloques con intersección de n elementos con B es

n:	5	4	3	2	1	0
s:	1	45	40	45	0	1

COROLARIO 6.8

El complemento de un bloque es un bloque.

Sea B un conjunto con 6 elementos. Definimos $G_1(B)$ como la gráfica cuyos vértices son los subconjuntos de B de 4 elementos, y $\{A, A'\}$ es una arista si y sólo si $|A \cap A'| = 3$.

Es fácil verificar que $G_1(B) \cong L(K_6)$, la gráfica de líneas de la gráfica completa de seis vértices.

$G_2(B)$ es la gráfica cuyos vértices son las 2,2,2 particiones de B. Las aristas son las parejas $\{P, P'\}$ tales que $P \cap P' = \emptyset$.

Notemos de paso que el número de vértices de $G_1(B)$ es $\binom{6}{4} = 15$, y el de $G_2(B)$ es $\frac{1}{3!}\binom{6}{2}\binom{4}{2}\binom{2}{2} = \frac{6\cdot5\cdot4\cdot3}{3\cdot2\cdot2\cdot2} = 15$ también.

Por otro lado, el número de aristas de $G_1(B)$ es el número de subconjuntos de 4 elementos de B con 3 elementos en común, i.e.

$$\binom{6}{3}\cdot\binom{3}{2} = \frac{6\cdot5\cdot4\cdot3\cdot2}{3\cdot2\cdot2} = 60.$$

En cuanto al número de aristas de $G_2(B)$, es igual al número de 2,2,2 particiones ajenas de B que se pueden hacer. Dada una 2,2,2 partición, hay ocho 2,2,2 particiones de B ajenas a ella. De manera que el número de aristas será igual a $\frac{15\cdot8}{2} = 60$ también.

$G_1'(B)$ denotará la gráfica complementaria de $G_1(B)$, y $G_2'(B)$ la de $G_2(B)$.

En una gráfica G, un triángulo son tres vértices, v_1, v_2, v_3, tales que $\{v_1, v_2\}$, $\{v_2, v_3\}$ y $\{v_3, v_1\}$ son aristas de G.

Denotaremos por BB el conjunto de subconjuntos $p \subset B$ con 2 elementos. Si S, S' es una 3,3 partición de B, entonces

$$S \times S' = \{p \in BB \mid p \cap S \text{ tiene un sólo elemento}\}$$
$$SS = \{p \in BB \mid p \subset S\}$$
$$S'S' = \{p \in BB \mid p \subset S'\}$$

El siguiente lema se utilizará a menudo más adelante. Las pruebas son triviales e inmediatas.

LEMA 6.9

Si S, S' es una 3,3 partición de B, entonces:

(i) La descomposición

$$BB = (S \times S') \cup SS \cup S'S'$$

es una partición de BB.

(ii) Si P es una 2,2,2 partición de B, entonces $P \subset S \times S'$, o interseca a $S \times S'$, SS y $S'S'$ en exactamente 1 elemento cada uno.

(iii) Si $P \cap (S \times S')$ tiene más de un elemento, entonces $P \subset S \times S'$.

(iv) Si $P, P', P'' \subset S \times S'$ es un triángulo en $G_2(B)$, entonces $S \times S' = P \cup P' \cup P''$.

Definimos ahora cuatro gráficas más:

$L_1(S, S')$ es la gráfica inducida en $G_1(B)$ por el conjunto de vértices A tales que $S \subset A$ o $S' \subset A$.

$L_2(S, S')$ es la gráfica inducida en $G_2(B)$ por el conjunto de vértices P tales que $P \subset S \times S'$.

$L_i'(S, S')$ denota la gráfica complementaria de $L_i(S, S')$, para $i = 1, 2$.

PROPOSICIÓN 6.10

Sea S, S' una 3,3 partición de B. Entonces las gráficas $L_i(S,S')$ (con $i=1,2$) tienen dos componentes conexas, cada una de ellas un triángulo.

Demostración: Podemos identificar, sin perder generalidad, a B con $\{1,2,3,4,5,6\}$, y a $S=\{1,2,3\}$, $S'=\{4,5,6\}$. De manera que los vértices de $L_1(S,S')$ son 1234, 1235, 1236, 1456, 2456 y 3456. Los tres primeros forman un triángulo ajeno al formado por los últimos tres.

Para $i=2$, tenemos a

$$S\times S'=\Big\{\{1,4\},\{1,5\},\{1,6\},\{2,4\},\{2,5\},\{2,6\},\{3,4\},\{3,5\},\{3,6\}\Big\}$$

de manera que los vértices son $\{1,4\}\{2,5\}\{3,6\}$, $\{1,5\}\{2,6\}\{3,4\}$, $\{1,6\}\{2,4\}\{3,5\}$, $\{1,4\},\{2,6\},\{3,5\}$, $\{1,6\}\{2,5\}\{3,4\}$, y $\{1,5\}\{2,4\}\{3,6\}$. Los primeros tres nuevamente forman un triángulo ajeno al formado por los últimos tres.

□

LEMA 6.11

Si $\{P,P'\}$ es una arista de $G_2(B)$, entonces existe una 3,3 partición S,S' de B tal que $\{P,P'\}\subset S\times S'$.

Demostración: Sea s_1 un elemento fijo de B. Sean s_1',s_2' tales que $P_1=\{s_1,s_1'\}\in P$ y $P_1'=\{s_1,s_2'\}\in P'$. Por lo tanto, $s_1\neq s_1'$, $s_1\neq s_2'$, y $s_1'\neq s_2'$. Sean s_2,s_3 con $P_2=\{s_2,s_2'\}\in P$, $P_2'=\{s_2',s_3\}\in P'$.

Por último, definimos $S=\{s_1,s_2,s_3\}$, y $S'=\{s_1',s_2',s_3'\}$. Ya que $P\cap P'=\emptyset$ por ser $\{P,P'\}$ una arista de $G_2(B)$, tenemos que

$$B-(P_1\cup P_2)\neq B-(P_1'\cup P_2')$$

y por lo tanto $s_2\neq s_3$. Además, podemos concluir que $P_1\cap P_2=\emptyset$ y $P_1'\cap P_2'=\emptyset$. Por lo tanto, $s_1'\neq s_2$, $s_2'\neq s_3$, y por construcción $P_1,P_2,P_1',P_2'\in S\times S'$. Por Lema 6.9*(iii)*, $P,P'\subset S\times S'$.

□

LEMA 6.12

Sea $\{P_1, P_2\}$ una arista de $G_2(B)$, y S, S' una 3,3 partición de B. Si $P_3 \in G_2(B)$ tiene un elemento en común tanto con P_1 como con P_2, entonces

$$P_1, P_2 \subset S \times S' \Longrightarrow P_3 \subset S \times S'.$$

Demostración: En primer lugar, P_1 y P_2 no tienen elementos en común, por ser una arista de $G_2(B)$. Entonces, el elemento en común de P_3 con cada una de ellas es distinto. Concluimos que P_3 tiene dos elementos que pertenecen a $S \times S'$, y con esto, por Lema 6.9, *(ii)* que $P_3 \subset S \times S'$.

□

PROPOSICIÓN 6.13

Sea $L \subset G_i(B)$ (para $i = 1, 2$) tal que la gráfica inducida en L está formada por dos componentes conexas, cada una de ellas un triángulo. Entonces existe S, S' una 3,3 partición de B tal que $L = L_i(S, S')$ (para $i = 1, 2$).

Demostración: Para $i = 1$, S es la intersección de los vértices de uno de los triángulos, y S' la del otro triángulo. Bastará ver que $S \cap S' = \emptyset$, pero si no fuera vacío necesariamente habría una arista entre los dos triángulos, de manera que tenemos una partición.

Para $i = 2$, sean P_1, P_2, P_3 y P_1', P_2', P_3' los dos triángulos de L, y sea S, S' una 3,3 partición de B tal que $P_1, P_2 \subset S \times S'$ (posible por Lema 6.11). Puesto que P_1', P_2', P_3' no son ajenos con P_1 ni con P_2 (si lo fueran habría una arista entre ellos), entonces se sigue del Lema 6.12 que $P_1', P_2', P_3' \subset S \times S'$. Como P_3 no es ajeno a P_1' ni a P_2', tenemos nuevamente por Lema 6.12 que $P_3 \subset S \times S'$, que es lo que se requería.

□

LEMA 6.14

Sean S_1, S_1' y S_2, S_2' dos 3,3 particiones de B, con $S_1 \cap S_2 = \{s\}$ y $S_1' \cap S_2' = \{s'\}$. Si P y P' son dos vértices de $G_2(B)$, tales que

$$P, P' \subset S_1 \times S_1' \qquad \text{y} \qquad P, P' \subset S_2 \times S_2'$$

entonces $\{s, s'\} \in P \cap P'$.

Demostración: Sea $\{s,t\} \in P$. Ya que $s \in S_1$ y $P \subset S_1 \times S_1'$, tenemos que $t \in S_1'$. Además, puesto que $s \in S_2$ y $P \subset S_2 \times S_2'$, tenemos también que $t \in S_2'$. Por lo tanto $t \in S_1' \cap S_2' = \{s'\}$, de manera que $t = s'$.

Análogamente, si $\{s,u\} \in P'$, ya que $P' \subset S_1 \times S_1'$ y $s \in S_1$, necesariamente $u \in S_1'$. Y como $P' \subset S_2 \times S_2'$, se sigue que $u \in S_2'$, y por lo tanto $u = s' = t$. En conclusión, $\{s,s'\} \in P \cap P'$.

□

PROPOSICIÓN 6.15

Si $\{v,v'\}$ es una arista de $G_i(B)$ (para $i = 1,2$), entonces existe una y sólo una 3,3 partición de B, denotada por S,S', tal que $v,v' \in L_i(S,S')$ (para $i = 1,2$).

Demostración: Si $i = 1$, la intersección $v \cap v'$ determina de manera única la partición, pues dicha intersección debe ser S o bien S'.

Si $i = 2$, por Lema 6.11 hay una 3,3 partición S,S' de B tal que $\{v,v'\} \subset S \times S'$; Si R,R' es otra 3,3 partición de B con la propiedad de que $\{v,v'\} \subset R \times R'$, entonces por Lema 6.14, como

$$v,v' \in S \times S' \qquad \text{y} \qquad v,v' \in R \times R'$$

entonces (sin perder generalidad podemos suponer que $S \cap R = \{s\}$ y $S' \cap R' = \{s'\}$) tenemos que $\{s,s'\} \in v \cap v'$. Pero la última intersección es vacía, pues $\{v,v'\}$ es una arista de $G_2(B)$, lo cual nos da una contradicción. Concluimos pues que S,S' es la única partición con la propiedad, terminando la demostración.

□

Sea S,S' una 3,3 partición de B. Denotamos por D_i (para $i = 1,2$) el conjunto de aristas de $L_i'(S,S')$. Definimos una función

$$T\colon D_i \dashrightarrow \Big(G_i(B) - L_i(S,S')\Big)$$

dada de la siguiente manera:

Para $i = 1$, si $\{A,A'\} \in D_1$, entonces $T(A,A') = B - (A \cap A')$.

Para $i=2$, si $\{P_1,P_2\}\in D_2$, sea $P_1\cap P_2=\{p\}$. Existe una y sólo una $P_3\in G_2(B)$ con $\{p\}\in P_3$ y $P_1\neq P_3\neq P_2$. Definimos pues $T(P_1,P_2)=P_3$.

Tenemos que si $\{v,v'\}\subset D_i$ (para $i=1,2$), entonces $\{v,v',T(v,v')\}$ es un triángulo en $G_i'(B)$. Para $i=1$, esto se debe a que v y v' tienen sólo 2 elementos en común, y $T(v,v')$ tiene sólo 2 elementos en común con cada una de ellas (los otros dos). Para $i=2$, pues los tres tienen intersección no vacía.

Notemos además que $L_i'(S,S')$ no puede tener triángulos, pues $L_i'(S,S')$ es isomorfa a la gráfica bipartita $K_{3,3}$, y una gráfica bipartita no tiene ciclos impares, y en particular no tiene triángulos. Tenemos pues, que necesariamente $T(v,v')\notin L_i'(S,S')$ (y por lo tanto, tampoco en $L_i(S,S')$).

LEMA 6.16

Sea S,S' una 3,3 partición de B. Si $A\in G_1(B)-L_1(S,S')$, entonces $A_1=B-(A\cap S)$ y $A_2=B-(A\cap S')$ son tales que $T(A_1,A_2)=A$.

Demostración: Sin perder generalidad, tenemos que $S=\{1,2,3\}$, $S'=\{4,5,6\}$, y $A=\{1,2,5,6\}$. Por lo tanto la A_1 construida es $\{3,4,5,6\}$ y la A_2 es igual a $\{1,2,3,4\}$. Entonces

$$T(A_1,A_2)=\{1,2,3,4,5,6\}-\Big(\{3,4,5,6\}\cap\{1,2,3,4\}\Big)=\{1,2,5,6\}=A.$$

□

LEMA 6.17

Sea S,S' una 3,3 partición de B. Si $P\in G_2(B)-L_2(S,S')$, entonces existen $\{P_1,P_2\}\in D_2$ tales que $T(P_1,P_2)=P$.

Demostración: Sea $P\in G_2(B)-L_2(S,S')$. Entonces por Lema 6.9 *(ii)*, $P=\{p_1,p_2,p_3\}$ con $p_1\in S\times S'$, $p_2\in SS$ y $p_3\in S'S'$.

Si $p_2=\{s_1,s_2\}$, $p_3=\{s_1',s_2'\}$ y definimos $p_2'=\{s_1,s_1'\}$, $p_3'=\{s_2,s_2'\}$, $p_2''=\{s_1,s_2'\}$, y $p_3''=\{s_2,s_1'\}$. Finalmente si definimos $P_1=\{p_1,p_2',p_3'\}$ y $P_2=\{p_1,p_2'',p_3''\}$ tenemos que $T(P_1,P_2)=P$.

□

LEMA 6.18

Sea S, S' una 3,3 partición de B. Entonces la función

$$T: D_i \longrightarrow G_i(B) - L_i(S, S')$$

es biyectiva (para $i = 1, 2$).

Demostración: Por Lemas 6.16 y 6.17, T es suprayectiva. Para la inyectividad, simplemente notemos que el número de aristas en $L_i'(S, S')$ es 9, que es el mismo número de vértices de $G_i(B) - L_i(S, S')$ (para $i = 1, 2$).

□

PROPOSICIÓN 6.19

Sea S, S' una 3,3 partición de B, y $\{A_1, A_2\}$ una arista de $G_1(B) - L_1(S, S')$. Entonces existen $\{A_1', A_1''\}$ y $\{A_1', A_2''\}$ aristas de $L_1'(S, S')$ tales que $T(A_1', A_1'') = A_1$ y $T(A_1', A_2'') = A_2$.

Demostración: Puesto que $\{A_1, A_2\} \notin L_1(S, S')$, $|A_1 \cap S| = |A_1 \cap S'| = 2$. Además, $|A_1 \cap A_2| = 3$ por ser arista de $G_1(B)$.

Sea $C = A_1 \cap A_2$, y supongamos que $|C \cap S| = 2$. Consideramos, por Lema 6.18, $B - (A_1 \cap S)$, $B - (A_1 \cap S')$, y $B - (A_2 \cap S), B - (A_2 \cap S')$.

Pero $B - (C \cap S) = B - (A_1 \cap S) = B - (A_2 \cap S)$, de manera que tomamos $A_1' = B - (C \cap S)$, $A_1'' = B - (A_1 \cap S')$ y $A_2'' = B - (A_2 \cap S')$.

Si $|C \cap S| = 1$, entonces $|C \cap S'| = 2$ y procedemos como arriba.

□

PROPOSICIÓN 6.20

Sea S, S' una 3,3 partición de B. Si $\{P, P'\}$ y $\{P', P''\}$ son dos aristas de $L_2'(S, S')$, entonces $\{T(P, P'), T(P', P'')\}$ es una arista de $G_2(B) - L_2(S, S')$.

Demostración: Sean $P = \{p_1, p_2, p_3\}$, $P' = \{p_1, p_2', p_3'\}$, y $P'' = \{p_1'', p_2', p_3''\}$. Entonces $T(P,P') = \{p_1, q_2, q_3\}$ y $T(P',P'') = \{q_1', p_2', q_3'\}$, donde $q_2, q_3; p_2, p_3$; y p_2', p_3' son las 3 particiones distintas de $B - p_1$; y $q_1', q_3'; p_1, p_3'$; y p_1'', p_3'' son las 3 particiones distintas de $B - p_2'$.

Tenemos que $p_1 \notin \{q_1', p_2', q_3'\}$, $p_2' \notin \{p_1, q_2, q_3\}$, y

$$q_2 \cap p_2' \neq \emptyset \neq q_3 \cap p_2'$$

Pero

$$q_1' \cap p_2' = \emptyset = q_3' \cap p_2'$$

Por lo tanto $T(P,P') \cap T(P',P'') = \emptyset$, y por lo tanto es arista de $G_2(B)$. Puesto que $T(P,P')$ y $T(P',P'')$ no están en $L_2(S,S')$, el resultado se sigue.

□

LEMA 6.21

Sean $A_1, A_2, A_3 \in G_1(B)$ tales que

$$|A_1 \cap A_2| = |A_2 \cap A_3| = |A_3 \cap A_1| = 2.$$

Entonces $A_1 = B - (A_2 \cap A_3)$.

Demostración: $|B| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_1| + |A_1 \cap A_2 \cap A_3|$. Por lo tanto $6 = 4 + 4 + 4 - 2 - 2 - 2 + |A_1 \cap A_2 \cap A_3|$. De ahí que $A_1 \cap (A_2 \cap A_3) = \emptyset$.

□

PROPOSICIÓN 6.22

Sean $P = \{p_1, p_2, p_3\}$, $P' = \{p_1, p_2', p_3'\}$ y $P'' = \{p_1'', p_2', p_3''\}$. Entonces $\{P, P''\}$ es arista en $G_2(B)$.

Demostración: Puesto que P' es partición y $P \neq P'$, tenemos que $|p_i \cap p_1| = 0$ y $|p_i' \cap p_2| = 1$ para $i = 2, 3$.

Para $j = 1, 3$, tenemos por la misma razón que $|p_j'' \cap p_1| = 1$. Por último, para $i = 2, 3$, y $j = 1, 3$, tenemos que $p_1 \neq p'i$, $p_i' \neq p_j'$, y $p_2 \neq p_i'$. De manera que $P \cap P'' = \emptyset$, y es una arista.

□

PROPOSICIÓN 6.23

Sea S, S' una 3,3 partición de B, y $\{v, v'\}$ una arista de $L_i'(S, S')$ (para $i = 1, 2$). Entonces son equivalentes:

(a) $\{v, v', v''\}$ es un triángulo en $G_i'(B)$

(b) $T(v, v') = v''$.

Demostración: (b) $\Rightarrow$ *(a)* Si $T(v, v') = v''$, entonces por construcción de T tenemos que $\{v, v', v''\}$ es un triángulo de $G_i'(B)$ (para $i = 1, 2$).

(a) $\Rightarrow$ *(b)* Para $i = 2$ es consecuencia inmediata del Lema 6.17. Para el caso de $i = 1$, como no son aristas de $G_1(B)$, tenemos que

$$|v \cap v'| = |v' \cap v''| = |v'' \cap v| = 2$$

Por lo tanto, (Lema 6.21) $v = B - (v' \cap v'')$, y por lo tanto $T(v, v') = v''$.

□

Consideremos ahora un Sistema de Steiner de tipo $S(5, 6, 12)$, y un bloque B de él, junto con su complemento B'. Denotemos por ST el conjunto de bloques del sistema. Puesto que tanto B como B' son conjuntos de seis elementos, podemos construir las gráficas $G_i(B)$ y $G_i(B')$, con $i = 1, 2$. Veremos como el Sistema de Steiner dado define un isomorfismo entre las gráficas $G_1(B)$ y $G_2(B')$.

PROPOSICIÓN 6.24

Si A es un vértice de $G_1(B)$ entonces hay exactamente 3 subconjuntos $p_1, p_2, p_3 \subset B'$ tales que $A \cup p_i \in ST$ para $i = 1, 2, 3$. Además, $\{p_1, p_2, p_3\}$ es vértice de $G_2(B')$.

Demostración: Ya se tiene que hay exactamente 3 bloques que intersecan a B en A, así que hay exactamente 3 subconjuntos de B' que acompletan A a un bloque distinto de B. Además, si $(A \cup p_i) \cap (A \cup p_j) \neq A$, entonces $i = j$, pues de lo contrario serían bloques distintos que tienen a cinco puntos en común, lo cual es imposible. De manera que $p_i \cap p_j \neq \emptyset \Rightarrow i = j$, y $\{p_1, p_2, p_3\}$ es una 2,2,2 partición de B'.

□

Definimos entonces una función entre los vértices de $G_1(B)$ y $G_2(B')$, que depende de ST y de B,

$$P_{ST,B}: G_1(B) \longrightarrow G_2(B')$$

dada por

$$P_{ST,B}(A) = \{p_1, p_2, p_3\}$$

con p_1, p_2, p_3 los únicos tres subconjuntos de B' que completan un bloque con A.

Si el bloque B queda sobrecntendido, entonces se escribirá simplemente P_{ST}, o incluso P, en vez de $P_{ST,B}$.

PROPOSICIÓN 6.25

La función $P_{ST}: G_1(B) \rightarrow G_2(B')$ definida en la Proposición 6.24, es un morfismo de gráficas.

Demostración: Sean $A_1, A_2 \in G_1(B)$ tales que $|A_1 \cap A_2| = 3$.

Sea $P(A_1) = \{p_1, p_2, p_3\}$ y $P(A_2) = \{p_1', p_2', p_3'\}$. Si $p_1 = p_j'$ para alguna j, entonces tanto $A_1 \cup p_1$ y $A_2 \cup p_j'$ tienen 5 elementos en común sin ser el mismo bloque, lo cual es imposible. De manera que $p_1 \neq p_j'$ para $j \in \{1,2,3\}$. Análogamente se prueba con p_2 y p_3, probando que $\{P(A_1), P(A_2)\}$ es una arista de $G_2(B')$.

□

PROPOSICIÓN 6.26

Sean $S \subset B$ y $T \subset B'$ conjuntos con 3 elementos cada uno, y tales que $S \cup T$ es un bloque. Entonces

$$\Big(A \in G_1(B)\Big) \wedge \Big(S \subset A\Big) \Longrightarrow P(A) \subset T \times T'$$

donde $T' = B' - T$.

Demostración: Si $P(A) \not\subset T \times T'$, entonces $\exists p \in P(A)$ con $p \subset T$. Por lo tanto, $A \cup p$ y $S \cup T$ tienen al menos cinco elementos en común, lo cual es imposible.

□

COROLARIO 6.27

Si S, S' es una 3,3 partición de B, y T, T' es un 3,3 partición de B', tales que $S \cup T$ es un bloque, entonces

$$P_{ST}(L_1(S,S')) = L_2(T,T').$$

Demostración: La igualdad es inmediata de las definiciones de $L_1(S,S')$, $L_2(T,T')$, y de que gracias a la Proposición 6.26, $A \in L_1(S,S') \Rightarrow P_{ST}(A) \in L_2(T,T')$.

□

PROPOSICIÓN 6.28

Si $S_1, S_2 \subset B$, $(S_1 \neq S_2)$ son conjuntos con 3 elementos tales que $S_1 \cup T$ y $S_2 \cup T$ son bloques, con $T \subset B'$, entonces S_1 y S_2 son complementarios.

Demostración: Consideremos la función $P_{ST,B'}: G_1(B') \to G_2(B)$. Sean $A, A' \in G_1(B')$ tales que $A \cap A' = T$. Por Proposición 6.25, $P(A)$ y $P(A')$ son ajenos, pues forman una arista de $G_2(B)$. Por Proposición 6.26, $P(A), P(A') \subset S_1 \times S_1'$, y $P(A), P(A') \subset S_2 \times S_2'$ (Con $S_i' = B - S_i$).

Por Lema 6.12, $\{S_1, S_1'\} = \{S_2, S_2'\}$, y como $S_1 \neq S_2$, tenemos que $S_1 = S_2'$, y se prueba el resultado.

□

PROPOSICIÓN 6.29

Si $L_1(S_1, S_1')$ y $L_1(S_2, S_2')$ no tienen aristas en común, entonces $P(L_1(S_1, S_1'))$ y $P(L_1(S_2, S_2'))$ no tienen aristas en común.

Demostración: Del Corolario 6.27, $P(L_1(S_i, S_i')) = L_2(T_i, T_i')$ $(i = 1, 2)$ para algunas 3,3 particiones de B', T_i, T_i', tales que $S_i \cup T_i$ es bloque.

Si $L_2(T_1, T_1')$ y $L_2(T_2, T_2')$ tienen una arista $\{P, P'\}$ en común, por la Proposición 6.15, $\{T_1, T_1'\} = \{T_2, T_2'\}$. Pero la Proposición 6.28 nos diría que $\{S_1, S_1'\} = \{S_2, S_2'\}$, y por lo tanto $L_1(S_1, S_1') = L_1(S_2, S_2')$.

□

COROLARIO 6.30

Si A_1, A_2 son vértices de $G_1(B)$, y $A_1 \cap A_2$ tiene dos elementos, entonces $P(A_1)$ y $P(A_2)$ son diferentes.

Demostración: Sea $A_3 \in G_1(B)$ tal que $\{A_1, A_3\}$, $\{A_2, A_3\}$ son aristas de $G_1(B)$. Entonces hay dos 3,3 particiones de B, distintas, $\{S_1, S_1'\}$ y $\{S_2, S_2'\}$ tales que

$$A_1, A_3 \in L_1(S_1, S_1') \qquad y \qquad A_2, A_3 \in L_1(S_2, S_2').$$

Por la Proposición 6.29, $P(A_1) \neq P(A_2)$, y además no son adyacentes.

□

PROPOSICIÓN 6.31

Sea ST el conjunto de bloques de un $S(5,6,12)$. Entonces el morfismo

$$P_{ST,B}: G_1(B) \longrightarrow G_2(B')$$

es un isomorfismo de gráficas.

Demostración: Por Proposición 6.25, es morfismo. Por la Proposición 6.30, manda vértices no adyacentes en vértices no adyacentes, y manda vértices adyacentes en vértices adyacentes. De manera que es inyectiva, y ambas con el mismo número de vértices y aristas. Por lo tanto es un isomorfismo de gráficas.

□

COROLARIO 6.32

Si hay un Sistema de Steiner de tipo $S(5,6,12)$, entonces hay un isomorfismo de gráficas entre $G_1(B)$ y $G_2(B)$.

Demostración: Claramente hay un isomorfismo de $G_2(B')$ en $G_2(B)$ definido mediante cualquier biyección de B' en B. El resultado se sigue ahora de la Proposición 6.31.

□

Pasaremos ahora a ver cómo un morfismo entre dos gráficas da lugar a un $S(5,6,12)$. Consideremos un conjunto M de doce elementos, y B, B' una 6,6 partición de M. Sea

$$P: G_1(B) \longrightarrow G_2(B')$$

un morfismo de gráficas biyectivo en los vértices. Tenemos pues que P es un isomorfismo de gráficas.

LEMA 6.33

Si S, S' es una 3,3 partición de B, entonces existe una, y sólo una 3,3 partición de B', T, T', tal que

$$P(L_1(S,S')) = L_2(T,T').$$

Demostración: Del hecho de que P sea un isomorfismo, se deduce que la gráfica inducida en $G_2(B')$ por $P(L_1(S,S'))$ tiene dos componentes conexas, cada una de ellas un triángulo. De la Proposición 6.13 tenemos que existe una partición T, T'' con la propiedad deseada.

Además sólo hay una, pues uno de los triángulos forza la partición por el Lema 6.12, y la función es inyectiva.

□

Dada la partición S, S' de B, denotemos por $Q_P(S,S')$ la única 3,3 partición de B', T, T', tal que $P(L_1(S,S')) = L_2(T,T')$. De esta definición obtenemos:

PROPOSICIÓN 6.34

La función

$$Q_P: \{3,3 \text{ particiones de } B\} \longrightarrow \{3,3 \text{ particiones de } B'\}$$

es una biyección.

Demostración: Puesto que está bien definida por el Lema 6.33, y que por la Proposición 6.13 es suprayectiva, basta probar que es inyectiva. Pero ya que P es un isomorfismo, distintas particiones dan lugar a distintas gráficas, y por lo tanto a su vez a distintas particiones de B'.

□

LEMA 6.35

Sea S, S' una 3,3 partición de B. Si A, A', A'' contienen a S y $Q_P(S, S') = \{T, T'\}$, entonces

$$T \times T' = P(A) \cup P(A') \cup P(A'').$$

Demostración: Puesto que A, A', A'' es uno de los triángulos de $L_1(S, S')$, $P(A)$, $P(A')$, $P(A'')$ es uno de los triángulos de $L_2(T, T')$. Por lo tanto

$$P(A), P(A'), P(A'') \in T \times T'$$

y de ahí que

$$P(A) \cup P(A') \cup P(A'') \subset T \times T'.$$

Además, son disjuntas dos a dos por formar un triángulo en $G_2(B')$, de manera que tienen nueve elementos distintos. Puesto que esa es la cardinalidad de $T \times T'$, tenemos la igualdad.

□

LEMA 6.36

Sea $b \in B$, y $R = \{A \in G_1(B) \mid b \notin A\}$. Entonces la familia $\{P(A) \mid A \in R\}$ es una partición de $B'B' = \{p' \subset B' \mid |p'| = 2\}$.

Demostración: Ya que si $|A \cap A'| = 3$, entonces $P(A)$ es disjunta de $P(A')$, tenemos que en efecto forman una partición, si es que cubren a todos. Como $|R| = 5$, y cada $P(A)$ tiene 3 elementos, en total tengo 15, que es precisamente la cardinalidad de $B'B'$, así que tengo una partición.

□

Ahora asociaremos al isomorfismo P dado una familia de subconjuntos de M, todos con 6 elementos, que llamaremos bloques. Denotaremos esa familia por $ST(B, P)$.

(i) B y B' son bloques.

(ii) Para cada $A \in G_1(B)$, si $P(A) = \{p_1, p_2, p_3\}$, entonces $A \cup p_1$, $A \cup p_2$, y $A \cup p_3$ son bloques.

(iii) El complemento en M de los bloques de *(ii)*.

(iv) Para cada 3,3 partición S, S' de B, sea $Q_P(S,S') = \{T,T'\}$. Entonces $S \cup T$, $S \cup T'$, $S' \cup T$ y $S' \cup T'$ son bloques.

Tenemos pues 2 bloques de tipo *(i)*. Tres bloques de tipo *(ii)* por cada $A \in G_1(B)$, para un total de 45. 45 bloques de tipo *(iii)*. Y cuatro por cada 3,3 partición de B, para un total de 40 de tipo *(iv)*.

En total, hemos definido 132 bloques en $ST(B,P)$.

TEOREMA 6.37

Sea M un conjunto con 12 elementos, B, B' una 6,6 partición de M, y

$$P: G_1(B) \longrightarrow G_2(B')$$

un isomorfismo de gráficas. Entonces M y la familia $ST(B,P)$ forman un Sistema de Steiner de tipo $S(5,6,12)$.

Demostración: Sea D un subconjunto de M con 5 elementos. Basta ver que existe un único elemento de $ST(B,P)$ que contenga a D. Sea $a = |D \cap B| = |C|$, y $b = |D \cap B'| = |C'|$. Analizaremos los casos de (a,b).

Caso 1) $(a,b) = (5,0)$. Entonces $D \subset B$, y por construcción de los bloques ningún otro tiene más de 4 en común con B, por lo tanto B es el único.

Caso 2) $(a,b) = (4,1)$. Consideremos $P(C) = \{p_1, p_2, p_3\}$. Los únicos bloques que contienen a C son B, $C \cup p_1$, $C \cup p_2$, y $C \cup p_3$. Puesto que $|C'| = 1$, $\exists i \in \{1,2,3\}$ tal que $C' \subset p_i$, de manera que $D \subset C \cup p_i$, y es el único.

Caso 3) $(a,b) = (3,2)$. El bloque debe de ser de tipo *(ii)* o de tipo *(iv)*. Sean A, A', A'' los tres vértices de $G_1(B)$ que contienen a C. Sea $\{T,T'\} = Q_P(C,C'')$ donde $C'' = B' - C'$.

Por Lema 6.9 tenemos que $T \times T' = P(A) \cup P(A') \cup P(A'')$. Por Lema 6.9, $C' \in P(A) \cup P(A') \cup P(A'') \cup T \cup T' \cup T'$, que es una partición de BB (pues C' tiene 2 elementos). Si $C' \in P(A) \cup P(A') \cup P(A'')$, entonces existe uno y sólo un bloque de tipo *(ii)* que contiene a D. Este bloque se obtiene fijándonos en cual de los 3 uniendos está, y tomando

el bloque correcto. Por ejemplo, si $C' \in P(A)$, entonces $D \subset A \cup p_1, A \cup p_2$, o $A \cup p_3$, donde $P(A) = \{p_1, p_2, p_3\}$.

Si $C' \notin P(A) \cup P(A') \cup P(A'')$, entonces $C' \in TT'UT'T'$. Como tanto CUT como CUT' son bloques, hay uno de ellos, y obviamente sólo uno de ellos, que contiene a D, y es de tipo *(iv)*.

Caso 4) $(a,b) = (2,3)$. Un bloque que contenga a D en este caso debe ser de tipo *(iii)* o de tipo *(iv)*. Sea $A = B - C$. Hay dos casos: $C' = B' - p$ para alguna $p \in P(A)$, o en el otro caso $P(A) \subset C \times C'$.

En el primer caso, tenemos que $C \cup C' \subset M - (A \cup p)$, de tipo *(iii)*, y claramente es el único.

En el segundo caso, tenemos que existe S, S' una 3,3 partición de B tal que $Q_P(S, S') = \{C', C''\}$. Por lo tanto $P(L_1(S, S')) = L_2(C', C'')$. De ahí que $A \in L_1(S, S')$, y por lo tanto $S \subset A$ o bien $S' \subset A$. Por lo tanto $C \cup C' \subset S \cup C'$, ó $C \cup C' \subset S' \cup C'$, bloque de tipo *(iv)*, y claramente el único.

Caso 5) $(a,b) = (1,4)$. De haber dicho bloque, debe ser de tipo *(iii)*. Por Lema 6.36, tenemos que

$$P\Big(\{A \mid A \subset B - C\}\Big)$$

es una partición de $B'B'$. De manera que $B' - C' \in P(A)$ para una y sólo una A de las $A \subset B - C$. Para dicha A, y sólo para esa, $A \cup (B' - C')$ es un bloque de tipo *(iii)*, y $C \cup C' \subset M - (A \cup (B' - C'))$.

Caso 6) $(a,b) = (0,5)$. El único bloque que contiene a D es B', pues es el único con cinco o más puntos en común con B'.

□

Hemos pues asocindo a cada morfismo de gráficas un $S(5,6,12)$. Teníamos también asociado a cada $S(5,6,12)$ un morfismo de gráficas. Veamos que dichas asociaciones son inversas una de la otra.

PROPOSICIÓN 6.38

Sea M un conjunto con doce elementos, B, B' una 6,6 partición de M, y

$$P: G_1(B) \longrightarrow G_2(B')$$

un morfismo de gráficas biyectivo en los vértices. Entonces

$$P_{ST(B,P),B} = P$$

Demostración: Claramente, la P' asociada a $ST(B,P),B$ es tal que

$$ST(B,P') = ST(B,P),$$

pues los bloques de tipo *(ii)* se definen a partir de P, y estos permiten definir P' que será igual a P.

□

PROPOSICIÓN 6.39

Si ST es la familia de bloques de un Sistema de Steiner de tipo $S(5,6,12)$, con $B \in ST$, entonces

$$ST(B, P_{ST,B}) = ST.$$

Demostración: Si S, S' es una 3,3 partición de B, por el Corolario 6.27 tenemos que

$$P_{ST,B}\Big(L_1(S,S')\Big) = L_2(T,T')$$

donde $S \cup T$, y $S \cup T'$ son bloques de ST.

Por la definición de los bloques de $ST(B, P_{ST,B})$, en el caso en que intersequen a B en tres puntos, tenemos que en efecto estos son bloques. Por lo mismo, sus complementos también son bloques de ST.

Claramente B y B' son bloques del sistema creado. Por último, la construcción de $P_{ST,B}$ garantiza que los bloques de tipo *(ii)* en $ST(B, P_{ST,B})$ son bloques de ST.

Puesto que ambos sistemas tienen 132 bloques, y hemos visto que

$$ST(B, P_{ST,B}) \subset ST$$

tenemos la igualdad.

□

Hemos pues establecido una biyección entre los isomorfismos de gráficas entre $G_1(B)$ y $G_2(B')$, y los Sistemas de Steiner de tipo $S(5,6,12)$ que contienen a B y a B' como bloques. Entonces, dado un conjunto M de doce elementos y una 6,6 partición B, B' de él, el número de isomorfismos de $G_1(B)$ en $G_2(B')$ es independiente de la elección de B, pues si C, C' es otra partición, biyecciones entre B y C, y entre B' y C' establecen isomorfismos de gráficas $G_1(C) \cong G_1(B)$ y $G_2(C') \cong G_2(B')$. Llamemos n a dicho número. De ahí que:

COROLARIO 6.40

Dado un conjunto M de doce elementos, el número de familias ST que definen un Sistema de Steiner $S(5,6,12)$ en M es $7 \times n$.

Demostración: Como ya se dijo, la correspondencia $(B, P) \mapsto ST(B, P)$ es suprayectiva, y $\forall B \in ST$, $P_{ST}(B)$ está en la imágen inversa de ST bajo dicha asignación.

Además, si la imágen de (B, P) es ST, entonces $B \in ST$ por la Proposición 6.39. De manera que

$$P = P_{ST(B,P),B} = P_{ST,B}.$$

Finalmente, el número de bloques de ST es 132, y el número de funciones n. Tenemos entonces que hay

$$\frac{\binom{12}{6} \cdot n}{132} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot n}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 12 \cdot 11} = 7 \times n$$

Sistemas de Steiner de tipo $S(5,6,12)$ en M.

□

Ahora, para establecer la existencia de un Sistema de Steiner de tipo $S(5,6,12)$, basta establecer un isomorfismo entre las gráficas dadas. Esto lo haremos a continuación.

Sea M un conjunto con doce elementos; B, B' una 6,6 partición de M; S, S' una 3,3 partición de B; y T, T' una 3,3 partición de B'.

PROPOSICIÓN 6.41

Dado un morfismo de gráficas

$$R: L_1(S,S') \longrightarrow L_2(T,T')$$

biyectivo en los vértices, existe un único isomorfismo de gráficas

$$P: G_1(B) \longrightarrow G_2(B')$$

que extiende a R.

Demostración: Por la Proposición 6.16, dado $A \in G_1(B) - L_1(S,S')$ tenemos que

$$\exists! A', A'' \in L_1(S,S')$$

tales que $T(A',A'') = A$. Consideremos $R(A'), R(A'') \in L_2(T,T')$, y sea

$$P = T(R(A'), R(A''))$$

.

Definamos $P(A) = P = T(R(A'), R(A''))$.

Supongamos que $\{A_1, A_2\}$ es una arista de $G_1(B) - L_1(S,S')$. Tomamos como en la Proposición 6.19 a aristas $\{A_1', A_1''\}$ y $\{A_1', A_2''\}$ en $L_1'(S,S')$ tales que $T(A_1', A_1'') = A_1$ y $T(A_1', A_2'') = A_2$.

Por lo tanto $T(R(A_1'), R(A_1'')) = P(A_1)$ y $T(R(A_1'), R(A_2'')) = P(A_2)$. Por propiedades de R, tenemos que $\{R(A_1'), R(A_1'')\}$ es una arista de $G_2'(B')$, lo mismo que $\{R(A_1'), R(A_2'')\}$.

Por Proposición 6.20, tenemos que $\{P(A_1), P(A_2)\}$ es una arista.

Por último, tomemos $\{A_1, A_2\}$ una arista de $G_1(B)$ que tiene un extremo en $L_1(S,S')$, y el otro fuera. Supongamos que $A_1 \in G_1(B) - L_1(S,S'2)$. Entonces A_1 es adyacente a A_2 y a otro vértice del mismo triángulo que A_2, y a dos vértices del otro triángulo de $L_1(S,S')$. Por lo tanto A_1 es la imágen bajo T de los dos vértices de $L_1(S,S')$ a los cuales no es adyacente. De ahí que bajo P es la imágen de los dos vértices en $L_2(T,T')$ que corresponden a los dos vértices a los que no es adyacente. Entonces tiene uno en común

con cada uno de ellos, y tiene un elemento de la 2,2,2 partición en $T \times T'$, uno en TT', y uno en $T'T'$. Por lo tanto, es adyacente a los otros dos vértices de cada triángulo, y en particular a $R(A_2)$. De manera que la adyacencia también se respeta en este caso.

Por lo tanto P es un morfismo que extiende a R.

Por la Proposición 6.15 que garantiza la unicidad de la partición (que ya está dada) cualquier otra función coincidirá con P fuera de $dom(R)$, y P es única.

□

COROLARIO 6.42

Las gráficas $G_1(B)$ y $G_2(B')$ son isomorfas. Por lo tanto la gráfica $G_2(B')$ también es la gráfica de líneas de K_6, y por lo tanto existen Sistema de Steiner de tipo $S(5,6,12)$.

Demostración: Basta dar M, B, B', S, S', T, T' y R como en la Proposición 6.41. Sean:

$$M = \{1,2,\ldots,12\}$$
$$B = \{1,2,\ldots,6\}$$
$$B' = \{7,8,\ldots,12\}$$
$$S = \{1,2,3\}$$
$$S' = \{4,5,6\}$$
$$T = \{7,8,9\}$$
$$T' = \{10,11,12\}$$

Por lo tanto, $L_1(S,S')$ esta formado por los triángulos $\{A_1, A_2, A_3\}$ y $\{A'_1, A'_2, A'_3\}$ donde

$$A_1 = \{1,2,3,4\} \quad A_2 = \{1,2,3,5\} \quad A_3 = \{1,2,3,6\}$$
$$A'_1 = \{1,4,5,6\} \quad A'_2 = \{2,4,5,6\} \quad A'_3 = \{3,4,5,6\}$$

$L_2(T,T')$ está formado por los triángulos $\{P_1,P_2,P_3\}$, y $\{P_1',P_2',P_3'\}$, donde

$$P_1=\Big\{\{7,10\},\{8,11\},\{9,12\}\Big\}$$
$$P_2=\Big\{\{7,11\},\{8,12\},\{9,10\}\Big\}$$
$$P_3=\Big\{\{7,12\},\{8,10\},\{9,11\}\Big\}$$
$$P_1'=\Big\{\{7,10\},\{8,12\},\{9,11\}\Big\}$$
$$P_2'=\Big\{\{7,12\},\{8,11\},\{9,10\}\Big\}$$
$$P_3'=\Big\{\{7,11\},\{8,10\},\{9,12\}\Big\}$$

Definimos por último a $R\colon L_1(S,S')\to L_2(T,T')$ por $R(A_i)=P_i; R(A_i')=P_i'$. Este isomorfismo se extiende para darnos los siguientes valores de P:

$$P(\{1234\})=\Big\{\{7,10\},\{8,11\},\{9,12\}\Big\}\quad P(\{1256\})=\Big\{\{7,9\},\{8,11\},\{10,12\}\Big\}$$
$$P(\{1235\})=\Big\{\{7,11\},\{8,12\},\{9,10\}\Big\}\quad P(\{1345\})=\Big\{\{7,9\},\{8,10\},\{11,12\}\Big\}$$
$$P(\{1236\})=\Big\{\{7,12\},\{8,10\},\{9,11\}\Big\}\quad P(\{1346\})=\Big\{\{7,11\},\{8,9\},\{10,12\}\Big\}$$
$$P(\{1245\})=\Big\{\{7,12\},\{8,9\},\{10,11\}\Big\}\quad P(\{1356\})=\Big\{\{7,8\},\{10,11\},\{9,12\}\Big\}$$
$$P(\{1246\})=\Big\{\{7,8\},\{11,12\},\{9,10\}\Big\}\quad P(\{1456\})=\Big\{\{7,10\},\{8,12\},\{9,11\}\Big\}$$

$$P(\{2345\})=\Big\{\{7,8\},\{10,12\},\{9,11\}\Big\}$$
$$P(\{2346\})=\Big\{\{7,9\},\{8,12\},\{10,11\}\Big\}$$
$$P(\{2356\})=\Big\{\{7,10\},\{8,9\},\{11,12\}\Big\}$$
$$P(\{2456\})=\Big\{\{7,12\},\{8,11\},\{9,10\}\Big\}$$
$$P(\{3456\})=\Big\{\{7,11\},\{8,10\},\{9,12\}\Big\}$$

□

PROPOSICIÓN 6.43

El número de isomorfismos de gráficas $P\colon G_1(B)\to G_2(B')$ es 6!.

Demostración: La Proposición 6.41 establece una correspondencia entre el conjunto de (S,R,T) y el conjunto de isomorfismos P.

Dado un isomorfismo $P: G_1(B) \to G_2(B')$, dando $\{T,T'\} = Q_P(S,S')$, tenemos que

$$\left(S, P|_{L_1(S,S')}, T\right)$$

es la imágen inversa bajo dicha correspondencia. De manera que la correspondencia es biyectiva. Y habrá tantos isomorfismos como elementos de (S,R,T).

Se elige una 3,3 partición de uno, y una 3,3 partición del otro, y una función entre las gráficas correspondientes.

Hay $\frac{1}{2}\binom{6}{3} = \frac{6\cdot5\cdot4}{3\cdot2\cdot2} = 10$ 3,3 particiones de B, y 10 de B'. Hay el siguiente número de isomorfismos:

6 maneras de elegir la imágen de un vértice distinguido y dos de extenderla a todo el triángulo, y 3! de extenderla a toda la gráfica, para un total de $6\cdot6\cdot2 = 72$. ¿Cuántos conté repetidamente? Una misma función se puede aplicar a cualquiera de las 10 particiones de B, tomando una y sólo una de las particiones de B' al mismo tiempo. De manera que se contaron 10 veces cada función.

Por lo tanto hay $\frac{10\cdot10\cdot72}{10} = 720 = 6!$ isomorfismos.

□

TEOREMA 6.44

Dado un conjunto M fijo con 12 elementos, el número de familias ST que definen un $S(5,6,12)$ en M es 7!.

Demostración: Por Corolario 6.40, el número de familias es $7 \times n$, donde n es el número de isomorfismos que hay. Puesto que $n = 6!$ por la Proposición 6.43, hay $7 \cdot 6! = 7!$ familias que definen un $S(5,6,12)$ en M.

□

Sea M un conjunto con 12 elementos, y B, B' una 6,6 partición de M. Identifiquemos como $S(B)$ el grupo de las permutaciones de elementos de B, y análogamente como $S(B')$ al grupo de permutaciones de elementos de B'.

Identifiquemos cada vértice de $G_1(B)$ con la permutación de los dos elementos de B que no están contenidos en el vértice. Con esta identificación, las aristas de $G_1(B)$ estarán entre parejas de transposiciones (a,b), (c,d) tal que el orden de $(a,b)(c,d)$ sea tres, i.e., $a=c$.

Definamos también $G_3(B')$ como la gráfica cuyos vértices son los productos $\pi = \tau_1\tau_2\tau_3$ de tres transposiciones ajenas de $S(B')$. Las aristas son las parejas $\{\pi,\pi'\}$ tales que $\pi\pi'$ sea de orden tres, i.e., tales que π y π' no tengan factores en común.

Tenemos que $G_3(B')$ es isomorfa a $G_2(B)$, identificando a cada 2,2,2 partición de B' con el producto de transposiciones correspondientes. Por ejemplo, identificando a

$$\{\{1,2\},\{3,4\},\{5,6\}\} \text{ con } (1,2)(3,4)(5,6)$$

En general, si $\sigma=(a_1,a_2,\ldots,a_k)$ es un ciclo, entonces $\{\sigma\}$ denotará el conjunto

$$\{a_1,a_2,\ldots,a_k\},$$

y su complemento en B (o en B') se denotará por $\overline{\{\sigma\}}$.

Puesto que $G_1(B)\cong G_2(B')\cong G_3(B')$, tenemos que $G_1(B)\cong G_3(B')$, y cada isomorfismo P entre ellos determina un Sistema de Steiner $S(5,6,12)$. El sistema que queda, ya traducido en términos de la nueva identificación que hemos hecho a los vértices de $G_1(B)$, y a los vértices de $G_3(B')$, es el siguiente:

(i) B y B' son bloques.

(ii) Por cada vértice $\alpha=(a,b)$ de $G_1(B)$, si $P(\alpha)=\tau_1\tau_2\tau_3$, entonces $\overline{\{\alpha\}}\cup\{\tau_i\}$ es bloque, para $i=1,2,3$.

(iii) Los complementos en M de los bloques de tipo *(ii)* son bloques.

(iv) Dada una arista $\{\alpha,\alpha'\}$ en $G_1(B)$, $\alpha=(a,b)$, y $\alpha'=(a,c)$, entonces $P(\alpha)P(\alpha')=\gamma\gamma'$ con $\gamma=(r,s,t)$ y $\gamma'=(r',s',t')$ 3-ciclos disjuntos. Entonces $\{\alpha\alpha'\}\cup\{\gamma\}$ y $\{\alpha\alpha'\}\cup\{\gamma'\}$ son bloques.

Consideremos ahora ST_1 y ST_2 las familias de bloques de dos Sistemas de Steiner de tipo $S(5,6,12)$ sobre M. Un isomorfismo

$$\sigma: ST_1 \longrightarrow ST_2$$

es una permutación σ de M tal que $\forall B \in ST_1 \ \sigma(B) \in ST_2$.

El grupo de automorfismos de un Sistema de Steiner de tipo $S(5,6,12)$ lo denotaremos por M'.

PROPOSICIÓN 6.45

Sean ST_1 y ST_2 familias de bloques de dos $S(5,6,12)$ sobre M, y sean B_1 y B_2 bloques de ST_1 y ST_2 respectivamente. Sean $P_1: G_1(B_1) \to G_3(B_1')$ y $P_2: G_1(B_2) \to G_3(B_2')$ isomorfismos de gráficas determinados por ST_1 y ST_2 respectivamente. Si σ es una permutación de M con $\sigma(B_1) = B_2$, entonces las siguientes dos condiciones son equivalentes:

(i) $\sigma: ST_1 \to ST_2$ es un isomorfismo de Sistemas de Steiner.

(ii) El siguiente diagrama conmuta:

$$\begin{array}{ccc} G_1(B_1) & \xrightarrow{P_1} & G_3(B_1') \\ {\scriptstyle G_1(\sigma)}\downarrow & & \downarrow{\scriptstyle G_3(\sigma)} \\ G_1(B_2) & \xrightarrow{P_2} & G_3(B_2') \end{array}$$

Demostración: (i) $\Rightarrow$ *(ii)* Sea $\alpha \in G_1(B_1)$. Denotemos $P_2(\sigma(\alpha)) = \tau_1'\tau_2'\tau_3'$. Entonces tenemos que $\overline{\{\sigma(\alpha)\}} \cup \{\tau_1'\}$, $\overline{\{\sigma(\alpha)\}} \cup \{\tau_2'\}$ y $\overline{\{\sigma(\alpha)\}} \cup \{\tau_3'\}$ son bloques de ST_2' que contienen a $\overline{\{\sigma(\alpha)\}}$.

Por otro lado, si $P_1(\alpha) = \tau_1\tau_2\tau_3$, entonces

$$\sigma\Big(\overline{\{\alpha\}} \cup \{\tau_1\}\Big)$$
$$\sigma\Big(\overline{\{\alpha\}} \cup \{\tau_2\}\Big)$$
$$\sigma\Big(\overline{\{\alpha\}} \cup \{\tau_3\}\Big)$$

son bloques. Por lo tanto tenemos los tres bloques de la forma $\overline{\{\sigma(\alpha)\}} \cup \{\tau_i'\}$ con $i = 1,2,3$, y los tres bloques de la forma $\overline{\{\sigma(\alpha)\}} \cup \{\sigma(\tau_i)\}$ con $i = 1,2,3$. Todos estos bloques contienen a $\overline{\{\sigma(\alpha)\}}$, que tiene 4 elementos.

Sólo hay cuatro bloques distintos que contienen a un subconjunto de 4 elementos dados. Además, sólo hay tres cuya intersección con $\overline{\{\sigma(\alpha)\}} \cup \{\tau_1'\}$ es exactamente $\overline{\{\sigma(\alpha)\}}$. Estos son:

$$\overline{\{\sigma(\alpha)\}} \cup \{\tau_2'\}$$
$$\overline{\{\sigma(\alpha)\}} \cup \{\tau_3'\}$$
$$B_2.$$

De manera que tenemos

$$\left\{\sigma(\tau_2), \sigma(\tau_3)\right\} \subset \left\{\tau_1', \tau_2', \tau_3'\right\}$$

Además, tenemos que $\{\tau_1\} \cap \{\tau_2\} = \emptyset$, $\{\tau_1\} \cap \{\tau_3\} = \emptyset$, y $\{\tau_1'\} \cap \{\tau_2'\} = \emptyset$, $\{\tau_1'\} \cap \{\tau_3'\} = \emptyset$. Supongamos sin perder generalidad de $\sigma(\tau_2) = \tau_2'$ y que $\sigma(\tau_3) = \tau_3'$. Tenemos entonces que

$$\begin{aligned}\sigma(\tau_1) &= B_2' - (\{\sigma(\tau_2)\} \cup \{\sigma(\tau_1)\}) \\ &= B_2' - (\{\tau_2'\} \cup \{\tau_3'\}) \\ &= \tau_1'\end{aligned}$$

De manera que

$$\left\{\sigma(\tau_1), \sigma(\tau_2), \sigma(\tau_3)\right\} = \left\{\tau_1', \tau_2', \tau_3'\right\}$$

y el diagrama conmuta.

(ii) $\Rightarrow$ *(i)* Supongamos que el diagrama conmuta. Usando la notación de arriba tenemos que

$$\left\{\tau_1', \tau_2', \tau_3'\right\} = \left\{\sigma(\tau_1), \sigma(\tau_2), \sigma(\tau_3)\right\}$$

Sea B un bloque en ST_1. Debemos demostrar que $\sigma(B)$ es un bloque en ST_2.

Si $B = B_1$ ó $B = B_1'$, entonces $\sigma(B) = B_2$ ó B_2' respectivamente, y por lo tanto es un bloque.

Si B es de tipo *(ii)*, entonces es de la forma $\overline{\{\alpha\}} \cup \{\tau_i\}$ para α y τ_i adecuada. Por lo tanto,

$$\sigma(B) = \overline{\{\sigma(\alpha)\}} \cup \sigma(\tau_i) = \overline{\{\sigma(\alpha)\}} \cup \tau_i'$$

Pero puesto que $\tau_i' \in P_2(\sigma(\alpha))$, tenemos que $\sigma(B)$ es un bloque en ST_2 de tipo *(ii)*.

Si B es de tipo *(iii)*, entonces $M - B$ es de tipo *(ii)*; por el caso anterior, tenemos que $\sigma(M - B)$ es un bloque en ST_2. Pero por ser σ una permutación, tenemos que $\sigma(M - B) = M - \sigma(B)$. Por lo tanto $\sigma(B)$ es el complemento de un bloque de tipo *(ii)*, y es un bloque (de tipo *(iii)*).

Supongamos por último que B es de tipo *(iv)*. Esto es, tenemos que $|B \cap B_1'| = 3$. Sean $\alpha, \alpha' \in G_1(B_1)$ con $\alpha\alpha' = B \cap B_1$; por lo tanto $\{\alpha, \alpha'\}$ es una arista de $G_1(B_1')$, y por lo tanto $P_1(\alpha)P_1(\alpha')$ se puede descomponer como el producto de dos 3-ciclos ajenos, i.e., $\exists \gamma, \gamma'$, $\{\gamma\} \cap \{\gamma'\} = \emptyset$ tales que $P_1(\alpha)P_2(\alpha') = \gamma\gamma'$.

Por lo tanto tenemos que $B = \{\alpha\alpha'\} \cup \{\gamma\}$ o bien $B = \{\alpha\alpha'\} \cup \{\gamma'\}$. Además, $\{\sigma(\alpha), \sigma(\alpha')\}$ es una arista, y por conmutatividad del diagrama tenemos que

$$\begin{aligned} P_2\Big(\sigma(\alpha)\Big)P_2\Big(\sigma(\alpha')\Big) &= \sigma\Big(P_1(\alpha)P_1(\alpha')\Big) \\ &= \sigma(\gamma\gamma') \\ &= \sigma(\gamma)\sigma(\gamma') \end{aligned}$$

Sólo hay dos bloques en ST_2 que intersecan a B_1 en exactamente $\sigma(\alpha)\sigma(\alpha')$, y esos bloque son exactamente

$$\Big\{\sigma(\alpha)\sigma(\alpha')\Big\} \cup \Big\{\sigma(\gamma)\Big\}$$
$$\Big\{\sigma(\alpha)\sigma(\alpha')\Big\} \cup \Big\{\sigma(\gamma')\Big\}$$

que satisfacen ambos el criterio para ser bloques de tipo *(iv)*.

En cualquier caso, tenemos que $\sigma(B)$ es un bloque, de lo que concluimos que σ es un isomorfismo de Sistemas de Steiner.

□

Si $\sigma \in S(B')$, entonces la conjugación por σ es un automorfismo de $G_3(B')$ que denotaremos por $G_3(\sigma)$. Esto se debe a que $\sigma(B') = B'$.

LEMA 6.46

Sea σ una permutación de B' tal que $G_3(\sigma)$ es la identidad. Entonces σ es la identidad.

Demostración: Supongamos sin perder generalidad que $B' = \{1,2,3,4,5,6\}$.

Sea $p = (1,2)(3,4)(5,6)$, $p' = (1,2)(3,5)(4,6)$. Por lo tanto,

$$\sigma(p) = \big(\sigma(1),\sigma(2)\big)\big(\sigma(3),\sigma(4)\big)\big(\sigma(5),\sigma(6)\big) = p$$

$$\sigma(p') = \big(\sigma(1),\sigma(2)\big)\big(\sigma(3),\sigma(5)\big)\big(\sigma(4),\sigma(6)\big) = p'$$

Por lo tanto $(\sigma(1),\sigma(2)) = (1,2)$, y tenemos que $\sigma(\{1,2\}) = \{1,2\}$. Consideremos ahora $p_2 = (1,3)(2,4)(5,6)$, y $p_2' = (1,3)(2,5)(4,6)$. Obtenemos entonces que $\sigma(\{1,3\}) = \{1,3\}$, y por lo tanto $\sigma(1) = 1$, $\sigma(2) = 2$, y $\sigma(3) = 3$. Proseguimos en forma análoga para obtener que $\sigma(4) = 4$, $\sigma(5) = 5$ y $\sigma(6) = 6$, concluyendo que $\sigma = 1_{S_6}$.

□

PROPOSICIÓN 6.47

La función $S_6 \longrightarrow Aut(G_3)$ es un isomorfismo.

Demostración: Tenemos que $G_1 \cong G_3$ como gráficas. Puesto que G_1 tiene 6! automorfismos, tenemos que $|Aut(G_3)| = 6!$. La correspondencia es inyectiva por el Lema 6.46, y el dominio y el contradominio tienen ambos 6! elementos, demostrándose que es isomorfismo.

□

PROPOSICIÓN 6.48

Sean ST_1 y ST_2 dos $S(5,6,12)$ sobre M, y sean B_1, B_2 bloques en ST_1 y ST_2 respectivamente; sea $\sigma: B_1 \to B_2$ una biyección. Entonces existe una única $\sigma': B_1' \to B_2'$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} G_1(B_1) & \xrightarrow{P_1} & G_3(B_1') \\ {\scriptstyle G_1(\sigma)}\downarrow & & \downarrow{\scriptstyle G_3(\sigma')} \\ G_1(B_2) & \xrightarrow{P_2} & G_3(B_2') \end{array}$$

Demostración: $P_2 \circ G_1(\sigma) \circ P_1^{-1}$ es un isomorfismo de $G_3(B_1')$ en $G_3(B_2')$. Por la Proposición 6.47, tenemos que $\exists \sigma' \in S_6$ tal que

$$G_3(\sigma') = P_2 \circ G_1(\sigma) \circ P_1^{-1}$$

y claramente hace conmutativo al diagrama. Puesto que la correspondencia era un isomorfismo, la σ' es única.

□

TEOREMA 6.49

Salvo isomorfismos, existe un único Sistema de Steiner de tipo $S(5,6,12)$.

Demostración: Todo Sistema de Steiner de tipo $S(5,6,12)$ se puede pensar sobre el mismo conjunto M.

Todo Sistema de Steiner de tipo $S(5,6,12)$ proviene de un isomorfismo de gráficas

$$G_1(B_1) \xrightarrow{P_1} G_3(B_1').$$

Dados dos isomorfismos

$$G_1(B_1) \xrightarrow{P_1} G_3(B_1'),$$

$$y \quad G_1(B_2) \xrightarrow{P_2} G_3(B_2')$$

y dada una biyección τ de B_1 en B_2, hay una σ' de B_1' en B_2' que hace conmutativo el diagrama por la Proposición 6.45. Considerando la permutación $\tau \cup \sigma'$, tenemos que el siguiente diagrama

$$\begin{array}{ccc} G_1(B_1) & \xrightarrow{P_1} & G_3(B_1') \\ {\scriptstyle G_1(\tau\cup\sigma')}\downarrow & & \downarrow{\scriptstyle G_3(\tau\cup\sigma')} \\ G_1(B_2) & \xrightarrow{P_2} & G_3(B_2') \end{array}$$

conmuta. Por el Lema 6.46, $\tau \cup \sigma'$ es un isomorfismo entre los dos $S(5,6,12)$ dados.

□

Esto termina nuestra discusión del Sistema de Steiner de tipo $S(5,6,12)$. En el capítulo siguiente estableceremos la relación que guarda con el Grupo de Mathieu.

VII. Construcción de Cárdenas–Lluis

Este capítulo consta de dos parte. En la primera, analizaremos la relación entre el Sistema de Steiner de tipo $S(5,6,12)$ y el Grupo de Mathieu M_{12}. De esa relación se obtendrán algunos conjuntos de generadores, una vez dado el grupo. En la segunda parte, se dará un método para obtener un conjunto de permutaciones que generan a M_{12}. Ambas partes están basadas en el trabajo del Dr. Humberto Cárdenas Trigos, y del Dr. Emilio Lluis Riera.

Consideremos un Sistema de Steiner de tipo $S(5,6,12)$ sobre el conjunto $M = \{1,\ldots,12\}$. Llamemos al grupo de sus automorfismos M'. Puesto que el $S(5,6,12)$ es único salvo isomorfismos, el grupo M' queda bien determinado salvo isomorfismos.

TEOREMA 7.1

M' es nítidamente 5-transitivo.

Demostración: Sean $x_1,x_2,x_3,x_4,x_5 \in M$ distintos entre sí, y $y_1,y_2,y_3,y_4,y_5 \in M$ distintos entre sí. Hay que exhibir un elemento $\sigma \in M'$ tal que $\sigma(x_i) = y_i$ para $i = 1,\ldots,5$.

Denotemos por $A = \{x_1,\ldots,x_5\}$, y sea $B \in ST$ el único bloque que contiene a A, digamos $B = A \cup \{z\}$. Sea B_1 el único bloque que contiene a $A_1 = \{y_1 \ldots, y_5\}$, digamos $B_1 = A_1 \cup \{z_1\}$.

Construyamos la σ en cuestión. Claramente pedimos que $\sigma(x_i) = y_i$, y además pedimos $\sigma(z) = z_1$. Tenemos pues que $\sigma(B) = B_1$.

Por Proposición 6.48, tenemos que existe una única $\sigma' : B' \to B_1'$ (donde $B' = M - B$, y $B_1' = M - B_1$) que hace conmutativo el diagrama correspondiente:

$$\begin{array}{ccc} G_1(B) & \xrightarrow{P_1} & G_3(B') \\ {\scriptstyle G_1(\sigma)}\downarrow & & \downarrow{\scriptstyle G_3(\sigma')} \\ G_1(B_1') & \xrightarrow{P_1'} & G_3(B_1') \end{array}$$

donde P_1 y P_1' son isomorfismos entre las gráficas determinados por el Sistema de Steiner con el que comenzamos.

Tomemos $\rho \in S_{12}$ de tal forma que $\rho|_B = \sigma$ y $\rho|_{B'} = \sigma'$. Por Proposición 6.45, puesto que el diagrama conmuta tenemos que ρ es un automorfismo del Sistema de Steiner, y por lo tanto $\rho \in M'$.

Tenemos pues que M' es 5-transitivo.

Sea $\tau \in M'$ tal que $\tau(A) = \sigma(A)$. Como $\tau \in M'$, tenemos que necesariamente $\tau(B) = B_1$ y por lo tanto $\tau(z) = z_1$.

Entonces tenemos que $\tau' = \tau|_B = \sigma$, y como la Proposición 6.48 garantiza que la manera de completarla a todo M es única, tenemos que $\tau|_{B'} = \sigma'$, de manera que $\tau = \sigma$. Por lo tanto σ es la única que manda A en A_1, y la acción es nítida.

En conclusión, M' es nítidamente 5-transitivo sobre M.

□

Puesto que ya tenemos clasificados a todos los grupos nítidamente 5-transitivos, tenemos de hecho ya clasificado a M'. Notemos simplemente que la acción de M' es sobre un conjunto con doce elementos, para concluir que

COROLARIO 7.2

$M' \cong M_{12}$, el Grupo de Mathieu de grado 12.

COROLARIO 7.3

El grupo de automorfismos del Sistema de Steiner de tipo $S(5, 6, 12)$ es el grupo de Mathieu de grado 12.

Convenimos pues es denotar por M_{12} al grupo de automorfismos de un $S(5, 6, 12)$, pues debe ser isomorfo al grupo de Mathieu.

Procederemos ahora en sentido inverso. Dado un grupo nítidamente 5- transitivo de grado 12 (y por lo tanto isomorfo a M_{12}), definiremos un sistema de bloques asociado a él, que se probará después es un $S(5, 6, 12)$.

Sea $M \subset S_{12}$ un grupo nítidamente 5-transitivo. Las letras $\{1, 2, \ldots, 12\}$ las denominaremos puntos. Notemos que $M \cong M_{12}$.

LEMA 7.4

Si $\sigma = (1)(2)(3)(4)(5,6)\cdots$ es un elemento de M, y $\{a,b,c,d,e,f\} = \{1,2,3,4,5,6\}$, entonces $(a)(b)(c)(d)(e,f)\cdots$ también es un elemento de M.

Demostración: Tomemos $\rho \in M$ con $\rho = (1,2)(3)(5,6)\cdots$. Tenemos que ρ es de orden 2. Por lo tanto

$$\rho\sigma\rho = (2)(1)(3)(x)(6,5)\cdots$$

donde $x = \rho(4)$. Ya que $\rho\sigma\rho$ coincide en 5 elementos con σ, tenemos que $\rho\sigma\rho = \sigma$ y por lo tanto $\rho(4) = 4$. Tenemos pues que

$$\rho\sigma = (1,2)(3)(4)(5)(6)\cdots \in M$$

De manera análoga obtenemos el resultado para los 6 subconjuntos de dos elementos de $\{a,b,c,d,e,f\}$ ajenos a $\{5,6\}$, multiplicando por la ρ adecuada. Tomando ahora a $\sigma' = \rho\sigma$ lo probamos para los ajenos de $\{1,2\}$, y así sucesivamente hasta cubrir todos los casos.

□

DEFINICIÓN

Un Bloque en M es un conjunto $\{a,b,c,d,e,f\}$ tal que $(a)(b)(c)(d)(e,f)\cdots \in M$.

Debido al Lema 7.4, el concepto de Bloque está bien definido.

$M(a,b,c,d)$ denotará el estabilizador de a,b,c,d en M.

Notemos que puesto que $M \cong M_{12}$, tenemos ya información sobre su estructura, y la de $M(a,b,c,d)$ para cualesquiera cuatro puntos a,b,c,d. En primer lugar, $M(a,b,c,d) \cong Q$ el grupo de los cuaternios. En particular, $M(a,b,c,d)$ tendrá sólo un elemento de orden 2. También tenemos que es regular (i.e. nítidamente 1- transitivo). Tenemos también que un elemento de orden 2 que fija al menos un elemento debe fijar cuatro, y que un elemento que fije exactamente tres puntos debe ser de orden 3.

TEOREMA 7.5

La familia de bloques de M definidos arriba forman un Sistema de Steiner de tipo $S(5,6,12)$ sobre el conjunto de puntos.

Demostración: Sea $X = \{a, b, c, d, e\} \subset \{1, 2 \ldots, 12\}$ con 5 elementos.

Sea $\sigma \in M$ tal que $\sigma = (a)(b)(c)(d, e)\cdots$. Por lo tanto σ es de orden 2, y fijará algún otra letra, digamos f. Entonces

$$\sigma = (a)(b)(c)(f)(d, e)\cdots$$

Entonces $\{a, b, c, d, e, f\}$ es un bloque. Si $B' = \{a, b, c, d, e, g\}$ es también un bloque, entonces

$$(a)(b)(c)(d)(e, g) \in M$$

Como tenemos también a $(a)(b)(c)(d)(e, f)\cdots$ en M, ambos de orden 2 y elementos de $M(a, b, c, d)$. Puesto que $M(a, b, c, d) \cong Q$ tiene sólo un elemento de orden dos, y tenemos que ambos son iguales y $f = g$. Entonces $B' = B$, y el bloque es el único que contiene a X. Tenemos pues que forman un $S(5, 6, 12)$.

□

Denotemos al $S(5, 6, 12)$ asociado a M por $ST(M)$.

LEMA 7.6

$M \subset Aut\Big(ST(M)\Big)$.

Demostración: Sea $B \in ST(M)$, $\sigma \in M$.

Si $B = \{a, b, c, d, e, f\}$, entonces $(a)(b)(c)(d)(e, f)\cdots \in M$. Por lo tanto

$$(\sigma(a))\,(\sigma(b))\,(\sigma(c))\,(\sigma(d))\,(\sigma(e), \sigma(f))\cdots \in M$$

Por lo tanto,

$$\{\sigma(a), \sigma(b), \sigma(c), \sigma(d), \sigma(e), \sigma(f)\} \in ST(M)$$

y por lo tanto $\sigma \in Aut\,(ST(M))$.

□

De esto deducimos, por supuesto, que de hecho $M = Aut(ST(M))$, pues tienen la misma cardinalidad.

LEMA 7.7

Si $\sigma \neq 1$ y $\sigma \in M$, entonces existe $\rho \in M$ tal que $\sigma\rho$ tiene más puntos fijos que σ.

Observación. En caso de que σ tenga 4 puntos fijos, ρ será σ^{-1} necesariamente. Si σ tiene menos de cuatro puntos fijos, $\sigma\rho$ tendrá más puntos fijos que σ, pero sin ser la identidad.

Demostración: Sea $F(\sigma)$ el conjunto de puntos fijos de σ, y sea $F(\sigma) \subset \{a,b,c,d\}$.

Sean e, f tales que $\sigma(e) = f$, y $e, f \notin \{a,b,c,d\}$.

Sea $\rho \in M(a,b,c,d)$ con $\rho(f) = e$. Entonces $\rho \neq \sigma^{-1}$ si σ no tiene cuatro puntos fijos, pues entonces $\sigma \notin M(a,b,c,d)$.

Pero $\sigma\rho(f) = \sigma(e) = f$, y $\sigma\rho|_{F(\sigma)}$ es la identidad, de manera que $\sigma\rho$ fija más elementos que σ. Si σ no fija cuatro elementos, $\sigma\rho$ no es la identidad.

□

TEOREMA 7.8

El conjunto

$$\bigcup_{\substack{\{a,b,c,d\}\subset\{1,\ldots,12\}\\ |\{a,b,c,d\}|=4}} M(a,b,c,d)$$

genera a M.

Demostración: Dado $a \in M^*$, $\exists \rho \in M$ tal que ρa fija exactamente 4 puntos. Por lo tanto, ρa está en la unión dada arriba.

Además, por construcción, $\exists x,y,z,w \in \{1,\ldots,12\}$ tales que $\rho \in M(x,y,z,w)$ (ver Lema 7.7).

Por lo tanto $\rho a \in \langle \bigcup M(a,b,c,d) \rangle$. Como $\rho \in \langle \bigcup M(a,b,c,d) \rangle$, entonces también está su inverso, y tenemos que

$$\rho^{-1}(\rho a) = a \in \left\langle \bigcup M(a,b,c,d) \right\rangle$$

Por lo tanto $M \subset \langle \bigcup M(a,b,c,d) \rangle \subset M$, y tenemos la igualdad.

□

De aquí podemos también concluir que $M < A_{12}$ (aunque este resultado ya lo teníamos por la construcción de Hall), pues cada $M(a,b,c,d)$ está formado de permutaciones pares, y ellas generan a M.

PROPOSICIÓN 7.9

Si $\gamma: B_1 \to B_2$ es una biyección entre bloques B_1 y B_2 de $ST(M)$, entonces $\exists! \sigma \in M$ tal que $\sigma|_{B_1} = \gamma$.

Demostración: Sea X un conjunto con 5 elementos de $B_1 = \{a, b, c, d, e, f\}$, y $\tau = (a)(b)(c)(d)(e, f) \cdots \in M$.

Sea $\sigma \in M$ tal que $\sigma|_X = \gamma|_X$ (lo cual es posible pues es 5-transitivo). Tal σ es única.

$$\sigma\tau\sigma^{-1} = \Big(\sigma(a)\Big)\Big(\sigma(b)\Big)\Big(\sigma(c)\Big)\Big(\sigma(d)\Big)\Big(\sigma(e), \sigma(f)\Big)\cdots$$

y $\sigma(B_1) = \{\sigma(a), \sigma(b), \sigma(c), \sigma(d), \sigma(e), \sigma(f)\}$ es un bloque de $ST(M)$. Puesto que contiene a $\gamma(X)$, tenemos que $\sigma(B_1) = \gamma(B_1)$ y es única por construcción.

□

Sea B un bloque de $ST(M)$, y $B' = \{1, \ldots, 12\} - B$ su complemento. Definimos una función

$$P: S(B) \longrightarrow S(B')$$

como sigue: dado $\beta \in S(B)$, $\exists! \sigma \in M$ tal que $\sigma|_B = \beta$. Definimos entonces $P(\beta) = \sigma|_{B'}$.

Si $\gamma: B_1 \to B_2$ es una biyección de B_1 en B_2, denotaremos por $S(\gamma): S(B_1) \to S(B_2)$ el homomorfismo dado por $S(\gamma)(\beta) = \gamma\beta\gamma^{-1}$.

PROPOSICIÓN 7.10

(i) $P: S(B) \to S(B')$ es un isomorfismo.

(ii) Sean B_1 y B_2 bloques de $ST(M)$, y B_1', B_2' sus complementos en $\{1, \ldots, 12\}$. Si $\sigma \in M$ es tal que $\sigma(B_1) = B_2$, y $\gamma = \sigma|_{B_1}$, $\gamma' = \sigma|_{B_1'}$, entonces el siguiente diagrama conmuta

$$\begin{array}{ccc} S(B_1) & \xrightarrow{S(\gamma)} & S(B_2) \\ P_1 \downarrow & & \downarrow P_2 \\ S(B_1') & \xrightarrow{S(\gamma')} & S(B_2') \end{array}$$

(iii) $P(G_1(B)) = G_2(B')$ y $P(G_2(B)) = G_1(B')$

Demostración: *(i)* Claramente es inyectiva, y por lo tanto es biyectiva. Si $\beta, \delta \in S(B)$, entonces $\exists! \sigma, \tau$ tales que $\sigma|_B = \beta$, $\tau|_B = \delta$, y por lo tanto $\tau \circ \sigma|_B = \delta \circ \beta$, y es la única. Por lo tanto es un isomorfismo.

(ii) Sea $\varphi \in S(B_1)$. Por lo tanto $\exists! \delta \in M$ tal que $\delta|_{B_1} = \varphi$. Por lo tanto $P_1(\varphi) = \delta|_{B_1'}$.

Tenemos pues que

$$S(\gamma)(P_1(\varphi)) = S(\gamma)(\delta|_{B_1'}) = \gamma\delta|_{B_1'}\gamma^{-1}$$

y por lo tanto $S(\gamma)(\varphi) = \gamma\varphi\gamma^{-1}$. Entonces la $\eta \in M$ tal que $\eta|_{B_2} = \gamma\varphi\gamma^{-1}$ es $\eta = \gamma\delta\gamma^{-1}$. Tenemos entonces que

$$P_2\Big(S(\gamma)(\varphi)\Big) = P_2(\gamma\varphi\gamma^{-1}) = \gamma\delta|_{B_1}\gamma^{-1}$$

y el diagrama conmuta.

(iii) Si $\alpha = (a, b) \in G_1(B)$, entonces la $\sigma \in M$ para la P es de orden 2 y es única. Entonces $P(\alpha) \in G_3(B')$.

Si $\alpha = (a, b), \alpha' = (a, c)$, entonces las $P(\alpha)$ y $P(\alpha')$ son ajenas, o de lo contrario coinciden en las tres letras fijas de B, y la permutación que tienen en común, de manera que coinciden en 5 letras, y por lo tanto son iguales. Pero ya que P es isomorfismo, manda distintas en distintas. Tenemos pues que $P(\alpha)$ es ajena de $P(\alpha')$, y P manda aristas en aristas.

Puesto que es biyectivo en los vértices, $P(G_1(B)) = G_3(B')$.

Notemos que, abusando un poco de la notación, P es su propia inversa (tomando la P' asociada a la asignación inversa $B' \to B$). De manera que $P(G_1(B)) = G_3(B') \Rightarrow P(P(G_1(B))) = P(G_3(B')) \Rightarrow G(B) = P(G_3(B'))$, y tenemos que $P(G_3(B)) = G_1(B)$.

□

COROLARIO 7.11

Si $\tau = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12) \in M$, entonces $\{1,2,3,4,5,6\}$ no es bloque de $ST(M)$.

Demostración: Si $\{1,2,3,4,5,6\}$ es bloque, entonces

$$P\Big((1,2)(3,4)(5,6)\Big) = (7,8)(9,10)(11,12)$$

pues $\tau \in M$ y por Proposición 7.10*(iii)* $\exists a, b \in \{1,\ldots,12\}$ tal que

$$P\Big((a,b)\Big) = (7,8)(9,10)(11,12).$$

Pero esto es una contradicción, pues P es isomorfismo.

□

Del inciso *(iii)* de la Proposición 7.10 se sigue el siguiente resultado, aunque ya lo conocíamos por conteo:

COROLARIO 7.12

Si B es un bloque de $ST(M)$, entonces $B' = \{1,\ldots,12\} - B$ también es un bloque.

Denotemos ahora por $T \subset M$ el conjunto de los elementos de orden 2 que fijan al menos un punto. Tenemos pues que cada elemento de T fija exactamente 4 puntos.

PROPOSICIÓN 7.13

(i) El conjunto T genera a M.

(ii) Los elementos de T son conjugados 2 a 2.

Demostración: (i) Basta ver que los elementos de T generan al conjunto de elementos de orden 4 que fijan 4 puntos, pues entonces generan a los $M(a,b,c,d)$ (que están formados por la identidad, 6 elementos de orden 4 que fijan cuatro letras, y uno de orden 2), y por lo tanto a todo M.

Sea $\sigma = (1)(2)(3)(4)(5,6,7,8)\cdots$ un tal elemento. Consideremos a los siguientes tres elementos de T:

$$\tau_1 = (4)(5,6)(7)(8)\cdots$$

$$\tau_2 = (4)(5)(6,7)(8)\cdots$$

$$\tau_3 = (4)(5)(6)(7,8)\cdots$$

Entonces $\tau_1\tau_2\tau_3 = (4)(5,6,7,8)\cdots$, y que coincide con σ en 5 puntos. Por lo tanto, $\sigma = \tau_1\tau_2\tau_3$, y T genera a los $M(a,b,c,d)$, y por lo tanto a todo M.

(ii) Sean $\sigma = (1)(2)(3)(4)(5,6)\cdots$ y $\tau = (a)(b)(c)(d)(e,f)\cdots$ elementos de T. Sea $\rho \in M$ tal que

$$\rho(1) = a; \quad \rho(2) = b; \quad \rho(3) = c; \quad \rho(5) = e; \quad \rho(6) = f$$

entonces

$$\rho\sigma\rho^{-1} = (a)(b)(c)(\rho(4))(e,f).$$

De ahí que $\rho(4) = d$, y σ y τ son conjugados.

□

Probaremos ahora que M (y por lo tanto M_{12} a quien es isomorfo) es un grupo simple.

LEMA 7.14

Sea $H \neq \{1\}$, $H \lhd M$. Entonces $\exists \rho \in H^*$ que fija al menos un punto.

Demostración: Sea $1 \neq \rho \in H$. Si el orden de ρ es par, entonces $2 \big| o(\rho) \big| o(H)$, y H tiene un elemento τ de orden 2.

Si τ tiene puntos fijos, hemos terminado. Si no tiene puntos fijos, entonces sin perder generalidad tenemos que

$$\tau = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12).$$

Sea $\sigma \in M$, $\sigma = (2)(3)(4)(5,6)\cdots$. Entonces

$$\sigma\tau\sigma = (3,4)(5,6)\cdots$$

y $\tau\sigma\tau\sigma(5) = 5$. Por Corolario 7.11, $\sigma(1) \neq 1$ (pues de lo contrario $\{1,2,3,4,5,6\}$ sería un bloque).

Tenemos pues que $\tau\sigma\tau\sigma(2) \neq 2$. Entonces $\tau\sigma\tau\sigma \in H$, fija al 5, y no es la identidad, así que es el elemento que buscabamos.

Supongamos entonces que ρ tiene orden impar. Si el orden de ρ es 11, entonces es un ciclo de longitud 11 con un punto fijo, y hemos terminado. Supongamos entonces que ρ no es de orden 11. Escribimos a ρ de la siguiente manera:

$$\rho = (a,b,c,\ldots)(d,e,f,\ldots)\cdots$$

con a, b, c, d, e, f distintos entre sí. Tomemos el elemento de M $\tau = (a,b)(c)(e)(f)\cdots$. Por lo tanto, $\tau\rho\tau \in H$, y $\rho\tau\rho\tau \in H$. Pero

$$\rho\tau\rho\tau(b) = \rho\tau\rho(a) = \rho\tau(b) = \rho(a) = b$$

de manera que fija al menos un punto, y

$$\rho\tau\rho\tau(d) = \rho\tau\rho(c) = \rho\tau(e) = \rho(f) = f$$

de manera que no es la identidad, y es el elemento que buscabamos.

□

TEOREMA 7.15

Si $M \subset S_{12}$ es nítidamente 5-transitivo, entonces M es simple.

Demostración: Sea $\{1\} \neq H \triangleleft M$. Por Lema 7.14, tenemos que $\exists \rho \in H^*$ con puntos fijos.

Si el orden de ρ es par, entonces H tiene un elemento de orden 2 con puntos fijos, a saber, si $o(\rho) = 2n$, ρ^n es de orden 2 con puntos fijos. Por Proposición 7.13*(ii)*, tiene a todos los elementos de orden dos con puntos fijos, y por la Proposición 7.13*(i)*, es todo M.

Si el orden de ρ es impar, podemos escribirlo como

$$\rho = (a)(b, c, \ldots, x, d)\cdots$$

con $x = c$ ó $x \neq c$. Sea $\tau \in M$ con $\tau = (a,d)(b)(c,x)\cdots$ (i.e., si $x = c$ entonces τ fija a c; si $x \neq c$, entonces los intercambia). Entonces $\rho\tau = (a,b,c,d)\cdots$ y

$$\sigma = \rho\tau\rho\tau = (a,c)(b,d)\cdots \in H.$$

Si $\tau\rho$ es de orden 4, entonces σ tiene puntos fijos (pues $M < A_{12}$, y por lo tanto $\rho\tau \neq (a,b,c,d)(e,f,g,h)(j,k,l,m)$), y tenemos el resultado, por el caso anterior.

Si $\sigma^2 \neq 1$, entonces $\rho\tau$ no es de orden 4, y tenemos en H un elemento, distinto de la identidad, que fija 4 puntos. Entonces ya sea él, o su cuadrado, son de órden 2, y fijan puntos, pues $\sigma^2 \in M(a,b,c,d)$, y el resultado nuevamente se sigue.

□

COROLARIO 7.16

M_{12} es simple.

Veremos ahora como exhibir un conjunto de cuatro generadores para M.

LEMA 7.17

Si $\alpha = (1)(2)(3)(4)(5,6)(7,8)(9,10)(11,12) \in M$, entonces

$$\alpha' = (5,6)(7,8)(9)(10)(11)(12)\cdots \in M.$$

Demostración: Puesto que $\alpha \in M$, $B_1 = \{1,2,3,4,5,6\}$ y $B_2 = \{1,2,3,4,7,8\}$ son bloques de $ST(M)$.

Tenemos pues que sus complementos, $B_1' = \{7,\ldots,12\}$ y $B_2' = \{5,6,9,10,11,12\}$ también son bloques.

Entonces

$$\gamma_1 = (7,8)(9)(10)(11)(12)\cdots$$
$$\gamma_2 = (5,6)(9)(10)(11)(12)\cdots$$

son elementos de M. Pero en M sólo hay un elemento de orden dos que fije a cuatro puntos dados, de manera que $\gamma_1 = \gamma_2$. Por lo tanto

$$\alpha' = \gamma_1 = \gamma_2 = (5,6)(7,8)(9)(10)(11)(12)\cdots \in M.$$

□

LEMA 7.18

Si $\alpha = (1)(2)(3)(4)(5,6)(7,8)(9,10)(11,12) \in M$, entonces existe

$$\sigma = (1)(2)(3)(7,a,b)(8,c,d)\cdots \in M$$

con $\{a,b,c,d\} = \{9,10,11,12\}$.

Demostración: Sea $\rho = (1)(2)(3)(4,5)\cdots \in M$. Entonces ρ fija también al 6, y

$$\sigma = \rho\alpha = (1)(2)(3)(4,5,6)\cdots$$

Por lo tanto σ es de orden 3, y $\rho(7) \neq 8$ y $\rho(8) \neq 7$. Esto último, pues si $\rho(7) = 8$, tenemos que σ fija a 4 elementos sin ser de orden 2 ó 4, y lo mismo pasaría si $\rho(8) = 7$. Entonces

$$\sigma = (1)(2)(3)(4,5,6)(7,a,b)(8,c,d).$$

□

TEOREMA 7.19

Si $B_1 = \{1,2,3,4,5,6\}$ y $B_2 = \{1,2,3,4,7,8\}$ son bloques en $ST(M)$, y

$$G = \left\{\sigma \in M \;\middle|\; (\sigma(B_1) = B_1) \vee (\sigma(B_2) = B_2)\right\}$$

entonces G genera a M. Además

$$\alpha = (1)(2)(3)(4)(5,6)(7,8)\cdots$$
$$\alpha' = (5,6)(7,8)(9)(10)(11)(12)\cdots$$

están ambos en G, y para cada $\tau \in T$, existe $\sigma \in G$ tal que $\tau = \sigma\alpha\sigma^{-1}$ o bien $\tau = \sigma\alpha'\sigma^{-1}$.

Demostración: Por Lema 7.17, $\alpha \in G$ por construcción de B_1. Por el mismo lema, tenemos que $\alpha' \in M$, y por lo tanto $\alpha' \in G$.

Sean B_1' y B_2' los complementos de B_1 y B_2 en $\{1,\ldots,12\}$ respectivamente. Sea

$$\tau = (a)(b)(c)(d)(e,f)\cdots \in T.$$

Tenemos tres casos:

(i) $\{a,b,c,d\} \subset B_1$. Entonces existe $\sigma \in M$ tal que $\sigma(\{1,2,3,4\}) = \{a,b,c,d\}$. Por lo tanto $\sigma\alpha\sigma^{-1}$ fija a a,b,c,d y es de orden dos. Puesto que sólo hay un elemento de orden dos que fije a a,b,c,d, tenemos que $\sigma\alpha\sigma^{-1} = \tau$; además, podemos elegir σ que mande alguno de los otros dos puntos de B_1 en B_1, de manera que σ manda B_1 en sí mismo y es elemento de G.

El mismo procedimiento se usa si $\{a,b,c,d\} \subset B_1', B_2,$ o B_2'.

(ii) $\{a,b,c\} \subset B_1$ y $d \in B_1'$. Tomamos entonces $\sigma \in G$ tal que $\sigma(\{a,b,c\}) = \{1,2,3\}$. Entonces

$$\sigma\tau\sigma^{-1} = (1)(2)(3)(\sigma(d))\cdots.$$

Por Lema 7.18, $\exists \rho \in G$ tal que

$$\rho = (1)(2)(3)(4,5,6)(7,a,b)(8,c,d).$$

Entonces si $\sigma(d) \neq 7$ y $\sigma(d) \neq 8$, tenemos que

$$\rho\sigma\tau\sigma^{-1}\rho^{-1} = (1)(2)(3)(x)\cdots$$

con $x = \rho(\sigma(d))$. Como $\rho(\sigma(d))$ no es igual a $\rho(7)$ ni a $\rho(8)$, tenemos que $x = 7, 8, b,$ o d. En cualquier caso se puede elegir ya sea el anterior o

$$\rho^2\sigma\tau\sigma^{-1}\rho^{-2} = (1)(2)(3)(x)\cdots$$

con $x = 7$ o $x = 8$, y estamos en el caso *(i)*.

Si $\sigma(d) = 7$ o $\sigma(d) = 8$, $\sigma\tau\sigma^{-1}$ ya está en el caso *(i)*. Despejando τ llegamos a la conjugación deseada.

(iii) $\{a,b\} \subset B_1$ y $\{c,d\} \subset B_1'$. Sea $\sigma \in G$ tal que $\sigma(\{a,b\}) = \{1,2\}$. Sea ρ como en el caso *(ii)*.

Si $\sigma(c) \neq 7,8$, entonces $\rho\sigma(c) = 7$ u 8, o bien $\rho^2\sigma(c) = 7$ u 8. En cualquier caso tenemos ya sea $\{1,2,3,7\} \subset B_2$, o bien $\{1,2,3,8\} \subset B_2$, y estamos en el caso *(i)* o en el *(ii)*.

De lo anterior, G genera a T, y por lo tanto a M.

□

TEOREMA 7.20

Si $\alpha = (1)(2)(3)(4)(5,6)(7,8)(9,10)(11,12) \in M$, entonces

$$\alpha' = (5,6)(7,8)(9)(10)(11)(12)\cdots$$

$$\beta = (1)(2,3)(4,5)(6)\cdots$$

$$\beta' = (1)(2,3)(4,7)(8)\cdots$$

y α generan M.

Demostración: $\{\alpha, \alpha', \beta\}$ generan el conjunto de las $\sigma \in M$ tales que $\sigma(B_1) = B_1$, y $\{\alpha, \alpha', \beta'\}$ generan el conjunto de las $\sigma' \in M$ tales que $\sigma'(B_2) = B_2$. El resultado se sigue ahora inmediatamente del Teorema 7.19.

□

Pasemos ahora a la segunda parte del capítulo. En esta parte, como se mencionó antes, se dará un algoritmo para obtener conjuntos de generadores de subgrupos de S_{12} nítidamente 5-transitivos.

Tómese una permutación de S_{12}, de orden 5 y con dos puntos fijos, digamos

$$\rho = (1,2,3,4,5)(6)(7,8,9,10,11)(12).$$

Consideremos por separado a $\rho_1 = \rho|_{\{1,\ldots,6\}}$, y $\rho_2 = \rho|_{\{7,\ldots,12\}}$.

Fijamos cuatro de los puntos permutados por ρ_1, digamos $1, 2, 3, 4$. Consideramos el otro punto permutado por σ_1, en este caso 5; el correspondiente de ρ_2, en este caso el 11; y los puntos fijos de ρ_1 y ρ_2, en este caso 6 y 12; en ese orden, y formamos una permutación de orden 4, $\sigma_1 = (5, 11, 6, 12)$.

Tomamos ahora los cuatro puntos permutados por ρ_2 que corresponden a los que dejamos fijos de los que permuta σ_1, en este caso 7,8,9,10. Intercambiando los últimos dos, formamos otra permutación de orden cuatro, $\sigma_2 = (7, 8, 10, 9)$.

Denotemos por $\sigma = \sigma_1 \cup \sigma_2$, en este caso $\sigma = (5, 11, 6, 12)(7, 8, 10, 9)$.

Aseguramos que $\langle \rho, \sigma \rangle \cong M_{12}$. Para probarlo, busquemos construir un Sistema de Steiner de tipo $S(5, 6, 12)$ que sea respetado por ρ y por σ.

Claramente, un bloque sería $B_1 = \{1, 2, 3, 4, 5, 6\}$, y otro sería entonces

$$B_2 = \sigma(B_1) = \{1, 2, 3, 4, 11, 12\}.$$

El Sistema de Steiner ST estará dado a través de un isomorfismo $P: G_1(B_1) \longrightarrow G_3(B_1')$. ¿Quién es P? Hagamos unos cálculos con ρ y σ para averiguarlo.

Tenemos que

$$\sigma^2 = (1)(2)(3)(4)(5,6)(7,10)(8,9)(11,12)$$

así que $P(5,6) = (7,10)(8,9)(11,12)$, para respetar el sistema. Haciendo más cálculos obtenemos:

$$\rho\sigma^2\rho^{-1} = (2)(3)(4)(5)(1,6)(7,12)(8,11)(9,10)$$
$$\rho^2\sigma^2\rho^{-2} = (1)(3)(4)(5)(2,6)(8,12)(9,7)(10,11)$$
$$\rho^3\sigma^2\rho^{-3} = (1)(2)(4)(5)(3,6)(9,12)(10,8)(7,11)$$
$$\rho^4\sigma^2\rho^{-4} = (1)(2)(3)(5)(4,6)(10,12)(11,9)(7,8).$$

Denotemos $\sigma^2\rho\sigma^2 = \varphi = (1,2,3,4,6)(5)(10,9,8,7,12)(11)$, y calculamos:

$$\varphi\sigma^2\varphi^{-1} = (2)(3)(4)(6)(1,5)(11,10)(12,9)(7,8)$$
$$\varphi^2\sigma^2\varphi^{-2} = (1)(3)(4)(6)(2,5)(11,9)(8,10)(12,7)$$
$$\varphi^3\sigma^2\varphi^{-3} = (1)(2)(4)(6)(3,5)(8,11)(7,9)(10,12)$$
$$\varphi^4\sigma^2\varphi^{-4} = (1)(2)(3)(6)(4,5)(11,7)(8,12)(10,9)$$
$$\rho\varphi\sigma^2\varphi^{-1}\rho^{-1} = (3)(4)(5)(6)(1,2)(7,11)(12,10)(8,9)$$
$$\rho^2\varphi\sigma^2\varphi^{-1}\rho^{-2} = (1)(4)(5)(6)(2,3)(8,7)(11,12)(9,10)$$
$$\rho^3\varphi\sigma^2\varphi^{-1}\rho^{-3} = (1)(2)(5)(6)(3,4)(8,9)(7,12)(10,11)$$
$$\rho\varphi^2\sigma^2\varphi^{-2}\rho^{-1} = (2)(4)(5)(6)(1,3)(8,12)(9,11)(7,10)$$
$$\rho^2\varphi^2\sigma^2\varphi^{-2}\rho^{-2} = (1)(3)(5)(6)(2,4)(9,12)(7,10)(11,8)$$
$$\rho^4\varphi^2\sigma^2\varphi^{-2}\rho^{-4} = (2)(3)(5)(6)(1,4)(11,12)(7,9)(8,10).$$

Con estos cálculos podemos ahora establecer a

$$P: G_1(B_1) \longrightarrow G_3(B_1')$$

dada por la siguiente correspondencia:

$$(1,2) \mapsto (7,11)(8,9)(10,12) \qquad (2,5) \mapsto (7,12)(8,10)(9,11)$$

$$(1,3) \mapsto (7,10)(8,12)(9,11) \qquad (2,6) \mapsto (7,9)(8,12)(10,11)$$

$$(1,4) \mapsto (7,9)(8,10)(11,12) \qquad (3,4) \mapsto (7,12)(8,9)(10,11)$$

$$(1,5) \mapsto (7,8)(9,12)(10,11) \qquad (3,5) \mapsto (7,9)(8,11)(10,12)$$

$$(1,6) \mapsto (7,12)(8,11)(9,10) \qquad (3,6) \mapsto (7,11)(8,10)(9,12)$$

$$(2,3) \mapsto (7,8)(9,10)(11,12) \qquad (4,5) \mapsto (7,11)(8,12)(9,10)$$

$$(2,4) \mapsto (7,10)(8,11)(9,12) \qquad (4,6) \mapsto (7,8)(9,11)(10,12)$$

$$(5,6) \longmapsto (7,10)(8,9)(11,12)$$

que es un isomorfismo de gráficos. Por Teorema 6.37, esto da lugar a un Sistema de Steiner de tipo $S(5,6,12)$, que denotamos por ST, sobre el conjunto $\{1,\ldots,12\}$.

Notemos que en ST, B_2 es un bloque de tipo *(ii)*, que surge al considerar $(5,6)$ y $P(5,6) = (7,10)(8,9)(11,12)$.

Tenemos entonces que el Sistema de Steiner ST da lugar a un isomorfismo

$$P_2 \colon G_1(B_2) \to G_3(B_2')$$

por la Proposición 6.31. Haciendo los cálculos correspondientes si verifica con facilidad que P_2 es la siguiente función:

$$(1,2) \mapsto (7,10)(5,9)(6,8) \qquad (2,11) \mapsto (5,8)(6,7)(9,10)$$

$$(1,3) \mapsto (8,9)(5,10)(6,7) \qquad (2,12) \mapsto (5,10)(6,9)(7,8)$$

$$(1,4) \mapsto (9,10)(7,8)(5,6) \qquad (3,4) \mapsto (7,10)(5,8)(6,9)$$

$$(1,11) \mapsto (5,7)(6,9)(8,10) \qquad (3,11) \mapsto (5,9)(6,10)(7,8)$$

$$(1,12) \mapsto (5,8)(6,10)(7,9) \qquad (3,12) \mapsto (5,7)(6,8)(9,10)$$

$$(2,3) \mapsto (8,10)(5,6)(7,9) \qquad (4,11) \mapsto (5,10)(6,8)(7,9)$$

$$(2,4) \mapsto (8,9)(5,7)(6,10) \qquad (4,12) \mapsto (5,9)(6,7)(8,10)$$

$$(11,12) \longmapsto (5,6)(7,10)(8,9).$$

LEMA 7.21

$\rho, \sigma \in Aut(ST)$.

Demostración: Por la Proposición 6.45, basta probar que los siguientes diagramas son conmutativos:

$$\begin{array}{ccc} G_1(B_1) & \xrightarrow{P} & G_3(B_1') \\ {\scriptstyle G_1(\rho)}\downarrow & & \downarrow{\scriptstyle G_3(\rho)} \\ G_1(B_1) & \xrightarrow{P} & G_3(B_1') \end{array}$$

y

$$\begin{array}{ccc} G_1(B_1) & \xrightarrow{P} & G_3(B_1') \\ {\scriptstyle G_1(\sigma)}\downarrow & & \downarrow{\scriptstyle G_3(\sigma)} \\ G_1(B_2) & \xrightarrow{P_2} & G_3(B_2') \end{array}$$

Ambos diagramas son conmutativos, como se verifica a continuación:

$$P(\rho(1,2)) = P(2,3) = (7,8)(9,10)(11,12) = \rho(7,11)(8,9)(10,12) = \rho(P(1,2))$$
$$P(\rho(1,3)) = P(2,4) = (7,10)(8,11)(9,12) = \rho(9,11)(7,10)(8,12) = \rho(P(1,3))$$
$$P(\rho(1,4)) = P(2,5) = (8,12)(8,10)(9,11) = \rho(11,12)(7,9)(8,10) = \rho(P(1,4))$$
$$P(\rho(1,5)) = P(1,2) = (7,11)(8,9)(10,12) = \rho(10,11)(7,8)(9,12) = \rho(P(1,5))$$
$$P(\rho(1,6)) = P(2,6) = (7,9)(8,12)(10,11) = \rho(8,11)(7,12)(9,10) = \rho(P(1,6))$$
$$P(\rho(2,3)) = P(3,4) = (7,12)(8,9)(10,11) = \rho(11,12)(7,8)(9,10) = \rho(P(2,3))$$
$$P(\rho(2,4)) = P(3,5) = (7,9)(8,11)(10,12) = \rho(8,11)(7,10)(9,12) = \rho(P(2,4))$$
$$P(\rho(2,5)) = P(1,3) = (7,10)(8,12)(9,11) = \rho(9,11)(7,12)(8,10) = \rho(P(2,5))$$
$$P(\rho(2,6)) = P(3,6) = (7,11)(8,10)(9,12) = \rho(10,11)(7,9)(8,12) = \rho(P(2,6))$$
$$P(\rho(3,4)) = P(4,5) = (7,11)(8,12)(9,10) = \rho(10,11)(7,12)(8,9) = \rho(P(3,4))$$
$$P(\rho(3,5)) = P(1,4) = (7,9)(8,10)(11,12) = \rho(8,11)(7,9)(10,12) = \rho(P(3,5))$$
$$P(\rho(3,6)) = P(4,6) = (7,8)(9,11)(10,12) = \rho(7,11)(8,10)(9,12) = \rho(P(3,6))$$
$$P(\rho(4,5)) = P(1,5) = (7,8)(9,12)(10,11) = \rho(7,11)(8,12)(9,10) = \rho(P(4,5))$$

$$P(\rho(4,6)) = P(5,6) = (7,10)(8,9)(11,12) = \rho(9,11)(7,8)(10,12) = \rho(P(4,6))$$
$$P(\rho(5,6)) = P(1,6) = (7,12)(8,11)(9,10) = \rho(11,12)(7,10)(8,9) = \rho(P(5,6))$$

con lo cual $\rho \in Aut(ST)$. Y como

$$P_2(\sigma(1,2)) = P_2(1,2) = (7,10)(5,9)(6,8) = \sigma(7,11)(8,9)(10,12) = \sigma(P(1,2))$$
$$P_2(\sigma(1,3)) = P_2(1,3) = (5,10)(8,9)(6,7) = \sigma(9,11)(7,10)(8,12) = \sigma(P(1,3))$$
$$P_2(\sigma(1,4)) = P_2(1,4) = (9,10)(7,8)(5,6) = \sigma(11,12)(7,9)(8,10) = \sigma(P(1,4))$$
$$P_2(\sigma(1,5)) = P_2(1,11) = (5,7)(6,9)(8,10) = \sigma(10,11)(7,8)(9,12) = \sigma(P(1,5))$$
$$P_2(\sigma(1,6)) = P_2(1,12) = (5,8)(6,10)(7,9) = \sigma(8,11)(7,12)(9,10) = \sigma(P(1,6))$$
$$P_2(\sigma(2,3)) = P_2(2,3) = (8,10)(5,6)(7,9) = \sigma(11,12)(7,8)(9,10) = \sigma(P(2,3))$$
$$P_2(\sigma(2,4)) = P_2(2,4) = (8,9)(5,7)(6,10) = \sigma(8,11)(7,10)(9,12) = \sigma(P(2,4))$$
$$P_2(\sigma(2,5)) = P_2(2,11) = (5,8)(6,7)(9,10) = \sigma(9,11)(7,12)(8,10) = \sigma(P(2,5))$$
$$P_2(\sigma(2,6)) = P_2(2,12) = (5,10)(6,9)(7,8) = \sigma(10,11)(7,9)(8,12) = \sigma(P(2,6))$$
$$P_2(\sigma(3,4)) = P_2(3,4) = (7,10)(5,8)(6,9) = \sigma(10,11)(7,12)(8,9) = \sigma(P(3,4))$$
$$P_2(\sigma(3,5)) = P_2(3,11) = (5,9)(6,10)(7,8) = \sigma(8,11)(7,9)(10,12) = \sigma(P(3,5))$$
$$P_2(\sigma(3,6)) = P_2(3,12) = (5,7)(6,8)(9,10) = \sigma(7,11)(8,10)(9,12) = \sigma(P(3,6))$$
$$P_2(\sigma(4,5)) = P_2(4,11) = (5,10)(6,8)(7,9) = \sigma(7,11)(8,12)(9,10) = \sigma(P(4,5))$$
$$P_2(\sigma(4,6)) = P_2(4,12) = (5,9)(6,7)(8,10) = \sigma(9,11)(7,8)(10,12) = \sigma(P(4,6))$$
$$P_2(\sigma(5,6)) = P_2(11,12) = (5,6)(7,10)(8,9) = \sigma(11,12)(7,10)(8,9) = \sigma(P(5,6))$$

con lo cual $\sigma \in Aut(ST)$.

□

Concluimos entonces que

TEOREMA 7.22

$\langle \rho, \sigma \rangle \subset Aut(ST) \cong M_{12}$.

LEMA 7.23

$\langle \rho, \sigma \rangle$ contiene una copia isomorfa a M_{12}.

Demostración: Puesto que ρ y σ ya vimos que forman parte del grupo de automorfismos de un $S(5,6,12)$ y que

$$\alpha = \sigma^2 = (1)(2)(3)(4)(5,6)(7,10)(9,8)(11,12)$$

podemos utilizar el Teorema 7.20, y tratar de exhibir a los siguientes tres elementos como generados por $\langle \rho, \sigma \rangle$:

$$\alpha' = (5,6)(7,10)(9)(8)(11)(12)\cdots$$

$$\beta = (1)(2,3)(4,5)(6)\cdots$$

$$\beta' = (1)(2,3)(4,7)(10)\cdots$$

para tener que ρ y σ generan a todo M_{12}.

Haciendo los cálculos, descubrimos que

$$\alpha' = (9)(8)(11)(12)(5,6)(7,10)(1,3)(2,4)$$

$$\beta = (1)(6)(9)(10)(2,3)(4,5)(7,12)(8,11)$$

$$\beta' = (1)(5)(10)(12)(2,3)(4,7)(6,8)(9,11)$$

y que los podemos obtener a partir de ρ y σ de la siguiente manera:

$$\alpha = \sigma^2$$

$$\alpha' = \rho\sigma^3\rho\sigma^3\rho^3\sigma\rho\sigma\rho$$

$$\beta = \rho\sigma^2\rho\sigma^2\rho^2\sigma^2\rho^2\sigma^2$$

$$\beta' = \rho\sigma\rho\sigma\rho\sigma^2\rho\sigma^2\rho\sigma\rho^2\sigma^3$$

con lo cual tenemos que $\langle \rho, \sigma \rangle$ contiene todo el grupo de automorfismos de ST, que es isomorfo a M_{12}.

□

TEOREMA 7.24

Los generadores de Cárdenas-Lluis generan al Grupo de Mathieu de grado 12, i.e.

$$\langle \rho, \sigma \rangle = M_{12}.$$

Con este resultado, damos por terminado este capítulo.

VIII. Construcción de Curtis

En este capítulo presentaremos la construcción de generadores para M_{12}, dado por R.T. Curtis, en su artículo *Natural Constructions of the Mathieu Groups*. Daremos primero el algoritmo de construcción de conjuntos de generadores. Después pasaremos a demostrar que los grados de libertad que intervienen en la construcción son irrelevantes, es decir, que todos los posibles resultados que se obtienen siguiendo el método son isomorfos entre sí. Finalmente, se dará la igualdad explícitamente de uno de los resultados de este proceso con una de las representaciones del grupo de Mathieu que ya tenemos.

Consideremos el grupo alternante A_5, y P un 5-subgrupo de Sylow de A_5.

Tomemos un subgrupo $H < A_5$, con $H \cong A_4$. Tendremos un elemento de H en cada clase lateral derecha de P, pues el producto de elementos en A_4 nunca da un elemento de orden 5, y no pueden estar dos distintos en la misma clase lateral.

Consideremos la acción de un elemento de orden 3 de H sobre los otros elementos de H al multiplicarlos por la izquierda, y consideremos la representación de dicha acción en S_{12}, inducida por la numeración de las clases laterales de P en A_5.

Sea σ dicha representación, y sea τ la representación de un generador de P en el mismo conjunto, pero multiplicando por la derecha.

Entonces aseguramos que $M_{12} = \langle \tau, \sigma \rangle$.

Apliquemos primero el proceso a una elección particular de P, H, numeración de las clases, σ y τ, y veamos que se obtiene.

Tomemos el siguiente 5-subgrupo de Sylow de A_5:

$$P = \Big\{1, (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2)\Big\}$$

y a H como el estabilizador del 5 en A_5.

Las clases laterales izquierdas inducidas por P en A_5 son las siguientes:

$$C_1 = P \cdot 1 = \Big\{1;(1,2,3,4,5);(1,3,5,2,4);(1,4,2,5,3);(1,5,4,3,2)\Big\}$$
$$C_2 = P \cdot (1,2,3) = \Big\{(1,2,3);(1,3,2,4,5);(1,4)(2,5);(1,5,3,4,2);(3,5,4)\Big\}$$
$$C_3 = P \cdot (1,2,4) = \Big\{(1,2,4);(1,3,4,2,5);(1,4,3,5,2);(1,5,3);(2,3)(4,5)\Big\}$$
$$C_4 = P \cdot (2,4,3) = \Big\{(2,4,3);(1,2,5);(1,3,4,5,2);(1,4)(3,5);(1,5,4,2,3)\Big\}$$
$$C_5 = P \cdot (1,3,4) = \Big\{(1,3,5);(1,4,2,3,5);(1,5,2,4,3);(2,5,3);(1,2)(4,5)\Big\}$$
$$C_6 = P \cdot (1,2)(3,4) = \Big\{(1,2)(3,4);(1,3,5);(1,4,5,2,3);(1,5,3,2,4);(2,5,4)\Big\}$$
$$C_7 = P \cdot (1,3,2) = \Big\{(1,3,2);(1,4,5);(1,5,2,3,4);(2,4)(3,5);(1,2,5,4,3)\Big\}$$
$$C_8 = P \cdot (2,3,4) = \Big\{(2,3,4);(1,2,4,3,5);(1,3)(2,5);(1,4,5,3,2);(1,5,4)\Big\}$$
$$C_9 = P \cdot (1,4,2) = \Big\{(1,4,2);(1,5)(3,4);(2,3,5);(1,2,4,5,3);(1,3,2,5,4)\Big\}$$
$$C_{10} = P \cdot (1,4,3) = \Big\{(1,4,3);(1,5)(2,3);(2,4,5);(1,2,5,3,4);(1,3,5,4,2)\Big\}$$
$$C_{11} = P \cdot (1,3)(2,4) = \Big\{(1,3)(2,4);(1,4,3,2,5);(1,5,2);(2,4,5);(1,2,3,5,4)\Big\}$$
$$C_{12} = P \cdot (1,4)(2,3) = \Big\{(1,4)(2,3);(1,5)(2,4);(2,5)(3,4);(1,2)(3,5);(1,3)(4,5)\Big\}$$

El 3-elemento de H que elegiremos será $(1,2,3)$, y el generador de P será $(1,2,3,4,5)$. La acción de $(1,2,3)$ al multiplicar por la izquierda a los representantes de las clases laterales es la siguiente:

$$1 \mapsto (1,2,3) \mapsto (1,3,2) \mapsto 1$$
$$(1,2,4) \mapsto (1,3)(2,4) \mapsto (2,4,3) \mapsto (1,2,4)$$
$$(1,3,4) \mapsto (2,3,4) \mapsto (1,2)(3,4) \mapsto (1,3,4)$$
$$(1,4,2) \mapsto (1,4,3) \mapsto (1,4)(2,3) \mapsto (1,4,2)$$

quedando entonces su representación en S_{12} dada por el elemento

$$\sigma = (1,2,7)(3,11,4)(5,8,6)(9,10,12).$$

La acción de $(1,2,3,4,5)$ al multiplicar por la derecha las clases laterales es la siguiente:

$$C_1 \longmapsto C_1$$
$$C_2 \mapsto C_4 \mapsto C_7 \mapsto C_{11} \mapsto C_8 \mapsto C_2$$
$$C_3 \mapsto C_6 \mapsto C_{10} \mapsto C_5 \mapsto C_9 \mapsto C_3$$
$$C_{12} \longmapsto C_{12}$$

quedando su representación en S_{12} dada por el elemento

$$\tau = (1)(12)(2,4,7,11,8)(3,6,10,5,9).$$

El grupo que generamos, que denotaremos por M, será entonces

$$M = \Big\langle (1,2,7)(3,11,4)(5,8,6)(9,10,12)\ ,\ (2,4,7,11,8)(3,6,10,5,9) \Big\rangle$$

Veamos ahora que la construcción es independiente de nuestra elección de P, H, 3-elemento, generador, y numeración de las clases laterales que hicimos, i.e., veremos que sin importar que escojamos en cada decisión, el resultado será un conjugado de nuestro M.

Llamemos h al 3-elemento de H elegido, y α al generador de P.

PROPOSICIÓN 8.1

La construcción es independiente de la elección de α.

Demostración: Puesto que $P = \{\alpha, \alpha^2, \ldots, \alpha^5\}$, tenemos que la acción de α^n estará dada por τ^n. Puesto que $1 \leq n \leq 4$, y τ es de orden 5, claramente

$$M = \Big\langle \sigma\ ,\ \tau \Big\rangle = \Big\langle \sigma\ ,\ \tau^n \Big\rangle$$

□

PROPOSICIÓN 8.2

La construcción es independiente de la numeración de las clases laterales.

Demostración: Sea $\mu \in S_{12}$ una renumeración de las clases laterales. Entonces la acción de h estará dada por $\mu\tau\mu^{-1}$, y la de α por $\mu\sigma\mu^{-1}$. Tenemos que el resultado es $\mu M\mu^{-1}$, y por lo tanto un conjugado de M

□.

PROPOSICIÓN 8.3

La construcción es independiente del h elegido.

Demostración: Consideremos el elemento $\rho = (1,3,4,2) \in S_5$. Tenemos que bajo conjugación ρ manda a A_5 en sí mismo, y normaliza a P:

$$(1,3,4,2)(1,2,3,4,5)(1,2,4,3) = (1,4,2,5,3) = (1,2,3,4,5)^3 \in P.$$

Puesto que normaliza a P, mandará bajo conjugación a clases laterales de P en clases laterales de P, y simplemente las renumera. Puesto que ya tenemos que la construcción es independiente de la renumeración de clases, esto nos tiene sin cuidado. Tenemos además que normaliza a H, pues fija al 5, y manda bajo conjugación a

$$(1,2,3) \mapsto (1,4,3) \mapsto (2,4,3) \mapsto (1,2,4) \mapsto (1,2,3)$$

de manera que la acción de $(1,4,3)$ en las clases laterales está dada por un conjugado de $\rho\sigma\rho^{-1}$, el de $(2,4,3)$ por un conjugado de $\rho^2\sigma\rho^{-2}$, etc. De manera que las cuatro elecciones de h como $(1,2,3)$, $(1,4,3)$, $(2,4,3)$, y $(1,2,4)$ dan como resultado construcciones conjugadas de M.

Tenemos además que elegir a h^{-1} en vez de h (puesto que $h^{-1} = h^2$) da simplemente como resultado σ^2 en vez de σ. Puesto que σ es de orden 3, tenemos claramente que

$$M = \langle \sigma\ ,\ \tau \rangle = \langle \sigma^2\ ,\ \tau \rangle$$

y con esto cubrimos a $(1,3,2)$, $(1,4,3)$, $(2,3,4)$, y $(1,4,2)$ (pues sus inversos ya están cubiertos). Hemos pues cubierto a las ocho posibles elecciones de h, y todas ellas dan construcciones conjugadas de M.

□

LEMA 8.4

Sea $H < A_5$, $H \cong A_4$. Entonces H es el estabilizador de un punto en A_5.

Demostración: En A_4, el producto de elementos de orden 2 es un elemento de orden 2:

$$(1,2)(3,4)\cdot(1,3)(2,4) = (1,4)(2,3) \qquad (1,3)(2,4)\cdot(1,2)(3,4) = (1,4)(2,3)$$
$$(1,2)(3,4)\cdot(1,4)(2,3) = (1,3)(2,4) \qquad (1,4)(2,3)\cdot(1,2)(3,4) = (1,3)(2,4)$$
$$(1,3)(2,4)\cdot(1,4)(2,3) = (1,2)(3,4) \qquad (1,4)(2,3)\cdot(1,3)(2,4) = (1,2)(3,4)$$

Supongamos sin perder generalidad que $\zeta = (1,2)(3,4) \in H$. Si no todo elemento de orden 2 fija al 5, tenemos dos casos:

(i) Alguna de las transposiciones es igual a una de ζ, digamos el $(1,2)(3,5)$. Pero

$$(1,2)(3,4)\cdot(1,2)(3,5) = (3,5,4)$$

de orden 3, y producto de elementos de orden 2 en H debe ser un elemento de orden 2.

(ii) Ambas transposiciones son distintas de las de ζ. Entonces tenemos un elemento de la forma $(1,3)(2,5)$ o uno de la forma $(1,3)(4,5)$. Pero tenemos que

$$(1,2)(3,4)\cdot(1,3)(2,5) = (1,4,3,2,5)$$
$$(1,2)(3,4)\cdot(1,3)(4,5) = (1,4,5,3,2)$$

y en ambos casos no es de orden 2.

Concluimos que todo elemento de orden 2 fija al 5. Basta ver que todo elemento de orden 3 fija tambien al 5 para terminar.

Notemos que en A_4, el producto de un elemento de orden 2 por uno de orden 3 siempre es un elemento de orden 3:

$$(1,2)(3,4)\cdot(1,2,3) = (2,4,3) \qquad (1,2)(3,4)\cdot(1,3,2) = (1,4,3)$$
$$(1,2)(3,4)\cdot(1,2,4) = (2,3,4) \qquad (1,2)(3,4)\cdot(1,4,2) = (1,3,4)$$
$$(1,2)(3,4)\cdot(1,3,4) = (1,4,2) \qquad (1,2)(3,4)\cdot(1,4,3) = (1,3,2)$$
$$(1,2)(3,4)\cdot(2,3,4) = (1,2,4) \qquad (1,2)(3,4)\cdot(2,4,3) = (1,2,3)$$

Pero si un elemento de orden 3 de H no fija al 5, tenemos que el producto con ζ no es de orden 3:

$$(1,2)(3,4)\cdot(1,2,5) = (2,5)(3,4) \qquad (1,2)(3,4)\cdot(2,3,5) = (1,2,4,3,5)$$
$$(1,2)(3,4)\cdot(1,5,2) = (1,5)(3,4) \qquad (1,2)(3,4)\cdot(2,5,3) = (1,2,5,4,3)$$
$$(1,2)(3,4)\cdot(1,3,5) = (1,4,3,5,2) \qquad (1,2)(3,4)\cdot(2,4,5) = (1,2,3,4,5)$$
$$(1,2)(3,4)\cdot(1,5,3) = (1,5,4,3,2) \qquad (1,2)(3,4)\cdot(2,5,4) = (1,2,5,3,4)$$
$$(1,2)(3,4)\cdot(1,4,5) = (1,3,4,5,2) \qquad (1,2)(3,4)\cdot(3,4,5) = (1,2)(4,5)$$
$$(1,2)(3,4)\cdot(1,5,4) = (1,5,3,4,2) \qquad (1,2)(3,4)\cdot(3,5,4) = (1,2)(3,5)$$

de manera que todo elemento de orden 3 debe también fijar al 5, y tenemos que H es el estabilizador de 5 en A_5.

□

PROPOSICIÓN 8.5

La construcción es independiente de la elección de H.

Demostración: El elemento $(1,2,3,4,5)$ normaliza a A_5 y a P (pues es elemento de P), y bajo conjugación permuta a los estabilizadores de una letra en A_5 entre sí. Puesto que todas las elecciones de H están caracterizadas como estabilizador de una letra por el Lema 8.4, tenemos que $(1,2,3,4,5)$ bajo conjugación, manda una elección de H en cualquier otra, de manera que conjugando con la potencia adecuada podemos regresar al caso de la H que elegimos al construir M.

□

PROPOSICIÓN 8.6

La construcción es independiente de la elección de P.

Demostración: Puesto que todo 5-Subgrupo de Sylow es conjugado de nuestra elección de P, la conjugación inversa nos lleva de cualquier elección de P al que elegimos originalmente. De manera de que la elección de P también es irrelevante.

□

TEOREMA 8.7

La Construcción de Curtis está bien definida, es decir, es independiente de la elección de P, H, h, y α que hagamos, lo mismo que de la numeración que demos de clases laterales. Cualquier elección dará un grupo isomorfo a M.

Recordemos ahora que en el Capítulo 7 se demostró que el grupo de Mathieu está generado por ρ y σ los generadores de Cárdenas-Lluis, donde

$$\rho = (1,2,3,4,5)(6)(7,8,9,10,11)(12)$$
$$\sigma = (1)(2)(3)(4)(5,11,6,12)(7,8,10,9).$$

Conjuguemos por el elemento $(6,12,8,11,9,10) \in S_{12}$. Tenemos entonces a M_{12} generado por ρ' y σ', donde

$$\rho' = (1,2,3,4,5)(12)(7,11,10,6,9)(8)$$
$$\sigma' = (1)(2)(3)(4)(5,9,12,8)(7,11,6,10).$$

TEOREMA 8.8

$M = \langle \rho', \sigma' \rangle$.

Demostración: Tenemos a M generado por

$$\varphi = (1,2,7)(3,11,4)(5,8,6)(9,10,12)$$
$$\psi = (2,4,7,11,8)(3,6,10,5,9).$$

En primero lugar, tenemos que $M_{12} \subset M$, pues

$$\rho' = \psi\varphi^2\psi^3\varphi\psi^2\varphi^2\psi\varphi\psi\varphi^2\psi\varphi$$
$$\sigma' = \psi^4\varphi\psi\varphi\psi^4\varphi^2\psi^2\varphi\psi^2$$

y por lo tanto $M_{12} = \langle \rho', \sigma' \rangle \subset \langle \varphi, \psi \rangle$.

Y en segundo lugar, tenemos que $M \subset M_{12}$, pues tenemos que

$$\psi = \rho'\sigma'\rho'^4\sigma'\rho'^3\sigma'^2\rho'^4\sigma'$$
$$\varphi = \rho'\sigma'^3\rho'^2\sigma'^2\rho'\sigma'^3\rho'\sigma'^3\rho'$$

y por lo tanto $\langle \psi, \varphi \rangle \subset \langle \rho', \sigma' \rangle = M_{12}$, lo cual nos da la igualdad.

□

COROLARIO 8.9

$M = \langle \varphi, \psi \rangle \cong M_{12}$.

COROLARIO 8.10

La construcción de Curtis produce un grupo isomorfo al Grupo de Mathieu de grado 12, M_{12}.

IX. Propiedades de M_{12}

En este capítulo vamos a resumir algunas de las propiedades que hemos demostrado de M_{12} a lo largo de las construcciones desarrolladas. En algunos casos, daremos demostraciones alternativas, que permiten visilumbrar un poco más de la estructura de grupo de M_{12}. También mencionaremos algunas otras propiedades que no se han tocado anteriormente. Por último mencionaremos unos cuantos otros resultados que no se pudieron contemplar en este trabajo.

TEOREMA 9.1

$N_{S_{12}}(M_{12}) = M_{12}$.

Demostración: Consideremos ST el Sistema de Steiner de tipo $S(5,6,12)$ asociado a M_{12}. Tenemos que M_{12} es el grupo de automorfismos de ST.

Será $r \in S_{12}$ tal que r no manda bloques en bloques (i.e., $r \notin M_{12}$). Hay que demostrar que r no normaliza a M_{12}. Se hará por reducción al absurdo, suponiendo que r normaliza a M_{12}.

Supongamos sin perder generalidad que $\{1,2,3,4,5,6\}$ es un bloque en ST, y que

$$r(\{1,2,3,4,5,6\}) = \{a,b,c,d,e,f\}$$

no es un bloque de ST.

Consideremos el elemento $m \in M_{12}$ que manda $a \mapsto a$, $b \mapsto b$, $c \mapsto c$, $d \mapsto d$, y $e \mapsto f$. Llamemos a' al elemento de $\{1,\ldots,12\}$ que completa el bloque que contiene a $\{b,c,d,e,f\}$. Notemos que puesto que $\{a,b,c,d,e,f\}$ no es un bloque por hipótesis, tenemos que $a' \neq a$.

Puesto que $r \in N_{S_{12}}(M_{12})$, tenemos que $r^{-1}mr \in M_{12}$, y por lo tanto manda el bloque $\{1,2,3,4,5,6\}$ en un bloque. Tenemos que

$$r^{-1}mr(\{1,2,3,4,5,6\}) = \{1,2,3,4,6,r^{-1}(m(f))\}$$

y puesto que $\{1,2,3,4,5,6\}$ es el único bloque que contiene a $1,2,3,4,6$, tenemos que $r^{-1}(m(f)) = 5$, y por lo tanto $m(f) = e$.

Pero puesto que m manda bloques en bloques, tenemos que

$$m(\{a', b, c, d, e, f\}) = \{m(a'), b, c, d, f, e\}$$

con este último un bloque, de lo que deducimos que necesariamente $m(a') = a'$. Entonces tenemos que m debe fijar a a, b, c, d, a', pero $m(e) = f \neq e$, y por lo tanto no es la identidad, contradiciendo el hecho de que $m \in M_{12}$.

La contradicción surgió de suponer que r normalizaba a M_{12}, por lo que concluimos que M_{12} es su propio normalizador en S_{12}.

□

LEMA 9.2

Sea $M_{12} \subsetneq H$, con H un grupo. Entonces $\exists \sigma \in H - M_{12}$, distinto de la identidad, tal que σ fija a 8,9,10,11, y 12.

Demostración: Sea $\sigma \in H - M_{12}$, y supongamos que $\sigma(8) = a$, $\sigma(9) = b$, $\sigma(10) = c$, $\sigma(11) = d$, y $\sigma(12) = e$.

Sea $m \in M_{12}$ tal que $m(a) = 8$, $m(b) = 9$, $m(c) = 10$, $m(d) = 11$, y $m(e) = 12$. Entonces $m \neq \sigma^{-1}$, pues $\sigma \notin M_{12}$. Tenemos pues que $m\sigma \in H$, y claramente fija al 8,9,10,11, y al 12.

□

TEOREMA 9.3

M_{12} es un subgrupo máximo de A_{12}.

Demostración: Basta probar que si $M_{12} < H$, entonces H tiene un elemento de la forma (a, b) o de la forma (a, b, c), pues por ser M_{12} 5-transitivo, H también es 5-transitivo, y contendrá a todos los 3-ciclos, y por lo tanto a todo A_{12}.

Sea $\sigma \in H^*$ que fije al 8,9,10,11, y 12 (posible por el Lema 9.2). Tenemos que la estructura de σ como producto de permutaciones ajenas debe ser una de las siguientes:

(a) Un 2-ciclo.

(b) Un 3-ciclo.

(c) Un 4-ciclo.

(d) Dos 2-ciclos.

(e) Un 5-ciclo.

(f) Un 3-ciclo y un 2-ciclo.

(g) Un 6-ciclo.

(h) Un 4-ciclo y un 2-ciclo.

(i) Dos 3-ciclos.

(j) Tres 2-ciclos.

(k) Un 7-ciclo.

(l) Un 5-ciclo y un 2-ciclo.

(m) Un 4-ciclo y un 3-ciclo.

(n) Dos 2-ciclos y un 3-ciclo.

y sólo mueve a las letras $1, 2, \ldots, 7$.

Analicemos por casos:

(a) Entonces H contiene un 2-ciclo, y hemos terminado, pues contiene a todos.

(b) Entonces H contiene a un 3-ciclo, y contiene a todos.

(c) Por transitividad, tenemos que $(1,2,3,4) \in H$, y por lo tanto

$$(1,2,3,4)^2 = (1,3)(2,4) \in H$$

y estamos en el caso *(d)*.

(d) Por 5-transitividad, conjugando con los adecuados tenemos que $(1,2)(3,4) \in H$, y $(1,2)(3,5) \in H$. Su producto es el $(3,4,5)$, que estará en H, y H contiene a todos los 3-ciclos.

(e) Por transitividad, tenemos que $(1,2,3,4,5) \in H$, y $(1,2,5,4,3) \in H$. Entonces el producto, que es igual a $(1,3,2) \in H$, y H contiene a todos los 3-ciclos.

(f) Por transitividad, $(1,2,3)(4,5) \in H$, y su cuadrado, $(1,3,2) \in H$, por lo que H contiene a todos los 3-ciclos.

(g) Tenemos a $(a,b,c,d,e,f) \in H$, y por lo tanto a $(a,d)(b,c)(e,f) \in H$, y se reduce al caso *(j)*.

(h) Tenemos a $(a,b,c,d)(e,f) \in H$, y por lo tanto a su cuadrado $(a,c)(b,d) \in H$, que lo reduce al caso *(d)*.

(i) Tenemos a $(a,b,c)(d,e,f) \in H$. Conjugando por el elemento que fija a a,b,c,d y manda e en f, tenemos también a $(a,b,c)(d,f,h) \in H$.

Si $h = e$, entonces el producto de los dos es $(a,c,b) \in H$, y H contiene a todos los 3-ciclos.

Si $h \neq e$, entonces el producto es $(a,c,h)(e,f,h)$, y multiplicar $(a,b,c)(d,f,h)$ por él nos da $(d,f)(e,h) \in H$, reduciendolo al caso *(d)*.

(j) Tenemos a $(a,b)(c,d)(e,f) \in H$. Conjugando por un elemento que fije a a,b,c,d y que no fije e ni lo mande en f, tenemos al elemento $(a,b)(c,d)(h,k)$, con $h \neq e$, $h \neq f$. Si $\{h,k\}$ es ajeno de $\{e,f\}$, el producto es un producto ajeno de dos 2-ciclos, reduciendolo al caso *(d)*. Si no es ajeno, el producto es un 3- ciclo, reduciendolo al caso *(b)*.

(k) Renumerando, podemos suponer sin perder generalidad que $(1,2,3,4,5,6,7) \in H$. Tomemos el elemento $m \in M_{12}$ que fija a $1,2,3$ e intercambia 4, y 5. Conjugando por él, tenemos a $(1,2,3,5,4,h,g) \in H$. m es de orden 2, por lo tanto hay dos casos: Si $h = 7$ y $g = 6$, entonces tenemos

$$(1,2,3,4,5,6,7)\cdot(1,2,3,5,4,7,6) = (1,3,5,2,4) \in H$$

reduciendolo al caso *(c)*. Si $h \neq 7$, entonces $g \neq 6$, y tenemos sin perder generalidad que $h = 8$ y $g = 9$, en cuyo caso

$$\Big((1,2,3,4,5,6,7)\Big)^3(1,2,3,5,4,8,9) = (1,4,7,3,6,2,5)(1,2,3,5,4,8,9)$$
$$= (1,5,7,3)(2,6)(4,8,9) \in H.$$

Si llamamos τ a dicho resultado, tenemos que $\tau^4 = (4,8,9) \in H$, y estamos en el caso *(b)*.

(l) Elevando σ al cuadrado, tenemos un 5-ciclo, y estamos en el caso *(c)*.

(m) Elevando σ a la cuarta potencia, tenemos un 3-ciclo y estamos en el caso *(b)*.

(n) Elevando σ al cuadrado, tenemos un 3-ciclo y estamos en el caso *(b)*.

En conclusión, $A_{12} < H$, con lo que probamos que M_{12} es máximo en A_{12}.

□

TEOREMA 9.4

M_{12} no tiene extensiones transitivas.

Demostración: Este resultado ya lo teníamos como consecuencia del Corolario 3.6, y de la construcción de Hall. Sin embargo, lo probaremos directamente aquí. Veremos que de hecho, no hay un grupo nítidamente 6-transitivo en 13 letras.

Un grupo nítidamente 6-transitivo en 13 letras tendría orden $13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$. Si $g \in G$ es de orden 5, entonces g es el producto de dos 5-ciclos disjuntos, pues de lo contrario fijaría $8 > 6$ letras. Denotemos los tres puntos fijos de g por a, b, c. Sea H el estabilizador en G de a, b, c. Entonces $\langle g \rangle$ es un 5-subgrupo de Sylow de H (de hecho es un 5- subgrupo de Sylow de G), y por Teorema 4.2, tenemos que el normalizador de $\langle g \rangle$ en G es 3-transitivo en las letras a, b, c.

Tenemos pues que hay un homomorfismo φ del normalizador (que denotaremos por N) en S_3, dado por la acción del normalizador en a, b, c. Sea C el normalizador de $\langle g \rangle$ en G.

En primer lugar, $C \not\subset \mathrm{Nuc}(\varphi)$. Supongamos que sí estuviera contenido. Tenemos que $S_3 = \mathrm{Im}(\varphi)$. Definiendo

$$\varphi_* : \frac{N_G(\langle g \rangle)}{C_G(\langle g \rangle)} \longrightarrow S_3$$

dado por $\varphi_*(\sigma C) = \varphi(\sigma)$, tenemos que $\frac{N}{C}$ se puede inyectar en $Aut(\langle g \rangle)$, y este último grupo es abeliano. De manera que forzamos a $\frac{N}{C}$, y por lo tanto a S_3 a ser abeliano, lo cual es una contradicción. Tenemos pues que $C \not\subset \mathrm{Nuc}(\varphi)$.

Puesto que el centro es normal en el grupo, tenemos también que $\varphi(C) \triangleleft \varphi(N)$. Pero puesto que $\varphi(N) = S_3$, y $\varphi(C) \neq \{1\}$ (pues $C \not\subset \mathrm{Nuc}(\varphi)$), tenemos que $\varphi(C) = A_3 \cong Z_3$. De ahí que 3 divida al órden de C, y tenemos un elemento $h \in C$ de orden 3.

El elemento gh tiene orden 15, puesto que g y h conmutan. Puesto que G es de grado 13, no puede ser un 15-ciclo, y su factorización como producto de ciclos ajenos debe tener tanto 5-ciclos como 3- ciclos. Tenemos sólo tres posibilidades:

(i) Dos 5-ciclos y un 3-ciclo.

(ii) Un 5-ciclo y dos 3-ciclo.

(iii) Un 5-ciclo y un 3-ciclo.

En cualquier caso, $(gh)^5$ tiene orden 3, y por lo tanto no es la identidad, y fija a más de 6 puntos, una contradicción. Por lo tanto, no existe tal G.

□

Para demostrar la simplicidad de M_{11}, y la de M_{12} de una manera distinta a la que ya dimos, se requerirán dos lemas. El primero es muy sencillo, y el segundo, conocido como el Teorema de Burnside, no se demostrará en el presente trabajo. Referimos al lector a *"An Introduction to the Theory of Groups"* de Joseph J. Rotman, pp. 156.

LEMA 9.5

(Argumento de Frattini) Sea G un grupo finito, y $K \lhd G$. Si P es un p-subgrupo de Sylow de K para algún primo p, entonces

$$G = KN_G(P).$$

Demostración: Si $g \in G$, entonces $gPg^{-1} \subset gKg^{-1} = K$. Se sigue que gPg^{-1} es un p-subgrupo de Sylow de K, y existe $k \in K$ con $kPk^{-1} = gPg^{-1}$. Entonces $P = (k^{-1}g)P(k^{-1}g)^{-1}$, y entonces $k^{-1}g \in N_G(P)$, y $g \in KN_G(P)$.

□

LEMA 9.6

(Burnside, 1900) Sea G un grupo finito y Q un subgrupo de Sylow contenido en el centro de su normalizador; entonces Q tiene un complemento normal K, que además es subgrupo característico de G.

Estamos ahora en condiciones de probar la simplicidad de M_{11}.

TEOREMA 9.7

(Cole 1896) M_{11} es un grupo simple.

Demostración: Supongamos que H es un subgrupo normal de M_{11}, con $H \neq \{1\}$. Por Teorema 2.14 H es transitivo de grado 11, y por lo tanto $|H|$ es divisible por 11. Sea P un 11- subgrupo de Sylow de H.

Puesto que 11^2 no divide al orden de M_{11}, P es un 11- subgrupo de Sylow de M_{11}, y es cíclico de orden 11.

Si $P = N_H(P)$, entonces P, siendo abeliano, es el centro de su normalizador. Por el Teorema de Burnside tenemos que P tiene un complemento normal Q en H, y por lo tanto $(11, |Q|) = 1$ y Q es característico en H; puesto que $H \lhd M_{11}$, tenemos $Q \lhd M_{11}$. El Teorema 2.14 muestra que Q es transitivo de grado 11, y por lo tanto 11 divide al orden de Q, lo cual es una contradicción. Tenemos pues que $P \neq N_H(P)$.

Calculemos ahora $N_{M_{11}}(P)$. En S_{11} hay $\frac{11!}{11} = 10!$ 11- ciclos, y por lo tanto 9! subgrupos cíclicos de orden 11, cada uno de ellos formado por la identidad y diez 11-ciclos.

Por lo tanto

$$[S_{11} : N_{S_{11}}(P)] = 9!$$

y $|N_{S_{11}}(P)| = 110$. Hay un elemento τ de orden 2 que invierte un 11-ciclo σ dado: si $\sigma = (1, \ldots, 11)$, entonces $\sigma^{-1} = \tau\sigma\tau$, con

$$\tau = (1,11)(2,10)(3,9)(4,8)(5,7);$$

notemos que τ es una permutación impar. Puesto que $M_{11} \subset A_{11}$, tenemos que

$$N_{M_{11}}(P) = N_{S_{11}}(P) \cap M_{11} \subset N_{S_{11}}(P) \cap A_{11};$$

puesto que τ es una permutación impar, tenemos que $|N_{M_{11}}(P)| = 11$ ó $|N_{M_{11}}(P)| = 55$ (los dos divisores impares de 110).

Como $P \subset N_H(P) \subset N_{M_{11}}(P)$, y vale alguna de las igualdades, $P \neq N_H(P)$ implica que $N_H(P) = N_{M_{11}}(P)$, y ambos tienen orden 55. Por el argumento de Frattini, puesto que M_{11} es finito, tenemos que

$$M_{11} = HN_{M_{11}}(P) = HN_H(P) = H$$

de manera que $M_{11} = H$ y es simple.

□

COROLARIO 9.8

M_{12} es simple.

Demostración: Es consecuencia del teorema anterior, y del Corolario 2.18.

□

Cabe hacer una pequeña pausa para hablar acerca de los grupos simples. Existen dieciocho familias infinitas de grupos simples, que en total contienen casi todos los grupos simples finitos que se conocen.

Estas 18 familias contienen a todos los grupos finitos simples, excepto por 26 grupos simples, que se conocen como **"esporádicos"**. De entre los grupos esporádicos, los cinco grupos de Mathieu (M_{11}, M_{12}, y tres grupos que no discutimos, M_{22}, M_{23}, M_{24} que actúan en 22, 23 y 24 letras respectivamente) fueron los primeros en conocerse, y durante varios años fueron los únicos grupos simples esporádicos conocidos.

Los Grupos de Mathieu están involucrados unos en otros. Hemos probado que M_{11} está contenido (de hecho doce copias de él están contenidas) en M_{12}. Se puede probar que M_{22} y M_{23} están contenidos en M_{24}, que también contiene copias homomorfas de M_{12}. M_{12} también está involucrado en el grupo de Suzuki, Sz, en el primer y tercer grupos de Conway C_1 y C_3, en el cuarto grupo de Janko J_4, y en los grupos esporádicos simples F_{22}, HN, F_{23}, F_{24}, F_2 y F_1. Bajo el apelativo "involucrado" nos referimos a que son cocientes de subgrupos del grupo dado.

Para mayor información véase el Apéndice B, y referimos al lector al *"ATLAS of Finite Groups"*, editado por J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, y R.A. Wilson.

Así como M_{12} está íntimamente relacionado con el Sistema de Steiner de tipo $S(5,6,12)$, tenemos que M_{24} es el grupo de automorfismos de un Sistema de Steiner de tipo $S(5,8,24)$ (que se puede probar es único salvo isomorfismos). En ese sistema, elegimos doce puntos de X, y consideramos los bloques que intersecan a dichos puntos en exactamente 6 puntos. Estos seis puntos dan lugar a los bloques de un $S(5,6,12)$, que definirá a M_{12} como su grupo de automorfismos.

Se puede probar que los Sistemas de Steiner de tipos $S(4,5,11)$, $S(5,6,12)$, $S(3,6,22)$, $S(4,7,23)$, y $S(5,8,24)$ son únicos salvo isomorfismos. Tendremos a los grupos de Mathieu

clasificados grupos o subgrupos de los grupos de automorfismos de estos sistemas. M_{24} es el grupo de automorfismos del $S(5,8,24)$; M_{23} del $S(4,7,23)$; M_{12} del $S(5,6,12)$ como se vió en el presente trabajo; M_{11} del $S(4,5,11)$, y M_{22} es un subgrupo de índice dos del grupo de automorfismos de un $S(3,6,22)$.

PROPOSICIÓN 9.9

M_{11} es un subgrupo máximo de M_{12}.

Demostración: Puesto que $\{1,\ldots,12\}$ es un M_{12}-conjunto multiplemente transitivo, es primitivo. Por Teorema 2.12, tenemos que el estabilizador de un punto es máximo en M_{12}, y dicho estabilizador es M_{11}.

COROLARIO 9.10

M_{12} tiene 12 subgrupos máximos simples, conjugados uno del otro, e isomorfos a M_{11}.

También hemos probado que $M_{12} < A_{12}$; que el estabilizador de tres puntos es isomorfo al producto directo de los cuaternios Q por $Z_3 \times Z_3$; y que el estabilizador de cuatro puntos es isomorfo a Q. Tenemos además que un elementos de orden dos en M_{12} que fija al menos un punto fija exactamente cuatro, y que un elemento que fija exactamente tres puntos es de orden tres.

Además hemos caracterizado a M_{12} como el único grupo nítidamente 5-transitivo no trivial, y como el grupo de automorfismos de un Sistema de Steiner de tipo $S(5,6,12)$. Así mismo está caracterizado como la única extensión transitiva del grupo M_{11}, y como la única doble extensión transitiva (i.e. extensión transitiva de la extensión transitiva) de $Sh(9)$.

Existen otros métodos para la construcción del Grupo de Mathieu M_{12}. Entre ellos cabe destacar la construcción dada por John H. Conway al considerar el grupo generado por "ciertas permutaciones bien escogidas" (Ver *"Three Lectures on Exceptional Groups"* de Conway). Tenemos también la construcción del mismo Mathieu, que consiste en "pegar" varias copias de grupos lineales fraccionarios (sin embargo, Mathieu únicamente menciona las propiedades de sus grupos sin siquiera esbozar una demostración de varias de ellas).

También se puede caracterizar al Grupo de Mathieu como el grupo de automorfismos del único código de dimensión 6, longitud 12 y peso 6 sobre $CG(3)$, conocido como el Código de Golay ternario, o a partir del Código de Golay binario, como el estabilizador de una palabra de peso 12 (el Código de Golay binario se utiliza para construír el Grupo de Mathieu de grado 24, M_{24}, en donde tenemos inmerso un grupo isomorfo a M_{12}).

M_{12} también está relacionado con el automorfismo exterior de S_6 (se sabe que S_n tiene automorfismos externos si y sólo si $n = 6$, que es un Teorema de Hölder. Véase [11], [18] y [20]), en el sentido de que M_{12} permite definir el automorfismo exterior, y el automorfismo exterior de S_6 permite construír M_{12}. Daremos un par de resultados preliminares, y por último esbozaremos la construcción del automorfismo a partir de M_{12}.

LEMA 9.11

S_n no puede actuar transitivamente en un conjunto X con t elementos, donde $2 < t < n$.

Demostración: Consideremos la representación de la acción $\varphi: S_n \to S_t$. El núcleo de dicho homomorfismo es normal en S_n, y por lo tanto es $\{1\}$, A_n ó S_n. El núcleo no puede ser S_n, pues la acción es transitiva. Si el núcleo es $\{1\}$, entonces $n \leq t$, pues φ es inyectiva. Si el núcleo es A_n, entonces la imágen de S_n es isomorfa a $\mathbb{Z}_2$, y por lo tanto $t = 2$.

□

LEMA 9.12

Si X es un G-conjunto y H es un subgrupo de G, entonces toda G-órbita se puede expresar como la unión disjunta de H-órbitas.

Demostración: Sea Gx una G-órbita, y definimos la relación de equivalencia en Gx dada por $z \sim y \iff \exists h \in H$ tal que $hz = y$. Entonces $\sim$ pártе a Gx en clases de equivalencia, que son sus H-órbitas. Basta ver que éstas coinciden con las H-órbitas de X. Pero si $z \in Gx$ está en la misma H-órbita que y, entonces z y y están en la misma G-órbita, i.e., Gx, y el resultado queda establecido.

□

DEFINICIÓN

Si X es un G–conjunto, y U es un subgrupo de G, entonces

$$F(U) = \{x \in X \mid gx = x \ \forall g \in U\}.$$

PROPOSICIÓN 9.13

Sea U un subgrupo de G, y $g \in G$. Si X es un G– conjunto, entonces $F(gUg^{-1}) = gF(U)$, y $|F(gUg^{-1})| = |F(U)|$.

Demostración: Sea $x \in F(gUg^{-1})$. Por lo tanto, $\forall u \in U$ tenemos que $(gug^{-1})(x) = x$. Por lo tanto, para toda $u \in U$, $u(g^{-1}x) = g^{-1}x$. Por lo tanto $g^{-1}x \in F(U)$.

Entonces $g(g^{-1}x) = x \in gF(U)$. Por lo tanto

$$F(gUg^{-1}) \subset gF(U).$$

Sea ahora $x \in gF(U)$. Por lo tanto, $\forall u \in U$ tenemos que $(ug^{-1})(x) = g^{-1}x$. Entonces para toda $u \in U$, $(gug^{-1})x = x$, y $x \in F(gUg^{-1})$. Por lo tanto tenemos la otra contención, y la igualdad. De la igualdad tenemos que

$$\left|F(gUg^{-1})\right| = \left|gF(U)\right| = \left|F(U)\right|.$$

□

DEFINICIÓN

Si $U < H < G$ son subgrupos, entonces H controla fusión de U sii $gUg^{-1} \subset H$ implica $\exists h \in H$ tal que $gUg^{-1} = hUh^{-1}$.

LEMA 9.14

Sea G un grupo de permutaciones y t–transitivo sobre X (con $t \geq 2$ y $|X| = n$). Sea $H = G_{x_1,\ldots,x_t}$ el estabilizador de t puntos de X, y supongamos que H controla fusión de un subgrupo U de H dado. Entonces $N_G(U)$ actúa t–transitivo en $F(U)$.

Observación. Este es un caso más general que el Lema 4.2, pues todo grupo controla fusión en su subgrupo de Sylow.

Demostración: Notemos que $\{x_1,\ldots,x_t\} \subset F(U)$ pues $U \subset H = G_{x_1,\ldots,x_t}$; de manera que $m = |F(U)| \geq t$.

Sean $y_1,\ldots,y_t$ elementos distintos entre sí de $F(U)$. Como G actúa t-transitivo en X, existe $g \in G$ tal que $gy_i = x_i$ para $i = 1,\ldots,t$. Se sigue que $gUg^{-1} \subset H$ (pues gug^{-1} fija cada x_i para toda $u \in U$).

Como H controla fusión de U, entonces existe $h \in H$ tal que $gUg^{-1} = hUh^{-1}$. Por lo tanto $h^{-1}g \in N_G(U)$, y $(h^{-1}g)(y_i) = x_i$ para cada i.

□

TEOREMA 9.15

Considere a $X = CG(9) \cup \{\infty,\omega,\Omega\}$ un M_{12} - conjunto. Entonces hay una copia isomorfa T de S_6 contenida en M_{12}, que actúa 6-transitivo en

$$\beta_0 = \{\infty,\omega,\Omega,1,-1,0\}.$$

Demostración: Por cada permutación σ de los cinco elementos $\infty,\omega,\Omega,1,-1$, la transitividad nítida de M_{12} nos da una única $\sigma' \in M_{12}$ que actúa en ellos igual que σ. La función $\sigma \mapsto \sigma'$ es un isomorfismo de S_5 con un subgrupo S de M_{12}.

Consideremos a X como un S-conjunto. ¿Cuáles son sus órbitas? Claramente una de las órbitas será $\{\infty,\omega,\Omega,1,-1\}$, de manera que nos podemos concentrar en la acción sobre el conjunto de los otros siete puntos, Y.

Sea $g \in S$ de orden 3 que permuta $\{\infty,\omega,\Omega\}$ y fije a 1 y -1. Tenemos que g debe ser el producto de tres 3-ciclos disjuntos, pues menos 3-ciclos implicarían que g fija más de cuatro puntos. De manera que las órbitas de $\langle g\rangle$ en Y deben tener los siguiente tamaños: dos de 3 y una de 1; una de 6 y una de 1; o bien una de 3 y una de 4. (S no puede actuar transitivamente en Y pues 7 no divide a $|S| = 120$). Pero puesto que S_n no puede actuar transitivamente en conjuntos con menos de n elementos por el Lema 9.11, tenemos que los tamaños de las órbitas deben ser 6 y 1.

Sea $\sigma \in S$ que corresponda a la transposición $(1,-1)$; entonces σ fija a ∞,ω,Ω, y $\sigma(\lambda) = -\lambda$ para $\lambda \in CG(9)$. El único otro punto fijo de σ es 0, de manera que $\{0\}$ debe ser la órbita de tamaño 1 para S.

Consideremos ahora a $\gamma \in M_{12}$ que fija a ∞, ω, Ω, y tal que $\gamma(\lambda) = \lambda + 1$ para $\lambda \in CG(9)$. Tenemos que γ es un elemento de orden 3 de $(M_{12})_{\infty,\omega,\Omega} = (M_{10})_\infty$. Denotemos por H a $(M_{10})_\infty$. Tenemos ya que todos los 3-elementos de H son conjugados uno del otro en H, de manera que H controla fusión de $\langle\gamma\rangle$.

Consideremos a M_{12} como 3-transitivo, con H el estabilizador de 3 puntos. El Lema 9.14 muestra que $N(\gamma)$, el normalizador de $\langle\gamma\rangle$ en M_{12} actúa 3- transitivo en $F(\langle\gamma\rangle) = \{\infty, \omega, \Omega\}$ (los elementos de orden 3 fijan a lo más a tres puntos).

Esta acción da un homomorfismo $\varphi: N(\gamma) \to S_3$, permutando a ∞, ω, Ω, que es suprayectiva, y cuyo núcleo es $N(\gamma) \cap H_\infty$. Puesto que ya tenemos descrito a H_∞, podemos calcular fácilmente que $\mathrm{Nuc}(\varphi) = \langle\gamma\rangle$; concluimos que $|N(\gamma)| = 6 \cdot 3 = 18$.

Pero podemos exhibir 18 elementos que normalizan a $\langle\gamma\rangle$. Tenemos los elementos

$$h = (\infty,\omega)(\alpha^2\lambda + \alpha\lambda^3); \qquad k = (\Omega,\omega)\lambda^3$$

dadas en la Construcción de Rotman-Witt, Teoremas 5.10 y 5.11. Tenemos que h y k conmutan con γ:

$$\begin{aligned} k\gamma &= (\Omega,\omega)(\lambda+1)^3 \\ &= (\Omega,\omega)(\lambda^3+1). \\ \gamma k &= (\Omega,\omega)(\lambda^3+1) \\ &= k\gamma. \end{aligned}$$

$$\begin{aligned} h\gamma &= (\infty,\omega)\left(\alpha^2(\lambda+1) + \alpha(\lambda+1)^3\right) \\ &= (\infty,\omega)(\alpha^2\lambda + \alpha^2 + \alpha\lambda^3 + \alpha) \\ (\text{pues } \alpha^2+\alpha = 1) \quad &= (\infty,\omega)(\alpha^2\lambda + \alpha\lambda^3 + 1). \\ \gamma h &= (\infty,\omega)(\alpha^2\lambda + \alpha\lambda^3 + 1) \\ &= h\gamma. \end{aligned}$$

además, $\langle h, k\rangle \cong S_3$. Por lo tanto $\langle\gamma, h, k\rangle = \langle\gamma\rangle \times \langle h, k\rangle$ es un subgrupo de orden 18 y que centraliza a $\langle\gamma\rangle$, y por lo tanto también lo normaliza. Como deben ser todas, además tenemos que

$$N(\gamma) = \langle\gamma, h, k\rangle.$$

Sea $T = \langle S, N(\gamma)\rangle$; ya que S es subgrupo de T, los tamaños posibles para T-órbitas en X son: dos de 6; una de 5 y una de 7; una de 11 y una de 1; una de 12 (si T es transitivo). Esto se debe a que X tiene una S-órbita de tamaño 6, y como sólo hay dos S-órbitas, hay a lo más dos T- órbitas, y una de ellas debe tener tamaño al menos 6.

No puede ser una de 5 y una de 7, pues 7 no divide a $|T|$ (ni siquiera divide a $|M_{12}|$). Tampoco puede ser una de 11 y una de 1, pues el punto fijado tendría que ser el fijado por S, a saber el 0, y el 0 se mueve bajo $\gamma \in T$. Por último, la acción no puede ser transitiva, pues los elementos de S mandan 1 en $\{\infty, \omega, \Omega, 1, -1\}$, y los elementos de $N(\gamma)$ mandan 1 en $\{1, -1, 0\}$, de manera que ningún elemento de T lo manda en, por ejemplo, i.

Concluimos que T tiene dos órbitas de tamaño 6, una de las cuales contiene a la órbita de S y debe ser

$$\beta_0 = \{\infty, \omega, \Omega, 1, -1, 0\}.$$

Entonces tenemos que T actúa transitivamente en β_0, y el estabilizador de 0 es S. Puesto que $S \cong S_5$ por contrucción y actúa nítidamente 5-transitivo en $\beta_0 - \{0\}$, tenemos que T actúa nítidamente 6-transitivo en β_0, y $T \cong S_6$.

□

De hecho, este bloque β_0 se puede utilizar para definir un $S(5,6,12)$, donde los bloques serán los conjuntos de la forma $g\beta_0$, con $g \in M_{12}$.

Esbozamos ahora la prueba de la existencia del automorfismo externo para S_6. Hay dos T-órbitas de tamaño 6 en X, digamos β_0 (la dada), y β_1. Un elemento $\sigma \in T$ de orden 5 es el producto de dos 5-ciclos disjuntos y fija a dos puntos; cada β_i (con $i = 0, 1$), consiste de una σ-órbita de tamaño 5 y una de tamaño 1. Considerando a M_{12} como 2- transitivo, notemos que $\langle\sigma\rangle \subset M_{10}$, el estabilizador de dos puntos; como $\langle\sigma\rangle$ es un 5-subgrupo de Sylow de M_{10}, tenemos por Lema 9.14 que $N(\sigma)$, el normalizador de $\langle\sigma\rangle$ in M_{12} actúa dos transitivo en el conjunto $F(\langle\sigma\rangle)$ de dos puntos. Por lo tanto existe un elemento $\tau \in N(\sigma)$, de orden 2. Se prueba que τ intercambia β_0 con β_1, y por lo tanto normaliza a T, y la conjugación por τ es un automorfismo externo de T, que nos da un automorfismo externo en S_6.

Por último, mencionamos que uno puede probar que hay un subgrupo G de M_{24} con $G \cong M_{12}$, y que hay dos G-órbitas de tamaño 12 en el conjunto de acción de M_{24}. Empezando con $g \in G$ de orden 11, con un argumento similar al dado arriba se prueba que hay un elemento de orden dos $\gamma \in N(g)$ que intercambia las dos G-órbitas, y que normaliza a G. La conjugación por γ da un automorfismo externo para M_{12}.

X. Bibliografía

[1] Cannon, John. *CAYLEY: A Language for Group Theory.* Department of Pure Mathematics, University of Sydney. 1981.

[2] Cárdenas, Humberto—Lluis, Emilio. *On the* $(5,6,12)$*-Steiner System.* Publicaciones Preliminares **208**, Instituto de Matemáticas. 1992.

[3] Cárdenas, Humberto—Lluis, Emilio. *On the Mathieu Group* M_{12}. En Preparación.

[4] Cárdenas, Humberto—Lluis, Emilio. Comunicaciones personales sobre generadores de M_{12}.

[5] Conway, J.H. *Three Lectures on Exceptional Groups.* En "Finite Simple Groups", Powell and Higman, eds, pp. 215–247. Academic Press, 1971.

[6] Conway, J.H—Curtis, R.T.—Norton, S.P.— Parker, R.A.—Wilson, R.A. *ATLAS of Finite Groups.* Oxford University Press, 1985.

[7] Curtis, R.T. *A New Combinatorial Approach to* M_{24}. Mathematical Procedures of the Cambridge Philosophical Society **79**, pp. 25–42. 1976.

[8] Curtis, R. T. *Natural Constructions of the Mathieu Groups.* Mathematical Procedures of the Cambridge Philosophical Society **106**, pp. 423–429. 1989.

[9] Curtis, R.T. *Geometric Interpretations of the 'Natural' Generators of the Mathieu Groups.* Mathematical Procedures of the Cambridge Philosophical Society **107**, pp. 19–26. 1990.

[10] Gardner, Martin. *The Capture of a Monster: A Mathematical Group with a Ridiculous Number of Elements.* En "Mathematical Games". Scientific American, Junio 1980.

[11] Hall Jr., Marshall. *The Theory of Groups.* MacMillan Co., 1959, pp. 72–81.

[12] Hölder, O. *Bildung Zusammengesetzter Gruppen.* Math. Annalen **46**, pp. 321–422. 1895.

[13] Holyoke, T.C. *On the Structure of Multiply Transitive Permutation Groups.* American Journal of Mathematics **74**, pp. 787– 796. 1952.

[14] Jordan, Camille. *Recherches sur les Substitutions.* Journal de Mathématiques Pures et Appliquées **17**, pp. 351–367. 1872.

[15] Jordan, Camille. *Traité de Substitutions et des Équations Algébriques.* Paris, 1870.

[16] Mathieu, E. *Mémoire sur l'étude des fonctions de plusieurs quantités.* Journal de Mathématiques Pures et Appliquées **6**, pp. 241-243. 1861.

[17] Mathieu, E. *Sur la fonctions cinq fois transitive de 24 quantités.* Journal de Mathématiques Pures et Appliquées **18**, pp. 24-46. 1873.

[18] Miller, Donald W. *On a Theorem of Hölder.* American Mathematical Monthly **65**, pp. 253-254. 1958.

[19] Newman, James R., editor. *The Supreme Art of Abstraction: Group Theory.* En "The World of Mathematics" Vol III. Simon & Schuster, pp. 1534-1537. 1956.

[20] Rotman, Joseph J.—Janusz, Gerald. *Outer Automorphisms of S_6.* American Mathematical Monthly **89** pp. 407-410. 1982.

[21] Rotman, Joseph J. *An Introduction to the Theory of Groups, 3rd edition.* Allyn and Bacon, Inc., pp 158-240. 1984.

[22] Witt, E. *Die 5-fach Transitiven Gruppen von Mathieu.* Abh. Math. Sem. Hamburg **12**, pp. 256-264. 1938.

[23] Witt, E. *Über Steinersche Systeme.* Abh. Math. Sem. Hamburg **12**, pp. 265-275. 1938.

Apéndice A

A Simple Ballad

What are the orders of all simple groups?
I speak of the honest ones, not of the loops.
It seems that old Burnside their orders has guessed
Except for the cyclic ones, even the rest.

Groups made up with permutes will produce some more:
For A_n is simple, if n exceeds 4.
Then, there was Sir Mathieu who came into view
Exhibiting groups of an order quite new.

Still others have come on to study this thing.
Of Artin and Chevalley now we shall sing.
With matrices finite they made quite a list,
The question is: Could there be others they've missed?

Suzuki and Ree then maintained it's the case
That these methods had not reached the end of the chase.
They wrote down some matrices, just four by four,
That made up a simple group. Why not make more?

And then came the opus of Thompson and Feit
Which shed on the problem remarkable light.
A group, when the order won't factor by two,
Is cyclic or solvable. That's what is true.

Suzuki and Ree had caused eyebrows to raise,
But the theoreticians they just couldn't faze.
Their groups were not new: if you added a twist,
You could get them from old ones with a flick of the wrist.

Still, some hardy souls felt a thorn in their side.
For the five groups of Mathieu all reason defied:
Not A_n, not twisted, and not Chevalley,
They called them sporadic, and filed them away.

Are Mathieu groups creatures of heaven or hell?
Zvonimir Janko determined to tell.
He found out what nobody wanted to know:
The masters had missed 1 7 5 5 6 0.

The floodgates were opened! New groups were the rage!
(And twelve or more sprouted, to greet the new age.)
By Janko, and Conway, and Fischer, and Held,
McLaughlin, Suzuki, and Higman, and Sims.

No doubt you noted the last lines don't rhyme.
Well, that is, quite simply, a sign of the time.
There's chaos, not order, among simple groups;
and maybe we'd better go back to the loops.

Apéndice B

La Tabla 1 contiene los nombres, ordenes y descubridores de los 26 grupos simples finitos esporádicos que existen. Los primeros cinco grupos se conocen como **Grupos de Mathieu** en 11, 12, 22, 23, y 24 letras respectivamente. Los siguientes cuatro se conocen como los cuatro grupos de Janko, independientemente de su descubridor, pues fueron todos propuestos por Janko.

El siguiente es el grupo de Higman–Sims (HS), y viene seguido de el grupo de McLaughlin y el de Suzuki. Posteriormente siguen los tres grupos de Conway, y el grupo de Held. Tenemos despues los grupos de Fischer en 22, 23 y 24 letras. Sigue el grupo de Lyons, el de O'Nan y el de Rudvalis.

Despues tenemos los grupos de Fischer de grado 5, 3, 2 y 1. El último, F_1, se conoce como el **monstruo** debido a su gran tamaño: tiene

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

elementos. F_2 es a veces llamado el **bebé monstruo**. F_1 es a veces denotado tambien por M, y F_2 por B.

La Tabla 2 contiene la información sobre cómo están involucrados los grupos esporádicos simples unos en otros. Para cada grupos simple esporádico G, nos preguntamos cuáles de los esporádicos más pequeños están involucrados en él (i.e. son cocientes de un subgrupo de G). En la tabla la entrada en el renglón de G y la columna de S es:

- $+$ si S está involucrado en G.
- $-$ si S no está involucrado en G.
- ? si no sabemos ($S \cong J_1$, $G \cong F_1$)

Si J_1 está involucrado en F_1, entonces debe ser un subgrupo máximo.

TABLA 1

Grupos Finitos Simples Esporádicos

Nombre del Grupo	Número de Elementos	Descubierto por
M_{11}	$2^4 \times 3^2 \times 5 \times 11$	E. Mathieu
M_{12}	$2^6 \times 3^3 \times 5 \times 11$	E. Mathieu
M_{22}	$2^7 \times 3^2 \times 5 \times 7 \times 11$	E. Mathieu
M_{23}	$2^7 \times 3^2 \times 5 \times 7 \times 11 \times 23$	E. Mathieu
M_{24}	$2^{10} \times 3^3 \times 5 \times 7 \times 11 \times 23$	E. Mathieu
J_1	$2^3 \times 3 \times 5 \times 7 \times 11 \times 23$	Janko
J_2	$2^7 \times 3^3 \times 5^2 \times 7$	Hall, Wales
J_3	$2^7 \times 3^5 \times 5 \times 17 \times 19$	Higman, McKay
J_4	$2^{21} \times 3^3 \times 5 \times 7 \times 11^3 \times 23 \times$ $\times 29 \times 31 \times 37 \times 43$	Benson, Conway, Janko Norton, Parker, Thackray
HS	$2^9 \times 3^2 \times 5^3 \times 7 \times 11$	Higman, Sims
MC	$2^7 \times 3^6 \times 5^3 \times 7 \times 11$	McLaughlin
Sz	$2^{13} \times 3^7 \times 5^2 \times 7 \times 11 \times 13$	Suzuki
C_1	$2^{21} \times 3^9 \times 5^4 \times 7^2 \times 11 \times 13 \times 23$	Conway
C_2	$2^{18} \times 3^6 \times 5^3 \times 7 \times 11 \times 23$	Conway
C_3	$2^{10} \times 3^7 \times 5^3 \times 7 \times 11 \times 23$	Conway
He	$2^{10} \times 3^3 \times 5^2 \times 7^3 \times 17$	Held, Higman, McKay
F_{22}	$2^{17} \times 3^9 \times 5^2 \times 7 \times 11 \times 13$	Fischer
F_{23}	$2^{18} \times 3^{13} \times 5^2 \times 7 \times 11 \times 13 \times 17 \times$ $\times 23$	Fischer
F_{24}	$2^{21} \times 3^{16} \times 5^2 \times 7^3 \times 11 \times 13 \times 17 \times$ $\times 23 \times 29$	Fischer
Ly	$2^8 \times 3^7 \times 5^6 \times 7 \times 11 \times 31 \times 37 \times$ $\times 67$	Lyons, Sims
O	$2^9 \times 3^4 \times 5 \times 7^3 \times 11 \times 19 \times 31$	O'Nan, Sims
R	$2^{14} \times 3^3 \times 5^3 \times 7 \times 13 \times 29$	Conway, Rudvalis, Wales
F_5	$2^{14} \times 3^6 \times 5^6 \times 7 \times 11 \times 19$	Smith, Thompson
F_3	$2^{15} \times 3^{10} \times 5^3 \times 7^2 \times 13 \times 19 \times 37$	Smith, Thompson
F_2	$2^{11} \times 3^{13} \times 5^6 \times 7^2 \times 11 \times 13 \times 17 \times$ $\times 19 \times 23 \times 31 \times 47$	Fischer, Leon, Sims
F_1	$2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times$ $\times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$	Fischer, Griess

TABLA 2

Cómo están Involucrados los Grupos Simples Esporádicos unos en otros

	M_{11}	M_{12}	J_1	M_{22}	J_2	M_{23}	HS	J_3	M_{24}	MC	He	R	Sz	O	C_3	C_3	F_{22}	HN	Ly	F_3	F_{23}	C_1	J_4	F_{24}	F_2	F_1
M_{11}	·	M_{12}																								
M_{12}	+	·	J_1																							
J_1	−	−	·	M_{22}																						
M_{22}	−	−	−	·	J_2																					
J_2	−	−	−	−	·	M_{23}																				
M_{23}	+	−	−	+	−	·	HS																			
HS	+	−	−	+	−	−	·	J_3																		
J_3	−	−	−	−	−	−	−	·	M_{24}																	
M_{24}	+	+	−	+	−	+	−	−	·	MC																
MC	+	−	−	+	−	−	−	−	−	·	He															
He	−	−	−	−	−	−	−	−	−	−	·	R														
R	−	−	−	−	−	−	−	−	−	−	−	·	Sz													
Sz	+	+	−	−	+	−	−	−	−	−	−	−	·	O												
O	+	−	+	−	−	−	−	−	−	−	−	−	−	·	C_3											
C_3	+	+	−	+	−	+	+	−	−	+	−	−	−	−	·	C_3										
C_2	+	−	−	+	−	+	+	−	−	+	−	−	−	−	−	·	F_{22}									
F_{22}	+	+	−	+	−	−	−	−	−	−	−	−	−	−	−	−	·	HN								
HN	+	+	−	+	−	−	+	−	−	−	−	−	−	−	−	−	−	·	Ly							
Ly	+	−	−	+	−	−	−	−	−	+	−	−	−	−	−	−	−	−	·	F_3						
F_3	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	·	F_{23}					
F_{23}	+	+	−	+	−	+	−	−	−	−	−	−	−	−	−	−	+	−	−	−	·	C_1				
C_1	+	+	−	+	+	+	+	−	+	+	−	−	+	−	+	+	−	−	−	−	−	·	J_4			
J_4	+	+	−	+	−	+	−	−	+	−	−	−	−	−	−	−	−	−	−	−	−	−	·	F_{24}		
F_{24}	+	+	−	+	−	+	−	−	+	−	+	−	−	−	−	−	+	−	−	−	+	−	−	·	F_2	
F_2	+	+	−	+	−	+	+	−	−	+	−	−	−	−	−	+	+	+	−	+	+	−	−	−	·	F_1
F_1	+	+	?	+	+	+	+	−	+	+	+	−	+	−	+	+	+	+	−	+	+	+	−	+	+	·