USC
UNIVERSIDADE
DE SANTIAGO
DE COMPOSTELA

FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

As matemáticas do cubo de Rubik

Laura Freire Míguez

2020/2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

As matemáticas do cubo de Rubik

Laura Freire Míguez

Xullo, 2021

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: As matemáticas do cubo de Rubik
Breve descrición do contido
O cubo de Rubik é un pasatempo deseñado nos anos 80 cuxa solución basase na concatenación de movementos que poden codificarse matematicamente mediante a estrutura de grupo. Neste traballo describiremos esa estrutura e daremos indicacións de como o coñecemento desa estrutura nos axuda a deseñar solucións ao pasamento
Recomendacións
Ter un bo coñecemento das materias de álxebra de 3^{o} e 4^{o} curso do grao
Outras observacións

Índice xeral

Resumo

Neste traballo imos introducir a matemática necesaria para entender como o cubo de Rubik opera como un grupo e construír este explicitamente. Para isto, incluímos os conceptos básicos de grupos e subgrupos, os tipos de grupos máis relevantes para o traballo (cíclicos e simétricos) e os produtos de grupos (directo, semidirecto e coroa). Finalmente, describimos o grupo do cubo de Rubik, tanto os movementos das súas pezas como as posicións e orientacións posibles da totalidade do cubo, grazas a dous teoremas fundamentais. Estes permítennos, á súa vez, dar unha solución (das moitas que existen) que describiremos no final da memoria. Tamén expoñemos os conceptos matemáticos detrás da solución.

Abstract

In this work we introduce the mathematics needed to understand how the Rubik's cube operates as a group and construct it explicitly. For this we include the basic concepts of groups and subgroups, the most relevant types of groups for the work (cyclic and symmetric) and the products of groups (direct, semi-direct and wreath). Finally, we describe the Rubik's cube group, both the movements of its pieces as well as the possible positions and orientations of the whole cube, thanks to two fundamental theorems. These also allow us to give a solution (of the many that exist) that we will describe at the end of the memory. The memory is completed by showing the mathematical concepts behind the solution.

Introdución

En 1974, Erno Rubik, escultor e profesor de arquitectura húngaro, inventou o quebracabezas mecánico tridimensional coñecido por todos como o cubo de Rubik tradicional de tamaño 3×3. No ano 1980 saíu á venda e empezou a gañar popularidade rapidamente ata converterse no xoguete máis vendido do mundo, ata xaneiro de 2009 levábanse vendidos 350 millóns de cubos. Como resulta lóxico, esta popularidade evolucionou no desenvolvemento de variacións do cubo de Rubik clásico, con distintas dimensións e formas pero, que hai detrás do cubo de Rubik? Aínda que a finalidade orixinal do cubo era resolver o problema estrutural que lograse mover as partes independentemente sen que o mecanismo enteiro se destruíse, Erno Rubik non caeu na conta de que creara un quebracabezas ata que desfixo o cubo e intentou retornalo á posición inicial, é dicir, resolvelo.

Nos seus comezos, a idea central e o interese sobre o cubo centrábase na súa resolución pero isto foi cambiando ata que, hoxe en día, sen deixar de lado a súa resolución, o foco está posto na competición tanto en tempo como en número de movementos que levan a esta solución. O récord actual en tempo é de 5,55 segundos mentres que o mínimo número de movementos necesarios para resolvelo dende calquera posición é como moito 20.

O cubo foi estudado por diferentes disciplinas como son a informática, a enxeñería ou as matemáticas. O certo é que como base do cubo están as matemáticas, máis concretamente a teoría de grupos, e este vai ser o tema central desta memoria. Analizaremos a matemática básica que hai detrás do cubo de Rubik así como proporcionaremos as indicacións necesarias para resolvelo mediante un método válido para calquera persoa, independentemente do seu nivel de coñecemento tanto en matemáticas como sobre o cubo, e que teñen un certo interese nas matemáticas.

A visión de grupo marca o punto de partida da álxebra moderna. A álxebra abstracta xorde a principios do século pasado e céntrase no estudo das estruturas alxébricas. As estruturas máis importantes son as de grupo, anel e corpo. Xorden en conexión coa resolución de ecuacións polinómicas. Este tema é moi importante polas súas aplicacións á teoría de números e á xeometría.

A estrutura máis básica é a estrutura de grupo. Esta expresa a idea dun conxunto de

transformacións que se poden compoñer e desfacer. Xeneraliza a idea de permutación, de feito, xorde como unha estrutura que especifica as posibles permutacións das raíces dun polinomio. Esta idea sérvelle a Galois para desenvolver a súa exitosa teoría de resolución de ecuacións polinómicas por radicais.

A utilidade e versatilidade desta estrutura revelouse rapidamente. De especial importancia foi o emprego dos grupos de transformacións en xeometría. Félix Klein planteouse a frutífera idea de que as diversas xeometrías caracterízanse polo grupo das súas tansformacións xeométricas.

Neste traballo pretendemos introducir a idea de grupo a través dun pasatempo matemático. Pretendemos facer a noción de grupo accesible a un público amplo. A memoria preséntase de modo que permita aos estudantes, especialmente das áreas STEM, acceder a esta interesante cuestión.

As transformacións necesarias para resolver o cubo de Rubik forman un grupo. Este, a pesar de ser finito, ten un cardinal moi grande.

Neste traballo definimos o grupo de tansformacións do cubo de Rubik. Esto permítenos introducir conceptos básicos de teoría de grupos, a través dos cales alcanzamos unha descrición matemática precisa do grupo, o que proporciona unha forma de manexar a súa gran complexidade.

Entre os conceptos involucrados aparecen de forma natural o concepto de grupo cíclico e de grupo de permutacións. Ademais, introdúcense diversas nocións de produto de grupos. Desde o produto directo de grupos, pasando polo produto semidirecto, alcanzamos o produto coroa.

A noción de produto coroa é a clave para a descrición do grupo do cubo de Rubik. Ao realizar a descrición, vémonos na necesidade de comprender de forma precisa o resultado da actuación dos movementos sobre as pezas do cubo.

Aparecen de forma destacada os conceptos de conxugación e os conmutadores. Con esta bagaxe e comprensión do mecanismo, é posible obter solucións do quebracabezas, como a que presentamos nesta memoria.

Pasamos agora á descrición máis detallada do contido deste traballo.

Esta memoria só presupón familiaridade coa noción de conxunto e unha certa madurez matemática e gusto polo razoamento formal.

No primeiro capítulo, comezaremos a definir e exemplificar os conceptos máis elementais da teoría de grupos que sentarán a base do noso traballo como son as definicións de grupo, subgrupo, orde, clases laterais, índice, conxugado, subgrupo normal, homomorfismo, isomorfismo, conxunto cociente, acción de grupo, órbita etc... As accións son un concepto importante dado que expresan formalmente a idea de que un grupo está formado polas

simetrías dun certo sistema.

No segundo capítulo, exemplificaremos os tipos de grupos principais e máis utiles para o noso cometido, grupos cíclicos e grupos simétricos ou de permutacións, así como daremos os resultados principais que caracterizan estes diferentes tipos entre os que se encontran teoremas de gran renome no ámbito da teoría de grupos como é o Teorema de Cayley, entre outros. Este teorema afirma que todo grupo se pode expresar como un subgrupo dun grupo de permutacións.

No terceiro, falaremos de produtos, máis concretamente de produtos directos, semidirectos e coroa, que serán de vital importancia á hora de estudar o grupo do cubo, para ser máis precisos, a peza fundamental, xa que deles dependen todos os movementos do quebracabezas. Os produtos permiten construír novos grupos utilizando grupos coñecidos previamente como pezas de construcción.

Entraremos máis en materia no capítulo catro, onde estableceremos a notación necesaria e explicaremos os movementos das distintas pezas que conforman o cubo para acabar dando os resultados fundamentais en forma de teoremas, os cales permitirannos distinguir as configuracións e os movementos posibles do cubo.

Finalmente, no capítulo cinco, aplicaremos todos estes conceptos para a resolución mecánica do pasatempo capa a capa. Este método é o máis xeral e común, sobre todo en persoas que se están a iniciar no mundo do cubo de Rubik, sendo apta así para todo tipo de público.

Capítulo 1

Preliminares

1.1. Definicións básicas e motivación

Imos comezar introducindo algúns conceptos básicos a modo de preliminares sobre os que construiremos o grupo do cubo de Rubik. En primeiro lugar, imos dar a definición formal de grupo e acción de grupo e máis tarde imos ver a motivación dos axiomas usados para estas definicións e, desta forma, comprender mellor o seu significado.

Definición 1.1. Sexa G un conxunto cunha operación interna:

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (g_1, g_2) &\longmapsto g_1 \cdot g_2 \end{aligned}$$

Entón, o par $(G,\cdot)$ formado por un conxunto non baleiro G dotado da operación binaria $\cdot$ dise que é un **grupo** se cumpre:

1. Para todo $g_1, g_2, g_3 \in G$:
$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$$
Esta propiedade coñécese como **asociativa**.

2. Existe un elemento $1 \in G$:
$$g \cdot 1 = 1 \cdot g = g$$
para todo $g \in G$. Dise que 1 é o **elemento neutro**.

3. Para todo $g \in G$, existe $g^{-1} \in G$:
$$g \cdot g^{-1} = g^{-1} \cdot g = 1$$
Dise que g^{-1} é o **inverso** de g.

Cando a operación $\cdot$ se dea por suposta diremos simplemente que G é un grupo.

Se G verifica a **propiedade conmutativa**, é dicir, se para todos $g_1, g_2 \in G$, $g_1 \cdot g_2 = g_2 \cdot g_1$, dise que G é un **grupo conmutativo** ou **abeliano** (na honra de Niels K. Abel (1802-1829) quen, a pesar de non traballar explicitamente con grupos, utilizounos no estudo das ecuacións alxébricas que poden resolverse por radicais).

Dise que un grupo G **actúa** nun conxunto X cando se ten unha aplicación $f\colon G \longrightarrow S_X$, onde S_X denota o grupo de bixeccións de X en si mesmo (ou permutacións de X), falaremos del en detalle na sección 2 do capítulo 2. Isto é equivalente a ter unha función

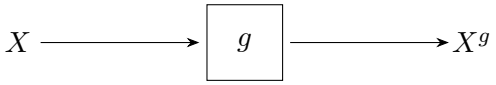
$$\begin{aligned} \varphi\colon G \times X &\longrightarrow X \\ (g, x) &\longrightarrow g \cdot x \end{aligned}$$

que verifique as seguintes condicións:

1. $(gh) \cdot (x) = g \cdot (h \cdot x)$, para todos $g, h \in G, x \in X$,
2. $1 \cdot x = x$ para toda $x \in X$.

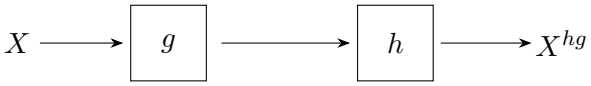
Dise que φ é unha **acción** do grupo G sobre o conxunto X.

Estas definicións poden resultar demasiado formais ou abstractas a primeira vista para a súa comprensión. Intentemos dar unha visión máis gráfica do que veñen a dicir: De onde veñen os axiomas da definición de grupo? Supoñamos que G actúa sobre X, interpretamos os elementos de G como transformacións que se lle fan a X, dado $g \in G$ podemos representalo como:

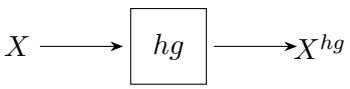


X está sendo modificado por g, cada elemento é unha máquina que tranforma X.

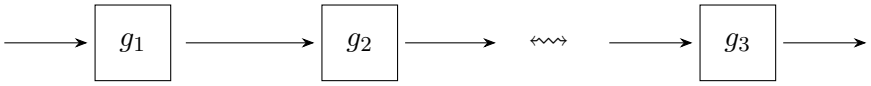
Estas máquinas poden "acoplarse":



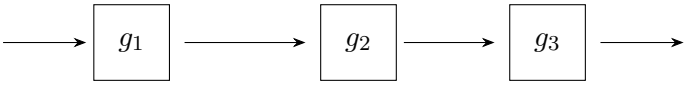
isto é o mesmo que



- A asociatividade, dá igual a orde na que montemos as tres máquinas:



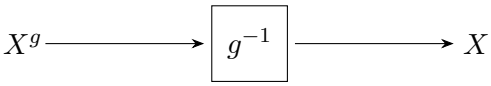
é o mesmo que



e á súa vez é igual a

- O elementro neutro, correspóndese coa transformación "non facer nada":

- O inverso, é dicir, poden desfacerse as transformacións:



Podemos relacionar desta forma os axiomas dados nas definicións previas de grupo e acción dun grupo coas distintas propiedades que se cumpren nas transformacións que lle podemos facer ao conxunto X.

1.2. Resultados importantes

Exemplo 1.2. Algúns exemplos de grupos son: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ coa operación suma. Estes son os chamados grupos aditivos dos enteiros, racionais, reais e complexos, respectivamente.

Tamén temos o grupo aditivo dos enteiros modulo $m \geq 0$: $(\mathbb{Z}/m\mathbb{Z}, +)$. Para $m = 5$, a operación do grupo aditivo $\mathbb{Z}_5$ pode representarse mediante a seguinte táboa:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Da mesma forma, son grupos, neste caso coa operación multiplicación: $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\})$, $(\mathbb{C}\setminus\{0\},\cdot)$. Son denominados grupos multiplicativos dos racionais, reais e complexos, respectivamente.

Outro grupo é $(\{1,-1\},\cdot)$, este correspóndese coa regra dos signos, xa que, se representamos a operación nunha táboa como antes:

$\cdot$	1	-1
1	1	-1
-1	-1	1

obtemos que $1\cdot 1 = 1 = (-1)\cdot(-1)$ e $(-1)\cdot 1 = -1 = 1\cdot(-1)$, a coñecida e antes mencionada regra dos signos.

Se H é un subconxunto do grupo G, $H \subseteq G$, diremos que H é un **subgrupo** de G cando H sexa un grupo coa mesma operación de G e denotarémolo por $H < G$, é dicir, se:

1. $h_1, h_2 \in H \implies h_1 \cdot h_2 \in H$
2. $1 \in H$
3. $h \in H \implies h^{-1} \in H$

Exemplo 1.3. Algúns exemplos de subgrupos son:

- $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.
- $n\mathbb{Z} < \mathbb{Z}$, $n \in \mathbb{N}$.

Sexa $a \in G$, $\langle a\rangle = \{a^n | n \in \mathbb{Z}\} < G$ é o **subgrupo cíclico xerado por** a.

A **orde** dun grupo G é n se ten n elementos e noutro caso dise que G é de orde infinita e denótase por $|G|$. Dado $a \in G$, a orde de a é a orde de $\langle a\rangle$. Ademais, tense que, se a orde de a é n, $a^n = 1$, e n é o menor número que cumpre isto.

A orde dun subgrupo divide á orde do grupo se este é finito.

Sexa G un grupo e $H \subset G$. O conxunto $aH = \{ah | h \in H\}$ para calquera $a \in G$ é a **clase pola esquerda** de H en G. Da mesma forma, $Ha = \{ha | h \in H\}$ para calquera $a \in G$ é a **clase pola dereita** de H en G. O número de **clases laterais** de H en G é $|G|/|H|$ se G é finito e é denominado **índice** de H en G, $[G : H]$.

Exemplo 1.4. Consideramos $G = \mathbb{Z}/8\mathbb{Z} = \{0,1,2,3,4,5,6,7\}$ e $H = \{0,2,4,6\}$ tense que $[G : H] = \frac{|G|}{|H|} = 8/4 = 2$ e polo tanto hai dúas clases laterais distintas de H en G.

O conxunto $aHa^{-1} = \{aha^{-1} \in G | h \in H\}$ chámase **conxugado** de H e é un subgrupo de G.

Dise que o subgrupo H de G é **normal** se para cada $a \in G$, $aHa^{-1} = H$ (ou $aH = Ha$) e denótase por $H \lhd G$. Se G é abeliano, todo subgrupo de G é normal. Ademais, todo subgrupo de índice 2 é normal.

Unha aplicación $f\colon G \longrightarrow H$ sendo G e H grupos é un **homomorfismo** de grupos se $f(a \cdot b) = f(a) \cdot f(b)$ para todos a, $b \in G$.

Sexa G grupo, $H < G$, $a, b \in G$ temos que $a \sim b \Leftrightarrow a^{-1}b \in H$, $\sim$ é relación de equivalencia e define o **conxunto cociente** $G/H = G/\sim$. As clases de equivalencia veñen dadas por: $[a] = \{b \in G | a \sim b = a^{-1}b \in H\} = \{b \in G | b = ah, h \in H\} = aH$ para $a \in G$.

Teorema 1.5. *Se $H \lhd G$, entón o conxunto cociente $G/H = \{a \cdot H | a \in G\}$ ten estrutura de grupo, que fai da proxección $p\colon G \longrightarrow G/H$ un homomorfismo.*

Demostración. Para todas $a, b \in G$, $(aH)(bH) = abH$ e $(aH)^{-1} = a^{-1}H$, ante a multiplicación de bloques, que é asociativa coa identidade H. [8] □

Exemplo 1.6. Retomando o exemplo anterior, no que $G = \mathbb{Z}/8\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ e $H = \{0, 2, 4, 6\}$, como o índice é 2, sabemos que $H \lhd G$, H é normal. Calculemos agora G/H, como a operación do grupo é a aditiva temos que:

$$\begin{aligned} G/H &= \{a + H | a \in G\} \\ &= \{(0 + \{0,2,4,6\}), (1 + \{0,2,4,6\}), (2 + \{0,2,4,6\}), (3 + \{0,2,4,6\}), (4 + \{0,2,4,6\}), \\ &\quad (5 + \{0,2,4,6\}), (6 + \{0,2,4,6\}), (7 + \{0,2,4,6\})\} \\ &= \{\{0,2,4,6\}, \{1,3,5,7\}, \{2,4,6,0\}, \{3,5,7,1\}, \{4,6,0,2\}, \{5,7,1,3\}, \{6,0,2,4\}, \{7,1,3,5\}\} \\ &= \{\{0,2,4,6\}, \{1,3,5,7\}\} \end{aligned}$$

é dicir, G/H é un grupo con dous elementos, aínda que cada elemento ten catro "nomes" distintos.

Un homomorfismo de grupos bixectivo dise que é un **isomorfismo** de grupos. Dous grupos G e H son **isomorfos** se existe un isomorfismo $f\colon G \longrightarrow H$ e escríbese $G \simeq H$.

Retomando o exemplo 1.2 podemos observar que o grupo dos signos é isomorfo a $(\mathbb{Z}/2\mathbb{Z}, +)$ xa que

$$\begin{aligned} f\colon (\{1, -1\}, \cdot) &\longrightarrow (\mathbb{Z}/2\mathbb{Z}, +) \\ 1 &\longmapsto 0 \\ -1 &\longmapsto 1 \end{aligned}$$

é un isomorfismo, o cal se ve claro comparando as táboas dos dous grupos:

$\cdot$	1	-1
1	1	-1
-1	-1	1

$+$	0	1
0	0	1
1	1	0

1.3. Accións de grupos

Unha vez introducido o concepto de acción dun grupo, dado un grupo G que actúa sobre un conxunto X: para cada $x \in X$, o conxunto $G \cdot x = \{g \cdot x \in X | g \in G\}$ chámase **órbita** de x e o conxunto $G_x = \{g \in G | g \cdot x = x\}$ **estabilizador** de x.

Exemplo 1.7.

- Acción de G sobre si mesmo por multiplicación (pola esquerda):

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

- Acción de G sobre si mesmo por conxugación:

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto g \cdot x \cdot g^{-1} \end{aligned}$$

Teorema 1.8. *Se o grupo G actúa no conxunto X, entón X é a unión disxunta das órbitas. Existe unha bixección dos elementos da órbita de x ás clases laterais de G_x en G. En particular, o cardinal de $G \cdot x$ é $[G : G_x]$.*

Demostración. A condición "a,b pertencen a mesma órbita" define unha relación de equivalencia, R_G, tal que

$$xR_Gy \text{ se existe } g \in G \text{ tal que } y = g \cdot x,$$

é dicir, cada clase de eqivalencia é unha órbita da acción, y está relacionada con x se $y \in G = \{g \cdot x \in X | g \in G\}$, polo que a primeira afirmación é clara.

Definimos $\varphi \colon G/G_x \longrightarrow G \cdot x$ así: $\varphi(aG_x) = a \cdot x$. Desta forma φ está ben definida, $aG_x = bG_x \implies a \cdot x = \varphi(aG_x) = \varphi(bG_x) = b \cdot x$, e é claramente unha aplicación sobrexectiva. Por outra banda, tamén é inxectiva, $\varphi(aG_x) = \varphi(bG_x) \implies b^{-1}a \in G_x \implies bG_x = b(b^{-1}a)G_x = aG_x$, polo que φ é unha bixección. A terceira afirmación é unha consecuencia inmediata. [8] □

Un exemplo de accións de grupos é o grupo simétrico do que falaremos despois: S_X actúa sobre o conxunto $X(\sigma \cdot x = \sigma(x))$. En particular, o grupo S_n actúa sobre $\{1, 2, \dots, n\}$.

Capítulo 2

Tipos de grupos

Nesta sección introduciremos algúns tipos de grupos interesantes que ademais de selo serán unha "peza" clave do noso grupo do cubo de Rubik.

2.1. Grupos cíclicos

En primeiro lugar, imos introducir o concepto de grupos cíclicos. Son os máis simples, non obstante, teñen a capacidade de expresar propiedades moi interesantes que empregaremos na construción do grupo do cubo. En certo sentido, os grupos cíclicos son os elementos básicos cos que se poden construír todos os grupos abelianos. Esta teoría coñécese como o problema de clasificación de grupos abelianos finitamente xerados pero non a trataremos nesta memoria por non ser necesaria para o noso cometido.

O subgrupo xerado por X, $\langle X\rangle = \cap\{H|H < G, X \subset H\}$, sendo $X \neq \emptyset$ e $X < G$, é o **menor subgrupo de G que contén a X**.

Definición 2.1. Se G é un grupo tal que $\exists g \in G|\langle g\rangle = G$ dise que G é un **grupo cíclico** e que g é un **xerador** de G.

Por exemplo, $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$, $\mathbb{Z}$ é un grupo cíclico de orde infinita.
Outros resultados interesantes son:

- Todo cociente dun grupo cíclico é un grupo cíclico:

  Sexa $G = \langle a\rangle$, se consideramos a proxección canónica $p\colon G \longrightarrow G/H$ é un homomorfismo (probado no Teorema 1.5) sobrexectivo de grupos, polo tanto como a é xerador de G tense que $p(a)$ é xerador de G/H e polo tanto o grupo cociente é cíclico.

- Todo subgrupo dun grupo cíclico é un grupo cíclico:

Sexa $G = \langle a \rangle$ e supoñamos $H < G$, se $H = \{e\}$, entón $H = \langle e \rangle$ trivialmente. Supoñamos que H contén algún outro elemento $g \neq e$, neste caso g pode ser escrito como a^n para algún enteiro n por ser G cíclico. Por ser H un subgrupo temos que $g^{-1} = a^{-n} \in H$. Como n ou $-n$ é positivo, podemos supoñer que H contén potencias positivas de a e que $n > 0$. Sexa m o menor número natural que cumpre que $a^m \in H$, $h = a^m$ é un xerador de H, todo $h' \in H$ pode ser escrito como unha potencia de h. Como $h' \in H$ y H é un subgrupo de G, $h' = a^k$ para algún enteiro k. Usando o algoritmo da división, podemos atopar q e r tal que $k = mq + r$ con $0 \leq r < m$, temos así que

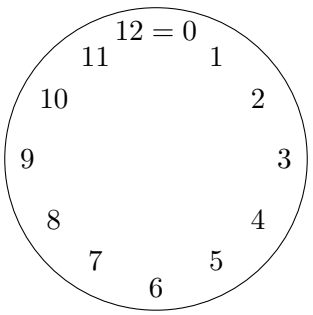
$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r$$

de onde $a^r = a^k h^{-q}$. Como a^k e h^{-q} pertencen a H, a^r tamén. Pero como m era o menor número natural que cumpría $a^m \in H$, temos que $r = 0$ e $k = mq$. Concluímos entón que $h' = a^k = a^{mq} = h^q$ e $H = \langle h \rangle$. [6]

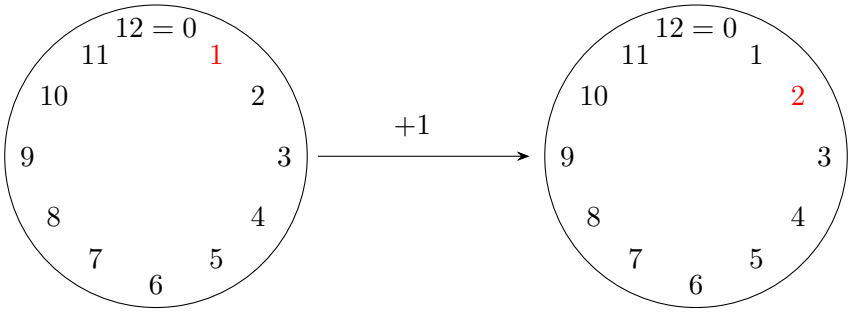
Ademais, sexa G un grupo cíclico de orde finita n, para cada divisor r de n existe un único subgrupo H de G de orde r, se $g \in G$ é un xerador de G, entón $g^{\frac{n}{r}}$ é un xerador de H.

Para ilustrar mellor o concepto de grupo cíclico imos desenvolver un exemplo "gráfico":

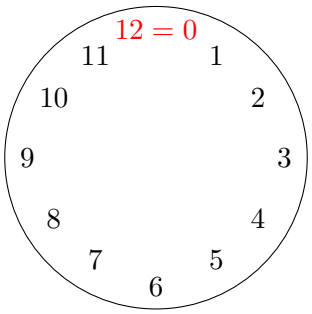
Exemplo 2.2. Considérase un reloxo coas horas marcadas mediante os números do 1 ao 12. O noso grupo é $\mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ (coa operación suma) se identificamos a hora 12 como o $0 \in \mathbb{Z}/12\mathbb{Z}$, é dicir, $(\mathbb{Z}/12\mathbb{Z}, +)$, o grupo cíclico de orde 12 é o grupo das horas do reloxo. Representémolo:



Se comezamos no 1 observamos que ao facer 1+1=2 avanzamos ata a hora 2

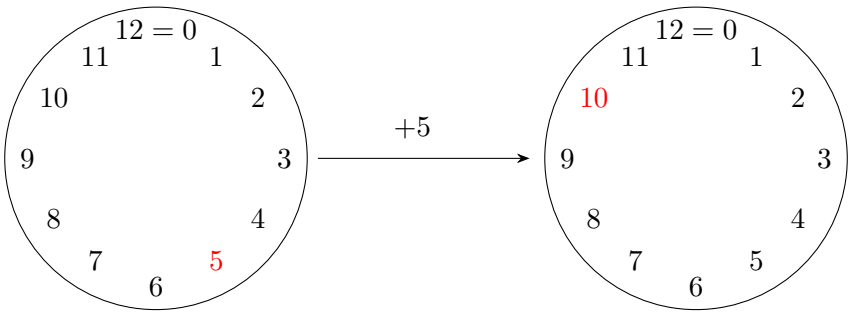


se facemos isto repetidas veces imos avanzando no reloxo dunha en unha unidade ata que facemos esta operación 12 veces, que chegamos á hora 12, o noso 0, o elemento neutro do grupo.

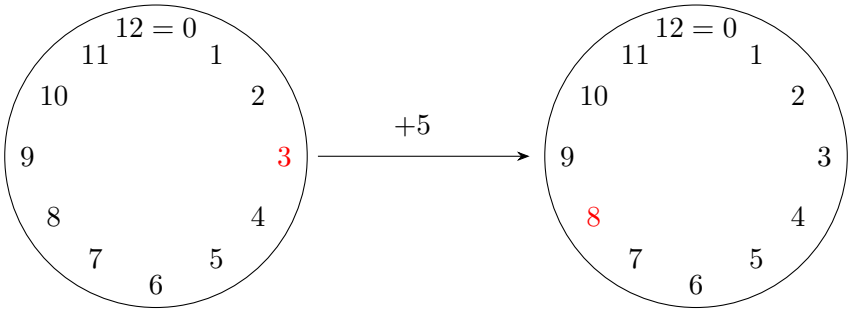


Desta forma $\mathbb{Z}/12\mathbb{Z} = \langle 1 \rangle$, é dicir, $\mathbb{Z}/12\mathbb{Z}$ é un grupo cíclico xerado por 1 xa que podemos obter todos os seus elementos a partir del (sumando repetidas veces, ata 12), e a orde deste elemento é trivialmente 12, $|1|$=12, é dicir, o menor n para o cal $1^n = 0$ é 12. Xa sabiamos que tiña que ser 12 porque a orde dos xeradores coincide coa orde do grupo no caso dos grupos cíclicos.

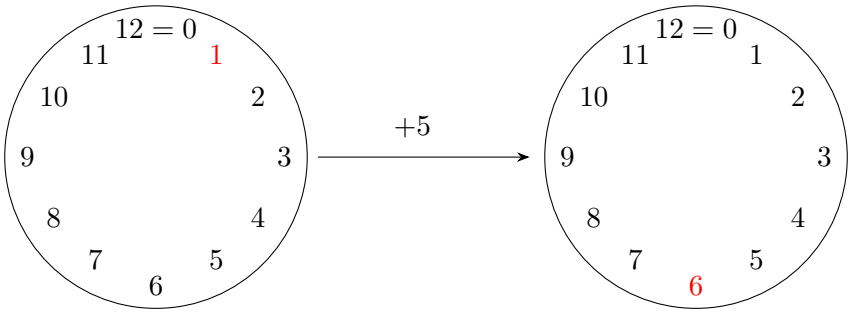
Outros xeradores deste grupo son 5,7 e 11. Fagámolo para o 5:



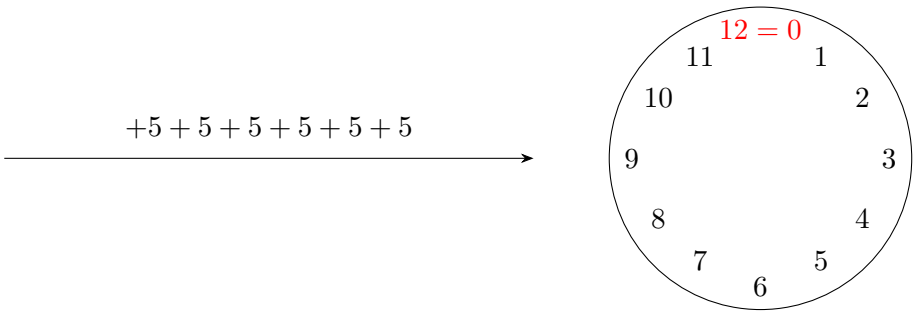
$10 + 5 = 15 \equiv 3(12)$



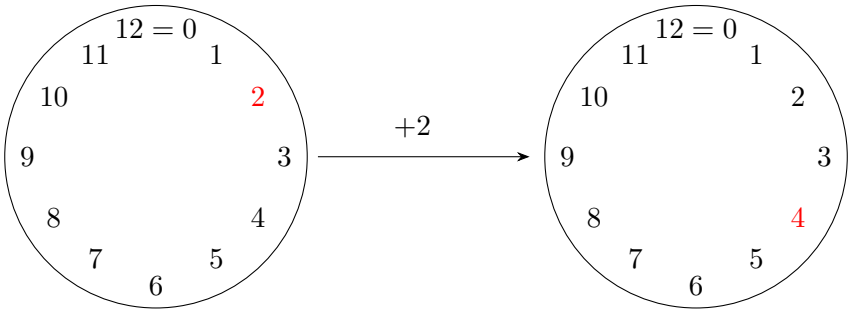
$8 + 5 = 13 \equiv 1(12)$



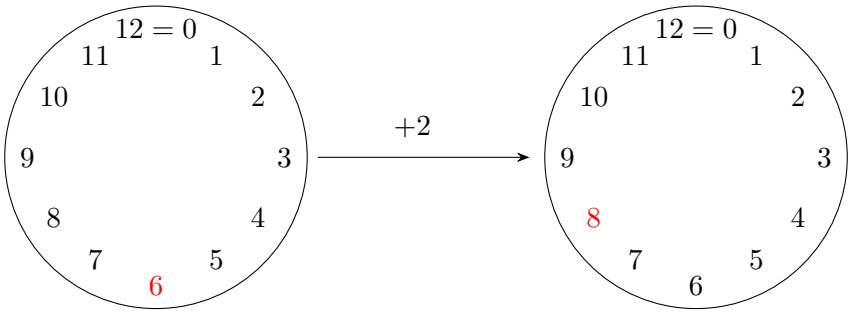
Como xa sabemos, este proceso requirirá 12 sumas, outra vez, ata chegar ao 12.



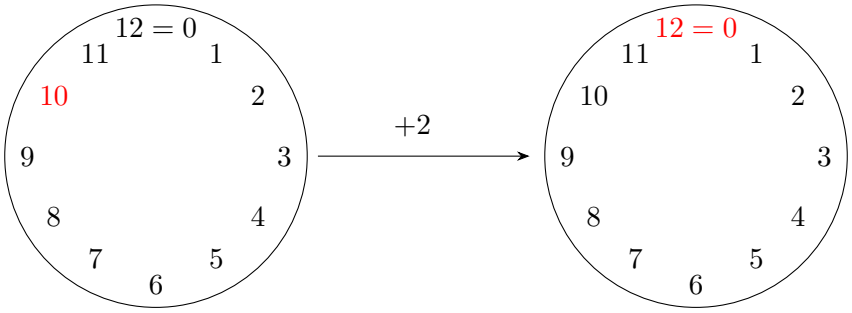
Agora tomemos un elemento que non sexa xerador, por exemplo, o 2. Facemos os mesmos pasos: 2+2=4



4+2=6



así sucesivamente ata que chegamos a 12



temos así que $\langle 2\rangle = \{0, 2, 4, 6, 8, 10\}$ polo tanto $|2| = |\langle 2\rangle| = 6$.

Do mesmo xeito, poderiamos calcular os grupos xerados polos elementos restantes de $\mathbb{Z}/12\mathbb{Z}$ e as súas ordes.

2.2. Grupos simétricos

A continuación falaremos dos grupos simétricos, fundamentais na construción do grupo do cubo. Veremos a súa definición, os seus elementos e as principais propiedades deste tipo de grupos.

Dado un conxunto X, o conxunto $S_X = \{f\colon X \longrightarrow X : f \text{ bixectiva}\}$ xunto coa composición é un grupo. Se $X = \{1, 2, \dots, n\}$, X ten n elementos, é finito, entón o grupo S_X represéntase por S_n e chámase n-ésimo **grupo simétrico** ou **grupo de permutacións**. Os elementos deste grupo chámanse **permutacións** de X e a súa orde é $|S_n| = n!$.

Notación 2.3. $\sigma \in S_n = \{\sigma\colon X \longrightarrow X : \sigma \text{ bixectiva}\}$

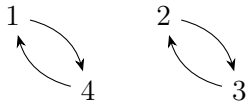
Exemplo 2.4. Consideremos $n = 4$ e $\sigma \in S_4$ tal que

$$\sigma(1) = 4, \sigma(2) = 3, \sigma(3) = 2, \sigma(4) = 1$$

o expresaremos como

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

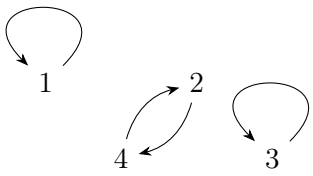
onde a primeira fila corresponde cos elementos do conxunto os cales imos permutar e a segunda fila son as súas correspondentes imaxes. Graficamente:



Outra permutación de S_4 é

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

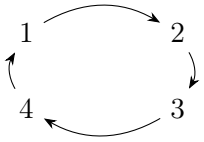
expresado graficamente como antes:



Entón, o produto $\tau\sigma$, que consiste en facer σ e despois aplicarlle τ é

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

graficamente:



Tamén o podemos expresar da forma:

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

que denotamos como **ciclo** ou **permutación cíclica**.

Ademais podemos expresar τ como produto de ciclos, $\tau = (1)(24)(3)$.

Unha definición máis formal de **ciclo (de orde r)** é: unha permutación $\sigma \in S_4$ con r elementos non invariantes $a_1, \dots, a_r$ tal que $\sigma(a_i) = a_{i+1}$ para $0 \leq i \leq r-1$ e $\sigma(a_r) = a_1$. Desta forma, expresando $\tau\sigma$ como ciclo como fixemos antes, $\tau\sigma = (1234)$, estamos dicindo que levamos o 1 ao 2, o 2 ao 3, o 3 ao 4 e o 4 ao 1. Cando expresamos τ como produto de ciclos, $\tau = (1)(24)(3)$, estamos a dicir que o 1 e 3 permanecen sen cambios e o 2 e o 4 intercámbianse.

Se $\sigma \in S_n$, entón o grupo $\langle\sigma\rangle$ actúa sobre $\{1, 2, \dots, n\}$ e descompón a este conxunto en órbitas que son denominadas **órbitas de** σ. A notación consistente en escribir unha órbita tras outra ($\sigma = (1, \sigma(1), \sigma^2(1)), \dots$) é a acabada de mencionar. Por exemplo, se consideramos a permutación σ do exemplo anterior: $\sigma(1) = 4, \sigma(2) = 3, \sigma(3) = 2, \sigma(4) = 1$, podemos escribila como $\sigma = (14)(23)$. en conclusión, cada órbita así escrita é un ciclo.

Exemplo 2.5. Retomando o exemplo anterior, podemos facer a permutación inversa, por exemplo, a permutación inversa do produto $\tau\sigma$, $(\tau\sigma)^{-1}$, é:

$$(\tau\sigma)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

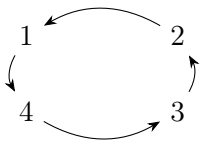
xa que

$$\begin{aligned} \tau\sigma \colon X &\longrightarrow X \\ 1 &\longmapsto \tau\sigma(1) = 2 \\ 2 &\longmapsto \tau\sigma(1) = 3 \\ 3 &\longmapsto \tau\sigma(1) = 4 \\ 4 &\longmapsto \tau\sigma(1) = 1 \end{aligned}$$

e entón

$$\begin{aligned} \tau\sigma \colon X &\longrightarrow X \\ 2 &\longmapsto \tau\sigma(1) = 1 \\ 3 &\longmapsto \tau\sigma(1) = 2 \\ 4 &\longmapsto \tau\sigma(1) = 3 \\ 1 &\longmapsto \tau\sigma(1) = 4 \end{aligned}$$

Graficamente podemos representalo como:



Dúas permutacións $\sigma, \tau \in S_n$ dise que son **disxuntas** se os elementos que move unha quedan fixos pola outra, é dicir, se para todo $i \in \{1, 2, \dots, n\}$ se verifican as seguintes condicións:

- se $\sigma(i) \neq i$ entón $\tau(i) = i$,
- se $\tau(i) \neq i$ entón $\sigma(i) = i$.

É dicir, σ e τ nunca moven o mesmo elemento. En particular, dous ciclos son disxuntos se e só se os conxuntos sobre os que actúan o son.

É importante destacar que dous ciclos disxuntos conmutan entre si.

Proposición 2.6. *Toda permutación pódese escribir como produto de ciclos disxuntos: as súas órbitas. Esta descomposición é única, salvo a orde na que aparecen escritos os ciclos.*

Demostración. Imos probar primeiro a existencia e logo a unicidade. Sexa

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

unha permutación arbitraria de S_n. Supoñamos que $\sigma \neq 1$, e sexa b un número tal que $\sigma(b) \neq b$ (xa que o caso $\sigma = 1$ é trivial). Constrúese entón $\sigma^2(b)$, $\sigma^3(b)$ etc., ata que, por este procedemento, se obteña b de novo ao cabo, digamos, de i+1 pasos. Entón o ciclo

$$(b, \sigma(b), \sigma^2(b), \dots)$$

describe parte da permutación σ. Se o resto da permutación non contén números ou consta de números que permanecen invariantes, está demostrado o resultado, pois σ é, entón, un ciclo. No caso contrario, repítese o procedemento anterior con ese resto e así sucesivamente. Despois dun número finito de pasos tense a descomposición.

Probemos agora a unicidade, vexamos que dous ciclos disxuntos conmutan. Supoñamos que $\sigma = \sigma_r \dots \sigma_2\sigma_1 = \tau_s \dots \tau_2\tau_1$ fosen dúas descomposicións de σ en produto de ciclos disxuntos. Sexa a_1 un número que non permanece invariante por σ. É evidente que a_1 debe estar nun ciclo e só un de entre os $\{\sigma = \sigma_r \dots \sigma_2\sigma_1\}$, e nun e só un de entre os $\{\tau_s \dots \tau_2\tau_1\}$. Pola conmutatividade pódese supoñer que a_1 está en σ_1 e en τ_1. Como os números que aparecen en σ_1 (respec. en τ_1) permanecen invariantes polo resto dos ciclos σ_i (respec. τ_i), o elemento a_1 transformarase nun mesmo elemento a_2 mediante σ_1 e mediante τ_1.

Pola mesma razón, a_2 debe transformarse nun mesmo elemento a_3 mediante σ_1 e τ_1, e así sucesivamente. Isto proba que $\sigma_1 = \tau_1$. Repetindo convenientemente este razoamento, dedúcese que $p = q$ e os ciclos σ_i son iguais aos τ_i. [7] □

Unha **transposición** é un ciclo de orde 2.

Ademais, definimos a **signatura** da permutación σ como:

$$\begin{aligned} \varepsilon\colon S_n &\longrightarrow \{-1, 1\} \\ \sigma &\longrightarrow \varepsilon(\sigma) = (-1)^r \end{aligned}$$

sendo r o número de transposicións dunha factorización de σ. O número de transposicións da descomposición non é único pero si a súa paridade como probaremos no seguinte resultado. Unha permutación $\sigma \in S_n$ dise que é **par** se r é un número par e **impar** se é un número impar, é dicir, se temos dúas descomposicións distintas de σ con r e s transposicións, ambas terán a mesma paridade, serán ambas pares ou impares.

O conxunto de todas as permutacións pares é un subgrupo de S_n, o **grupo alternado**, denotado por $A_n = \{\sigma \in S_n | sig(\sigma) = 1\} < S_n$. A súa orde é $\frac{n!}{2}$ e polo tanto o seu índice é $[S_n : A_n] = \frac{S_n}{A_n} = \frac{n!}{n!/2} = 2$, que implica que $A_n \lhd S_n$.

Proposición 2.7. *Todo ciclo pode factorizarse como produto de transposicións e dúas factorizacións en produto de transposicións teñen a mesma paridade.*

Demostración. Se $\sigma = 1$, $\sigma = (12)(21)$. Se $\sigma \neq 1$. entón σ é un produto de ciclos disxuntos, como consecuencia basta probar que todo ciclo de lonxitude maior ou igual que 2 é un produto de ciclos de lonxitude 2 (transposicións). Temos:

$$(x_1 \dots x_n) = (x_1 x_n) \dots (x_1 x_2),$$

xa que o termo da esquerda, de acordo coa definición de ciclo que vimos anteriormente, corresponde con levar x_1 a x_2, x_2 a x_3, ... , x_{n-1} a x_n e x_n a x_1, é dicir:

$$\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_n & x_1 & \dots & x_{n-1} \end{pmatrix}$$

e o termo da dereita é un produto de transposicións que primero intercambia x_1 con x_2

$$\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_2 & x_1 & \dots & x_n \end{pmatrix}$$

logo x_2 (xa que agora é o que está na primeira posición) con x_3

$$\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ x_3 & x_1 & x_2 & \dots & x_n \end{pmatrix}$$

e así sucesivamente ata a ultima transposición, que corresponde con cambiar o que está na primeira posición, que agora é x_{n-1}, con x_n obtendo:

$$\begin{pmatrix} x_1 & x_2 & ... & x_n \\ x_n & x_1 & ... & x_{n-1} \end{pmatrix}$$

sendo certa así a igualdade mencionada anteriormente.

Demostremos agora a invarianza da paridade: como sabemos, a signatura dunha transposicións calquera τ é $\varepsilon(\tau) = -1$, polo tanto a dun produto de k transposicións é $\varepsilon(\tau_1 ... \tau_k) = (-1)^k$ e entón, para cada permutación $\sigma \in S_n$, se a factorizamos en produto de transposicións, o cal acabamos de probar que é posible, $\sigma = \tau_1 ... \tau_k$ tense que:

$$\varepsilon(\sigma) = \varepsilon(\tau_1 ... \tau_k) = (-1)^k$$

e como o valor da parte esquerda só depende de σ, o número k de transposicións en calquera factorización de σ mantén a paridade. [4] □

Exemplo 2.8. Se temos o ciclo $(165432) \in S_6$ podemos factorizalo da forma:

$$(165432)=(16)(65)(54)(43)(32)=(12)(13)(14)(15)(16)$$

temos que $r = 6$, o ciclo mencionado trátase dunha permutación par e a súa signatura polo tanto é 1, como vemos, aínda que existan distintas factorizacións en produtos de transposicións, a paridade permanece invariante.

Teorema 2.9 (Cayley)**.** *Todo grupo G é isomorfo a un grupo de permutacións.*

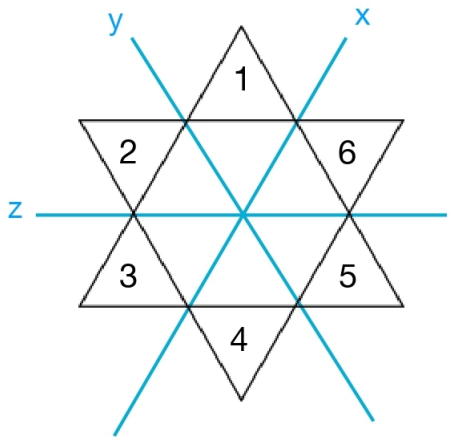
Demostración. Definimos unha función $f\colon G \longrightarrow S_G$ así: $f(a) = f_a$ é multiplicación esquerda por a, é dicir, $f_a(x) = ax$ para toda $x \in G$.

Temos que para todos a, $b \in G$, $(f_a \circ f_b)(x) = a(bx) = abx = f_{ab}(x)$ para toda $x \in G$, polo que $f_a \circ f_b = f_{ab}$ e entón f é un homomorfismo de grupos. Desta forma, a imaxe de f, $\mathrm{Im}f$, é un subgrupo de S_G.

Probemos que f é inxectiva, para todo a, $b \in G$, se $f_a = f_b$, $ax = bx$ para todo $x \in G$ e entón $a = b$.

Como consecuencia, a aplicación f en $\mathrm{Im}f$ tamén é un homomorfismo inxectivo. Ademais é sobrexectiva pola propia construción, tendo así que f é un isomorfismo de grupos. Así, G é isomorfo a $\mathrm{Im}f$, $G \cong \mathrm{Im}f$, un subgrupo de S_G ($\mathrm{Im}f < S_G$). [1] □

Exemplo 2.10. Vexamos un exemplo gráfico:



Consideramos a figura mostrada, as permutacións asociadas ás simetrías sobre os eixos x,y e z son:

$$\sigma_x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}$$

$$\sigma_z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix}$$

xa que cando facemos a simetría sobre o eixo x estamos intercambiando o 1 polo 6, o 2 polo 5 e o 3 polo 4; cando facemos a simetría sobre o eixo y estamos intercambiando o 1 polo 2, o 3 polo 6 e o 4 polo 5; e cando facemos a simetría sobre o eixo y estamos intercambiando o 2 polo 3, o 1 polo 4 e o 5 polo 6.

Obsérvese que $\sigma_x^2 = id$ xa que se corresponde con facer dúas veces unha simetría repecto ao eixo x, que é volver ao principio. Da mesma forma $\sigma_y^2 = \sigma_z^2 = id$.

Por outro lado, se facemos $\sigma_x\sigma_z$, o resultado é facer primeiro a simetría respecto ao eixo z e despois respecto ao eixo x, é dicir:

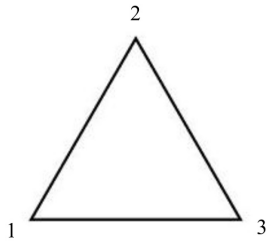
$$\sigma_x\sigma_z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$$

Outro exemplo é facer $\sigma_y\sigma_z$, a simetría respecto ao eixo z e despois respecto ao eixo y:

$$\sigma_y\sigma_z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Como dixemos cando falamos de accións de grupos, o grupo simétrico é un exemplo delas, ilustremos esta idea a modo de exemplo:

Exemplo 2.11. Tomemos o grupo simétrico S_3 sobre un triángulo:

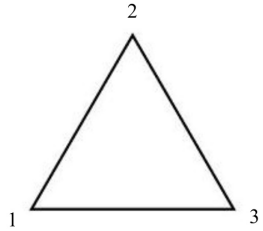


Como $|S_3| = 3! = 6$ os distintos elementos son:

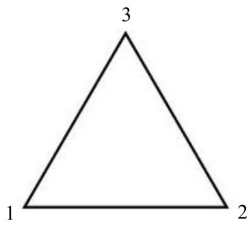
$$I = \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

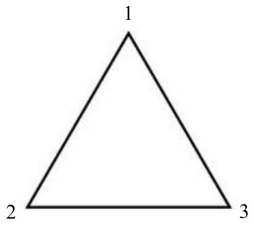
que poden ser representados graficamente como:



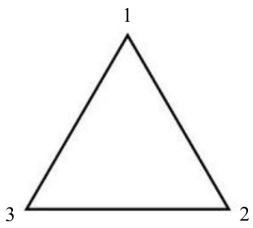
(a) σ_1



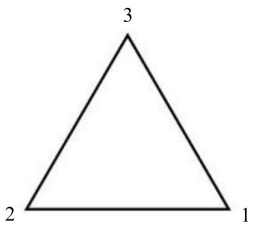
(b) σ_2



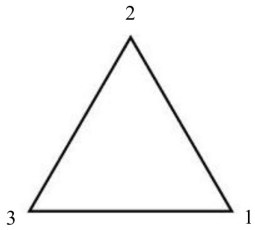
(c) σ_3



(a) σ_4



(b) σ_5



(c) σ_6

Quedemos agora soamente co grupo alternado A_3, no que se encontran as permutacións pares de S_3. Tense que:

$$A_3 = \{\sigma_1, \sigma_4, \sigma_5\}$$

Podemos observar que estas tres permutacións son as rotacións do triángulo: σ_1 é a rotación de 0^{o} ou 360^{o}, σ_4 é a rotación de 120^{o} e σ_5 é a rotación de 240^{o} (todas no sentido das agullas do reloxo).

En conclusión, podemos identificar A_3 coas rotacións do triángulo.

Capítulo 3

Produto de grupos

Neste capítulo imos tratar con tres tipos de produtos de grupos, que serán de gran utilidade, máis ben necesarios, para falar dos movementos que se describen no cubo. Estes son o produto directo, o produto semidirecto e o produto corona, presentémolos.

3.1. Produto Directo

Sexan G_1 e G_2 dous grupos, definimos o conxunto **produto directo**

$$G_1 \times G_2 := \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}$$

respecto á operación multiplicación

$$(g_1, g_2) \times (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$$

para g_1,$g_1' \in G_1$ e g_2,$g_2' \in G_2$.

Como G_1 e G_2 son grupos, $G_1 \times G_2$ é unha forma de darlle unha estrutura de grupo ao produto cartesiano dos dous conxuntos onde o elemento neutro é $(1_{G_1}, 1_{G_2})$ e os elementos inversos son $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

Da mesma forma, para unha familia de grupos $G_1, G_2, \dots, G_n$, definimos o **produto directo** $G_1 \times \cdots \times G_n$ como o conxunto $\{(g_1, \dots, g_n) | g_i \in G_i\}$ respecto á operación multiplicación

$$(g_1, \dots, g_n) \cdot (g_1', \dots, g_n') = (g_1 \cdot g_1', \dots, g_n \cdot g_n')$$

para g_i,$g_i' \in G_i$.

Deste modo, é unha forma natural de darlle ao produto cartesiano de $G_1, \dots, G_n$ estrutura de grupo.

Son claramente certos os seguintes enunciados (a súa demostración aburre máis que ilumina):

1. Se os grupos son abelianos, o produto tamén o será.
2. $G_1 \times G_2 \cong G_2 \times G_1$
3. $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3) \cong G_1 \times G_2 \times G_3$
4. Para $G_1 \times G_2$, tense que $(g_1, 1)(1, g_2) = (g_1, g_2) = (1, g_2)(g_1, 1)$ para todo $g_1 \in G_1$, $g_2 \in G_2$.
5. $G_1 \times \{1\}$ e $\{1\} \times G_2$ son subgrupos normales de $G_1 \times G_2$ que xeran o produto directo.

Exemplo 3.1. Se consideramos o grupo $G_1 = G_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ o produto directo consigo mesmo, $G_1 \times G_2$, é:

$$G_1 \times G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (0,1), (1,0), (1,1)\}$$

Este grupo chámase grupo de Klein e adoita denotarse como V polo vocábulo alemán *Vierergruppe*, que significa "grupo de catro".

Teorema 3.2. *Sexan H, $K \lhd G$ tales que $HK = G$ e $H \cap K = \{1\}$. Entón, $G \cong H \times K$.*

Demostración. Definimos $\varphi\colon H \times K \longrightarrow G$ tal que $\varphi(h, k) = hk$. Entón φ é un homomorfismo sobrexectivo. Temos que $\ker\varphi = \{(h, k) | hk = 1, h \in H, k \in K\}$; e polo tanto $(h, k) \in \ker\varphi \implies h = k^{-1} \in H \cap K = \{1\}$. Desta forma, $\ker\varphi = \{1\}$ e φ é un isomorfismo. [8] □

Teorema 3.3. *Se $G = G_1 \times G_2$, $H \lhd G_1$ e $K \lhd G_2$, entón $H \times K \lhd G$ e $G/(H \times K) \cong (G_1/H) \times (G_2/K)$.*

Demostración. Sexan $\varphi\colon G_1 \longrightarrow G_1/H$ e $\psi\colon G_2 \longrightarrow G_2/K$ os homomorfismos naturais. Definimos:

$$\begin{aligned} \eta\colon G &\longrightarrow (G_1/H) \times (G_2/K) \\ (a, b) &\longmapsto (\varphi(a), \psi(b)). \end{aligned}$$

Vese que η é un homomorfismo sobrexectivo con núcleo $H \times K$. [8] □

3.2. Produto Semidirecto

Máis necesario na construción do grupo do cubo ca o produto directo é o produto semidirecto. Sexan G e X dous grupos tales que G actúa sobre X mediante un morfismo

$\varphi\colon G \longrightarrow \mathrm{Aut}X$ que vén dada por $\varphi(g)(x) = g \cdot x$ para $g \in G$ e $x \in X$, equivalentemente

$$\varphi\colon G \times X \longrightarrow X$$
$$(g, x) \longrightarrow g \cdot x,$$

entón $A = X \rtimes G$ é o **produto semidirecto** de X e G ante a acción dada. A multiplicación en A defínese como

$$(x_1, g_1)(x_2, g_2) = (x_1(g_1 \cdot x_2), g_1 g_2)$$

para x_1, $x_2 \in X$ e g_1, $g_2 \in G$.

Claramente verifica a propiedade asociativa xa que:

$$(x_1(g_1 \cdot x_2), g_1 g_2)(x_3, g_3) = (x_1(g_1 \cdot x_2)(g_1 g_2 \cdot x_3), g_1 g_2 g_3)$$

e

$$(x_1, y_1)(x_2(g_2 \cdot x_3), g_2 g_3) = (x_1 g_1 \cdot [x_2(g_2 \cdot x_3)], g_1 g_2 g_3)$$

son iguais debido a que φ é un homomorfismo.

O elemento neutro é $(1, 1)$ e os elementos inversos son $(x, g)^{-1} = (g^{-1} \cdot x^{-1}, g^{-1})$ xa que, por un lado,

$$(x, g)(g^{-1} \cdot x^{-1}, g^{-1}) = (xg \cdot [g^{-1}x^{-1}], gg^{-1}) = (xx^{-1}, gg^{-1}) = (1, 1)$$

e polo outro,

$$(g^{-1} \cdot x^{-1}, g^{-1})(x, g) = ([g^{-1} \cdot x^{-1}][g^{-1} \cdot x], g^{-1}g) = (g^{-1} \cdot [x^{-1} \cdot x], g^{-1}g) = (1, 1).$$

Cando a acción de G en X é trivial, $g \cdot x = x$, para todas as $g \in G$, $x \in X$, entón $X \rtimes G = X \times G$ é o produto directo.

Unha caracterización do produto semidirecto é, sexan X e G subgrupos, entón $A = X \rtimes G$ é produto semidirecto se:

1. $A = XG$
2. $X \cap G = \{1\}$
3. $X \lhd A$.

é dicir, o produto semidirecto fai de X un subgrupo normal do produto a través da acción.

Exemplo 3.4. O grupo diédrico (grupo das reflexións e rotacións dun polígono regular de n lados) $D_n = \{\langle r, s\rangle | r^n = s^2 = 1, srs = r^{-1}\}$ pode ser expresado como produto semidirecto. Sexan $X = \langle r\rangle$ onde r son as rotacións de orde n e $G = \langle s\rangle$ onde s son as reflexións de orde 2. Definindo a acción de G en X tal que $s \cdot r^i = r^{-i}$ para todo $i \in \mathbb{N}$, tense que $X \cap G = 1$ e $X \lhd D_n$. e entón $X \rtimes G \cong D_n$. A orde de D_n é $2n$.

3.3. Produto Coroa

O produto de dous grupos pode ser xeneralizado do produto semidirecto ao denominado produto coroa.

O produto coroa de dous grupos G e H é construído da seguinte forma:

1. preséntese $H < S_X$,
2. fanse $n = |X|$ copias do grupo G,
3. H actúa sobre as copias de G permutando os elementos.

O produto coroa de G por H é un produto semidirecto do produto directo das n copias de G por H.

Máis formalmente, sexa X un conxunto finito ($X = \{x_1, x_2, \dots, x_n\}$, $|X| = n$), G un grupo e H un grupo actuando sobre X e sexa G^n o produto directo de G consigo mesmo n veces, entón o **produto coroa** de G e H é $G^n \wr H = G^n \rtimes H$ onde H actúa sobre G^n pola súa acción sobre X. É dicir, se $g \in G$, entón a acción de H sobre G^n é $(g_1, g_2, \dots, g_n)^h = (g_{1h}, g_{2h}, \dots, g_{nh})$.

Exemplo 3.5. Sexa $G = \mathbb{Z}/m\mathbb{Z}$, $H = S_n$ e $X = \{1, 2, 3, \dots, n\}$. O produto coroa de G por H é $(\mathbb{Z}/m\mathbb{Z})^n \wr S_n$ onde $\varphi\colon S_n \longrightarrow Aut((\mathbb{Z}/m\mathbb{Z})^n)$ é definida por $\varphi(\sigma)(x_1, x_2, \dots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$. O grupo $(\mathbb{Z}/m\mathbb{Z})^n \wr S_n$ denomínase grupo simétrico xeneralizado.

En particular, se tomamos $m = 2$ e $n = 3$, $G = \mathbb{Z}/2\mathbb{Z}$, $H = S_3$ e $X = \{1, 2, 3\}$, o produto coroa de G por H é:

$$(\mathbb{Z}/2\mathbb{Z})^3 \wr S_3 = \{(0,0,0)\sigma, (0,0,1)\sigma, (0,1,0)\sigma, (1,0,0)\sigma, (0,1,1)\sigma, (1,0,1)\sigma, (1,1,0)\sigma, (1,1,1)\sigma\}$$

onde $\sigma \in S_3$.

Polo tanto, o produto coroa simplemente mestura os elementos de $(\mathbb{Z}/m\mathbb{Z})^n$ de acordo coa acción de S_n e o resultado é unha permutación do elemento orixinal.

Este exemplo é unha peza básica para describir o grupo do cubo de Rubik.

Capítulo 4

O grupo do cubo de Rubik

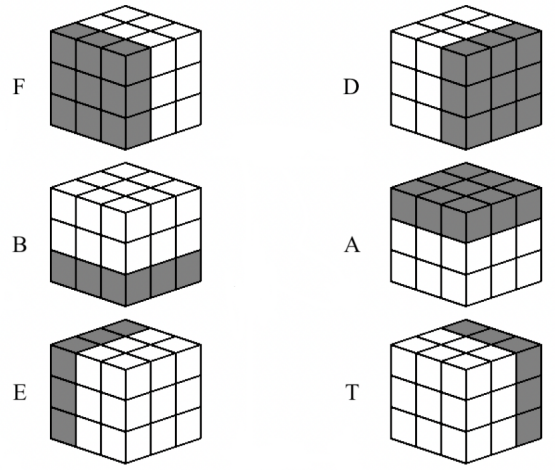
Chegados a este punto, temos toda a matemática necesaria para introducir e describir matematicamente o grupo do cubo de Rubik clásico, de dimensións $3 \times 3 \times 3$.

Antes, cabe dicir que o cubo ten seis caras, compostas cada unha por nove pezas da mesma cor. En cada cara, a peza do centro é fixa, non pode moverse e, para resolvelo, todas as pezas da mesma cor teñen que estar na mesma cara para as seis cores.

4.1. Notación

Para resolver o cubo, necesitamos xirar as distintas caras e, para describir estes xiros, imos introducir a notación que usaremos. Imos supoñer que cada xiro dunha cara é de 90^{o} no sentido das agullas do reloxo.

- F denota a cara da Fronte,
- D denota a cara da Dereita,
- B denota a cara de aBaixo,
- A denota a cara de Arriba,
- E denota a cara da Esquerda,
- T denota a cara de aTrás.



Desta forma, os xiros no sentido das agullas do reloxo dunha cara son feitas dende a perspectiva do que está a resolvelo, como se estivese mirando cara a esa cara en particular. Por exemplo, denotamos como AFE xirar a cara de arriba 90^{o} no sentido das agullas do reloxo, facer logo o mesmo coa cara da fronte e finalmente coa cara da esquerda. A^2 corresponderíase con facer dous xiros seguidos na cara de arriba ($A^2 = AA$), é dicir,un xiro de 180^{o}.

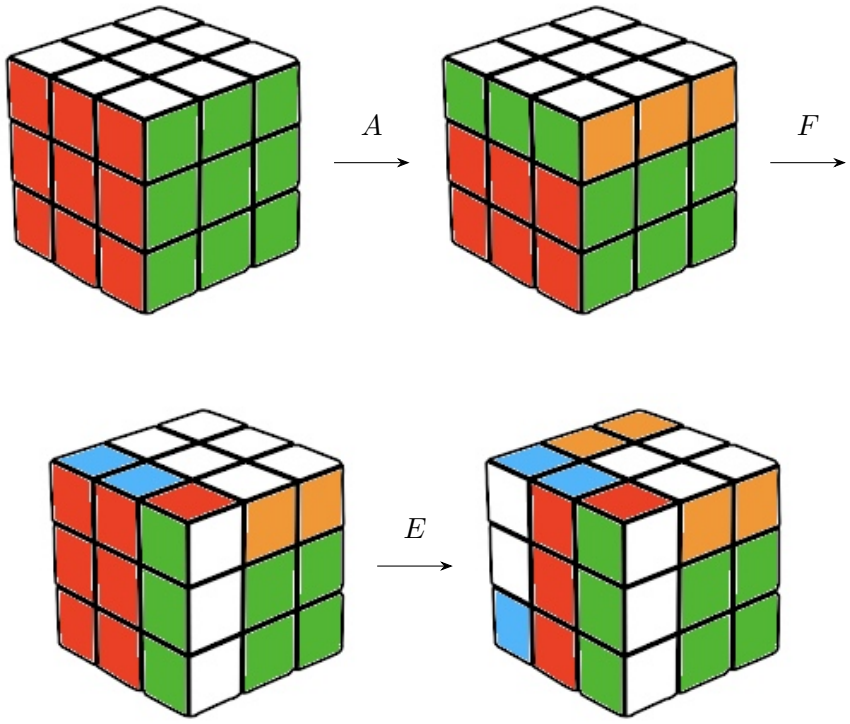


Figura 4.2: Movemento AFE

O inverso de cada xiro consistirá no xiro de 90^{o} esta vez no sentido contrario ás agullas do reloxo e será denotado como A^{-1}, F^{-1}, E^{-1},D^{-1}, T^{-1} e B^{-1} dependendo da cara coa que esteamos traballando. Facendo $(AFE)^{-1} = E^{-1}F^{-1}A^{-1}$ estamos xirando a cara da esquerda 90^{o} no sentido contrario ás agullas do reloxo, facendo o mesmo despois coa cara da fronte e, por último, coa de arriba, desfacendo o movemento anterior e volvendo así á posición inicial.

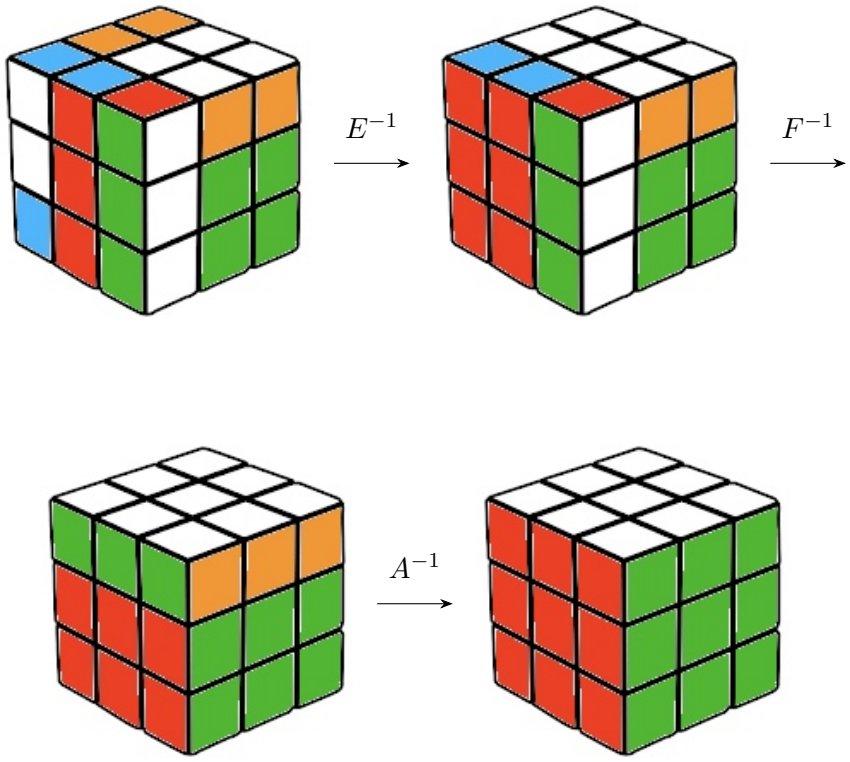
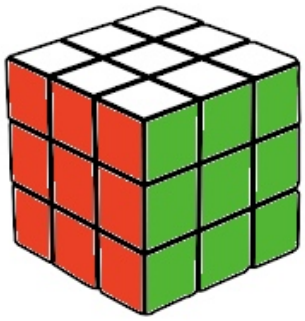


Figura 4.4: Movemento $(AFE)^{-1} = E^{-1}F^{-1}A^{-1}$

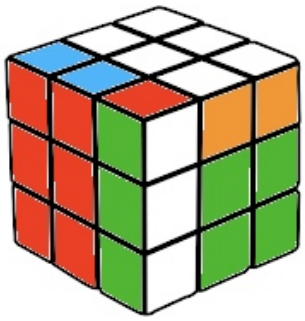
4.2. Grupo do cubo

Como o cubo está formado por $6 \times 9 = 54$ pezas que van ser movidas cos xiros, calquera posición do cubo pode ser descrita como unha permutación, e entón o grupo do cubo de Rubik é un subgrupo do grupo de permutacións de 54 elementos, S_{54}. En conclusión, o grupo de permutacións $G = \langle A, F, E, D, T, B \rangle \subset S_{54}$ é o chamado **Grupo do cubo de Rubik**.

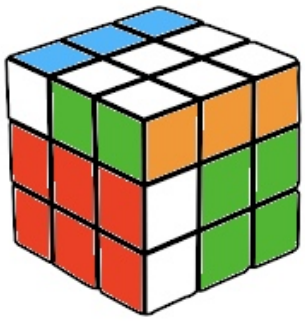
Non é un grupo abeliano xa que non é o mesmo facer, por exemplo, AF que FA.



(a) Posición orixinal

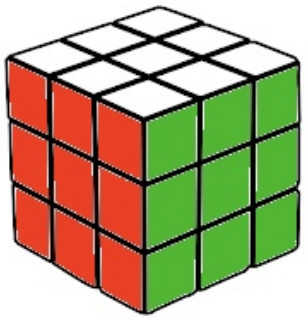


(b) AF

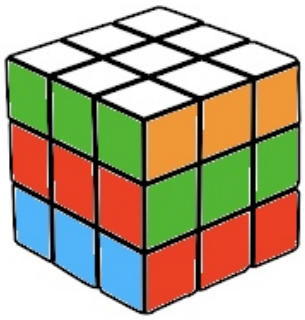


(c) FA

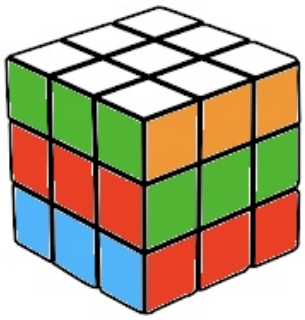
Non obstante, hai algúns movementos que si conmutan, como por exemplo $AB = BA$.



(a) Posición orixinal



(b) AB



(c) BA

Hai tres tipos diferentes de pezas no cubo segundo as caras que teñen visibles: as das esquinas (que teñen tres caras visibles), que a partir de agora denominaremos como vértices (V); as pezas que chamaremos arestas (A) (con dúas caras visibles); e os centros (C) (cunha soa cara visible).

Figura 4.7: Tipos de pezas do cubo.

Non todas as permutacións van ser posibles no cubo xa que os vértices só poden ir aos ocos dos vértices, as arestas só poden ir aos ocos doutras arestas e, como xa dixemos antes, os centros son fixos. Outras permutacións non van ser posibles fisicamente e, debido a isto, G é un subgrupo de S_{54} e non son isomorfos.

4.2.1. Vértices

Como se pode observar na figura, e xa mencionamos antes, cada vértice ten tres caras. En total, no cubo, hai oito vértices e cada unha das súas caras se encontra nunha cara diferente do cubo.

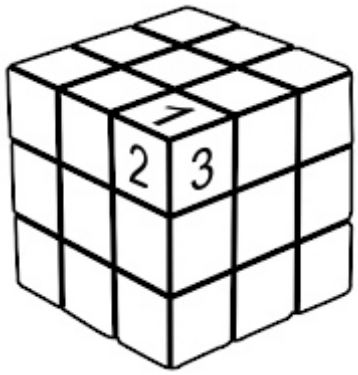


Figura 4.8: As tres caras dun vértice

Na figura 4.8 podemos ver que a cara 1 do vértice se sitúa na cara de arriba, a cara 2 na fronte e a 3 na dereita. É posible reorientar as caras dos vértices, mandando o 1 a posición do 2, o 2 ao 3 e o 3 ao 1 ou mandando o 1 ao 3, o 3 ao 2 e o 2 ao 1. Isto quere dicir

que estamos traballando con grupos cíclicos de tres elementos. Como hai un total de oito vértices, calquera reorientación dunha cara dun vértice pode ser descrita polo conxunto $C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 = C_3^8$.

De forma parecida podemos describir as posibles reorganizacións dos vértices, cada un pode ocupar o oco dos oito, polo que poden ser descritas polo grupo simétrico de oito elementos S_8.

Lema 4.1. *A posición de todas as pezas das esquinas, os vértices, do cubo de Rubik poden ser descritas polo grupo* $C_3^8 \wr S_8$.

Demostración. Séguese da definición de produto coroa e do feito de que cada posición de cada vértice pode ser descrita pola súa posición no cubo e a orientación cíclica das tres caras da peza. [3] □

4.2.2. Arestas

O cubo ten doce arestas, compostas cada unha delas por dúas caras que se encontran en distintas caras do cubo.

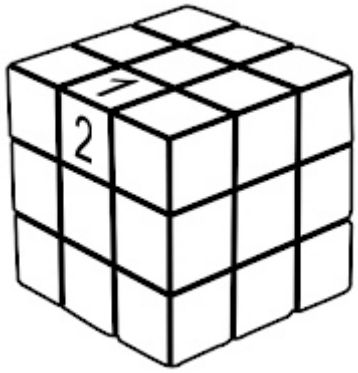


Figura 4.9: As dúas caras dunha aresta.

Na figura 4.9 podemos ver que a cara 1 da aresta se sitúa na cara de arriba e a cara 2 na cara da fronte. Estas dúas caras poden intercambiarse pasando 1 á posición de 2 e 2 á de 1 polo tanto pertencen ao grupo cíclico de dous elementos C_2. Como o cubo ten doce arestas e as súas caras poden ocupar a posición de calquera outra delas, cada unha estará no conxunto $C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 = C_2^{12}$.

Podemos reorganizar cada unha das doce arestas no oco de calquera outra igual que fixemos no caso dos vértices, entón, estas posibles reorganizacións poden ser descritas polo grupo simétrico de doce elementos S_{12}.

Lema 4.2. *A posición de todas as arestas do cubo de Rubik poden ser descritas polo grupo* $C_2^{12} \wr S_{12}$.

Demostración. Séguese da definición de produto coroa e do feito de que cada posición de cada aresta pode ser descrita pola súa posición no cubo e a orientación cíclica das súas dúas caras. [3] □

4.3. Posición do cubo

Dos lemas 4.1 e 4.2 obtemos que cada vértice do cubo pode ser expresado como unha 8-tupla e cada aresta como unha 12-tupla. Para determinar cada compoñente individual destas tuplas necesitamos establecer un sistema de numeración. [5]

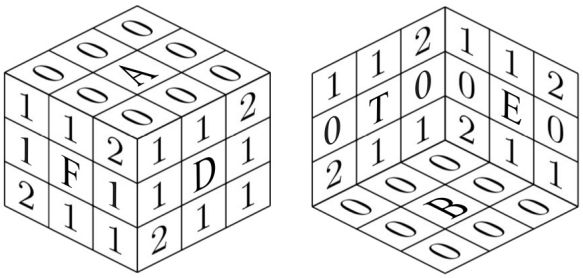
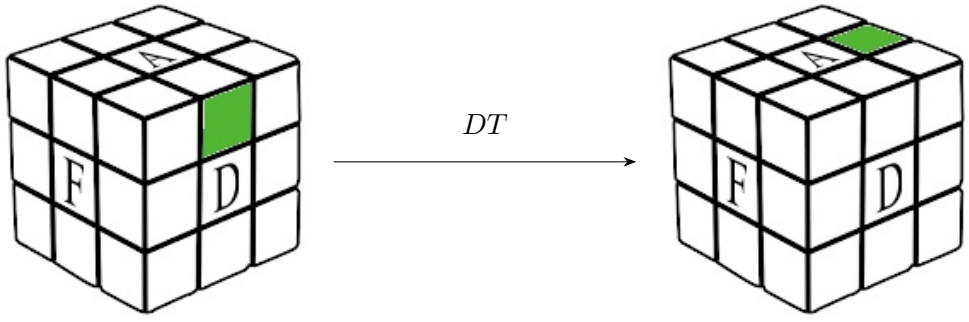


Figura 4.10: As marcas de orientación fixa.

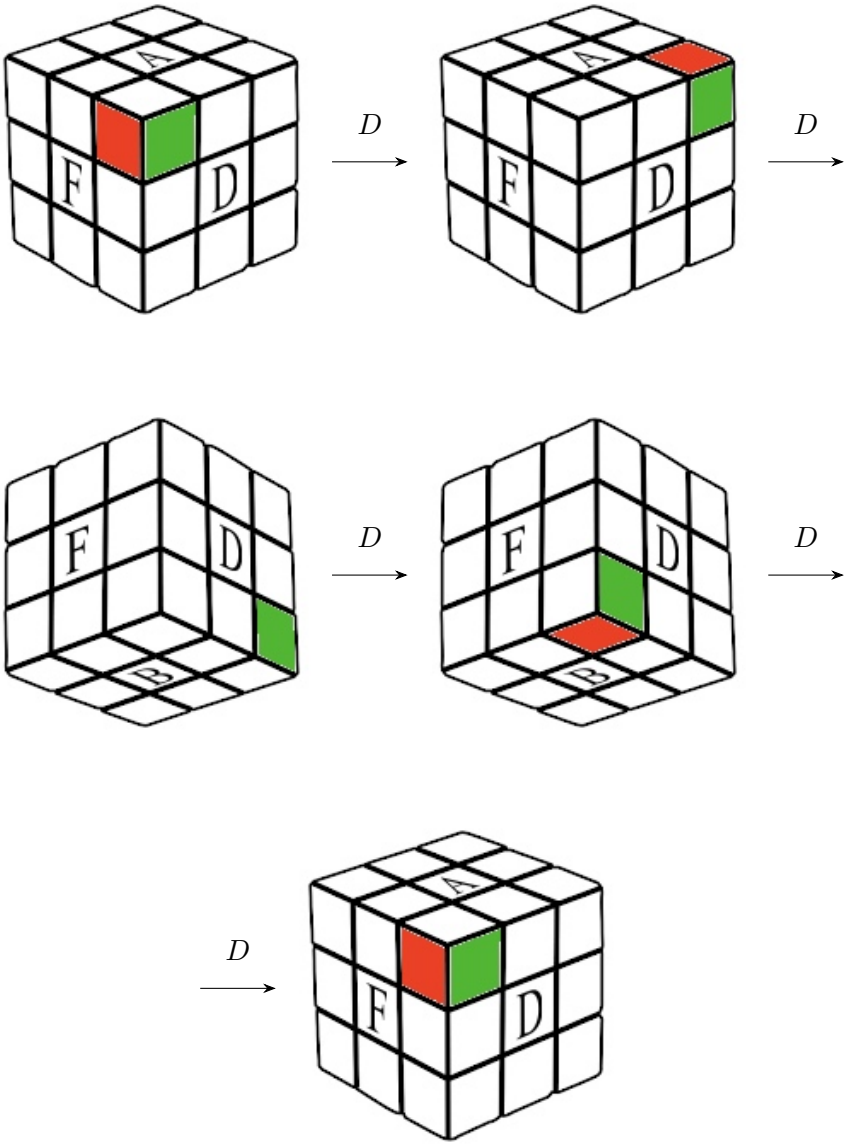
Para calquera cara arbitraria, á posición da cara se lle asigna o número correspondente da figura 4.10 e, aínda que as caras se van mover polo cubo, o sistema de numeración permanece fixo.

Ilustremos isto cun exemplo, consideremos a aresta superior da cara da dereita, está marcada incicialmente cun 1 pero se facemos o movemento DT vaise para a cara de arriba no lado dereito e o numero asignado para esta posición é o 0.



Con cada xiro, o número de orientación dunha aresta é cambiado por 0 mod2 ou 1 mod2.

Se consideramos agora o vértice que comparten as caras F, A e D.



A cara vermella comeza co número 2, logo ten o número 0, número 2, número 0 e finalmente volve á posición inicial e polo tanto co número 2. A cara verde comeza co número 1, vai ao número 2, número 1, número 2 e despois á posición inicial co número 1. Por último, a cara branca ten inicialmente o número 0, logo o 1, 0, 1 e volve ao 0.

Con cada xiro das caras A e B, o número de orientación dun vértice permanece fixo (0 mod3) mais co xiro das caras restantes é cambiado por 1 mod3 ou 2 mod3.

4.4. Teoremas fundamentais

Nesta sección introduciremos os dous teoremas fundamentais que establecen as propiedades que cumpren os movementos que son posibles no cubo e o seu significado.

Teorema 4.3 (Primeiro teorema fundamental)**.** *Sexa $c \in C_3^8$, $r \in S_8$, $d \in C_2^{12}$ e $s \in S_{12}$. A 4-tupla (c, r, d, s) correspóndese cunha posible posición do cubo se e só se:*

1. $sign(r) = sign(s)$
2. $c_1 + c_2 + \cdots + c_8 = 0$ *(mod3)*
3. $d_1 + d_2 + \cdots + d_{12} = 0$ *(mod2)*

Demostración. ($\Rightarrow$) Sexa $c \in C_3^8$, $r \in S_8$, $d \in C_2^{12}$, $s \in S_{12}$ e $g \in G$ sendo g un movemento que reorganiza o cubo da posición inicial ao estado (c, r, d, s). Entón g pode ser escrito como $g = L_1, L_2, \ldots, L_n$ con $L_i \in \{A, F, E, D, T, B\}$.

1. Con cada movemento móvense un total de catro arestas e catro vértices, é dicir, o mesmo número de arestas e de vértices. Cada permutación é un 4-ciclo, que é impar e ten polo tanto $sign = -1$. Polo que para cada g temos: $sign(r) = \prod_{k=1}^{n} sign(L_i) = sign(s)$.

2. Se L_i é A ou B, entón c non cambia (coas nosas convencións), xa que todos os vértices permanecen na mesma cara. Se, polo contrario, L_i é un dos restantes (F, E, D, T), entón dous vértices son movidos. Un vértice é movido cara a abaixo da cara A e outro é movido cara a arriba á cara A. Desta forma, as compoñentes de c ou diminúen 1(mod3) ou incrementan 1(mod3) respectivamente. Isto implica que para cada F, E, D ou T, $c_1 + c_2 + \cdots + c_8 = 1$ (mod3) -1 (mod3)$= 0$ (mod3). Polo tanto, para cada movemento g, $c_1 + c_2 + \cdots + c_8 = 0$ (mod3) consérvase o número total de xiros dos oitos vértices.

3. Por cada movemento g, catro arestas son reorganizadas, polo que $d_1 + d_2 + \cdots + d_{12} = 4$ (mod2) $= 0$ (mod2), consérvase o número total de xiros das doce arestas.

($\Leftarrow$) Sexa $M = (c, r, d, s)$ verificando as condicións 1, 2 e 3. A condición 1 dinos que $sign(r) = sign(s)$ polo que hai unha igualdade na paridade das permutacións, é dicir, as permutacións dos vértices e das arestas son ambas pares ou impares. Supoñamos que son pares ($sign(r) = sign(s) = 1$). Se fosen impares basta aplicar un dos movementos (A, F, E, D, T, B) e a nova posición será par.

Agora consideremos o movemento 3-cíclico dun vértice, por exemplo,

$$L = DT^{-1}DF^2D^{-1}TDF^2D^2$$

.

O movemento L move ciclicamente os vértices arriba-fronte-esquerda (a_1), arriba-fronte-dereita (a_2) e arriba-atrás-dereita (a_3) sen cambiar os demais (a_4, a_5, a_6, a_7 e a_8) e sen cambiar tamén o resto de pezas. Para cada a_i con $i = 4, 5, 6, 7, 8$ existe un movemento x de $\{A, F, E, D, T, B\}$ de como moito dous movementos de forma que a_i é movido á posición de a_3 sen cambiar as posicións de a_1 e a_2. Se agora aplicamos a transformación xLx^{-1}, conxugación de L por x, creamos o 3-ciclo (a_1, a_2, a_i), que pode ser obtido para calquera dos a_i co movemento x apropiado. Isto xera todas as permutacións pares dos vértices polo que existe un movemento apropiado x que devolverá todos os vértices ás súas posicións iniciais.

Podemos facer un procedemento análogo para as arestas. Consideremos agora o movemetento 3-cíclico dunha aresta, por exemplo,

$$L^* = D^2AFT^{-1}D^2F^{-1}TAD^2$$

.

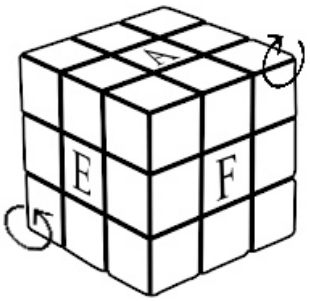
O movemento L^* move ciclicamente as arestas arriba-fronte (b_1), arriba-atrás (b_2) e arriba-dereita (b_3) sen cambiar as demais (b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11} e b_{12}) e sen cambiar tamén o resto de pezas. Como no caso dos vértices, para cada b_i con $i = 4, 5, 6, 7, 8, 9, 10, 11, 12$ existe un movemento y de $\{A, F, E, D, T, B\}$ de como moito dous movementos de forma que b_i é movido á posición de b_3 sen cambiar as posicións de b_1 e b_2. Aplicando agora a transformación (conxugación) yL^*y^{-1} creamos o 3-ciclo (b_1, b_2, b_i), que pode ser obtido para calquera dos b_i co movemento y apropiado. Isto xera todas as permutacións pares das arestas polo que existe un movemento apropiado y que devolverá todas as arestas ás súas posicións iniciais.

O único que queda por facer é reorientar as pezas para que as caras coincidan nas cores.

A condición 2 dinos que hai unha preservación dos xiros totais (o número de xiros no sentido das agullas do reloxo e no sentido contrario ás agullas do reloxo é o mesmo). Isto significa que existe un movemento que xira exactamente dous vértices e conserva a orientación e posición de todas as outras pezas. Concretamente, o movemento

$$L_1 = (D^{-1}B^2DT^{-1}A^2T)^2$$

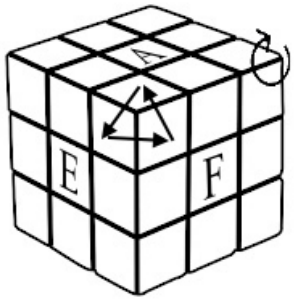
que xira o vértice arriba-fronte-dereito 120^{o} e xira o vértice abaixo-abaixo-esquerdo -120^{o}.



Este movemento pode ser modificado para cambiar dous vértices calquera. Para empezar a cadrar as caras dos vértices, primeiro hai que xirar calquera par no sentido das agullas do reloxo e en sentido contrario nas orientacións das solucións. As orientacións do vértice restante danse en triplos xa que os vértices cumpren $\sum_{i=1}^{8} c_i = 0$ mod3, polo tanto daránse en 3 xiros no sentido horario ou en 3 xiros no sentido antihorario. A estas tres pezas chamarémolas c_1, c_2 e c_3. Os vértices restantes poden ser resoltos mediante unha secuencia de movementos de xiro dos vértices, por exemplo,

$$L_1^* = E^{-1}B^2ETB^2T^{-1}ATB^2T^{-1}E^{-1}B^2EA^{-1}$$

ou un movemento similar para dous dos vértices restantes que teñen que ser reorientados.

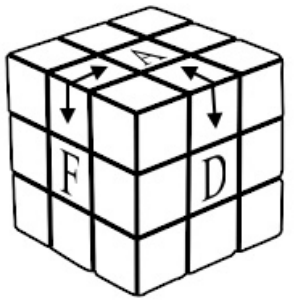


Agora, L_1^* vai resolver un dos vértices restantes, por exemplo c_1, e reorientar o outro, digamos c_2, na posición oposta do vértice intacto c_3. Isto é, se c_3 necesita ser resolto por un xiro no sentido horario entón L_1^* reorientará c_2 nunha posición que necesite un xiro no sentido antihorario para ser resolto e viceversa. Os dous vértices restantes poden ser resoltos co movemento L_1 apropiado e así quedarían todos resoltos, é dicir, existen movementos para reorientar calquera dous vértices que manteñen o resto das pezas intactas e permiten cadrar as cores destes vértices coas cores das caras do cubo.

A condición 3 dinos que $d_1 + d_2 + \cdots + d_{12} = 0 \pmod 2$, é dicir, hai un número par de arestas que teñen que ser volteadas pero existe un movemento que voltea exactamente dúas arestas e preserva a orientación e posición das restantes pezas. Tomamos o movemento

$$L_2 = EFD^{-1}F^{-1}E^{-1}A^2DADA^{-1}D^2A^2D$$

que voltea a aresta ariba-fronte e a arriba-dereita e mantén o resto do cubo intacto.



Este movemento pode ser modificado de forma apropiada para voltear dúas arestas calquera. Como hai un número par de arestas, todas elas poden ser devoltas ás súas orientacións da solución do cubo.

En conclusión M é unha posición resoluble no cubo de Rubik e polo tanto, (c, r, d, s) é unha posición posible do cubo. [3] □

Este teorema vén a dicir que calquera posición posible do cubo cumpre que a paridade das permutacións das arestas e dos vértices é a mesma (debido a que con cada movemento móvense catro de cada) así como a conservación do número total de xiros dos oitos vértices (en módulo 3) e das doce arestas (en módulo 2) co sistema de numeración fixado na figura 4.10.

Teorema 4.4 (Segundo teorema fundamental)**.** *Unha operación do cubo é posible se e só se se verifican:*

1. *O número total de ciclos de arestas e de vértices de lonxitude par é par.*

2. *O número de ciclos de vértices xirados á dereita é igual ao número de ciclos de vértices xirados á esquerda (mod3).*

3. *Hai un número par de ciclos de arestas reorientados.*

Demostración. ($\Rightarrow$) Sexa L unha operación no cubo que o modifique da posición inicial (na que está o cubo resolto) á dada por $g = (c, r, d, s)$, onde $c \in C_3^8$, $r \in S_8$, $d \in C_2^{12}$ e $s \in S_{12}$.

1. Polo apartado (1) do teorema 4.3, $sign(r) = sign(s)$. Isto significa que a permutación é par polo que a lonxitude dos ciclos de arestas e vértices é par.

2. Para calquera movemento L, os vértices son movidos á dereita, á esquerda, ou permanecen no sitio. Entón o ciclo cambia a suma dos c_i por 2,1 ou 0(mod3) respectivamente. Polo teorema 4.3, $\sum_{i=1}^{8} c_i = 0$ o número de xiros á dereita e o número de xiros á esquerda é o mesmo (teñen que compensarse).

3. Un ciclo dunha aresta só se reorienta se é cambiado por un número impar, isto é $d_i = 1$ para algún $i = \{1, 2, ..., 12\}$. Polo teorema 4.3, $\sum_{i=1}^{12} d_i = 0$ pero isto significa que se un ciclo dunha aresta é reorientado, entón outro ciclo doutra aresta ten que ser reorientado para que a suma sexa cero, polo tanto, ten que haber un número par de ciclos de arestas reorientados.

($\Leftarrow$) Supoñamos certas 1, 2 e 3. Polo teorema 4.3 exite un movemento L que modifica a posición inicial do cubo pola posición g. Existe tamén o movemento M^{-1} que modifica a posición g pola posición inicial. Agora, asumindo que M e M^{-1} satisfan 1, 2 e 3 temos que ambas son operacións válidas no cubo de Rubik, polo tanto, se 1, 2 e 3 son certas, a operación é posible. [3] □

Este teorema caracteriza os movementos posibles. Os teoremas eliminan as posicións e orientacións fisicamente imposibles.

Grazas a eles temos as propiedades que cumpre o cubo e poderemos obter así a orde do grupo do cubo. Como sabemos, hai 8! formas de combinar os vértices do cubo. Pola condición 2 do teorema 4.3 sete destas poden orientarse independentemente e a orientación da octava dependerá das sete anteriores, dando lugar a 3^7 posibilidades. O mesmo pasa coas arestas, hai 12! formas de dispoñelas, once poden ser volteadas independentemente e a rotación da duodécima dependerá das anteriores, dando lugar a 2^{11} posibilidades pola condición 3 do teorema 4.3. Ademais, pola condición 1, temos que o número de permutacións pares é o mesmo que o de permutacións impares. Con todo isto temos que:

$$|G| = \frac{|C_3^7| \cdot |S_8| \cdot |C_2^{11}| \cdot |S_{12}|}{2} = \frac{3^7 \cdot 8! \cdot 2^{11} \cdot 12!}{2} = 43252003274489856000$$

Capítulo 5

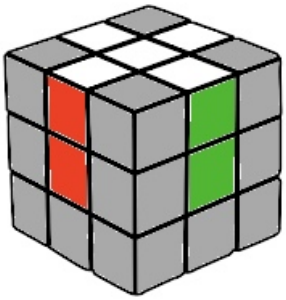
Unha posible solución para o cubo de Rubik

Finalmente, con todos os resultados previos, estamos no lugar de dar indicacións para a resolución do cubo de Rubik.

O método de resolución que imos explicar, o máis típico dada a súa facilidade de aplicación para principiantes neste ámbito, consiste na resolución capa a capa.

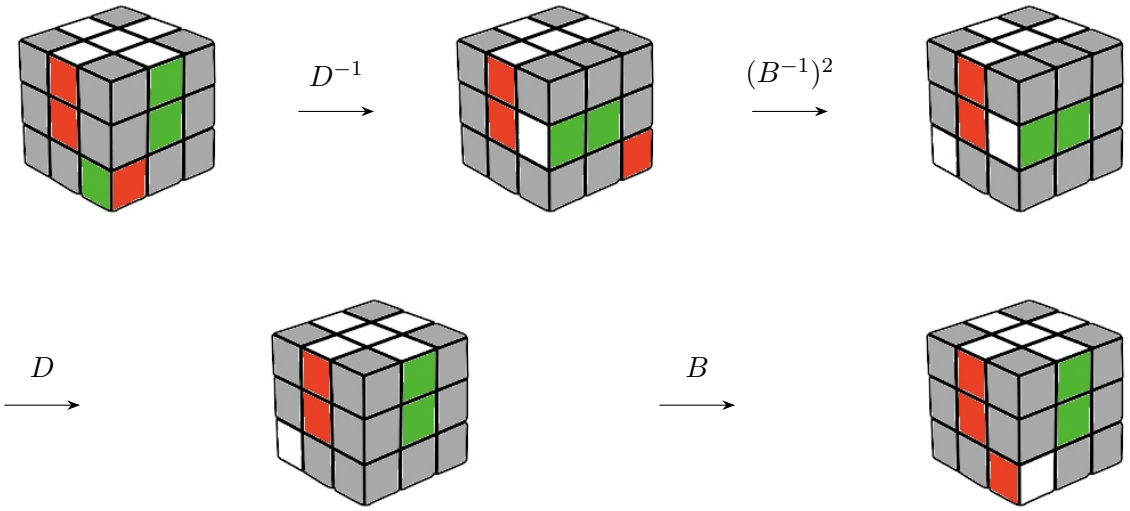
5.1. Primeira capa

Para a primeira capa non hai un algoritmo directo de resolución, ten que facerse mediante intuición pero algunha indicación podemos dar. Seleccionamos en primeiro lugar a cara que imos resolver e hai que conseguir facer unha cruz levando as arestas da cara á súa posición, na que ten que coincidir a cor en ambas caras nas que se encontra cada aresta da seguinte forma:



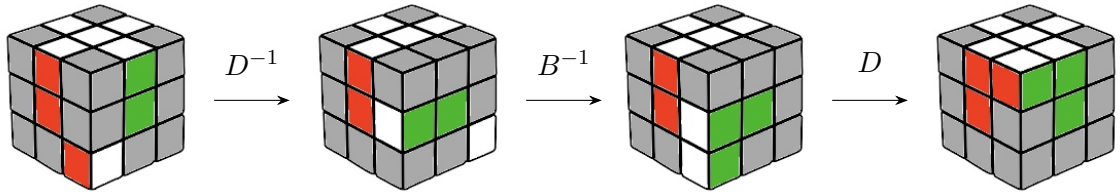
Despois hai que conseguir reorientar correctamente os vértices un a un facendo que

cadren as cores coas tres caras que comparten cada vértice. Primeiro levamos o vértice que queremos colocar á capa de abaixo, xusto debaixo de onde o queremos colocar. Supoñamos que este vértice está agora na cara da fronte abaixo á dereita. Hai tres posibilidades, que a cara branca estea na cara F, na D ou na B. Se está en B basta con aplicar o movemento $D^{-1}(B^{-1})^2DB$ para estar nalgún dos outros dous casos.

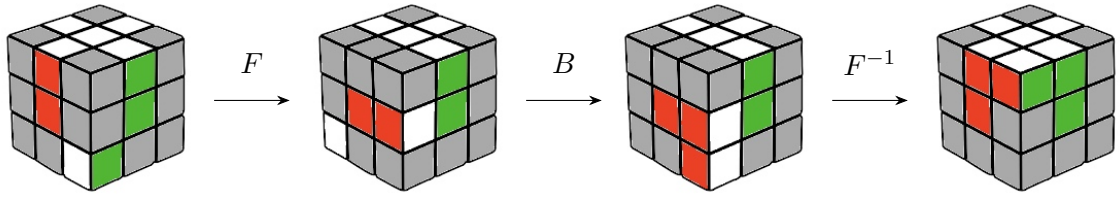


Agora xiramos a capa de abaixo ata que a outra cor que non estea en B estea na cara co centro da mesma cor. Temos dúas posibilidades:

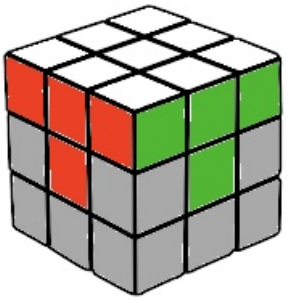
- Se a cara branca está en D e a outra cor en F aplicamos o movemento $D^{-1}B^{-1}D$.



- Se a cara branca está en F e a outra cor en D aplicamos o movemento FBF^{-1}.



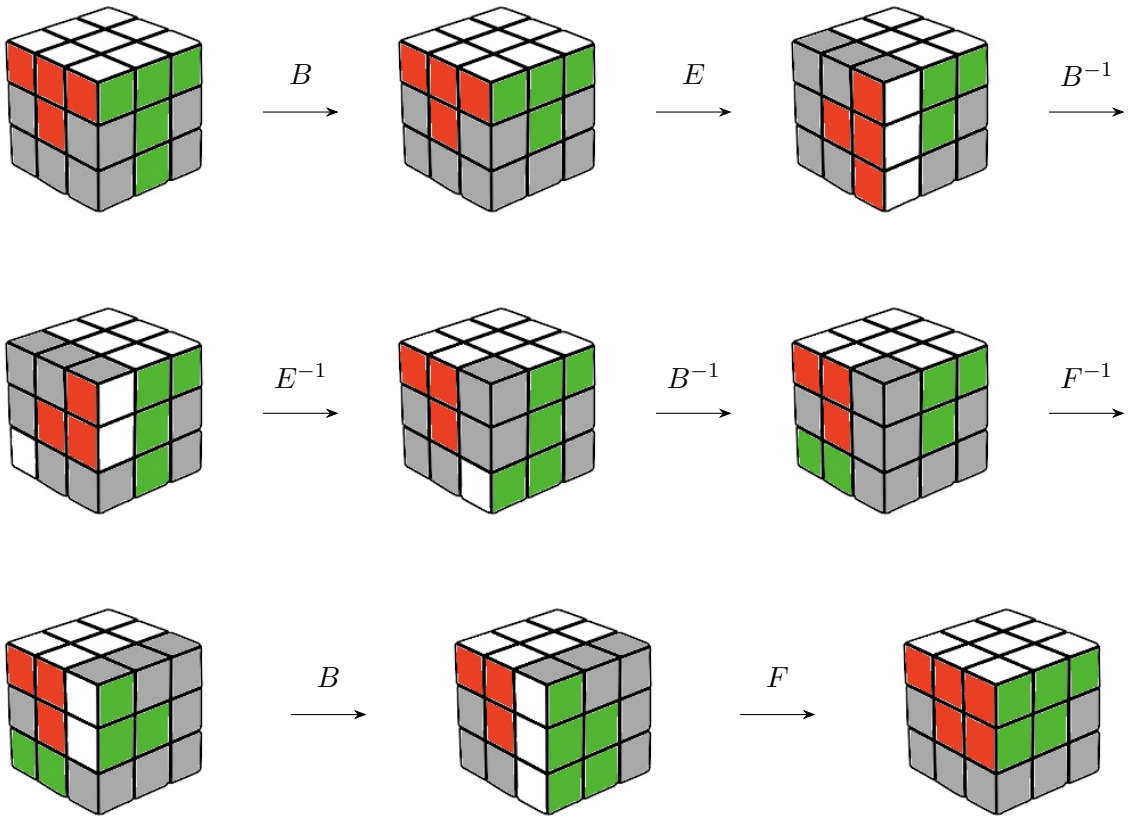
Despois de realizar este proceso para os catro vértices teriamos:



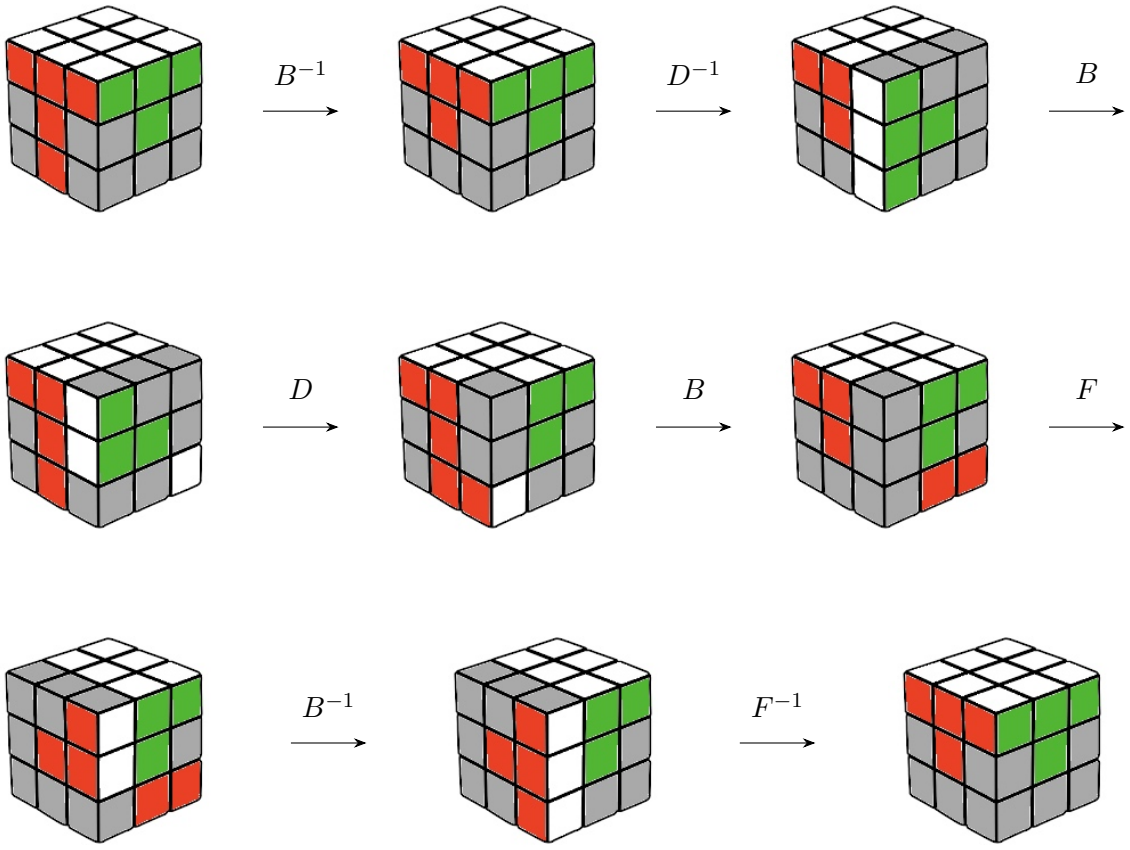
5.2. Segunda capa

Imos agora coa segunda capa. Para resolvela temos que colocar as catro arestas que faltan para completala. Buscamos na capa inferior unha aresta da segunda capa, emparellamos a cor que se encontra na cara F co seu centro e vemos se a cor que se encontra na cara B corresponde coa cor do centro da cara E ou D:

- Se é E aplicamos o movemento $BEB^{-1}E^{-1}B^{-1}F^{-1}BF$

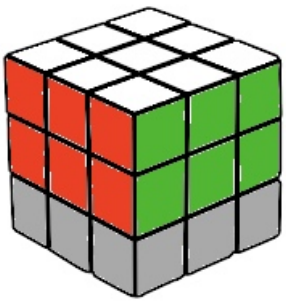


- Se é D aplicamos o movemento $B^{-1}D^{-1}BDBFB^{-1}F^{-1}$



No caso de que non atopemos a aresta na capa inferior estará na segunda capa (xa que a primeira xa está resolta). O que temos que facer entón é introducir outra que non nos interese nesa posición cun dos movementos anteriores e así chegamos a un dos casos xa vistos.

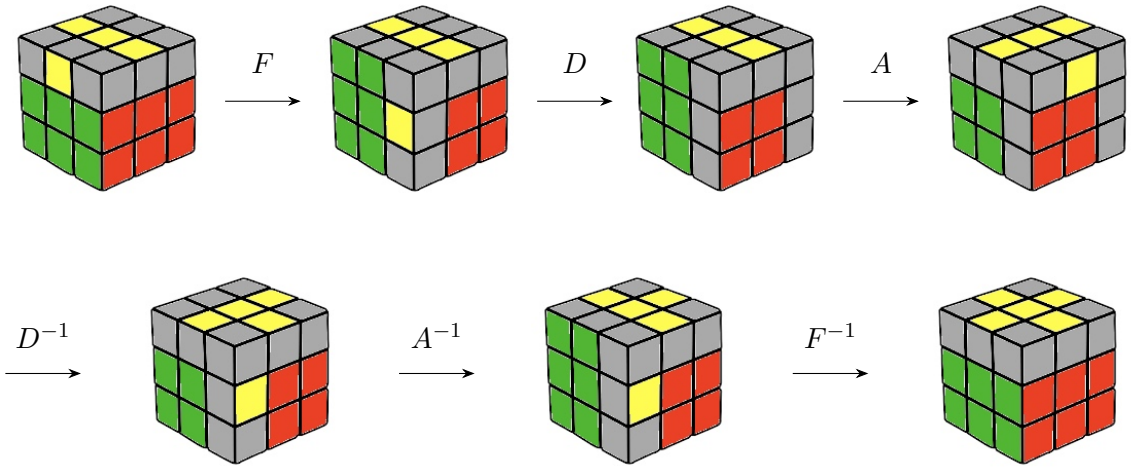
O resultado tras este proceso é:



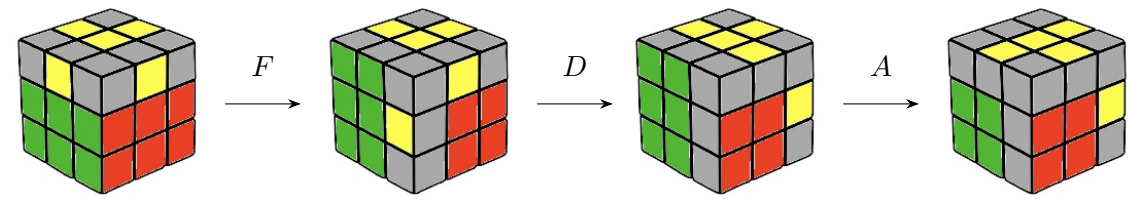
5.3. Terceira capa

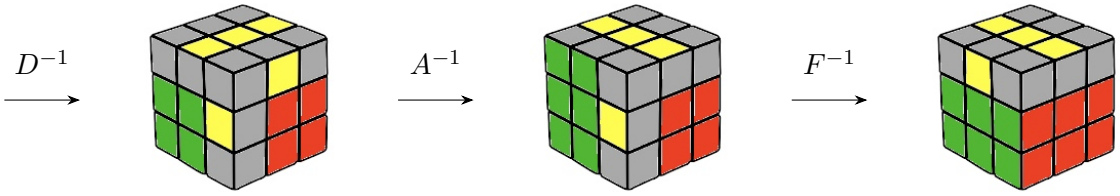
Para resolver a terceira capa imos comezar coas arestas. En primeiro lugar colocamos a cara resolta abaixo e imos tratar de conseguir, como na primeira capa, unha cruz na de arriba (no noso exemplo vai ser a cara amarela) aínda que as arestas non queden correctamente colocadas. Neste caso temos que poñer as arestas de dúas en dúas, facelo dunha en unha é imposible. O movemento que realizaremos sempre será o mesmo pero o número de veces que o faremos dependerá da posición das arestas (pero sempre hai un número par delas que teñen na cara de arriba a cor amarela):

- Pode darse que xa estean todas as de cor amarelo na cara amarela (neste caso non facemos nada).
- Se as únicas arestas coa cor amarela na cara amarela son as que comparten as caras A e D e A e E (dúas arestas "opostas") utilizaremos o movemento $FDAD^{-1}A^{-1}F^{-1}$ unha soa vez e chegaremos á cruz.

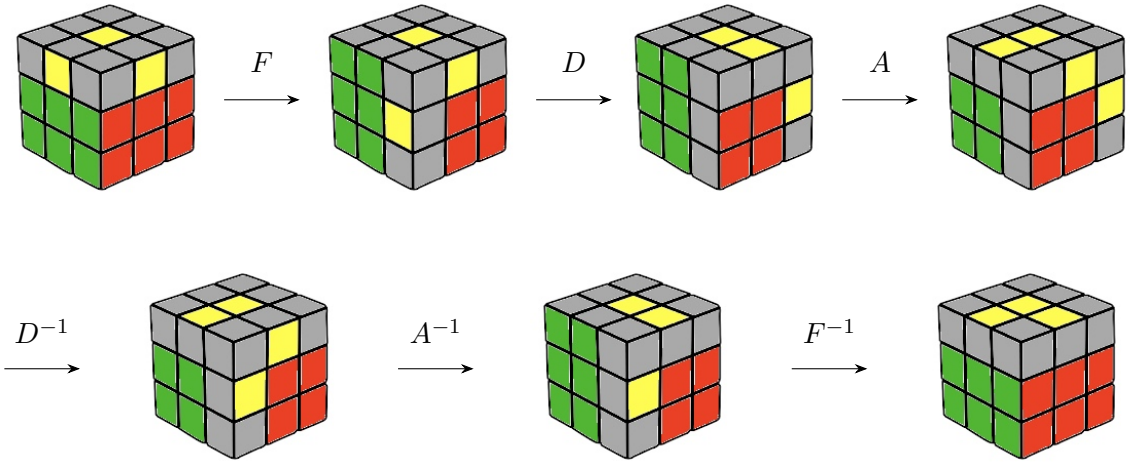


- Se as únicas arestas coa cor amarela na cara amarela son as que comparten as caras A e E e A e T (dúas arestas "contiguas") utilizaremos o movemento $FDAD^{-1}A^{-1}F^{-1}$ dúas veces e chegaremos á cruz. Nótese que se realizamos o movemento unha soa vez chegamos ao caso anterior

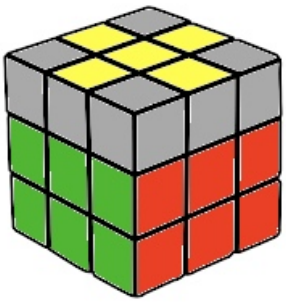




- Se non temos ningunha aresta coa cor amarela na cara amarela basta con realizar o movemento $FDAD^{-1}A^{-1}F^{-1}$ tres veces e chegaremos á cruz. Neste caso pasamos por todas as etapas citadas anteriormente.

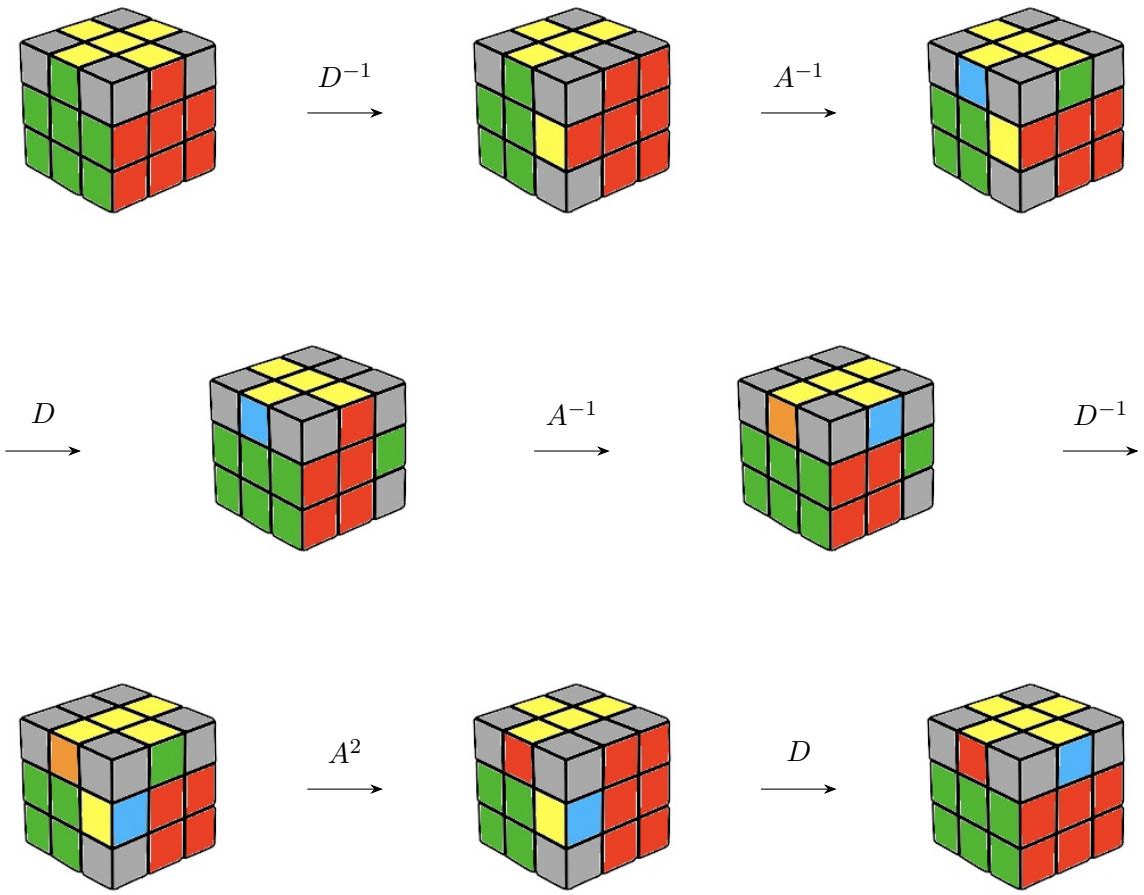


O resultado tras facer o proceso indicado en cada caso é:



Agora temos que reorientar as arestas de forma que coincidan as cores coa cara na que se encontran, é dicir, que a cruz estea ben colocada. Para isto, o primeiro que imos facer é xirar a cara de arriba ata que estean ben orientadas dúas arestas, é dicir, que as dúas cores das arestas coincidan coas cores dos centros das dúas caras nas que se encontran cada unha delas. Poden darse dúas posibilidades, pero como antes, o movemento vai ser o mesmo e só variará o número de veces que o fagamos:

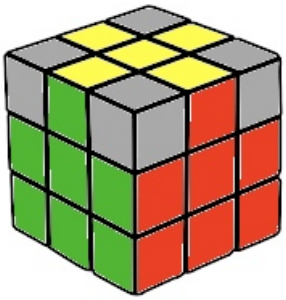
- Se as dúas arestas que están ben orientadas están en dúas caras contiguas colocamos o cubo para que estas caras sexan F e D e aplicamos o movemento $D^{-1}A^{-1}DA^{-1}D^{-1}A^2D$.



(Xirando a cara de arriba en sentido antihorario xa chegamos ao resultado de ter as catro arestas ben orientadas)

- Se as dúas arestas que están ben orientadas están en dúas caras opostas colocamos o cubo para que estas caras sexan F e T e aplicamos o mesmo movemento, $D^{-1}A^{-1}DA^{-1}D^{-1}A^2D$, pero nesta ocasión dúas veces xa que coa primeira chegamos ao caso anterior.

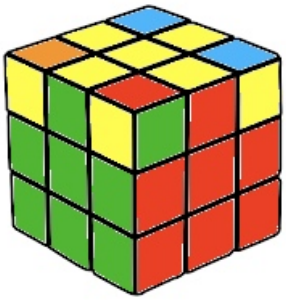
Despois deste proceso obtemos o seguinte:



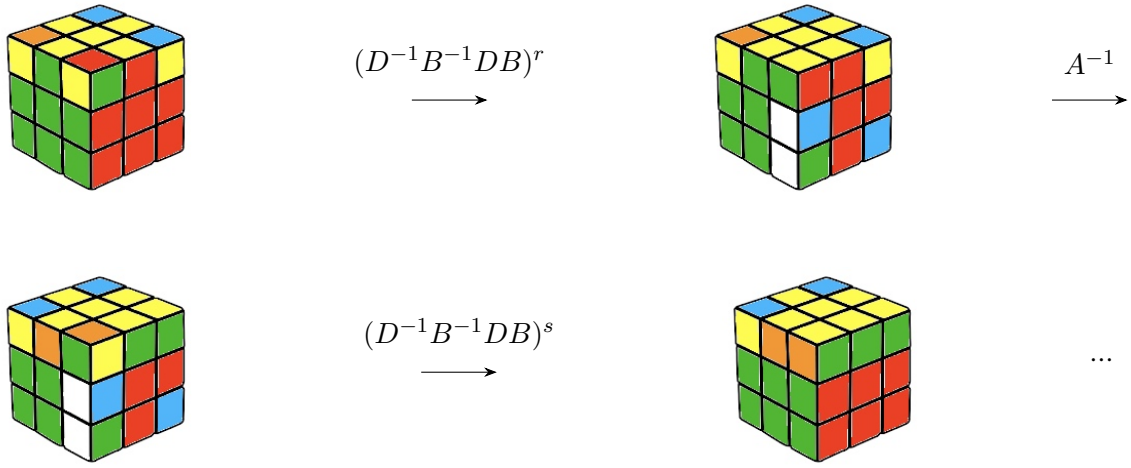
Neste punto, o único que queda para resolver o cubo na súa totalidade é colocar e orientar os vértices desta capa. Observamos o cubo e vemos en que posibilidade estamos destas dúas:

- Se atopamos un vértice que está na súa posición aínda que estea mal orientado observámolo de forma que ese vértice sexa o compartido polas caras F, D e A e aplicamos o movemento $ADA^{-1}E^{-1}AD^{-1}A^{-1}E$. Prodúcese unha permutación en sentido antihorario dos tres vértices que non estaban no seu sitio. Se aínda non están no seu sitio aplicamos o movemento outra vez.
- Se ningún vértice está ben colocado aplicamos o mesmo movemento, $ADA^{-1}E^{-1}A$ $D^{-1}A^{-1}E$, ata que algún estea no seu sitio e entón estamos na situación anterior.

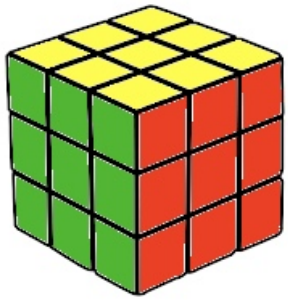
Un posible resultado (hai varios dependendo da orientación de cada vértice) despois destes pasos podería ser:



Finalmente, o único restante é reorientar de forma correcta estes vértices, bastará aplicarlle o movemento $D^{-1}B^{-1}DB$ a un vértice o número de veces necesario para que estea ben orientado. Cando consigamos isto observaremos que fixemos cambios na parte inferior do cubo. Agora xiraremos a capa superior do cubo ata que coloquemos na posición do vértice que acabamos de orientar o seguinte ao que lle queremos facer este proceso e realizamos o mesmo movemento ata que quede ben orientado.



Despois de facer isto cos catro vértices, teríamos ao fin o cubo resolto na súa totalidade:



5.4. Observacións matemáticas

Por último, imos comentar a matemática detrás dalgúns dos movementos que acabamos de mencionar na sección anterior.

Na segunda capa, na etapa de colocación das arestas aplicamos $BEB^{-1}E^{-1}B^{-1}F^{-1}BF$ ou $B^{-1}D^{-1}BDBFB^{-1}F^{-1}$. Ámbolos dous movementos están formados por dous conmutadores, o primeiro por $[B, E] = BEB^{-1}E^{-1}$ e $[B^{-1}, F^{-1}] = B^{-1}F^{-1}BF$ e o segundo por $[B^{-1}, D^{-1}] = B^{-1}D^{-1}BD$ e $[B, F] = BFB^{-1}F^{-1}$.

Na terceira capa, cando estamos tratando de conseguir a cruz, utilizamos o movemento $FDAD^{-1}A^{-1}F^{-1}$ o número de veces necesario, como xa describimos, para obtela. Estamos entón ante un movemento cíclico de orde 4, xa que empecemos na posición que empecemos, despois de realizar o movemento esas 4 veces volvemos a ela. Trátase además dunha conxugación por F do conmutador $[D, A]= DAD^{-1}A^{-1}$.

Na etapa de colocación das arestas de forma que cadren as cores, o movemento utilizado é $D^{-1}A^{-1}DA^{-1}D^{-1}A^2D$, composición de tres elementos $D^{-1}A^{-1}D$, A^{-1} e $D^{-1}A^2D$.

Observemos que tanto o primeiro como o terceiro son conxugacións por D^{-1} , o primeiro conxugación de A^{-1} e o segundo de A^2. Esta estrutura vese repetida en numerosos movementos vistos, como na etapa de colocación dos vértices da última capa. Nesta etapa consideramos o movemento $ADA^{-1}E^{-1}AD^{-1}A^{-1}E$, separándoo en dous, ADA^{-1} e $E^{-1}AD^{-1}A^{-1}E$, observamos que o primeiro é a conxugación de D por A e o segundo a conxugación por E^{-1} da conxugación por A de D. Este movemento tamén é cíclico, de orde 3 neste caso, o cal se pode observar facilmente xa que o que produce é unha rotaciónn en sentido antihorario de tres vértices, coa realización do movemento 3 veces volvemos á posición inicial.

Tamén está visible o uso dos conmutadores na reorientación dos vértices da última capa, cando aplicamos o movemento $D^{-1}B^{-1}DB$, que é o conmutador $[D^{-1}, B^{-1}]$.

Polo tanto concluímos esta memoria destacando a relevancia dos conmutadores e das conxugacións á hora de analizar e resolver o cubo de Rubik.

Bibliografía

[1] Barrera Mora, F. (2004). *Introducción a la teoría de grupos*, coedición Universidad Autónoma del Estado de Hidalgo y Sociedad Matemática Mexicana. ISBN: 970-769-020-8.

[2] Chen, J. (2004). *Group Theory and the Rubik's Cube*, Notas, Harvard University: `http://people.math.harvard.edu/~jjchen/docs/Group%20Theory%20and%20the%20Rubik%27s%20Cube.pdf`

[3] Daniels, L. (2014). *Group Theory and the Rubik's Cube*, Lakehead University, Ontario, Canada.

[4] Jara Martínez, P. (2001-2017). *Teoría de Grupos. Estructura de grupos finitos*, Universidad de Granada: `http://www.ugr.es/~anillos/textos/pdf/2019/3000-Grupos-TE.pdf`

[5] Joyner, D. (2008). *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*, Johns Hopkins University Press.

[6] Judson, T. W. (1994). *Abstract Algebra: Theory and Applications*, Edición digital 2020: `http://abstract.ups.edu/aata-es/section-cyclic-subgroups.html`

[7] Narváez Macarro, L., Piedra Sánchez, R. y Tornero Sánchez J.R. (2000-2001). Temario de álgebra de la Licenciatura de Matemáticas, Facultad de Matemáticas, Universidad de Sevilla: `http://www.departamento.us.es/da/planantiguo/notas-ant/algebra/t11.pdf`

[8] Vargas, J. A. (2006). *Álgebra Clásica*, Segunda Edición, Sociedad Matemática Mexicana. ISBN 968-9161-17-2.