BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS FÍSICO-MATEMÁTICAS

Título de la tesis:

"JUEGOS Y TEORÍA DE GRUPOS"

Presenta:

Irene Carmona Sánchez

Para obtener el título de:

LICENCIADA EN MATEMÁTICAS

Director de tesis:

Lic. Pablo Rodrigo Zeleny Vázquez

PUEBLA, PUE. *Agosto 2013*

Jurado

Dr. José Dionicio Zacarías Flores
Dra. Olga Leticia Fuchs Gómez
Dra. María Teresa Torrijos Muñoz

Dedicatoria

A mis padres.

A mi gran inspiración durante estos 9 años, Oscar G. De Maria, muchas gracias por todo tu apoyo, cariño, y respeto. Por estar siempre pendiente de mí durante todo este tiempo, conoces mis sueños y las metas que quiero cumplir desde que estaba en el bachillerato, gracias por acompañarme en esta meta, por escucharme, por enseñarme a ser mejor cada día, por ayudarme a crecer como persona, por ser el mejor ejemplo a seguir, por darme alegrías y fuerzas para cumplir mis sueños, te quiero. Me da mucha alegría y orgullo el terminar el presente trabajo, se los dedico con todo mi cariño.

Agradecimientos

En primer lugar quiero dar gracias a Dios por permitirme elaborar el presente trabajo, por todas las bendiciones que he recibido durante toda la carrera y por haberme permitido conocer a mis maestros y amigos que me han ayudado a crecer profesionalmente y a ser una mejor persona.

A mis padres Ramiro y Juanita, por todo el apoyo incondicional que me han brindado desde el primer momento que decidí estudiar la Licenciatura en Matemáticas, por su cariño, confianza y comprensión, gracias papá, gracias mamá por creer en mí, por apoyarme económicamente cuando lo necesitaba y sobre todo muchas gracias por levantarme el ánimo en las ocasiones en las que sentía que no lograría la meta, todo lo que he logrado se los debo a ustedes.

A mi hermana Angélica, por su cariño, apoyo, sus porras y sus críticas.

A Nayelli Nava por tu amistad incondicional, tu cariño, por la gran responsabilidad que muestras en tus estudios y que hizo no me rindiera en cada paso de esta meta.

A mi primo Ian Sánchez, por su apoyo incondicional, por su buen ejemplo y sus valiosos consejos.

A mi asesor de tesis: Pablo Rodrigo Zeleny Vázquez, por darme la oportunidad de trabajar con él, por su gran apoyo en todo momento, por sus valiosos comentarios, sus observaciones, por corregir mis errores para realizar un mejor trabajo, por su comprensión, sobre todo muchas gracias por siempre mostrar entusiasmo en la realización de este trabajo, por siempre estar al pendiente de los materiales que se necesitaran para la elaboración del mismo, por ser el mejor ejemplo, por apoyarme en todo momento para el siguiente paso que es la Maestría, por el tiempo dedicado a este trabajo, por siempre crear un ambiente de respeto, confianza y amistad, por compartir su conocimiento, sus ideas, por guiarme cuando lo necesitaba, por mostrarnos en los diferentes cursos de la carrera su agrado hacia las matemáticas, por sus enseñanzas, por su profesionalismo, por mostrarnos que las matemáticas aparte de ser abstractas también son divertidas, no olvidaré sus valiosos consejos y observaciones, ha sido un gran honor el trabajar con usted. ¡Gracias maestro¡

A mis sinodales por apoyarme desde el primer momento en que les describí el presente trabajo, gracias por su guía y sus observaciones, por corregir

mis errores, por siempre compartir su conocimiento y experiencia profesional.
Dr. José Dionicio Zacarías Flores, gracias maestro por el tiempo dedicado en la revisión de la tesis, por brindarme su apoyo y sus valiosos consejos en el siguiente paso que es la maestría, por sus enseñanzas durante la carrera, por siempre mostrar en los diferentes cursos su interés por mejorar nuestra educación, por guiarme y corregirme cuando lo necesitaba siempre en un ambiente de confianza y respeto, por ser un ejemplo a seguir y por siempre mostrar su dedicación y su profesionalismo.
Dra. Olga Leticia Fuchs Gómez, gracias por darme guía y soporte desde el primer curso de la carrera, nunca olvidaré los primeros 6 cursos de la carrera, gracias a usted y a su trabajo permanecí en la facultad, mucho de lo que he logrado se lo debo a usted, gracias por sus enseñanzas, por exigirnos pero a la vez no dejarnos solos, porque al formar profesionales también forma seres humanos, por siempre compartir y transmitir su conocimiento, sus ideas, gracias por brindarme su confianza y amistad desde el primer día que entre a la facultad, por preocuparse por nuestra educación, por corregirme y sobre todo por ser el mejor ejemplo a seguir. ¡Gracias!
Dra. María Teresa Torrijos Muñoz, gracias por brindarme su confianza ya que desde el primer momento que le pedí que fuera mi sinodal acepto revisar el presente trabajo, por siempre compartir su experiencia profesional, por sus valiosos consejos y observaciones desde el primer momento que tuve la oportunidad de trabajar con usted, gracias por transmitir su dedicación, responsabilidad y el respeto hacia su trabajo, es un gran ejemplo a seguir.
Al Maestro Jaime Arroyo, recuerdo que cuando le comente que tenía dificultades en Teoría de grupos, que quería comprender cada concepto del curso y le pedí que me permitiera tomar el curso de oyente así como presentar los exámenes usted me dijo que ¡claro que sí! Y gracias a sus enseñanzas y a su dedicación, me agradó cada vez más ésta parte de las matemáticas, gracias maestro, este trabajo también es dedicado a usted. Gracias por exigirnos dar lo mejor de nosotros y no darnos por vencidos.
Un agradecimiento especial a Rafael García por ayudarme a conseguir los puzzles los cuales me permitieron mostrar algunas de sus estrategias en el presente trabajo y a Mauricio Rodríguez por compartir algunos de sus algoritmos para la mejora en la resolución de los puzzles.

A Nayelli Nava, Israel Méndez, Juan Manuel Contreras, Guztavo Meza y Yazmin Vázquez por su gran apoyo y sus críticas constructivas durante la elaboración de la tesis. Gracias hermanitos por todo su apoyo incondicional.

A mis grandes amigos que en realidad ahora considero una familia, por todo su apoyo durante toda la carrera, por las porras, por las críticas, por la buena vibra, por apoyarme en las buenos y en las malas, por todos los momentos de alegría que compartimos durante la carrera, por escucharme y por aconsejarme cuando lo necesitaba, gracias por compartir su conocimiento y su amistad:

Marisol Lucas
Nantzy Tecuanhuey
Socorro Zaragoza
Juan Manuel Contreras
José Luis Ramos (Mecatrónica)
Israel Méndez
Guztavo Meza
Abel Jesús Morales
Angel Rodríguez
Rebeca Zambrano
Yazmin Vázquez
Mario A. López
Rene Contreras
Atayan García
Viridiana Galicia
Iván Cortés (Computación)
Ricardo Mejía (Física)
Paulina Zeleny (Química)
Mayra Alejandra Herrera
Vanesa Nava
Erika Cervantes (Física)
Ivett Ortega

A la directora de Liceo Serdán Consuelo Diana Muñoz Ávalos, gracias por darme la oportunidad de trabajar con ustedes durante el ciclo escolar 2012-2013, por sus valiosas observaciones y consejos, por la confianza y por siempre estar al pendiente de mi progreso en la tesis, sobre todo por ayudarme con los horarios y así poder realizar la misma, finalmente a mis alumnos de Liceo Serdán-Secundaria y Bachillerato por todo su apoyo, por realizar un buen trabajo durante el ciclo escolar, en especial al grupo primero A de nivel secundaria, gracias por todos sus buenos deseos en la culminación del presente trabajo.

Gracias.

ÍNDICE

INTRODUCCIÓN *10*

Capítulo 1 ..... *13*

VOLTEO DE CAMPANAS Y PERMUTACIONES *13*

1.1 *Permutaciones* *13*

1.2 *Inversos* *16*

1.3 *Notación cíclica* *21*

1.4 *Un algoritmo para listar todas las permutaciones* *26*

1.5 *Permutaciones y volteo de campanas* *28*

Capítulo 2 ..... *33*

PUZZLES DE PERMUTACIÓN *33*

2.1 *Puzzle 15* *34*

2.2 *Rainbow Masterball* *35*

2.3 *Cubos de Rubik* *38*

2.4 *Pyraminx* *42*

Capítulo 3 ..... *44*

¿QUÉ ES CONMUTATIVIDAD? *44*

3.1 *Cuaterniones* *45*

3.2 *Grupos cíclicos finitos* *45*

3.3 *El grupo diedro* *46*

3.4 *El grupo simétrico* *48*

3.5 *Subgrupos* *54*

3.6 *Ejemplos* *56*

3.7 *Conmutadores* *59*

3.8 *Conjugación* *62*

3.9 *Órbitas y acciones* *64*

3.10 *Clases laterales* *67*

3.11 *Campanología, revisión* *71*

3.12 *Algoritmo de Dimino* *71*

Capítulo 4 ..... *73*
ALGORITMO DE DIOS Y GRAFOS *73*
4.1 *En el principio…* *73*
4.2 *Grafos de Cayley* *74*
4.3 *Algoritmo de Dios* *76*
4.4 *El grafo del Puzzle 15* *77*
Capítulo 5 ..... *82*
SIMETRÍA Y LOS SÓLIDOS PLATÓNICOS *82*
5.1 *Descripciones* *82*
5.2 *Antecedentes de simetrías en el espacio tridimensional* *84*
5.3 *Simetrías del tetraedro* *86*
5.4 *Simetrías del cubo* *87*
5.5 *Simetrías del dodecaedro* *89*
5.6 *Algunas reflexiones sobre el icosaedro* *91*
Capítulo 6 ..... *93*
EL GRUPO CUBO ILEGAL *93*
6.1 *Homomorfismos* *93*
6.2 *Acciones en un grupo* *96*
6.3 *Cuando dos grupos son realmente el mismo* *97*
6.4 *Kernels son normales, algunos subgrupos no* *101*
6.5 *Grupos cociente* *103*
6.6 *Incursionando en productos directos* *105*
6.7 *Una mezcla heterogénea de productos semi-directos* *111*
6.8 *Productos corona* *113*
Capítulo 7 ..... *117*
EL GRUPO CUBO DE RUBIK (LEGAL) *117*
7.1 *Descripción matemática de los movimientos del cubo* $\mathbf{3 \times 3 \times 3}$ *117*
7.2 *Estructura del grupo cubo* *121*
7.3 *Los movimientos de orden 2* *126*
Capítulo 8 ..... *129*
ALGUNAS ESTRATEGIAS DE SOLUCIÓN *129*

8.1 *Una estrategia para resolver el Cubo de Rubik* $\mathbf{2 \times 2 \times 2}$ *129*

8.2 *Una estrategia para resolver el Cubo de Rubik* $\mathbf{3 \times 3 \times 3}$ *133*

8.3 *El método de subgrupo* *136*

8.4 *Una estrategia para resolver el Cubo de Rubik* $\mathbf{4 \times 4 \times 4}$ *138*

8.5 *Una estrategia para resolver el Pyraminx* *149*

Anexo *154*

Reflexión final *157*

Bibliografía *158*

Créditos de figuras *160*

INTRODUCCIÓN

¿Quién no ha intentado resolver juegos como el Cubo de Rubik o el Puzzle 15? Es sorprendente la matemática implícita que nos ofrecen varios juguetes de este tipo. En este trabajo hablaremos de la teoría grupos aplicada a algunos juegos, como el Cubo de Rubik, el Puzzle 15 y el Pyraminx, el objetivo principal es explicar cómo se resuelven ya que lejos de pasar de moda surgen nuevas variantes. Nos basamos en el texto de David Joyner: "Adventures in Group Theory" y consultamos varios autores entre ellos D. Singmaster, J. J. Rotman, I. N. Herstein, D.A.R. Wallace, y J. Durbin.

¿Por qué resulta fascinante el Cubo de Rubik? Dejemos que su autor nos explique:

"Para mí este objeto es un ejemplo admirable de la belleza rigurosa, de la gran riqueza de las leyes naturales; es un ejemplo sorprendente de las posibilidades admirables del espíritu humano para probar su rigor científico y para dominar esas leyes... Es el ejemplo de la unidad de lo verdadero y de lo bello, lo que para mí significan la misma cosa. Todo esto podría parecer exagerado a propósito de un simple juguete, pero confío en que quienes, aprovechando sus posibilidades, intenten penetrar en este mundo científico y asimilarlo, harán descubrimientos y serían de mi opinión. Mi convicción íntima es que jugando con él, reflexionando sobre él, podemos alcanzar algo de la lógica pura del Universo, de su esencia sin límites, de su movimiento perpetuo en el espacio y en el tiempo." [A]

La primera vez que intente resolverlo, no fue nada fácil, pero cuando entendí su construcción y después de varios meses de preparar esta tesis ya soy capaz de explicar cómo se resuelve, porque no existe método sencillo para resolverlo y esto alimenta la curiosidad.

En el capítulo 1 revisamos algunos conceptos y notación sobre permutaciones, también hablaremos del volteo de campanas (pasatiempo inglés) que consiste en hacer sonar varias campanas permutándolas en cierto orden. El Plan Bob Minimus es un método para recordar las 24 permutaciones posibles de cuatro campanas en una secuencia que puede recodarse usando las 24 simetrías de un cubo (ver *Figura 1b*). Veremos cómo las secuencias del Plan Bob Minimus actúan como un puente entre el mundo matemático de rotaciones de un cubo y el mundo de la música en este caso a través del volteo de campanas.

Figura* 1*a

Figura* 1*b

Figura 1c

Figura 1d

En el capítulo 2 consideramos un tipo especial de juegos para una sola persona conocidos como puzzles, por ejemplo el Puzzle 15, que no corresponde a la traducción literal como "rompecabezas" (que consiste en armar una imagen con muchas piezas). Explicamos las características del puzzle en su sentido original que incluye mover piezas como el juego del 15 (ver *Figura 1e*) donde cada movimiento tiene un inverso, es decir existe otro movimiento que reestablece el puzzle a la posición de la que se había partido. Veremos cómo cada movimiento básico de los puzzles puede ser descrito usando notación cíclica disjunta para permutaciones.

Figura 1e

También hablamos brevemente del juego conocido como Rainbow Masterball y el Cubo de Rubik $2 \times 2 \times 2, 3 \times 3 \times 3$ *y* $4 \times 4 \times 4$.

En el capítulo 3 revisamos algunas definiciones y teoremas básicos de Teoría de Grupos, continuando con la introducción de terminología que nos permita analizar puzzles de permutación matemáticamente y los tipos de grupos que surgen al analizar el Cubo de Rubik, introducimos el concepto de conmutador, finalmente volvemos al volteo de campanas visto en capítulo 1, en el contexto de la teoría de grupos.

En el capítulo 4 introducimos una interpretación de un grupo de permutación desde el punto de vista de la teoría de grafos. Uno de los objetivos de los aficionados de los puzzles es encontrar el número de movimientos en la mejor solución posible a partir del peor caso, esto en matemáticas se conoce como el diámetro del grafo Cubo de Rubik, revisaremos los logros de muchas personas que han trabajado en el "algoritmo de Dios" para el Cubo de Rubik

$3\times 3\times 3$, así como los diámetros que han sido encontrados para el Cubo $2\times 2\times 2$ y el Pyraminx.

En el capítulo 5 hablaremos acerca de las simetrías de algunos poliedros regulares, sabemos que el Cubo de Rubik $3\times 3\times 3$ está cortado por seis planos paralelos a las caras, que el Pyraminx es un puzzle tetraédrico, similar en algunos aspectos, pero en otros es diferente al Cubo de Rubik, el estudiar la simetría hexaédrica y tetraédrica nos permitirá entender la construcción mecánica del Cubo de Rubik y del Pyraminx.

En el capítulo 6 veremos brevemente homomorfismos entre grupos, acciones en un grupo, productos directos de grupos. Un ejemplo importante será el estudio del grupo slice (generado por los movimientos de los cortes medios del cubo) que es más fácil de analizar que el grupo Cubo de Rubik en sí mismo.

En el capítulo 7 describiremos matemáticamente los movimientos del cubo $3\times 3\times 3$ como orientaciones esquina y orientaciones arista. Al tratar de resolver el Cubo de Rubik se presentan situaciones cómo ¡necesito mover 3 subcubos de una cara, que están en los cortes medios! ¿Encontraré algún movimiento que me permita moverlos sin afectar el resto del cubo? En este capítulo consideraremos este tipo de cuestiones.

El capítulo 8 incluye algunas estrategias para resolver el Pyraminx, el Cubo de Rubik $2\times 2\times 2, 3\times 3\times 3$, y el $4\times 4\times 4$. Además, se analizan algunas de las ideas matemáticas detrás de los algoritmos utilizados, cómo movimientos que nos permiten permutar esquinas y aristas cíclicamente dejando el resto del cubo fijo, el uso de algunos conmutadores elegidos cuidadosamente, movimientos torsión esquina, movimientos flip que nos permiten voltear aristas, es decir invertir el color de las etiquetas de una arista, para resolver el Cubo de Rubik. Comparamos la estructura mecánica del cubo $2\times 2\times 2, 3\times 3\times 3$, el $4\times 4\times 4$ y determinamos que hay alguna relación en la solución de estos.

La presente tesis podría usarse como auxiliar en un curso introductorio de Teoría de Grupos por ello se incluyen algunos problemas o como lectura adicional para los interesados en el tema. Al intentar resolver el Cubo de Rubik utilizamos las definiciones básicas de teoría de grupos, "ya no caen del cielo", es decir es más fácil introducirlas en el contexto de juegos.

Nota: las referencias bibliográficas se indican con [ ] por ejemplo [Si] se refiere a Singmaster D.

Capítulo 1

Volteo de campanas y permutaciones

En este capítulo se introducen algunas definiciones sobre permutaciones y combinatoria, notación, símbolos y propiedades básicas deben ser recordadas para mayor claridad. Todo mundo conoce el Cubo de Rubik, nuestra intención es aplicar los conceptos de teoría de grupos a la solución del Cubo de Rubik, por ejemplo al mover las caras del cubo las estamos permutando, el objetivo es no perder de vista la reorganización de los objetos, (las caras de un Cubo de Rubik), que cambian cada vez que hacemos un movimiento, posteriormente veremos los detalles (hay diferentes versiones $2 \times 2, 3 \times 3, 4 \times 4$, fáciles de conseguir). En este capítulo también hablaremos de un pasatiempo inglés que se remonta a más de 300 años: el volteo de campanas, que también aplica permutaciones siguiendo un "plan".

1.1 Permutaciones

Supongamos que se mezcla un paquete de cartas. Simplemente reorganizamos las 52 cartas. La equivalencia matemática de barajar es una permutación.

Sea $\mathbb{Z}_n = \{1,2, \dots, n\}$ el conjunto de los enteros desde 1 hasta n, donde n es un entero positivo. Una **permutación** de $\mathbb{Z}_n$ es una biyección de $\mathbb{Z}_n$ sobre sí mismo.

Por otro lado si T es cualquier conjunto finito entonces una permutación de T es una biyección de T sobre sí mismo. En el caso de que T tenga n elementos, podemos denotar los elementos de T por $T = \{t_1, \dots, t_n\}$ consideramos una permutación como una función $f: T \to T$ con $f(t_i) = t_j$ Pero por brevedad consideramos otra función ϕ, $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ donde $f(t_i) = t_j$ si y sólo si $\phi(i) = j$.

En otras palabras, una vez que denotamos los elementos de T, existe una correspondencia inyectiva entre las permutaciones de T y las de $\mathbb{Z}_n$. Dado que los elementos de $\mathbb{Z}_n$ son más fáciles de escribir (menos subíndices), a menudo sólo trabajamos con $\mathbb{Z}_n$.

Como un ejemplo, en el Cubo de Rubik 3×3 hay $9 \cdot 6 = 54$ caritas. Si numeramos las caritas del $1,2, \dots, 54$ (en cualquier forma que desee), cualquier movimiento del Cubo de Rubik corresponde a una permutación de $\mathbb{Z}_{54}$.

Notación: Podemos denotar una permutación $f : \mathbb{Z}_n \to \mathbb{Z}_n$ por una matriz $2 \times n$:

$$f \leftrightarrow \begin{pmatrix} 1 & 2 & \dots & n \\ f_1 & f_2 & \cdots & f_n \end{pmatrix}$$

Donde $f_1, f_2, \dots, f_n$ es simplemente un reordenamiento (en algún orden dependiendo de f) de enteros $1,2, \dots, n$. Esta notación significa que f envía 1 a f_1, f envía 2 a f_2, ..., f envía n a f_n. En otras palabras, $f_1 = f(1)$, $f_2 = f(2), \dots, f_n = f(n)$, y $f_i \neq f_j$, a menos que $i = j$.

Nota: Utilizo la notación de David Joyner

Ejemplo 1.1.1.

(a) La permutación **identidad**, denotado por I, es la permutación que no hace cambios:

$$I = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

(b) La permutación $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ definida por

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

intercambia 1 y 3 y deja al 2 igual.

El **n-ciclo** es una permutación que permuta los valores cíclicamente:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 2 & 3 & \dots & 1 \end{pmatrix}$$

La permutación $\begin{pmatrix} 1 & 2 & \dots & n \\ n & 1 & \dots & n-1 \end{pmatrix}$

también es llamada un **n-ciclo**.

Definición 1.1.1. Sea $f : \mathbb{Z}_n \to \mathbb{Z}_n$ una permutación y sea

$$e_f(i) = card\{j > i \mid f(i) > f(j)\}, \qquad 1 \le i \le n-1.$$

Sea $swap(f) = e_f(1) + \dots + e_f(n-1)$

Llamamos a esto el **swapping number** de la permutación f, ya que cuenta el número de veces que f intercambia la desigualdad $i < j$ a $f(i) > f(j)$. Diremos que f es **par** si $swap(f)$ es par y llamamos f **impar** en caso contrario, es decir, encontramos una manera muy fácil de determinar si una permutación f es par o impar. Dada una fila de enteros, diremos que el número de intercambios es igual al número de enteros que son menores que el entero que encabeza la fila. Así, por ejemplo, el número de intercambios en la fila 3, 1, 2 (ejemplo 1.1.2) es 2.

El número $sign(f) = (-1)^{swap(f)}$ se llama el signo (o función **signum**) de la permutación f.

Lema 1.1.1. Sea $f : \mathbb{Z}_n \to \mathbb{Z}_n$ una permutación. Entonces

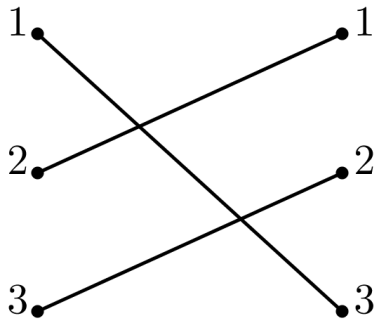
$$sing(f) = \prod_{i<j\le n} \frac{f(i) - f(j)}{i - j}.$$

Observación 1.1.1. Sea $S \subset \mathbb{Z}_n$. Sea $f : \mathbb{Z}_n \to \mathbb{Z}_n$ una permutación para la cual $f(i) = i$, para todo $i \in S$. En otras palabras, f permuta los elementos de $S^c = \mathbb{Z}_n - S$ pero no los elementos de S. Definimos una nueva permutación g de S^c (no de $\mathbb{Z}_n$) por $g(i) = f(i)$ para todo $i \in S^c$. El lema anterior implica que el signo de la permutación $f : \mathbb{Z}_n \to \mathbb{Z}_n$ es el mismo que el signo de la permutación $g : S^c \to S^c$.

Ejemplo 1.1.2. Definimos la permutación $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ como $f(1) = 3,\ f(2) = 1,\ f(3) = 2,$ la escribimos en una matriz 2×3

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Hay 3 desigualdades para $\mathbb{Z}_3 : 1 < 2,\ 2 < 3,\ y\ 1 < 3.$ Tenemos $f(1) = 3 > f(2) = 1,$ $f(2) = 1 < f(3) = 2,$ y $f(1) = 3 > f(3) = 2.$ Por lo que la primera y tercera desigualdad cambian, así el número de intercambios es $swap(f) = 2.$ Otra forma de dibujar f es por un"diagrama cruce", donde f envía la columna de la izquierda a la columna de la derecha:



El número de cruces en este diagrama es el número de intercambios de f, de los cuales podemos ver que f es una permutación par y su signo $sign(f) = (-1)^2 = 1.$

Definición 1.1.2. Sea $f: \mathbb{Z}_n \to \mathbb{Z}_n$ y $g: \mathbb{Z}_n \to \mathbb{Z}_n$ dos permutaciones. Podemos componerlas para obtener otra permutación, la **composición**, que se denota como $fg: \mathbb{Z}_n \to \mathbb{Z}_n$:

$$\begin{array}{ccccc} k & \mapsto & f(k) & \mapsto & g\big(f(k)\big) \\ \mathbb{Z}_n & \to & \mathbb{Z}_n & \to & \mathbb{Z}_n \end{array}$$

¡Una advertencia sobre la notación! Vamos a seguir las convenciones estándar y escribir nuestras composiciones de permutaciones de **izquierda a derecha**. (Esto contrasta con la composición de funciones de derecha a izquierda que puede haber en otros libros.)

Cuando $f = g$ entonces escribimos ff como f^2. En general, escribimos n-veces la composición $f \ldots f$ (n veces) como f^n. Cada permutación f tiene la propiedad de que existe algún número entero $N > 0,$ el cual depende de $f,$ tal que $f^N = 1.$ Es decir, si componemos una permutación un número suficiente de veces se llega a la permutación identidad.

Lema 1.1.2. Sean f y g permutaciones $\mathbb{Z}_n \to \mathbb{Z}_n$. $sign(fg) = sign(f)sign(g).$

Observe que para f, g como en el Lema 1.1.1, tenemos

$$\prod_{i<j\leq n} \frac{fg(i) - fg(j)}{i - j} = \prod_{i<j\leq n} \frac{g(i) - g(j)}{i - j} \prod_{i<j\leq n} \frac{fg(i) - fg(j)}{g(i) - g(j)}$$

Definición 1.1.3. El menor entero $N > 0$ tal que $f^N = 1$ se llama el **orden** de f.

Ejemplo 1.1.3. Sean $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

permutaciones de $\mathbb{Z}_n$. Tenemos que

$$fg = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad f^2 = 1, \qquad g^3 = 1.$$

Por lo que el orden de f es 2 y el orden de g es 3.

1.2 Inversos

Tratemos de visualizar la gráfica de una función $f: \mathbb{Z}_n \to \mathbb{Z}_n$. Podemos pensar en esto, ya sea como una colección de puntos $(i, f(i)), i = 1,2, \dots, n,$ o como una gráfica de barras. En cualquier caso, podemos analizar la gráfica de f y determinar

(a) si f es inyectiva,
(b) si f es sobreyectiva,
(c) la inversa f^{-1}, si es que existe.

¿Cómo hacer ese análisis? Bueno, a partir de la gráfica de f podemos determinar la imagen $f(\mathbb{Z}_n)$ y esto indica si f es sobreyectiva o no. La inversa, sólo existe si f es biyectiva. Su gráfica es determinada porque refleja la gráfica de f sobre la diagonal, $x = y$.

Lema 1.2.1. Las siguientes afirmaciones son equivalentes:

(1) $f: \mathbb{Z}_n \to \mathbb{Z}_n$ es inyectiva.
(2) $f: \mathbb{Z}_n \to \mathbb{Z}_n$ es sobreyectiva.
(3) $|f(\mathbb{Z}_n)| = |\mathbb{Z}_n|$.

Prueba: Sugerencia: primero demuestra (1) implica (2) usando reducción al absurdo, luego, demuestra (2) implica (1), utilizando de nuevo reducción al absurdo. La afirmación (2) es equivalente a (3) por la definición de sobreyectividad.

Ejemplo 1.2.1. La inversa de

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

es

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Ejemplo 1.2.2: Determinar f^{-1}, g^{-1} y h^{-1}

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}.$$

Solución: Intercámbiense las filas en f, g y h,

$$\begin{pmatrix}3 & 1 & 2\\ 1 & 2 & 3\end{pmatrix}, \qquad \begin{pmatrix}2 & 3 & 4 & 1\\ 1 & 2 & 3 & 4\end{pmatrix}, \qquad \begin{pmatrix}2 & 1 & 5 & 3 & 4\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}.$$

Ordénense las columnas de manera que la fila superior esté en orden ascendente

$$f^{-1} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \qquad g^{-1} = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}, \qquad h^{-1} = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & 4 & 5 & 3\end{pmatrix}.$$

Hay dos formas de uso común para expresar una permutación. La primera es la "notación matricial:

Definición 1.2.1. A una permutación $f: \mathbb{Z}_n \to \mathbb{Z}_n$, dada por

$$f = \begin{pmatrix}1 & 2 & \dots & n\\ f(1) & f(2) & \dots & f(n)\end{pmatrix},$$

le asociamos la matriz $P(f)$ de ceros y unos definida de la siguiente manera: la entrada ij-ésima de $P(f)$ es 1 si $j = f(i)$ y es 0 en otro caso.

Ejemplo 1.2.3. La matriz de la permutación f dada por

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

es

$$P(f) = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Definición 1.2.2. Una matriz cuadrada que tiene exactamente un 1 por fila y por columna (como $P(f)$ lo hace) es llamada una **matriz permutación.**

Lema 1.2.2. Hay $n!$ distintas matrices permutación $n \times n$ y hay $n!$ permutaciones distintas del conjunto $\{1,2, \dots, n\}$.

Ejemplo 1.2.4. La matriz de la permutación f dada por

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

es

$$P(f) = \begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Tenga en cuenta que la multiplicación de matrices da

$$\begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1\\ 2\\ 3\end{pmatrix} = \begin{pmatrix}2\\ 1\\ 3\end{pmatrix},$$

de la que podemos obtener la matriz 2×3.

¿Cómo se relacionan la función permutación con la matriz permutación? El siguiente teorema explica partes de esta relación.

Teorema 1.2.1. Si $f: \mathbb{Z}_n \to \mathbb{Z}_n$ es una permutación entonces

(a)
$$P(f)\begin{pmatrix}1\\2\\\vdots\\n\end{pmatrix} = \begin{pmatrix}f(1)\\f(2)\\\vdots\\f(n)\end{pmatrix},$$

(b) $P(f)^{-1} = P(f^{-1})$ (la inversa de la matriz permutación es la matriz de la inversa de la permutación),

(c) $P(fg) = P(f)P(g)$ (la matriz permutación del producto es el producto de las matrices permutación),

(d) $sign(f) = det\big(P(f)\big)$.

Demostración: Si $\vec{v}$ es el vector columna con entradas $v_1, v_2, \dots, v_n$ (las v_i son números reales arbitrarios) luego $P(f)\vec{v}$ es el vector columna cuya i-ésima coordenada es igual a v_j si f envía i a j. Dado que, en este caso, $j = f(i)$ (escribimos $f(i)$ para denotar la imagen de i bajo la permutación f, aunque i realmente debería evaluarse en f a la izquierda), esto implica que $P(f)\vec{v}$ es el vector columna con entradas $v_{f(1)}, v_{f(2)}, \dots, v_{f(n)}$. Esto prueba (a).

Tenga en cuenta que (b) es una consecuencia de (c) por lo que sólo debemos probar (c). Calculamos $P(fg)\vec{v}$ y $P(f)P(g)\vec{v}$. Por el mismo razonamiento que en (a), encontramos que la i-ésima coordenada de $P(fg)\vec{v}$ es $v_{(fg)(i)}$. Del mismo modo, la coordenada i-ésima de $P(g)\vec{v}$ es $v'_i = v_{g(i)}$. Por lo tanto, la i-ésima coordenada de $P(f)(P(g)\vec{v})$ es $v'_{f(i)} = v_{g(f(i))} = v_{(fg)(i)}$. Esto implica $P(fg)\vec{v} = P(f)P(g)\vec{v}$. Dado que las v_i fueron números reales arbitrarios, esto demuestra el teorema.

Ejemplo 1.2.5. Sean

$$f = \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}, \qquad g = \begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}, \qquad h = \begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix},$$

por lo que $f = f^{-1}$, $g = g^{-1}$, $h = fg$. Más aun,

$$P(g) = \begin{pmatrix}0 & 0 & 1\\0 & 1 & 0\\1 & 0 & 0\end{pmatrix}, \qquad P(h) = \begin{pmatrix}0 & 1 & 0\\0 & 0 & 1\\1 & 0 & 0\end{pmatrix}.$$

Con un cálculo directo de la matriz verificamos que $P(f)P(g) = P(fg) = P(h)$ y $P(h^{-1}) = P(g^{-1}f^{-1}) = P(g^{-1})P(f^{-1}) = P(g)^{-1}P(f)^{-1}$, según lo previsto por el teorema anterior.

La matriz puede determinarse a partir de la gráfica de la función $f: \mathbb{Z}_n \to \mathbb{Z}_n$ de la siguiente manera. Primero, tomamos la gráfica de la función f y damos la reflejamos sobre el eje de abscisas. En esta cuadrícula $n \times n$ de puntos enteros (x, y), la primera coordenada baja, la segunda coordenada cruza, y x y y son enteros entre 1 y n inclusive. (Esto no debe confundirse con la orientación de los "ejes" en el plano xy) Ahora, rellenamos todos los puntos marcados con unos y todos los puntos no trazados con ceros. El resultado de la matriz $n \times n$ es la matriz $P(f)$.

Ejemplo 1.2.6. Considere la

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

cuyo gráfico e imagen espejo aparecen en la *Figura 1.1*

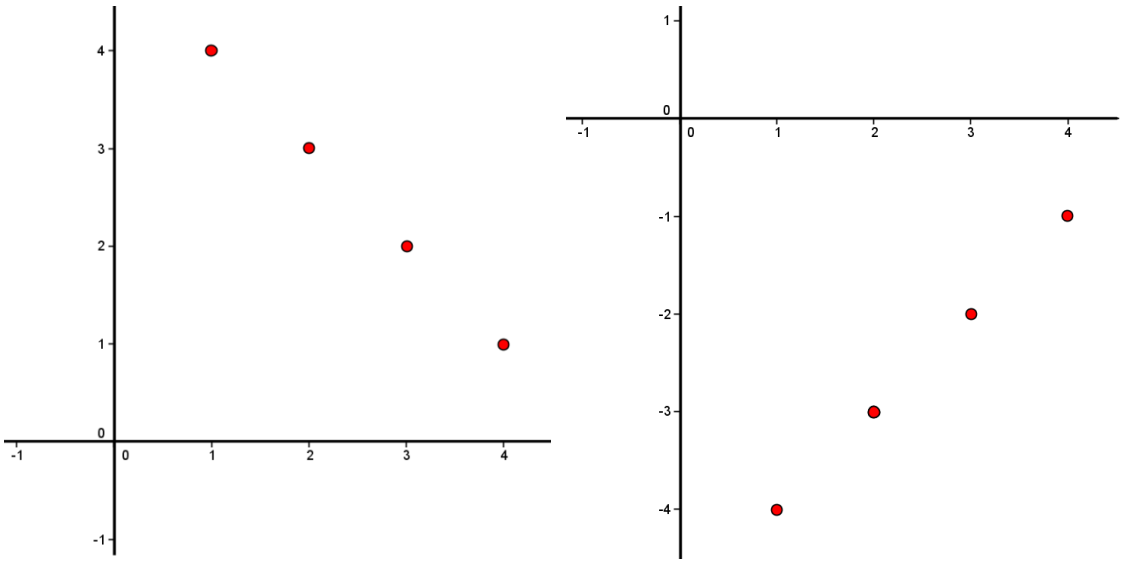


Figura 1.1: *gráfico e imagen espejo de* f.

La matriz asociada a esta permutación es

$$P(f) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

como en el gráfico imagen espejo.

El conjunto de todas las permutaciones de $\mathbb{Z}_n$ se denota S_n y es llamado **grupo simétrico** de grado n.

Apliquemos las permutaciones y movimientos al Cubo de Rubik: al intentar resolverlo es frecuente el caso de que estemos haciendo varios movimientos del siguiente tipo: hacer un movimiento m_1, luego otro movimiento m_2, a continuación, hacer la inversa de la primera jugada o movimiento, m_1^{-1}. Por ejemplo, $(R^{-1}D^2RB^{-1}U^2B)^2$ se compone de tales movimientos. Este movimiento es una “torsión” de dos esquinas: la esquina urf (la notación

Singmaster, se explica en el Ejemplo 1.2.7 más adelante) se gira una vez según las agujas del reloj, y la esquina bld se "tuerce" una vez en sentido antihorario, como se ilustra en la *Figura 1.2*

Figura 1.2: $(R^{-1}D^2RB^{-1}U^2B)^2$ *permuta aristas y caras pero no los vértices.*

En general, para calcular el efecto de un movimiento como $m_1 m_2 m_1^{-1}$, necesitamos saber cómo se mueve cada vértice y cada arista. Está implícito el uso del siguiente lema cuando resolvemos el Cubo de Rubik.

Lema 1.2.3. Si $r \in S_n$ denota cualquier permutación e i, j son enteros distintos pertenecientes a $\{1,2,\dots,n\}$. Sea s una permutación que envía i a j:

$$s(i) = j.$$

Entonces $s^r = r^{-1}sr$ es una permutación que envía $r(i)$ a $r(j)$:

$$s^r\big(r(i)\big) = r(j).$$

Más específicamente: Sean $i_1, i_2, \dots, i_k$ enteros distintos que pertenecen a $\{1,2,\dots,n\}$. Sea s la permutación que envía i_j a i_{j+1}:

$$s(i_j) = i_{j+1}, \quad 1 \le j < k, \quad s(i_k) = i_1, \quad s(m) = m, \forall m \notin \{i_1, \dots, i_k\}.$$

Entonces $s^r = r^{-1}sr$ es la permutación que envía $r(i_j)$ a $r(i_{j+1})$:

$$s^r\big(r(i_j)\big) = r(i_{j+1}), \quad 1 \le j < k, \quad s^r(r(i_k)) = r(i_1),$$

$$s^r(m) = m, \quad \forall m \notin \{r(i_1), \dots, r(i_k)\}.$$

Ejemplo 1.2.7. Denotamos el conjunto de **movimientos básicos** por $\{U, D, L, R, F, B\}$, donde

- U denota el movimiento del Cubo de Rubik donde usted gira la cara superior según las agujas del reloj un cuarto de vuelta,
- D denota el movimiento donde usted gira la cara inferior según las agujas del reloj un cuarto de vuelta,
- L gira la cara izquierda según las agujas del reloj un cuarto de vuelta,
- R gira la cara derecha según las agujas del reloj un cuarto de vuelta,

- F gira la cara frontal según las agujas del reloj un cuarto de vuelta,
- B gira la cara posterior según las agujas del reloj un cuarto de vuelta,

Esta forma "corta" es llamada **la notación Singmaster**. [Si]

Vamos a etiquetar las 12 aristas del Cubo de Rubik usando la notación Singmaster:

- uf denota la "arista frontal, superior",
- ul denota la "arista izquierda, superior",
- ur denota la "arista derecha, superior",
- ub denota la "arista posterior, superior",
- df denota la "arista frontal, inferior",
- dl denota la "arista izquierda, inferior",
- dr denota la "arista derecha, inferior",
- db denota la "arista posterior, inferior",
- fl denota la "arista izquierda, frontal",
- fr denota la "arista derecha, frontal",
- bl denota la "arista izquierda, posterior",
- br denota la "arista derecha, posterior".

Finalmente las esquinas se denotan similarmente como sigue (fru denota la "esquina superior derecha, frontal", etcétera)

Si tenemos un Cubo de Rubik el movimiento s es un 3-ciclo, en 3 aristas en particular, por decir

$$uf \mapsto ul \mapsto ur \mapsto uf,$$

y otro movimiento r que envía estas aristas a algún otro lugar, por ejemplo $r = F^2$ de modo que $r: uf \mapsto df$ pero deja las otras aristas fijas, entonces $r^{-1}sr$ es la permutación

$$df \mapsto ul \mapsto ur \mapsto df$$

Una prueba de este lema se dará en el capítulo 6 (ver Teorema 6.3.1).

1.3 Notación cíclica

La notación más común para una permutación es la "notación cíclica", debida a Cauchy (mediados de 1800). Esta notación es más compacta que la notación matricial que hemos estado utilizando, y desde este punto vamos a cambiar a la notación cíclica.
Si $a_1, a_2, \dots, a_r \in \mathbb{Z}_n$ son distintos entonces el símbolo

$$(a_1, a_2, \dots, a_r)$$

denota la permutación f de $\mathbb{Z}_n$ que envía a_1 a a_2, envía a_2 a a_3, ..., envía a_{r-1} a a_r , envía a_r a a_1, y deja todos los otros números en $\mathbb{Z}_n$ fijos (donde r es un entero menor o igual a n). En otras palabras,

$$f(a_1) = a_2, \ f(a_2) = a_3, \dots, f(a_r) = a_1,$$

y $f(i) = i,$ si i no es igual a uno de los $a_1, \dots, a_r$. Tal permutación es llamada **cíclica.** El número r se llama la **longitud** del ciclo.

Llamamos a dos de estos ciclos $(a_1, a_2, \dots, a_r)$ y $(b_1, b_2, \dots, b_t)$ disjuntos si los conjuntos $(a_1, a_2, \dots, a_r)$ y $(b_1, b_2, \dots, b_t)$ no tienen ningún entero en común.

Lema 1.3.1. Si f y g son permutaciones cíclicas disjuntas de $\mathbb{Z}_n$ entonces $fg = gf$.

Prueba: Esto es verdad porque las permutaciones f y g de $\mathbb{Z}_n$ afectan colecciones disjuntas de números enteros, por lo que el producto de permutaciones se puede realizar en cualquier orden.

Lema 1.3.2. La permutación cíclica $(a_1, a_2, \dots, a_r)$ tiene orden r.

Prueba: Nótese que $f(a_1) = a_2$, $f^2(a_1) = a_3, \dots, f^{r-1}(a_1) = a_r$, $f^r(a_1) = a_1$, por definición de f. Asimismo, para cualquier $i = 1, \dots, r$ tenemos que $f^r(a_i) = a_i$.

Definición 1.3.1. Una **transposición** es un ciclo (i, j) de longitud 2 que intercambia i y j $(i \neq j)$.

Teorema 1.3.1. Toda permutación $f: \{1,2, \dots, n\} \to \{1,2, \dots, n\}$ es el producto de permutaciones cíclicas disjuntas. Más precisamente, si f es una permutación de $\{1,2, \dots, n\}$ (con $n > 1$) entonces hay subconjuntos disjuntos no vacios de distintos enteros

$$\begin{gathered} A_1 = \{a_{11}, \dots, a_{1,r_1}\} \subset \{1,2, \dots, n\}, \\ A_2 = \{a_{21}, \dots, a_{2,r_2}\} \subset \{1,2, \dots, n\}, \\ \vdots \\ A_k = \{a_{k1}, \dots, a_{k,r_k}\}, \end{gathered}$$

tal que

$$\{1,2, \dots, n\} = A_1 \cup \dots \cup A_k, \qquad n = r_1 + r_2 + \cdots + r_k,$$

y

$$f = (a_{11}, \dots, a_{1,r_1}) \dots (a_{k1}, \dots, a_{k,r_k}).$$

Este producto se llama **descomposición cíclica** de f. Si reorganizamos las cardinalidades r_i de estos conjuntos A_i en orden decreciente, digamos escribimos esto como

$$r_1' \geq r_2' \geq \cdots \geq r_k',$$

entonces la k-tupla $(r_1', \dots, r_k')$ es llamada la **estructura cíclica** de f y f es llamado un $(r_1', \dots, r_k')$**-ciclo**. Por ejemplo, $(1, 2)(3, 4, 5)$ es un $(3, 2)$-ciclo en S_5.

Prueba: La prueba es constructiva.
Sea $f: \mathbb{Z}_n \to \mathbb{Z}_n$ una permutación. Todos los *distintos* elementos de $\mathbb{Z}_n$ se obtienen por la aplicación repetida de f a 1. Llamémoslos (¡por falta de una notación mejor!),
$a_{10}, a_{11}, a_{12}, \dots, a_{1,r_1}$, donde,

$$O_1 = \{a_{10} = 1,\ a_{11} = f(1),\ a_{12} = f^2(1), \dots,\ a_{1,r_1} = f^{r_1}(1)\}.$$

(Esto es llamado **la órbita de 1 respecto a f**. Vamos a discutir las órbitas más tarde, en el 3.9) Ahora listamos los elementos de la 'órbita de 2':

$$O_2 = \{a_{20} = 2,\ a_{21} = f(2),\ a_{22} = f^2(2), \dots,\ a_{2,r_2} = f^{r_2}(2)\},$$

y así sucesivamente hasta llegar a la 'órbita de n':

$$O_n = \{a_{n0} = n,\ a_{n1} = f(n),\ a_{n2} = f^2(n), \dots,\ a_{n,r_n} = f^{r_n}(n)\}.$$

Un ejemplo: Sea $f: \mathbb{Z}_3 \to \mathbb{Z}_3$ es el 3-ciclo, $f(1) = 2,\ f(2) = 3,\ f(3) = 1$. En este caso, $O_1 = \{1,\ 2,\ 3\},\ O_2 = \{2,\ f(2) = 3,\ f(f(2)) = f(3) = 1\}$ y $O_3 = \{3,\ f(3) = 1,\ f(f(3)) =$ *f1=2*, por lo que las tres órbitas son iguales unas a otras en este ejemplo.

En general, si elige cualquiera dos de estas n órbitas $O_1, \dots, O_n$, serán la misma o bien disjuntas. Denotemos todas las órbitas distintas por $O'_1, \dots, O'_K$. (Las $O'_1, \dots, O'_K$ son una subsecuencia de las $O_1, \dots, O_n$. No importa en qué orden escriba las O'_i ni en qué orden escriba los elementos en cada órbita individual.)

Supongamos que

$$\begin{aligned} O'_1 &= \{b_{11}, \dots, b_{1,s_1}\} \text{ por lo que } |O'_1| = s_1, \\ O'_2 &= \{b_{21}, \dots, b_{2,s_2}\} \text{ por lo que } |O'_2| = s_2, \\ &\vdots \\ O'_k &= \{b_{k1}, \dots, b_{k,s_k}\} \text{ por lo que } |O'_k| = s_k. \end{aligned}$$

(Las a_{ij} han sido reetiquetadas como b_{ij} para tratar de simplificar la notación.) En este caso,

$$\mathbb{Z}_n = \bigcup_{i=1}^{k} O'_i = O'_1 \cup \dots \cup O'_k,$$

y $s_1 + s_2 + \cdots + s_k = n$. La restricción de f a O'_1, denotada $f_{O'_1}: O'_1 \to O'_1$, es igual al s_1-ciclo $(b_{11}, b_{12}, \dots, b_{1,s_1})$. En general, la restricción de f a O'_j, denota $f_{O'_j}: O'_1 \to O'_j$, es igual al s_j-ciclo $(b_{j1}, b_{j2}, \dots, b_{j,s_j})$. Dado que las O'_j particionan $\mathbb{Z}_n$ de la definición de f y nuestra construcción implica que

$$f = (b_{11}, b_{12}, \dots, b_{1,s_1}) \dots (b_{k1}, b_{k2}, \dots, b_{k,s_k}).$$

Ejemplo 1.3.1

- La notación cíclica para $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

  es $(1,2)(3)$ o, simplemente $(1,2)$. En general, si cualquiera de las órbitas O_j en la anterior construcción es un producto único, a menudo se omite de la notación, con el entendimiento implícito que f no permuta los números omitidos.

- La notación cíclica para $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

  es $(1,2,3)$.

- La notación cíclica para $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

es $(1,3)(2,4) = (2,4)(1,3)$.

- La notación cíclica para
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

es $(1,3)(2,4,5) = (4,5,2)(1,3)$.

Ejemplo 1.3.2. Dividimos un cuadrado en 4 "caras" y etiquetamos 1, 2, 3, 4. Por ejemplo,

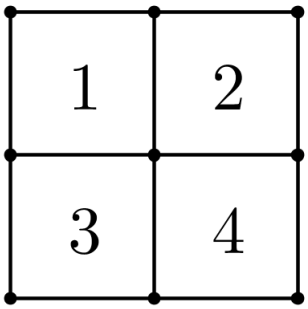


Figura 1.3

Sea r la rotación de 90 grados en sentido contrario a las agujas del reloj. Entonces, como una permutación sobre las caras, $r = (1,3,4,2)$. Sea f_x la reflexión sobre la línea horizontal que divide el cuadrado en dos, sea f_y la reflexión sobre la línea vertical que divide al cuadrado en dos. Utilizar la notación cíclica para determinar las permutaciones de las caras (a) r^2, (b) r^3, (c) f_x , (d) f_y , (e) $f_x r f_x$, (f) $f_x f_y$.

Solución:

(a) $r^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1,4)(2,3).$

(b) $r^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1,2,4,3).$

(c) $f_x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1,3)(2,4).$

(d) $f_y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1,2)(3,4).$

(e) $f_x r f_x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1,2,4,3).$

(f) $f_x f_y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1,4)(2,3).$

Ejemplo 1.3.3. Etiquetamos las 24 caritas del Cubo de Rubik 2 x 2 x 2 de la siguiente manera:

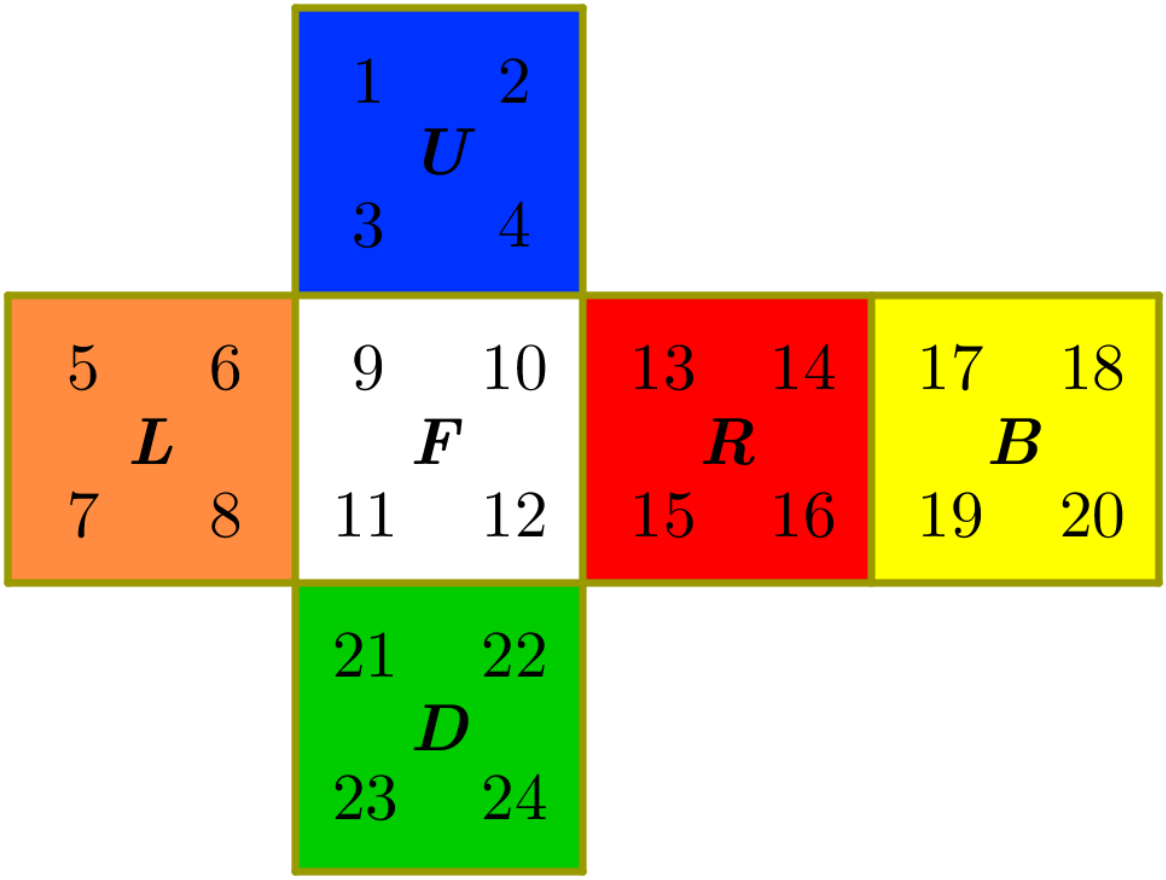


Figura 1.4

Sea X la rotación de 90 grados en sentido anti horario de la cara etiquetada x, donde $x \in \{r, l, f, b, u, d\}$ (así, por ejemplo, si $x = f$ entonces: $X = F$). Use la notación cíclica para determinar las permutaciones de las caras dadas por (a) R, (b) L, (c) F, (d) B, (e) U, (f) D.

(a) $R = (13, 15, 16, 14)$
(b) $L = (5, 7, 8, 6)$
(c) $F = (9, 11, 12, 10)$
(d) $B = (17, 19, 20, 18)$
(e) $U = (1, 3, 4, 2)$
(f) $D = (21, 23, 24, 22)$

Lema 1.3.3. Una permutación cíclica es par si y sólo si la longitud de su ciclo es impar. Una permutación $f: \mathbb{Z}_n \to \mathbb{Z}_n$ es impar si y sólo si el número de ciclos de longitud par en su descomposición cíclica disjunta es impar.

Esto sigue de la definición de una permutación par/impar (ver Definición 1.1.1), el hecho de que

$$sign(p_1 p_2 \dots p_k) = sign(p_1) sign(p_2) \dots sign(p_k)$$

para permutaciones p_i (por el Lema 1.1.2.), y el hecho de que cualquier k-ciclo se puede escribir como un producto de $k-1$ transposiciones,

$$(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_2). \qquad (1.1)$$

(Ecuación (1.1) se puede probar por inducción matemática. Para más información, consulte los resultados relacionados en el capítulo 1 de Rotman [R] o el Teorema 3.3 en Gaglione [G], 3.2, por ejemplo.)

Lema 1.3.4. El orden de una permutación es el mínimo común múltiplo (mcm) de las longitudes de $r_1, r_2, \dots, r_k$ de los ciclos disjuntos en su descomposición cíclica.

Ejemplo 1.3.4. El orden de $(1,3)(2,4)$ es 2. Es par. El orden de $(1,3)(2,4,5)$ es 6. Es impar.

1.4 Un algoritmo para listar todas las permutaciones

Martin Gardner [Gar1] menciona un algoritmo que lista todas las permutaciones de $\{1,2,\dots,n\}$. Este algoritmo proporciona el mejor método conocido del listado de todas las permutaciones de $\{1,2,\dots,n\}$. Redescubierto muchas veces desde entonces, el procedimiento es debido originalmente al matemático polaco Hugo Steinhaus (1887-1972). Un estudiante de David Hilbert en Göttingen, que hizo un importante trabajo sobre series ortogonales, teoría de probabilidad, funciones reales y sus aplicaciones.
Denotaremos cada permutación en la segunda fila en su notación matricial $2 \times n$. Por ejemplo, en el caso $n = 2$

$$\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix}$$

son las permutaciones.

Para ver el caso $n = 3$, la idea es

(a) escribir debajo de cada fila $n = 3$ veces como sigue:

$$\begin{matrix} 1 & 2 \\ 1 & 2 \\ 1 & 2 \\ 2 & 1 \\ 2 & 1 \\ 2 & 1 \end{matrix}$$

(b) 'entrelazar' un 3, como sigue

$$\begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 3 & 1 & 2 \\ 3 & 2 & 1 \\ 2 & 3 & 1 \\ 2 & 1 & 3 \end{matrix}$$

En el caso $n = 4$, la idea es

(a) Escribir debajo de cada fila 4 veces como sigue

1 2 3	3 2 1
1 2 3	3 2 1
1 2 3	3 2 1
1 2 3	3 2 1
1 3 2	2 3 1
1 3 2	2 3 1
1 3 2	2 3 1
1 3 2	2 3 1
3 1 2	2 1 3
3 1 2	2 1 3
3 1 2	2 1 3
3 1 2	2 1 3

(b) ahora "entrelazar" un 4 en:

1 2 3 4	4 3 2 1
1 2 4 3	3 4 2 1
1 4 2 3	3 2 4 1
4 1 2 3	3 2 1 4
4 1 3 2	2 3 1 4
1 4 3 2	2 3 4 1
1 3 4 2	2 4 3 1
1 3 2 4	4 2 3 1
3 1 2 4	4 2 1 3
3 1 4 2	2 4 1 3
3 4 1 2	2 1 4 3
4 3 1 2	2 1 3 4

En la sub sección 1.4.1 describe el procedimiento general. Estas construcciones conducen al siguiente resultado.

Teorema 1.4.1. (Steinhaus) Hay una secuencia de 2-ciclos (no necesariamente distintos), $(a_1, b_1), \dots, (a_N, b_N)$, donde $N = n! - 1$, tal que cada permutación no trivial f de $\{1,2, \dots, n\}$ puede ser expresada en la forma

$$f = \prod_{i=1}^{k} (a_i, b_i)$$

para algún k, $1 \leq k \leq N$. Estas transposiciones (a_i, b_i), para $k = 1,2, \dots, N$, son no necesariamente disjuntas

En particular, cada permutación se puede escribir como un producto de 2-ciclos (no necesariamente disjuntos). Este teorema dice mucho más. Se dice que el conjunto de todas las permutaciones puede ser generado por la multiplicación sucesiva por una transposición definida. Este resultado se probará en la siguiente sección.
Hay un resultado análogo válido, sólo para permutaciones *pares*: cada permutación par puede ser escrita como un producto de 3-ciclos (no necesariamente disjuntos). Esto se indicará con mayor precisión y será probado en la siguiente sección, véase la Proposición 6.4.1.

1.4.1 ¿Por qué funciona el algoritmo de Steinhaus?

El argumento es por inducción matemática.

1. Primero, notar que el algoritmo de Steinhaus funciona para $n = 2,\ n = 3$.

2. Escriba todos los elementos de S_{n-1} como una lista utilizando el algoritmo de Steinhaus (Por la hipótesis de inducción, cada elemento difiere del anterior por una transposición conveniente en esta lista). Representamos cada elemento en la notación matricial $2 \times (n-1)$. En nuestra lista, simplemente registramos la segunda fila en la lista, es decir, como una $(n-1)$-tupla. Hay $(n-1)!$ elementos en esta lista.

3. Para la primera $(n-1)$-tupla, escribir una n al final, para la segunda $(n-1)$-tupla, escribir una n al principio, para la tercer $(n-1)$-tupla, escribir una n al final, para la cuarta $(n-1)$-tupla, escribir una n al principio, y así sucesivamente. Observe que tenemos una secuencia de $(n-1)!$ n-tuplas.

4. Supongamos que la i-ésima n-tupla $(n, a_1, a_2, \dots, a_{n-1})$. Primero, actúa en esto por la transposición (n, a_1), luego por la transposición (n, a_2), luego por (n, a_3), ..., por (n, a_{n-1}). El resultado de la última es $(a_1, a_2, \dots, a_{n-1})$. Supongamos que la j-ésima n-tupla es $(b_1, b_2, \dots, b_{n-1}, n)$. (Note que por la hipótesis de inducción, $(a_1, a_2, \dots, a_{n-1}, n)$ y $(b_1, b_2, \dots, b_{n-1}, n)$ 'difieren' sólo por una transposición conveniente, en S_{n-1}). Primero, actúa por la transposición (b_1, n), luego por la transposición (b_2, n), luego por (b_3, n), ..., por (b_{n-1}, n). El resultado de la última es $(n, b_1, b_2, \dots, b_{n-1})$.

5. Nótese que todos estos (para i, j corriendo sobre números enteros pares o impares del 1 al $n-1$), el resultado $n!$ n-tuplas son distintas. Esto proporciona una lista de S_n como se deseaba.

1.5 Permutaciones y volteo de campanas

Figura 1.5

Desde el siglo XVII, y posiblemente antes, las campanas de la catedral en Inglaterra han sonado permutando el orden de una "ronda" de campanas. El arte y el estudio de tal volteo de campanas como se conoce como **campanología.**
Fabian Stedman proporcionó importantes contribuciones al volteo de campanas. Nació en 1640, las conexiones de Fabián Stedman con campanología echaron raíces a la temprana edad de 15 años cuando se trasladó a Londres para trabajar como aprendiz de un maestro impresor. Importantes contribuciones de Stedman a la campanología se reflejan en sus esfuerzos en **Tintinnalogia y Campanología** (ver Henry Hubbard) los primeros dos libros publicados sobre el tema, en 1668 y 1677, respectivamente.
A continuación se presenta un glosario de algunos términos esenciales:

Figura 1.6

• **Cambiar:** el intercambio de uno o más pares de campanas adyacentes.
• **Cambio plano:** el intercambio de un par de campanas adyacentes solamente.
• **Cambio cruzado:** el intercambio de más de un par de campanas.
• **Ronda:** un ordenamiento de las campanas (es decir, una permutación de $(1,2,3,\dots,n)$).

En un principio, *cambio de sonido* concierne a una sola fila de campanas cuyo orden puede ser denotado por $(1,2,3,\dots,n)$. Teniendo en cuenta el caso de que $n = 6$ los conceptos de cambios cruzados y planos se pueden entender con mayor claridad.
Si usamos solo cambios planos podemos generar permutaciones de las campanas de la siguiente manera:

1 2 3 4 5 6
2 1 3 4 5 6
2 1 4 3 5 6
2 1 4 3 6 5

Debe ser bastante obvio en la inspección que el primer cambio plano intercambia 1 y 2, el segundo intercambia 3 y 4, y el tercero intercambia 5 y 6. Teniendo en cuenta el mismo conjunto de seis campanas actuando por cambio cruzado, el mismo resultado se obtiene en un cambio, como se ve a continuación:

1 2 3 4 5 6
2 1 4 3 6 5

Patrones más útiles e interesantes pueden ser generados por la combinación cambios cruzados y planos. El plan nos conduce en el caso de cuatro campanas a uno de los más

simples patrones y fue ideado alrededor de 1621 alternando consecutivamente cambios cruzados y cambios planos como se muestra a continuación:

$$\begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 2 & 4 & 1 & 3 \\ 4 & 2 & 3 & 1 \\ 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \\ 3 & 1 & 4 & 2 \\ 1 & 3 & 2 & 4 \\ 1 & 2 & 3 & 4 \end{matrix}$$

El patrón que define el plan producido sobre cuatro campanas no es más que un cambio cruzado seguido de un cambio plano en el centro dos campanas hasta llegar a la ronda, que es donde empezamos.

Generar las permutaciones contenidas en el plan producido sobre cuatro campanas se puede describir fácilmente usando la notación para permutaciones que hemos desarrollado. Comenzaremos representando el cambio cruzado como $a = (1,2)(3,4)$, que intercambia las dos primeras y las últimas dos campanas, y representando el cambio plano como b$= (2,3)$, que intercambia el par medio. Comenzamos con el primer elemento a.

Para generar la siguiente permutación multiplicamos este primer elemento por b. Para generar el tercer elemento simplemente multiplicamos este segundo término ab, por a para obtener aba. Continuando de esta manera multiplicamos alternativamente, por a luego por b para generar el conjunto $D_4 = \{a, ab, aba, (ab)^2, (ab)^2a, (ab)^3, (ab)^3a, (ab)^4\}$. Este es el conjunto de permutaciones en el plan producido sobre cuatro campanas. (Se denota D_4 aquí por razones que serán explicadas más adelante.) Dado que $(ab)^4$ produce la ronda inicial, decimos $(ab)^4 = 1$ y $D_4 = \{1, a, ab, aba, (ab)^2, (ab)^2a, (ab)^3, (ab)^3a\}$.

Figura 1.7

Ahora, para un ejemplo más complejo. Nos dirigimos ahora nuestra atención a la composición que se conoce comúnmente como **Plan Bob Minimus**.

Figura 1.8

Figura 1.9

Figura 1.10

1	2	3	4
2	1	4	3
2	4	1	3
4	2	3	1
4	3	2	1
3	4	1	2
3	1	4	2
1	3	2	4

Figura 1.11

Figura 1.12

Plan Bob Minimus comienza y termina en la ronda $(1,2,3,4)$ y contiene todas las permutaciones posibles de estas cuatro campanas (en un orden particular, se describen a continuación):

1	2	3	4	1	3	4	2	1	4	2	3
2	1	4	3	3	1	2	4	4	1	3	2
2	4	1	3	3	2	1	4	4	3	1	2
4	2	3	1	2	3	4	1	3	4	2	1
4	3	2	1	2	4	3	1	3	2	4	1
3	4	1	2	4	2	1	3	2	3	1	4
3	1	4	2	4	1	2	3	2	1	3	4
1	3	2	4	1	4	3	2	1	2	4	3
								1	2	3	4

Ahora podemos describir esta composición usando la notación permutación como hicimos para el plan producido sobre cuatro campanas. Sea $a = (1,2)(3,4)$ y $b = (2,3)$, representan los posibles cambios entre filas. Si nos fijamos en la primera columna de la composición Plan Bob Minimus, vemos que no es más que el plan producido sobre cuatro campanas. Para generar la segunda columna, introducimos una nueva permutación $c = (3,4)$, y simplificamos nuestra notación dejando $k = (ab)^3ac$. Multiplicando por k, generamos la segunda columna:

$$\{k, ka, k\ ab, kaba, k(ab)^2, k(ab)^2a, k(ab)^3, k(ab)^3a\}.$$

Multiplicando por k de nuevo, generamos la tercera columna:

$$\{k^2, k^2a, k^2ab, k^2aba, k^2(ab)^2, k^2(ab)^2a, k^2(ab)^3, k^2(ab)^3a\}.$$

¡Esta generación de Plan Bob Minimus demuestra que puede ser expresado como la unión disjunta de "traslaciones" del plan conducido sobre las cuatro campanas! Vamos a explicar este hecho usando teoría de grupos en el próximo capítulo 3.
Ahora, ya que elegimos $a = (1,2)(3,4)$, $b = (2,3)$, y $c = (3,4)$, donde b y c son, evidentemente, por definición, 2-ciclos o transposiciones y a es el producto de dos de estos 2-ciclos o transposiciones, hemos mostrado un resultado más, que cada permutación de $\mathbb{Z}_4$ se puede escribir como un producto de 2-ciclos. En términos más generales, podemos afirmar el siguiente teorema originalmente por H. Steinhaus.

Teorema 1.5.1. Sea f un elemento de S_n, es decir, sea f cualquier permutación de grado n. Entonces f se puede escribir como un producto de transposiciones.

Para bosquejar una prueba de este teorema (siguiendo [G]) y por lo tanto, demostrar el Teorema 1.4.1 como se había prometido, sólo tenemos que recordar que cada permutación de S_n se puede escribir únicamente (hasta el fin), como un producto de ciclos disjuntos (Teorema 1.3.1. más arriba).

Prueba: Cualquier k-ciclo puede escribirse como un producto de $k-1$ trasposiciones, como en la ecuación (1.1). Dado que cualquier permutación se puede escribir en términos de ciclos, y cualquier ciclo puede ser escrito como producto de transposiciones, se sigue que toda permutación de $\mathbb{Z}_n$ se puede escribir como un producto de transposiciones.

Capítulo 2

Puzzles de permutación

Veremos varios juegos que técnicamente pueden considerarse como puzzles de permutación. Veremos cuán admirablemente se adapta la combinatoria (y más tarde teoría de grupos) en la descripción de estos puzzles.

Un juego de una sola persona (como el juego del 15) consiste en una secuencia de movimientos que siguen ciertas reglas:

- Hay un número finito de movimientos en cada etapa.
- Hay una secuencia finita de movimientos que conducen a una solución.
- No hay azar ni movimientos aleatorios
- Hay información completa acerca de cada movimiento.
- Cada movimiento depende sólo de la posición presente, no en la existencia o la no existencia de un cierto movimiento anterior (tal como en el ajedrez, donde el enroque es movimiento ilegal si el rey ha sido trasladado con anterioridad).

Un **"puzzle de permutación"** es un juego de una sola persona con un conjunto finito T de piezas puzzle el cual satisface las cuatro propiedades que se listan a continuación:

(1) Para algún, $n > 1$ dependiendo sólo de la construcción del puzzle, cada movimiento del puzzle corresponde a una única permutación de los números en $\mathbb{Z}_n$.

(2) Si la permutación de $\mathbb{Z}_n$ en (1) corresponde a más de un movimiento puzzle, entonces las dos posiciones obtenidas por los dos movimientos respectivos deben ser indistinguibles.

(3) Cada movimiento, digamos M, debe ser "invertible" en el sentido de que debe existir otro movimiento, digamos M^{-1}, que restaura el puzzle a la posición en que estaba antes que M se efectuara.

(4) Si M_1 es un movimiento que corresponde a una permutación f_1 de T y si M_2 es un movimiento que corresponde a una permutación f_2 de T, entonces $M_1 * M_2$ (el movimiento M_1 seguido por el movimiento M_2) es

– No es un movimiento legal, o bien
– Corresponde a la permutación $f_1 * f_2$.

Notación: Como en el paso 4, siempre vamos a escribir movimientos puzzle sucesivos de *izquierda a derecha*.

2.1 Puzzle 15

El puzzle 15 es un juego solitario, es decir un solo jugador, es asociado con el inventor de rompecabezas y de problemas Sam Loyd (1841 -1911). Él comenzó a publicar problemas de ajedrez a la edad de 14 años, tuvo su propia columna en una revista periódica sobre problemas de ajedrez. En 1914 publico su "Cyclopedia of Puzzles". El puzzle 15 es uno de los primeros y el más popular puzzle de permutación. La "posición resuelta' es la siguiente:

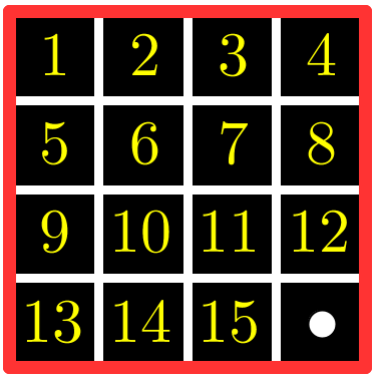


Figura 2.1

Cada uno de estos cuadrados numerados representan un bloque deslizante que sólo puede moverse a la casilla desocupada, que se denota por un •. A veces se etiqueta al cuadrado vacío como '16' por conveniencia. Los movimientos del puzzle consisten en deslizar cuadrados numerados (tal como 12, por ejemplo) en el cuadro vacío (intercambiando 12 con 16). De esta forma, cada movimiento de este puzzle puede ser considerado como una permutación de los enteros en {1, 2, … , 16}.

No todas las permutaciones del {1, 2, … , 16} corresponden a una posible posición del puzzle. Por ejemplo, la posición

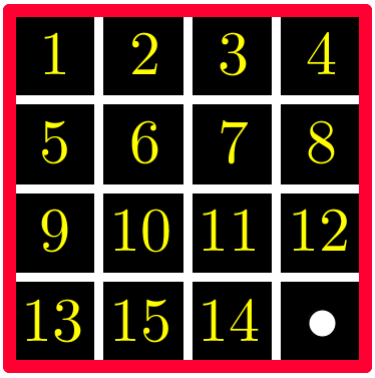


Figura 2.2

no puede ser obtenida desde la posición anterior. (La razón matemática para esto se explica en 4.4, más adelante.)

Antes de que el Cubo de Rubik se inventara el Puzzle 15 fue probablemente el puzzle más popular de todos los tiempos.

Los movimientos del Puzzle 15 pueden representarse de la siguiente manera. Supongamos que estamos en una posición tal como

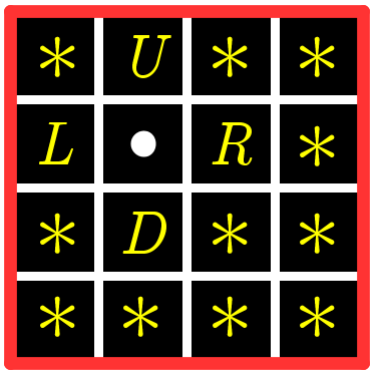


Figura 2.3

Donde los cuadrados etiquetados con un asterisco pueden ser cualquier número. Los posibles movimientos en el diagrama anterior son

$$R = R_{u,r,d,l} = (r, 16) = intercambiar\ r\ y\ 16,$$
$$L = L_{u,r,d,l} = (l, 16) = intercambiar\ l\ y\ 16,$$
$$U = U_{u,r,d,l} = (u, 16) = intercambiar\ u\ y\ 16,$$
$$D = D_{u,r,d,l} = (d, 16) = intercambiar\ d\ y\ 16,$$

Donde '16' denota el espacio vacío •.

Vamos a llamar al Puzzle 15 un **puzzle plano** dado que todas sus piezas se encuentran en un tablero. Este puzzle se discute en 4.4 más adelante.

2.2 Rainbow Masterball

El puzzle Rainbow Masterball simplemente se conocerá como una 'Masterball' en lo siguiente. La Masterball es una esfera que ha sido cortada como una manzana a lo largo de su núcleo en 8 trozos congruentes, cada uno con un color diferente. También se ha cortado tres veces en dirección ortogonal: visto como un globo, una vez a lo largo del ecuador, una vez a lo largo del Trópico de Cáncer, y una vez a lo largo del Trópico de Capricornio. De hecho, estas líneas se producen en aproximadamente 23 grados norte y sur del ecuador, no a 45 grados como lo vamos a describir a continuación.

Figura 2.4

Un camino geodésico desde el polo norte al polo sur es llamado **línea longitudinal** y un camino geodésico cerrado paralelo al ecuador es llamado una **línea latitudinal.** Hay 8 líneas longitudinales y 3 líneas latitudinales. En coordenadas esféricas $\theta, \phi,$ y ρ (θ es el ángulo medido a partir del ***plano*** xz, ϕ es el ángulo hacia abajo desde el eje z, ρ es el radio de la Masterball), las líneas longitudinales se encuentran en los ángulos que son múltiplos de $\pi/4$ radianes (es decir, en $\theta = n\,\pi/4$ radianes, $n = 1, \ldots, 8$) y las líneas latitudinales se encuentran en $\phi = \pi/4\ , \pi/2\ , 3\pi/4$ radianes. (Aquí $\pi = 3.141592\ldots$ como de costumbre.)
Sin estos segmentos latitudinales, se parece a una pelota de playa. Por lo tanto, una esfera Masterball tiene 32 piezas de 8 colores distintos. Vamos a suponer que la Masterball está en una posición fija en el espacio, centrado en el origen.
La esfera deberá estar orientada por la regla de la mano derecha: el pulgar de la mano derecha envolviendo a lo largo de los puntos de eje polar hacia el polo norte. Asumimos que una de las líneas longitudinales se ha fijado una vez por todas. Esta línea fija deberá ser etiquetada por '1', la siguiente línea (con respecto a la orientación anterior) como '2', y así sucesivamente.

Movimientos permitidos: Se puede girar la Masterball de este a oeste por múltiplos de $\pi/4$ a lo largo de cada una de las cuatro bandas latitudinales o en múltiplos de π en cada una de las 8 líneas longitudinales.
Una **cara** será una de las 32 subdivisiones de la Masterball creados por estos círculos. Una cara se considerará como una posición inmóvil sobre la esfera y etiquetada, ya sea por un número entero $i \in \{1, \ldots, 32\}$ o por una pareja $(i, j) \in [1, 4] \times [1, 8]$, que sea más conveniente en ese momento. Si una cara tiene ya sea el polo norte o el polo sur como un vértice entonces la llamamos una cara **pequeña** (o **polar**). De lo contrario, llamamos una cara **grande** (o **media** o **ecuatorial**). Una **coloración** de la Masterball será un etiquetado de cada cara de uno de los 8 colores de tal manera que

(a) cada uno de los 8 colores ocurre exactamente dos veces en el conjunto de las 16 caras pequeñas,

(b) cada uno de los 8 colores ocurre exactamente dos veces en el conjunto de las 16 caras grandes.

Un **movimiento** de la Masterball será un cambio en la coloración de la Masterball asociado con una secuencia de maniobras como se describió anteriormente.

Podemos identificar cada uno de los 8 colores con un número entero en $\{1, \dots, 8\}$ e identificar la colección de caras de la Masterball con una matriz 4×8 de enteros en este rango.
Para **resolver** una matriz se debe, por una secuencia adecuada de movimientos correspondientes a las rotaciones descritas anteriormente de la Masterball, poner esta matriz en un posición 'arco iris' para que las entradas de la matriz de cada columna tengan el mismo número. Así la matriz

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{matrix}$$

es "resuelta". La matriz

$$\begin{matrix} 6 & 7 & 8 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{matrix}$$

corresponde a una rotación de las caras polo norte por $3\pi/4$.
Notación. Nosotros usamos la notación de matrices para denotar a las 32 caras de la Masterball. Los generadores de rotaciones latitudinales se denotan r_1, r_2, r_3, r_4. Por ejemplo, r_1 envía

$$\begin{matrix} 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 \\ 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 \end{matrix}$$

a

$$\begin{matrix} 12 & 13 & 14 & 15 & 16 & 17 & 18 & 11 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 \\ 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 \end{matrix}$$

Al mirar hacia abajo a la pelota desde el polo norte, este movimiento hace girar la parte superior de la bola hacia la derecha, según las agujas del reloj. Los otros movimientos, r_2, r_3, r_4 rotan la banda asociada de la pelota en la misma dirección según las agujas del reloj, visto desde el polo norte. Los generadores de rotaciones longitudinales se denotan $f_1, f_2, \dots, f_8$. Por ejemplo, el movimiento $f_1 r_1$ envía

$$\begin{matrix} 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 \\ 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 \end{matrix}$$

a

$$\begin{matrix} 44 & 43 & 42 & 41 & 15 & 16 & 17 & 18 \\ 34 & 33 & 32 & 31 & 25 & 26 & 27 & 28 \\ 24 & 23 & 22 & 21 & 35 & 36 & 37 & 38 \\ 14 & 13 & 12 & 11 & 45 & 46 & 47 & 48 \end{matrix}$$

Con estas reglas, se puede comprobar la relación

$$f_5 = r_1^4 * r_2^4 * r_3^4 * r_4^4 * f_1 * r_1^4 * r_2^4 * r_3^4 * r_4^4.$$

Además, se puede comprobar que

$$r_1 = (f_3 * f_7)^{-1} * r_4^{-1} * f_3 * f_7 \, .$$

Identificar las caras de la Masterball con las entradas de la matriz

$$\begin{matrix} 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 \\ 24 & 23 & 22 & 21 & 20 & 19 & 18 & 17 \\ 32 & 31 & 30 & 29 & 28 & 27 & 26 & 25 \end{matrix}$$

Podemos expresar los generadores del grupo Masterball en la notación cíclica disjunta como un subgrupo de S_{32} (el grupo simétrico de grado 32):

$$r_1^{-1} = (1,2,3,4,5,6,7,8),$$
$$r_2^{-1} = (9,10,11,12,13,14,15,16),$$
$$r_3^{-1} = (17,18,19,20,21,22,23,24),$$
$$r_4^{-1} = (25,26,27,28,29,30,31,32),$$
$$f_1 = (5,32)(6,31)(7,30)(8,29)(13,24)(14,23)(15,22)(16,21),$$
$$f_2 = (4,31)(5,30)(6,29)(7,28)(12,23)(13,22)(14,21)(15,20),$$
$$f_3 = (3,30)(4,29)(5,28)(6,27)(11,22)(12,21)(13,20)(14,19),$$
$$f_4 = (2,29)(3,28)(4,27)(5,26)(10,21)(11,22)(12,23)(13,24),$$
$$f_5 = (1,28)(2,27)(3,26)(4,25)(9,20)(10,19)(11,18)(12,17),$$
$$f_6 = (8,27)(1,26)(2,25)(3,32)(16,19)(9,18)(10,17)(11,24),$$
$$f_7 = (7,26)(8,25)(1,32)(2,31)(15,18)(16,17)(9,24)(10,23),$$
$$f_8 = (6,25)(7,32)(8,31)(1,30)(14,17)(15,24)(16,23)(9,22).$$

2.3 Cubos de Rubik

Vamos a considerar brevemente los Cubos de Rubik $2 \times 2 \times 2$ y $3 \times 3 \times 3$.

2.3.1 Cubo de Rubik $2 \times 2 \times 2$

El Cubo de Rubik de 'bolsillo' tiene seis 'caras', cada una con $2 \cdot 2 = 4$ "caritas", para un total de 24 caritas:

Fijemos una orientación del Cubo de Rubik en el espacio. Es posible etiquetar los 6 lados como f, b, l, r, u, d ('frontal', 'posterior', 'izquierda', 'derecha', 'superior', 'inferior', respectivamente). El cubo de bolsillo tiene 8 subcubos. Cada cara del cubo está asociada a un 'corte' de 4 subcubos que comparten una carita con la cara. La cara, junto con todos los 4 cubos en el 'corte', se puede girar 90 grados según las agujas del reloj. Denotamos este movimiento por la letra mayúscula asociada a la letra minúscula que indica la cara. Por ejemplo, F denota el movimiento que hace girar la cara frontal 90 grados en sentido horario.

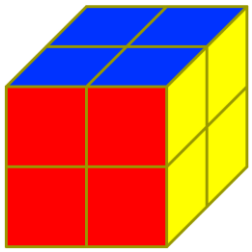


***Figura 2.5**: Etiquetando caritas en el Cubo de Rubik* $2 \times 2 \times 2$

Llamamos las 24 caritas del Cubo de Rubik 2×2 como en problema 1.3.3. Las 24 caritas se denotan por xyz, donde x es la cara en la cual la carita vive e y, z (o z, y-no importa) indican las dos aristas de la carita. Escrito en orden según las agujas del reloj, la 'notación Singmaster' es

Cara frontal	*fru*	*frd*	*fld*	*flu*
Cara posterior	*blu*	*bld*	*brd*	*bru*
Cara derecha	*rbu*	*rbd*	*rfd*	*rfu*
Cara izquierda	*lfu*	*lfd*	*lbd*	*lbu*
Cara superior	*urb*	*urf*	*ulf*	*ulb*
Cara inferior	*drf*	*drb*	*dlb*	*dlf*

Tabla 2.1

Para futuras referencias, llamamos a este sistema de notación (que también se utiliza para los Cubos de Rubik $3 \times 3 \times 3$ y $4 \times 4 \times 4$) la **notación Singmaster**, llamado en honor al matemático británico y entusiasta del Cubo de Rubik David Singmaster.

2.3.2 Cubo de Rubik $3 \times 3 \times 3$

En esta sección se dedica en su mayor parte a introducir la notación (debida a Singmaster [Si]) que nos permite comprobar que el puzzle es de hecho un puzzle de permutación.

El Cubo de Rubik tiene 6 caras, cada una con $3 \cdot 3 = 9$ 'caritas', para un total de 54 caritas. Dado que las caritas centrales son fijadas por los movimientos básicos, hay sólo $54 - 6 = 48$ caritas que necesitan etiquetado. Etiquetamos estas caritas $1, 2, \ldots, 48$ como en la figura 2.2.

Los generadores estándares, que corresponden a las seis caras del cubo, pueden ser escritos en notación cíclica disjunta como:

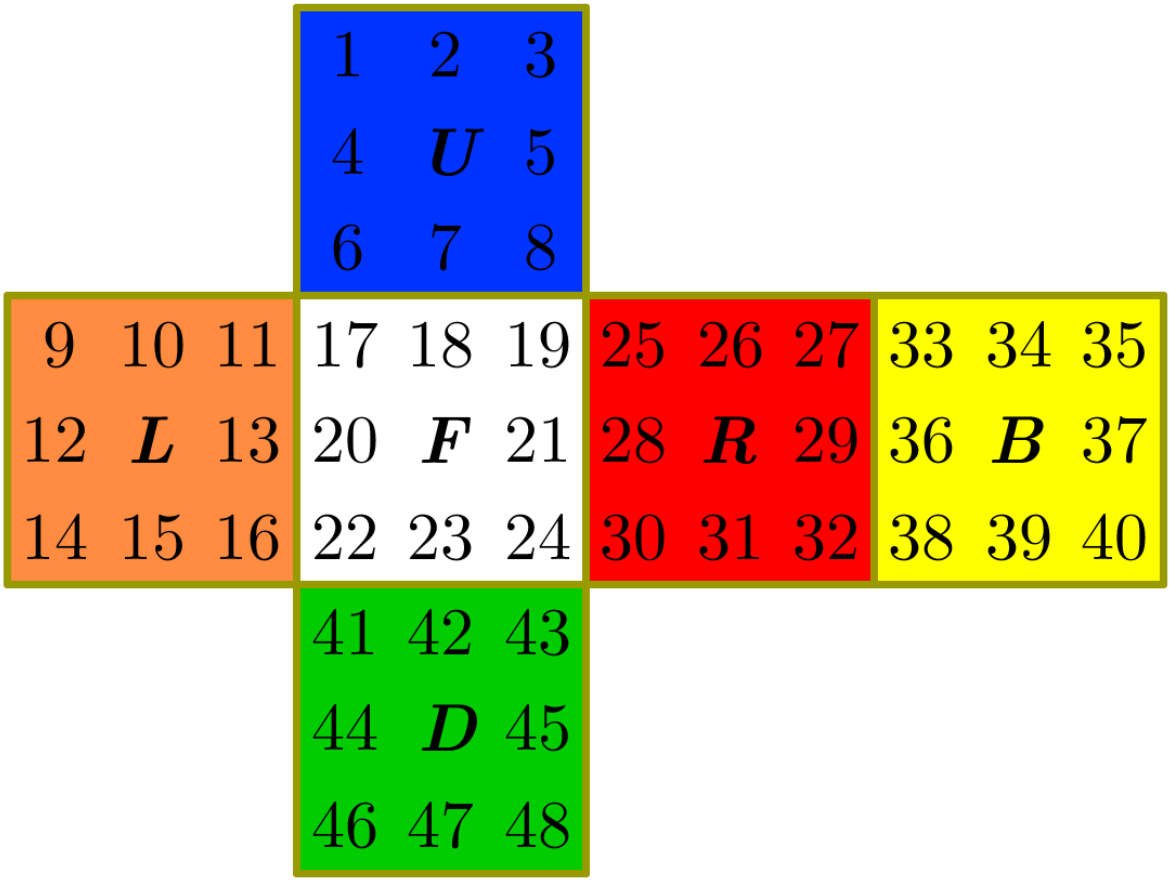


Figura 2.6: *Etiquetando caritas en el Cubo de Rubik* $3 \times 3 \times 3$

$F = (17, 19, 24, 22)(18, 21, 23, 20)(6, 25, 43, 16)(7, 28, 42, 13)(8, 30, 41, 11),$
$B = (33, 35, 40, 38)(34, 37, 39, 36)(3, 9, 46, 32)(2, 12, 47, 29)(1, 14, 48, 27),$
$L = (9, 11, 16, 14)(10, 13, 15, 12)(1, 17, 41, 40)(4, 20, 44, 37)(6, 22, 46, 35),$
$R = (25, 27, 32, 30)(26, 29, 31, 28)(3, 38, 43, 19)(5, 36, 45, 21)(8, 33, 48, 24),$
$U = (1, 3, 8, 6)(2, 5, 7, 4)(9, 33, 25, 17)(10, 34, 26, 18)(11, 35, 27, 19),$
$D = (41, 43, 48, 46,)(42, 45, 47, 44)(14, 22, 30, 38)(15, 23, 31, 39)(16, 24, 32, 40).$

La notación de las caritas será similar a la notación utilizada para el Cubo de Rubik $2 \times 2 \times 2$. Las caritas esquina tendrán la misma notación y las caritas arista se denotarán por xy, donde x es la cara en la cual se encuentra la carita e y es la cara de la carita adyacente. En orden según las agujas del reloj, empezando por la esquina superior derecha de cada cara, la 'notación Singmaster' es

Cara frontal	*fru*	*fr*	*frd*	*fd*	*fld*	*fl*	*flu*	*fu*
Cara posterior	*blu*	*bl*	*bld*	*bd*	*brd*	*br*	*bru*	*bu*
Cara derecha	*rbu*	*rb*	*rbd*	*rd*	*rfd*	*rf*	*rfu*	*ru*
Cara izquierda	*lfu*	*lf*	*lfd*	*ld*	*lbd*	*lb*	*lbu*	*lu*
Cara superior	*urb*	*ur*	*urf*	*uf*	*ulf*	*ul*	*ulb*	*ub*
Cara inferior	*drf*	*dr*	*drb*	*db*	*dlb*	*dl*	*dlf*	*df*

Tabla 2.2

2.3.3 Cubo de Rubik $4 \times 4 \times 4$

El cubo $4 \times 4 \times 4$ fue inventado por Péter Sebestény. Al contrario de lo que ocurre con el cubo original y con la versión $5 \times 5 \times 5$, no posee piezas fijas: las caras centrales, divididas en cuatro piezas, pueden moverse a diferentes posiciones.

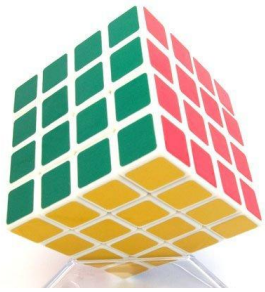


Figura 2.7

En el Cubo de Rubik $3 \times 3 \times 3$ la cara central indicaba el color de cada cara, ahora en él $4 \times 4 \times 4$ la cara central van a ser 4 caritas (lo que antes era una, ahora son 4 caritas), a diferencia del cubo $3 \times 3 \times 3$ las caras de en medio si se pueden mover, utilizamos la misma notación que para el cubo $3 \times 3 \times 3$ (ver Ejemplo 1.2.7)
Denotamos el conjunto de **movimientos básicos** por $\{U, D, L, R, F, B\}$, agregamos la notación para las "rebanadas intermedias" donde:

- u denota el movimiento del Cubo de Rubik que gira la rebanada intermedia adyacente a la cara superior un cuarto de vuelta en sentido horario.
- d denota el movimiento del Cubo de Rubik que gira la rebanada intermedia adyacente a la cara inferior un cuarto de vuelta en sentido horario.
- l gira la rebanada intermedia adyacente a la cara izquierda un cuarto de vuelta en sentido horario.
- r gira la rebanada intermedia adyacente a la cara derecha un cuarto de vuelta en sentido horario.
- f gira la rebanada intermedia adyacente a la cara frontal un cuarto de vuelta en sentido horario.
- b gira la rebanada intermedia adyacente a la cara posterior un cuarto de vuelta en sentido horario.

Finalmente H_L denota el movimiento del Cubo $4 \times 4 \times 4$ que gira la mitad izquierda en sentido horario, de manera similar para las demás mitades.

Figura 2.8 *Movimiento* H_L

2.4 Pyraminx

El Pyraminx (1981) es uno de los rompecabezas inventado por Uwe Méffert (1939 -), que también comercializa varios de sus inventos.
Un **tetraedro** es un sólido platónico regular de 4 lados, cuyas caras son triángulos equiláteros. En el Pyraminx, cada una de las 4 caras del puzzle se divide en 9 caritas triangulares.
Hay un total de $4 \cdot 9 = 36$ caritas en el Pyraminx. Serán etiquetadas como en las siguientes figuras.

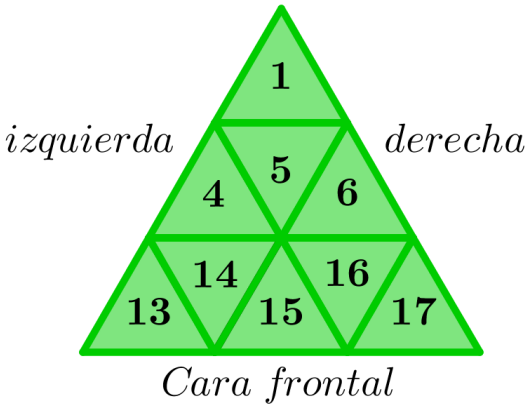


Figura 2.9

Figura 2.10

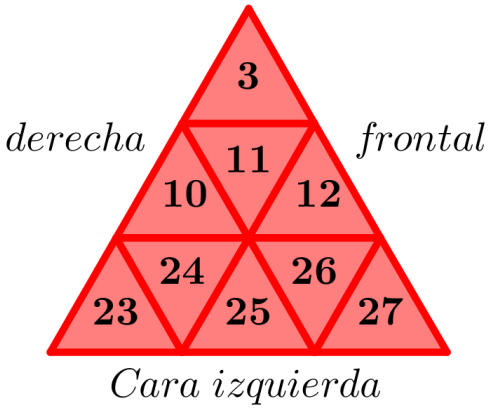


Figura 2.11

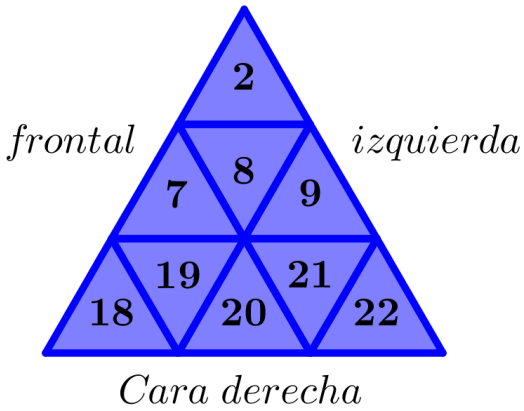


Figura 2.12

Fijamos una orientación del tetraedro en el espacio de modo que estemos mirando en una cara lo que llamamos el "frente". También podemos hablar de una cara "derecha", "izquierda", y la cara "inferior". Etiquetamos las 4 caras como f (frontal), d (derecha), i (izquierda), d (inferior). Etiquetamos los vértices U (superior), R (derecho), L (izquierdo) y B (posterior).

El tetraedro en sí ha sido subdividido en sub-tetraedros de la siguiente manera: para cada vértice X (tal que $X \in \{U, R, L, B\}$) hay una cara opuesta F del sólido.
Para cada cara, cortamos el sólido a lo largo de dos planos paralelos (en el vértice y en un sub-tetraedro) a la cara F y que están entre de la cara y el vértice igualmente espaciados. Los sub-tetraedros en el corte de la propia cara son llamados el **corte cara** asociado a la cara F, denotado F_1, los sub-tetraedros en el corte medio paralelo a la cara F serán llamados el **corte medio** asociado con esa cara, denotado F_2, y el sub-tetraedro que contiene el vértice X=U asociado a ese vértice, denotado F_3.

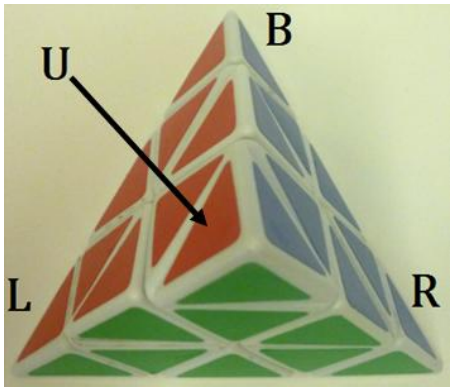


Figura 2.13

Para cada cara F etiquetada, tenemos una rotación de 120 grados en sentido horario del primer corte F_1 de la cara. Denotamos esta rotación también por F_1. Esta rotación sólo mueve las caritas del corte F_1. Análogamente, tenemos una rotación de 120 grados en sentido horario del segundo corte F_2 de la cara. Denotamos esta rotación como F_2. F_3 es la rotación de 120 grados del sub-tetraedro opuesto que contiene al vértice X. Estos movimientos permutan las etiquetas de las 36 caritas, y por lo tanto puede ser considerado como una permutación de los números del $1, 2, \ldots, 36$.
Por ejemplo, la rotación de 120 grados en sentido horario (mirando la cara frontal) del sub-tetraedro opuesto a la cara frontal se denota F_3. La notación cíclica disjunta para este movimiento, considerado como una permutación, es

$$F_3 = (23, 22, 36).$$

Los **movimientos básicos** son dados de la siguiente manera:

$$F_1 = (2, 32, 27)(8, 31, 26)(7, 30, 12)(19, 29, 11) \times$$
$$\times (18, 28, 3)(1, 17, 13)(6, 15, 4)(5, 16, 14)$$
$$F_2 = (9, 35, 25)(21, 34, 24)(20, 33, 10)$$
$$F_3 = (23, 22, 36)$$
$$R_1 = (3, 36, 17)(11, 34, 16)(10, 35, 6) \times$$
$$\times (24, 31, 5)(23, 32, 1)(2, 22, 18)(9, 20, 7)(8, 21, 19)$$
$$R_2 = (12, 33, 15)(26, 29, 14)(25, 30, 4)$$
$$R_3 = (27, 28, 13)$$
$$L_1 = (1, 28, 22)(5, 29, 21)(4, 33, 9) \times$$
$$\times (14, 34, 8)(13, 36, 2)(3, 27, 23)(11, 26, 24)(12, 25, 10)$$
$$L_2 = (6, 30, 20)(16, 31, 19)(15, 35, 7)$$
$$L_3 = (17, 32, 18)$$
$$D_1 = (13, 18, 23)(14, 19, 24)(15, 20, 25) \times$$
$$\times (16, 21, 26)(17, 22, 27)(28, 32, 36)(29, 31, 34)(30, 35, 33)$$
$$D_2 = (4, 7, 10)(5, 8, 11)(6, 9, 12)$$
$$D_3 = (1, 2, 3)$$

Todos los otros movimientos se obtienen mediante la combinación de estos movimientos secuencialmente. Queremos utilizar movimientos de forma $F_2 * F_3$, para cada cara F, pero la notación cíclica disjunta para estas permutaciones es un poco más complicada de escribir. Mas detalles acerca de este puzzle se dan en el Capítulo 8.

Capítulo 3

¿Qué es conmutatividad?

Una historia contada por Freeman Dyson (1923-), uno de los grandes físicos matemáticos de nuestro tiempo, es como sigue: En la primera parte del siglo pasado, el matemático Oswald Veblen y el físico James Jeans estaban discutiendo la reforma del currículo de matemáticas en la Universidad de Princeton. Jeans argumentó que la teoría de grupos debe omitirse, afirmando que la teoría de grupos es un tema que nunca va a ser de alguna utilidad a la física. Veblen debe haber ganado el argumento porque la teoría de grupos continuó siendo enseñada. Es realmente irónico que la teoría de grupos, no sólo se convirtió en uno de los temas centrales de la física, pero gran parte de la investigación innovadora en realidad se llevó a cabo en Princeton.
A groso modo, la teoría de grupos es el estudio matemático de simetría. El Cubo de Rubik muestra una notable cantidad de simetrías. Este capítulo es una introducción a la teoría de grupos, otra herramienta útil para el Cubo de Rubik.

Cuando estudiamos puzzles de permutación en el capítulo anterior, uno de los criterios fue que cada movimiento sea "invertible". Esto es, de hecho, una de las condiciones para el conjunto de todos los movimientos legales de un puzzle de permutación para formar un grupo.
Un grupo puede ser definido como un conjunto que tiene un pequeño número de propiedades. Una de estas propiedades es que debemos ser capaces de combinar dos elementos del conjunto de alguna manera en particular para obtener otro elemento. En el caso del Cubo de Rubik, si combina dos movimientos, obtiene otro movimiento. La manera abstracta precisa para declarar este tipo de propiedad es utilizando la noción de una “operación binaria”.
Una **operación binaria** $*$ en un conjunto no vacío G es una función que asocia cada par de elementos (g_1, g_2) de G un solo elemento g_3, también denotado $g_3 = g_1 * g_2$, en G:

$$* : G \times G \to G.$$

Un grupo G es un conjunto con una operación binaria $*$ (llamada ‘operación de grupo’) que satisface ciertas propiedades que se darán más adelante. Por ejemplo, una propiedad es que cualquier elemento tiene un ‘elemento inverso’ asociado con él. En el caso del Cubo de Rubik, si realizamos cualquier movimiento (o secuencia de movimientos), siempre se puede deshacer el efecto simplemente invirtiendo cada paso. Este ‘movimiento inverso’ es el ‘inverso’ del movimiento original, como veremos más adelante.

Antes de definir un grupo, debemos tomar la decisión sobre que notación utilizar para describir un grupo G. Si G es finito entonces una forma es listar todos los elementos de G y listar (o tabular) todos los valores de la función $*$. Otro método consiste en describir G en términos de algunas propiedades y luego definir una operación binaria $*$ en G. Cada método tiene sus ventajas y desventajas. Eventualmente, deberemos utilizar los dos métodos.
Empezamos con algunos ejemplos.

3.1 Cuaterniones

En el otoño de 1843, William R. Hamilton (1805-1865) estaba caminando a lo largo del Royal Canal en Irlanda con su esposa. Fue entonces que Hamilton encontró una generalización de los números complejos: los cuaterniones. Los cuaterniones son 'números' de la forma $a + bi + cj + dk$, donde $a, b, c, d \in \mathbb{R}$ son números reales, i es el usual $\sqrt{-1}$ j y k satisfacen

$$i^2 = j^2 = k^2 = ijk = -1$$

De hecho, Hamilton no pudo resistir el impulso de tallar las reglas básicas del producto para los cuaterniones en la piedra del puente de Brougham, mientras él y su esposa pasaban.
Se pueden sumar o restar fácilmente:

$$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k)$$
$$= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

Para multiplicar dos cuaterniones, se utiliza la ley distributiva y las reglas básicas de multiplicación para i, j, k dadas anteriormente. Una diferencia importante entre la multiplicación de dos cuaterniones q_1, q_2 juntos y la multiplicación de dos números reales r_1, r_2 juntos es que, en general, $q_1 q_2 \neq q_2 q_1$ (por ejemplo, $ij \neq ji$), mientras que siempre tenemos $r_1 r_2 = r_2 r_1$ (por ejemplo, $\sqrt{2} \cdot 3 = 3 \cdot \sqrt{2}$).
Sea Q el **grupo de cuaterniones**:

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

Los elementos de Q son conocidos como **cuaterniones unitarios**, los elementos satisfacen las reglas: $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$.
La multiplicación para este grupo se puede visualizar en la siguiente figura:

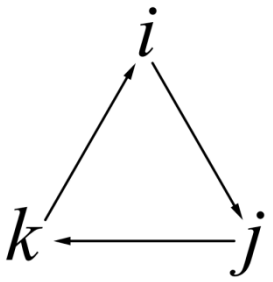


Figura 3.1

Si recorremos el triángulo en el sentido de las manecillas del reloj el producto de cualquier par de elementos sucesivos es el que sigue, y al recorrerse en sentido opuesto al del reloj se obtienen productos negativos, por ejemplo $ji = -k$.

3.2 Grupos cíclicos finitos

Considere el conjunto de movimientos del Cubo de Rubik $G = \{1, R, R^2, R^3\}$. Hacemos varias observaciones más o menos evidentes:

• Si realizamos cualquier rotación de la cara derecha del cubo no conseguiremos ningún movimiento nuevo. En particular, si componemos cualesquiera dos movimientos en este conjunto obtendremos otro movimiento en este conjunto.

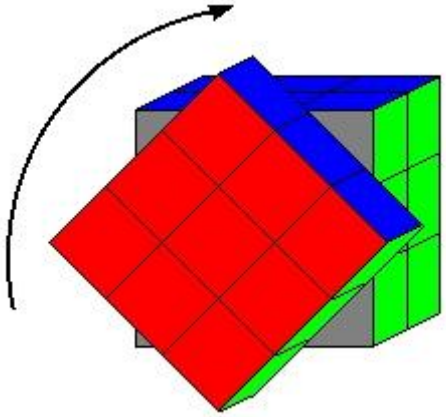


Figura 3.2

• El movimiento que 'deshace' el efecto de R se encuentra en este conjunto (de hecho, R seguido de R^3 es el movimiento identidad 1, por lo que R^3 debe 'deshacer' R).

• Si $* : G \times G \to G$ es simplemente el mapeo definido por el envío de un par (R^i, R^j), con $0 \leq i, j \leq 3$, a la composición de estos dos movimientos, $R^i * R^j = R^{i+j}$, entonces $*$ es una operación binaria.

Resulta que este conjunto G con esta operación $*$ es un ejemplo de un grupo.

Ejemplo 3.2.1. Sea C_{12} el conjunto cuyos elementos son $\{0, 1, \dots, 11\}$ la operación $*$ es simplemente 'adición mod 12'. Así es como se suman horas en un reloj, observar que '12 horas´ o '0 horas en punto' significan lo mismo). Así $5 + 8 = 1$, $1 + 11 = 0$, y así sucesivamente.

Este grupo es llamado el **grupo cíclico de orden 12**.

Definición 3.2.1. Sea $n > 1$ un número entero y sea C_n el grupo cuyos elementos son $\{0, 1, \dots, n-1\}$ y para los cuales la operación del grupo es simplemente la 'adición módulo n'. Este grupo es llamado el grupo cíclico (aditivo) de orden n. A menudo también se denota por $\mathbb{Z}/n\mathbb{Z}$.

Geométricamente, esto puede ser considerado como el grupo de todas las posibles rotaciones de un n -agono regular. Esta idea se explora con más detalle en 3.3.

3.3 El grupo diedro

Elegir un entero $n > 2$, y sea R un n -agono regular centrado sobre el origen en el plano. Si $n = 3$, entonces R es un triángulo equilátero, si $n = 4$, entonces R es un cuadrado, si $n = 5$, entonces R es un pentágono, y así sucesivamente. Sea G el conjunto de todas las transformaciones lineales del plano a sí mismo que preservan la figura de R. La operación

binaria $\circ : G \times G \to G$ dada por la composición de funciones da a G la estructura de un grupo. Este grupo es llamado el grupo de simetrías de R.
Si consideramos R como una figura en el espacio tridimensional centrado sobre el origen y sea G el conjunto de todas las transformaciones lineales del espacio tridimensional, entonces obtenemos un grupo ligeramente más grande en algunos casos (véase el Ejemplo 6.3.3 a continuación y [NST] para más detalles).

Etiquetando los vértices del n-agono como $1, 2, \dots, n$. El grupo G permuta éstos vértices entre ellos mismos, por lo que, cada $g \in G$ puede ser considerado como una permutación del conjunto de vértices $V = \{1, 2, \dots, n\}$. De esta manera, podemos considerar a G como un grupo de permutación, ya que es el subgrupo de S_n generado por los elementos de G.

El hecho de que este grupo tiene $2n$ elementos sigue de un argumento de conteo simple: Sea $r \in G$ el elemento que gira R por $2\pi/n$ radianes en sentido antihorario alrededor del centro. Sea L un eje de simetría de R que divide la figura en dos mitades. Sea s el elemento de G que es la reflexión sobre L. Hay n rotaciones por un múltiplo de $2\pi/n$ radianes alrededor del centro en $G : 1, r, r^2, \dots, r^{n-1}$. Hay n elementos de G que están compuestos de una reflexión sobre L y una rotación de un múltiplo de $2\pi/n$ radianes alrededor del centro: $s, s \circ r, s \circ r^2, \dots, s \circ r^{n-1}$. Estos comprenden todos los elementos de G.
El grupo simétrico de R es conocido como el grupo diedro de orden $2n$, denotado D_n. (Nota: Algunas personas denotan este grupo, en lugar de D_{2n}.)

Ejemplo 3.3.1. Sea G el grupo simétrico del cuadrado, es decir, el grupo de simetrías del cuadrado generado por los movimientos rígidos

$g_0 =$ es una rotación en sentido horario alrededor de O, en un ángulo de 90 grados,
$g_1 =$ reflexión respecto a l_1 ,
$g_2 =$ reflexión respecto a l_2 ,
$g_3 =$ reflexión respecto a l_3 ,
$g_4 =$ reflexión respecto a l_4 ,

donde l_1, l_2, l_3 denotan los ejes de simetría en la siguiente figura:

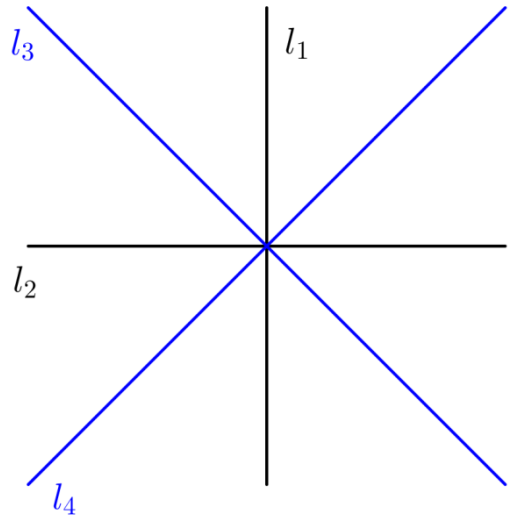


Figura 3.3

Los elementos de G son $1, g_0, g_0^2, g_0^3, g_1, g_2, g_3, g_4$.
Sea X el conjunto de vértices del cuadrado. Entonces G actúa sobre X.

3.4 El grupo simétrico

El arte de hacer matemáticas consiste en encontrar un caso especial que contenga todos los gérmenes de la generalidad.

David Hilbert

Antes de las definiciones, vamos a dar un poco de motivación para algunas nociones generales que se presentarán más adelante. Cada movimiento del Cubo de Rubik puede ser considerado como una permutación del conjunto de 54 caritas del cubo. Es natural desde nuestra perspectiva para el estudio de permutaciones, como Hilbert nos aconsejó, buscar un caso especial muy bueno para centrar nuestra atención en él, y el grupo Cubo de Rubik es el ejemplo que utilizaremos.
Primero, algunas ideas básicas para que podamos empezar.

Sea X un conjunto finito y sea S_X el conjunto de todas las permutaciones de X sobre sí mismo:

$$S_X = \{f : X \to X \mid f \text{ es una biyección}\}$$

Este conjunto tiene las siguientes propiedades:

1. Si f, g pertenecen a S_X entonces fg (la composición de estas permutaciones) también pertenece a S_X ('cerrado bajo composición').

2. Si f, g, h pertenecen a S_X entonces $(fg)h = f(gh)$ ('asociatividad').

3. La permutación identidad $I : X \to X$ pertenece a S_X ('existencia de la identidad').

4. Si f pertenece a S_X entonces la permutación inversa f^{-1} también pertenece a S_X ('existencia del inverso').

El conjunto S_X es llamado el grupo simétrico de X. En el caso particular en que $X = \{1, 2, \dots, n\}$, escribimos $S_X = S_n$. S_n es el grupo simétrico de grado n.

Ejemplo 3.4.1. Supongamos que $X = \{1, 2, 3\}$. Podemos describir S_X como

$$S_X = \{I, s_1 = (1,2), s_2 = (2,3), s_3 = (1,3,2), s_4 = (1,2,3), s_5 = (1,3)\}.$$

Podemos calcular todos los productos posibles de dos elementos del grupo y tabularlos en una tabla de multiplicación como

	I	s_1	s_2	s_3	s_4	s_5
I	I	s_1	s_2	s_3	s_4	s_5
s_1	s_1	I	s_3	s_2	s_5	s_4
s_2	s_2	s_4	I	s_5	s_1	s_3
s_3	s_3	s_5	s_1	s_4	I	s_2
s_4	s_4	s_2	s_5	I	s_3	s_1
s_5	s_5	s_3	s_4	s_1	s_2	I

Tabla 3.1 *Tabla de multiplicar*

Tomamos las cuatro propiedades anteriores del grupo simétrico como las cuatro propiedades que definen un grupo. La siguiente definición de grupo la formuló por primera vez Cayley en 1854.

Definición 3.4.1. Se dice que un conjunto no vacío G es un **grupo** si en él hay definida una operación binaria $*$

$$\begin{array}{rccc} * : & G \times G & \to & G \\ & (g_1, g_2) & \mapsto & g_1 * g_2 \end{array}$$

tal que:

(G1) Si $g_1,\ g_2 \in G$, implica que $g_1 * g_2 \in G$ (G es **cerrado** respecto a $*$),

(G2) Dados $g_1,\ g_2, g_3 \in G$ entonces $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ (Es válida la **ley de asociatividad** en G),

(G3) Existe un elemento $e \in G$ tal que $e * g = g * e = g$ para todo $g \in G$ (e se llama **elemento identidad** o **unidad** de G),

(G4) Para todo $g \in G$ existe un elemento $g^{-1} \in G$, llamado el **inverso de** g tal que $g * g^{-1} = g^{-1} * g = e$ (Existencia del inverso).

Por ejemplo, si R es el movimiento Cubo de Rubik asociado con la rotación de la cara derecha un cuarto de vuelta, entonces $R^{-1} = R^3$.

Observación 3.4.1. En general, cuando un conjunto G y una operación binaria $*$ son explícitamente dados y cuando $(G,\ *)$, se espera que sea un grupo, generalmente la condición más difícil de verificar es la asociatividad. En el caso especial cuando G es un conjunto de permutaciones de un conjunto X y $*$ es simplemente la multiplicación usual de permutaciones, la asociatividad es fácil de verificar, ya que todos los elementos de G son funciones (de X a X) y la operación binaria es la función composición.

Ejemplo 3.4.2. En realidad, este es un 'no-ejemplo'. Sea S el conjunto de todos los movimientos legales (uno puede eventualmente hacer un movimiento a partir de una posición dada obtenida legalmente) del Puzzle 15 (como se describe en el capítulo 2). En una posición dada, por ejemplo, la posición resuelta, no hay muchas posibilidades: hay sólo 2 movimientos en la posición resuelta y nunca hay más de 4 movimientos posibles desde cualquier posición.

Desde la posición resuelta podemos mover $(15, 16)$ y $(12, 16)$ (donde 16 denota el cuadrado vacío), pero no podemos mover, por ejemplo $(1, 16)$. Puesto que $(15, 16), (12, 16) \in S$ y puesto que $(12, 16)$ $(15, 16)$ no es un movimiento legal, se sigue que la composición de movimientos legales no siempre es legal. Esto demuestra que la composición no es una operación binaria, así la propiedad $(G1)$, no se mantiene.

Lema 3.4.1. (Ley de Cancelación) Sea G un grupo y $a, b, c \in G$. Si $a * c = b * c$, donde $a, b, c \in G$, entonces a $a = b$.

En la definición anterior, no hemos asumido explícitamente que el elemento identidad e de G, sea único. (Supongamos que hay dos elementos identidad en G, denotados e_1, e_2 digamos. Por definición, $e_1 = e_1 * e_2 = e_2$. Del mismo modo, si G es un grupo y $g \in G$ entonces el elemento inverso de g es único. Hay otras propiedades de un grupo que pueden ser derivadas de $(G1) - (G4)$. Vamos a demostrarlas según sea necesario.

La **tabla de multiplicar** (también llamada 'tablas de Cayley' en honor a Cayley, quien fue el primero en introducirlas) de un grupo finito G es una tabulación de los valores de la operación binaria $*$, como en el Ejemplo 3.4.1 Sea $G = \{g_1, \ldots, g_n\}$. La tabla multiplicación de G es

$*$	g_1	g_2	$\cdots$	g_j	$\cdots$	g_n
g_1						
g_2						
$\vdots$						
g_i				$g_i * g_j$		
$\vdots$						
g_n						

Tabla 3.2

Algunas propiedades:

Lema 3.4.2.

(a) Cada elemento $gk \in G$ ocurre exactamente una vez en cada fila de la tabla.

(b) Cada elemento $gk \in G$ ocurre exactamente una vez en cada columna de la tabla.

(c) Si la entrada (i, j) de la tabla es igual a la entrada (j, i), entonces, $g_i * g_j = g_j * g_i$.

(d) Si la tabla es simétrica respecto a la diagonal, entonces $g * h = h * g$ para todo $g, h \in G$. (En este caso, llamamos a G **abeliano**.)

Los grupos abelianos llevan el nombre del matemático noruego Niels Abel (1802-1829). La corta vida de Abel fue trágica, marcada por la pobreza y la muerte de su padre en 1820. Sin embargo, él tenía un gran talento matemático y demostró antes de Galois que las raíces del polinomio de 5 º grado en general,

$$x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0,$$

no se pueden expresar en términos de únicamente radicales. (Galois demostró un resultado más general unos seis años más tarde.) Por desgracia, su salud no era buena, y durante un viaje para visitar a su novia en la Navidad de 1828 cayó gravemente enfermo y murió. En su corta vida, Abel hizo importantes contribuciones a otras áreas de las matemáticas y fue galardonado con el Gran Premio en matemáticas por la Academia de París en 1830.

Definición 3.4.2. Sean g y h dos elementos de un grupo G. Decimos que g **conmuta** con h (o que g, h **conmutan**) si $g * h = h * g$. Llamamos a un grupo **conmutativo** (o **abeliano**) si todo par de elementos g, h pertenecientes a G conmutan. Si G es un grupo que es no necesariamente conmutativo, entonces llamamos a G **no conmutativo** (o **no abeliano**).

Ejemplo 3.4.3.

• Los elementos en $G = \{1, R, R^2, R^3\}$ todos conmutan entre sí, por lo que G es un grupo abeliano.

• Los números enteros, con la adición ordinaria como la operación del grupo, constituye un grupo abeliano.

Ahora que sabemos la definición de grupo, surge la pregunta: ¿cómo se puede describir? La respuesta más simple es que se podría hacer una lista con todos sus elementos y dar la "tabla de multiplicar", o podríamos describir todos sus elementos y su multiplicación en términos de alguna propiedad de la cual podemos verificar las cuatro propiedades de grupo. Aunque la primera forma tiene la ventaja de ser explícita, es esta segunda alternativa que es la más común, ya que suele ser más concisa.

Nuestro objetivo es introducir la terminología y las técnicas que nos permitan analizar los 'puzzles de permutación' matemáticamente. Los tipos de grupos que surgen en este contexto se definen a continuación.

Definición 3.4.3. Sea X un conjunto finito. Sea $S = \{g_1, g_2, \dots, g_n\}$ un conjunto finito de permutaciones de X (de modo que todos ellos pertenecen a S_X). Sea G el conjunto de todos los productos posibles de la forma

$$g = x_1 * x_2 \cdots * x_m , \qquad m > 0,$$

donde cada uno de los $x_1, \dots, x_m$ se toma del conjunto S. El conjunto G, junto con la operación binaria dada por la composición de permutaciones, es llamado un **grupo de permutación** con **generadores** $g_1, \dots, g_n$ (o el grupo de permutación generado por S). A veces escribimos

$$G = \langle g_1, \dots, g_n \rangle \subset S_X .$$

Ejemplo 3.4.4.

- Si $X = \{1, 2, \dots, 54\}$ y $S = \{(1, 2, 3, \dots, 54)\} \subset S_{54}$ entonces el grupo de permutación generado por S es un grupo cíclico G con elementos $\{1, g, g^2, \dots, g^{53}\}$.
- Sea X el conjunto de 54 caritas del Cubo de Rubik y sean $R, L, U, D, F, B \in S_X$ los movimientos básicos del Cubo de Rubik, en la notación introducida en el capítulo anterior. El grupo de permutación

$$G = \langle R, L, U, D, F, B \rangle \subset S_X$$

es llamado el **grupo Cubo de Rubik**. Vamos a determinar la 'estructura' de este grupo (es decir, su relación con 'grupos conocidos') más adelante en este trabajo.

Lema 3.4.3. Un grupo de permutación es un grupo.

Prueba: Sea G un grupo de permutación como en la definición anterior.
Nos limitaremos a demostrar que cada $g \in G$ tiene un inverso. El conjunto $\{g^n \mid n \geq 1\} \subset S_X$ es finito. Hay $n_1 > 0$, $n_2 > n_1$ tal que $g^{n_1} = g^{n_2}$. Entonces $g^{-1} = g^{n_2 - n_1 - 1}$ puesto que $g \cdot g^{n_2 - n_1 - 1} = 1$.

Definición 3.4.4. Si G es un grupo, entonces el **orden** de G, denotado $|G|$, es la cardinalidad de G. (En otras palabras, si G es un conjunto finito entonces su orden es el número de elementos de G, y si G no es finito entonces $|G| = \infty$.) Si g es un elemento del grupo G, entonces el **orden de** g, denotado $ord(g)$, es el mínimo entero positivo m tal que $g^m = 1$, si es que existe. Si por ejemplo un número m no existe, entonces decimos que g tiene **orden infinito**.

- Matemáticamente, más adelante veremos (en el anexo) por qué el grupo Cubo de Rubik G tiene orden $2^{27}3^{14}5^3 7^2 11$, (aproximadamente 4.3×10^{19}).

- Hay una permutación impar de orden 42 en S_{12},
  por ejemplo, $(1,2)(3,4,5)(6,7,8,9,10,11,12)$. Hay una permutación par de orden 15 en S_8, por ejemplo $(1,2,3)(4,5,6,7,8)$.

- Hay un elemento en el grupo Cubo de Rubik, cuyo orden es 1260 y no hay ningún elemento de orden superior. J. Butler, encontró el siguiente movimiento de este orden: $m = RU^2D^{-1}BD^{-1}$ (ver el libro de Bandelow de [B1], página 51, para otro movimiento simple de orden de 1260).

3.4.1 Teorema de Cauchy

(a) Sea p un número primo que divide al $|G|$, entonces G contiene un elemento g de orden p.

(b) Sea n un entero que no divide al $|G|$. No existe un $g \in G$ de orden n.

Augustin Louis Cauchy (1789-1857) hizo contribuciones significativas a muchas ramas de las matemáticas y fue uno de los más grandes matemáticos de su tiempo.
La parte (a) será demostrada en 3.10 a continuación (ver Corolario 3.10.2) y la parte (b) es un corolario del Teorema 3.5.1 que vamos a ver a continuación.

Aplicación. Como el grupo Cubo de Rubik G tiene la propiedad de que $|G| = 2^{27}3^{14}5^3 7^2 11$, se sigue de esto y la parte (b) del teorema anterior que no hay movimiento del Cubo de Rubik de orden 13 (ya que el 13 no divide a $|G|$), pero hay uno de orden 11. (Dicho esto, sólo porque sabemos que existe un movimiento de orden de 11 no significa que ¡sepamos cómo encontrar uno!) Esto es equivalente a decir existe un subgrupo cíclico del grupo Cubo de Rubik de orden 11. No hay ningún subgrupo cíclico de grupo Cubo de Rubik de orden 13.

Definición 3.4.5. G es un grupo **cíclico** si y sólo si $\exists\ a \in G\ \forall\ g \in G, : g = a^j$ para algún $j \in \mathbb{Z}$

Lema 3.4.4. Si $G = \langle g \rangle$ es un grupo cíclico finito con generador g entonces $|G| = ord(g)$.

Demostración: Sea $m = ord(g)$, por lo que $g^m = 1$. Podemos listar todos los elementos de G como sigue:

$$1, g, g^2, \dots, g^{m-1}.$$

Hay m elementos en esta lista.

3.4.2 El juego Gordon

Sea $(G, *)$ un grupo finito, escrito $G = \{g_0 = \text{la identidad}, g_1, \dots, g_n\}$

así que $g_0 = 0$ si $*$ es la suma y $g_0 = 1$ si $*$ es la multiplicación o composición. Usted y su oponente comparten un conjunto de **fichas de M**, denotadas

$$M = \{g_1, \dots, g_n\},$$

y **fichas de P**, denotadas

$$P = \{g_1, \dots, g_n\}.$$

Reglas para el juego:

- Los jugadores alternan turnos. Cada turno consiste en retirar una ficha de movimiento y una ficha de lugar de acuerdo con las condiciones listadas a continuación. La primera persona que no pueda hacer una jugada legal pierde.
- Sea $m_0 = p_0 = 1$ (o $m_0 = p_0 = 0$, si G está escrito aditivamente) y sea $i = 1$.
- El primer jugador escoge cualquier ficha de movimiento $m_1 = M$ y la ficha de lugar $p_1 = m_1 = P$. Estas fichas m_1 y p_1 son entonces retiradas de M y P, respectivamente.
- El siguiente jugador escoge una ficha de movimiento m_{i+1} y una ficha de lugar p_{i+1} tal que $p_{i+1} = m_{i+1}\, p_i \in P$. Estas fichas m_{i+1} y p_{i+1} son entonces retiradas de M y P, respectivamente.
- Incrementar i e ir al paso anterior.

Ejemplo 3.4.5. Sea $G = \mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$,

en la notación de la Definición 3.2.1. Los movimientos de un juego son determinados por el registro de las fichas de movimiento. Un juego posible es posible

•	4	1			3	2
0	1	2	3	4	5	6

donde el • sobre el elemento identidad 0 del grupo indica que no se mueve y los números por encima de un elemento del grupo indican cuando fue movido:

$\boldsymbol{jugador}$	$\boldsymbol{m}$	$\boldsymbol{p}$	$\boldsymbol{P}$	$\boldsymbol{M}$
1	$m_1 = 2$	$p_1 = 2$	$\{1,3,4,5,6\}$	$\{1,3,4,5,6\}$
2	$m_2 = 4$	$p_2 = 2 + 4 = 6$	$\{1,3,4,5\}$	$\{1,3,5,6\}$
1	$m_3 = 6$	$p_3 = 6 + 6 = 5$	$\{1,3,4\}$	$\{1,3,5\}$
2	$m_4 = 3$	$p_4 = 3 + 5 = 1$	$\{3,4\}$	$\{1,5\}$

El segundo jugador gana.

Observación 3.4.2. Si $G = \mathbb{Z}/p\mathbb{Z}$ (el grupo cíclico con p elementos) hay una conjetura de que el 2do jugador tiene una estrategia ganadora cuando $p > 5$. Para los grupos más generales, las estrategias no son conocidas. De hecho, ni siquiera se han conjeturado.

Observación 3.4.3. Si usted y su oponente intentan alargar el juego al mayor tiempo posible, ¿puede agotar el conjunto de fichas de movimiento y el conjunto de fichas de lugar? La respuesta es conocida para los grupos abelianos, grupos diedros y los grupos de orden > 32. La respuesta general parece ser desconocida.

3.5 Subgrupos

Como ya se señaló, el conjunto de movimientos del Cubo de Rubik forman un grupo G bajo la operación de composición. Supongamos que consideramos un subconjunto de G que también es un grupo bajo composición. Este subconjunto es llamado un 'subgrupo'. Por ejemplo, $\{1, R, R^2, R^3\}$ es un subgrupo de G.

Definición 3.5.1. Sea G un grupo. Un **subgrupo** de G es un subconjunto H de G tal que H, junto con la operación $*$ heredada como un subconjunto de G, satisface las operaciones del grupo $(G1) - (G4)$, (con G reemplazado por H por todas partes).

Notación: Si G es un grupo, entonces denotaremos la afirmación 'H es un subgrupo de G' por $H \subset G$.

Ejemplo 3.5.1.

• $2\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$.

• $2\mathbb{Z}/10\mathbb{Z} = \{0, 2, 4, 6, 8\}$ (con suma mod 10) es un subgrupo de $\mathbb{Z}/10\mathbb{Z}$.

• $H = \{1, (1,2,3), (1,3,2)\}$ es un subgrupo de S_3.

• Un grupo de permutación G generado por elementos $g_1, \dots, g_n$ pertenecientes a S_X es un subgrupo de S_X, es decir, $G \subset S_X$.

Uno podría preguntarse: ¿cuáles son todos los subgrupos del grupo Cubo de Rubik? Desafortunadamente, resulta que esta pregunta es muy poco práctica. Hay muchos subgrupos por listar, por lo que una respuesta simple no es posible. De hecho, nadie sabe exactamente cuántos subgrupos tiene el grupo Cubo de Rubik. Nos gustaría un criterio fácil de usar para saber cuando un determinado subgrupo H de S_{54} es un subgrupo del grupo Cubo de Rubik G. Este tipo de condición no parece existir, al menos no en una forma práctica, pero el siguiente criterio es muy útil. Otra versión del siguiente resultado se dará en el Teorema 3.10.1 a continuación.

Teorema 3.5.1. (Teorema de Lagrange) Si G es un grupo finito y H es un subgrupo de G, entonces $|H|$ divide a $|G|$.

Vale la pena señalar que, contrariamente a lo que pudiera sugerir el nombre del resultado, el teorema de Lagrange, en la forma establecida aquí, no se debe a Lagrange. En la forma dada, el teorema de Lagrange (para los grupos de permutaciones) fue probablemente conocido por Galois y apareció en las obras de Serret y Camile Jordan en la década de 1860.

Prueba: Para $x, y \in G$, definimos $x \sim y$ si $xH = yH$, donde

$$xH = \{x * h \mid h \in H\}.$$

Esto es una relación de equivalencia. (Se puede comprobar fácilmente las propiedades reflexiva, simétrica y transitiva.) Por otra parte, la clase de equivalencia de x consiste de todos los elementos de G de la forma $x * h$, para algún $h \in H$, es decir, $[x] = xH$. Sean $g_1, \dots, g_m \in G$ un conjunto completo de representantes de las clases de equivalencia de G. Debido a la ley de cancelación para grupos, $|xH| = |H|$ para cada $x \in G$. Por otro lado, sabemos que las clases de equivalencia particionan a G, por lo que

$$G = \bigcup_{i=1}^{m} [g_i] = \bigcup_{i=1}^{m} g_i H.$$

Comparando cardinalidades de ambos lados, obtenemos $|G| = |g_1 H| + \cdots + |g_m H| = m|H|$. Esto demuestra el teorema.

J. Durbin hace un tratamiento de las relaciones de equivalencia previo al teorema de Lagrange y explica el hecho de que toda relación de equivalencia induce una partición en el conjunto dado.

Definición 3.5.2. Si H y G son grupos finitos y $H \subset G$, entonces $|G|/|H|$ (que es un número entero por el teorema de Lagrange 3.5.1, más arriba) es llamado el índice de H en G, denotado $[G : H] = |G|/|H|$.

Ejemplo 3.5.2. Sea $A_n = \{g \in S_n \mid g \text{ es par}\}$.

Este es un subgrupo de S_n llamado el grupo alternante de grado n. Es conocido (y no es difícil de probar usando clases laterales) que $|A_n| = |S_n|/2$.

Definición 3.5.3. El centro de un grupo G es el subgrupo $Z(G)$ de todos los elementos que conmutan con todos los elementos de G:

$$Z(G) = \{z \in G \mid z * g = g * z, \forall\, g \in G\}.$$

Observe que

- El elemento identidad siempre pertenece a $Z(G)$. (Si el elemento identidad es el único elemento de $Z(G)$, entonces decimos que G tiene un **centro trivial**.)

- G es conmutativo si y sólo si $G = Z(G)$.

Problema 3.5.1. Sea $G = S_3$. Determine $Z(G)$ usando cálculos explícitos.
Si $n \geq 3$, demostrar que $Z(S_n)$ tiene un centro trivial. (Sugerencia: considere los elementos que conmutan con todos los n-ciclos.)

Para el centro del grupo Cubo de Rubik, véase 3.6.1 y Corolario 7.2.2 a continuación.

3.6 Ejemplos

Hay muchos puzzles en el mercado que dan lugar a los grupos de interés en las matemáticas. Unos ejemplos simples se dan en esta sección. Ejemplos más complicados se estudiaran más adelante.

Ejemplo 3.6.1. Considere un tablero de ajedrez infinito, el cual nos imaginamos es colocado en el plano cartesiano.

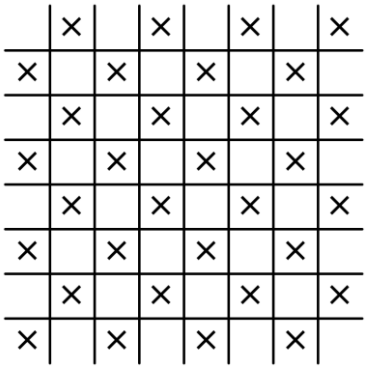


Figura 3.4

Etiquetemos un cuadrado como $(0, 0)$ y lo llamamos el **origen**. Etiquetemos los demás (m, n), como si etiquetaremos los vértices en una red en el plano. Coloque sólo una pieza de ajedrez, un rey, en $(0, 0)$. Etiquetamos el movimiento un cuadrado a la derecha por x, un cuadrado a la izquierda por x^{-1}, el movimiento un cuadrado hacia adelante por y, un cuadrado hacia atrás por y^{-1}, y etiquetamos los demás movimientos por xy, $x^{-1}y$, $x^{-1}y^{-1}$, y xy^{-1}, de la manera obvia. El conjunto de todos los movimientos posibles del rey pueden ser identificados con el conjunto

$$\{x^m y^n \mid m, n \in \mathbb{Z}\}$$

Este es un grupo abeliano infinito bajo multiplicación. El número de formas en que el rey puede llegar al cuadrado (m, n) en N movimientos es el coeficiente $K_N(m, n)$, de $x^m y^n$ en la expansión de

$$(x + x^{-1} + y + y^{-1} + xy + x^{-1}y + x^{-1}y^{-1} + xy^{-1})^N.$$

Para más detalles sobre esta construcción se pueden encontrar en el capítulo 'Wanderungen von Schachfiguren' por K. Fabel. Hay exactamente

$$K_{10}(1, 1) = 19246920 \approx 1.9 \times 10^7$$

formas de llegar a $(1, 1)$ desde el origen en 10 movimientos.

Ejemplo 3.6.2. Sea M_R la rotación del corte medio paralelo al lado derecho en un ángulo de 90 grados. Definir M_F, por la cara frontal, y M_U de manera similar. Considerar el subgrupo H del grupo Cubo de Rubik generado por los movimientos corte cuadrados,

$$H = \langle M_R^2 , M_F^2 , M_U^2 \rangle$$

Entonces $H = \langle M_R^2 \rangle \times \langle M_F^2 \rangle \times \langle M_U^2 \rangle \cong C_2 \times C_2 \times C_2 \times C_2 = C_2^3$, donde C_n denota el grupo cíclico de orden n.

3.6.1 El superflip

La colección de todos los movimientos del Cubo de Rubik puede ser vista como un subgrupo G de S_{48}. Denotamos la multiplicación en S_{48} (y por lo tanto en G) por $(\cdot)$.
El centro de G consiste de exactamente dos elementos, la identidad y el movimiento **superflip** que tiene el efecto de mover de un tirón cada arista, dejando todas las esquinas fijas y dejando todos los subcubos en su posición original ([B1], página 48):

$$Z(G) = \{1, \text{superflip}\}.$$

Más tarde, en 7.2, veremos que esto es una consecuencia del 'segundo teorema fundamental de la teoría del cubo'. Un movimiento para el superflip es

$$\begin{aligned}\text{superflip} &= R \cdot L \cdot F \cdot B \cdot U \cdot D \cdot R \cdot L \cdot F \cdot B \cdot U \cdot F^2 \cdot M_R \cdot F^2 \cdot U^{-1} \cdot M_R^2 \cdot B^2 \cdot U \cdot M_R^2 \cdot D \\ &= R \cdot L \cdot F \cdot B \cdot U \cdot D \cdot R \cdot L \cdot F \cdot B \cdot U \cdot F^2 \cdot R^{-1} \cdot L \cdot D^2 \cdot F^{-1} \cdot R^2 \cdot L^2 \cdot D^2 \cdot R \cdot \\ &\quad \cdot L^{-1} \cdot F^2 \cdot D \cdot R^2 \cdot L^2 \cdot D \ \ (34 \text{ cuartos de vuelta}),\end{aligned}$$

donde M_R es la rotación del corte medio paralelo al lado derecho en un ángulo de 90 grados. Otras expresiones para el superflip son el movimiento de Dik T. Winter

$$\begin{aligned}\text{superflip} &= F \cdot B \cdot U^2 \cdot R \cdot F^2 \cdot R^2 \cdot B^2 \cdot U^{-1} \cdot D \cdot F \cdot U^2 \cdot R^{-1} \cdot L^{-1} \cdot U \cdot B^2 \cdot D \cdot \\ &\quad \cdot R^2 \cdot U \cdot B^2 \cdot U \ (28 \text{ cuartos de vuelta})\end{aligned} \tag{3.1}$$

y la expresión de Mike Reid (encontrada con una computadora)

$$\begin{aligned}\text{superflip} &= R^{-1} \cdot U^2 \cdot B \cdot L^{-1} \cdot F \cdot U^{-1} \cdot B \cdot D \cdot F \cdot U \cdot D^{-1} \cdot L \cdot D^2 \cdot F^{-1} \cdot R \cdot B^{-1} \cdot \\ &\quad \cdot D \cdot F^{-1} \cdot U^{-1} \cdot B^{-1} \cdot U \cdot D^{-1} \ (24 \text{ cuartos de vuelta})\end{aligned}$$

En cuanto a este último movimiento, Jerry Bryan (el 19 de febrero de 1995, anunció la lista de correos electrónicos de los amantes del cubo, [CL]) mostró que no hay un número menor de movimientos de un cuarto de vuelta tomados de

$$\{R, R^{-1},\ L, L^{-1},\ U, U^{-1},\ D, D^{-1},\ B, B^{-1},\ F, F^{-1}\},$$

que también dará el superflip. En jerga, el movimiento de Mike Reid es 'mínimo en la métrica de un cuarto de vuelta'.

Observación 3.6.1. Hay un elemento 'más largo' del grupo Cubo de Rubik, medido en la métrica de un cuarto de vuelta.

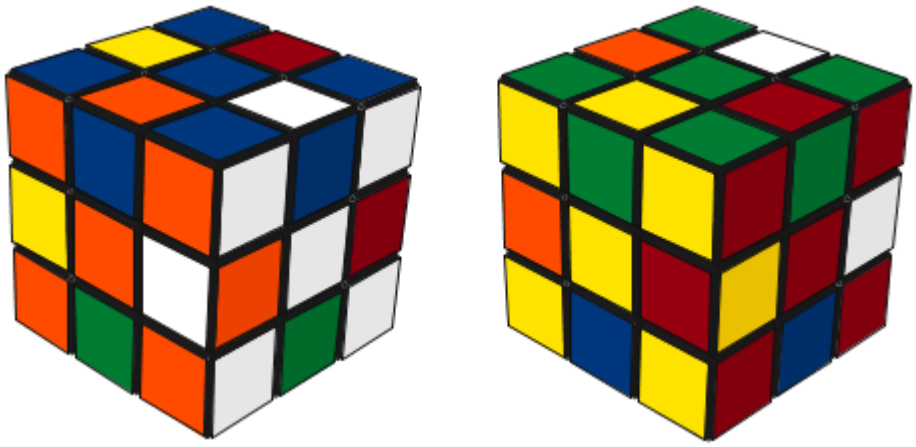


Figura 3.5: *Superflip con cuatro-puntos de Michael Reid.*

El **superflip con cuatro puntos**, es mostrado en la Figura 3.5, es dado por 26 cuartos de vuelta

$$\text{superflip} = U^2 \cdot D^2 \cdot L \cdot F^2 \cdot U^{-1} \cdot D \cdot R^2 \cdot B \cdot U^{-1} \cdot D^{-1} \cdot R \cdot L \cdot F^2 \cdot \\ \cdot R \cdot U \cdot D^{-1} \cdot R^{-1} \cdot L \cdot U \cdot F^{-1} \cdot B^{-1}. \tag{3.2}$$

Esto fue comprobado por Mike Reid (que descubrió el movimiento y la expresión anterior con la ayuda de su programa de ordenador) a ser mínimo en la métrica de un cuarto de vuelta (ver 02 de agosto 1998, la publicación en [CL]). Es posible que no haya un movimiento más largo que el superflip en el grupo Cubo de Rubik en la métrica de un cuarto de vuelta.

Observación 3.6.2. En el momento de escribir estas líneas (primavera 2013), no hay elemento más largo que el superflip del grupo Cubo de Rubik, medido en la métrica de vuelta de cara. Es posible que no haya movimiento más largo que el superflip en el grupo Cubo de Rubik en la métrica de vuelta de cara.

3.6.2 Ejemplo: El grupo dos cuadrados

Sea $H = \langle R^2, U^2 \rangle$, el grupo generado por los dos movimientos cuadrados R^2 y U^2 del Cubo de Rubik. (**Agarre mágico Singmaster:** el pulgar y el dedo índice de la mano derecha se colocan en la cara frontal y la cara posterior de la arista fr, br; y el pulgar y el dedo índice de la mano izquierda se colocan en la cara frontal y la cara posterior de la arista uf, ub. Todos los movimientos en este grupo se pueden hacer sin tener los dedos en el cubo.) Este grupo contiene la utilidad un par de movimientos intercambio de arista $(R^2 \cdot U^2)^3$.

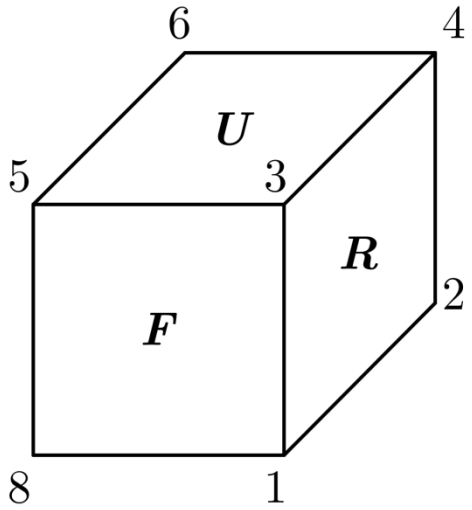


Figura 3.6: *Etiquetas de las esquinas para el cubo*

Podemos encontrar todos los elementos de este grupo con bastante facilidad:

$$H = \{1, R^2, R^2 \cdot U^2, R^2 \cdot U^2 \cdot R^2, (R^2 \cdot U^2)^2, (R^2 \cdot U^2)^2 \cdot R^2, (R^2 \cdot U^2)^3, (R^2 \cdot U^2)^3 \cdot \\ \cdot R^2, (R^2 \cdot U^2)^4, (R^2 \cdot U^2)^4 \cdot R^2, (R^2 \cdot U^2)^5, (R^2 \cdot U^2)^5 \cdot R^2\}$$

Por lo tanto, $|H| = 12$. Note que $1 = (R^2 \cdot U^2)^6$, $U^2 = (R^2 \cdot U^2)^5 \cdot R^2$, y $U^2 \cdot R^2 = (R^2 \cdot U^2)^5$
Para descubrir más acerca de este grupo, etiquetamos los vértices del cubo como en la Figura 3.6.
El movimiento R^2 actúa sobre el conjunto de vértices por la permutación $(1,4)(2,3)$ y el movimiento de U^2 actúa sobre el conjunto de vértices por la permutación $(4,5)(3,6)$. Etiquetamos los vértices de un hexágono regular como en la Figura 3.6.

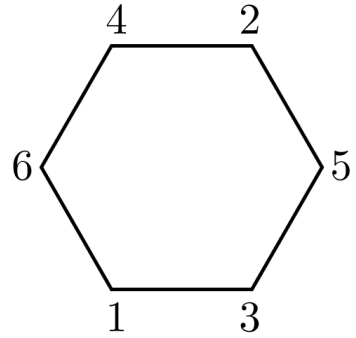


Figura 3.7: *Etiquetas de las esquinas para el hexágono*

La permutación $(1,4)(2,3)$ es simplemente la reflexión sobre el eje de simetría que contiene tanto 5 y 6. La permutación $(4,5)(3,6)$ es simplemente la reflexión sobre el eje de simetría que contiene tanto 1 y 2. Por un hecho establecido en la sección 3.3, estas dos reflexiones generan el grupo de simetría del hexágono.

3.7 Conmutadores

Cuando 'jugamos' con el Cubo de Rubik, ciertas operaciones pueden ocurrir con más frecuencia que otras. Además de la combinación de dos movimientos juntos, otra operación

que se lleva a cabo con frecuencia es la operación 'movimiento 1, luego movimiento 2, luego inverso del movimiento 1, luego inverso del movimiento 2'. Este tipo de movimiento es llamado un 'conmutador'.

Definición 3.7.1. Si g, h son dos elementos de un grupo G, entonces llamamos el elemento

$$[g, h] = g * h * g^{-1} * h^{-1}$$

el **conmutador** de g, h.

Note que $[g, h] = 1$ si y sólo si g, h conmutan. Así el conmutador puede considerarse como una medida aproximada de la falta de conmutatividad.

Problema 3.7.1. Sea $G = S_3$, el grupo simétrico de grado 3. Calcular los conmutadores

$$[s_1, s_2], \qquad [s_2, s_1].$$

Problema 3.7.2. Sea R, U como en la notación para los movimientos del Cubo de Rubik introducido en el primer capítulo. Determinar el orden del movimiento $[R, U]$.
$(Respuesta: 6)$

Definición 3.7.2. (Singmaster [Si]) Sea G el grupo de permutación generado por las permutaciones R, L, U, D, F, B, consideradas como permutaciones en S_{54}.

El **conmutador** $\boldsymbol{Y}$ es el elemento

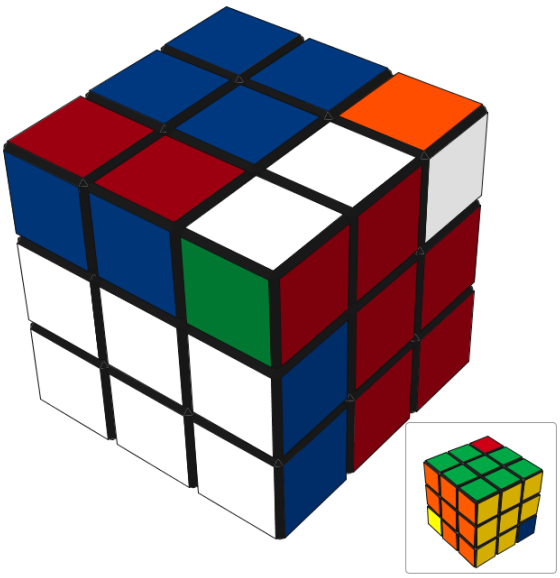


Figura 3.8 $\boldsymbol{[F, R^{-1}] = F \cdot R^{-1} \cdot F^{-1} \cdot R.}$

El **conmutador** $\boldsymbol{Z}$ es el elemento

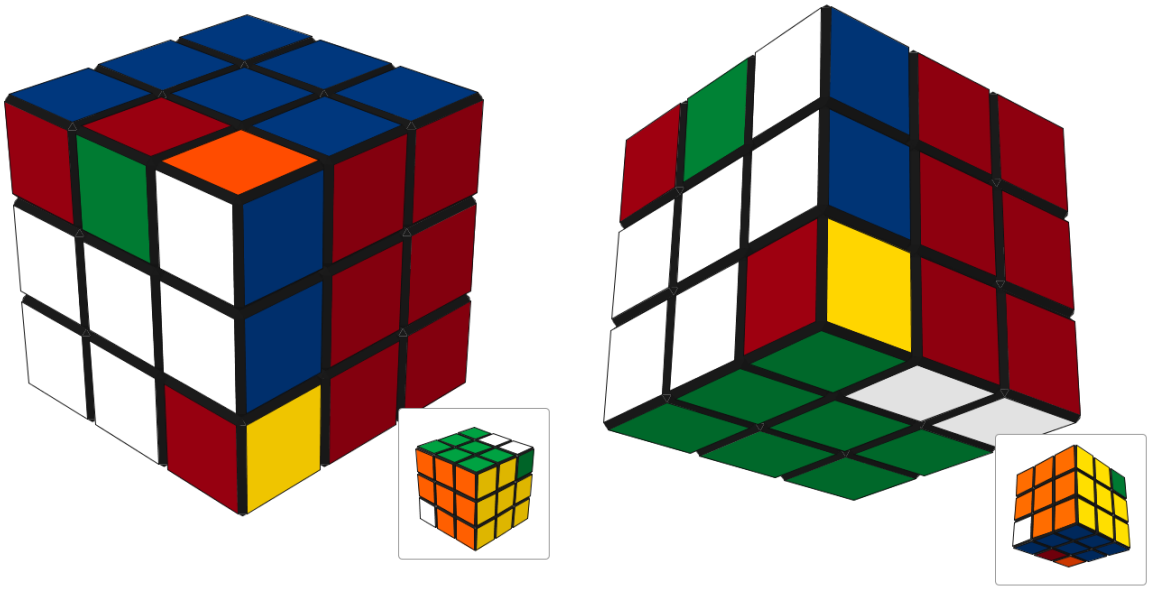


Figura 3.9 $[\boldsymbol{F}, \boldsymbol{R}] = \boldsymbol{F} \cdot \boldsymbol{R} \cdot \boldsymbol{F}^{-1} \cdot \boldsymbol{R}^{-1}$.

Ejemplo 3.7.1. Si x, y son movimientos básicos del Cubo de Rubik asociados con caras que comparten una arista, entonces

(a) $[x, y]^2$ permuta exactamente tres aristas y no permuta cualesquiera esquinas;

(b) $[x, y]^3$ permuta exactamente dos pares de esquinas y no permuta cualesquiera aristas.

Definición 3.7.3. Sea G cualquier grupo. El grupo G' generado por todos los conmutadores

$$\{[g, h] \mid g, h \text{ pertenecientes a } G\}.$$

Es llamado el **subgrupo conmutador** de G. A veces esto también se denota $[G, G]$.

Este grupo puede ser considerado como una medida aproximada de la falta de conmutatividad del grupo G.

Observación 3.7.1. Veremos más adelante que el grupo generado por los movimientos básicos del Cubo de Rubik-R, L, U, D, F, B-tiene un subgrupo conmutador relativamente grande. En otras palabras, hablando aproximadamente la mayoría de movimientos del Cubo de Rubik pueden ser generados por los conmutadores tales como el conmutador Y o el conmutador Z.

Definición 3.7.4. Si tomamos repetidamente subgrupos conmutadores, obtenemos una serie de grupos $G, G', G'' = (G')'$, y así sucesivamente. La **serie derivada** de un grupo G es la secuencia de los subgrupos

$$\ldots \subset (G')' \subset G' \subset G.$$

Un grupo G es llamado **soluble** si uno de los grupos en la serie derivada es el grupo trivial que consiste solamente de la identidad.

La idea de un grupo soluble surgió por primera vez y su importancia se destaca en el trabajo de Galois. Sin embargo, fue Camille Jordan (1838-1922) quien introdujo el concepto de una serie de composición (de la que serie derivada es un caso especial). Jordan también es conocido por la "forma normal de Jordan" en el álgebra lineal. Se argumenta en el artículo de Jordan [MT] que la teoría de grupos finitos comenzó con Jordan, su texto *Traités des substitutions et des équations algebraique* en 1870 siendo el primer libro sobre la teoría de grupos.

Problema 3.7.3. Sea G un grupo abeliano. Demostrar que G es soluble.

3.8 Conjugación

Además de la composición dos movimientos juntos y utilizar el conmutador, otra operación que se produce con frecuencia en el Cubo de Rubik es 'el movimiento 1, luego el movimiento 2, luego el inverso del movimiento 1'. Este tipo de movimiento es llamado una 'conjugación'.

Definición 3.8.1. Si g, h son dos elementos de un grupo G, entonces llamamos al elemento

$$g^h = h^{-1} * g * h$$

el **conjugado** de g por h.

Note que $g^h = h$ si y sólo si g, h conmutan. Así, los conjugados pueden ser considerados como una medida aproximada de la falta de conmutatividad. La notación exponencial se justifica por los siguientes hechos, que son fáciles de verificar.

Problema 3.8.1. Demuestre que

(a) $(g_1 g_2)^h = g_1^h g_2^h$,

(b) $g^{h_1 h_2} = \left(g^{h_1}\right)^{h_2}$.

Problema 3.8.2. Sea $G = S_3$, el grupo simétrico de grado 3, en la notación del Ejemplo 3.4.1 Calcular las conjugaciones

$$s_1^{s_2},\ s_2^{s_1}.$$

Problema 3.8.3. Sean R, U como en la notación para los movimientos del Cubo de Rubik introducido en el primer capítulo. Determinar el orden del movimiento R^U. ($Respuesta$: 4)

Definición 3.8.2. Decimos que dos elementos g_1, g_2 de G son conjugados si existe un elemento $h \in G$ tal que $g_2 = g_1^h$.

Es fácil ver cuando dos permutaciones $g, h \in S_n$ son conjugados: son conjugados si y sólo si los ciclos en su respectiva descomposición cíclica disjunta tiene la misma longitud cuando se ordenan del más corto al más largo. (Este resultado se debe a Cauchy.) Por ejemplo, los elementos

$$g = (6,9)(1,3,4)(2,5,7,8), \qquad h = (1,2)(3,4,5)(6,7,8,9)$$

son conjugados en S_9. Dejaremos los detalles y la prueba para más adelante (ver 6.3.1).

Problema 3.8.4. Mostrar que la noción de conjugado define una relación de equivalencia. Es decir, mostrar que

(a) cualquier elemento $g \in G$ es conjugado a sí mismo **(reflexiva)**;

(b) si g es conjugado a h (g, h pertenecientes a G), entonces h es conjugado a G **(simetría)**;

(c) si g_1 es conjugado a g_2 y g_2 es conjugado a g_3 entonces g_1 es conjugado a g_3 **(transitividad)**.

Notación: El conjunto de clases de equivalencia de G bajo la relación de equivalencia dada por la conjugación será denotada por G_*.

Problema 3.8.5. Sea G un grupo finito. Demuestre que

(a) $|G_*| \leq |G|$, y

(b) $|G| = |G_*|$ si y sólo si G es abeliano.

El polinomio

$$p_G(t) = \sum_{c \in G_*} t^{ord(c)}, \tag{3.3}$$

es llamado el **polinomio generador** de la función orden sobre G.

Problema 3.8.6. Mostrar que dos elementos que son conjugados deben tener el mismo orden. *(Sugerencia:* $(h^{-1}g\,h)^n = (h^{-1}g\,h)(h^{-1}g\,h)\ldots(h^{-1}g\,h) = h^{-1}g^n h,\ para\ n = 1, 2, \ldots y$ $g, h \in G$.*)*

Por lo tanto, la expresión $ord : G \to \mathbb{N}$ puede ser definida en G_*. Sea

$$ord(\{h^{-1}g\,h \mid h \in G\}) = ord(g).$$

Note que si $g_1, g_2 \in G$ son ambos de orden d, entonces $t^{ord(g_1)} = t^{ord(g_2)} = t^d$. Esto nos dice que

$$p_G(t) = \sum_{d \geq 1} n_G(d) t^{\boldsymbol{d}},$$

Donde $n_G(d)$ denota el número de elementos en G_* de orden d. En otras palabras, este polinomio codifica, a través de sus coeficientes, información sobre los elementos de un orden dado en G. Sin embargo, como lo resume en clases de conjugación (no en los elementos de G a sí mismos), no hace distinción entre los dos elementos de G si son conjugados.

Ejemplo 3.8.1. Para D_6 (el grupo diedro de orden 12), el polinomio generador es

$$2t^6 + 2t^3 + 7t^2 + t;$$

para S_8, el polinomio generador es

$$t + 4t^2 + 2t^3 + 4t^4 + t^5 + 5t^6 + t^7 + t^8 + t^{10} + t^{12} + t^{15};$$

y para S_{12}, es

$$t + 6t^2 + 4t^3 + 9t^4 + 2t^5 + 16t^6 + t^7 + 4t^8 + 2t^9 + 6t^{10} + t^{11} + 9t^{12} + 2t^{14} + 2t^{15} + t^{18} + 2t^{20} + t^{21} + t^{24} + t^{28} + 3t^{30} + t^{35} + t^{42} + t^{60}.$$

Como ya se mencionó, el orden máximo (de cualquier elemento) del grupo Cubo de Rubik es 1260. Esto y la ecuación (3.3) nos dice que el grado del polinomio generador del grupo de Cubo de Rubik es de 1260.

Definición 3.8.3. Fijar un elemento g en un grupo G. El conjunto

$$Cl(g) = Cl_G(g) = \{h^{-1} * g * h \mid h \in G\}$$

es llamado la **clase de conjugación de** $g \in G$. Es la clase de equivalencia del elemento g bajo la relación dada por la conjugación.

Problema 3.8.7. Encontrar los elementos en $S_4 = \langle (1,2), (2,3), (3,4) \rangle$ que *son conjugados* de $(1,2,3,4)$.

Teorema 3.8.1. Cualquier grupo finito puede ser particionado en sus diferentes clases de conjugación,

$$G = \bigcup_{c \in G_*} Cl(c).$$

Si H es un subgrupo de G y si g es un elemento fijo de G, entonces el conjunto

$$H^g = \{g^{-1} * h * g \mid h \in H\}$$

es un subgrupo de G. Tal subgrupo de G es llamado un subgrupo conjugado a H.

Problema 3.8.8. Sea S el conjunto de todos los subgrupos de G. Definimos una relación R sobre S por

$$R = \{(H_1, H_2) \in S \times S \mid H_1 \text{ es conjugado a } H_2\}.$$

Demuestre que R es una relación de equivalencia.

3.9 Órbitas y acciones

Las órbitas son muy importantes para nuestros propósitos. Sin ellas, la comprensión de las matemáticas del Cubo de Rubik es como tratar de arreglar un carro sin tener una llave. El concepto de órbita es una herramienta esencial en nuestra caja de herramientas, ya que nos ayuda tanto a nivel conceptual y computacional. Richard Feynmann (1918-1988), el famoso físico, al parecer dijo algo como lo siguiente: "*Mi trabajo aquí no es hacerte comprender tal y tal cosa, sino de convencerte de no darte por vencido. Porque nadie, ni siquiera yo, realmente comprendo todo lo relacionado con este tema. Al menos, es interesante y merecedor de nuestro tiempo".*

Vamos a comenzar nuestro estudio de órbitas con un ejemplo. Sea G el grupo Cubo de Rubik y X el conjunto de las caritas de Cubo de Rubik. Imaginemos que tenemos dos cubos idénticos, desarmamos uno y colocamos las caritas sobre una mesa. Imaginemos también que cuando movemos el cubo ensamblado, las caritas sobre la mesa permutan ellas mismas de acuerdo al movimiento, en consecuencia podemos ver entonces que cada elemento de G 'mueve' los elementos de X. La terminología matemática más comúnmente utilizada para describir este tipo de situaciones, es decir 'G actúa sobre X'. La definición general es la siguiente.

Figura 3.10

Figura 3.11

Definición 3.9.1. Sea X un conjunto y sea G un grupo. Llamamos X un G-**conjunto** y decimos que G **actúa sobre** X **a la derecha** siempre que cumpla las siguientes condiciones:

1. Cada g perteneciente a G da lugar a una función

$$\phi_g : X \to X.$$

2. La identidad 1 del grupo G define la función identidad en X.
3. Si g, h pertenecen a G entonces la composición

$$\phi_{gh} : X \to X$$

satisface $\phi_{gh}(x) = \phi_h\left(\phi_g(x)\right)$.

Llamamos a esto una **acción derecha**.
Uno puede, en general, definir para todo $g \in G$, ϕ_g el mapeo identidad de X a sí mismo. Puesto que esta acción no hace nada, es llamada la **acción trivial**.
Aquí estamos interesados sólo en las acciones no triviales.
Definimos '**las acciones izquierda**' de manera similar.
Definición 3.9.2. Sea X un conjunto y sea G un grupo. Decimos que G **actúa sobre** X siempre que cumpla las siguientes condiciones:

1. Cada g perteneciente a G da lugar a una función

$$\phi_g : X \to X.$$

2. La identidad 1 del grupo G define la función identidad en X.

3. Si g, h pertenecen a G entonces la composición

$$\phi_{gh} : X \to X$$

satisface $\phi_{gh}(x) = \phi_g(\phi_h(x))$.

Nosotros llamamos a esta acción una **acción izquierda**.

Observación 3.9.1.

(a) Vamos a ver otra interpretación de estas definiciones más adelante en 6.2.
(b) Dada una acción izquierda ϕ_g, se puede crear una acción derecha por la definición $\phi'_g = \phi_{g^{-1}}$.

Después de la convención estándar, el Cubo de Rubik actuará sobre el conjunto de caritas del cubo *a la derecha*. Por ejemplo, comenzamos con un movimiento básico, digamos U, que mueve la cara superior en sentido horario un cuarto de vuelta. Hagamos otro movimiento básico, por ejemplo F. Los dos movimientos juntos se denotan $U * F$, donde F se escribe *a la derecha* de U.

Definición 3.9.3. Sea G actúa sobre un conjunto X. Llamamos la acción **transitiva** si para cada par x, y pertenecientes a X existe un $g \in G$ tal que $y = \phi_g(x)$.

En otras palabras, un grupo G actúa transitivamente sobre un conjunto X si *cualquier* elemento x de X puede ser enviado a *cualquier* otro elemento y de X por algún elemento g de G (dependiendo de x, y).
Esta noción de acción transitiva no debe confundirse con la noción de transitividad de las relaciones de equivalencia, a pesar de que muchas órbitas son clases de equivalencia.
La transitividad de una acción resulta ser una condición fuerte para un grupo G que actúa sobre un conjunto X. Esto ilustra cómo el inusual Cubo de Rubik es, ya que actúa transitivamente en dos conjuntos diferentes. Por ejemplo, sí permuta transitivamente el conjunto de subcubos esquina y permuta transitivamente el conjunto de subcubos arista.
Aquí hay varios ejemplos más.

Ejemplo 3.9.1. Sea X un conjunto finito y sea $G = S_X$ el grupo simétrico de X. Entonces X es un G-conjunto y G actúa transitivamente sobre X.

Ejemplo 3.9.2. Sea G el grupo de todas las matrices 2×2 invertibles con entradas reales, $G = GL_2(\mathbb{R})$. Este grupo actúa sobre el conjunto de vectores columna a la izquierda.

Definición 3.9.4. Sea G un grupo que actúa sobre un conjunto X. Para cada x perteneciente a X, el conjunto

$$G * x = \{\phi_g(x) \mid g \in G\}$$

es llamado la **órbita** de $x \in X$ bajo G.

Ejemplo 3.9.3. Sea X el conjunto formado por las 48 caritas del Cubo de Rubik que no son caritas centrales, es decir, las caritas movibles. Sea V el subconjunto de las caritas que pertenecen a algún subcubo esquina, y E el subconjunto de las caritas que pertenecen a algún

subcubo arista. Sea G el grupo Cubo de Rubik. Como se ha indicado anteriormente, G actúa sobre X, V, E. La acción de G sobre X induce una relación de equivalencia de la siguiente manera: decimos que una carita f_1 es 'equivalente' a una carita f_2 si hay un elemento de G (es decir, un movimiento del Cubo de Rubik) que envía una carita a la otra. Hay exactamente dos clases de equivalencia, o órbitas, de G en X: V y E. En particular, la acción de G sobre V es transitiva y la acción de G sobre E es transitiva.

Sea G el grupo Cubo de Rubik, V el conjunto de vértices, y sea $ruf \in V$ el vértice frontal superior derecho. El movimiento de la cara izquierda L claramente no afecta ruf. En este caso, decimos que L 'estabiliza' o 'fija' ruf. La definición general es dada a continuación.

Definición 3.9.5. Sea G un grupo que actúa sobre un conjunto X con la acción denotada por ϕ. Para cada x perteneciente a X, el subgrupo

$$stab_G(x) = G_x\{g \in G \mid \phi_g(x) = x\}$$

es llamado el **estabilizador** de x en G.

Ejemplo 3.9.4. Sea G el grupo de simetrías del cuadrado (ver el ejemplo, en 3.3 anterior), sea X el conjunto de vértices del cuadrado, y sea x_0 el vértice en la esquina inferior derecha. Entonces $stab_G(x_0) = \langle g_3 \rangle$.

Lema 3.9.1. Sea G cualquier grupo y sea $X = G$. Sea G actúa sobre X por conjugación:

$$\phi_g : X \to X$$
$$x \mapsto \phi_g(x) = g * x * g^{-1}.$$

El estabilizador satisface

$$stab_G(x) = \{g \in G \mid g * x = x * g\}$$

para todo x perteneciente a $X = G$.

El subgrupo "estabilizador" para la acción de conjugación,

$$C_G(x) = \{g \in G \mid g * x = x * g\}$$

es llamado el **centralizador** de x en G.

3.10 Clases laterales

Clases laterales son ciertos tipos de subconjuntos de un grupo G. Como G puede ser no conmutativo hay clases laterales izquierdas y clases laterales derechas. En este trabajo por lo general se utilizan clases laterales izquierdas.

Ejemplo 3.10.1. Sea G el grupo Cubo de Rubik y $H = \{1, D, D^2, D^3\}$ el subgrupo de movimientos de la cara inferior. Sea $g \in G$ un movimiento. El conjunto $gH = \{g, gD, gD^2, gD^3\}$ es llamado 'clase lateral izquierda de H'. El conjunto $Hg =$

$\{g, Dg, D^2g, D^3g\}$ es llamado 'clase lateral derecha de H'. Cada movimiento en Hg tiene el mismo efecto como g, excepto es posible que hayamos movido la cara inferior después.

Ejemplo 3.10.2. Sea $H = S_2 = \{1, (1,2)\}$ y

$$G = S_3 = \{1, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}.$$

Las clases laterales izquierdas de H en G son

$$H, \quad (1,2)H = H, \quad (2,3)H = \{(2,3), (1,2,3)\},$$
$$(1,3)H = \{(1,3), (1,3,2)\}, \quad (1,2,3)H = \{(1,2,3), (2,3)\} = (2,3)H,$$
$$(1,3,2)H = \{(1,3,2), (1,3)\} = (1,3)H.$$

Nótese que $G = H \cup (2,3)H \cup (1,3)H$.

Problema 3.10.1. Sea H un subgrupo de G y sean $g, g' \in G$. Demostrar que $gH = g'H$ o $gH \cap g'H = \emptyset$.

Entender clases laterales, como órbitas, no sólo ayuda en el conteo de los argumentos, también nos ayuda a entender la 'estructura de grupo' de G (es decir, saber cómo es construido G a partir de ciertos 'subgrupos bien entendidos'). Note que si $g \in H$ entonces, $gH = Hg = H$. Recíprocamente, si $gH = Hg = H$ entonces $g \in H$.

Definición 3.10.1. Sea G un grupo, escrito multiplicativamente, y H un subgrupo de G. Para g perteneciente a G, el subconjunto $g * H$ de G es llamado **clase lateral izquierda** de H en G y el subconjunto $H * g$ de G es llamado **clase lateral derecha** de H en G.

Si G es un grupo abeliano, escrito aditivamente, y H es un subgrupo, entonces las clases laterales izquierdas y las clases laterales derechas son las mismas: $H_{+g} = {}_{g+}H$.

Si G es abeliano o no, a veces abusamos de la terminología y omitimos las palabras 'izquierda' o 'derecha' frente a clase lateral.
Si G no es abeliano entonces el conjunto de clases laterales izquierdas por lo general difiere del conjunto de clases laterales derechas. Sin embargo, cuando G es finito, siempre hay el mismo número de clases laterales izquierdas como clases laterales derechas.

Fue Galois, a principios de la década de 1830, quien primero observo subgrupos para los cuales el conjunto de clases laterales izquierdas era el mismo que el conjunto de clases laterales derechas. (Estos subgrupos son ahora llamados 'normales' y se estudiaran más adelante.) El trabajo de Galois se aplicó al estudio de las raíces de los polinomios.

Ejemplo 3.10.3. Sea $G = \mathbb{Z}, H = 12\mathbb{Z}$, bajo la suma ordinaria. Si $n \in G$ es cualquier entero entonces $n + H$ es una clase lateral de H en G. De hecho, todas las clases laterales de H pueden ser tabuladas.

Cada clase lateral ocurre como una columna exactamente una vez en la siguiente tabla:

⋮	⋮			⋮
-12	-11	…	-2	-1
0	1	…	10	11
12	13	…	22	23
⋮	⋮			⋮

Tabla 3.3

Notación: El conjunto de todas las clases laterales izquierdas se denotan G/H y el conjunto de todos las clases laterales derechas de H en G se denotan $H\backslash G$.
Estos dos conjuntos en general no heredan una estructura de grupo de G, pero son útiles (G/H es un grupo con la 'evidente' multiplicación $(g_1 * H) * (g_2 * H) = (g_1 g_2) * H$ si y sólo si H es un subgrupo 'normal' de G. Se definirá 'normal' a continuación.)
Como un ejemplo de su utilidad, tenemos la siguiente relación entre órbitas y clases laterales de los estabilizadores.

Proposición 3.10.1. Sea G un grupo finito que actúa sobre un conjunto X. Entonces

$$|G * x| = |G/stab_G(x)$$

para todo x perteneciente a X.

Prueba: El mapeo

$$g * stab_G(x) \mapsto g * x$$

define una función $f : G/stab_G(x) \to G * x$. Esta función es una biyección, ya que es tanto inyectiva y sobreyectiva.

Corolario 3.10.1. Sea G un grupo finito que actúa sobre sí mismo por conjugación. Sea $S \subset G$ un conjunto completo de representantes de la clase de conjugación G_* en G y sea $S' = S - Z(G)$, es decir, el subconjunto de S de aquellos elementos que no están en el centro. Entonces

$$G = \bigcup_{x \in S} Cl(x) \cong \bigcup_{x \in S} G/stab_G(x) = Z(G) \cup \bigcup_{x \in S'} G/stab_G(x)\,,$$

para todo x perteneciente a X. En particular,

$$|G| = \sum_{x \in S} |G/stab_G(x)| = |Z(G)| + \sum_{x \in S'} |G/stab_G(x)|.$$

A veces esto es llamado la **ecuación de clase** o la **fórmula de clase** para grupos.

Demostración: La primera igualdad, $G = \cup_{x \in S} Cl(x)$, es el Teorema 3.8.1. La segunda igualdad se sigue del isomorfismo $G/stab_G(x) \cong G * x$, establecida en la prueba de la proposición anterior.
Al tomar cardinalidades, la segunda ecuación que se muestra es una consecuencia de la primera.

Corolario 3.10.2.

Teorema de Cauchy (3.4.1)

(a) Sea p un número primo que divide al $|G|$, entonces G contiene un elemento g de orden p.

El argumento es por inducción sobre $|G|$.
El resultado es trivial si $|G| = 1$ (dado que entonces ningún primo divide $|G|$). Y *el teorema se cumple por vacuidad* (ver Herstein)
Supongamos que $|G| > 1$ y sea p un número primo que divide $|G|$. Por la hipótesis de inducción asumimos que el resultado es cierto para todos los subgrupos H de G con $|H| < |G|$.
Supongamos que $x \in G$ no está en el centro de G. Entonces su centralizador $C_G(x)$ es un subgrupo propio de G. Si $p| \, |C_G(x)|$ entonces el resultado se sigue de la hipótesis de inducción.
Si p no divide a $|C_G(x)|$ (para todo x no está en el centro), puesto que $|G| = |C_G(x)||G/stab_G(x)|$ (note que el estabilizador y centralizador son los mismos en este caso), se sigue que p divide a $|G/stab_G(x)|$. Por el Corolario 3.10.1 anterior, debemos tener $p\big||Z(G)|$. Si $Z(G)$ es un subgrupo propio de G, entonces se aplica la hipótesis de inducción.
Por lo tanto podemos asumir que $G = Z(G)$, G es abeliano. Si G es cíclico G contiene un elemento de orden p. Vamos a suponer que G no es cíclico. Sea H un subgrupo propio de G de orden máximo (esto existe puesto que G no es cíclico) y sea $a \in G - H$. Entonces $G = H \cdot \langle a \rangle$ (H demás no lo haría ser máxima). Esto implica que p divide ya sea a H o $|\langle a \rangle|$. El resultado se sigue de la hipótesis de inducción. Para más detalles, consultar cualquier texto sobre la teoría de grupos (Herstein).

Problema 3.10.2. Sea G el grupo de simetrías del cuadrado. Usando la notación del Ejemplo 3.3.1, calcular $G/\langle g_3 \rangle$ y $G * x_0$.

Esta es otra versión del Teorema 3.5.1.
Teorema 3.10.1. (Teorema de Lagrange) Si G es un grupo finito y H un subgrupo entonces

$$|G/H| = |G|/|H|.$$

Joseph Louis Lagrange (1736-1813) fue un italiano que estudió en la Universidad de Turín y más tarde profesor de matemáticas allí. Más tarde enseñó en la Universidad de Berlín y luego tomó una posición de investigación en la Academia de Ciencias de París, aunque él enseñó en la Escuela Politécnica. Hizo importantes contribuciones a la mecánica, aplicaciones de cálculo, y la teoría de funciones. Muchos historiadores de las matemáticas creen que la teoría de grupos finitos comenzó con Camille Jordan, que nació 25 años después de que Lagrange murió. Así que es justo decir que la versión original del 'teorema de Lagrange' no estaba en la forma que vemos más arriba.
Como consecuencia inmediata de la segunda versión del teorema de Lagrange anterior, obtenemos la primera versión (Teorema 3.5.1).
Demostración del teorema: Sea X el conjunto de clases laterales izquierdas de H en G y sea G actúa sobre X por multiplicación izquierda. Aplicar el lema anterior con $x = H$.

Definición 3.10.2. Sea H un subgrupo de G y sea C una clase lateral izquierda de H en G.
Llamamos un elemento g de G un **representante de clase lateral** de C si $C = g * H$. Un **conjunto completo de representantes de las clases laterales** es un subconjunto de $G, x_1, x_2, \dots, x_m$, tal que

$$G/H = \{x_1 * H, \dots, x_m * H\}$$

sin repetición (es decir, todos los $x_i * H$ son disjuntos).

Problema 3.10.3. Para $G = S_4$ y $H = S_3$, encontrar un conjunto completo de representantes clases laterales de G/H en G.

Teorema 3.10.2. Si S es un conjunto completo de representantes de clase lateral de G/H, entonces

$$G = \bigcup_{s \in S} s * H$$

y $|G| = \sum_{s \in S} |s * H|$.

Esto se sigue de la definición anterior, cuando G es finito.

3.11 Campanología, revisión

Volvemos al volteo de campanas visto en 1.5, ahora en el contexto de la teoría de grupos.
La generación del plan (Bob minimus) para cuatro campanas es análogo algebraicamente a la generación del grupo diedro de orden 8, D_4. Si $a = (1,2)(3,4)$, que intercambia las dos primeras y las dos últimas campanas, y si $b = (2,3)$, que intercambia el par medio, entonces el plan producido sobre cuatro campanas corresponde a

$$D_4 = \{1, a, ab, aba, (ab)^2, (ab)^2 a, (ab)^3, (ab)^3 a\}.$$

Plan Bob Minimus es equivalente algebraicamente a la generación del grupo simétrico de 4 elementos, S_4 . Sean a y b como antes. Si nos fijamos en la primera columna del Plan Bob Minimus, vemos que no es nada más que el grupo diedro D_4 , que es un subgrupo de S_4. Para generar la segunda columna de S_4 introducimos $c = (3,4)$ y sea $k = (ab)^3 ac$. La segunda columna corresponde a kD_4 y la tercera columna a $k^2 D_4$. La generación del Plan Bob Minimus muestra que S_4 se puede expresar como la unión disjunta de clases laterales del subgrupo D_4, es decir, las clases laterales de D_4 en S_4 particionan S_4. Esto da una ejemplo del hecho de que, para cualquier grupo G y cualquier subgrupo H, las clases laterales de H en G particionan G (véase también el Teorema 3.10.2).
Fabián Stedman no estaba usando la teoría de grupos de manera explícita, sino más bien que las ideas teóricas del grupo estaban implícitas en los escritos y composiciones de Stedman.

3.12 Algoritmo de Dimino

Vimos en un capítulo anterior un algoritmo simple para el cálculo de los elementos de un grupo de permutación G. Como el tiempo es dinero y tiempo en la computadora es limitado, eficiencia de los sistemas es un tema importante. Vamos a hablar de un algoritmo mucho más eficiente en esta sección.
Recordamos el algoritmo de Dimino de Butler [Bu], pero primero alguna notación.

Notación: Sea $S = \{g_1, g_2, \dots, g_n\}$ un conjunto de generadores de un grupo de permutación G. Sea

$$S_0 = \emptyset,$$
$$S_i = \{g_1, \dots, g_i\},$$

$$G_0 = \{1\},$$

$$G_i = \langle S_i \rangle = \text{el grupo generado por los elementos en } S_i, \text{ para } 1 \leq i \leq n.$$

Ejemplo 3.12.1. Sea $G = S_3 = \langle s_1, s_2 \rangle$. Usamos el algoritmo de Dimino para listar todos los elementos de G. Tenemos

$$G_0 = \{1\} \subset G_1 = \langle s_1 \rangle \subset G_2 = G.$$

Primero, listamos los elementos de $G_1 = \langle s_1 \rangle$. Puesto que $s_1 = (1, 2)$, es de orden 2, de modo que $G_1 = \{1, s_1\}$.

Esta es nuestra lista L a la que vamos a aplicar el 'paso inductivo' del algoritmo de Dimino (con $i = 2$). Comenzamos con $C = \{1\}$. Ahora nos fijamos en las clases laterales izquierdas de G_1 en $G_2 = G$. Tenemos (con $g = 1,\ s = s_1$)

$$s_1 * G_1 = G_1,$$

por lo que no aumenta el tamaño de C o L. Luego, tenemos (con $g = 1,\ s = s_2$)

$$s_2 * G_1 = \{s_2, s_2 * s_1\} \neq G_1,$$

asi $= \{1, s_1,\ s_2,\ s_2 * s_1\}$, $C = \{1, s_2\}$. A continuación, tenemos (con $g = s_2,\ s = s_1$)

$$s_1 * s_2 * G_1 = \{s_1 * s_2, s_1 * s_2 * s_1\} \neq G_1.$$

(Sabemos $s_1 * s_2 * G_1 \neq G_1$ ya que ninguno de los dos elementos en $s_1 * s_2 * G_1$ es la identidad.) Por lo tanto, aumentar L, C:

$$L = \{1, s_1,\ s_2,\ s_2 * s_1, s_1 * s_2, s_1 * s_2 * s_1\},$$

y $C = \{1, s_2,\ s_1 * s_2\}$. Sabemos que podemos parar aquí ya que sabemos que $|S_3| = 6$ pero el algoritmo aún tiene una afirmación más. A continuación, tenemos (con $g = s_2,\ s = s_2$)

$$s_2 * s_2 * G_1 = G_1,$$

por lo que no aumenta el tamaño de C o L (como se esperaba). Este paso termina el algoritmo y $S_3 = L$.

Problema 3.12.1. Realizar algoritmo de Dimino en

$$S_4 = \langle s_1 = (1\ 2), s_2 = (2\ 3), s_3 = (3\ 4) \rangle.$$

Capítulo 4

Algoritmo de Dios y Grafos

> *Desafortunadamente, lo que es poco reconocido es que los libros científicos más valiosos son aquellos en los que el autor indica claramente lo que él no sabe, porque un autor lastima más a sus lectores al ocultar las dificultades*.
>
> *Evariste Galois*

En este capítulo introducimos una interpretación gráfica de un grupo de permutación, el grafo de Cayley. Esto es aplicado en el caso especial de un grupo que surge de un puzzle de permutación.

4.1 En el principio…

Para empezar, ¿qué es un grafo? Un **grafo** es un par de conjuntos (V, E), donde

- V es un conjunto de elementos llamados **vértices,**
- E es un subconjunto del conjunto de todos los pares *no ordenados* $\{\{v_1, v_2\} | \, v_1, v_2 \in V, v1 \neq v2\}$. Los elementos de E son llamados **aristas.**

En teoría de grafos, un **bucle** o **loop** es una arista que conecta un vértice consigo mismo. Un grafo (sin "loops") también es llamado **grafo simple**. Un grafo se dibuja simplemente conectando los puntos que representan los vértices unidos por un segmento de línea si pertenecen a la misma arista. Un **grafo finito** es un grafo (V, E), con V un conjunto finito.
Un **digrafo,** o **grafo dirigido,** es un par de conjuntos (V, E), donde

- V es un conjunto numerable de vértices,
- E es un subconjunto de pares *ordenados* $\{(v_1, v_2) | \, v_1, v_2 \in V, v_1 \neq v_2\}$ llamados **aristas**

Un digrafo se dibuja simplemente conectando los puntos que representan los vértices unidos por una flecha si pertenecen a la misma arista (v_1, v_2), la flecha se origina en v_1 y apunta a v_2.
Si $e = \{v_1, v_2\}$ pertenece a E, entonces decimos que e es una **arista** de v_1 a v_2 (o de v_2 a v_1) y decimos v_1 y v_2 son **vecinos** o **adyacentes** en el grafo. Si v y w son vértices, un **camino** de v a w es una secuencia finita de aristas empezando en v y terminando en w:

$$e_0 = \{v, v_1\}, e_1 = \{v_1, v_2\}, \dots, e_n = \{v_n, w\}.$$

Si hay un camino de v a w entonces decimos que v es **conectado** a w. Decimos que un grafo (V, E), es **conexo** si cada par de vértices están conectados. El número de aristas que emanan de un vértice v es llamado el **grado** (o **valencia**) de v, denotado $grado(v)$.

Ejemplo 4.1.1. Si

$$V = \{a, b, c\}, \qquad E = \big\{\{a, b\}, \{a, c\}, \{b, c\}\big\},$$

entonces podemos visualizar el grafo $\Gamma = (V, E)$, como en la Figura 4.1.

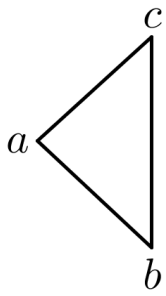


Figura 4.1: *Cada vértice tiene valencia 2.*

Definición 4.1.1. Si v y w son vértices conectados el uno al otro en un grafo (V, E), entonces definimos la **distancia de** v **a** w $d(v, w)$, por

$$d(v, w) = \min_{v,w \in V \ conectado} \#\{\text{aristas en un camino de v a w}\}$$

Por *convención*, si v y w no están conectados, entonces escribimos $d(v, w) = \infty$. El **diámetro** de un grafo es la mayor distancia posible:

$$diam\big((V, E)\big) = \max_{v,w \in V} d(v, w).$$

Que coincide con la definición de diámetro de un círculo.

4.2 Grafos de Cayley

Sea G un grupo finito con generadores prescritos g_i:

$$G = \langle g_1, g_2, \dots, g_n \rangle.$$

Supongamos que el conjunto generador $X = \{g_1, g_2, \dots, g_n\}$ no contiene la identidad y es cerrado bajo inversos (es decir, si $x \in X$, entonces $x^{-1} \in X$). El **grafo de Cayley** de G con respecto a $X = \{g_1, g_2, \dots, g_n\}$ es el grafo (V, E) cuyos vértices V son los elementos de G y cuyas aristas están determinadas por la siguiente condición: si x e y pertenecen a $V = G$, entonces hay una arista de x a y (o de y a x) si y sólo si $y = g_i \cdot x$ o $x = g_i \cdot y$, para algún $i = 1, 2, \dots, n$.
Grafos de Cayley en honor a Arthur Cayley. Cayley, aunque comenzó a trabajar como abogado, con el tiempo publicó más de 900 trabajos y notas que cubren casi todos los aspectos de las matemáticas.

Lema 4.2.1. Sea $\Gamma_G = (V, E)$ el grafo de Cayley asociado con el grupo finito $G = \langle g_1, g_2, \dots, g_n \rangle$. Sea $N = |\{g_1, g_1^{-1}, g_2, g_2^{-1}, \dots, g_n, g_n^{-1}\}|$. Entonces, para todo v $\in V$, $grado(v) = N$.

Prueba: Supongamos que no. Entonces hay un $v \in V = G$ con alguna de las siguientes opciones

(i) $grado(v) < N$, o

(ii) $grado(v) > N$.

Primero, notamos que, para cada $h \in \{g_1, g_1^{-1},\ g_2, g_2^{-1}, \dots, g_n, g_n^{-1}\}$, el conjunto $\{v, h \cdot v\}$ es una arista de Γ_G. Esto se sigue de la definición de grafo de Cayley.
Si $r = grado(v) > N$, entonces, por definición de grafo de Cayley, hay distintos $v_1, \dots, v_r \in V$ con $v = h_i \cdot v_i$, para todo $1 \leq i \leq r$, donde los $h_1, \dots, h_r$ son elementos distintos de $\{g_1, g_1^{-1},\ g_2, g_2^{-1}, \dots, g_n, g_n^{-1}\}$. Esto contradice la definición de N.
Si $r = grado(v) < N$ entonces, por definición de grafo Cayley, hay distintos h_i, h_j en $\{g_1, g_1^{-1},\ g_2, g_2^{-1}, \dots, g_n, g_n^{-1}\}$ tal que $h_i \cdot v = h_j \cdot v$. Puesto que G es un grupo y $V = G$ (como conjuntos), podemos cancela v en ambos lados de la ecuación $h_i \cdot v = h_j \cdot v$, contradiciendo la suposición de que h_i es distinta de h_j.

Ejemplo 4.2.1. Sea $G = \langle s_1, s_2 \rangle = S_3$,

donde $s_1 = (1,2)$, y $s_2 = (2,3)$. Entonces el grafo de Cayley de G con respecto a $X = \{s_1, s_2\}$ puede ser visualizado como se ve abajo (notar que $s_1 = s_1^{-1}$ y $s_2 = s_2^{-1}$, de este modo X es cerrado bajo inversos).

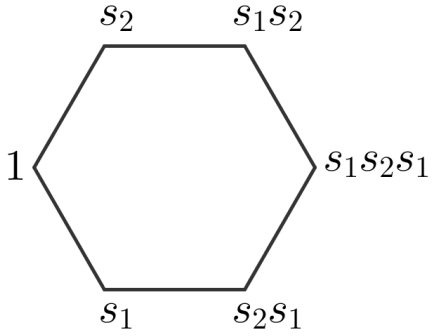


Figura 4.2

Ejemplo 4.2.2. Sea

$$G = \langle R, L, U, D, F, B \rangle \subset S_{54}$$

el grupo Cubo de Rubik 3 × 3. Cada posición del cubo corresponde a un elemento del grupo G (es decir, el movimiento que hemos tenido que hacer para obtener tal posición). En otras palabras, cada posición del cubo corresponde a un vértice de ya sea que

- el grafo de Cayley asociado con la **métrica de un cuarto de vuelta** generando el conjunto $\{R, L, U, D, F, B, R^{-1}, L^{-1}, U^{-1}, D^{-1}, F^{-1}, B^{-1}\}$, o bien
- el grafo de Cayley asociado con la **métrica de vuelta de cara** generando el conjunto $\{R, R^2, L, L^2, U, U^2, D, D^2 F,\ F^2\ B, B^2, R^{-1}, L^{-1}, U^{-1}, D^{-1}, F^{-1}, B^{-1}\}$.

Cada vértice del primer (métrica de un cuarto de vuelta) grafo tiene valencia 12, mientras que cada vértice del último (métrica de vuelta de cara) grafo tiene valencia 16.

Por otra parte, una solución del Cubo de Rubik es simplemente un camino en el grafo de Cayley desde el vértice asociado a la posición actual del cubo al vértice asociado con el elemento identidad. El número de movimientos en la solución más corta posible es simplemente la distancia desde el vértice asociado con la posición actual del cubo hasta el vértice asociado al elemento identidad. El diámetro del grafo de Cayley de G es el número de

movimientos en la mejor solución posible en el peor caso posible. Este diámetro se puede medir ya sea en métrica de un cuarto de vuelta o la métrica de vuelta de cara**.**

4.3 Algoritmo de Dios

(El siguiente resultado no se ha probado) Sea G el grupo de un puzzle de permutación (con un conjunto generado fijo). Encontrar el diámetro del grafo de Cayley de G.

A veces esto es llamado 'Algoritmo de Dios', aunque en este caso ese término está reservado para una versión más difícil del problema, se indica a continuación. El problema del diámetro no está resuelto para la mayoría de los puzzles (incluso el Cubo de Rubik 3×3) y parece ser muy difícil computacionalmente en general. Los casos en que se sabe incluyen (sin ningún intento de exhaustividad) los puzzles siguientes:

Puzzle	Diámetro
Pyraminx	11 (no incluye movimientos punta)
Cubo de Rubik $2\times 2 \times 2$	14 (giros de un cuarto)

Tabla 4.1

Los diámetros fueron encontrados con la ayuda de una computadora.

Muchas personas han trabajado sobre el Algoritmo de Dios para el Cubo de Rubik. Durante un tiempo se conjeturo que la posición superflip es la posición que está tan lejos del 'inicio' (la posición resuelta) como sea posible. La posición superflip es de 24 cuartos de vuelta desde el inicio en la métrica de un cuarto de vuelta (como ya se mencionó, este hecho se debe a Jerry Bryan y Michael Reid [CL]) y 20 vueltas desde el inicio en la métrica de vuelta de cara (esto se debe a Michael Reid y Dik Winter). Sin embargo, Reid descubrió un movimiento más largo en la métrica de un cuarto de vuelta-26 cuartos de vuelta lejos del inicio (el superflip compuesto con los cuatro puntos, ver (3.2)). Ningún movimiento más largo se ha encontrado en la métrica de vuelta de cara. Por el momento, uno podría suponer que el diámetro del grafo Cubo de Rubik es 26 en la métrica de un cuarto de vuelta y 20 movimientos en la métrica de vuelta de cara. Al momento de escribir esto (primavera 2008), la mejor cota superior conocida es la siguiente:

- Tom Rokicki demostró en 2008 que 25 giros de cara son suficientes [Rok]. (Gene Cooperman y Daniel Kunkle probaron en 2007 que 26 giros de cara son suficientes, pero creen que su técnica puede ser llevada a la marca de 25 también.)

- En 2006, Silviu Radu demostró que cada posición puede ser resuelta en un máximo de 35 cuartos de vuelta.

Problema 4.3.1. Sea G el grupo de un puzzle de permutación (con un grupo generado fijo) y sea v un vértice en el grafo de Cayley de G. Encontrar un algoritmo práctico y eficaz para la determinación de un camino de v al vértice v_0 asociado a la identidad que tiene una longitud igual a la distancia de v a v_0.

¡Este problema es aún más difícil! Este algoritmo se llama **Algoritmo de Dios.** En realidad se refiere a un método óptimo de solución para el puzzle de permutación.

Problema 4.3.2. Encuentra el grafo de Cayley del grupo cuadrado **sliced** (rebanada intermedia)

$$G = \langle M_R^2, M_F^2, M_D^2 \rangle,$$

donde M_R denota el movimiento un cuarto de vuelta en sentido horario del corte medio paralelo al lado derecho. Encontrar el diámetro de este grafo.

Sea Γ un grafo. Un **circuito Hamiltoniano** sobre Γ es una secuencia de aristas que forman un camino en Γ que pasa a través de cada vértice exactamente una vez. (Si pensamos en los vértices como ciudades y las aristas como carreteras, entonces, un circuito Hamiltoniano es un recorrido visitando cada ciudad exactamente una vez.)
El siguiente problema no resuelto fue mencionado por primera vez en este contexto por A. Schwenk (en un documento inédito escrito mientras estaba en la Academia Naval de los Estados Unidos.)

Problema 4.3.3. (Muy difícil) Sea G el grupo del puzzle Cubo de Rubik 3×3. ¿Tiene el grafo de Cayley de G un circuito Hamiltoniano? En otras palabras, ¿podemos (en principio) 'visitar' cada posición posible del Cubo de Rubik exactamente una vez, haciendo un movimiento a la vez usando sólo los generadores básicos R, L, U, D, F, B?

Observación 4.3.1. Este es un caso especial de un **problema** *sin resolver* más general: Para un grupo de permutación arbitrario con un conjunto generador dado, ¿es su grafo de Cayley Hamiltoniano?

Un ejemplo de un grupo (con generadores) donde se sabe que su grafo de Cayley tiene un circuito Hamiltoniano es el grupo simétrico (con generadores el conjunto de todas las transposiciones).

Ejemplo 4.3.1. Sea G el grupo S_n con generadores dados por el conjunto de todas las transposiciones:

$$G = S_n, \qquad X = \{(i, j) |\ 1 \leq i < j \leq n\}.$$

(Hay muchas más transposiciones de lo necesario para generar S_n puesto que el subconjunto de transposiciones de la forma $(i, i+1), 1 \leq i < j \leq n-1$, suficientes para generar S_n [R].) El algoritmo de Steinhaus (véase 1.4) muestra que hay un circuito Hamiltoniano en el grafo de Cayley de S_n con respecto a X.

4.4 El grafo del Puzzle 15

Esta sección se discute el Puzzle 15 desde el punto de vista grafo-teórico. El objetivo del puzzle fue ordenar las piezas del 1 al 15 de izquierda a derecha y de arriba abajo, como se muestra en la **posición resuelta** dada en 2.1

Para resolver un puzzle "desordenado", se podrían deslizar los cuadrados alrededor en el puzzle. Con el fin de hacer esto debemos deslizar un cuadrado numerado al lugar vacío.

Podríamos representar esto matemáticamente diciendo que se trata de una transposición de ese cuadrado numerado y el cuadrado vacío.
Si etiquetamos cada espacio en el puzzle como un vértice, y etiquetamos los vértices numéricamente, entonces el grafo resultante está representado por la siguiente figura.

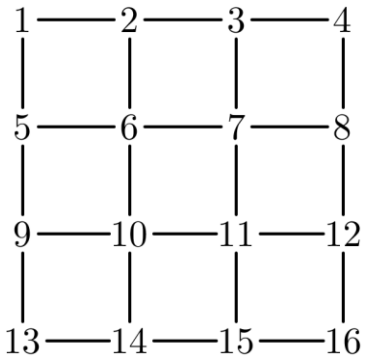


Figura 4.3

Vamos a denotar el espacio vacío por 16 y llamemos a este grafo Γ. Los únicos movimientos legales del puzzle son transposiciones del vértice 16 y un vértice que es adyacente al mismo. Por lo tanto, cualquier permutación de los vértices produce un etiquetado sobre Γ.

4.4.1 Definiciones generales

Ahora sea Γ un grafo simple con el conjunto de vértices $V(\Gamma)$ de cardinalidad N. (En el ejemplo anterior $N = 16$). Por un **etiquetado** nos referimos a la colocación de los números del 1 al N de vértices distintos de Γ, donde N denota el espacio vacío. En otras palabras, un etiquetado sobre Γ es un mapeo biyectivo $f : V(\Gamma) \to \{1, 2, \dots, N\}$.
Dos etiquetados f, g sobre Γ son **adyacentes** si y sólo si g es un resultado de una transposición simple sobre f del vértice N con un vértice adyacente a N de f. En otras palabras, f y g son adyacentes si difieren por un movimiento legal del puzzle. De Γ, hacemos un nuevo grafo $puz(\Gamma)$ como sigue: el conjunto vértice $V(puz(\Gamma))$ contiene todos los etiquetados sobre Γ, y dos vértices en $puz(\Gamma)$ están unidos por una arista si los etiquetados asociados son adyacentes.

Por ejemplo, los etiquetados en la Figura 4.4 y la Figura 4.5 son adyacentes.

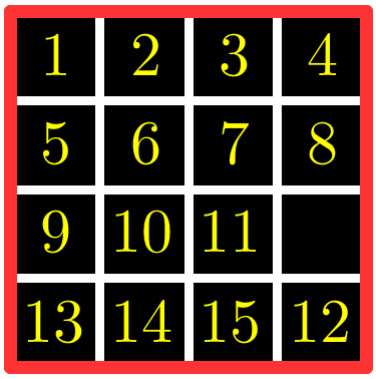


Figura 4.4

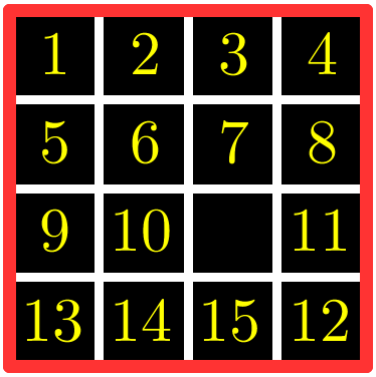


Figura 4.5

Podemos considerar un **camino** p como una secuencia de movimientos sobre el grafo $puz(\Gamma)$, $p = (x_0, x_1, x_2, \dots, x_n)$, donde los x_i son vértices de Γ, y (si $n \geq 1$) x_i y x_{i-1} son adyacentes en Γ para $1 \leq i \leq n$. Tal camino p se dice que es de x_0 (su **vértice inicial**) a x_n (su **vértice terminal**). El camino p es **simple** si $x_0, x_1, x_2, \dots, x_n$ son distintos. Si $x_0 = x_n$, entonces p es llamado un **camino cerrado basado en** x_0. Sea x_0 un vértice fijo de Γ. Si p, p' son caminos cerrados basados en x_0, entonces la **composición** pp' es el camino obtenido por la yuxtaposición del camino de p con el camino de p'. El **inverso** de un camino p, denotado p^{-1}, es el camino que atraviesa p en la dirección opuesta. El camino identidad es el camino desde x_0 a sí mismo que no contiene aristas de Γ. El conjunto de caminos cerrados basados en x_0 forman un grupo (bajo composición de caminos) llamado el **grupo de homotopía** de Γ basado en x_0, denotado $\Gamma(x_0)$.
Ahora supongamos que pintamos los bloques del Puzzle 15 en un tablero de ajedrez:

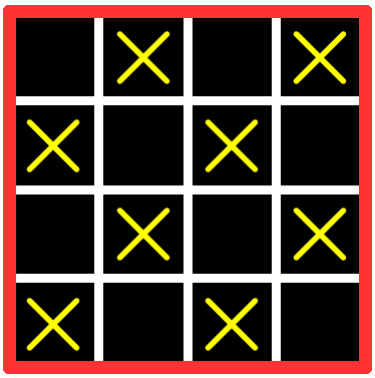


Figura 4.6

En este arreglo el espacio vacío empezaría con un cuadrado amarillo. Si tuviéramos que mover el cuadrado vacío hacia arriba, entonces es ahora un cuadrado negro. Esa es una transposición; por lo tanto, el movimiento es impar. Si movemos el espacio vacío a la izquierda, el espacio vacío estaría en un cuadrado amarillo. Esto es un total de dos transposiciones, por lo tanto, el movimiento es par. Después de tres transposiciones el espacio vacío estaría sobre cuadrado negro, por lo tanto, sería una permutación impar. Por lo tanto, si el espacio vacío termina en un cuadrado amarillo, una permutación par ha ocurrido. Si el espacio vacío termina en un cuadrado negro, una permutación impar ha ocurrido.

Una **posición legal** del Puzzle 15 es cualquier secuencia a partir de transposiciones legales empezando desde la posición resuelta tal que el hueco termina en la esquina inferior derecha. Cada posición corresponde a una permutación de los 15 vértices numerados y por tanto a un elemento del grupo simétrico S_{15}. El conjunto de todas las permutaciones (que surgen como una secuencia de transposiciones) en S_{15} forman un grupo llamado el **grupo (homotopía) del Puzzle 15.**

Note que el grupo del Puzzle 15 es isomorfo al grupo homotopía del grafo Puzzle 15 basado en el 'vértice vacío'.

Si asignamos el número 16 al hueco, entonces podemos ver que podemos arreglar las piezas del puzzle en 16! maneras diferentes. Sin embargo, si tomamos sólo posiciones legales del Puzzle 15, entonces estamos fijando una de las piezas. Como resultado el número de maneras de permutar el resto de las piezas, con el hueco sobre el cuadrado blanco en la parte inferior esquina derecha, es a lo sumo 15! Todas las tales permutaciones tienen que ser pares, por el análisis de tablero de ajedrez anterior. El número de permutaciones pares de 15 elementos

(hay un número igual de permutaciones pares e impares) es de 15!/2. De esto vemos que el puzzle 15 tiene a lo sumo 15!/2 posibles posiciones legales. De hecho, tiene exactamente este número:

Teorema 4.4.1. Las posiciones con el espacio vacío en la parte inferior derecha que se puede alcanzar desde la posición inicial del Puzzle 15 por piezas de desplazamiento se encuentran en una correspondencia biyectiva con las 15!/2 = 1,307,674,368,000 permutaciones pares de los números del 1 al 15.

Observación 4.4.1. El puzzle 14-15 no se puede resolver, porque es una permutación impar. Sólo tiene una transposición, 14 intercambiado con 15.

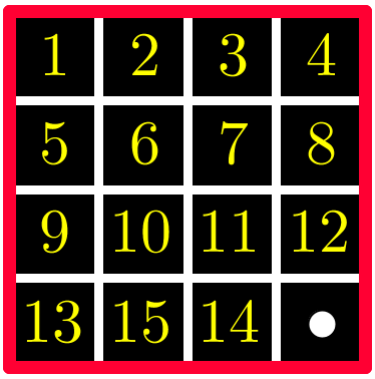


Figura 4.7

Prueba: Si etiquetamos el espacio vacío por 16, entonces cada posición posible de puzzle puede ser considerado como un elemento del grupo simétrico S_{16} y un elemento de $puz(\Gamma)$. Hay 16! elementos en S_{16}, y 16! vértices de $puz(\Gamma)$. Con el argumento anterior podemos demostrar que todas las posiciones legales del puzzle son obtenidas por un número par de transposiciones. Por lo tanto, todos los movimientos legales son permutaciones pares del puzzle.

Ahora debemos demostrar que hay un 3-ciclo en el grupo del Puzzle 15. Por ejemplo, si desplazamos las tres piezas que rodean el espacio vacío alrededor de un círculo, siguiendo el orden de los movimientos sur-este-norte-oeste, entonces el tres-ciclo (11, 12, 15) se produce. Se puede demostrar que si se fijan las piezas 11 y 12, entonces cualquier otra pieza puede tomar el lugar de la 15 siguiendo uno de los ciclos en las figuras siguientes.

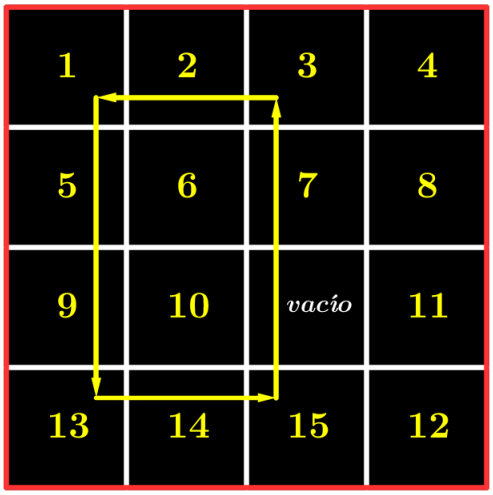


Figura 4.8

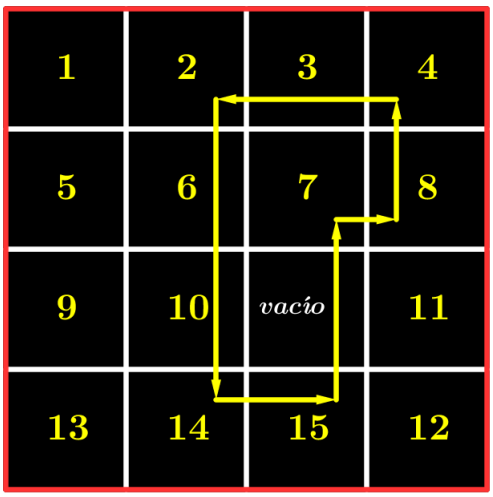


Figura 4.9

Por el Lema 6.4.4, tales 3-ciclos generan A_{15}. Esto demuestra el teorema (ver [J]).

Demostrar que algo es imposible tiene un efecto en los alumnos, porque sin importar que nos pasemos horas jugando e intentando resolver el 14-15, (cumpliendo las reglas) no lo resolveremos, pero demostrar que es *imposible* significa que no importa como lo intentemos, no lo lograremos, como ocurre con la demostración de que la cuadratura del círculo es imposible con regla y compás.

Observación 4.4.2. Otra prueba es posible. Alternativamente, con algún trabajo podemos demostrar que cualquier número puede sustituir el 11 en el tres-ciclo, y podemos demostrar que cualquier otro número puede sustituir el 12. De esto podemos concluir que cualquier tres-ciclo puede ser formado. Puesto que cada permutación par es una combinación de tres-ciclos (por Proposición 6.4.1), cada permutación par del Puzzle 15 puede ser alcanzada.

Con esta información, podemos hacer una generalización de los puzles rectangulares de tamaño $m \times n$ con $m > 1$ y $n > 1$.

Teorema 4.4.2. El grupo homotopico de un puzzle rectangular $m \times n$ es el grupo alternante A_{mn-1}.

La prueba de esto es similar a la prueba para el puzzle 4×4, si $m > 3$ y n> 3. (Los casos especiales, cuando $1 < m < 4$ o $1 < n < 4$ deben ser tratados por separado) El tamaño del grupo alternante está dado por $(mn - 1)!/2$.

Capítulo 5

Simetría y los Sólidos Platónicos

Un poliedro regular es el análogo tridimensional a los polígonos regulares. Polígono regular es un cuerpo geométrico cuyas caras son polígonos regulares congruentes (planos). Muchos puzzles se realizan por corte de un poliedro regular, así que es natural estudiarlos junto con sus simetrías.

5.1 Descripciones

Los **sólidos platónicos** son los 5 poliedros regulares:

Poliedro	***# Caras***	***# Vertices***	***# Aristas***	***Grupo***	p, q
Tetraedro	4	4	6	T	$3, 3$
Hexaedro	6	8	12	O	$4, 3$
Octaedro	8	6	12	O	$3, 4$
Dodecaedro	12	20	30	I	$5, 3$
Icosaedro	20	12	30	I	$3, 5$

Tabla 5.1

- p, llamado el **grado de la cara**, indica el número de aristas que delimitan cada cara,
- q, llamado el **grado del vértice**, indica el número de caras que se encuentran en cada vértice.

Estos sólidos llevan el nombre del gran filósofo griego Platón (427-347 a. C.). Un vértice de uno de estos sólidos, por consiguiente se especifica por la q-tupla de caras que se encuentran en cada vértice.

Estos sólidos se pueden dibujar en coordenadas rectangulares usando

Poliedro	***Coordenadas***
Tetraedro	$(1, 1, 1), (1, -1, -1), (-1, -1, 1), (-1, 1, -1)$
Hexaedro	$(1, 1, 1), (1, 1, -1), (1, -1, 1), (-1, 1, 1),$ $(1, -1, -1), (-1, 1, -1), (-1, -1, 1), (-1, -1, -1)$
Octaedro	$(1, 0, 0), (0, 0, 1), (0, 1, 0),$ $(-1, 0, 0), (0, -1, 0), (0, 0, -1)$

Dodecaedro	$(0, \pm\phi^{-1}, \pm\phi), (\pm\phi^{-1}, \pm\phi, 0),$ $(\pm\phi, 0, \pm\phi^{-1},), (\pm 1, \pm 1, \pm 1)$
Icosaedro	$(1, 0, \phi), (1, 0, -\phi), (-1, 0, \phi), (-1, 0, -\phi),$ $(0, \phi, 1), (0, \phi, -1), (0, -\phi, 1), (0, -\phi, -1),$ $(\phi, 1, 0), (\phi, -1, 0), (-\phi, 1, 0), (-\phi, -1, 0)$

Tabla 5.2

donde $\phi = \frac{1+\sqrt{5}}{2} = 1.61803\ldots$ denota la proporción áurea.

Un detalle importante es la existencia de los poliedros duales por ejemplo el dual del cubo es el octaedro que se obtiene uniendo los puntos medios de cada cara.

Figura 5.1

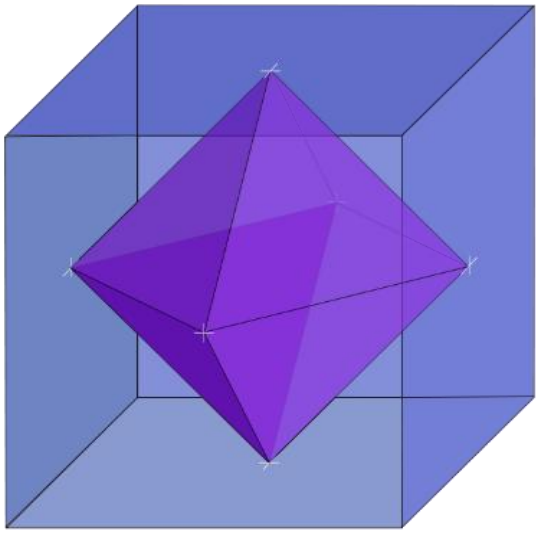


Figura 5.2

Dual del cubo

Si P_1, P_2, P_3 son tres vértices de una cara del icosaedro, entonces $(P_1 + P_2 + P_3)/3$ forma un vértice del dodecaedro dual y cada vértice del dodecaedro dual surge de esta manera.
Los tres 'grupos Platónicos' (el grupo de 'simetrías' de estas figuras) se describen a continuación. Sus nombres:

- T = grupo de simetría del tetraedro = **grupo tetraédrico,**
- O = grupo de simetría del octaedro (o cubo) = **grupo octaédrico,**
- I = grupo de simetría del icosaedro (o dodecaedro) = **grupo icosaédrico.**

5.2 Antecedentes de simetrías en el espacio tridimensional

En esta sección consideramos las isometrías en 3 dimensiones, esto es necesario para la comprensión de los grupos de simetría de los sólidos platónicos. Motivados por el estudio de la estructura de los cristales, Camille Jordan fue el primero en considerar la clasificación de las simetrías en el espacio tridimensional. Jordan (1838-1922) fue uno de los pioneros de la teoría de grupos, uso los grupos para entender mejor los cristales.
Establezcamos la 'Regla de la mano derecha' orientación en el espacio tridimensional. Llamamos a una transformación que preserva distancia en el espacio tridimensional **simetría en** $\mathbb{R}^3$la cual deja fijo el origen (Lo que otros autores llaman isometría). Decimos que tal simetría **preserva la orientación** sí preserva la orientación de la regla de la mano derecha.

Ejemplo 5.2.1. Sea $s: \mathbb{R}^3 \to \mathbb{R}^3$ la función que toma cada vector v perteneciente a $\mathbb{R}^3$ y devuelve su reflexión $s(v)$ sobre el plano yz. Este no preserva la orientación, ya que invierte la dirección en sentido antihorario trayectoria circular en el plano yz. En términos de coordenadas rectangulares, $s(x, y, z) = (-x, y, z)$.

Sea $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \text{ números reales}\}$ espacio tridimensional. También escribimos esto, cuando sea conveniente, como vectores columna

$$\mathbb{R}^3 = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mid x, y, z \text{ reales} \right\}$$

La **función distancia** en $\mathbb{R}^3$ es la función

$$d(\overrightarrow{v_1}, \overrightarrow{v_2}) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2},$$

donde $\overrightarrow{v_1} = (x_1, y_1, z_1)$, $\overrightarrow{v_2} = (x_2, y_2, z_2)$. Esto puede expresarse en términos del **producto interno** $\overrightarrow{v_1} \cdot \overrightarrow{v_2} = x_1x_2 + y_1y_2 + z_1z_2$ como $d(\overrightarrow{v_1}, \overrightarrow{v_2}) = \sqrt{(\overrightarrow{v_1} - \overrightarrow{v_2}) \cdot (\overrightarrow{v_1} - \overrightarrow{v_2})}$.
Recíprocamente, la **identidad de polarización**

$$\overrightarrow{v_1} \cdot \overrightarrow{v_2} = \frac{1}{4}(\|\overrightarrow{v_1} + \overrightarrow{v_2}\|^2 - \|\overrightarrow{v_1} - \overrightarrow{v_2}\|^2)$$

permite recuperar el valor del producto interno a partir del conocimiento de valores de la función distancia.
Llamamos una función $f: \mathbb{R}^3 \to \mathbb{R}^3$ una **isometría** si satisface

$$d\big(f(\overrightarrow{v_1}), f(\overrightarrow{v_2})\big) = d(\overrightarrow{v_1}, \overrightarrow{v_2})$$

para todo $\overrightarrow{v_1}$ y $\overrightarrow{v_2}$ en $\mathbb{R}^3$.
Queremos entender un poco mejor las isometrías, puesto que se preservan distancias (y, en particular, preservan las formas de los sólidos) y por lo tanto nos proporciona los tipos de simetrías del espacio tridimensional que queremos considerar. Podemos construir isometrías usando ciertos tipos de matrices 3×3.

Lema 5.2.1. Si A es una matriz 3×3 entonces la función $A: \mathbb{R}^3 \to \mathbb{R}^3$ es una isometría si y sólo si $A^tA = I_3$, donde A^t denota la matriz transpuesta (que se obtiene al voltear las entradas de A respecto de la diagonal).

Observación 5.2.1. En particular, si A es una isometría entonces $det(A)^2 = det(A^t)det(A) = det(A^tA) = det(I_3) = 1$.

Prueba: La función distancia es preservada si y sólo si la función producto escalar es preservada. (Esto es una consecuencia de la 'identidad polarización' citada anteriormente). Sea $m(\vec{v}, \vec{w}) = \vec{v} \cdot \vec{w}$, donde $\cdot$ denota el producto punto. Puesto que
$m(A\vec{v}, B\vec{w}) = \vec{v} \cdot (A^tB)\vec{w}$, tenemos

$$m(A\vec{v}, A\vec{w}) = m(\vec{v}, \vec{w}), \qquad \forall\, v, w \in \mathbb{R}^3$$

si y sólo si

$$\vec{v} \cdot (A^tA)\vec{w} = \vec{v} \cdot \vec{w}, \qquad \forall\, v, w \in \mathbb{R}^3$$

si y sólo si $A^tA = I_3$.

Ejemplo 5.2.2. Una matriz rotación en 3 dimensiones puede ser escrita en la forma

$$R(\phi, \theta, \psi) = \begin{pmatrix} r_{11} & r_{12} & \sin(\theta)\sin(\psi) \\ r_{21} & r_{22} & \sin(\theta)\cos(\psi) \\ \sin(\phi)\sin(\theta) & -\sin(\theta)\cos(\phi) & \cos(\theta) \end{pmatrix},$$

donde

$$\begin{aligned} r_{11} &= \cos(\phi)\cos(\psi) - \cos(\theta)\sin(\phi)\sin(\psi), \\ r_{12} &= \sin(\phi)\cos(\psi) + \cos(\theta)\cos(\phi)\sin(\psi), \\ r_{21} &= -\cos(\phi)\sin(\psi) - \cos(\theta)\sin(\phi)\cos(\psi), \\ r_{22} &= -\sin(\phi)\sin(\psi) + \cos(\theta)\cos(\phi)\cos(\psi). \end{aligned}$$

y donde los ángulos ϕ, θ, ψ son los 'ángulos de Euler'. Esto representa la rotación del espacio tridimensional obtenido mediante la siguiente secuencia de rotaciones: rotar un ángulo ψ alrededor del eje z, rotar un ángulo θ alrededro el eje x $(0 \leq \theta \leq \pi)$, a continuación, rotar un ángulo ϕ sobre el eje z otra vez.
Aunque se trata de un hecho interesante debido a su carácter explícito, no vamos a utilizar esta expresión.

Pregunta: ¿Hay algunas isometrías que no provienen de las matrices como en el lema ya mencionado? Sí: la traslación da lugar a una isometría pero la traslación no es lineal, por lo que no puede ser descrita como una matriz. Por otra parte, cualquier reflexión sobre un plano que contiene el origen también es una isometría. Una reflexión no pertenece al grupo generado por las traslaciones y rotaciones.
Pregunta: ¿Hay algunos ejemplos de isometrías que no se deriven de una composición de una traslación y una matriz ortogonal? No: el siguiente teorema clasifica todas las isometrías.

Teorema 5.2.1. Una función $f: \mathbb{R}^3 \to \mathbb{R}^3$ es una isometría fijando el origen si y sólo si f es una multiplicación a izquierda por una matriz ortogonal.

Esta no será probado aquí (ver Artin [Ar], capítulo 4, sección 5, Proposición 5.16).

Como consecuencia de este lema, podemos ver que si la matriz A da lugar a una isometría entonces $det(A)$ es igual a 1 o bien a -1 (Puesto que $det(A)^2 = det(A^tA) = det(I_3) = 1$. La matriz es invertible ya que, por definición, $A^{-1} = A^t$.

Lema 5.2.2. El conjunto de todas las matrices A 3×3 tal que la función $A : \mathbb{R}^3 \to \mathbb{R}^3$ es una isometría forma un grupo bajo la multiplicación de matrices.

Notación: Este grupo se denotará $O_3(\mathbb{R})$ y llamado el grupo ortogonal de $\mathbb{R}^3$. Denotamos por $SO_3(\mathbb{R})$, el siguiente subconjunto

$$SO_3(\mathbb{R}) = \{A \in O_3(\mathbb{R}) \mid det(A) = 1\}$$

que es llamado el **grupo ortogonal especial** de $\mathbb{R}^3$.

Lema 5.2.3. $SO_3(\mathbb{R})$ es un subgrupo de $O_3(\mathbb{R})$.

Es fácil verificar los axiomas de grupo para $SO_3(\mathbb{R})$.

Se sabe que el número de clases laterales en $O_3(\mathbb{R})/SO_3(\mathbb{R})$ es 2. De hecho, se sabe que

$$O_3(\mathbb{R}) = SO_3(\mathbb{R}) \cup s \cdot SO_3(\mathbb{R}) \quad \text{(unión disjunta)}, \tag{5.1}$$

donde s es la reflexión en el ejemplo anterior (esto sigue de [Ar], en el capítulo 4, sección 5).

Lema 5.2.4. La isometría A en $O_3(\mathbb{R})$ preserva orientación si y sólo si $det(A) = 1$.

No vamos a demostrar este lema aquí (véase, [Ar]).

5.3 Simetrías del tetraedro

Fijar un tetraedro centrado en el origen, con un vértice a lo largo del eje z. Cada arista tiene una arista 'opuesta' sobre el tetraedro (que en realidad es perpendicular a él si lo miramos de frente). Cada vértice tiene una cara 'opuesta'.

Hay simetrías que preservan orientación (llamadas **rotaciones**) del tetraedro y las simetrías que invierten orientación del tetraedro. Las simetrías que preservan orientación del tetraedro se denotan ST. Se obtienen como sigue:

- Los 4 ejes de simetría a través de los centros de las caras opuestas obtienen 2 elementos cada uno (rotación de 120 grados en sentido horario y una rotación de 240 grados), para un total de 8 elementos. (Esta 'simetría tetraédrica' permite la construcción de la Pyraminx).
- Los 3 pares de aristas (formado por una arista y su opuesta) obtienen un elemento de cada uno (una rotación de 180 grados), para un total de 3 elementos.

Estos, además de la identidad, dan 12 elementos en ST.
Usando la descomposición de clases laterales (5.1), tenemos $T = ST \cup s \cdot ST$ (disjuntos), por lo que

$$|T| = |ST| + |s \cdot ST| = 12 + 12 = 24.$$

Observación 5.3.1. Resulta que ST es esencialmente el grupo alternante A_4 de permutaciones pares en S_4 y T es esencialmente S_4 mismo.

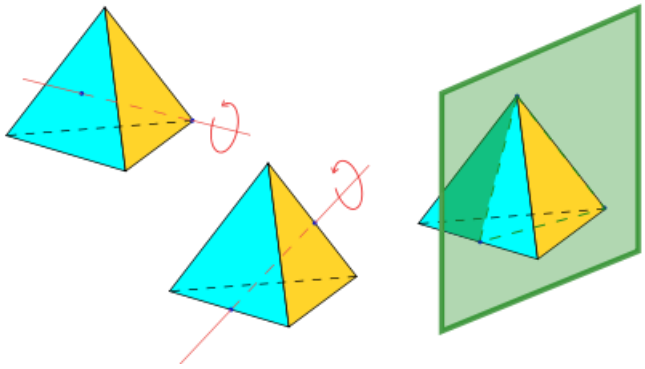


Figura 5.3

5.4 Simetrías del cubo

Fijamos un cubo centrado en torno al origen en el espacio tridimensional. El conjunto de centros de las caras de un cubo forma un conjunto de vértices de un octaedro dibujado en el interior del cubo. Este octaedro es llamado poliedro 'dual'. Estos dos poliedros tienen el mismo grupo de simetría, el cual se denota por O.

Hay simetrías que preservan orientación, o rotaciones, del cubo y las simetrías que invierten orientación del cubo. Las simetrías que preservan orientación del cubo se denotan SO. Se obtienen como sigue:

- Los 3 ejes de simetría a través de los centros de las caras opuestas producen 3 elementos cada uno (rotación de 90 grados en sentido horario, una rotación de 180 grados, y una rotación de 270 grados), para un total de 9 elementos.
  (Esta 'simetría hexaédrica' permite la construcción mecánica del Cubo de Rubik.)

- Los 4 ejes a través de los vértices opuestos producen 2 elementos cada uno (todos de orden 3), para un total de 8 elementos.

- Los 6 ejes a través de los puntos medios de las aristas opuestas producen un elemento cada uno (de orden 2), para un total de 6 elementos.

Estos elementos, además de la identidad, producen 24 elementos.

Lema 5.4.1. Hay 24 elementos que preservan orientación en O, es decir, $|SO| = 24$.

He aquí otra prueba de este resultado.
Prueba: Sea V el conjunto de vértices del cubo. El grupo SO actúa sobre el conjunto V. Fijamos un v perteneciente a V y sea $H = stab_{SO}(v)$. Se puede comprobar que $|H| = 3$. (Puesto que solamente la simetría fija V es una rotación g sobre la línea a través de V y su vértice opuesto. Puesto que g es de orden 3, $H = \langle g \rangle$ también es el orden 3.) Tenemos $|V| = 8$, así que por la

Proposición 3.10.1 sobre las órbitas y los estabilizadores, tenemos que $|SO/H| = |V|$. Por el teorema de Lagrange, $|SO| = |SO/H||H| = 8 \cdot 3 = 24$.

Ahora que conocemos SO, ¿qué es O? Nótese que s, la reflexión en el ejemplo de la sección anterior, pertenece a O. Usando la descomposición de clases laterales de la sección anterior, tenemos la descomposición de clase laterales

$$O = SO \cup s \cdot SO \quad \text{(unión disjunta)}.$$

Sabemos que $|s \cdot SO| = |SO| = 24$, por lo que el principio aditivo una vez más llega al rescate, dando el siguiente resultado.

Lema 5.4.2. El orden del grupo octaédrico es $|O| = 48$.

Observación 5.4.1. Resulta que SO es esencialmente el grupo simétrico S_4 y O es 'isomorfo al producto directo' $S_4 \times C_2$.

Figura 5.4

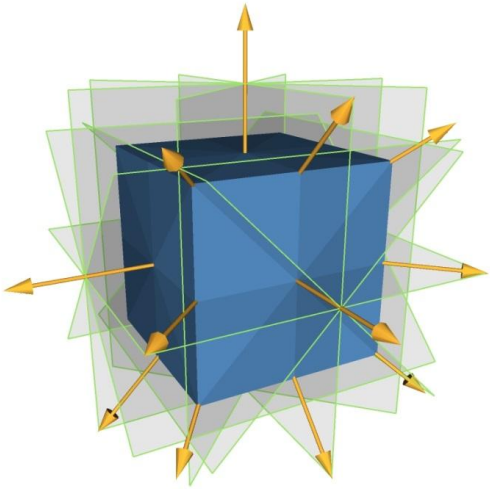


Figura 5.5

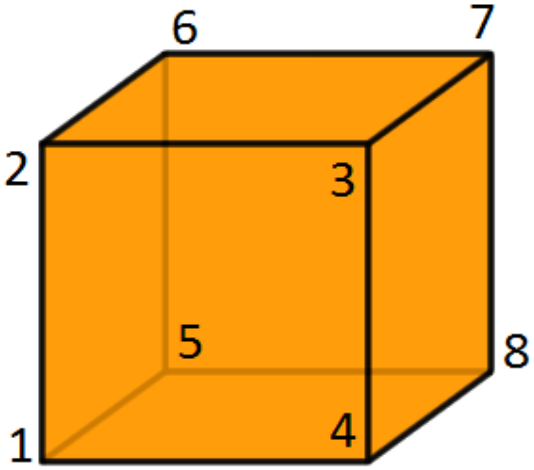


Figura 5.6

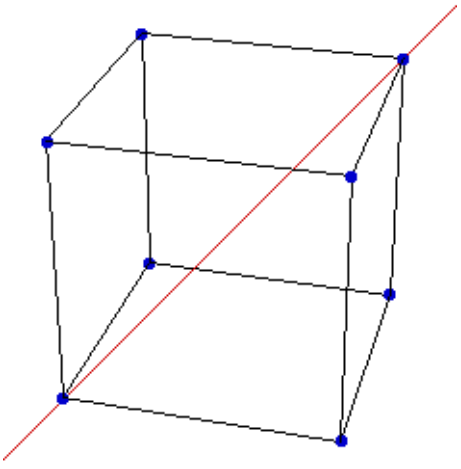


Figura 5.7

Simetrías del cubo diferentes de la identidad *(se numeran los vértices del cubo de alguna manera, la Figura 5.6 muestra una opción)*

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
P_1	2	5	6	3	7	8	1	4
P_2	5	7	8	6	1	4	2	3
P_3	7	1	4	8	2	3	5	6
P_4	7	5	2	1	6	3	8	4
P_5	8	6	5	7	3	2	4	1
P_6	4	3	6	8	2	5	1	7
P_7	2	3	4	1	6	8	6	7
P_8	3	4	1	2	8	7	6	7
P_9	4	1	2	3	7	5	8	6
P_{10}	1	7	5	2	8	6	4	3
P_{11}	1	4	8	7	3	6	2	5
P_{12}	5	2	1	7	3	4	6	8
P_{13}	3	2	5	6	1	7	4	8
P_{14}	8	7	1	4	5	2	6	3
P_{15}	3	6	8	4	5	7	2	1
P_{16}	8	4	3	6	1	2	7	5
P_{17}	5	6	3	2	8	4	7	1
P_{18}	2	1	7	5	4	8	3	6
P_{19}	6	5	7	8	2	3	1	4
P_{20}	6	8	4	3	7	1	5	2
P_{21}	7	5	6	8	2	3	1	4
P_{22}	4	8	7	1	6	5	3	2
P_{23}	6	3	2	5	4	1	8	7

Tabla 5.3

5.5 Simetrías del dodecaedro

El conjunto de los centros de las caras de un dodecaedro forman un conjunto de vértices de un icosaedro dibujado en el interior. Este icosaedro es llamado el poliedro 'dual'. Fijamos un dodecaedro en el espacio tridimensional para que los vértices del icosaedro dual sean como se enumeran al comienzo de este capítulo.

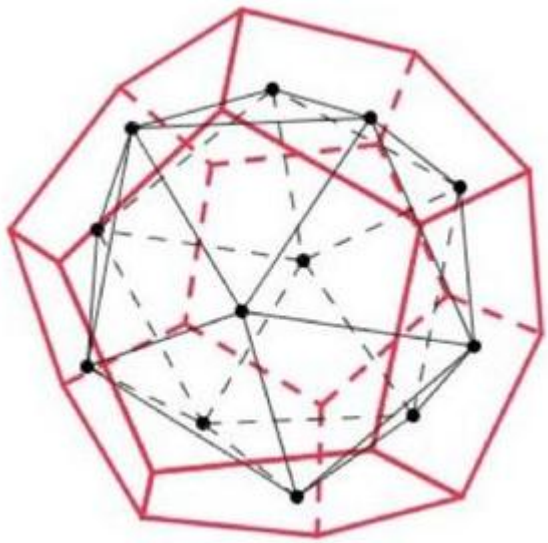


Figura 5.8: *Un dodecaedro.*

Sea SI el grupo de simetrías que preservan orientación del dodecaedro. Nótese que SI es un subgrupo finito de $SO_3(\mathbb{R})$. Sea I el grupo de todas las simetrías del dodecaedro. Nótese que I es un subgrupo finito de $O_3(\mathbb{R})$ y SI es un subgrupo de I. Sea F el conjunto de caras del dodecaedro, así que $|\boldsymbol{F}| = 12$. SI actúa sobre F.

Lema 5.5.1. SI actúa sobre F transitivamente.

No vamos a probar esto. Si nos fijamos en un dodecaedro se sigue 'por inspección'. La razón por la cual esto es útil es que se nos dice que si x es cualquier cara, entonces cualquier otra cara puede obtenerse a partir de x mediante la aplicación de algún elemento de SI. En otras palabras, la órbita de x es todo $F : SI \cdot x = F$.
Si x es cualquier cara entonces las únicas simetrías que preservan orientación que no envían x hacia una cara diferente son rotaciones por un múltiplo entero de 72 grados alrededor de la línea que pasa por el centro de x y el centro de su cara opuesta. Hay para cada x, exactamente 5 rotaciones distintas de este tipo. Por lo tanto,

$$|stab_{SI}(x)| = 5.$$

Por Proposición 3.10.1 tenemos

$$|SI/stab_{SI}(x)| = |SI \cdot x|,$$

así que $|SI| = |SI/stab_{SI}(x)||SI \cdot x| = 5 \cdot 12 = 60$
Los elementos de SI incluyen

- rotación por $2\pi k/5$ (para $k \in \{0, 1, 2, 3, 4\}$) sobre la línea que pasa a través del centro de una cara y su opuesta;
- rotación por $2\pi k/3$ (para $k \in \{0, 1, 2\}$) sobre la línea que pasa a través de un vértice y su opuesto;
- rotación por π que pasa a través del centro de una arista.

Los subgrupos incluyen los siguientes

(a) Estabilizador de un vértice. Estos son todos los cíclicos de orden 3, y todos ellos son conjugados. Hay 10 subgrupos distintos puesto que un vértice y su opuesto comparten el mismo estabilizador.
(b) Estabilizador de una cara. Estos son todos los cíclicos de orden 5, y todos ellos son conjugados. Hay 6 distintos de tales subgrupos puesto que una cara y su opuesta comparten el mismo estabilizador.
(c) Estabilizador de una arista. Estos son todos los cíclicos de orden 2, y todos ellos son conjugados. Hay 15 distintos de tales subgrupos.

Observación 5.5.1. Resulta que SI es esencialmente el grupo alternante A_5 de permutaciones pares en S_5 e I es 'isomorfo al producto directo' $A_5 \times C_2$.

5.6 Algunas reflexiones sobre el icosaedro

Esta sección se basa en una de las columnas de Internet semanales de John Baez.
Un **duada** es un par de diagonales (una diagonal es un segmento de un vértice a su vértice opuesto) del icosaedro. La parte superior del icosaedro tiene 6 vértices y cada diagonal debe tener exactamente uno de esos 6 vértices como un punto final. Hay 12 vértices, por lo tanto 6 diagonales, por lo tanto

$$\binom{6}{2} = 15$$

duadas diferentes. Cada duada determina un 'rectángulo de oro' (es decir, un rectángulo cuya razón longitud anchura es o bien la proporción áurea $\phi = \left(1 + \sqrt{5}\right)/2$ o su inversa). Podemos identificar una duada con un par de enteros distintos $\{(i,j)|1 \leq i < j \leq 6\}$, es decir, con un 2-ciclo en S_6.
James J. Sylvester llamó una partición $X = X_1 \cup \ldots \cup X_n$ (disjunto)

de un conjunto X un **syntheme** si cada uno de los conjuntos X_i, $1 \leq i \leq n$, tiene el mismo número de elementos. Si tomamos

$$X = \{\text{conjunto de diagonales del icosaedro}\}$$

entonces, un syntheme es un conjunto de tres duadas, no hay dos que tienen una diagonal en común.
Hay

$$\binom{6}{2}\binom{4}{2} / 3! = 15$$

diferentes synthemes (3! puesto que hay 3! formas de permutar las duadas entre ellas). Un syntheme puede estar representado por una coloración de los vértices sobre la parte superior del icosaedro usando tres colores, cada uno para exactamente dos vértices. Podemos identificar un syntheme con un producto de 3 distintos 2-ciclos en S_6. Particionamos el conjunto de 15 duadas en 5 grupos de 3 como sigue. (Recuérdese cada syntheme es un triple de duadas.) Primero, elegimos un syntheme, A_1. Elegimos otro syntheme A_2, de modo que A_1, A_2 no tienen duada en común. Continuando por este camino hasta que elijamos 5 synthemes

$A_1, \ldots, A_5$, dos de los cuales no tienen una duada en común. Tal elección de 5 synthemes es llamada una **pentada**. Hay 6 pentadas que etiquetamos $P_1, \ldots, P_6$ en cualquier forma que deseemos. (Una lista de las 6 pentadas se da en [R], capítulo 7.) Cualquier permutación de las 6 diagonales del icosaedro da lugar a una permutación del conjunto de 6 pentadas. De ahí que cualquier permutación de las 6 diagonales del icosaedro, que puede ser considerada como un elemento de S_6, da lugar a una permutación del conjunto de 6 pentadas, que también pueden ser considerados como un elemento de S_6. Esto da un mapeo

$$f : S_6 \to S_6.$$

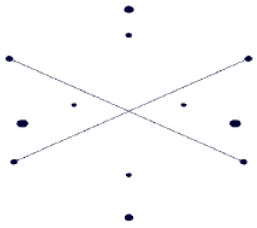


Figura 5.9: *Una duada*

Cada elemento del grupo de rotaciones de un icosaedro (es decir, el grupo de simetrías que preservan orientación simetrías del icosaedro) debe enviar una duada a una duada. Cada duada tiene 4-veces la simetría, es decir, pueden ser enviados a sí mismo en 4 formas. Hay 15 duadas, por lo que hay $4 \cdot 15 = 60$ maneras de enviar una duada a otra. Este es precisamente el número de simetrías que preservan orientación del icosaedro.

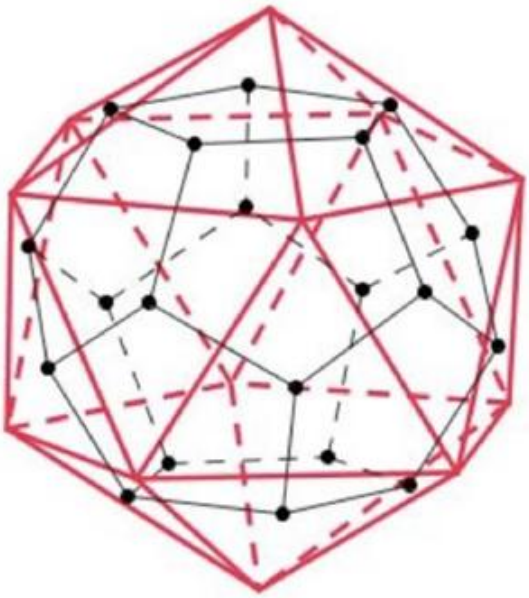


Figura 5.10: *Un icosaedro.*

Tenga en cuenta que los pares (0, 3) y (4, 8) forman una duada.
Algunas de estas ideas se tratarán más adelante en 6.3.2 Véase también [R].

Capítulo 6

El grupo cubo ilegal

Una forma de estudiar los grupos es considerar una analogía con las moléculas en química. Queremos saber "cómo se ven", para saber cómo describirlos, cómo compararlos, cómo hacer más con ellos, para saber si caen en familias con propiedades similares, y así sucesivamente.
Dadas dos moléculas, un químico quiere saber cómo compararlas, para entender sus similitudes y diferencias. Por ejemplo Figura 6.1.

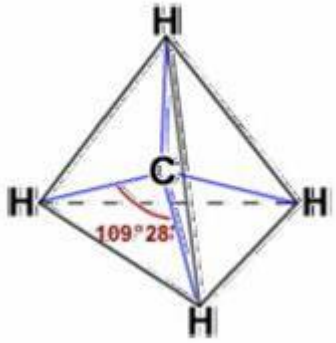


Figura 6.1 *El metano*

Dados dos grupos G_1, G_2, una pregunta análoga es ¿Qué tan similares son? (Exactamente lo que se entiende por 'similares' se explicará más adelante.) En este capítulo, vamos a introducir nociones y técnicas útiles para la comparación de dos grupos. En un capítulo posterior, nos centraremos en el grupo Cubo de Rubik 3×3 comparándolo con grupos que 'entendemos mejor', como los grupos cíclicos y los grupos simétricos que ya hemos estudiado. En este capítulo, nos vamos a centrar en la comprensión de un grupo algo más simple, pero estrechamente relacionado, el grupo de todos los movimientos 'legales' e 'ilegales' del Cubo de Rubik.
En un movimiento 'ilegal' podemos desarmar y volver a armar el cubo, pero ya no se puede desprender e intercambiar pegatinas de las caritas. Sorprendentemente, el grupo ilegal Cubo de Rubik es más sencillo de entender que el grupo Cubo de Rubik en sí, aunque es mucho más grande. Para 'la construcción explícita' del grupo Cubo de Rubik, necesitamos saber cómo construir

- Grupos cociente,
- Productos directos,
- Productos semi-directos.

Éstos se estudian en este capítulo. Una vez que el grupo Cubo de Rubik se construye, es un asunto relativamente fácil de encontrar su orden, entre otras cosas.

6.1 *Homomorfismos*

Para comparar dos grupos, es frecuente hablar primero de las funciones entre ellos. Si $f : G_1 \to G_2$ es una función de un grupo G_1 a un grupo G_2, entonces, como podemos imaginar, si f y G_1 fueron bien entendidos, entonces alguna información sobre G_2 probablemente podría

ser obtenida. Es el propósito de este capítulo averiguar hasta qué punto esto puede ser precisado.
Un homomorfismo entre dos grupos es, en términos generales, una función entre ellos, que preserva las operaciones (respectivas) del grupo. Estos tipos especiales de funciones son las de mayor utilidad para nuestros propósitos.

Definición 6.1.1. Sean G_1, G_2 grupos, donde $*_1$ denota la operación del grupo en G_1 y $*_2$ la operación del grupo en G_2. Una función $f : G_1 \to G_2$ es un **homomorfismo** si y sólo si, para todo $a, b \in G_1$, tenemos

$$f(a *_1 b) = f(a) *_2 f(b).$$

Cuando no cause confusión, designaremos la operación binaria en un grupo simplemente por $\cdot$ en lugar de $*$.

Ejemplo 6.1.1. Sea G un grupo y h un elemento fijo de G. Definimos $f : G \to G$ por

$$f(g) = h^{-1} \cdot g \cdot h, \qquad g \in G$$

Entonces el calculo

$$f(a \cdot b) = h^{-1} \cdot (a \cdot b) \cdot h = h^{-1} \cdot a \cdot h \cdot h^{-1} \cdot b \cdot h = f(a) \cdot f(b)$$

muestra que f es un homomorfismo. En este caso, $im(f) = G$, es decir, f es sobreyectiva.

Problema 6.1.1. Sea

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Ahora, Sea $G = \langle A, B \rangle$, denota el grupo de todas las matrices que pueden ser escritas como cualquier producto arbitrario de estas dos matrices (en cualquier orden y con el mayor número de términos como deseemos). Mostrar que tenemos

$$G = \left\{ I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

(Podemos comprobar esto en relación con cada una de esas matrices de permutación.) Definimos $f : G \to S_3$ por

g	$f(g)$
I_3	1
A	s_1
B	s_2
$A \bullet B$	$s_1 \bullet s_2$
$B \bullet A$	$s_2 \bullet s_1$
$A \bullet B \bullet A$	$s_1 \bullet s_2 \bullet s_1$

Tabla 6.1

Demostrar que esto es un homomorfismo.

Ejemplo 6.1.2. La función $sign : S_n \to \{\pm 1\}$,

que asigna a cada permutación su signo, es un homomorfismo. Esto quedó demostrado en 1.1 Sin embargo, otra razón por la cual esto es verdad es porque el signo de una permutación g es el determinante de la matriz permutación asociada $P(g)$. Dado que el determinante del producto es el producto de los determinantes, tenemos

$$sign(gh) = det\, P(gh) = det\big(P(g)P(h)\big) = det\, P(g)\, det\, P(h) = sign(g)sign(h),$$

para todos $g, h \in S_n$. De esto se deduce que el $sign$ es un homomorfismo.

Lema 6.1.1. Si $f : G_1 \to G_2$ es un homomorfismo entonces

(a) $f(e_1) = e_2$, donde e_1 denota el elemento identidad de G_1 y e_2 denota el elemento identidad de G_2,

(b) $f(x^{-1}) = f(x)^{-1}$, para todo x perteneciente a G_1,

(c) $f(y^{-1} *_1 x *_1 y) = f(y)^{-1} *_2 f(x) *_2 f(y)$, para todo x, y pertenecientes a G_1,

donde $*_1$ denota la operación del grupo en G_1 y $*_2$ la operación del grupo en G_2.

Prueba:

(a) Tenemos que $f(x) = f(x *_1 e_1) = f(x) *_2 f(e_1)$, para cualquier $x \in G_1$. Multiplicando ambos lados de esta ecuación a la izquierda por $f(x)^{-1}$.

(b) Tenemos, por la parte (a), $e_2 = f(e_1) = f(x *_1 x^{-1}) = f(x) *_2 f(x^{-1})$. Multiplicando ambos lados de esta ecuación a la izquierda por $f(x)^{-1}$.

Problema 6.1.2. Mostrar la parte (c). *(Sugerencia: usar la definición y la parte (b).)*

Definición 6.1.2. Sean G_1, G_2 grupos finitos. Decimos que G_1 es inyectivo en G_2 si existe un homomorfismo inyectivo $f : G_1 \to G_2$. Un homomorfismo $f : G_1 \to G_2$ es un **isomorfismo** si es una biyección (como una función entre conjuntos). En este caso, llamamos a G_1 y G_2 **isomorfos** y escribimos $G_1 \cong G_2$. Un isomorfismo de un grupo G en sí mismo se llama un **automorfismo**.

El concepto de un isomorfismo fue introducido por C. Jordan. Además de la teoría de grupos, Jordan es famoso en los círculos matemáticos por demostrar rigurosamente uno de los más obvios resultados, pero difícil de probar rigurosamente: cualquier curva cerrada simple divide el plano en dos regiones. (Aquí, una **curva simple** en el plano es un camino continuo que no es la unión disjunta de dos o más caminos. Una **curva cerrada** es un camino continuo que comienza y termina en el mismo punto).

Un isomorfismo es la noción que utilizaremos cuando queremos decir dos grupos son 'esencialmente el mismo grupo', es decir, uno es básicamente una copia al carbón del otro con los elementos re-etiquetados y la operación binaria modificada. Por ejemplo, si tenemos cualesquiera dos grupos de orden 2 entonces deben ser isomorfos. (Se puede verificar que el mapeo que envía la identidad de un grupo a la identidad del otro y el único elemento no

identidad de un grupo al único elemento no-identidad del otro debe ser un isomorfismo de grupo). En otras palabras, sólo hay un grupo de orden 2, salvo isomorfismo.
Sea $O(n)$ el número de grupos no isomorfos de orden n, por lo que O es una función $O : \mathbb{N} \to \mathbb{N}$. Esta es una función de comportamiento curioso, saltando los enteros que tienen gran cantidad de factores primos, tales como $16, 24, 32, 48, \ldots$.

Es fácil mostrar lo siguiente:

(a) Si $m \geq 1$, entonces $G = \{e^{2\pi ik/m} | 0 \leq k \leq m-1\}$, con la operación de grupo dada por la multiplicación ordinaria de números complejos, es isomorfo al grupo aditivo $\mathbb{Z}/m\mathbb{Z}$.

(b) Si $m > 1$, n> 1 no tiene divisores primos en común es decir, si m, n son primos entre sí, entonces $C_m \times C_n \cong C_{mn}$.

(Sugerencia: (a) Sea $a \in C_m$ un generador. El mapeo $f = f_{m,a} : C_m \to \mathbb{Z}/m\mathbb{Z}$ que satisface $f(a) = 1$ se extiende a un único homomorfismo entre estos grupos. Demostrar que esto es un isomorfismo. (b) Primero, demostrar que $g(x + mn\mathbb{Z}) = (x + m\mathbb{Z}, x + n\mathbb{Z})$, para todo $x \in \mathbb{Z}$ define un homomorfismo $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. A continuación, suponiendo que m, n son primos entre sí, mostrar que esta función g es inyectiva. Concluir, puesto que el dominio y el rango de g ambos tienen la misma cardinalidad, tal que g es también una función sobreyectiva. Por último, utilizando la parte (a) mostrar que $C_m \times C_n \cong C_{mn}$.)

6.2 Acciones en un grupo

Necesitamos estudiar las acciones, cuya discusión se inició en el capítulo 3, en más detalle.

Lema 6.2.1. Sea G un grupo y X un conjunto finito. Si G actúa sobre X (sobre la izquierda, respectivamente, sobre la derecha), entonces hay un homomorfismo $G \to S_X$ dado por $g \to \phi_g$. Recíprocamente, si $\phi : G \to S_X$ es un homomorfismo entonces $\phi(g) : X \to X$ define una acción (a la izquierda, respectivamente, a la derecha) de G en X.

Esto es una consecuencia inmediata de la definición de una acción.

Ejemplo 6.2.1. Sea G el grupo Cubo de Rubik generado por los movimientos básicos R, L, U, D, F, B. Para cada movimiento $g \in G$, sea

- $\rho(g)$ es la permutación correspondiente del conjunto de vértices V del cubo, y
- $\sigma(g)$ sea la permutación correspondiente del conjunto de aristas E del cubo.

Entonces es posible mostrar que

(a) $\rho : G \to S_V$ es un homomorfismo,
(b) $\sigma : G \to S_E$ es un homomorfismo.

Para comprobar esto, el primer teorema fundamental de la teoría del cubo en 6.6.1 es útil.

Sea G actúa sobre un conjunto X, denotado por $\phi(g) : X \to X$ para $g \in G$. Esta acción también da lugar a una acción en $X \times X$: $\phi_{2,g} : X \times X \to X \times X$ para $g \in G$, donde $\phi_{2,g}(x_1, x_2) =$

$\left(\phi_g(x_1), \phi_g(x_2)\right)$, para cada $(x_1, x_2) \in X \times X$. Cuando G actúa transitivamente sobre X (ver Definición 3.9.3 anterior), es bastante notable.
A veces, G incluso opera transitivamente sobre $X \times X - \Delta$ ($\Delta = \{(x, x) \mid x \in X\}$ la 'diagonal'), una circunstancia mucho más especial (en este caso, la acción es llamada **doblemente transitiva**). La siguiente definición generaliza esta idea.

Definición 6.2.1. Sea un grupo G actúa sobre un conjunto X. Llamamos a la acción ***k*-tupla transitiva** si para cada par de orden k -tuplas $(x_1, x_2, \dots, x_k)$, $(y_1, y_2, \dots, y_k)$ de distintos elementos que pertenecen a X (puesto que $x_i \neq x_j$ y $y_i \neq y_j$), hay un $g \in G$ tal que $y_i = \phi_g(x_i)$, para cada i con $1 \leq i \leq k$.

Si $k = 2$, entonces '2-tupla transitiva' es lo mismo que 'doblemente transitiva'.

Teorema 6.2.1. Si $k > 5$ y G es un grupo de permutación actuando k-transitivamente en un conjunto finito X (por lo que G es un subgrupo de S_X), entonces G es isomorfo a S_m o a A_n, para algún $m \geq k$ o algún $n \geq k + 2$.
Recíprocamente, S_n actúa n -transitivamente sobre $\{1, 2, \dots, n\}$ y A_n actúa $(n-2)$ -transitivamente sobre $\{1, 2, \dots, n\}$.
Esto se demuestra en [DiMo], Teorema 7.6A.

Observación 6.2.1. Debemos, junto con nuestra determinación teórica del grupo Cubo de Rubik demostrado más tarde, ser capaces de deducir del Teorema 6.2.1 el siguiente resultado.

Corolario 6.2.1.

(a) Supongamos que $c_1, \dots, c_6$ son cualesquiera 6 distintos subcubos esquina del Cubo de Rubik. Sean $c'_1, \dots, c'_6$ cualesquiera otros 6 distintos subcubos esquina. Hay un elemento del grupo G Cubo de Rubik que fija todos los subcubos arista y envía c_i a c'_i, para todo $i = 1, \dots, 6$. En términos generales, podemos expresar esto diciendo G actúa 6-transitivamente sobre las esquinas, fijando las aristas.

(b) Supongamos que $c_1, \dots, c_8$ son cualesquiera 8 distintos subcubos esquina del Cubo de Rubik. Sean $c'_1, \dots, c'_8$ cualesquiera otros 8 distintos subcubos esquina. Hay un elemento del grupo G Cubo de Rubik que envía c_i a c'_i, para todo $i = 1, \dots, 8$ (y no puede fijar todos los subcubos arista). En términos generales, podemos expresar esto diciendo G actúa 8-transitivamente sobre las esquinas (permitiendo que las aristas se muevan).

(c) G actúa 10-transitivamente sobre las aristas, fijando las esquinas.

(d) G actúa 12-transitivamente sobre las aristas pero pueden permutar las esquinas.

6.3 Cuando dos grupos son realmente el mismo

Esta sección trata sobre isomorfismos de grupo.

Ejemplo 6.3.1. Sea H el subgrupo del grupo Cubo de Rubik generado por el movimiento básico $R : H = \langle R \rangle$. Entonces $H \cong C_4$ (donde C_4 denota el grupo cíclico de orden 4).

Ejemplo 6.3.2. Recordemos que a cada permutación g del conjunto $\{1, 2, \dots, n\}$ podemos asociarle una matriz permutación $P(g)$ de tal manera que

$$P(g)\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{g(1)} \\ x_{g(2)} \\ \vdots \\ x_{g(n)} \end{pmatrix}.$$

(Aquí la imagen de i bajo la permutación g se denota $g(i)$, aunque en realidad i se conecta en g desde la izquierda.) Sea P_n el conjunto de todas las matrices $n \times n$ de permutación. Este es un grupo bajo la multiplicación de matrices. La función

$$\begin{gathered} P : S_n \to P_n, \\ g \to P(g) \end{gathered}$$

es un isomorfismo. Esta es una biyección y un homomorfismo, por la discusión dada anteriormente en el capítulo 1 sobre permutaciones (ver Lema 1.2.2 y el Teorema 1.2.1).

Ejemplo 6.3.3. En este ejemplo, consideramos que los grupos de simetría completa (en $O(3, \mathbb{R})$ de varios sólidos y figuras planas, las simetrías que se consideren como transformaciones 3-dimensionales.

A partir de [NST], Tabla 15.7, tenemos la siguiente tabla de isomorfismos:

Nombre	***Notación***	***Isomorfo a***
grupo de simetría del tetraedro	T	S_4
grupo de rotación del tetraedro	ST	A_4
grupo de simetría del octaedro	O	$S_4 \times C_2$
grupo de rotación del octaedro	SO	S_4
grupo de simetría del icosaedro	I	$A_5 \times C_2$
grupo de rotación del icosaedro	SI	A_5
grupo de simetría del $n-$ agon regular		D_{2n}, n impar $D_n \times C_2$, n par
grupo de rotación del $n-$ agon regular		D_n

Tabla 6.2

Ejemplo 6.3.4. Este ejemplo se puede encontrar en [B1].
Sea Q el grupo de cuaterniones,

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

donde $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$, como en 3.1. Entonces Q es isomorfo al grupo $Q^* = \langle a, b\rangle \subset G$, donde G es el grupo Cubo de Rubik y

$$\begin{gathered} a = F^2 \cdot M_R \cdot U^{-1} \cdot M_R^{-1} \cdot U^{-1} \cdot M_R \cdot U \cdot M_R^{-1} \cdot U \cdot F^2, \\ b = F \cdot U^2 \cdot F^{-1} \cdot U^{-1} \cdot L^{-1} \cdot B^{-1} \cdot U^2 \cdot B \cdot U \cdot L, \end{gathered}$$

a través del mapeo $f : Q^* \to Q$ definido por $\phi(a) = i,\ \phi(b) = k$.
Una prueba de esta afirmación se discutirá en un capítulo posterior.

Lema 6.3.1. Como anteriormente, sea $(G,\ \cdot)$ un grupo y h un elemento fijo de G.
Definimos $c_h : G \to G$ por

$$c_h(g) = h \cdot g \cdot h^{-1}, \qquad g \in G$$

Este es un automorfismo.

Prueba: Para comprobar esto, debemos demostrar que $f = c_h$ es un homomorfismo inyectivo y sobreyectivo (quitamos el subíndice para simplificar la notación).
Primero, demostremos que f es inyectiva. Supongamos que $f(g_1) = f(g_2)$. Entonces $f(g_1 \cdot g_2^{-1}) = 1$, por lo que $h \cdot g_1 \cdot g_2^{-1} \cdot h^{-1} = 1$. Multiplicamos ambos lados de esta ecuación a la derecha por h y a la izquierda por h^{-1}. Obtenemos $g_1 \cdot g_2^{-1} = 1$. Esto implica $g_1 = g_2$, por lo que f es inyectiva.
Ahora mostraremos que f es sobreyectiva. Sea x un elemento arbitrario pero fijo de G.
Sea $y = h^{-1} \cdot x \cdot h$. Entonces

$$f(y) = f(h^{-1} \cdot x \cdot h) = h \cdot h^{-1} \cdot x \cdot h \cdot h^{-1} = x.$$

Por lo tanto, f es sobreyectiva.
Se verificó previamente que f es un homomorfismo.

Definición 6.3.1. Un automorfismo como en el Lema 6.3.1 es llamado **interior**. Un automorfismo de G que no es de esta forma, para algún $h \in G$, es llamado **exterior**.

Los conceptos de automorfismos interior y exterior fueron introducidos por Otto Hölder (1859-1937). Hölder también clasifico todos los grupos finitos simples, hasta el isomorfismo, de orden ≤ 200. (La definición de 'simple' se da en la Definición 6.5.1 a continuación.) La clasificación de todos los grupos finitos simples sólo recientemente ha sido terminada y se dice que requieren más de 3000 páginas para los detalles.

Notación: El conjunto de todos los automorfismos de un grupo G se denota $Aut(G)$.
El subconjunto de automorfismos interiores se denota

$$Inn(G) := \{f \in Aut(G) \mid f = c_h, \text{algún } h \in G\},$$

en la notación del Lema 6.3.1.

6.3.1 Conjugación en S_n

En la primera parte de la década de 1900, un brillante matemático hindú, Srinivasa Ramanujan (1887-1920), yacía en el hospital en Inglaterra muy enfermo. El Gran matemático británico, G. H. Hardy (1877-1947), lo visitó y le comentó que él tomó el número de un taxi 1729, un 'número aburrido'. 'Por el contrario,' Ramanujan argumentó, 'es un número muy interesante, siendo el menor entero que es la suma de dos cubos en dos maneras diferentes.' Uno de los más interesantes y originales matemáticos de todos los tiempos, Ramanujan trabajó (a menudo en colaboración con Hardy) en las funciones elípticas, fracciones continuas y series infinitas [MT]. Él sabía un asombroso número de curiosidades sobre números enteros, como el presente.
¿Qué tiene que ver Ramanujan con la conjugación?

Nos encontraremos con un criterio simple para determinar cuando dos permutaciones (en S_n) son conjugadas (en S_n).

Lema 6.3.2. Supongamos que $f : S_n \to S_n$ es un automorfismo interior. Si $g \in S_n$ es un producto disjunto de ciclos de longitud $k_1, \dots, k_r$ entonces $f(g)$ es un producto disjunto de ciclos de longitud $k_1, \dots, k_r$.

En otras palabras, un automorfismo interior (es decir, conjugación) 'debe preservar la estructura de ciclo'.

Demostración: Puesto que f es interior, sea la conjugación por algún elemento $h \in S_n$, por decir $f(g) = h^{-1}gh$, para todo $g \in S_n$. Sea $(i)g \in \{1, \dots, n\}$ la imagen de $i \in \{1, \dots, n\}$ bajo $g \in S_n$. El lema es una consecuencia del siguiente cálculo simple: si $(i)g = j$ entonces, para todo i con $1 \leq i \leq n$, tenemos

$$\big((i)h\big)(h^{-1}gh) = (j)h. \qquad (6.1)$$

En otras palabras, si g envía $i \mapsto j$ entonces $h^{-1}gh$ envía $(i)h \mapsto (j)h$. Resulta que g y $h^{-1}gh$ tienen la estructura de ciclo.

Teorema 6.3.1. Dos elementos $g, g' \in S_n$ son conjugados si y sólo si tienen la misma estructura de ciclo.

Demostración: El lema demuestra la dirección 'sólo si' de esta equivalencia. Supongamos que $g, g' \in S_n$ tienen la misma estructura de ciclo. Escribamos sus descomposiciones de ciclo disjuntas utilizando el orden lexicográfico (orden de diccionario) impuesto sobre las longitudes de los ciclos que ocurren en la descomposición: decimos

$$g = (i_1, \dots, i_{n1})(i_1, \dots, i_{n2}) \dots (i_1, \dots, i_{nk}),$$
$$g' = (i'_1, \dots, i'_{n1})(i'_1, \dots, i'_{n2}) \dots (i'_1, \dots, i'_{nk}),$$

donde $1 \leq n_1 \leq \dots \leq n_k \leq n$ y $n = n_1 + \dots + n_r$. Elegir un $h \in S_n$ tal que $h : i_j \mapsto i'_j$, para todo j con $1 \leq j \leq n$. Entonces $g' = h^{-1}gh$, por (6.1).
Una **partición** de n es un r-tupla, $(n_1, \dots, n_r)$ de enteros positivos tal que $1 \leq n_1 \leq \dots \leq n_r \leq n$ y $n = n_1 + \dots + n_r$. De los resultados anteriores, se sigue que cada clase de conjugación de S_n corresponde a una y solo una partición de n. En particular, el número de clases de conjugación de S_n es igual al número $p(n)$ de particiones distintas de n. Una fórmula asintótica para este número fue encontrado por Srinivasa Ramanujan. Su fórmula es demasiado complicada para este trabajo, pero un caso especial de esta bella fórmula es la siguiente:

$$\lim_{n\to\infty} \frac{\log p(n)}{\sqrt{n}} = \pi\sqrt{\frac{2}{3}}.$$

6.3.2 ... Y una guarnición de automorfismos, por favor

A pesar de que no lo necesitamos aquí, el siguiente hecho es interesante, ya que ilustra que el grupo simétrico S_6 desempeña un rol único en la familia de todos los grupos simétricos.
Teorema 6.3.2. Si $n \neq 2, 6$ entonces el homomorfismo $\phi : S_n \to Aut(S_n)$ definido por $\phi(g) = c_g$ (donde c es como en el **Lema 6.3.1** anterior) es un isomorfismo:

$$S_n \cong Aut(S_n).$$

Si $n = 6$, entonces $|Aut(S_6)| = 2 \cdot |S_6|$.
El ejemplo siguiente continúa la discusión de 5.6.

Ejemplo 6.3.5. Cualquier permutación de las 6 diagonales del icosaedro, que puede ser considerado como un elemento de S_6 , da lugar a una permutación del conjunto de 6 pentadas, que también puede ser considerada como un elemento de S_6 . Esto da un mapeo

$$f : S_6 \to S_6,$$

que es de hecho un homomorfismo. Este homomorfismo es inyectivo por lo que en realidad es un automorfismo.
Sin embargo, un 2-ciclo en el conjunto de 6 diagonales (es decir, intercambiando exactamente 2 diagonales) no induce un 2-ciclo en el conjunto de estas 6 pentadas. De hecho, un 2-ciclo en el conjunto de diagonales da lugar a un producto de tres 2-ciclos disjuntos en el conjunto de estas 6 pentadas. Por lo tanto, por el teorema anterior (que dice que un automorfismo interior debe preservar la estructura de ciclo), este automorfismo f no puede ser un automorfismo interior.

6.4 Kernels son normales, algunos subgrupos no

Sea $f : G_1 \to G_2$ un homomorfismo entre dos grupos. Sea $ker(f) = \{g \in G_1 \mid f(g) = e_2\}$,

donde e_2 es el elemento identidad de G_2. Este conjunto es llamado el **kernel** de f.

Lema 6.4.1. $ker(f)$ es un subgrupo de G_1.

Ejemplo 6.4.1. Sea $sgn : S_n \to \{\pm 1\}$ el homomorfismo que se asocia con una permutación ya sea 1, si es par, o -1, si es impar. Entonces $A_n = ker(sgn) \subset S_n$.

Las siguientes propiedades del kernel son útiles.

Lema 6.4.2. Sea $f : G_1 \to G_2$ un homomorfismo entre dos grupos.

(a) El homomorfismo f es inyectivo si y sólo si $ker(f) = \{e_1\}$.
(b) Si g pertenece al kernel y x es cualquier elemento de G_1, entonces $x^{-1} \cdot g \cdot x$ también debe pertenecer al kernel.

Prueba:

(a) Que f es inyectiva si y sólo si $f(g_1) = f(g_2)$ implica $g_1 = g_2$ $(g_1, g_2 \in G_1)$. Notemos que $f(g_1) = f(g_2)$ es verdad si y sólo si $f(g_1 \cdot g_2^{-1}) = e_2$. Si $ker(f) = \{e_1\}$ entonces $f(g_1 \cdot g_2^{-1}) = e_2$ implica $g_1 \cdot g_2^{-1} = e_2$, lo que implica que $g_1 = g_2$, lo que implica que f es inyectiva.
Por lo tanto, si $ker(f) = \{e_2\}$ entonces f es inyectiva. Recíprocamente, si f es inyectiva entonces $f(x) = f(e_1) = e_2$ implica $x = e_1$ ($x \in G_1$). Esto implica $ker(f) = \{e_1\}$.

(b) Multiplicar ambos lados de $e_2 = f(g)$ a la izquierda por $f(x)^{-1}$ y a la derecha por $f(x)$. Obtenemos

$$e_2 = f(x)^{-1} \cdot e_2 \cdot f(x) = f(x^{-1}) \cdot f(g) \cdot f(x) = f(x^{-1} \cdot g \cdot x),$$

como se deseaba.

Definición 6.4.1. Sea H un subgrupo de G. Decimos que H es un subgrupo **normal** si, para cada $g \in G$, $g^{-1} \cdot H \cdot g = H$ (es decir, para cada $g \in G$ y cada $h \in H$, $g^{-1} \cdot h \cdot g$ pertenece a H).

Notación: A veces denotamos 'H es un subgrupo normal de G' por $H \lhd G$

6.4.1 Ejemplos de subgrupos no-normales

Hemos visto anteriormente que los ejemplos de subgrupos normales son fáciles de construir. Por ejemplo, el kernel de cualquier homomorfismo $f : G \to H$ es un subgrupo normal de G. Por ejemplo, el kernel del homomorfismo sgn es normal: $A_n \lhd S_n$ (véase el Ejemplo 6.4.1).
Más generalmente, si G es cualquier grupo entonces el subgrupo conmutador, G', es un subgrupo normal de G. (El subgrupo conmutador de S_n es A_n.)
¿Qué pasa con los subgrupos no normales? Ejemplos de subgrupos que no son normales, son fáciles de conseguir.

Ejemplo 6.4.2.

(a) Si $n > 5$ y H es cualquier subgrupo propio no trivial de A_n (por ejemplo, cualquier subgrupo cíclico no-trivial), entonces H no es normal en A_n (véase el Teorema 6.4.1 más adelante).
(b) Todo subgrupo de S_6 de orden 2 es no normal.

Esto nos dice los siguientes hechos.

1. Cualquier subgrupo de S_5 distinto de sí mismo, A_5 y el grupo trivial, no es normal.
2. Cualquier subgrupo de D_5 distinto de sí mismo, $C_5 = \langle (1,2,3,4,5) \rangle$, y el grupo trivial, no es normal.

Lema 6.4.3. Si $f : G_1 \to G_2$ es un homomorfismo entre dos grupos entonces $ker(f)$ es un subgrupo normal de G_1.

6.4.2 El grupo alternante

El siguiente resultado notable sobre el grupo alternante no será necesario para comprender la estructura del Cubo de Rubik. Sin embargo, el teorema siguiente es interesante por su relación con el hecho de (debido a Ruffini y Abel), que no podemos resolver el polinomio general de grado 5 o mayor usando radicales, es decir, que no existe el análogo a la fórmula cuadrática para polinomios de grado 5 o mayor. Al explicar esta conexión, por desgracia, nos llevaría demasiado lejos de nuestro tema principal.

Teorema 6.4.1. Si X tiene 5 elementos o más, entonces A_X no tiene subgrupos normales propios no triviales. En otras palabras, si $H \lhd A_X$ es un subgrupo normal, entonces $H = \{1\}$ o bien $H = A_X$.

Esto no será demostrado aquí. (Para una demostración, véase, por ejemplo, [R] o [Ar], capítulo 14.)
Sin embargo, el siguiente hecho acerca del grupo alternante será necesario más adelante en nuestra determinación de la estructura del grupo Cubo de Rubik. Este hecho también se planteó en relación con nuestra discusión de las 'posiciones legales' del Puzzle 15 en el capítulo 2 (véase 2.1).

Proposición 6.4.1. Sea H el subgrupo de S_n generado por todos los 3-ciclos en S_n, entonces $H = A_n$.

Demostración: Puesto que $sgn : S_n \to \{\pm 1\}$ es un homomorfismo, y dado que cualquier 3-ciclo es par, cualquier producto de 3-ciclos también debe ser par. Por lo tanto, $H \subset A_n$. Si $g \in A_n$ entonces g debe intercambiar un número par de las desigualdades $1 < 2 < \ldots < n - 1 < n$, por la Definición 1.1.1. Por lo tanto (ya que cualquier permutación puede escribirse como un producto de 2 ciclos, Teorema 1.4.1), g debe componerse de permutaciones de la forma $(i,j)(k,l)$ o $(i,j)(j,k)$. Pero $(i,j)(k,l) = (i,j,k)(j,k,l)$ y $(i,j)(j,k) = (i,j,k)$. Por lo tanto, $g \in H$. Esto implica $A_n \subset H$, por lo que $A_n = H$.
El siguiente resultado es muy útil para los fines del análisis de puzzles de permutación.

Lema 6.4.4. ([W]) Sea X un conjunto finito, $|X| \geq 3$ y fijar u, v, como elementos en X. Entonces los 3 ciclos (u, v, x), cuando x corre sobre todos los elementos de $X - \{u, v\}$, generan A_X.

Este lema da una afirmación aún más fuerte que la afirmación anterior. Ahora, en lugar de que sea un único elemento fijo, hay dos elementos fijos y el grupo alternante se sigue generando.

6.5 Grupos cociente

Uno de los hechos más útiles acerca de los subgrupos normales es el siguiente resultado/ definición.

Lema 6.5.1. Si H es un subgrupo normal de G, entonces el espacio de clases laterales G/H con la operación binaria,

$$aH \cdot bH = (ab)H, \quad (aH)^{-1} = a^{-1}H,$$

para todo a, b pertenecientes a G, es un grupo. El elemento identidad de este grupo es la clase lateral trivial H.

Este grupo G/H es llamado el **grupo cociente** de G por H y es a veces pronunciado 'G mod H'. Los textos más antiguos pueden utilizar la terminología 'grupo factor' en lugar de. Esta noción, para un grupo abstracto, se introdujo por primera vez por Otto Hölder. En un principio comenzó preparándose para llegar a ser un ingeniero. Hölder hizo importantes contribuciones no sólo a la teoría de grupos, sino también a las series de Fourier.

Recordar de 6.4.1 que el subgrupo conmutador es normal. Un ejemplo de un grupo cociente que surge de forma natural es llamado la **Abelianización** de G: el grupo cociente $G_{ab} = G/G'$, donde $G' = [G, G]$ denota el subgrupo conmutador.

Ejemplo 6.5.1. Si $f : G_1 \to G_2$ es un homomorfismo entre dos grupos, entonces $G_1/ker(f)$ es un grupo cociente.

A continuación introducimos una primera idea importante enfatizada primero por E. Galois. Aunque Galois asistió a la escuela secundaria, tuvo problemas para entrar en el sistema universitario francés. Lamentablemente, en el momento en que entró al École Normale Supérieure en Noviembre de 1829, él también comenzó a quedar atrapado en las actividades de la Revolución Francesa de 1830 que derrocó a Carlos X. Sus actividades políticas dieron lugar a su expulsión de la escuela en Diciembre de 1830. Aunque al parecer había sido un adolescente rebelde, esto sólo le frustraba aún más. Él murió en una pelea con otro Francés.

El primer trabajo de Galois fue empezar a iluminar los bloques básicos de construcción de la colección de grupos finitos (es decir, el análogo de la idea de que los átomos son los bloques básicos de construcción de moléculas). Galois introdujo las ideas de los grupos solubles y subgrupos normales, en el contexto de los grupos de permutación. En términos generales, se puede decir que la construcción de los bloques básicos de grupos finitos son aquellos grupos que no tienen subgrupos normales propios no triviales. Intuitivamente, esto es porque un grupo cociente no trivial (por un subgrupo normal) está estrechamente relacionado con el grupo original pero mucho menor en tamaño (y por tanto tal vez sujeto a análisis por un argumento inductivo de algún tipo). Los bloques básicos de construcción son llamados grupos 'simples'.

Definición 6.5.1. Un **grupo simple** es un grupo sin subgrupos normales propios además del subgrupo trivial {1}.

Ejemplo 6.5.2. Si p es un primo entonces C_p (el grupo cíclico de p elementos) es simple. De hecho, si G es cualquier grupo que es tanto abeliano y simple entonces hay un primo p tal que $G \cong C_p$. Si $n > 4$ entonces A_n es simple (como se ha establecido anteriormente en el Teorema 6.4.1). Estos hechos son demostrados en [R].

Los grupos simples no son muy abundantes. De hecho, el primer grupo simple no-abeliano es de orden 60 (que es A_5).
El siguiente resultado básico describe el grupo cociente $G_1/ker(f)$.

Teorema 6.5.1. (Primer teorema de isomorfismos) Si $f : G_1 \to G_2$ es un homomorfismo entre dos grupos, entonces $G_1/ker(f)$es isomorfo a $f(G_1)$.

Prueba: $ker(f)$ es un subgrupo normal de G_1, por lo que $G_1/ker(f)$es un grupo. Debemos demostrar que este grupo es isomorfo al grupo $f(G_1)$. Definimos $\phi : G_1/ker(f) \to f(G_2)$ por $\phi\big(g \cdot ker(f)\big) = f(g)$, para $g \in G_1$. Debemos demostrar

(a) ϕ está bien definida,
(b) ϕ es un homomorfismo,
(c) ϕ es una biyección.

Si $g \cdot ker(f) = g' \cdot ker(f)$, entonces $g^{-1}g' \in ker(f)$, ya que $ker(f)$ es un grupo. Esto implica que $f(g^{-1}g') \in f\big(ker(f)\big) = \{1\}$, por lo que $f(g) = f(g')$. Esto implica φ está bien definida.
Dado que $ker(f)$ es normal, $\big(g \cdot ker(f)\big)\big(g' \cdot ker(f)\big) = gg'(g'^{-1} \cdot ker(f)g')ker(f) = gg' \cdot ker(f)$. Por lo tanto $\phi\left(\big(g \cdot ker(f)\big)\big(g' \cdot ker(f)\big)\right) = \phi\big(gg' \cdot ker(f)\big) = f(gg') = f(g)f(g') = \phi\big(g \cdot ker(f)\big)\phi\big(g' \cdot ker(f)\big)$, para todo $g, g' \in G$. Esto implica que ϕ es un homomorfismo.
Es claro que ϕ es sobreyectiva. Para demostrar que ϕ es una biyección, basta probar que ϕ es inyectiva. Supongamos que $\phi\big(g \cdot ker(f)\big) = \phi\big(g' \cdot ker(f)\big)$, para algunos $g, g' \in G$. Entonces

$f(g) = f(g')$, por lo que $f(g^{-1}g') = 1$. Por definición del kernel, esto implica que $g^{-1}g' \in ker(f)$, por lo que $g \cdot ker(f) = g' \cdot ker(f)$. Esto implica que ϕ es inyectiva.

Los otros teoremas de isomorfismo no serán necesarios pero los establecemos para ayudar a ilustrar la utilidad de la noción de normalidad.

Teorema 6.5.2. (Segundo Teorema de isomorfismos) Si H, N son subgrupos de un grupo G y si N es normal, entonces

(a) $H \cap N$ es normal en H,
(b) existe un isomorfismo

$$H/(H \cap N) \cong NH/N.$$

Teorema 6.5.3. (Tercer Teorema de isomorfismos) Si N_1, N_2 son subgrupos de un grupo G, si $N_1 \subset N_2$, y si N_1 y N_2 son normales entonces

(a) N_2/N_1 es normal en G/N_1,
(b) existe un isomorfismo

$$(G/N_1)/(N_2/N_1) \cong G/N_2.$$

No vamos a probar estos resultados aquí, ver [G] o [R]. Estos se deben a Emmy Noether (1882-1935), una de las primeras mujeres en obtener un doctorado en matemáticas en Alemania. A pesar de su gran talento, el hecho de que fuera judía y mujer hizo su progreso en matemáticas difícil. D. Hilbert y F. Klein, dos de los matemáticos más importantes del mundo en ese momento, la apoyaron y ella llevó a cabo la investigación y la docencia en la Universidad de Göttingen hasta que los nazis llegaron al poder en la década de 1930. Ella se fue para el Bryn Mawr College en los E.U pero murió unos años más tarde. Ella hizo muchas contribuciones muy importantes al álgebra moderna.

6.6 Incursionando en productos directos

Dados dos enteros n_1 y n_2, siempre podemos formar otro a partir ellos, usando multiplicación, denotado $n_1 n_2$. Análogamente, dados dos grupos H_1 y H_2, siempre podemos formar otro grupo a partir de ellos usando la construcción del producto cartesiano, que se denota $H_1 \times H_2$.

Definición 6.6.1. Sean H_1, H_2 dos subgrupos. Decimos que un grupo G es el **producto directo** de H_1 con H_2, se escribe $G = H_1 \times H_2$, si

(a) $G = H_1 \times H_2$ (producto cartesiano, como conjuntos),
(b) la operación de grupo en G está dada 'coordenada a coordenada' (denotaremos ' $\cdot$ ' por simplicidad):

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2),$$

para $x_1, x_2 \in H_1,\ y_1, y_2 \in H_2$ (donde $\cdot$ denota multiplicación en H_1, H_2, y G).

Ejemplo 6.6.1. Sea G (como un conjunto) el producto cartesiano $G = C_2 \times C_3$, donde C_n denota el grupo cíclico de orden n (con adición $mod\ n$ como la operación, $n = 2, 3$). Definimos adición en G coordenada a coordenada ($mod\ 2$ en la primera coordenada, $mod\ 3$ en la segunda coordenada):

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2),$$

donde $0 \leq m_i \leq 1,\ 0 \leq n_j \leq 2,$ para $i = 1, 2, j = 1, 2.$

Ejemplo 6.6.2. El grupo simétrico O del octaedro es isomorfo a $S_4 \times C_2$. El grupo simétrico I del icosaedro es isomorfo a $A_5 \times C_2$. (Este no es isomorfo a S_5, a pesar del hecho de que ambos tienen el mismo número de elementos y que ambos contienen a A_5 como un subgrupo normal.)

6.6.1 Primer teorema fundamental de la teoría del cubo

El siguiente hecho básico se utiliza implícitamente en algunos de los ejemplos que siguen.
Con frecuencia se necesita el siguiente hecho.

Teorema 6.6.1. Comenzando con un cubo resuelto, etiquetemos las siguientes caras con un '+' invisible (es decir, marcar la posición espacial de la cara en el cubo con un '+'):

- Cara U del subcubo arista uf.
- Cara U del subcubo arista ur.
- Cara F del subcubo arista fr.

Entonces todas las caritas pueden obtenerse a partir de estos por un movimiento del grupo slice.

Etiquetemos las caras U y D de cada subcubo esquina con un '+' invisible. Estos signos '+' son llamados las **marcas de referencia estándar**. Cada movimiento g del Cubo de Rubik produce una nueva colección de etiquetas '+', llamadas las **marcas en relación a g**. Una posición de Cubo de Rubik está determinada por el siguiente proceso de decisión:

(a) ¿Cómo están permutados los subcubos arista?
(b) ¿Cómo están permutados los subcubos centro?
(c) ¿Cómo están permutados los subcubos esquina?
(d) ¿Cuál de las marcas relativas arista están volteadas (relativa a las marcas de referencia estándar)?
(e) ¿Cuál de las marcas relativas esquina son rotadas desde las marcas de referencia estándar y, en caso afirmativo, por cuánto son rotadas ($2\pi/3$ o $4\pi/3$ radianes en sentido horario, relativa a las marcas de referencia estándar)?

Esto es etiquetado como un teorema, debido a su importancia relativa para nosotros, ¡no debido a su dificultad! Este es el **Primer Teorema Fundamental de la teoría del Cubo de Rubik.**

6.6.2 Ejemplo: giros y flips del cubo

Recordamos una notación:

- X es el conjunto de las 48 caritas del Cubo de Rubik que no son caritas centrales.
- V denota el subconjunto de las caritas que pertenecen a algún subcubo esquina.
- E es el subconjunto de las caritas que pertenecen a algún subcubo arista.
- Sea G el grupo Cubo de Rubik.
- Sea F el grupo generado por todos los movimientos del grupo Cubo de Rubik que no permutan cualesquiera subcubos esquina o arista pero puede girarlos o voltearlos.

- Sean S_X, S_V, S_E, los grupos simétricos de X, V, E, respectivamente. Podemos considerar a F, G, como subgrupos de S_X. También podemos considerar a S_V, S_E como subgrupos de S_X (por ejemplo, S_V es el subgrupo de S_X que deja todos los elementos de E fijos).
- Sea
$$G_V = S_V \cap G, \qquad G_E = S_E \cap G, \qquad F_V = S_V \cap F, \qquad F_E = S_E \cap F.$$

Notar que la acción de G sobre X induce una relación de equivalencia como sigue: decimos que una cara f_1 es **equivalente** a una cara f_2 si hay un movimiento del Cubo de Rubik que envía una cara a la otra. Hay exactamente dos clases de equivalencia, o órbitas, de G en X: a saber, V y E. En particular, la acción de G en V es transitiva y la acción de G en E es transitiva. Por otro lado, F deja a cada vértice (respectivamente, arista) fijo, aunque puede permutar la cara esquina (respectivamente, cara arista) asociados a un vértice (respectivamente, arista).

6.6.3 Ejemplo: el grupo slice del cubo

Vale la pena estudiar un subgrupo del grupo Cubo de Rubik que es más fácil de analizar que el grupo Cubo de Rubik en sí mismo. Parte del siguiente material también se puede encontrar en [BH], [Si].

Sea H el grupo $\langle M_R, M_F, M_U \rangle$ generado por los movimientos de los cortes medios. Este grupo es llamado el 'grupo slice'. Sea E el conjunto de aristas del cubo (que identificamos con el conjunto de subcubos arista), sea C el conjunto de caras centrales del cubo, y sea $X = E \cup C$. Note que H actúa sobre X y que H no mueve los elementos de C (es decir, los vértices esquina del cubo).

Problema 6.6.1.

(a) ¿Es la acción de H sobre X transitiva?
(b) ¿Es la acción de H sobre C transitiva?
(c) ¿Es la acción de H sobre E transitiva?

Solución: La respuesta para (a) es no, por ejemplo, un subcubo arista no se puede enviar a una cara centro. En consecuencia, hay elementos de X que no pueden ser enviados a cada uno por un elemento de H. La respuesta para (b) es sí; cualquier cara centro puede ser enviada a cualquier otra cara centro por un elemento de H. La respuesta para (c) es no, por ejemplo, el subcubo arista uf no puede ser enviado al subcubo arista ur por un movimiento slice, por lo que hay un elemento de E que no se puede enviar a cualquier otro elemento de E por un elemento de H. Esto completa la solución.
La respuesta de 'no' a (c) lleva a la siguiente pregunta.

Problema 6.6.2. ¿Cuáles son las órbitas de H sobre E?

Solución: La respuesta se puede expresar de varias maneras, supongamos que llamamos a dos subcubos arista **equivalentes** si uno puede ser enviado al otro por un movimiento slice (es decir, un elemento de H). Hay 3 clases de equivalencia disjuntas: todos los subcubos del corte medio RL (el corte entre las caras R y L) son equivalentes, todos los subcubos del corte medio FB (el corte entre las caras F y B) son equivalentes, y todos los subcubos del corte medio UD (el corte entre las caras U y D) son equivalentes. Las órbitas distintas de H que actúan sobre E son las siguientes:

- el corte medio RL (el corte entre las caras R y L), denotado por E_{RL},
- el corte medio FB(el corte entre las caras F y B), denotado por E_{FB},
- el corte medio UD (el corte entre las caras U y D) , denotado por E_{UD}.

Notar que $E = E_{RL} \cup E_{FB} \cup E_{UD}$, es una partición de E en las distintas clases de equivalencia definidas por la acción de H sobre E. Esto completa la solución.
Cada elemento de H determina un elemento en S_X. Tenemos un homomorfismo

$$f : H \to S_X.$$

Esta es otra manera de decir que H actúa sobre el conjunto X, que ya sabemos.
Notar que cada movimiento slice básico M (de este modo M es M_R, M_F o M_U) es, como un elemento de S_X, de la siguiente forma:

$$M = (4 - ciclo\ en\ S_E)(4 - ciclo\ en\ S_C)$$

Recíprocamente, ¿un elemento de S_X determina de forma única un elemento de H? En otras palabras, ¿es f inyectiva?

Para responder a esto, fijemos un $h \in H$ y pensemos en lo que $f(h)$ nos dice: $f(h)$ nos dice que un subcubo se mueve a otro subcubo, pero no nos dice, por ejemplo, cómo un subcubo se voltea o gira.
El primer teorema fundamental del cubo (Teorema 6.6.1.) inspira la siguiente pregunta.

Problema 6.6.3. ¿Puede un elemento de H voltear (invertir los colores de un subcubo arista), pero no permutar, un subcubo arista (y, posiblemente, permutar o voltear otros subcubos del cubo)?

Solución: La respuesta es no. La razón es que los movimientos slice sólo pueden rotar un subcubo arista dado dentro del segmento slice al que pertenece. Esto completa la solución.
De ello se deduce, por tanto, que las permutaciones de los subcubos arista y centrales determinan un único elemento del grupo slice. En otras palabras, hemos demostrado lo siguiente

Proposición 6.6.1. El homomorfismo $f : H \to S_X$ es inyectivo.

Problema 6.6.4. ¡El análogo de esto para el grupo Cubo de Rubik es falso! ¿Por qué?

H actúa sobre el conjunto E_{RL}, así que tenemos un homomorfismo

$$r_{RL} : H \to S_{E_{RL}}$$

y de manera similar, $r_{UD} : H \to S_{E_{UD}}$ $r_{FB} : H \to S_{E_{FB}}$.
H actúa sobre cada uno de los conjuntos E y C, así que tenemos homomorfismos

$$r = r_{RL} \times r_{UD} \times r_{FB} : H \to S_{E_{RL}} \times S_{E_{UD}} \times S_{E_{FB}} \subset S_E,\ s : H \to S_C,$$

que podemos poner juntos para obtener un homomorfismo inyectivo

$$r \times s = H \to S_{E_{RL}} \times S_{E_{FB}} \times S_{E_{UD}} \times S_C \,.$$

Para determinar H, determinemos la imagen de H en $S_{E_{RL}} \times S_{E_{FB}} \times S_{E_{UD}} \times S_C$. Para hacer esto, primero miraremos la imagen de H en cada uno de $S_{E_{RL}}$, $S_{E_{FB}}$ y $S_{E_{UD}}$.
Esto es bastante fácil:

• la imagen de H en $S_{E_{RL}}$ es $\langle M_R \rangle \cong C_4$,
• la imagen de H en $S_{E_{FB}}$ es $\langle M_F \rangle \cong C_4$,
• la imagen de H en $S_{E_{UD}}$ es $\langle M_U \rangle \cong C_4$.

Más tarde, se quiere pensar en C_4 como $\{0, 1, 2, 3\}$, con adición mod 4, y la imagen de un elemento $h \in H$ bajo uno de los homomorfismos anteriores, $r_{RL} : H \to S_{E_{FB}}$, digamos, como un número entero $0 \leq r_{RL}(h) \leq 3$.
A continuación, debemos determinar la imagen de H en S_C. Esto es fácil si se mira en el camino correcto. En cuanto a los movimientos de las caras centro se refiere, los movimientos slice pueden ser sustituidos por sus rotaciones correspondientes de todo el cubo alrededor de un eje de simetría. En este caso, podemos ver que la imagen de H en S_C es la misma que la imagen del grupo simétrico ¡que preserva la orientación del cubo! Esto lo sabemos, por la discusión en el Ejemplo 6.3.3, anterior, es isomorfo a S_4.

Juntando todo, vemos que la imagen de H en $S_{E_{RL}} \times S_{E_{FB}} \times S_{E_{UD}} \times S_C$ es isomorfa a un subgrupo de $C_4^3 \times S_4$.

Podemos representar los elementos de H, por lo tanto, como 4-tuplas (h_1, h_2, h_3, h_4), con $h_1, h_2, h_3 \in C_4$ y $h_4 \in S_4$. Puesto que cada uno de los movimientos generadores de H (a saber, $M_R, M_U,$ y M_F) satisfacen

$$sgn\big(r(h)\big) = sgn\big(s(h)\big),$$

para todo $h \in H$, la imagen de H no puede ser todo $C_4^3 \times S_4$.

Proposición 6.6.2. La imagen de H en $C_4^3 \times S_4$ es isomorfa al kernel del mapeo

$$t : C_4^3 \times S_4 \to \{\pm 1\}$$
$$(h_1, h_2, h_3, h_4) \mapsto sgn(h_1) \cdot sgn(h_2) \cdot sgn(h_3) \cdot sgn(h_4),$$

donde cada sgn es el signo de la permutación, considerado como un elemento de S_X.

Problema 6.6.5. Demuestre que $|ker(t)| = (4^3 \cdot 4!)/2 = 768$.

Solución: Hemos demostrado que H es isomorfo a un subgrupo de $C_4^3 \times S_4$. De hecho, sabemos que los movimientos slice básicos M_R, M_U, M_F (que generan H) todos pertenecen al kernel de t, por lo que H es isomorfo a un subgrupo del $ker(t) \subset C_4^3 \times S_4$.
Queda por demostrar que cada elemento en el $ker(t)$pertenece a H. Para ello, consideramos el homomorfismo de proyección

$$p : H \to S_4$$

obtenido por composición de homomorfismos $r \times s : H \to C_4^3 \times S_4$ construido anteriormente con el homomorfismo de proyección $C_4^3 \times S_4 \to S_4$. Hemos demostrado que p es sobreyectiva.

Nuestro próximo objetivo es calcular el kernel de p y utilizar el primer teorema de isomorfismos para determinar H.
Afirmación: El kernel de p es

$$ker(p) = \{h \in H \mid s(h) = 1, r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2\}.$$

Nótese que $ker(p)$ es un subgrupo de H por lo que el signo de la permutación $s(h)$ es igual al signo de la permutación $r(h)$:

$$sgn\big(s(h)\big) = sgn\big(r(h)\big) = sgn\big(r_{RL}(h)\big) \cdot sgn\big(r_{UD}(h)\big) \cdot sgn\big(r_{FB}(h)\big).$$

Esto implica que $ker(p) \subset \{h \in H \mid s(h) = 1, r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2\}$.

Recíprocamente, elegimos un $h \in H$ tal que $s(h) = 1$ y $r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2$. Podemos representar este elemento h como una 4-tupla (n_1, n_2, n_3, s), con $0 \leq n_1, n_2, n_3 \leq 3$ y $s = 1 \in S_4$.
Por ejemplo,

- el elemento $M_1 = M_R \cdot M_F^{-1} \cdot M_D \cdot M_F$ es representado por la 4-tupla $(1, 1, 0, 1)$,
- el elemento $M_2 = M_R \cdot M_D \cdot M_F \cdot M_D^{-1}$ es representado por la 4-tupla $(0, 1, 1, 1)$,
- el elemento $M_3 = M_F \cdot M_D \cdot M_R^{-1} \cdot M_D^{-1} \cdot M_F \cdot M_D^{-1} \cdot M_R \cdot M_D$ es representado por la 4-tupla $(0, 0, 2, 1)$.

Estos elementos generan todos los elementos del grupo

$$\{(a, b, c, 1) \mid a, b, c \in C_4, a + b + c \equiv 0 \pmod 2\}$$

Nótese que el grupo

$$\{(a, b, c) \mid a, b, c \in C_4, a + b + c \equiv 0 \pmod 2\}$$

es decir, a su vez, el kernel del mapeo $C_4^3 \to C_2$ dado por $(a, b, c) \mapsto a + b + c \equiv 0 \pmod 2$.

Por lo tanto, el elemento h elegido anteriormente debe ser expresable como una 'palabra' en estos tres elementos M_1, M_2, M_3. Esto demuestra que

$$\{h \in H \mid s(h) = 1, r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2\} \subset ker(p),$$

lo que implica la afirmación.
Para resumir lo que tenemos hasta ahora: tenemos un homomorfismo sobreyectivo $p : H \to S_4$ con el kernel $\{h \in H \mid s(h) = 1, r_{RL}(h) + r_{UD}(h) + r_{FB}(h) \equiv 0 \pmod 2\}$. El kernel tiene $|ker(p)| = 32$ elementos y la imagen tiene $|im(p)| = |S_4| = 4! = 24$ elementos. Dado que, por el primer teorema de isomorfismos,

$$H/ker(p) \cong S_4\,,$$

tenemos que $|H| = 32 \cdot 24 = 768$. Pero el kernel del homomorfismo $t : C_4^3 \times S_4 \to \{\pm 1\}$, que sabemos que contiene H como un subgrupo, también tiene 768 elementos. Esto obliga a que $h = ker(t)$. Esto completa la solución.

6.7 Una mezcla heterogénea de productos semi-directos

Para 'construir de forma explícita' el grupo Cubo de Rubik, necesitamos saber cómo construir productos semi-directos. Estudiamos productos semi-directos en esta sección.
Un producto semi-directo es un tipo específico de construcción, más general que el producto directo, de un nuevo grupo, G, a partir de dos grupos, H_1 y H_2, con ciertas propiedades. Es a su vez que H_1 y H_2 serán subgrupos de G.
Si un grupo G contiene dos subgrupos H_1 y H_2, con $H_1 \lhd G$ normal, tal que cada elemento de G puede ser escrito de manera única como un producto h_1h_2, con $h_1 \in H_1$ y $h_2 \in H_2$ entonces decimos que G es el **producto semi-directo** de H_1 y H_2. En esta situación, H_2 es llamado un **complemento** de H_1. En esta sección, veremos otra manera de expresar un producto semi-directo. Más adelante, veremos que el grupo Cubo de Rubik puede ser descrito usando productos semi-directos.

Definición 6.7.1. Ahora supongamos que H_1, H_2 son ambos subgrupos de un grupo G. Decimos que G es el **producto semi-directo** de H_1 por H_2, y escribimos

$$G = H_1 \rtimes H_2$$

si

- $G = H_1 \cdot H_2$,
- H_1 y H_2 sólo tienen 1, la identidad de G, en común,
- H_1 es normal en G.

Esta es la 'versión interna' del producto semi-directo.

Por supuesto, si definimos cualquier cosa usando dos definiciones aparentemente diferentes, ¡sería mejor estar seguro de que son equivalentes! Este es el Teorema 7.23 en [R], que no demostraremos aquí.
Nótese que la regla de multiplicación en G no tiene que ser mencionada ya que estamos suponiendo aquí que G está dado.
La 'versión externa' está definida por una construcción como sigue:

Definición 6.7.2. Supongamos que tenemos un homomorfismo $\phi : H_2 \to Aut(H_1)$

Definimos la multiplicación sobre el conjunto $H_1 \times H_2$ por

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot \phi(y_1)(x_2),\ y_1 \cdot y_2\ ).$$

Esto define una operación de grupo. Este grupo, denotado por $H_1 \rtimes_\phi H_2$, es el **producto semi-directo** (externo).

Estas dos últimas definiciones son equivalentes por los Teoremas 7.22-7.23 en [R].
Como un conjunto, $H_1 \rtimes H_2$ es simplemente el producto cartesiano $H_1 \times H_2$.

Ejemplo 6.7.1. Sea $\mathbb{R}^2$ el producto directo del grupo aditivo de los números reales con sí mismo:

$$\mathbb{R}^2 = \{(x, y) \mid x, y \text{ reales}\}$$

la operación de grupo se realiza sumando componente a componente. Sea C_2 el grupo cíclico multiplicativo con 2 elementos, cuyos elementos escribimos como $C_2 = \{1, s\}$. (Podemos

pensar en s como igual a -1 pero hay una razón para esta notación la cual se aclarará pronto.) Definamos una acción de C_2 sobre $\mathbb{R}^2$ por

$$1(x,y) = (x,y), \qquad s(x,y) = (y,x), \qquad (x,y) \in \mathbb{R}^2$$

Sea G el conjunto $G = \mathbb{R}^2 \times C_2$.

Definamos la operación binaria $\cdot : G \times G \to G$ por

$$(g_1, z_1) \cdot (g_2, z_2) = (g_1 + z_1(g_2),\ z_1 \cdot z_2\ ),$$

para todo $g_1, g_2 \in G$ y todo $z_1, z_2 \in C_2$. Este es un grupo-el producto semi-directo de $\mathbb{R}^2$ con C_2.
Para ver esto, debemos responder algunas preguntas:

- ¿es cerrado bajo la operación? Sí
- ¿existencia de la identidad? Sí, $e = \big((0,0),1\big)$
- ¿existencia del inverso? Sí, $\big((x,y),1\big)^{-1} = \big((-x,-y),1\big)$, y $\big((x,y),s\big)^{-1} = \big((-y,-x),s\big)$
- ¿es asociativo? Esto es lo difícil:

$$\begin{gathered}\big((g_1,z_1)\cdot(g_2,z_2)\big)\cdot(g_3,z_3) = (g_1 + z_1(g_2),\ z_1\cdot z_2)\cdot(g_3,z_3)\\ = (g_1 + z_1(g_2) + (\,z_1\cdot z_2)g_3, (\,z_1\cdot z_2)\cdot z_3)\\ (g_1,z_1)\cdot\big((g_2,z_2)\cdot(g_3,z_3)\big) = (g_1,z_1)\cdot(g_2 + z_2(g_3),\ z_2\cdot z_3)\\ = \Big(g_1 + z_1(g_2) + z_1\big(z_2(g_3)\big),\ z_1\cdot(\,z_2\cdot z_3)\Big)\end{gathered}$$

Esto implica la asociatividad.

Ejemplo 6.7.2. Sea

$$S_3 = \{1, s_1, s_2, s_1\cdot s_2, s_2\cdot s_1, s_1\cdot s_2\cdot s_1\}, \qquad H_1 = \{1, s_2, s_1\cdot s_2\cdot s_1\}, \qquad H_2 = \{1, s_1\}.$$

Sea $\phi :\ H_2 \to Aut(H_1)$ definida por

$$\begin{gathered}\phi(1) = 1 \text{ (el automorfismo identidad)}\\ \phi(s_1)(h) = s_1^{-1}\cdot h\cdot s_1 = s_1\cdot h\cdot s_1\end{gathered}$$

(dado que $s_1^{-1} = s_1$), $h \in H_1$.

Denota el producto semi-directo (externo) de H_1, H_2 por $G = H_1 \rtimes_\phi H_2$.

Por supuesto, hay una estrecha relación entre productos semi-directos definidos internamente y los definidos externamente. El siguiente lema es probado en [R], explica esta conexión:

Lema 6.7.1. Si G es el producto semi-directo (interno) de H_1 por H_2 (por lo que H_1 es un subgrupo normal de G), entonces hay un homomorfismo

$$\phi :\ H_2 \to Aut(H_1)$$

tal que $G \cong H_1 \rtimes_\phi (H_2)$.

Ejemplo 6.7.3. Sea C_d el grupo cíclico de orden d, el cual podemos considerar como un conjunto $C_d = \{0, 1, \dots, d-1\}$, con la adición mod d. Sea $N = C_d^n$, que consideramos como el grupo de n-vectores con 'coeficientes en C_d'. Sea $H = S_n$ el grupo simétrico de grado n, es decir, el grupo de todas las permutaciones

$$p : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}.$$

El grupo H actúa sobre N permutando los índices, es decir, las coordenadas de los vectores. Para $f \in S_n$, definimos $f^* : C_d^n \to C_d^n$ por

$$f^*(v) = \left(x_{f^{-1}(1)}, \dots, x_{f^{-1}(n)}\right) = P(f^{-1})v^t, \quad v = (x_1, \dots, x_n) \in C_d^n, \tag{6.2}$$

donde $P(g)$ es la matriz permutación asociada a una permutación g y v^t denota la transpuesta (un vector columna) de v. Ahora, para $p, q \in S_n$ y $v, w \in C_d^n$ definamos

$$(p, v) \cdot (q, w) = \left(pq, w + q^*(v)\right)$$

Esto define un producto semi-directo $C_d^n \rtimes S_n$, el **grupo simétrico generalizado**. Una **matriz monomio** es una matriz que contiene exactamente un no-cero de entrada para cada fila y columna. (Se sabe que $C_d^n \rtimes S_n$ es isomorfo al grupo de todos los 'C_n-valores matrices monomios $n \times n$', [R], ejercicio 7.33.)

6.8 Productos corona

Haremos una inspección a los hechos básicos acerca de los productos corona. Productos Corona son generalizaciones de productos semi-directos. Ocurren de forma natural en la teoría del grupo Cubo de Rubik (ver [Si], por ejemplo). Seré breve porque los productos corona que ocurren en la teoría del Cubo de Rubik puede ser, si lo desea, reformulados en términos de productos semi-directos. De hecho, es suficiente para considerar grupos simétricos generalizados (véase el Teorema 6.8.1 a continuación), que son aún más fáciles de tratar y ellos mismos son tipos especiales de productos semi-directos.
Sea G_1 un grupo, y sea G_2 un grupo que actúa sobre un conjunto finito X_2. Fijemos un etiquetado de X_2 digamos $X_2 = \{h_1, h_2, \dots, h_m\}$, donde $m = |X_2|$ y sea $G_1^{X_2}$ el producto directo de G_1 consigo mismo m veces, con las coordenadas etiquetadas por los elementos de X_2.

Definición 6.8.1. El **producto corona** de G_1, G_2, es el grupo

$$G_1 \text{ wr } G_2 = G_1^{X_2} \rtimes G_2,$$

donde la acción de G_2 sobre $G_1^{X_2}$ es a través de su acción sobre X_2.

En particular, para cada $t \in G_1$ wr G_2 hay un $g_2 \in G_2$. Denotamos esta **proyección** por $g_2 = pr(t)$. Definamos la **base** del producto corona por

$$B = \{t \in G_1 \text{ wr } G_2 \mid pr(t) = 1\}$$

por lo que $B = G_1^{X_2}$.

Ejemplo 6.8.1. Sea $\mathbb{R}^n$ el producto directo del grupo aditivo de los números reales consigo mismo n veces. La operación de grupo en $\mathbb{R}^n$ es adición componente a componente. Sea S_n el grupo simétrico. Este actúa sobre $\mathbb{R}^n$ permutando coordenadas como en (6,2). Esta acción respeta la adición:

$$r^*(x_1 + y_1, \dots, x_n + y_n) = r^*(x_1, \dots, x_n) + r^*(y_1, \dots, y_n),$$

$(x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathbb{R}^n$. (Dicho sea de paso, sino que también preserva multiplicación escalar:

$$r^*(a * \vec{v}) = a \cdot r^*\vec{v},$$

para $\vec{v} \in \mathbb{R}^n$ y $a \in \mathbb{R}$. Por lo tanto, r define una transformación lineal invertible sobre $\mathbb{R}^n$. De hecho, hay un homomorfismo $S_n \to Aut(\mathbb{R}^n)$, donde $Aut(\mathbb{R}^n)$ denota el grupo de todas las transformaciones lineales invertibles sobre $\mathbb{R}^n$. ¿Reconoces este homomorfismo? Ha ocurrido anteriormente.)
Sea G el conjunto

$$G = \mathbb{R}^n \times S_n$$

y definamos una operación binaria $\cdot : G \times G \to G$ por

$$(\vec{v}_1, p_1) \cdot (\vec{v}_2, p_2) = (\vec{v}_1 + p_1^*(\vec{v}_2), p_1 \cdot p_2),$$

para todo $\vec{v}_1,\ \vec{v}_2 \in \mathbb{R}^n$ y todo $p_1, p_2 \in S_n$. Este es un grupo. Para ver esto, debemos responder algunas preguntas:

- ¿Es G cerrado bajo la operación $\cdot$? Sí.
- ¿Existe una identidad? Sí, $e = (\vec{0}, 1)$.
- ¿Existe un inverso? Sí, $(\vec{v}, p)^{-1} = (-(p^{-1})^*\vec{v}, p^{-1})$
- ¿Es G asociativo? Esto es lo difícil:

$$\begin{gathered}\big((\vec{v}_1, p_1) \cdot (\vec{v}_2, p_2) \cdot (\vec{v}_3, p_3)\big) = (\vec{v}_1 + p_1^*(\vec{v}_2), p_1 \cdot p_2)(\vec{v}_3, p_3) \\ = (\vec{v}_1 + p_1^*(\vec{v}_2) + (p_1 \cdot p_2)^*(\vec{v}_3), (p_1 \cdot p_2) \cdot p_3) \\ (\vec{v}_1, p_1) \cdot \big((\vec{v}_2, p_2) \cdot (\vec{v}_3, p_3)\big) = (\vec{v}_1, p_1) \cdot (\vec{v}_2 + p_2^*(\vec{v}_3), p_2 \cdot p_3) \\ = \Big(\vec{v}_1 + p_1^*(\vec{v}_2) + p_1^*\big(p_2^*(\vec{v}_3)\big),\ p_1 \cdot (p_2 \cdot p_3)\Big)\end{gathered}$$

Esto implica asociatividad.
Este grupo es el producto corona de $\mathbb{R}$ con S_n, $G = \mathbb{R}$ wr S_n donde $\mathbb{R}^n$ es la base.

Lema 6.8.1.

(a) La base B, que es isomorfa al producto directo $G_1^{|X_2|}$, es un subgrupo normal de G_1 wr G_2.
(b) $(G_1$ wr $G_2)/B$ es isomorfo a G_2.

Esto es una consecuencia del primer teorema de isomorfismos de la teoría de grupos. La prueba se omite. (Consulte el capítulo 8 de [NST] o [R] para más detalles.)

6.8.1 El grupo Cubo de Rubik ilegal

Sea H el **grupo Cubo de Rubik ilegal** de todos los movimientos legales e ilegales del Cubo de Rubik 3×3. En otras palabras, además de los movimientos básicos usuales (a saber, R, L, U, D, F, B), que nos permiten desarmar y volver a armar el cubo los subcubos esquina y arista (pero no podemos quitar las pegatinas de las caras). Sea C_3 el grupo de todas las rotaciones de un subcubo esquina en particular por un ángulo de 120 grados. (En realidad, este grupo depende de la esquina en rotación, pero puesto que estos grupos son todos isomorfos, podemos quitar la dependencia de la notación.) Sea C_2 el grupo de todos los flips de un subcubo arista particular. (Una vez más, este grupo depende de la arista que está siendo volteada, pero puesto que estos grupos son todos isomorfos, quitamos la dependencia de la notación.) Vamos a demostrar más tarde que

$$H = (C_3 \text{ wr } S_V) \times (C_2 \text{ wr } S_E),$$

donde V es el conjunto de subcubos esquina y E es el conjunto de subcubos arista.

6.8.2 Elementos de orden d en C_m wr S_n

En esta sección, vamos a aplicar nuestro conocimiento de los productos corona para incrementar nuestra habilidad para determinar todos los elementos de orden d en el grupo Cubo de Rubik. (El caso $d = 2$ será examinado en detalle más adelante.) En algunos casos (por ejemplo, en los casos con los que tratamos aquí), productos corona llegan a ser relativamente concretos y grupos familiares.
Sea $S(n, m)$ el grupo de todas las matrices monomios $n \times n$ con entradas en C_m. Comenzamos con el siguiente resultado, que nos permite identificar $S(n, m)$ con el grupo simétrico generalizado en el Ejemplo 6.7.3.

Teorema 6.8.1. Hay un isomorfismo entre C_m wr S_n y el grupo $S(n, m)$, que envía un elemento $(\vec{v}, f) \in C_m$ wr S_n, $\vec{v} = (v_1, v_2, \dots, v_n) \in C_m^n$ y $f \in S_n$, al vector $P(f)\text{diag}(\vec{v})$.

Es un caso especial de un ejercicio en [R].

Ejemplo 6.8.2. Si $n = 3$ y $m = 2$, entonces

- $\big((-1, 1, -1), (1, 2)\big)$ corresponde a

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix};$$

- $\big((1, -1, 1), (1, 2)\big)$ corresponde a

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Sea $\vec{v} = (v_1, v_2, \dots, v_n) \in C_m^n$ y $f \in S_n$. Es claro de este teorema que un elemento $(\vec{v}, f) \in C_m$ wr S_n es de orden d solo si la matriz permutación $P(f)$ es de orden d. En efecto,

$$(\vec{v}, f)^2 = (\vec{v} + f^*(\vec{v}), f^2),$$
$$(\vec{v}, f)^3 = (\vec{v} + f^*(\vec{v}) + (f^*)^2(\vec{v}), f^3),$$
$$\vdots$$
$$(\vec{v}, f)^k = \left(\vec{v} + \ \ldots + (f^*)^{k-1}(\vec{v}), f^k\right).$$

Concluimos con la siguiente clasificación de los elementos de orden d en el producto corona.

Proposición 6.8.1. Un elemento $(\vec{v}, f) \in C_m$ wr S_n, $\vec{v} = (v_1, v_2, \ldots, v_n) \in C_m^n$ y $f \in S_n$, es de orden d si y sólo si $f^d = 1$ y $\vec{v} + \ \ldots + (f^*)^{d-1}(\vec{v}) = 0$, donde f^* se define en (6,2).

Este resultado puede, en principio, ser utilizado en conjunción con la determinación explícita del grupo Cubo de Rubik dado más adelante para determinar todos los elementos de un orden dado. Ver 7.3

Capítulo 7

El grupo Cubo de Rubik (legal)

En este capítulo, construimos sobre el material de los capítulos anteriores para describir matemáticamente el grupo de movimientos (legales) del Cubo de Rubik 3×3. Para los principiantes, podría parecer que hemos terminado un camino largo a una colina. Sin embargo, ¡no hemos terminado! Aunque el terreno puede aplanarse, hay todavía un poco de una caminata hasta llegar a nuestro destino.

7.1 Descripción matemática de los movimientos del cubo $3 \times 3 \times 3$

En esta sección, se describen matemáticamente los movimientos del Cubo de Rubik $3 \times 3 \times 3$. Como veremos, esto conducirá finalmente a la descripción del grupo Cubo de Rubik como un subgrupo de índice 12 de un producto directo de dos productos corona.

7.1.1 Notación

Primero, orientamos todas las esquinas y aristas como en el Teorema 6.6.1
Las orientaciones arista se presentan como sigue en las caras F, R y U:

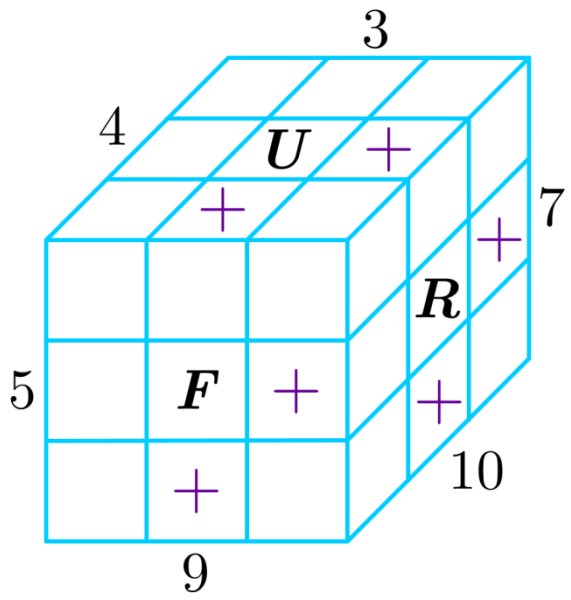


Figura 7.1: *Orientaciones arista y etiquetas para el cubo.*

Para las otras caras: colocar un '+' en las aristas, dl, db, lf, lu, bl *y* bu. Esto fija las orientaciones arista. Para las aristas etiquetadas, ordenar las aristas $uf, ur, ub, ul, lf, fr, rb, bl, df, dr, db, dl$, y etiquetarlas, en orden, del 1 al 12 (así, por ejemplo, la arista db es 11).
Para las orientaciones esquina, poner un signo de '+' en todas las caritas esquina superiores y en todas las caritas esquina inferiores. Las etiquetas y orientaciones esquina se representan en las caras F, R y D como en la siguiente figura 7.2 (El mismo etiquetado fue utilizado en el 3.6.2 anterior).

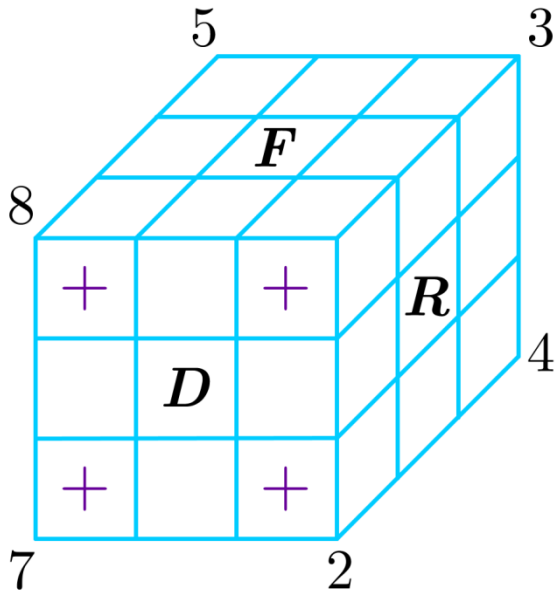


Figura 7.2: *Orientaciones esquina y etiquetas para el cubo.*

Sea $G = \langle R, L, U, D, F, B \rangle$ el grupo del Cubo de Rubik de $3 \times 3 \times 3$ y sea H el grupo 'ampliado' generado por R, L, U, D, F, B y todos los movimientos 'ilegales' (donde se permite desarmar y volver a armar el cubo, pero remover alguna caritas). Sea V el conjunto de vértices del cubo (que nosotros identificamos con el conjunto de subcubos esquina del Cubo de Rubik) y sea

$$\rho : H \to S_V$$

el homomorfismo que asocia a cada movimiento del Cubo de Rubik la correspondiente permutación de los vértices (ver Ejemplo 6.2.1). Sea E el conjunto de aristas del cubo (que nosotros identificamos con el conjunto de subcubos arista del Cubo de Rubik) y sea

$$\sigma : H \to S_E$$

el homomorfismo que asocia a cada movimiento del Cubo de Rubik con la correspondiente permutación de las aristas (ver el Ejemplo 6.2.1).
Estos homomorfismos ρ y σ serán reformulados de manera ligeramente diferente en 7.2.2 a continuación.

7.1.2 Orientaciones esquina

Sea $v : H \to C_3^8$ la función que asocia a cada movimiento $g \in H$ las correspondientes orientaciones esquinas. Más precisamente, sea $g \in H$ y decimos que g mueve la esquina i a la esquina j. Entonces $v_i(g) \in C_3$ es la orientación a la que el i-ésimo vértice es enviado por g, donde los vértices están etiquetados como en el diagrama mostrado y donde la orientación es el número de giros de 120 grados en sentido horario necesarios para convertir la referencia relativa '+' obtenido por movimiento de la esquina i a la j usando el movimiento g en el estándar de referencia '+' sobre la esquina j.

Ejemplo 7.1.1. Tenemos

X	$\vec{v}(X)$
F	$(2,0,1,0,1,0,0,2)$
U	$(0,0,0,0,0,0,0,0)$
D	$(0,0,0,0,0,0,0,0)$
B	$(0,1,0,2,0,2,1,0)$
R	$(1,2,2,1,0,0,0,0)$
L	$(0,0,0,0,1,2,1,2)$

Tabla 7.1

El etiquetado de las esquinas que se usa en esta tabla es como en el Teorema 6.6.1.

Observación 7.1.1. El efecto de un movimiento $g \in H$ en las orientaciones esquina puede también ser considerado como un reetiquetado de las marcas '+'.

Note que un movimiento $g \in H$ tiene dos efectos en las esquinas:

(a) una permutación $\rho(g) \in S_V$ de los vértices,
(b) una reorientación de los movimientos vértice en (a).

En particular, para $g, h \in H$, la orientación $\vec{v}(gh)$ sólo puede diferir de $v(g)$ en las coordenadas correspondientes a los vértices permutados por h.
Ahora vamos a verificar que la orientación 'relativa' $\vec{v}(gh) - \vec{v}(g)$ es la misma como la orientación $\vec{v}(h)$, supuesto que uno toma en cuenta el efecto de g en los vértices:
$\vec{v}(h) = \rho(g)\big(\vec{v}(gh) - \vec{v}(g)\big)$.

Lema 7.1.1. $\vec{v}(gh) = \vec{v}(g) + \rho(g)^{-1}\big(\vec{v}(h)\big)$.

Prueba: El movimiento gh orienta el subcubo esquina i-ésimo por $v_i(gh)$ y permuta los vértices por $\rho(gh)$, por definición
Por otro lado, gh primero actuará por g luego h. El movimiento g reorientará el subcubo esquina i-ésimo por $v_i(g)$ y envía el vértice i-ésimo al vértice $\rho(g)(i)$-ésimo.
Para estudiar el efecto posterior de h en esto, vamos a restar $\vec{v}(g)$ de $\vec{v}(gh)$, por lo que estamos de vuelta a nuestra orientación original (vamos a agregar $\vec{v}(g)$ de nuevo más tarde). Llamamos a esta posición **el cubo modificado** por ahora.

El movimiento h primero orienta el subcubo esquina j-ésimo del cubo modificado por $v_j(h)$ y permuta al vértice $\rho(h)(j)$. El subcubo i-ésimo del cubo modificado viene de (a través de g) el subcubo $\rho(g)^{-1}(i)$-ésimo del cubo original. Así, el subcubo esquina i-ésimo del cubo modificado es, por medio de h, reorientado por $v_{\rho(g)^{-1}(i)}(h)$. A esto hay que añadir en el $v_i(g)$ para obtener el efecto total de gh sobre el vértice i-ésimo del original:

$$v_i(gh) = v_i(g) + v_{\rho(g)^{-1}(i)}(h),$$

para cada $1 \leq i \leq 8$, lo que implica el Lema 7.1.1.

7.1.3 Orientaciones arista

Sea $w : H \to C_2^{12}$ la función que asocia a cada movimiento $g \in H$ las correspondientes orientaciones arista. Más precisamente, sea $g \in H$ y decimos que g mueve la arista i a la arista j. A continuación, $w_i(g) \in C_2$ es la orientación que la arista i-ésima envía a g, donde las aristas están etiquetadas como en el diagrama mostrado y donde la orientación es el número de flips de 180 grados necesarios para convertir la referencia relativa '+' obtenida por el movimiento de la arista i hasta la j usando el movimiento g en el referencia estandar '+' sobre la arista j.

Ejemplo 7.1.2. Tenemos

X	$\vec{w}(X)$
F	$(1,0,0,0,0,0,0,0,1,0,0,0)$
U	$(1,0,1,0,0,0,0,0,0,0,0,0)$
$F \bullet U$	$(1,0,1,0,1,0,0,0,1,0,0,0)$
$U \bullet F$	$(1,1,1,0,0,0,0,0,1,0,0,0)$
B	$(0,0,0,0,0,0,1,1,0,0,0,0)$
D	$(0,0,0,0,0,0,0,0,0,1,0,1)$
R	$(0,1,0,0,0,0,0,0,0,1,0,0)$
L	$(0,0,0,0,1,0,0,0,1,0,0,0)$

Tabla 7.2

El etiquetado de las aristas utilizado en esta tabla es como en el Teorema 6.6.1.

Observación 7.1.2. El efecto de un movimiento $g \in H$ en las orientaciones arista también puede ser considerado como un reetiquetado de las marcas '+'.

Note que un movimiento $g \in H$ tiene dos efectos en las aristas

(a) una permutación $\sigma(g) \in S_E$ de las aristas,
(b) una reorientación de las aristas que se han movido en (a).

En particular, para $g, h \in H$, la orientación $\vec{w}(gh)$ puede diferir de un $\vec{w}(g)$ sólo en las coordenadas correspondientes a las aristas permutadas por h.
Vamos a decir que

$$\vec{w}(gh) = \vec{w}(g) + \sigma(g)^{-1}\big(\vec{w}(h)\big) \qquad (7.1)$$

es decir, que

$$w_i(gh) = w_i(g) + w_{\sigma(g)^{-1}(i)}(h),$$

para cada $1 \leq i \leq 12$. La prueba de esto es similar a la demostración del Lema 7.1.1 para verificar (7.1).

7.1.4 El producto semi-directo

Considere el siguiente producto directo de dos productos semi-directos:

$$H' = (C_3^8 \rtimes S_V) \times (C_2^{12} \rtimes S_E).$$

Observación 7.1.3. Esto también puede ser escrito en la notación de los productos corona como el siguiente producto directo de dos productos corona:

$$H' = (C_3 \text{ wr } S_V) \times (C_2 \text{ wr } S_E).$$

Como un conjunto, pensamos de H como que pertenece a $C_3^8 \times S_V \times C_2^{12} \times S_E$. Si representamos elementos de h, h' de H como $h = (v, r, w, s), h' = (v', r', w', s') \in C_3^8 \times S_V \times C_3^8 \times S_V$ entonces, la operación del grupo se dará por

$$h \cdot h' = (v, r, w, s) \cdot (v', r', w', s') = (v + P(r)(v'), rr', w + P(s)(w'), ss').$$

Considere la función

$$\begin{aligned} \boldsymbol{\iota}: H &\to (C_3^8 \rtimes S_V) \times (C_2^{12} \rtimes S_E) \\ g &\mapsto \big(v(g), \rho(g), w(g), \sigma(g)\big). \end{aligned}$$

Proposición 7.1.1. El homomorfismo ι es un isomorfismo de grupo, $H \cong H'$.

Demostración: Puesto que

$$\begin{aligned} &\big(\vec{v}(g), \rho(g), \vec{w}(g), \sigma(g)\big) \cdot \big(\vec{v}(h), \rho(h), \vec{w}(h), \sigma(h)\big) \\ &= \Big(\vec{v}(g) + P\big(\rho(g)\big)\big(\vec{v}(h)\big), \rho(g)\rho(h), \vec{w}(g) + P\big(\sigma(g)\big)\big(\vec{w}(h)\big), \sigma(g)\sigma(h)\Big), \end{aligned}$$

el mapeo de ι es un homomorfismo. Dado que cualquier reorientación y permutación puede ser alcanzado por un movimiento ilegal, ι debe ser sobreyectiva. Por el teorema 6.6.1, el kernel de ι es trivial (esto es sólo una forma elegante de decir que si ningún subcubo es permutado o reorientado entonces el cubo no cambia).

7.2 Estructura del grupo cubo

El resultado principal de esta sección es el 'segundo teorema fundamental de la teoría del cubo.' El resultado de esta sección es a la vez hermoso y vale la pena conocerlo.
Algunos preliminares. Identificamos, como en 7.1, cada $g \in G$ con una 4-tupla

$$\big(\vec{v}(g), \rho(g), \vec{w}(g), \sigma(g)\big)$$

donde

- $\rho(g)$ es la permutación correspondiente del conjunto de vértices V del cubo,
- $\sigma(g)$ es la permutación correspondiente del conjunto de aristas E del cubo,
- $v(g), w(g)$ son las orientaciones definidas en 7.1.

Observación 7.2.1. Sea S_n el grupo simétrico de grado n e identifiquemos S_V con S_8, S_E con S_{12}. Por ejemplo 6.2.1, sabemos que

(a) $\rho : G \to S_8$ es un homomorfismo,
(b) $\sigma : G \to S_{12}$ es un homomorfismo.

7.2.1 El segundo teorema fundamental de la teoría del cubo

Pregunta: Teniendo en cuenta una 4-tupla (v, r, w, s), donde r, s son permutaciones de las esquinas, respectivamente aristas, como anteriormente y

$$v \in C_3^8, \quad w \in C_2^{12}$$

¿qué condiciones de r, s, v, w aseguran que corresponde a una posición posible del cubo de Rubik?
El siguiente resultado responde a esta pregunta. Debido a Ann Scott.

Teorema 7.2.1. (Segundo teorema fundamental de la teoría del cubo) Una 4-tupla $(\vec{v}, r, \vec{w}, s)$ como anteriormente $(r \in S_8,\ s \in S_{12},\ \vec{v} \in C_3^8,\ \vec{w} \in C_2^{12})$ corresponde a una posible posición del cubo de Rubik si y sólo si

(a) $sgn(r) = sgn(s)$, ('paridad igual como permutaciones')
(b) $v_1 + \ \ldots + v_8 \equiv 0 \pmod 3$, ('la conservación de los giros totales')
(c) $w_1 + \ \ldots + w_{12} \equiv 0 \pmod 2$, ('la conservación de un total de flips').

Prueba: Para simplificar, escribimos v por $\vec{v}$.
Primero, probaremos la parte 'sólo si'. Es decir, asumimos que $(v, r, w, s) \in S_V \times S_E \times C_3^8 \times C_2^{12}$ representa una posición (obtenida legalmente) del Cubo de Rubik.
De esto queremos demostrar (a) - (c).
Sea $g \in G$ el elemento el cual mueve el Cubo de Rubik de la posición resuelta a la posición asociada con esta 4-tupla. Entonces $r = \rho(g)$ y $s = \sigma(g)$. Sabemos que g se puede escribir como una palabra en los movimientos básicos R, L, U, D, F, B, digamos $g = X_1 \ldots X_k$, donde cada X_i es igual a uno de los R, L, U, D, F, B. Observar que si X es uno de estos movimientos básicos, entonces $sgn\big(\rho(X)\big) = sgn\big(\sigma(X)\big)$. Ya que sgn, ρ y σ son homomorfismos, se sigue que

$$sgn(r) = sgn\big(\rho(g)\big) = \prod_{i=1}^{k} sgn\big(\rho(X_i)\big) = \prod_{i=1}^{k} sgn\big(\sigma(X_i)\big) = sgn\big(\sigma(X)\big) = sgn(s).$$

Esto demuestra (a).

Hemos comprobado (b) para los movimientos básicos en el ejemplo anterior 7.1.1. Nótese que

(i) la conservación de la condición giros en (b) es cierto para $(v_1, \ldots, v_8)$ si y sólo si es cierto para cualquier permutación $P(p)(v) = \big(v_{(1)p}, \ldots, v_{(8)p}\big)$;
(ii) si $(v_1, \ldots, v_8)$ y $(v'_1, \ldots, v'_8)$ cada una satisfacen la conservación de la condición de giros en (b) entonces, su suma también satisface.

Como anteriormente, escribir g como una palabra en los movimientos básicos R, L, U, D, F, B, por ejemplo $g = X_1 \ldots X_k$, donde cada X_i es igual a uno de los R, L, U, D, F, B. Suponemos que esta expresión es mínima en el sentido que elijamos X_i de modo que k es tan pequeño

como sea posible. Esta k es llamada **longitud** de g. (Esta longitud es la misma que la distancia de g a la identidad en el grafo de Cayley de G.)
Ahora probaremos (b) por inducción sobre la longitud. Ya lo hemos comprobado para todas las palabras de longitud $k = 1$.
Supongamos que $k > 1$. Por la fórmula, dando la orientación del producto de dos movimientos en términos de las dos orientaciones de los movimientos, tenemos

$$\vec{v}(X_1 \dots X_{k-1}X_k) = \rho(X_1 \dots X_{k-1})^{-1}\big(\vec{v}(X_k)\big) + \vec{v}(X_1 \dots X_{k-1}).$$

El término $\rho(X_1 \dots X_{k-1})^{-1}\big(\vec{v}(X_k)\big)$ satisface la conservación de la condición de giros en (b) por (i) anterior. El término $\vec{v}(X_1 \dots X_{k-1}X_k)$ satisface la conservación de la condición de giros en (b) por la hipótesis de inducción. Su suma satisface la conservación de la condición de giros en (b) por (ii) anterior. Esto demuestra (b).
La demostración de (c) es muy similar a la demostración de (b), salvo que utilizaremos el Ejemplo 7.1.2 en lugar del Ejemplo 7.1.1.

Ahora, debemos demostrar el teorema en la dirección 'si'. En otras palabras, suponiendo (a), (b), y (c) debemos mostrar que existe una posición legal correspondiente del Cubo de Rubik. Esta parte de la prueba es constructiva.

Primero, probamos un caso especial. Supongamos que r y s son ambas la identidad y que $(w_1, \dots, w_{12}) = (0, \dots, 0)$.

Hay un movimiento que gira exactamente dos esquinas y conserva las orientaciones y las posiciones de todos los otros subcubos. Por ejemplo, el movimiento $g = (R^{-1}D^2RB^{-1}U^2B)^2$ gira la esquina ufr 120 grados en sentido horario, la esquina bdl 240 grados en sentido horario, y conserva las orientaciones y posiciones de todos los otros subcubos. Este movimiento se puede modificar fácilmente, por una conjugación adecuada, para obtener un movimiento que gira cualquier par de esquinas, y conserva las orientaciones y posiciones de todos los otros subcubos. Estos movimientos generan todas las 8-tuplas posibles satisfaciendo la condición de conservación de giros en (b). Esto demuestra la parte 'si' del teorema en el caso de que r y s son a la vez la identidad y que $(w_1, \dots, w_{12}) = (0, \dots, 0)$.

A continuación, probaremos otro caso especial. Supongamos que r y s son ambas la identidad y que $(v_1, \dots, v_8) = (0, \dots, 0)$.
Hay un movimiento que mueve exactamente dos aristas y conserva las orientaciones y las posiciones de todos los otros subcubos. Por ejemplo, el movimiento

$$g = LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$$

gira la arista uf, la arista ur, y preserva las orientaciones y las posiciones de todos los otros subcubos. Este movimiento se puede modificar fácilmente, por una conjugación adecuada, para obtener un movimiento que gira cualquier par de aristas, y conserva las orientaciones y posiciones de todos los otros subcubos. Estos movimientos generan todas las posibles 12-tuplas que satisfacen la conservación de la condición flip en (C). Esto demuestra la parte 'si' del teorema en el caso de que r y s son a la vez la identidad y que $(v_1, \dots, v_8) = (0, \dots, 0)$.
Como una consecuencia de estos dos últimos casos especiales, se deduce que la parte 'si' del teorema es cierto en el caso de que r y s son ambas la identidad.
Por último, probamos nuestro último caso especial. Supongamos que $(v_1, \dots, v_8) = (0, \dots, 0)$ y que $(w_1, \dots, w_{12}) = (0, \dots, 0)$. Considere las siguientes tres afirmaciones.

- Dados tres subcubos arista, hay un movimiento que es un 3-ciclo en estas aristas y preserva las orientaciones y posiciones de todos los otros subcubos.
- Dadas tres esquinas, hay un movimiento que es un 3-ciclo en estas esquinas y preserva las orientaciones y posiciones de todos los otros subcubos.
- Dado cualquier par de aristas y cualquier par de esquinas, hay un movimiento que es un 2-ciclo en estas aristas, un 2-ciclo en estas esquinas, y conserva las orientaciones y posiciones de todos otros subcubos.

Por proposición 6.4.1, sabemos que A_E es generada por la arista de 3-ciclos anterior y que A_V es generada por la esquina de 3-ciclos anterior. En otras palabras, podemos construir una posición del Cubo de Rubik asociada con cualquier 4-tupla $(r, s, 0, 0)$, siempre que $r \in A_V$ y $s \in A_E$. El subgrupo $A_V \times A_E$ es el índice 4 en $S_E \times S_V$ dado que $|S_n/A_n| = 2$. El tercer tipo de movimiento, la arista-esquina de 2 ciclos anterior, no se corresponde con un elemento del subconjunto $A_E \times A_V$ del grupo Cubo de Rubik porque una arista de 2-ciclos es una permutación impar de las aristas. Por lo tanto, si consideramos que el subgrupo de $S_E \times S_V$ generado por los tres tipos de movimientos que obtendrá ya sea todo $S_E \times S_V$ o algún subgrupo de índice 2 que contiene propiamente $A_E \times A_V$. La primera posibilidad se puede descartar, ya que contradice la condición de paridad en (a). El único subgrupo de $S_E \times S_V$ de índice 2, que contiene propiamente $A_E \times A_V$ es el subgrupo de los elementos que satisfacen la condición de paridad en (a).
De ello se desprende que la parte 'si' del teorema es cierto en el caso de que v y w son ambas cero.
El teorema es una consecuencia de estos casos especiales debido a lo siguiente.

Afirmación: No importa qué posición del Cubo de Rubik sea, siempre hay un movimiento que no permuta cualquier subcubo pero 'resuelve' la orientación del cubo de modo que v y w son ambas cero.
La prueba del teorema ha terminado.

Corolario 7.2.1. El grupo del Cubo de Rubik está dado por

$$G = \{g = (\vec{v}, r, \vec{w}, s) \in H \mid (a), (b), (c) \text{ mantener}\},$$

donde (a), (b), (c) son como en el teorema anterior.

Ahora demostremos que el centro del grupo del Cubo de Rubik consiste en la identidad y el superflip.

Corolario 7.2.2. El centro de G consiste de dos elementos: la identidad y el 'superflip' $z = (\vec{v}, r, \vec{w}, s)$ donde $\vec{w} = (1, 1, \dots, 1) \in C_2^{12}, \vec{v} = \vec{0} \in C_3^8,\ s = 1 \in S_{12}\ y\ r = 1 \in S_8$.

Prueba: La prueba dada aquí es esencialmente la misma que la de Bandelow [B1].
Escribir v en lugar de $\vec{v}$, por simplicidad. Recuérdese que el centro de $S_n, n > 2$, es trivial. Fijar $(v, r, w, s) \in G$. Tenemos

$$(v, r, w, s) \cdot (v', r', w', s') = (v + P(r)(v'), rr', w + P(s)(w'), ss')$$
$$= (v', r', w', s') \cdot (v, r, w, s) = (v' + P(r')(v), r'r, w' + P(s')(w), s's),$$

para todo $(v', r', w', s') \in G$, sólo si $r = 1$ y $s = 1$. Esto implica que $v + v' = v' + P(r')v$, para todo $r' \in S_8$. Esto obliga a v a ser $(0, 0, \dots, 0)$ o $(1, 1, \dots, 1)$ o $(2, 2, \dots, 2)$. Puesto que debe satisfacer la conservación de giros, no puede ser $(1, 1, \dots, 1)$ o $(2, 2, \dots, 2)$. Del mismo modo, $w + w' = w' + P(s')w$, para todo $s' \in S_{12}$ obliga a w a ser $(0, 0, \dots, 0)$ o $(1, 1, \dots, 1)$. Cualquiera de estas opciones es aceptable, ya que ambos satisfacen la conservación de los lanzamientos flips.

7.2.2 Algunas consecuencias

Vamos a reformular el hecho anterior sobre el grupo del cubo de Rubik desde un punto de vista diferente. Esta nueva perspectiva nos ayuda a determinar el tamaño de este grupo. Sea

$$G_0 = \{(\vec{v}, r, \vec{w}, s) \mid r \in S_8, s \in S_{12},$$
$$\vec{v} = (v_1, v_2, \dots, v_8), v_i \in \{0, 1, 2\}, v_1 + \dots + v_8 \equiv 0 \pmod 3,$$
$$\vec{w} = (w_1, w_2, \dots, w_8), w_i \in \{0, 1\}, w_1 + \dots + w_8 \equiv 0 \pmod 2\}$$

En otras palabras, G_0 contiene las permutaciones de las esquinas, permutaciones de las aristas, las orientaciones de las esquinas, y las orientaciones de las aristas. Hay una conservación de condiciones de flips y una conservación de la condición giros pero no condición de paridad en las permutaciones. Definir una operación binaria $\cdot : G_0 \times G_0 \to G_0$ por

$$(\vec{v}, r, \vec{w}, s) \cdot (\vec{v}', r', \vec{w}', s') = (\vec{v} + P(r)(\vec{v}'), r \cdot r', \vec{w} + P(s)(\vec{w}'), s \cdot s')$$

donde P es la matriz permutación (Definición 1.2.2). Esto define una estructura de grupo en G_0. Este es un subgrupo del grupo ilegal Cubo de Rubik de índice 6.

Teorema 7.2.2. Hay un isomorfismo

$$G_0 \cong (C_3^7 \rtimes S_8) \times (C_2^{11} \rtimes S_{12})$$

donde C_n es el grupo cíclico con n elementos y $\rtimes$ denota el producto semi-directo y donde C_n^k $(n = 2, 3, k = 7, 11)$ se identifica con el subgrupo de C_n^{k+1} definida por

$$\{\vec{v} = (v_1, v_2, \dots, v_k) \mid v_i \in \{0, 1, n-1\}, v_1 + \dots + v_k \equiv 0 \pmod n\},$$

En particular,

$$|G_0| = |S_8||S_{12}|\left|C_2^{11}\right||C_3^7| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7.$$

Prueba: Esto se deduce de la definición de producto semi-directo y el principio multiplicativo.

Corolario 7.2.3. El grupo G del Cubo de Rubik es el kernel del homomorfismo

$$\phi : G_0 \to \{1, -1\}$$
$$(\vec{v}, r, \vec{w}, s) \mapsto sgn(r)sgn(s).$$

En particular, $G < G_0$ es normal de índice 2 y $|G| = 8! \cdot 12! \cdot 2^{10} \cdot 3^7$.

Prueba: Esto se deduce del teorema y del primer teorema de isomorfismo de la teoría de grupos (Teorema 6.5.1).
Recordemos que el subgrupo conmutador G_1 de G es el subgrupo formado por todos los productos finitos de conmutadores, $[g, h] = g \cdot h \cdot g^{-1} \cdot h^{-1}$, donde g, h son elementos arbitrarios de G.

Teorema 7.2.3. $G_1 = \{g \in G \,|sgn(\rho(g)) = sgn(\sigma(g)) = 1\}$.

Prueba: Se sabe que el subgrupo conmutador de S_n es A_n, para $n > 4$ (Véase el capítulo 3 de [R], de hecho, para $n > 4$, An es el único subgrupo normal propio no trivial de S_n).
Considerar la proyección mapeo $\phi : C_n^k \rtimes S_n \to S_n$. El kernel de ϕ es C_n^k. Además,

$$\phi([g,h]) = \phi(g \cdot h \cdot g^{-1} \cdot h^{-1}) = \phi(g) \cdot \phi(h) \cdot \phi(g^{-1}) \cdot \phi(h^{-1}) = [\phi(g), \phi(h)],$$

para cualquier $g, h \in C_n^k \rtimes S_n$. Esto implica que los mapeos ϕ del subgrupo conmutador $\left(C_n^k \rtimes S_n\right)_1$ al subgrupo conmutador $(S_n)_1 = A_n$. De esto se deduce que $\left(C_n^k \rtimes S_n\right)_1 = C_n^k \rtimes A_n$. Esto implica el teorema.

Corolario 7.2.4. $|G_1| = |G|/2$.

Prueba: El teorema anterior implica que $|G/G_1| = 2$, utilizando el primer teorema de isomorfismos.

7.3 Los movimientos de orden 2

En esta sección se presenta, como había prometido, un método para determinar los movimientos de un determinado orden en el grupo del Cubo de Rubik. Nos limitaremos a calcular el número de movimientos de orden 2, aunque el método debe, en principio, trabajar de manera más general. Sin embargo, tal vez es posible que el lector curioso y emprendedor utilice una computadora para encontrar los movimientos de orden d, donde $d > 2$, de una manera similar a lo que hacemos aquí.
El conjunto de elementos de orden 2 se puede dividir en 3 subconjuntos disjuntos:

(a) los elementos moviendo sólo las piezas esquina,
(b) los elementos moviendo sólo las piezas arista,
(c) los elementos movimiento las piezas esquina y arista.

Echemos un vistazo a un subconjunto de (a), que consta sólo de las permutaciones pares de orden 2 de las 8 piezas esquina. Es evidente que estos elementos pueden solo consistir de swaps que preservan orientaciones de piezas esquinas donde alguno de los 2 pares (4 piezas esquinas) o 4 pares (todos las 8 piezas esquina) son afectadas. Dado un par de piezas esquina, siempre hay 3 swaps que preservan la orientación.
El resto de (a) y (b) (no olvidemos (b)) tiene que ser calculado análogamente.
Recuerde que en 6.8.2 que un elemento $(\vec{v}, f) \in C_m$ wr S_n, $\vec{v} = (v_1, v_2, \dots, v_n) \in C_m^n$, y $f \in S_n$, es el orden d si y sólo si $f^d = 1$ y $\vec{v} + \dots + f^{d-1}(\vec{v}) = 0$.
En particular, elementos de orden 2 en $C_3^7 \rtimes S_8$ son los $(\vec{v}, r)$ con r de orden 2 (Por lo tanto un producto de distintos 2 ciclos) y $\vec{v}$ que satisface $v_1 + \dots + v_8 \cong 0 \pmod 3$ y $v_1 + v_{(i)r} \cong 0 \pmod 3$. No todos estos elementos corresponden a un movimiento legal del Cubo de Rubik. Utilizando el 'principio multiplicativo de conteo', calculamos el número de elementos de orden 2 en $C_3^7 \rtimes S_8$ a ser

$$\frac{1}{4!}\binom{8}{2}\binom{6}{2}\binom{4}{2}3^4 + \frac{1}{3!}\binom{8}{2}\binom{6}{2}\binom{4}{2}3^3 + \frac{1}{2!}\binom{8}{2}\binom{6}{2}3^2 + \binom{8}{2}3 = 21819. \qquad (7.2)$$

El término '3^3' y el término '3' no cuentan en los movimientos legales del Cubo de Rubik, si se toman por su cuenta, ya que no son par (por lo tanto no satisfacen la 'conservación de condición de paridad'). El número de elementos $(\vec{v}, r)$ de orden 2 en $C_3^7 \rtimes S_8$ con r par es

$$\frac{1}{4!}\binom{8}{2}\binom{6}{2}\binom{4}{2}3^4 + \frac{1}{2!}\binom{8}{2}\binom{6}{2}3^2 = 10395. \qquad (7.3)$$

El número de elementos $(\vec{v}, r)$ de orden 2 en $C_3^7 \rtimes S_8$ con r impar es

$$\frac{1}{3!}\binom{8}{2}\binom{6}{2}\binom{4}{2}3^3 + \binom{8}{2}3 = 11424. \qquad (7.4)$$

Del mismo modo, a través del 'principio multiplicativo de conteo', calculamos el número de elementos de orden 2 en $C_2^{11} \rtimes S_{12}$ a ser

$$\frac{1}{6!}\binom{12}{2}\binom{10}{2}\cdots\binom{4}{2}2^6 + \frac{1}{5!}\binom{12}{2}\binom{10}{2}\cdots\binom{4}{2}2^6 +$$
$$\frac{1}{4!}\binom{12}{2}\cdots\binom{6}{2}2^7 + \frac{1}{3!}\binom{12}{2}\cdots\binom{8}{2}2^8 + \frac{1}{2!}\binom{12}{2}\binom{10}{2}2^9 +$$
$$\binom{12}{2}2^{10} + \binom{12}{0}2^{11} - 1 = 15687871. \qquad (7.5)$$

Una vez más, no todos éstos cuentan como movimientos legales del Cubo de Rubik, si se toman por su cuenta. El número de elementos $(\vec{w}, s)$ de orden 2 en $C_2^{11} \rtimes S_{12}$ con s par es

$$\frac{1}{6!}\binom{12}{2}\binom{10}{2}\cdots\binom{4}{2}2^6 + \frac{1}{4!}\binom{12}{2}\cdots\binom{6}{2}2^7 + \frac{1}{2!}\binom{12}{2}\binom{10}{2}2^9 = 8080447. \qquad (7.6)$$

El número de elementos $(\vec{w}, s)$ de orden 2 en $C_2^{11} \rtimes S_{12}$ con s impar es

$$\frac{1}{5!}\binom{12}{2}\binom{10}{2}\cdots\binom{4}{2}2^6 + \frac{1}{3!}\binom{12}{2}\cdots\binom{8}{2}2^8 + \binom{12}{2}2^{10} = 7607424. \qquad (7.7)$$

Los otros se puede comprobar de manera similar.

El segundo teorema fundamental de la teoría del cubo (7.2.1) implica que un elemento $(\vec{v}, r, \vec{w}, s)$ del grupo de Cubo de Rubik es de orden 2 si y sólo si es un elemento de orden 2 en el grupo $H = (C_3^7 \rtimes S_8) \times (C_2^{11} \rtimes S_{12})$ y $sgn(r) = sgn(s)$. Un elemento no trivial $(h_1, h_2) \in H$, con $h_1 = (\vec{v}, r)$ y $h_2 = (\vec{w}, s)$es de orden 2 si y sólo si exactamente uno de los siguientes casos mutuamente excluyentes ocurre:

(a) $h_1 \neq 1,\ h_2 = 1,\ h_1^2 = 1,\ sgn(r) = 1,$
(b) $h_1 = 1,\ h_2 \neq 1,\ h_2^2 = 1,\ sgn(s) = 1,$
(c) $h_1 \neq 1,\ h_2 \neq 1,\ h_1^2 = 1,\ sgn(r) = sgn(s) = 1,$
(d) $h_1 \neq 1,\ h_2 \neq 1,\ h_1^2 = h_2^2 = 1,\ sgn(r) = sgn(s) = -1,$

Contamos cada caso. Caso (a) se cuenta en (7.3), caso (b) se cuenta en (7.6), caso (c) se cuenta en (7.3) y (7.6) (los cuales se multiplican juntos para obtener el total), y el caso (d) se

cuenta en (7.4) y (7.7) (de nuevo, se multiplican juntos para obtener el total). Sumando todo, encontramos que el número de elementos de orden 2 en el grupo Cubo de Rubik es

$$(7.3) + (7.6) + (7.3)^*(7.6) + (7.4)^*(7.7) = 170911549183 = (1.7..) \times 10^{11}.$$

Observación 7.3.1. ¿Por qué toda esta teoría para resolver este problema? ¿Por qué no hacer que una computadora lo haga? ¿Cuánto tiempo le tomaría a una computadora contar el número de los movimientos de orden 2 en el grupo Cubo de Rubik? Supongamos que su computadora puede comprobar si un elemento g en el grupo Cubo de Rubik G es de orden 2 o no, en 0.001 segundos. Entonces la computadora comprobará todos los 4.3×10^{19} elementos, para hallar los movimientos de orden 2 en alrededor de 4.3×10^{15} segundos. Hay alrededor de 3.1×10^{6} segundos en un año, por lo que esto significa que se necesitarían alrededor de 136 millones de años ¡para ello, este método!
Una gran cantidad de problemas matemáticos que surgen en las aplicaciones requieren una gran cantidad de la teoría y la potencia de cálculo considerable. Éste es un ejemplo.

Capítulo 8

Algunas estrategias de solución

Este capítulo incluye algunas estrategias para resolver el Pyraminx, el Cubo de Rubik $2 \times 2 \times 2, 3 \times 3 \times 3$, y el $4 \times 4 \times 4$. Es bueno practicar: en palabras de Aristóteles, *'Lo que tenemos que aprender a hacer, lo aprendemos haciéndolo'*. Además, se analizan algunas de las ideas matemáticas detrás de los algoritmos utilizados para resolver el Cubo de Rubik. El método favorito de Joyner consiste en aplicar un poco de teoría de grupos (véase 8.3 más adelante).
Para la notación utilizada en algunas de las siguientes secciones, véase el capítulo 2. Una gran fuente en línea de soluciones de muchos puzzles de permutación esta en el sitio web de Jaap Scherphuis, [Sch].

8.1 Una estrategia para resolver el Cubo de Rubik $2 \times 2 \times 2$

Figura 8.1

Mecánicamente es más complicado que su antecesor $(3 \times 3 \times 3)$ pero es más fácil de resolver ya que el número de movimientos se reduce considerablemente. Podemos considerar que el cubo $2 \times 2 \times 2$ está compuesto por las cuatro esquinas de un $3 \times 3 \times 3$ por lo que su solución es similar a la de las esquinas de este cubo.

Muchos de los movimientos que se van a mostrar también son utilizados en el Cubo de Rubik $3 \times 3 \times 3$, la resolución del cubo $3 \times 3 \times 3$ es más fácil que la del cubo $2 \times 2 \times 2$. A partir de cualquier configuración, nuestro primer objetivo es conseguir una primera carita (blanca) en la parte superior, buscaremos caritas blancas y las moveremos hacia la cara superior de tal manera que cada arista este bien posicionada y orientada.

Elegimos el subcubo en el que se encuentra la carita blanca y la arista verde *(figura 8.2),* buscamos el otro subcubo en el que se encuentren las otras caritas (blanca y verde), enseguida posicionamos el subcubo tal que formemos una diagonal verde *(figura 8.3)* y realizamos el movimiento $DFD^{-1}F^{-1}$ *(figura 8.4)* (tomando el cubo de forma que la diagonal se encuentre en la cara frontal)

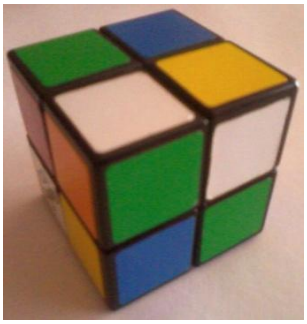


Figura 8.2

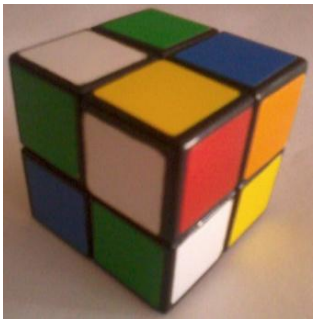


Figura 8.3

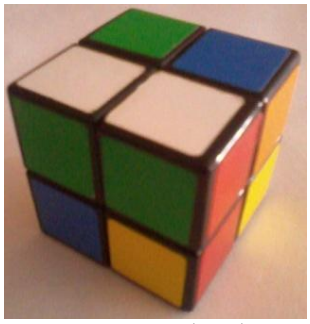


Figura 8.4 $DFD^{-1}F^{-1}$

El paso siguiente será buscar el subcubo que contenga las caritas blanca y roja, y repetimos el paso anterior, hasta completar la cara superior, como se muestra en las siguientes figuras:

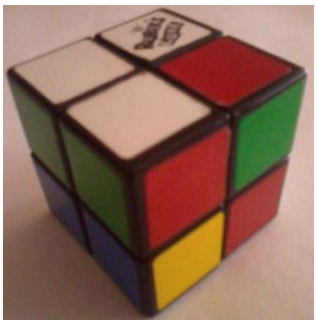


Figura 8.5

Figura 8.6

Figura 8.7 $DFD^{-1}F^{-1}$

Figura 8.8

Figura 8.9

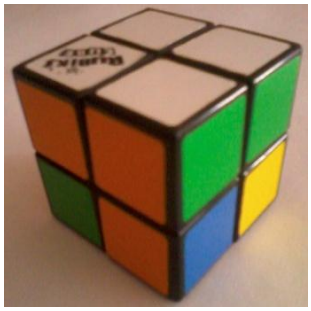


Figura 8.10

Ahora deseamos conseguir la cara inferior de forma que las aristas estén bien orientadas y terminar con la resolución del Cubo de Rubik.

Giramos el cubo y debemos conseguir una carita azul (por lo menos una) en la cara inferior, en caso de que no tengamos una carita azul en la cara inferior realizamos lo siguiente:

Tomando el cubo de forma que la cara blanca sea la cara superior, la cara frontal puede ser cualquier lateral de nuestro cubo, aplicamos $R^{-1}D^{-1}R$, luego giramos el cubo 90° en sentido horario (la cara frontal cambia a la izquierda) y aplicamos $LD^{-1}L^{-1}$, giramos el cubo 90° en sentido antihorario (volvemos al principio) y finalmente realizamos el movimiento $R^{-1}DR$.
Los movimientos anteriores nos permiten ir cambiando la posición de las caritas en la cara inferior sin modificar la cara superior, realizamos los movimientos anteriores tantas veces sea necesario hasta conseguir al menos una carita azul en la cara inferior.

En este ejemplo nuestro subcubo contiene la arista anaranjada y verde, el siguiente paso será fijar el subcubo en la posición que le corresponda *(ver figura 8.12)*, en mi caso realizo el movimiento U.

Figura 8.11

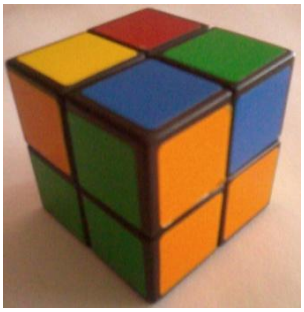


Figura 8.12

Nuestro siguiente objetivo será posicionar los 3 subcubos de la cara inferior en su esquina correcta:

Caso 1: Si los 3 subcubos están bien posicionados pero mal orientados realizamos los siguientes pasos:
Tomamos el cubo de forma que la cara blanca sea la cara inferior y el subcubo que está bien orientado se encuentre en la esquina superior izquierda y aplicamos $R^{-1}D^{-1}RD$ hasta conseguir una carita azul en la cara superior, enseguida realizamos el movimiento U y vamos alternando los dos movimientos anteriores hasta completar el Cubo de Rubik $2 \times 2 \times 2$.

Caso2: Al observar las siguientes figuras nos encontramos en el caso 2, es decir, dos de los subcubos están mal posicionados, por lo que nuestra primer tarea será posicionarlos y luego orientarlos, para esto tomamos el cubo de tal forma que el subcubo que está bien orientado se encuentre en la parte superior izquierda *(ver figura 8.16)*, y realizamos el siguiente movimiento:

$$\boldsymbol{U^{-1}R^2B^2RFR^{-1}B^2RF^{-1}R}$$

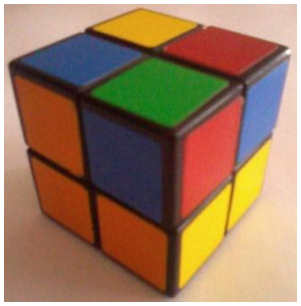


Figura 8.13
Mal posicionado

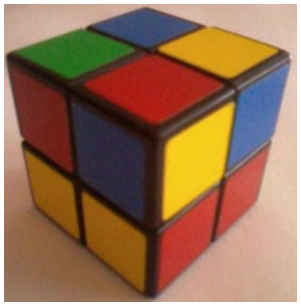


Figura 8.14
Bien posicionado

Figura 8.15
Mal posicionado

Figura 8.16

Y regresamos el subcubo bien orientado a su posición, en nuestro ejemplo aplicamos U^{-2} con esto conseguimos que nuestros tres subcubos estén mal posicionados *(figura 8.17)*,

Figura 8.17

Figura 8.18
Mal posicionado

Figura 8.19
Mal posicionado

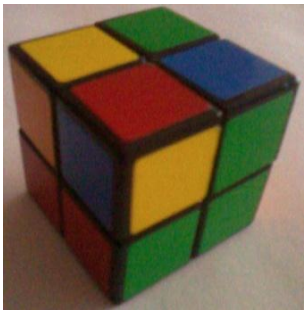


Figura 8.20
Mal posicionado

en este ejemplo debemos "permutar" las 3 esquinas

Figura 8.21

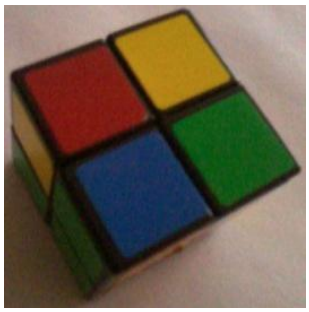


Figura 8.22

y lo haremos con el siguiente movimiento, tantas veces como sea necesario hasta que posicionemos los 3 subcubos, para esto tomamos el cubo de tal forma que el subcubo que está bien orientado se encuentre en la parte superior izquierda y realizamos :

$$\boldsymbol{R^2B^2RFR^{-1}B^2RF^{-1}R}$$

Ya tenemos todas las esquinas bien posicionadas, es decir nuestros 3 subcubos están bien posicionados

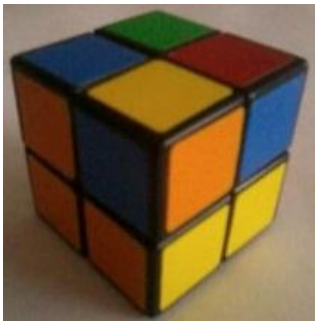


Figura 8.23
Bien posicionada

Figura 8.24
Bien posicionada

Figura 8.25
Bien posicionada

por lo que realizamos los pasos del caso 1 y terminamos.

Figura 8.26

Figura 8.27

Figura 8.28

Figura 8.29

Figura 8.30

Figura 8.31

8.2 Una estrategia para resolver el Cubo de Rubik $3 \times 3 \times 3$

Se recomienda que la persona que nunca ha 'jugado' con el Cubo de Rubik y quiere seguir la estrategia que se indica a continuación primero aprenda a 'jugar un movimiento' sin mirar el cubo. ¿Por qué? Pensemos en el cubo como un instrumento musical tal como una guitarra. Para tocar música en la guitarra, debemos saber cómo mirar la partitura y tocar sin tener que mantener constantemente la mirada en los dedos. El cubo es similar: en el inicio, queremos ser capaces de hacer un movimiento como $F^2 \cdot L^2 \cdot U^2 \cdot (F^2 \cdot L^2)^3 \cdot U^2 \cdot L^2 \cdot F^2$ sin tener que mantener constantemente la mirada en las manos. Esto nos ayudará a ser más rápidos y reducir los errores frustrantes.

Una forma de resolverlo es el **método esquina-arista**. La idea básica es como sigue.

- Ignorando orientaciones, es decir, giros y flips, primero resolver los subcubos esquina. Esto quiere decir, asegurarse de que los subcubos esquinas coincidan con los subcubos centro.

- Ignorando orientaciones, es decir, giros y flips, en segundo lugar resolver los subcubos arista. Esto significa, asegurarse de que las aristas salvo posibles giros coincidan con los subcubos centro.

- Fijar las orientaciones esquina, es decir, los giros de los subcubos esquina. Ahora todas las esquinas están totalmente resueltas.

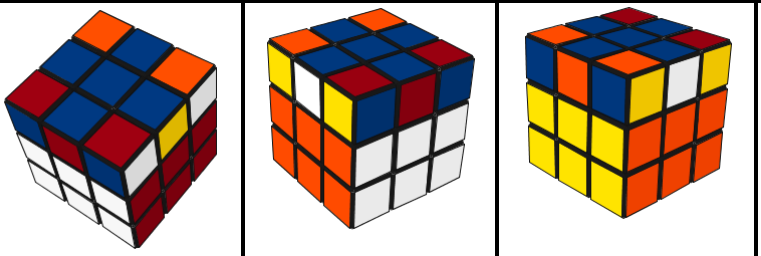
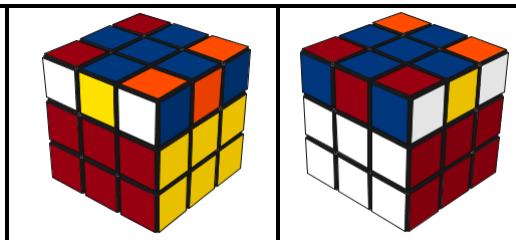
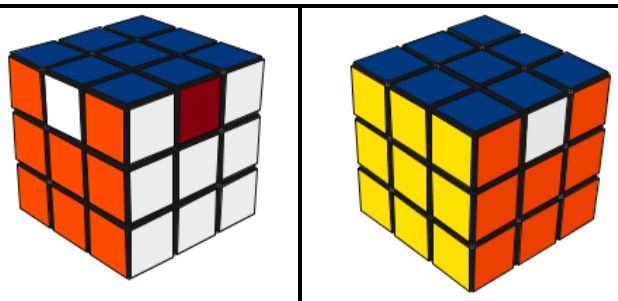
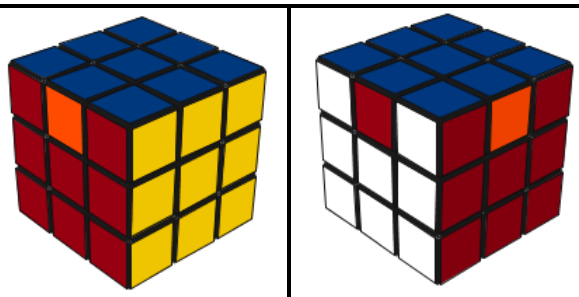
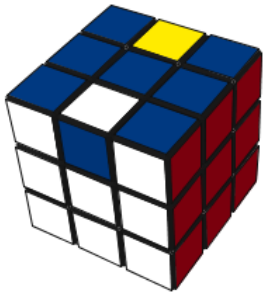
- Fijar las orientaciones arista, es decir, flips de los subcubos arista. Ahora el cubo está resuelto.

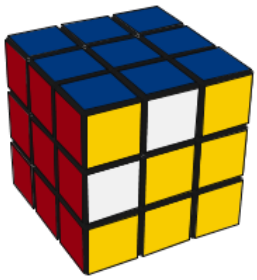
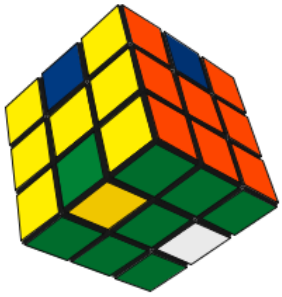
Para completar, menciono otro método. La estrategia es la solución **método de capas** que se compone de 3 etapas.

- Resolver la cara superior y aristas superiores.
- Resolver las aristas medias (y las aristas inferiores de la mejor manera posible).
- Resolver las esquinas inferiores y las aristas inferiores (si es necesario).

No hay nada malo con este método, pero no vamos a hablar más de este método. Es recomendable aprender ambos métodos.

8.2.1 Estrategia para resolver el cubo

Movimiento	***Efecto***
$\boldsymbol{U \cdot F \cdot [R, U]^3 \cdot F^{-1}}$	intercambia las esquinas (ubr, ufl) y permutas las aristas (uf, ul, ub, ur),
	
$\boldsymbol{M_R^2 \cdot U^{-1} \cdot M_R^{-1} \cdot U^2 \cdot M_R \cdot U^{-1} \cdot M_R^2}$	arista 3-ciclo (uf, ul, ur)
	
$\boldsymbol{(M_R \cdot U)^3 \cdot U \cdot \left(M_R^{-1} \cdot U\right)^3 \cdot U}$	flips las aristas superiores uf, ub
	

$(R^2 \cdot U^2)^3$	permuta (uf, ub), (fr, br)
	
$(M_R \cdot U)^4$	flips ub, ul, y flips df, db
  	
$(R^{-1} \cdot D^2 \cdot R \cdot B^{-1} \cdot U^2 \cdot B)^2$	$ufr+, bld++$
  	
$[R, U]^3 = (R \cdot U \cdot R^{-1} \cdot U^{-1})^3$	permuta (ufr, dfr), (ubr, ubl)
  	
$F^2 \cdot L^2 \cdot U^2 \cdot (F^2 \cdot L^2)^3 \cdot U^2 \cdot L^2 \cdot F^2$	permuta (uf, ub), (ur, ul)
	

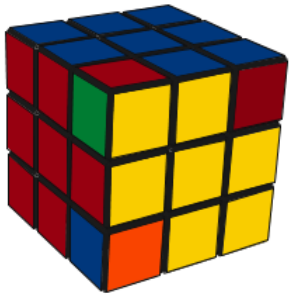
$\left(\boldsymbol{M_R^2 \cdot U \cdot M_R^2 \cdot U^2}\right)^{\boldsymbol{2}}$	permuta (ufl, ubr), (ufr, ubl)
	
$\boldsymbol{R \cdot D \cdot R^{-1} \cdot U \cdot R \cdot D^{-1} \cdot R^{-1} \cdot U^{-1}}$	Esquina 3-ciclo (brd, urb, ulb)
	

Tabla 8.1 Movimientos esquina y arista, ver [Si]

.

8.3 El método de subgrupo

Un enfoque para resolver el Cubo de Rubik usando una computadora es construir una cierta secuencia de subgrupos

$$G_n = \{1\} \subset G_{n-1} \subset \ \ldots \subset G_1 \subset G_0 = G,$$

donde $G = \langle R, L, F, B, U, D \rangle$ es el grupo de Cubo de Rubik, que permite implementar la siguiente estrategia:

- Representar a una posición dada del Cubo de Rubik por un elemento $g_0 \in G$.
- Determinar un conjunto completo de representantes de la clase lateral G_{k+1}/G_k:

$$G_{k+1}/G_k \ = \bigcup_{i=1}^{r_k} g_{k+1,i}\, G_{k+1}\,, \qquad \text{algunos } r_k > 1, \forall\ 0 \leq k < n$$

  (note $m_{n-1} = 1, g_{n,1} = 1$).

- (Paso 1) Si $g_0 \in g_{1,i} G_1$ (donde $i \in \{1, \ldots, n_1\}$) entonces sea $g_1 = g_{1,i}$ y $g'_1 = g_1^{-1} g_0$ (note $g'_1 \in G_1$).
- (Paso inductivo) $g'_k \in G_k$ se ha definido y si $g'_k \in g_{k+1,j}\, G_k$ (donde $j \in \{1, \ldots, n_1\}$), entonces sea $g_{k+1} = g_{k+1,j}$ y $g'_{k+1} = g_{k+1}^{-1}\, g'_k$ (note $g'_{k+1} \in G_{k+1}$).

- Colocando todo esto junto, se obtiene $1 = g_n^{-1} g_{n-1}^{-1} g_{n-2}^{-1} \dots g_1^{-1} g_0$, puesto que

$$g_0 = g_1 g_2 \cdots g_{n-1} g_n.$$

La esperanza es ser capaz de elegir la secuencia de los subgrupos G_i de tal manera que los representantes de las clases laterales son movimientos cortos y relativamente simples en el Cubo de Rubik de modo que la 'solución' $g_0 = g_1 g_2 \dots g_{n-1} g_n$ no sea demasiado larga.

8.3.1 Ejemplo: El método de la esquina-arista

Ahora se presenta un ejemplo-un poco sofisticado. Sea G_1 el subgrupo que no permuta las esquinas, sea G_2 el subgrupo que no permuta las esquinas o aristas, Sea G_3 el subgrupo que no permuta las esquinas o aristas y no reorienta cualesquiera esquinas, y sea $G_4 = \{1\}$:

$$G_4 = \{1\} \subset G_3 \subset G_2 \subset G_1 \subset G_0 = G.$$

Esta elección de los subgrupos aproximadamente corresponde con el método de la esquina arista descrito en Singmaster (ver [Si]).
La idea es simple.

1. Representar a una posición dada del Cubo de Rubik por un elemento $g_0 \in G$.

2. Sea g_1 el movimiento el cual mueve todas las esquinas a las posiciones correctas (es decir, las permutar hacia la posición resuelta y posiblemente las gira), así que $g_1^{-1} g_0 \in G_1$. Sea $g'_1 = g_1^{-1} g_0$.

3. Sea g_2 el movimiento el cual mueve todos las aristas hacia las posiciones correctas (es decir, las permuta en la posición resuelta y posiblemente reorienta esquinas y aristas) y deja todas las otras piezas sin permutar, así que $g_2^{-1} g'_1 \in G_2$. Sea $g'_2 = g_2^{-1} g'_1$.

4. Sea g_3 el movimiento que 'resuelve' todos las esquinas (es decir, gira todas ellas en una orientación correcta y puede voltear algunas aristas), pero no permuta cualesquiera piezas, así que $g_3^{-1} g'_2 \in G_3$. Sea $g'_3 = g_3^{-1} g'_2$.

5. Sea g_4 el movimiento que 'resuelve' todos las aristas (es decir, voltea a todas en la orientación correcta) y deja todas las otras caras fijas.

6. La 'solución' es $g_0 = g_1 g_2 g_3 g_4$.

8.3.2 Ejemplo: método de Thistlethwaite

Morwen Thistlethwaite (un matemático y un antiguo colega de David Singmaster) desarrolló uno de los mejores métodos de subgrupo para resolver el cubo (ver [FS]). Él toma

$$G_1 = \langle R, L, F, B, U^2, D^2 \rangle, \quad G_2 = \langle R, L, F^2, B^2, U^2, D^2 \rangle, \quad G_3 = \langle R^2, L^2, F^2, B^2, U^2, D^2 \rangle, \quad G_4 = \{1\}.$$

G_2 es isomorfo al grupo de Rubik Domino $3 \times 3 \times 2$. Su orden es $(8!)^2 \cdot 12$ de acuerdo con Frey- Singmaster [FS], G_3 es el grupo de los 'cuadrados'. Su orden es $2^{13} \cdot 3^4$ [FS].

Figura 8.32 *Rubik Domino*

Thistlethwaite demostró (con ayuda de una computadora) los siguientes hechos.

- Hay un conjunto completo de representantes de las clases laterales $\{g_{1,i} \mid 1 \leq i \leq n_1\}$ de G/G_1 tal que cada $g_{1,i}$ tiene a lo más 7 movimientos largos (y $n_1 = 2048$). Este conjunto de movimientos voltea aristas solamente.

- Hay un conjunto completo de representantes de las clases laterales $\{g_{2,i} \mid 1 \leq i \leq n_2\}$ de G_1/G_2 tal que cada $g_{2,i}$ tiene a lo más 13 movimientos largos (y $n_2 = 1082565$). Este conjunto de movimientos gira esquinas solamente.

- Hay un conjunto completo de representantes de las clases laterales $\{g_{3,i} \mid 1 \leq i \leq n_3\}$ de G_2/G_3 tal que cada $g_{3,i}$ tiene a lo más 15 movimientos largos (y $n_3 = 29400$). Este conjunto de movimientos pone todos los subcubos arista y subcubos esquina en la posición correcta.

- Hay un conjunto completo de representantes de las clases laterales $\{g_{4,i} \mid 1 \leq i \leq n_4\}$ de G_3/G_4 tal que cada $g_{4,i}$ tiene a lo mas 17 movimientos largos (y $n_4 = 663552$). ´

Por lo tanto, el Cubo de Rubik puede ser resuelto a lo más en $7 + 13 + 15 + 17 = 52$ movimientos. Las mejoras más recientes sobre este método han reducido este número (ver la página de Wikipedia [Wi] en las 'soluciones óptimas para el Cubo de Rubik' y [Lo] para detalles y actualizaciones recientes).

8.4 Una estrategia para resolver el Cubo de Rubik $4 \times 4 \times 4$

Es importante saber armar el cubo $3 \times 3 \times 3$ ya que muchos de los movimientos para resolver el cubo $4 \times 4 \times 4$ los obtenemos del Cubo de Rubik $3 \times 3 \times 3$.
Preparamos el cubo $4 \times 4 \times 4$ (*ver figuras 8.33 y 8.73*) para después resolverlo como si fuese el Cubo de Rubik $3 \times 3 \times 3$.

8.4.1 Conseguir las 6 caras centrales

En el Cubo de Rubik $3 \times 3 \times 3$ la cara central indicaba el color de cada cara, ahora en él $4 \times 4 \times 4$ la "*cara central*" van a ser 4 caritas (lo que antes era una, ahora son 4 caritas), a

diferencia del cubo 3 × 3 × 3 las caras de en medio si se pueden mover, debemos obtener 4 caritas blancas para conseguir una "*cara central*".

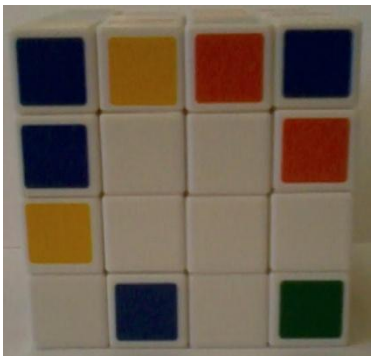


Figura 8.33 *Cara central*

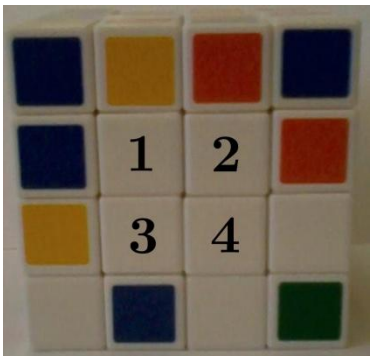


Figura 8.34 *Posiciones*

Conseguimos líneas

Desde este momento la "*cara central*" elegida a completar será la blanca, buscamos una carita blanca en cualquiera de las caras del cubo que este en cualquiera de las posiciones 1, 2, 3 o 4 (*ver figura 8.34*), luego giramos el cubo de manera que la cara central blanca que deseamos completar se encuentre en la cara superior de nuestro cubo.

Enseguida explicaré como obtener las 4 caritas blancas partiendo de cualquiera de las configuraciones de mi cubo, es importante mencionar que dependiendo de cada configuración serán los movimientos, pero esto depende de que carita elijamos, hay varios movimientos que podemos realizar dependiendo de en qué posición estén nuestras caritas blancas y si te encuentras con alguna otra posición los movimientos son análogos.

Observando la *figura 8.35* encuentro una carita blanca en la posición 4 (*ver figura 8.34*)

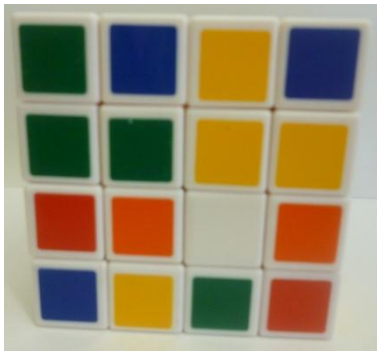


Figura 8.35

Busco una carita blanca en cualquiera de las caras laterales, en este caso la carita blanca sobre mi cara lateral se encuentra en la posición 1 (*figura 8.36*), giro la cara superior en sentido horario un cuarto de vuelta (*figura 8.37*), es decir realizo el movimiento *U* (ver [Si]), ahora mis dos caritas blancas se encuentran en la misma rodaja (*figura 8.38*).

Figura 8.36

Figura 8.37 *Movimiento U*

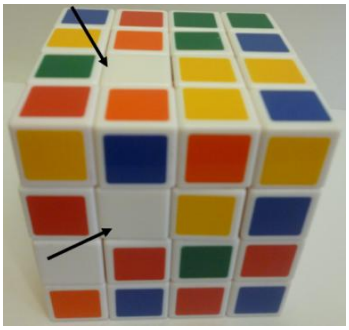


Figura 8.38

Ahora realizo el movimiento H_L^{-1} (ver notación en 2.3.3) que me permite mover la carita blanca que se encuentra en la cara frontal a la cara superior (*figura 8.39*).
Ahora la carita blanca ya se encuentra en la cara superior, pero recordemos que está sobre la misma rodaja, debemos girar la cara superior de manera que nuestra carita blanca no esté sobre la misma rodaja o sobre la misma línea que nuestra primera carita blanca elegida (*figura 8.35*), podemos realizar cualquiera de los siguientes movimientos U o U^{-2} yo elegiré U^{-2} (*figura 8.40*), luego regreso la mitad izquierda, es decir aplico el movimiento inverso H_L lo que me permite obtener una línea blanca, es decir ahora las caritas blancas se encuentran en las posiciones 3 y 4 (*figura 8.41*).

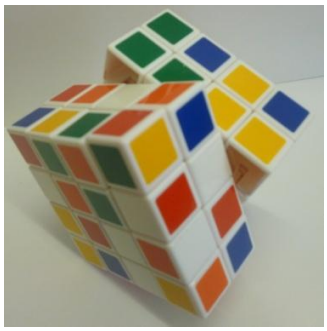


Figura 8.39 *Movimiento* H_L^{-1}

Figura 8.40

Figura 8.41

Enseguida busco una tercera carita blanca en cualquiera de las caras laterales, una vez elegida la carita giramos la cara superior de manera que las tres caritas blancas estén sobre la misma rodaja y repito el proceso anterior, en mi caso podemos observar en la *figura 8.43* que mis 3 caritas se encuentran en la mitad derecha, por lo que aplicaré el mismo proceso sólo cambiaré el subíndice que indicará que el movimiento afectará a la mitad derecha, aplicamos $H_R\ U^{-2}H_R^{-1}$.

Figura 8.42

Figura 8.43

Figura 8.44

Finalmente busco la cuarta carita blanca en las caras laterales, en este caso mi cuarta carita blanca se encuentra en la cara inferior en la posición 1, lo más recomendable es mover la carita blanca a una de las caras laterales del cubo, para lograrlo realicemos lo siguiente:

Giramos la cara superior de tal manera que dos de las caritas blancas que se encuentran en dicha cara estén sobre la misma rodaja que la cuarta carita blanca para lograrlo aplico U^2 luego aplicamos el movimiento H_L^{-1} , ahora la cuarta carita blanca se encuentra en la cara frontal en la posición 1 (*ver figura 8.45*) pero recordemos que la cuarta carita sigue sobre la misma rodaja que las otras 2 caritas blancas, por lo que el siguiente paso será aplicar F de esta manera la cuarta carita ya no está sobre la misma rodaja, ahora se encuentra en la posición 2 de la cara frontal, finalmente regresamos la mitad izquierda, es decir aplicamos H_L.

Perfecto, ahora nuestra cuarta carita blanca se encuentra en la cara frontal es decir en una de las caras laterales ¡como queríamos!

Enseguida giramos la cara superior del cubo de manera que alguna de las líneas blancas este sobre la misma rodaja que nuestra cuarta carita blanca, en mi caso aplicamos U (*ver figura 8.46*), es importante elegir la línea blanca correcta, ¿a qué me refiero con esto? Debemos elegir la línea blanca de forma que ésta al estar sobre la misma rodaja que la cuarta carita blanca y al realizar el movimiento H_R se forme una línea blanca nuevamente sobre la cara superior *(ver figura 8.49)* y no una diagonal como se ve en la *figura 8.47.*

Por lo que si elegimos la línea blanca que se observa en la *figura 8.46* fracasaríamos al obtener una diagonal, la elección correcta es la línea blanca de la *figura 8.48.*

Pero, ¿cómo conseguimos la línea blanca de la *figura 8.48*? Es muy sencillo, partiendo de la configuración de mi cubo en la *figura 8.46* sólo giro la cara superior, puedo aplicar U^{-1}o U^3 *y* obtengo la configuración de la *figura 8.48.*

Figura 8.45

Figura 8.46

Figura 8.47 *Diagonal*

El paso siguiente es aplicar H_R y obtenemos la línea blanca que tanto deseábamos. Finalmente aplicamos U^{-1} (*ver figura 8.50*) y regresamos la mitad derecha, es decir aplicamos H_R^{-1} lo que nos permite obtener la "*cara central*" blanca (*ver figura 8.52)*.

Figura 8.48

Figura 8.49 *Línea blanca*

Figura 8.50

Figura 8.51

Figura 8.52

Para completar el resto de caras centrales debemos memorizar como están colocadas las caras laterales.

Hay diferentes posiciones en los colores de cada cara, en el capítulo 2 proporcionamos los colores de cada cara del cubo, en este caso como estamos empezando por completar la cara central blanca, el paso siguiente será completar las caras centrales en el siguiente orden de aparición: la cara central Roja (que en este caso será la cara frontal), la cara central Verde (que en este caso será la cara izquierda), la cara central Azul (que en este caso será la cara derecha) la Anaranjada (que en este caso será la cara posterior) y finalmente Amarilla (que en este caso será la cara inferior).

Es decir rotamos el cubo de manera que la cara central blanca este en la parte superior, en la cara frontal debemos completar la cara central roja, en la cara izquierda debemos completar la cara central verde, en la cara derecha completamos la cara central azul, en la cara posterior debemos completar la cara central anaranjada y automáticamente se completará la cara central amarilla *(ver figuras 8.53, 8.54 y 8.55)*, ¿cómo las completamos? Siguiendo los mismos pasos que realizamos para completar la cara central blanca, siempre siguiendo el orden, cara central blanca (su opuesta será la cara central amarilla), roja-anaranjada, y verde- azul.

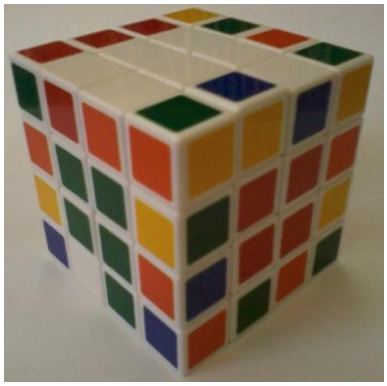


Figura 8.53

Figura 8.54

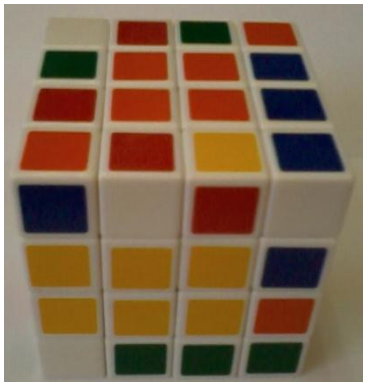


Figura 8.55

Figura 8.56

Figura 8.57

Figura 8.58

Figura 8.59

8.4.2 Colocación de las aristas (cubitos medios, es decir los 2 cubitos que se encuentran entre los subcubos esquina)

El paso siguiente será colocar y orientar las 12 aristas, debemos tener en cuenta que al usar las palabras "colocar y orientar aristas" en este caso me refiero a colocar y orientar siempre en parejas (cubitos medios, *ver figura 8.73)*.

El primer paso será elegir una par de aristas, por ejemplo en la *figura 8.60* elegimos dos aristas A y B (caritas roja y amarilla), notamos que las dos aristas se encuentran sobre la misma rodaja, debemos preparar el cubo de forma que las aristas A y B se encuentren sobre una de las diagonales *(ver figuras 8.62 y 8.64)* para esto apliquemos el movimiento $F^{-1}LDF^2$.

Nota: $F^{-1}LDF^2$ también nos permite mover 2 aristas a una misma rodaja en el caso de que éstas se encuentren sobre una de las diagonales.

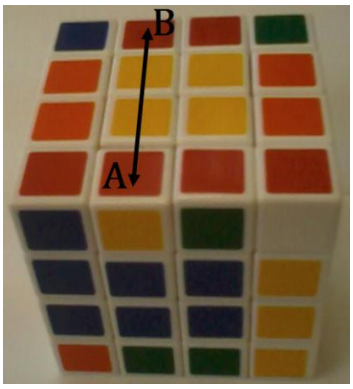


Figura 8.60

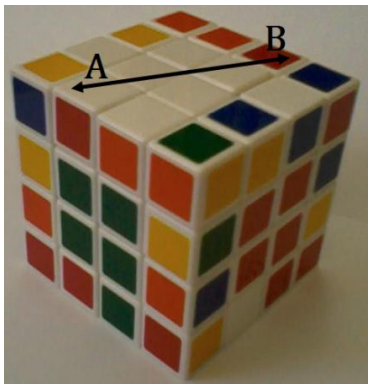


Figura 8.61 *Diagonal*

Cada que elijamos un par de aristas no debemos olvidar ubicarlas sobre alguna de las diagonales *(ver figuras 8.62 y 8.64),* agrego el algoritmo a realizar en cada caso, el cual nos permite juntar las dos aristas A y B.

Es importante mencionar que al realizar el respectivo algoritmo (dependiendo del caso en que nos encontremos) una par de aristas siempre se afectan, en las siguientes figuras indico con una llave las aristas que separamos *(ver figura 8.63)* al realizar el algoritmo, por lo que, sólo debemos girar la cara izquierda o derecha, buscando posicionar en la cara inferior del cubo un par de aristas que aún no estén juntas y de esta forma no afectemos aristas que ya hemos completado.

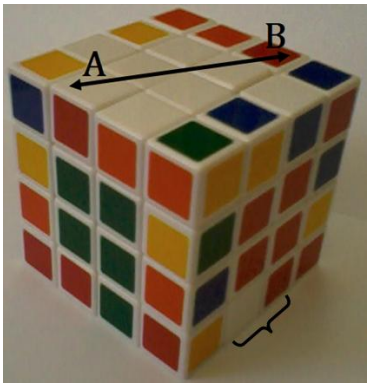


Figura 8.62
$H_R^{-1}U^{-1}R^{-1}UH_R$

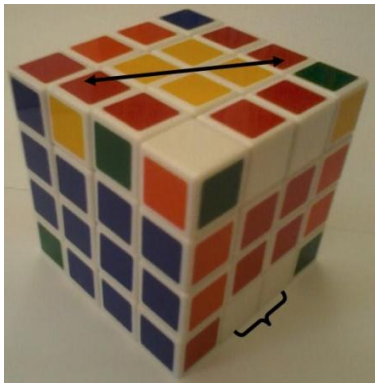


Figura 8.63

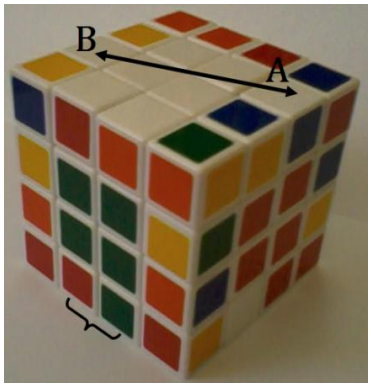


Figura 8.64
$H_LULU^{-1}H_L^{-1}$

Colocación del último par de aristas

Usando los algoritmos de las *figuras 8.62 y 8.64* completamos 10 aristas (*ver figuras 8.65, 8.66, 8.67 y 8.68)*, al final siempre nos quedarán 2 aristas por completar, *ver figuras 8.69, 8.70 y 8.71* en mi caso las dos aristas que debo juntar se encuentran sobre la cara en la que se encuentra la *"cara central amarilla"*, un par de aristas que debo juntar tienen las caritas de color rojo y amarilla y el segundo par de aristas contiene las caritas de color verde y rojo, se puede observar que ambas parejas se encuentran sobre las diagonales, el paso siguiente será colocar

cada par de aristas sobre la misma rodaja (*recordar figura 8.60*) para lograrlo apliquemos $F^{-1}LDF^2$.
Nuestra siguiente tarea será aplicar el siguiente algoritmo:

$$\boldsymbol{H_L U L U^{-1} F U^{-1} F^{-1} U H_L^{-1}}$$

¡Por fin hemos terminado! Ya tenemos las 12 aristas completas, (*ver figura 8.73*).

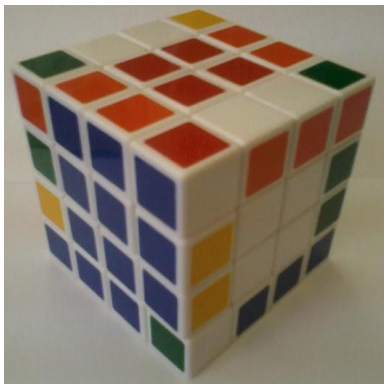


Figura 8.65

Figura 8.66

Figura 8.67

Figura 8.68

Figura 8.69

Figura 8.70

Figura 8.71

Figura 8.72 *Colocación del último par de aristas.*

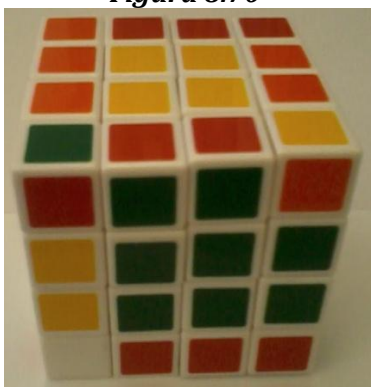


Figura 8.73 *Colocación de aristas*

Como había prometido en 8.4, ya habiendo preparado el cubo $4 \times 4 \times 4$ (ver 8.33 y 8.73) para después resolverlo como si fuese el Cubo de Rubik $3 \times 3 \times 3$.

8.4.3 Resolviendo el Cubo de Rubik $4 \times 4 \times 4$ como si fuese el Cubo de Rubik $3 \times 3 \times 3$.

A partir de este momento el lector podrá hacer uso de cualquier movimiento dado en 8.2.1 (Estrategia para resolver el cubo $3 \times 3 \times 3$, ver la tabla de movimientos esquina y arista), podemos empezar por completar cualquier cara, en mi caso empezaré por resolver la cara blanca *(ver figura 8.76)*, enseguida las aristas *(ver figuras 8.78 y 8.79)* y finalmente la cara amarilla *(ver figura 8.86)*.

Figura 8.74

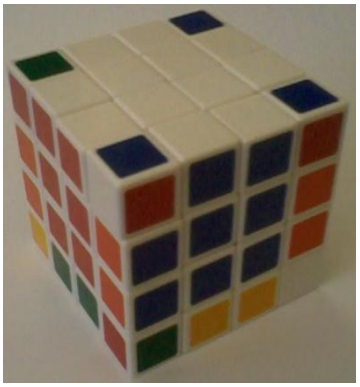


Figura 8.75

Figura 8.76

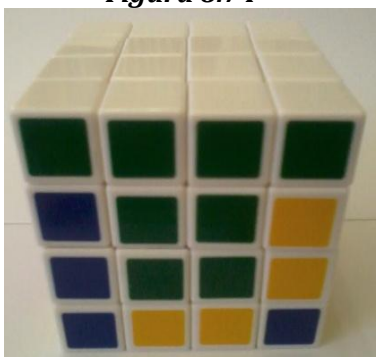


Figura 8.77

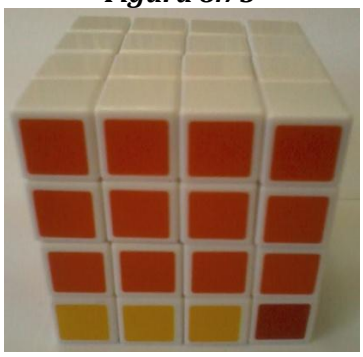


Figura 8.78

Figura 8.79

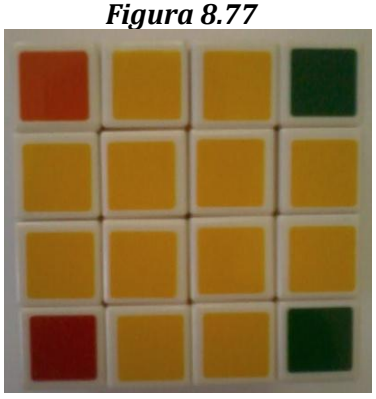


Figura 8.80

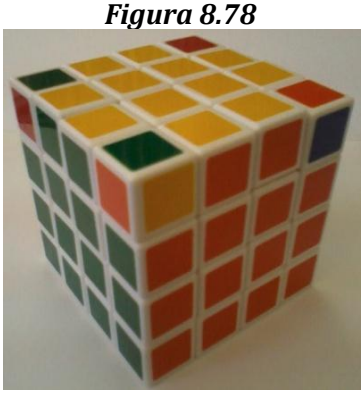


Figura 8.81

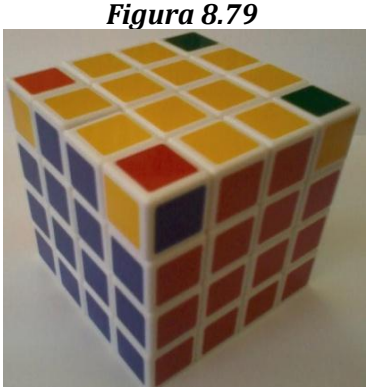


Figura 8.82

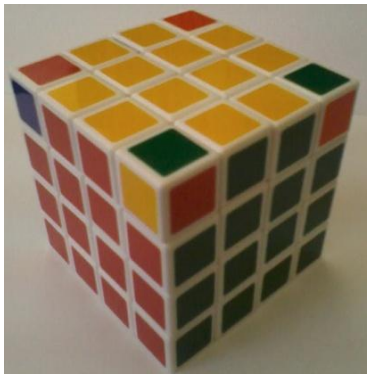


Figura 8.83

Figura 8.84

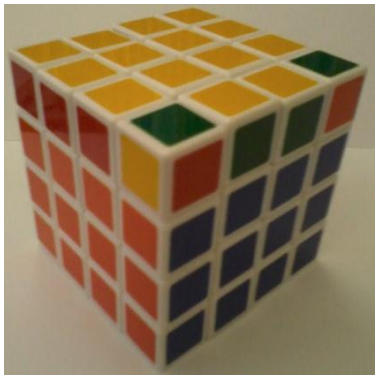


Figura 8.85

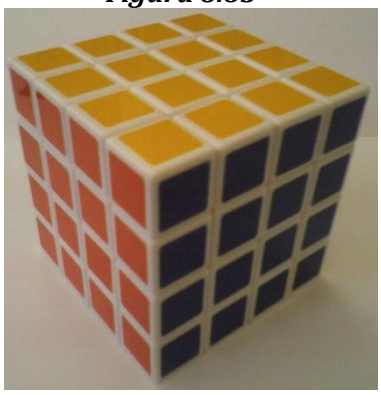


Figura 8.86

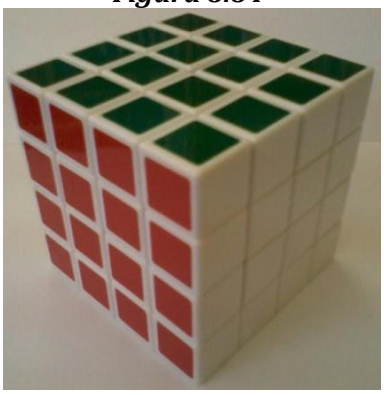


Figura 8.87

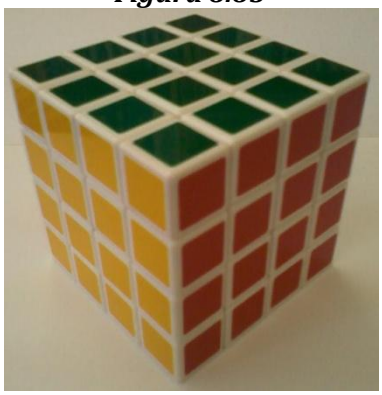


Figura 8.88

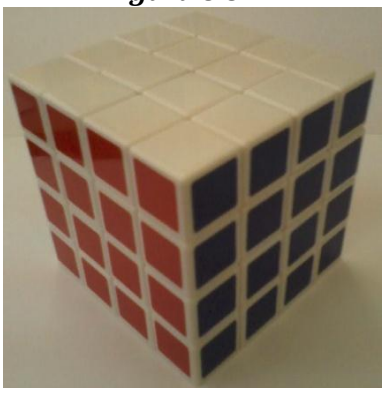


Figura 8.89

8.4.4 Paridad en el Cubo de Rubik $4 \times 4 \times 4$.

En este apartado revisaremos las paridades que presenta el cubo $4 \times 4 \times 4$, una de las características de éste cubo es que tiene un número par de capas, esta paridad se presenta en los cubos de lados pares.

Caso 1: Uno de los algoritmos que podemos necesitar al resolver la última capa del cubo $4 \times 4 \times 4$ es el que nos permite obtener la "cruz amarilla" *(ver figura 8.80)*, el caso que todos deseamos (por ser el más fácil) es que todas las caritas que forman la cruz sean amarillas, y el paso siguiente será aplicar algoritmos que nos posicionen las aristas y finalmente colocar las esquinas correctamente posicionadas y orientadas para terminar de resolver el cubo, ahora ¿qué pasa si no consigo que todas las caritas sobre mi cruz sean amarillas como en la *figura 8.80?*

La respuesta es, que el caso al que nos enfrentaríamos es el siguiente:

Al tratar de obtener la "cruz amarilla" podemos obtener 3 aristas bien orientadas y la cuarta arista bien posicionada pero mal orientada (en mi caso debo invertir los colores anaranjado y amarillo, *ver figura 8.90),* el siguiente algoritmo (ver notación en 2.3.3):

Figura 8.90

Figura 8.91

$$r^2B^2U^2lU^2r^{-1}U^2rU^2F^2rF^2l^{-1}B^2r^2$$

nos permite resolver ésta paridad, rotemos nuestro cubo de tal forma que la cuarta arista se encuentre en la posición uf (ver Ejemplo 1.2.7), al aplicar el algoritmo anterior lograremos orientar la cuarta arista (*ver figura 8.92)*.

Figura 8.92

Figura 8.93

Caso 2: Otra paridad con la que nos podemos encontrar al resolver la última capa del cubo $4 \times 4 \times 4$ es que obtengamos el cubo totalmente armado excepto dos esquinas consecutivas de una cara, que se encuentran en posiciones invertidas *(ver figuras 8.94 y 8.95)*.

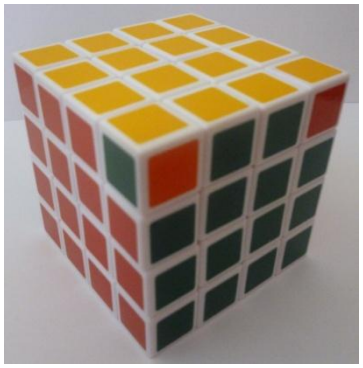


Figura 8.94

Figura 8.95

El primer paso para resolver esta paridad es rotar el cubo tal que las dos esquinas mal posicionadas se encuentren sobre la cara derecha y aplicamos el siguiente algoritmo:

$$\boldsymbol{r^2U^2r^2H_U^2r^2u^2}$$

tomando el cubo por la cara superior, rotarlo 90° en sentido antihorario y aplique lo siguiente

$$\boldsymbol{RU\ R^{-1}U^{-1}R^{-1}FR^2U^{-1}R^{-1}U^{-1}RUR^{-1}F^{-1}}.$$

El algoritmo anterior nos permite obtener 3 esquinas mal posicionadas *(ver figura 8.96)*, dejando el resto del cubo fijo que en este caso nos conviene porque ahora podemos utilizar el movimiento esquina 3-ciclo (brd, urb, ulb) visto en la tabla dada en 8.2.1, mimo que nos permitirá solucionar el puzzle.

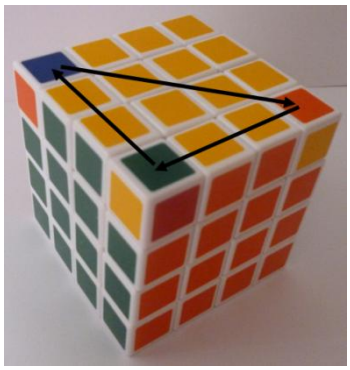


Figura 8.96

Figura 8.97

8.5 Una estrategia para resolver el Pyraminx

Supongamos que el tetraedro está sobre una superficie plana frente a nosotros. Las esquinas se denotan L (izquierda), R (derecha), U (superior) y B (parte posterior).

Los movimientos básicos son:

- ***L*** denota la rotación de 120 grados en sentido horario del subtetraedro de 2 niveles que contiene la esquina izquierda,
- ***R*** denota la rotación de 120 grados en sentido horario del subtetraedro de 2 niveles que contiene la esquina derecha,

- ***U*** denota la rotación de 120 grados en sentido horario del subtetraedro de 2 niveles que contiene la esquina superior,
- ***B*** denota la rotación de 120 grados en sentido horario del subtetraedro de 2 niveles que contiene la esquina posterior.

En primer lugar debemos orientar esquinas (puntas) de la cara elegida a completar, en mi caso primero completaré la cara amarilla *ver figura 8.98*), después orientamos la punta del tetraedro superior *ver figura 8.99* y finalmente resolvemos la parte media que desde este momento llamaremos aristas (como acostumbran los amantes de estos puzzles) *ver figura 8.100*.

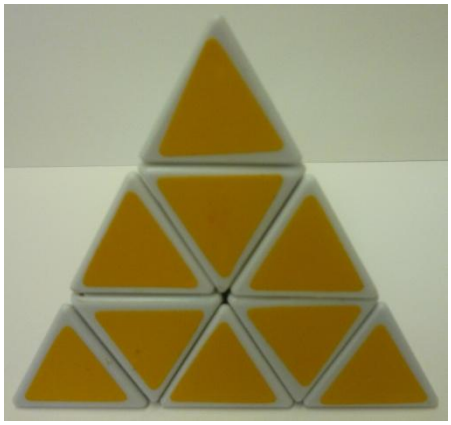


Figura 8.98

Figura 8.99

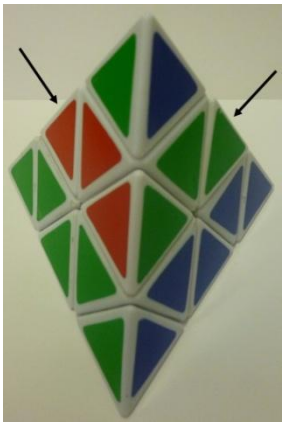


Figura 8.100 *Aristas*

Una vez que hemos resuelto la cara inferior (cara amarilla) y la punta del tetraedro superior, lo único que nos queda por hacer es resolver aristas. Recordemos que la primera cara que completamos fue la inferior (amarilla), por lo que, los colores para las demás caras serán el Azul (B), Rojo (R) y Verde (G). Revisemos 3 casos a los que podemos enfrentarnos:

Primer caso: En las *figuras 8.101 y 8.102* podemos observar que en la parte media cada cara contiene tres caritas del mismo color, por lo que sólo debemos girar el subtetraedro de 2 niveles que contiene la esquina superior hasta completar el Pyraminx.

Figura 8.101

Figura 8.102

BBB, RRR y GGG

También podemos obtener los colores de las 3 caritas de cada cara como en las *figuras 8.103 a la 8.107*, para resolverlas tomamos el puzzle de forma que cualquiera de las caras roja, verde o azul se encuentren frente a nosotros y aplicamos el siguiente movimiento que nos permite armar totalmente el Pyraminx $\boldsymbol{R^{-1}U^{-1}RU^{-1}R^{-1}U^{-1}R}$.

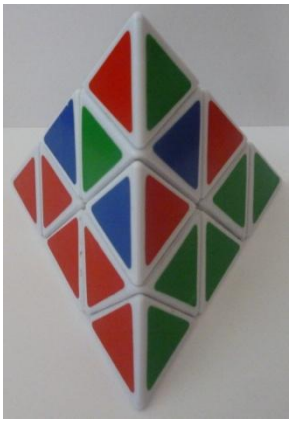


Figura 8.103 *BGB y RBR*

Figura 8.104 *GRG*

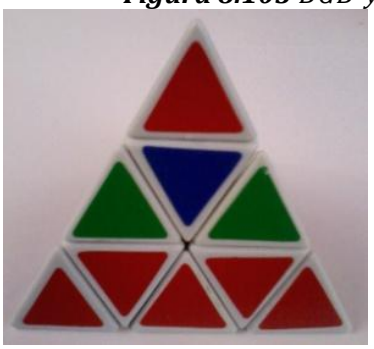


Figura 8.105 *GBG*

Figura 8.106 *BRB*

Figura 8.107 *RGR*

Segundo caso: Tenemos las 3 aristas mal posicionadas y orientadas, es importante mencionar que en este último caso tenemos 2 posibles caminos a seguir:

1: Las 3 aristas deben ser permutadas en sentido antihorario, ahora, observando el patrón que tenemos en la parte media:

En una cara tenemos 2 caritas iguales y la tercera de diferente color (*ver figura 8.108*), en otra cara 2 caritas iguales y la tercera de diferente color (*ver figura 8.109*), y en la tercer cara 3 caritas de diferente color (*ver figura 8.110*).

Rotamos el puzzle de forma que la cara que en la que se encuentren 2 caritas iguales y la tercera de diferente color, esté frente a nosotros, y la cara derecha contenga las 3 caritas de diferente color (*ver figura 8.113*), aplicando el siguiente algoritmo resolvemos el Pyraminx:

$$\boldsymbol{LRUR^{-1}U^{-1}L^{-1}}$$

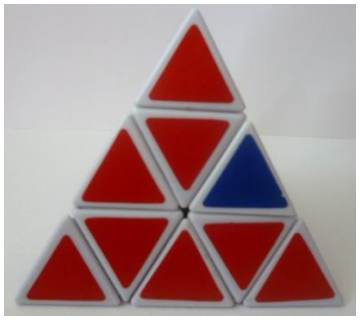


Figura 8.108

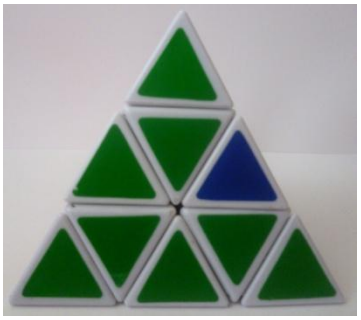


Figura 8.109

Figura 8.110

Figura 8.111

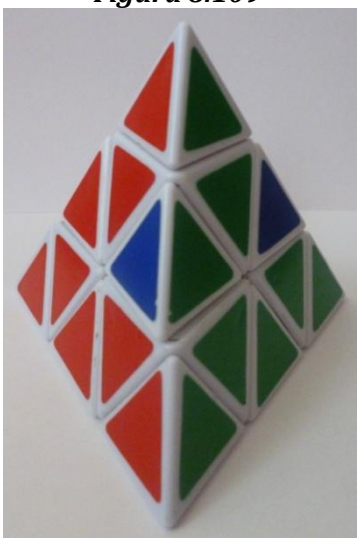


Figura 8.112

Figura 8.113

2: Es equivalente al caso 1, sólo que ahora las aristas deben ser permutadas en sentido horario, debemos rotar el puzzle de manera que la cara adyacente (la cara que contiene las 3 caritas de diferente color) se encuentre en el lado izquierdo, *ver figura 8.118*, finalmente aplicando el siguiente algoritmo tenemos el puzzle totalmente armado.

$$R^{-1}L^{-1}U^{-1}LUR$$

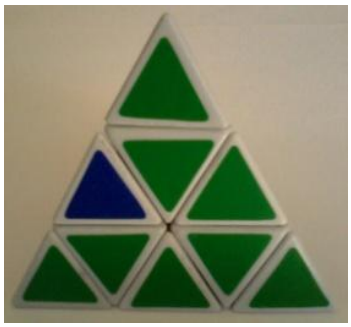


Figura 8.114

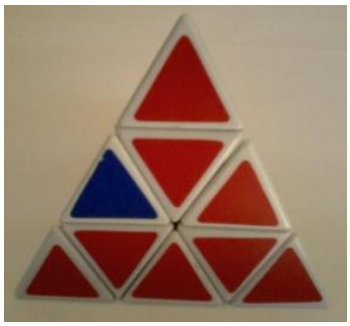


Figura 8.115

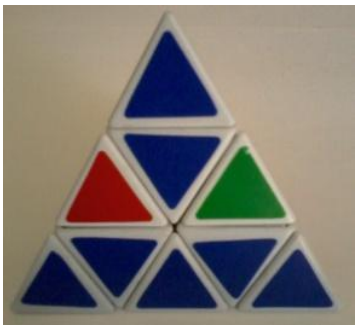


Figura 8.116

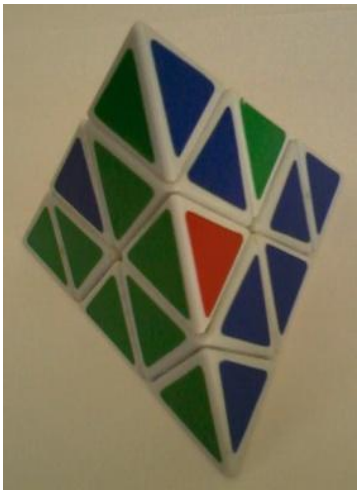


Figura 8.117

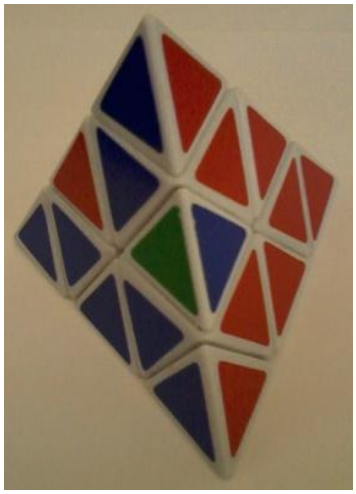


Figura 8.118

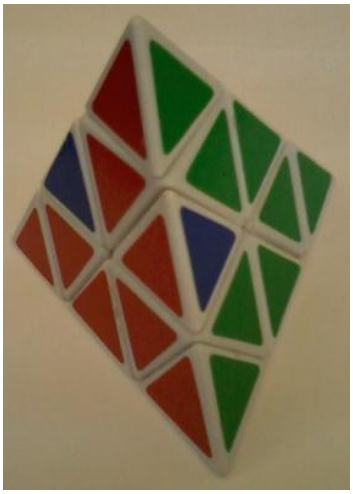


Figura 8.119

Tercer caso: Una arista fija (bien posicionada y orientada, *ver figura 8.120*) y dos que están bien posicionadas pero mal orientadas (están en su posición pero deben invertirse los colores *ver figuras 8.121 y 8.122*):

Rotamos el Pyraminx de forma que la cara en la que se encuentran las 2 aristas (de las cuales los colores de sus caritas deben ser invertidos) esté frente a nosotros y aplicamos el siguiente algoritmo que nos permite armar totalmente el Pyraminx:

$$\boldsymbol{R^{-1}UL^{-1}U^{-1}LU^{-1}RU.}$$

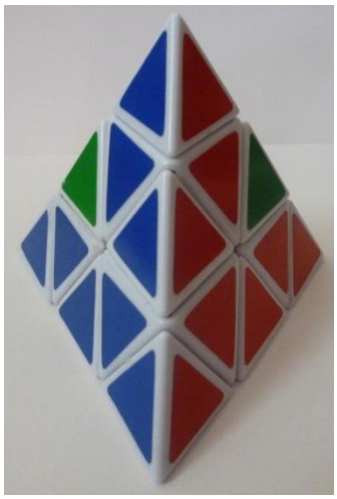


Figura 8.120

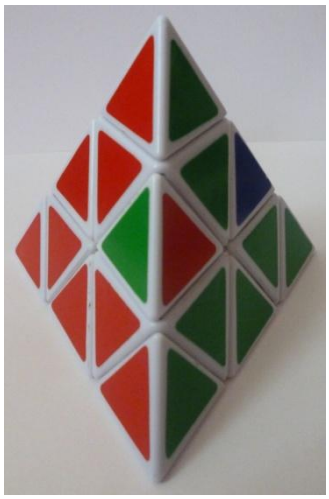


Figura 8.121

Figura 8.122

8.5.1 Estrategia para el Pyraminx usando conmutadores

En primer lugar, obtener las caritas "centro" resueltas, a continuación, girar las puntas para resolverlas y las caritas centrales. Por último, resolver las aristas, utilice los siguientes movimientos:

• $[R, U^{-1}]$ es un 3-ciclo de piezas arista sobre la cara URL,

• $[R, U^{-1}] * [R^{-1}, L]$es un giro (invertir colores de las etiquetas de cada arista) de dos aristas (arista UR y la arista UL) en la cara URL.

Anexo:

El orden del Grupo Cubo de Rubik (A. Frey y D. Singmaster, [FS])

¿Cuántas diferentes permutaciones del cubo hay, incluyendo orientaciones de arista y esquinas giros .

En primer lugar, ¿cuántas permutaciones de las ocho esquinas son posibles si ignoramos orientaciones? Sabemos que el número total de posibles permutaciones de un conjunto de n objetos en n ubicaciones es $n!$ Hemos encontrado un proceso el cual intercambia un solo par de esquinas, ignorando aristas, sin molestar a otras esquinas. Utilizando ya sea conjugados de este proceso o bien con distintas orientaciones del cubo, podemos intercambiar cualquier par de esquinas sin alterar a las otras. Puesto que toda permutación se puede descomponer en productos de transposiciones, toda permutación esquinas es posible en el cubo. Por lo tanto tenemos

$$8!=40{,}320$$

permutaciones posibles de esquinas en el cubo.

El mismo argumento muestra que hay $12! = 479\ 001\ 600$ permutaciones posibles de aristas en el cubo. Sin embargo, hemos visto que no todas las permutaciones de las esquina pueden ir con todas las permutaciones de las aristas. Las permutaciones de las esquinas y aristas juntas debe ser par, por lo que permutaciones esquina par deben ocurrir con permutaciones arista par e impar con impar. ¿Puede cada permutación par esquina ocurrir con cada permutación par arista? ¡Sí! Para ver esto se aplica el método anterior para obtener cualquier permutación par esquina. Esto producirá una permutación par arista que luego necesitamos para transformar a cualquier permutación par arista que deseemos, Esta transformación debe ser una permutación par arista la cual deja esquinas fijas. Cualquier permutación par arista, dejando esquinas fijas, se puede obtener usando ya sea 3 ciclos o parejas de 2 ciclos de aristas las cuales dejan esquinas fijas. Estos se pueden obtener como conjugados de cualquiera de

$$W = LR^{-1}F^2L^{-1}RU^2$$

o

$$V = (F^2R^2)^3$$

¿Puede cada permutación impar esquina ocurrir con cada permutación impar arista? ¡Sí! Podemos repetir el argumento anterior y de nuevo necesitamos obtener permutaciones pares arista que dejan esquinas fijas. Alternativamente, simplemente aplicamos cualquier giro de cara para transformar un caso impar-impar en un caso par-par, y utilizamos el argumento anterior. Dado que la mitad de las permutaciones son impares y la otra mitad son pares, se

observa que el número total de permutaciones del cubo sin contar orientaciones de esquinas y aristas es de

$$\frac{8! \cdot 12!}{2} = 9{,}656{,}672{,}256{,}000.$$

Ahora considerando orientaciones de esquinas y aristas. Cualquier esquina puede ser girada en tres orientaciones, a excepción de la última, cuya orientación está fijada por las otras siete. Del mismo modo cualquiera de las aristas se puede invertir en dos formas con excepción de la última, cuya orientación está determinada por la primeras 11. Por lo tanto cada permutación de los subcubos puede tener

$$\frac{3^8}{3} = 2{,}187$$

orientaciones esquina y

$$\frac{2^{12}}{2} = 2{,}048$$

orientaciones arista. Así, el número total de permutaciones del cubo contando orientaciones de esquinas y aristas es

$$\frac{8! \cdot 12!}{2} \cdot \frac{3^8}{3} \cdot \frac{2^{12}}{2} = 43{,}252{,}003{,}274{,}489{,}856{,}000$$

$$\approx 4.3 \times 10^{19}$$

Este es el orden del Grupo Cubo.

Teorema. El número de posibles posiciones del Pyraminx de Mèfferts es

$$\frac{6!}{2} \cdot 2^5 \cdot 3^8 = 75\ 582\ 720.$$

Prueba (Bandelow, [B1])**:** Cada giro de 120° de cualquier subtetraedro de segundo nivel causa un 3-ciclo arista, por lo tanto, una permutación par de las piezas arista. Por lo tanto, a lo sumo $\frac{6!}{2}$ posiciones para las 6 piezas arista son posibles. Por otra parte, cada giro de 120° de un subtetraedro de segundo nivel causa dos 3-ciclos disjuntos, por consiguiente una permutación par, para el conjunto de los 12 colores sobre las 6 piezas arista. Por lo tanto, en este conjunto también, obtenemos sólo permutaciones pares, lo que significa reorientamos una pieza arista como una transposición, por lo tanto, una permutación impar, es imposible. Por otra parte, las siguientes maniobras muestran que cada permutación par de piezas arista se puede realizar y que, en este proceso, 5 de 6 aristas pueden estar orientadas en 2^5. Las cuatro piezas núcleo pueden ser giradas arbitrariamente en 3^4 posiciones y lo mismo se aplica para las 4 puntas del Pyraminx 3^4.

El puzzle 14-15

La configuración original de Samuel Loyd Puzzle 14-15.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

puede ser cambiada en la siguiente configuración:

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

usando cuarenta y cuatro movimientos: Los siguientes números indican qué cuadrado (en orden) se debe colocar en el lugar vacío:
14, 11, 12, 8, 7, 6, 10, 12, 8, 7, 4, 3, 6, 4, 7, 14, 11, 15, 13, 9, 12, 8, 4, 10, 8, 4, 14, 11, 15, 13, 9, 12, 4, 8, 5, 4, 8, 9, 13, 14, 10, 6, 2, 1.

Reflexión final

Durante la carrera me enfrente al curso de Teoría de Grupos, el revisar la definición de grupo a través de algunos ejemplos concretos me permitió entender cada una de las propiedades, no tuve problemas al llegar la definición de subgrupo, al parecer todo estaba claro para mí, pero al llegar a definiciones como subgrupo normal, grupo cociente, los teoremas de isomorfismos… Por más que intentaba visualizar las definiciones no me quedaban claras, pero aún así intentaba resolver los problemas, recuerdo pocos ejemplos concretos en el curso y todo lo intentaba entender con permutaciones, sólo cambiaba el índice e intentaba particularizar, cuando me propusieron el tema de tesis *"Matemáticas del Cubo de Rubik"* me encanto la idea ya que mucho tiempo atrás tenía la curiosidad por saber cómo resolver el Cubo de Rubik, ahí me di cuenta que podía lograrlo y el saber que a la vez podía relacionar las matemáticas (en especial Teoría de grupos) con el cubo fue muy divertido.

Después de varios meses de trabajo ¡ya se resolver el cubo $3 \times 3 \times 3$! Y además pude relacionar cada movimiento que utilizaba en la resolución con los conceptos vistos en el Teoría de grupos, como conjugados y conmutadores, y aprendí algunos conceptos nuevos para mí, pues veía su aplicación al cubo.

Algunas personas resuelven el cubo en muy poco tiempo, pero han practicado muchas horas y descubren algunos algoritmos de manera empírica, lo cual tiene su mérito, pero con la ayuda de los conceptos básicos de Teoría de grupos me resulto más fácil entender por qué funcionan los algoritmos.

Mientras realizaba el presente trabajo aprendí a trabajar de manera independiente, buscando información, investigando…. Y esto me ayudará mucho en mi futuro. El trabajar en la realización de la tesis es una tarea que requiere bastante compromiso y que nos ayuda a crecer profesionalmente.

Finalmente debo mencionar que gracias a los maestros de la FCFM de la BUAP de quienes siempre recibí guía y soporte he logrado llegar a la meta, gracias a sus observaciones, críticas constructivas y a su gran compromiso.

Bibliografía

[A] P. Alegría, El cubo de Rubik y otros pasatiempos matemáticos.

[Ar] M. Artin, **Algebra**, Prentice-Hall, 1991.

[B1] C. Bandelow, **Inside Rubik's cube and beyond**, Birkh¨auser, Boston, 1980.

[BH] R. Banerji and D. Hecker, **"The slice group in Rubik's cube"**, Math. Mag. 58(1985)211-218. http://www.jstor.org/stable/2689516

[CL] Internet archives of the Cube-Lovers list at http://www.permutationpuzzles.org/rubik/cube-lovers/.

[D] Durbin J. R., **Modern Algebra an introduction**, fifth edition, USA 2005

[DiMo] J. Dixon and B. Mortimer, **Permutation Groups**, Springer-Verlag, Graduate Texts in Mathematics, 1996.

[FS] A. Frey and D. Singmaster, **Handbook of cubik math**, Enslow Pub., 1982.

[G] Gaglione A., **An introduction to group theory**, NRL, 1992 http://www.opensourcemath.org/books/gaglione-gp-thry/.

[Gar1] Gardner M. **"Combinatorial card problems",** in Time travel and other mathematical bewilderments, W.H. Freeman, New York, 1998. (Existe traducción al español)

[H] Herstein I. N., **Álgebra moderna**, ed. Trillas, 1980

[Hu] Henry Hubbard, **"Elements of campanalogia or an Essay on the Art of Ringing",** third edition, Norwich, 1868.

[J] David Joyner, **Adventures in Group Theory:** Rubik's Cube, Merlin's Machine, and Other Mathematical Toys, U.S.A. Johns Hopkins University Press, 2008.

[Koc] H. Kociemba, Cube solver site: http://kociemba.org/

[L] Loyd Sam, **Ciclopedia of Puzzles**, New York, The Lamb Publishing Company, 1914.

[Lo] M. Longridge, Cubeman's cube notes: http://cubeman.org/cubeman.html.

[MT] The MacTutor History of Mathematics Archive (maintained by J. J. O'Connor and E. F. Robertson at the School of Mathematical and Computational Sciences, University of St. Andrews, Scotland) http://www-history.mcs.st-and.ac.uk/

[NST] P. Neumann, G. Stoy, and E. Thompson, **Groups and geometry**, Oxford Univ. Press, 1994. Consultado en: http://books.google.com.mx/books/about/Groups_and_Geometry.html?id=DrEksWlmBtkC&redir_esc=y

[R] J. J. Rotman, **An introduction to the theory of groups**, 4th ed. Springer-Verlag, Graduate Texts in Math 148, 1995.

[Rok] T. Rokicki, **"Twenty-Five Moves Suffice for Rubik's Cube"**, 2008 preprint.
http://tomas.rokicki.com/rubik25.pdf

[Sch] Jaap Scherphuis' puzzle page: http://www.geocities.com/jaapsch/puzzles/.

[Si] Singmaster D., **Notes on Rubik's magic cube**, Enslow, 1981.

[W] R. M. Wilson, **"Graph puzzles, homotopy, and the alternating group",** J. Combin. Theory, 16 (1974)86-96.

[Wa] Wallace D.A.R., **Grupos**, México, Limusa, 1978.

[Wi] Optimal solutions for Rubik's Cube
http://en.wikipedia.org/wiki/Optimal_solutions_for_Rubik%27s_Cube.

Créditos de figuras

Figura 1e http://www.flickriver.com/photos/juliensart/2898873363/

Figura 1.5 https://es.m.wikipedia.org/wiki/Archivo:Volteo_de_campanas.jpg

Figura 1.6 http://proarte.jp/modules/bellWiki/?History

Figura 2.4 http://twistypuzzles.com/cgi-bin/puzzle.cgi?pkey=570

Figura 3.10 The 15-puzzle (and Rubik's cube) Keith Conrad

Figura 3.11 The 15-puzzle (and Rubik's cube) Keith Conrad

Figura 5.2 http://commons.wikimedia.org/wiki/File:Dual_Cube-Octahedron.jpg

Figura 5.3 http://commons.wikimedia.org/wiki/File:Symmetries_of_the_tetrahedron.svg

Figura 5.8 http://eulercap.wikispaces.com/6.2+Dualidad

Figura 5.10 http://eulercap.wikispaces.com/6.2+Dualidad

Figura 8.1 http://mundorubiko.blogspot.mx/

Figura 8.32 http://www.puzl.co.uk/fully-functional-3x3x2-cube-p-317.html