Group theory and rubik's cube

Lucas Bensaid

May 2019

1 Introduction

Rubik's Cube is a puzzle cube, and the world's biggest selling toy of all time with over 300 million sold. It was invented in 1974 by Hungarian sculptor and professor of architecture Ernő Rubik to help his students understand 3D objects.

At first view, this funny object is a toy. However with a mathematical vision the rubik's cube hides many applications of group theory. It allows to illustrate abstract properties of group theory in the real world.

So we will use the rubik's cube to illustrate some application of group theory.

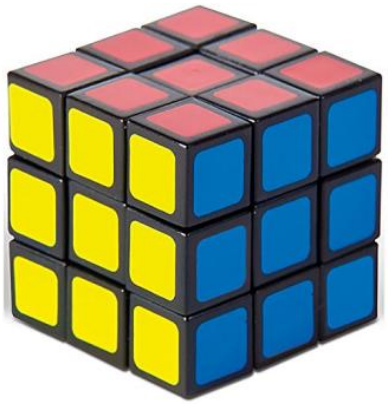

Figure 1: The Rubik's cube

2 Groups

The main sources for this chapter are [4] and [5].

2.1 Preliminaries

Before the Rubik's Cube Group can be constructed, many definitions from group theory will be needed. A review of the essential definitions from group theory are provided.

Definition 2.1. Let G be a set with a binary operation * such that

$$* : G \times G \longrightarrow G$$
$$(g1, g2) \rightarrow g1 * g2$$

Then G is a **group** under this operation if the following three properties are satisfied:

1. For every a, b and c in G, $(a * b) * c = a * (b * c)$ (associativity).
2. There exists an element e such that $a * e = e * a = a$ for all a in G (identity element).
3. For every element a in G, there exists a^{-1} such that $a * a^{-1} = e$ (inverses).

Example. Let G be the set of integers, $G = \mathbb{Z}$, and $x, y, z \in G$ under the operation of addition.

- Since $(x + y) + z = x + y + z = x + (y + z)$, G is associative.
- • The identity element of G is 0 since $x + 0 = 0 + x = x$.
- For each $x \in$ G, there exists $-x \in G$ with $x + (-x) = 0$. So G contains inverses.

So G is a group under addition. Notice that if the operation on the integers is changed to multiplication, then G would not be a group since the set would not contain inverses. For example, take the number $2 \in \mathbb{Z}$ The inverse of 2 would be 1/2 since $2 * 1/2 = 1$ but $1/2 \notin \mathbb{Z}$

Definition 2.2. Let H be a subset of a group G. If H is a group with the same operation as G, then H is a subgroup of G.

Example. Let G be the set of integers modulo 6, $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Then G is a group under addition mod 6. The order of G is $|G| = 6$. A subgroup of G would be $H = \{0, 2, 4\}$ under addition mod 6.

Definition 2.3. A group G is a finite group if $|G| < \infty$.

Definition 2.4. Let G be a group and $H \subset G$. The set $aH = \{ah | h \in H\}$ for any a $\in G$ is a left coset of H in G. Likewise the set $Ha = \{ha | h \in H\}$ for any a $\in G$ is a right coset of H in G.

Theorem 2.1 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Furthermore, the number of distinct right (or left) cosets of H in G is $|G|/|H|$.*

A proof of Lagrange's Theorem can be found in [4].

Definition 2.5. Let G and H be finite groups and $H \subset G$. The index of H in G is $[G : H] = |G|/|H|$.

Example. If $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and $H = \{0, 2, 4\}$, then $[G : H] = |G|/|H| = 6/3 = 2$. So there are 2 distinct left cosets of H in G, and these two cosets are $\{0, 2, 4\}$ and $\{1, 3, 5\}$.

$\{a+H | a \in G\} = \{(0+\{0, 2, 4\}), (1+\{0, 2, 4\}), (2+\{0, 2, 4\}), (3+\{0, 2, 4\}), (4+\{0, 2, 4\}), (5+\{0, 2, 4\})\} = \{\{0, 2, 4\}, \{1, 3, 5\}, \{2, 4, 0\}, \{3, 5, 1\}, \{4, 0, 2\}, \{5, 1, 3\}\} = \{\{0, 2, 4\}, \{1, 3, 5\}\}$

Definition 2.6. Let G and H be groups and $H \subset G$. The subgroup H is a normal subgroup of G, denoted by $H \lhd G$, if, for each a in G, $a^{-1}Ha = H$ (or aH = Ha).

Example. Let $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and $H = \{0, 2, 4\}$. For each $g \in G$, $g + H = H + g$ since in $\mathbb{Z}$ addition is commutative. So H is a normal subgroup of G and denote by $H \lhd G$.

lemma Let S1, S2, ..., Sn denote finite sets. Then $|S1 \times S2 \times ... \times Sn| = |S1| \cdot |S2| \cdot ... \cdot |Sn|$

2.2 Types of group

Definition 2.7. A group G is a cyclic group if there is some element g in G such that $G = \{g^n | n \in \mathbb{Z}\}$. The element g is a generator of the group G, denoted $G = \langle g \rangle$.The group C_n denotes the cyclic group of order n.

Example. If $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, then a cyclic subgroup would be $\langle 2 \rangle = \{0, 2, 4\}$.

Definition 2.8. A permutation of a set G is a one-to-one and onto function from G to itself. σ: G $\to G$

Example.

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

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

Definition 2.9. A cycle is a permutation of the elements in a set $X = \{1, 2, 3, ..., n\}$ such that $x_1 \to x_2 \to x_3 \to ... \to x_1$ where $x_i \in X$.

Definition 2.10. Any permutation can be written as a product of its cycles. This is called cycle notation. If in the permutation, an element is sent to itself ($\sigma(1) \to 1$), the cycle is omitted from the cycle notation.

Example. Take the set $X = \{1, 2, 3, 4\}$ and the permutation $\sigma : X \to X$ where $\sigma(1) = 2, \sigma(2) = 4, \sigma(3) = 1$ and $\sigma(4) = 3$.

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{smallmatrix}\right)$$

As a cycle, σ is $1 \to 2 \to 4 \to 3 \to 1$ and the cycle notation is (1243).

Definition 2.11. A cycle $(x_1 x_2 ... x_k)$ is called a cycle of length k. Moreover, a permutation that can be expressed as a cycle of length 2 is called a 2-cycle.

Definition 2.12. If a permutation can be expressed as an even number of 2-cycles,then the permutation is even. If a permutation can be expressed as an odd number of 2-cycles, then the permutation is odd.

Example. Consider the permutation:

$$\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{smallmatrix}\right)$$

In cycle notation, the permutation would be (12)(34)(5) or more simply, (12)(34). Since the permutation can be expressed by two 2-cycles, the permutation is even.

Definition 2.13. The permutation group (S) of the set T is the set of all permutations of T that form a group under composition.

Example. Let $T = \{1, 2, 3\}$. A permutation of T would be $\sigma : T \to T$ where $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$. The permutation can be written completely as

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$$

or in cycle notation $\sigma = (123)$. The set of all permutations of T is

$$S = \left\{ \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right) \right\}$$

In cycle notation, $S = \{(1), (23), (12), (123), (132), (13)\}$. The identity of S is the permutation

$$e = (1) = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$$

Definition 2.14. The permutation group of n elements, denoted S_n is called the symmetric group.

Definition 2.15. The group of all even permutations, denoted A_n, is called the alternating group.

Definition 2.16. Let G be a group and $H \lhd G$. Then the factor group is the group $G/H = \{aH | a \in G\}$ (left coset)under the operation $(aH)(bH) = abH$ for $a, b \in G$.
Proof H is normal $Ha = aH \Leftrightarrow (aH)(bH) = abHH = abH$

2.3 Isomorphisms

Definition 2.17. A function ϕ from a group G to a group H is a homomorphism if ϕ preserves the group operation; ϕ(ab)=ϕ(a)ϕ(b) for all a, b $\in$ G.

Definition 2.18. The sign or signature of a permutation σ is denoted $sgn(\sigma)$ and defined as +1 if σ is even and -1 if σ is odd. $sgn(\sigma)$ is a homomorphism $sgn(\sigma\phi) = sgn(\sigma)sgn(\phi)$

Example. Take $G = S_4$ and $H = \{1, -1\}$ under the operation multiplication. Define the map $\sigma : G \to H$ with $\forall a \in G, \sigma(a) = \begin{cases} 1 & \text{a even} \\ -1 & \text{a odd} \end{cases}$

To check that σ is a homomorphism, the 4 possible cases will be verified:

- If a and b are even, then $\phi(ab) = \phi(a)\phi(b) = (1)(1) = 1$
- If a is odd and b is even, then $\phi(ab) = \phi(a)\phi(b) = (-1)(1) = -1$
- If a is even and b is odd, then $\phi(ab) = \phi(a)\phi(b) = (1)(-1) = -1$
- If a and b are odd, then $\phi(ab) = \phi(a)\phi(b) = (-1)(-1) = 1$

It is clear that even permutations are sent to 1 and odd permutations are sent to -1. Thus σ is a homomorphism.

Definition 2.19. An isomorphism is a homomorphism $\phi : G \to H$ that is a one-to-one correspondence (mapping) between two sets that preserves binary relationships between elements of the sets. If such a function exists, then G is isomorphic to H and denote this by G $\cong$ H.

Example. Let G = $\mathbb{Z}$ and H = $2\mathbb{Z}$ both under the operation addition. Then $\phi : \mathbb{Z} \to 2\mathbb{Z}$ is an isomorphism where $\phi(a) = 2a$ for all $a \in \mathbb{Z}$.

Definition 2.20. An automorphism is an isomorphism from a group G onto itself. The set of automorphisms of a group G is denoted by Aut(G).

Example. Take G to be any group under the operation of addition. Then $\phi : G \to G$ is an automorphism where $\phi(a) = a$ for all $a \in G$.

Definition 2.21. Let G and H be groups and let $f : G \to H$ be a homomorphism.Then the kernel of G is the set $ker(f) = \{g \in G | f(g) = e_H\}$, where e_H is the identity element of H.

3 Constructing Groups

3.1 Direct Products

Given integers a and b, a new integer can be created by multiplying a and b. That is, a $\cdot$ b = ab. The same concept can be applied to groups. New groups can be formed by taking two existing groups, say G_1 and G_2, and 'multiplying' them together.

Definition 3.1. Let G_1 and G_2 be groups. Then the direct product of G1 and G2 is the set G1 $\times$ G2 under the operation (g1,g2).(g1',g2')=(g1.g1,g2.g2') for g1,g2$\in G_1$ and g1',g2' $\in G_2$

Example. Let $G_1 = \mathbb{Z}_2$ and $G_2 = \mathbb{Z}_2$. Then
$A = G_1 \times G_2$
$= (0,1) \times (0,1)$
$= \{(0,0),(0,1),(1,0),(1,1)\}$

Example. $\mathbb{R}_2 = \mathbb{R} \times \mathbb{R} = \{(x,y)|x,y \in R\}$ under addition. That is, if a, b, c, d $\in \mathbb{R}$, then (a, b) + (c, d) = (a + c, b + d).

Definition 3.2. Let G be a group and X be a set. Define a map G $\times$ X $\to$ X. Then the group G acts on X if the following happen:

Example. Let $G = S_4$ and $X = \{1,2,3,4\}$. Some examples of G acting on X are:

(12)(34) 2= 1 $(2 \to 1)$

(132)(12) 2 = 3 $(2 \to 1 \to 3)$

3.2 Semi-Direct Products

To construct the Rubik's Cube Group, a more general product than the direct product of two groups will be needed.

Definition 3.3. Let G_1 and G_2 be subgroups. Then $A = G_1 \rtimes G_2$ is a semi-direct product if:

1. $A = G_1 G2$.
2. $G_1 \cap G2 = e_A$ the identity element of A
3. $G_1 \lhd A$

3.3 Wreath Products

The product of two groups can be generalized from semi-direct products even further to wreath products.

Definition 3.4. Let X be a finite set, G a group and H a group acting on X. Fix a labelling of X, say $\{x1, x2, ..., xt\}$, with $|X| = t$. Let G^t be the direct product of G with itself t times. Then the wreath product of G and H is $G^t \wr H = G_t \rtimes H$ where H acts on G^t by its action on X.

Here, the action of H on G is by conjugation; that is, if $g \in G$, then the action of H on G^t is $(g_1, g_2, ..., g_t)h = (g_{1h}, g_{2h}, ..., g_{th})$.

The wreath product of two groups G and H is constructed by:

- write H as a permutation group on n items
- make n copies of the group G
- H acts on the copies of G by permuting the elements.

The wreath product of G by H is a semi-direct product of a direct products of n copies of G by H.

3.4 index of notation

- $\mathbb{Z}$ the set of relative integers
- $\mathbb{Z}_n$ the set of integers modulo n
- S_n the group of permutations
- A_n the alternative group (group of even permutations of S_n)
- $\epsilon(\sigma)$ denotes the signature of the permutation σ
- $|A|$ will designate the cardinal of set A
- $A_i \cup_{i=0}^{n}$ will denote the disjoint union of sets A_n
- $[g, h] = ghg^{-1}h^{-1}$ denote the commutator
- $\mathbb{Z}(\mathbb{G})$ the center of G, G group

4 The Rubik's Cube Group

The Rubik's Cube can be manipulated by rotating the faces of the cube. There are six faces, with each face composed of nine facets. In total, there are $6 \times 9 = 54$ facets on the cube. Each facet is also coloured, and solving the cube requires that each face be a solid colour. That is, the nine facets of the side must all be the same colour.

4.1 Singmaster Notation

To solve the Rubik's cube, a series of turns of the faces are needed. To describe these turns, the notation introduced by David Singmaster will be used. For this notation, assume that the cube is sitting on a flat surface and each turn of the face will be a one quarter turn (90 degrees) clockwise. The state of the cube at a given moment depends on:

- U denote one quarter turn of the upward (top) face.
- F denote one quarter turn of the front face.
- L denote one quarter turn of the left face.
- R denote one quarter turn of the right face.
- B denote one quarter turn of the back face.
- D denote the downward (bottom) face.

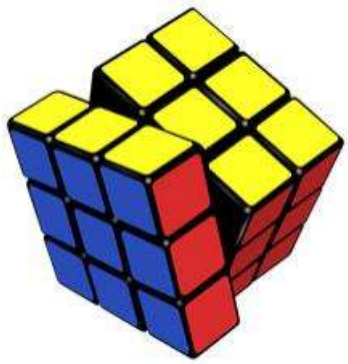

Figure 2: Example of manipulation F where the front face is blue

The inverse of each move would be the 90 degree rotation of the face counter-clockwise and denoted M_i^{-1} , where $Mi \in \{U, F, L, R, B, D\}$.

4.2 The Rubik's Cube Group

On the Rubik's Cube, there are 54 facets that can be arranged and rearranged through twisting and turning the faces. Any position of the cube can be describe as a permutation from the solved state. Thus, the Rubik's Cube group is a subgroup of a permutation group of 54 elements.

Definition 4.1. The permutation group $G = \langle F, L, U, D, R, B \rangle \subset S_{54}$ is called the Rubik's Cube Group.

There are two different classifications of the Rubik's Cube Group:

- The illegal Rubik's Cube Group; allows all the possible permutation of the cube (S_{54}).
- The (legal) Rubik's Cube Group; allows all the permutation feasible with the movements {F, L, U, D, R, B}.

4.2.1 G the group of manipulations of the Rubik's cube

- Given two manipulations g1 + g2 with $gi \in \{F, L, U, D, R, B\}$, we can define a third one the "PRODUCT" g2.g1 by applying g1 first then g2 to the state obtained.
- (g1.g2).g3=g1.(g2.g3)
- g1.g2≠ g2.g1 in general
- We can always do a reverse manipulation g^{-1}
- e do nothing the manipulation who does not change the state

4.2.2 Manipulation of the cube

We see the cube at his initial state, we mixed it and we note:

- The 6 middle facet do not move $\implies$ 48 pieces move
- the edge facets stay edge
- the corner facets stay corner

The middle facet on each side of the cube is fixed and cannot be permutated to a different position on the cube. The valid permutation on the cube will send corner facets to corner positions and edge facets to edge positions. Any other permutations will not be physically possible on the cube.

Not all of the permutations of S_{54} will be possible on the Rubik's Cube. Rubik's Cube Group is a subset of the Illegal Rubik's Cube group (S_{54}).

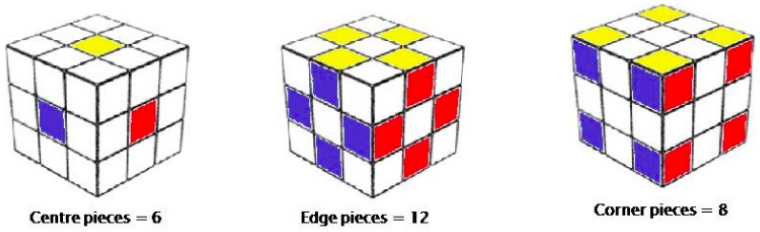

Figure 3: Rubik's cube of 54 pieces

The manipulation done, the cube is in a new state. We can describe this sate by the position and orientation of the edge and corner pieces in relation to the centers pieces stay fixed.

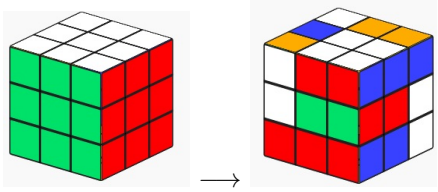

Figure 4: Initial to new state

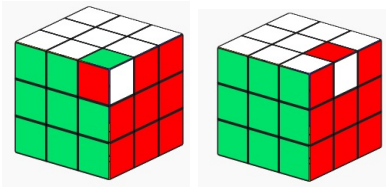

Figure 5: Corner and edge well positioned but bad oriented

The purpose of this section is to characterize exactly G. As well as some of the associated theorems and applications of the group. The state of the cube at a given moment depends on:

- The position of the corners cubes
- The position of the edges cubes
- The orientation of the corners cubes
- The orientation of the edges cubes

4.3 Corner Cubes

Each corner cube consists of three facets. There are a total of eight corner cubes on a Rubik's Cube and each of the facets that comprise the corner cube are on three different sides of the cube.

As shown in Figure 6, facet A is on the upper face, facet B is on the left face, and facet C is on the front face.

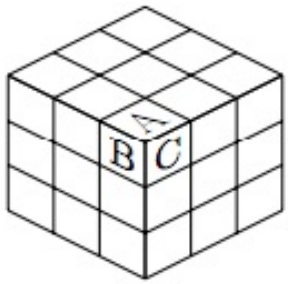

Figure 6: ABC

Now, it is possible to reorient the facets of a center cube:

- ACB
- BAC
- BCA
- CAB
- CBA

Facet A is in the position where facet B is, facet B is moved to where facet C was, facet C moved to the position of facet B; and facet A can be moved to the position of facet C, facet C to the position of facet B and facet B to the position of facet A. In terms of groups, this means that the facets of a corner cube belong to the cyclic group of three elements C_3.

There are eight corner cubes, the orientation of any facet of a corner cube can be described by the set $C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3 = C_3^8$. Now, the possible arrangements of the corner cubes can be described similarly. Again, any of the eight corner cubes can occupy any of the corner cube positions of the Rubik's Cube. So, the possible arrangements of the corner cubes can be described by the permutation group of eight elements, S_8.

Lemma: The position of all of the corner facets on the Rubik's Cube can be described by the group $C_3^8 \wr S_8$.

Proof This follows from the definition of wreath product and from the fact that any corner cube position can be described by its position on the cube and the cycle orientation of the three facets of the corner cube.

4.4 Edge Cubes

Every edge cube in the Rubik's Cube consists of two facets, as shown in 1 and there are 12 edge cube on the Rubik's Cube. Note that for every edge cube, each of the two facets of an edge cube lie on different faces of the cube.

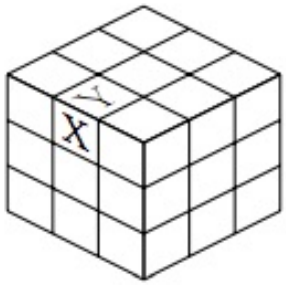

Figure 7: Rubik's cube of 54 pieces

As in figure 3, facet X is on the left face and facet Y is on the upper face. Likewise, it is also possible for facets X and Y to switch places. That is, facet X would be repositioned to where facet Y is and facet Y would be moved to the position where facet X is. In terms of groups, the facets of any edge cube belong to the cyclic group of two elements C_2. In addition, there are 12 edge cubes on the Rubik's Cube and any edge cube can occupy an edge cube spot. Thus any facet of an edge cube will be in the set $C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C2 = C_2^{12}$. Likewise to describe the different arrangements of the edge cubes. There are 12 edge

cubes on the Rubik's Cube and any edge cube can be in an edge cube spot. Thus, the possible arrangements of the edge cubes of the Rubik's Cube can be described by the permutation group of 12 elements, S_{12}.

Lemma The position of all of the edge facets on the Rubik's Cube can be described by the group $C_2^{12} \wr S_{12}$.

Proof This follows from the definition of wreath product and from the fact that any edge cube position can be described by its position on the cube and the cycle orientation of the two facets of the corner cube.

4.5 The Illegal Rubik's Cube Group

The Illegal Rubik's Cube Group allows the solver to take the cube apart and reassemble it in any orientation. Again, some of the orientations are not physically possible on the cube. When all the possible positions of the facets are combined as a whole, some of the arrangements will not be physically possible on the cube.

Lemma The Illegal Rubik's Cube Group is I = $(C_2^{12} \wr S_{12}) \times (C_3^8 \wr S_8)$. Proof. This follows from previous Lemma, and the definition of the direct product.

4.6 Fundamental Theorems of Cube Theory

To be able to distinguish the legal Rubik's Cube Group, the First Fundamental Theorems of Cube theory are needed.

The First Fundamental Theorem of Cube Theory gives the criteria for solvable arrangements of the Rubik's Cube.

Proposition 4.1. (First Fundamental Theorem of Cube Theory). Let $v \in C_3^8, r \in S_8, w \in C_2^{12}$, and $s \in S_{12}$. The 4-tuple (v, r, w, s) corresponds to a possible arrangement (position) of the cube if and only if:

1. sgn(r) = sgn(s) (equal parity of permutations).
2. v1 + v2 + v3 + ... + v8 = 0 (mod 3) (conservation of the total number of twists).
3. w1 + w2 + w3 + ... + w12 = 0 (mod 2) (conservation of the total number of flips).

The goal of the next section will be to analyze in detail the cube and demonstrate the fundamental theorem of cube theory.

5 Mathematics of the cube

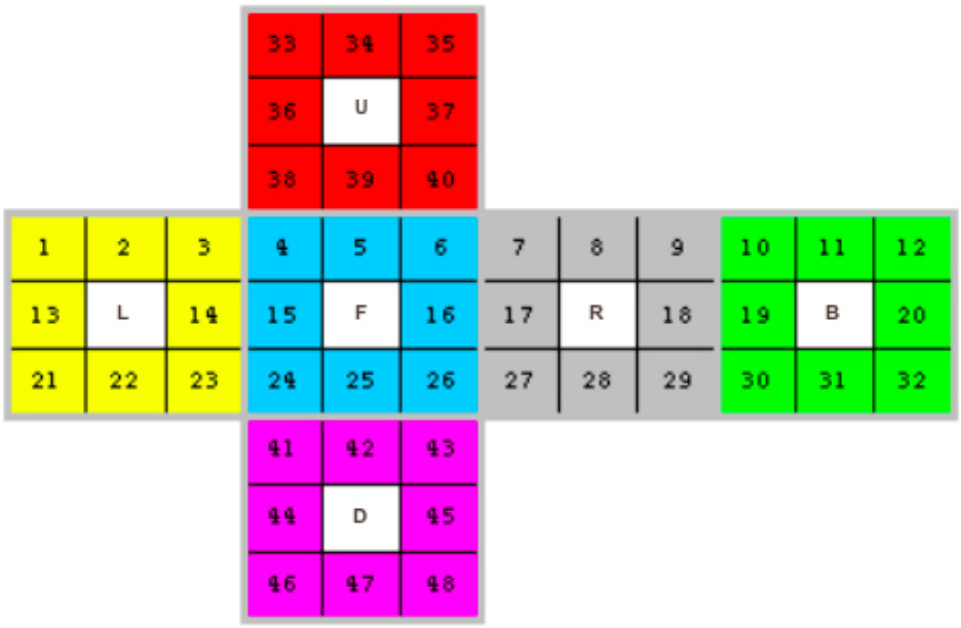

Figure 8: The numbering of facets

We will represented and ordered the corner edge CE (pairs of indivisible facets and the cube corner CC (triplets of indivisible facets) in the following lists:

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

In other words all manipulations of **G** can not change CE and CC.

The group G is generated by the manipulation {F, B, L, R, U, D}

Let's write the disjoint cycle decomposition of the facet permutation cubes-corners associated with elementary movements. We note σ_U the permutation associated with the movement Up, σ_D for the permutation associated with a Down etc. We have :

$$\sigma_F = (3,40,27,41),(4,6,26,24),(7,43,23,38)$$
$$\sigma_B = (46,29,35,1),(9,33,21,48),(10,12,32,30)$$
$$\sigma_L = (3,23,21,1),(4,41,32,33),(12,38,24,46)$$
$$\sigma_R =(6,35,30,43),(7,9,29,27),(10,48,26,40)$$
$$\sigma_U = (10,7,4,1),(3,12,9,6),(33,35,40,38)$$
$$\sigma_D = (21,24,27,30),(23,26,29,32),(41,43,48,46)$$

We do the same thing for edge cubes. We have:

$$\rho_F = (5,16,25,15),(14,39,17,42)$$
$$\rho_B = (11,20,31,19),(13,47,18,34)$$
$$\rho_L = (2,14,22,13),(15,44,20,36)$$
$$\rho_R = (8,18,28,17),(16,37,19,45)$$
$$\rho_U = (2,11,8,5),(34,37,39,36)$$
$$\rho_D = (22,25,28,31),(42,45,47,44)$$

5.1 Analyzing a state of the cube

As seen previously a valid movement is a movement obtained by a series of elementary movements. On the contrary, an invalid movement is a movement not obtained by a series of elementary movements, an illegal movement is obtained by dismounting the cube.

We have seen that a corner is a product of three 4- cycle and edge is a product of two 4- cycles. Make a movement g is to switch the pieces of the cubes. For that we give:

$$\begin{aligned} \phi_{cube} : G &\to S_{20} \\ g &\to \rho(g) \end{aligned}$$

$\sigma(g)$ means the permutation of the 20 moving cubes associated with the movement g

To look at the permutation of the 20 movable facets, it is to look at the permutation of 12 disjointed edge and the 8 disjointed corners

$$\begin{array}{c} \phi_{edge} : G \to S_{12} \\ g \ \to \tau(g) \\ \phi_{corner} : G \to S_8 \\ g \ \to \sigma(g) \end{array}$$

Proposition 5.1. $\epsilon(\rho_g) = 1 = \epsilon(\sigma_g)\epsilon(\tau_g)$

Proof: We start by verifying it for elementary movements. We have seen that in the case of elementary movements the permutation: $\sigma(X)$ is a 4-cycle $\forall X \in \{U, D, R, L, B, F\}$.

$$\Rightarrow \epsilon(\sigma_X) = -1$$

Same for τ_X

$$\begin{array}{c} \Rightarrow \epsilon(\tau X) = -1 \\ \rho_X = \sigma_X \tau_X = \tau_X \sigma_X \quad \forall X \in \{U, L, ..., B\} \\ \epsilon(\rho_X = 1) \quad \forall X \in \{U, L, ..., B\} \end{array}$$

The property is true for elementary movements. Now we look at the case of any movement. Any movement is a composition of $X_1 ... X_k$ with $X_i \in \{U, L, ..., B\}$.

$$\begin{array}{c} \rho_{X_1 ... X_k} = \rho X_1 ... \rho X_k \\ \Rightarrow \epsilon(\rho_{X_1 ... X_k}) = \prod \epsilon(\rho X_i) \end{array}$$

$$\begin{array}{c} \epsilon(\rho_g) = 1 = \epsilon(\sigma g)\epsilon(\tau_g) \\ \Rightarrow \epsilon(\sigma g) = \epsilon(\tau_g) \end{array}$$

CONSEQUENCE :If a movement g is legal then the permutation of the corners associated with g and the permutation of the edges cubes associated with g have the same signature.

5.2 Orientation

From previous Lemma any corner cube position can be expressed as a 8-tuple and any edge cube position can be expressed as a 12-tuple. However, to determine the individual components of the tuples, a fixed numbering system will be needed.

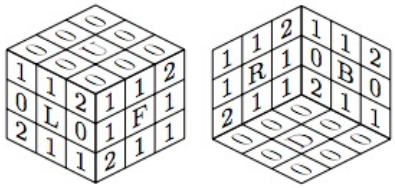

Figure 9: Rubik's cube orienatation

For any arbitrary facet, the position of the facet is assigned the corresponding number above. Even though the facets will be moving around the cube, the numbering system remains fixed.

Example. Consider the top edge cube on the front face of the Rubik's Cube. It begins with a number of 1. Now, by doing the move FR, the facet is moved to the upper face on the right side. This position of the edge cube is assigned the number 0.

Figure 10: Move FR

5.3 Corner orientation

As in figure 9, we attribute to each facet of each of the corners cube a scalar that will be either 0,1 or 2 element of $\mathbb{Z}_3$.

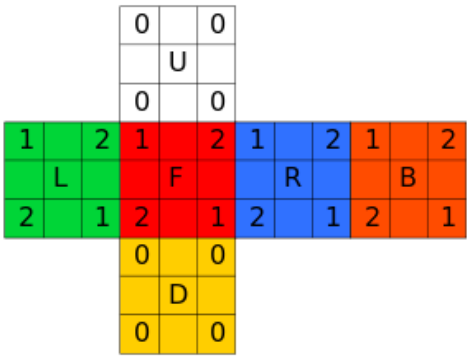

Figure 11: Orientation of facets

By this procedure we have just fixed the initial orientation of the cubes-corners of the cube.

Then we attribute a number of the corner facets of the face up and facets down Like below:

1. for ufl (face up, front corner left)
2. for ufr
3. for ubr
4. for ubl
5. for dbl
6. for dfl
7. for dfr
8. for dbr

x_4		x_3
	up	
x_1		x_2

x_5		x_8
	down	
x_6		x_7

After a movement g on the initial configuration, we observe the new orientation as follows: 'to each of the numbered facets i, $i = (1...8)$, we associate x_i the scalar on the facet i, i = 1. . . 8. We define the vector $f(g) = (x_1, ..., x_8) \in Z_3^8$

f(g) is therefore a vector that accounts for the orientation of cubes-corners after having made the cube move g.

Example. When the Rubik's cube is in its initial position we have f (g) = (0, $\cdots$, 0)

Example. Calculation of the vectors f (g) with g the elementary movements

f(R) = (1, 2, 0, 0, 2, 1, 0, 0)
f(L) = (0, 0, 1, 2, 0, 0, 2, 1)
f(U) = (0, 0, 0, 0, 0, 0, 0, 0)
f(D) = (0, 0, 0, 0, 0, 0, 0, 0)
f(B) = (0, 1, 2, 0, 0, 2, 1, 0)
f(F) = (2, 0, 0, 1, 1, 0, 0, 2)

Remark. In the example above we can see that the total rotation vectors is null: $\sum_{i=1}^{8} x_i = 0(mod 3)$

5.4 Edges cubes orientation

This time a edge cube presents two possible orientations. The idea is exactly the same as in the case of cubes-corners.

We start to label the 12 mobile cubes-corner :

1. for ub
2. for ur
3. for uf
4. for ul
5. for lb
6. for rb
7. for rf
8. for lf
9. for db
10. for dr
11. for df

12. for dl

	v_1	
v_4	up	v_2
	v_3	

Now each of the 12 moving cubes-edge has a numbered face in each of the 6 faces of the cube. To all these faces we assign 0, to the other faces of each cube-edge we assign 1. See figure 11.

After a movement we assign to each of the 12 cubes the number $v_i = 0$ or 1 on the face initially numbered i and that for i = 1. . . 12. This defines a vector $t(g) = (v_1, ..., v_{12}) \in Z_2^{12}$ look for cubes-edge orientation.

5.5 Results related to the orientation of the cubes

We have two results related to the orientation of the cubes: the first proposal expresses the orientation of the corner and edge vectors after a composition of two movements, second proposition expresses the nullity of the cubic vectors and resp. edge modulo 3 and 2 resp.

Proposition 5.2. $\forall g, h \in G$:

$$f(gh) = f(g) + \sigma_g.f(h)$$
$$t(gh) = t(g) + \tau_g.t(h)$$

Proof: One is interested in the formula concerning the corners, the demonstration is allowed to generalize in the case of cubes-edge in a similar way. To carry out the movement gh, it is to carry out first g then h. The movement g reorients the cube via the data of f (g). The motion h reorients the cubes after the action of $\sigma(g)$ on the cube of f (h). In the end we have: $f(gh) = f(g) + \sigma_g.f(h)$

Proposition 5.3. $\forall g \in G$:

$\sum_{i=1}^{8} x_i = 0(mod3)$

$\sum_{i=1}^{12} x_i = 0(mod2)$

Proof: It is only checked in the case of cubes-corners. This proof is carried out by induction on the length of the movement which, it is recalled, can be seen as a word in the letters in the set {U, F, ..., D}. For the elementary motions (word of length 1) this formula is true (we carried out the explicit calculations see for this the remark above).

We assume the property established for a movement of length k, that is to say for a movement g represented by a word of length k, $g = X_1...X_k$ where the X_i are elements of the set {U, D, L, R, B, F} Let us move to a length of length k + 1. Using Proposition 2.3, we write:

$$f(g) = f(X_1...X_{k+1})$$
$$= f(X_1...X_kX_{k+1}) = f(X_1...X_k) + \sigma_{X_1...X_k} f(X_{k+1})$$

The vector $f(X_1...X_k)$ is a zero total rotation vector using the recursion formula. $f(X_{k+1})$ is also a zero total rotation vector (rotation vector associated with elementary motion). Now we see that if $f(g) = (x1, ..., x8)$ then:

$$\sum_{i=1}^{8} x_i = 0(mod3) \Leftrightarrow \sum_{i=1}^{8} x_{\sigma_{(i)}} = 0(mod3), \forall \sigma \in S_8$$

$$f(g) = \underbrace{(f(X_1...X_k))}_{rot.null} + \underbrace{(\sigma_{X_1...X_k} f(X_{k+1})))}_{rot.null}$$

is a zero total rotation vector as sum of two zero total rotation vectors. This completes the proof.

We will model G as a direct product of semidirects product.

5.6 Semi-direct product applied to rubik's cube

S_8 act on Z_3^8:

$$Z_3^8 \times S_8 \to Z_3^8$$
$$(x = (x_1...x_8), \sigma) \to \sigma.x \neq \sigma x = (x_{\sigma(1)}, ...x_{\sigma(8)})$$

and in the same way: S_{12} acts on Z_2^{12}

$$Z_2^{12} \times S_{12} \to Z_2^{12}$$
$$(t = (v_1...v_{12}, \sigma) \to \sigma.t \neq \sigma t = (v_{\sigma(1)}...x_{\sigma(12)})$$

So we put the product $S_n \times Z_k^n$ a group law * as follows:

$$(S_n \times Z_k^n) \times (S_n \times Z_k^n) \to S_n \times Z_k^n$$
$$(\sigma_1, f_1) * (\sigma_2, f_2) \to (\sigma_1\sigma_2, f_1 + \sigma_1 f_2)$$

We can define two new morphisms:

$$\Gamma_{corner} : G \to S_8 \rtimes Z_3^8 \; g \to (\sigma, f)$$

and :

$$\Gamma_{edge} : G \to S_{12} \rtimes Z_2^{12} \; g \to (\rho, t)$$

that allow to account for the evolution of the position and orientation of the cubes - corners and edge where:

- σ designates the permutation of the corners associated with g
- the orientation of the cubes-corners
- ρ the permutation of the corners-edge associated with g

- t the orientation of the cube-edge

We obtain: $\Psi : G \to (Z_3^8 \rtimes S_8) \times (Z_2^{12} \rtimes S_{12})$
$g \to (\sigma, f, \rho, t)$

Example. By adopting the notations above, the initial position of the Rubik's cube is written (1, 0, 1, 0) where it is necessary to read:

- The first 1 of the 4-tuple as 1_{S_8} : all cubes-corners are at the good position.
- The first 0 of the 4-tuple as 0 of Z_3^8 : all the cubes-corners are correctly oriented.
- The second 1 of the 4-tuple as $1_{S_{12}}$:all the cubes-edge are at the good position.
- The second 0 of the 4-tuple as 0 of Z_2^{12} all cubes-edge are correctly oriented.

The following section is designed to characterize G according to this 4-tuples.

5.7 cube structure

The state of the cube at a given moment depends on:

1. the position and orientation of the wedge-cubes
2. the position and orientation of cubes-edge

Let us then give a 4-tuples (σ, f, ρ, t) with $\sigma \in S_8, \rho \in S_{12}, f \in Z_3^8$ and $t \in Z_2^{12}$.
The question is: on what conditions is this 4 - tuples representative of a licite movement? We will answer that question by saying that such a 4 - tuple is representative of a licite movement, if and only if

- a) $\epsilon(\sigma) = \epsilon(\rho)$
- b) $\sum_{i=1}^{8} x_i = 0(mod 3)$
- c) $\sum_{i=1}^{12} x_i = 0(mod 2)$

5.8 The fundamental theorem of the cube

Theoreme A movement g is licite if and only if the 4-tuples associated with g verifies the constraints a), b) and c) mentioned above.

proof Let us give a licite motion to which we correspond to the 4-tuples (σ, f, ρ, t). Regarding the equality of the signature it is proposition 5.1. Concerning the nullity of the vector orientations it is the proposition 5.3 Reciprocally one is given a 4-tuples (σ, f, ρ, t) satisfying the constraints above. We want to see that this 4 - tuples is representative of a general movement (Rub element),

that is to say that our 4 - tuples is in the correct orbit of the. initial position (1, 0, 1, 0). Our problem is therefore to go from (σ, f, ρ, t) to a (1, 0, 1, 0) in the same way. The evidence is quite constructive and is based on these four propositions.

Proposition 5.4. (Positioning the cubes-corners). If (σ, f, ρ, t) is a configuration satisfying the constraints a), b) and c) then there exists a legal movement M such that the action of M on the state of the cube has consequence of leading the cube in a configuration of the type (1, f', ρ ', t).

Proposition 5.5. (Orientation of cubes-corners). If (1, f, ρ, t) is a configuration satisfying the constraints then there exists a legal movement M such that the action of M on the state of the cube has as consequence to lead the cube in a configuration of the type (1, 0, ρ ', t').

Proposition 5.6. (Positioning cubes-edge). If (1, 0, ρ, t) is a configuration satisfying the constraints then there exists a legal movement M such that the action of M on the state of the cube has as consequence to lead the cube in a configuration of the type (1, 0, 1, t').

Proposition 5.7. (Orientation of cubes-edge). If (1, 0, 1, t) is a configuration satisfying the constraints then there exists a legal movement M such that the action of M on the state of the cube has as consequence to lead the cube in a configuration of the type (1, 0, 1, 0). If all these propositions are accepted then the proof is completed. The problem is to prove the propositions from 2.5 to 2.8. This is what we are doing now.

lemma (For proposition 5.4). The application $\phi_{coin} : G \to S_8$ is surjective.

Proof We recall that S_n is generated by the transpositions of S_n. S_8 is therefore generated by the transpositions of S_8. So just see that $Im\phi_{coin}$ contains all the transpositions.

$Im\phi_{coin}$ already contains one because the motion $M_0 = ([D, R]F)^3$ exchanges 2 corners (dbr urb) and fixes all the others. By conjugations Imcoin contains them all, let us explain. Indeed either C_1 and C_2 any two cubes corners. There is a legal move that sends dbr on C_1 and urb on C_2. We then have:

$$\begin{aligned}\phi_{coin}(M)^{-1}M_0M) &= \phi_{coin}(M)^{-1}\phi_{coin}(M_0)\phi_{coin}(M) \\ &= \sigma^{-1}(dbr \quad urb)\sigma = (\sigma(dbr) \quad \sigma(urb)) = (C_1C_2)\end{aligned}$$

Proof (of proposition 5.4) By the lemma, there exists a movement M such that $\phi_{coin}(M) = \sigma^{-1}$. It is then enough to apply the movement M 'to our cube so that all our cubes - corners are correctly positioned.

lemma (For the proposition 5.6) If C_1 and C_2 are two corner cubes, there is a legal move that changes the orientation of C_1 and C_2 and does not affect any other cube-corners.

Proof The idea is first to find a movement M satisfying the lemma then to combine this movement to act on any other cubes-corners. Movement:

$$M_0 = (DR^{-1})^3(D^{-1}R)^3$$

admits the following disjoint cycle decomposition:

(dfr, rdf, frd)(drb, rbd, bdr)(df, dr, fr, ur, br, db, dl).

Thus $\phi_{coin}(M_0) = 1$ and all the other well-corner cubes are unassigned. So if $C_1 = dbr$ and $C_2 = drf$ then the lemma is true. Exit to conjugate this movement M_0 like all the time by a movement M sending dbr on C_1 and drf on C_2 one has the result. In addition, $M^{'} = (M^{-1})(M_0M)$ rotates clockwise at C_1, counter-clockwise at C_2

Proof (For the proposition 5.5) We assume our Rubik's cube with at least two cube cubes C_1 and C_2 with bad orientation. Thanks to the previous lemma, there is a M licite movement

C_1 clockwise, C_2 counter-clockwise and not affecting any other cube-corners. Applying this motion again (if necessary), we can ensure that C_1 is correctly oriented. Since the movement does not affect any other cube, all our cubes except perhaps one (C_2) is maloriented. Two cases:

1. C_2 is correctly oriented and in this case the proof is complete
2. C_2 is misguided. In fact, this case can not be considered because it contradicts formula 5.3

In the end all our cubes-corners are correctly oriented.

At this point all our cubes-corners are correctly oriented and positioned. Now we treat the case of cubes-edge very similar way. To prove formula 5.6 we will use movements that affect neither the orientation nor the position of the corner cubes (ie, elements of Ker Γ_{coin}).

lemma (for the proposition 5.6) The image of $\phi_{arrete}|Ker\Gamma_{coin} : Ker\Gamma_{coin} \rightarrow S_{12}$ contains A_{12}

Proof We know that A_{12} is generated by the 3-cycles of A_{12}. The movement :

$$M_0 = LR^{-1}U^2L^{-1}RB^2$$

admits for decomposition (ub, uf, db). So M_0 belongs to Ker Γ_{coin} and $\phi_{edge}(M_0) = (ub, uf, db)$. If you combine as previously, you have the result.

Proof . (of Proposition 5.6) immediate thanks to the lemma (cf proposition 5.4)

All that remains is to correctly orient all the cube-edge without affecting the other cubes. We need a lemma analog that served us for Proposition 5.5.

lemma for proposition 5.7) If C_1 and C_2 are two cubes-stopped, there is a movement that changes the orientation of C_1 and C_2 without affecting the other cubes. The following M_0 movement satisfies the desired conditions:

$$M_0 = LR^{-1}FLR^{-1}DLR^{-1}BLR^{-1}ULR^{-1}F^{-1}LR^{-1}D^{-1}LR^{-1}LR^{-1}1B^{-1}LR^{-1}U^{-1}$$

The decomposition of this movement in cycle is: (fu, uf) (bu, ub). Moreover, we know that the action of Rub on the triplets (C_1, C_2, C_3) is transitive.

In particular if C_1 and C_2 are two cubes-stopped, there is a movement M sending uf on C_1 and ub on C_2. The $M^{-1}M_0M$ movement changes the orientation of C_1 and C_2 and does not affect any other cube.

Proof (of Proposition 5.7) similar to the proof of 5.5

We have therefore demonstrated the fundamental theorem of the cube and this proof contains a cube solving algorithm.

6 Conclusion

We explored some of the group theory applications to the Rubik's cube and constructed the Rubik's Cube Group. The Rubik's Cube Group was shown to be G = {R, B, L, U, F, D}, which is a subgroup of S_{54}. The First Fundamental Theorems of Cube Theory were presented, which gave the criteria for all the possible arrangements and moves allowed on the cube.

References

[1] Lindsey Daniels (2014) Group Theory and the Rubik's Cube, Lakehead University.

[2] Jerome Daquin (2010) Rubik's cube et theorie des groupes.

[3] Angèline Laberge Théorie des groupes et Rubik's cube.

[4] Brandelow, Christoph. Inside the Rubik's Cube and Beyond. Birkhauser.

[5] Singmaster, David. Notes on Rubik's 'Magic Cube'. Enslow Pub Inc. (1981).

[6] Wikipedia , Théorie mathématique sur le Rubik's Cube.