Euler Circle: Group Theory and the Rubik's Cube

Qu Gao

May 2020

Abstract

This expository paper will introduce some group theory concepts of the Rubik's cube, which will culminate in showing the two fundamental laws of cubology. The paper will use Joyner's book "Adventures in Group Theory" [1], Bandelow's book "Inside Rubik's cube and beyond" [2], and Daniels' paper [3] as reference material.

1 Introduction

From the author's (completely unbiased) opinion, the impact of the Rubik's cube on our lives is profound [1]. In 2015, over 350 million copies of the toy had been sold [4]. The elegant simplicity of matching up the faces, and the fiendish difficulty of attempting to do so, has captivated people of all generations. This paper will answer the following questions: if I disassemble the cube and reassemble the cube, how do I determine whether I can take the Rubik's cube back to its start position by rotating the layers? How do I know whether a given change in the position of the cube is possible without having to take the cube apart? How does composing operations behave? Which operations commute, and which operations do not?

2 Terminology of the Rubik's Cube

Before we can discuss the structure of the Rubik's cube, we must lay out some terminology to help us describe the components of the Rubik's cube and the actions that can be carried out on the Rubik's cube.

Definition 2.1 (Cubie)**.** *A cubie is one of the 26 small cubes that make up the Rubik's cube (abbrev. "the cube"). Cubies are either face, edge, or corner cubies.*

Definition 2.2 (Facet)**.** *A facet is one of the 54 small faces on the Rubik's cube. Face cubies have 1 facet, edge cubies have 2 facets and corner cubies have 3 facets.*

Definition 2.3 (Cubicle)**.** *A cubicle is the location of the cubie in the cube. The 8 corner cubies are located by 3 initials (e.g. urf denotes cubie on the right of the front facing corner of the upper face), and the 12 edge cubies are located by 2 initials (e.g ur denotes the cubie on the right edge of the upper face).*

[1] This can be seen from the fact that the Rubik's cube has infiltrated episodes of the Simpsons and music videos of the Spice girls. More personally, a friend of the author participated in the event at the London O2 Arena which created the world record in 2012 for the most simultaneous Rubik's cube solves (1,414) - sadly the author was too young to attend at the time.

Definition 2.4 (Orientation). *An edge cubie can be oriented in 2 different ways within its cubicle; a corner cubie can be oriented 3 different ways within its cubicle. To describe the orientation of a cubie, we label all the facets of the mobile cubies at the start position as in figure 1, and we imagine a fixed, immobile skin over the cube (which doesn't impede us from doing the basic moves) which labels all the facets, also as in figure 1. The orientation of each cubie is defined to be the number on the mobile facet of the cubie which is below the fixed facet labelled 0.*

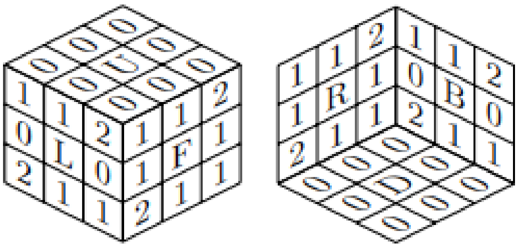

Figure 1: Labelling of the facets. [3]

Definition 2.5 (Right twisted, left twisted, incorrect orientation.). *A left twisted and right twisted edge cubie has its orientation increase by 1 and 2* $\pmod 3$ *respectively when an operation is carried out. An incorrectly twisted edge cubie its orientation increase by 1* $\pmod 2$ *when an operation is carried out.*

Definition 2.6 (Basic moves and anticlockwise moves). *Holding the cube with one face fully towards you, the six faces are labelled by their position in relation to you: up, down, right, left, front, back. A basic move is a 90 degrees clockwise rotation of one of the six outer layer faces, labelled by the face which is rotated - U, D, L, R, F, B. An anticlockwise move of a face is denoted by an apostrophe, e.g.* $U' = U^3$ *is rotating the upper face 90 degrees anticlockwise.*

Remark 2.6.1. *Technically we can include middle layer moves, but we will ignore them in this paper since middle layer moves can be written as a sequence of outer layer moves.*

Definition 2.7 (Cube move). *A cube move is a move which acts a distance-preserving rigid motion on the entire Rubik's cube (ignoring reflections, which are physically impossible on the cube). A cube move could either be a rotation about a face axis connecting the centres of opposite faces, a rotation about a corner axis connecting corners of maximal distance apart, and an edge rotation connecting centres of edges of maximal distance apart.*

Remark 2.7.2. *The group of cube moves is isomorphic to* S_4 *because each cube move has a 1-to-1 correspondence to a permutation of the four diagonally opposite corner axes.*

3 Wreath Products and the Signum Function

The signum function, as we will see in the First Fundamental Law of Cubology, is found in one of the criteria for determining whether a position is possible.

Definition 3.1 (Inversions, Even/Odd Permutations). *Consider a permutation $f \in S_n$. A pair (i, j) of elements in the set $\{1, 2, ..., n\}$ is an inversion iff $i < j$ and $f(i) > f(j)$. The number of inversions in a permutation is z. The parity of a permutation is the same as the parity of z.*

Definition 3.2 (The signum function). *The signum function of a permutation f is $sgn(f) = (-1)^z$.*

Theorem 3.1. *For all $f, g \in S_n$, $sgn(fg) = sgn(f) \cdot sgn(g)$.*

Proof. We have $sgn(f) = \prod_{1 \leq i < j \leq n} \frac{f(i)-f(j)}{i-j}$, where the product is across all ordered pairs of elements from $\{1, ..., n\}$. Then

$$\begin{aligned} sgn(fg) &= \prod_{1 \leq i < j \leq n} \frac{fg(i) - fg(j)}{i - j} \\ &= \prod_{1 \leq i < j \leq n} \frac{fg(i) - fg(j)}{g(i) - g(j)} \prod_{1 \leq i < j \leq n} \frac{g(i) - g(j)}{i - j} \\ &= sgn(f) \cdot sgn(g) \end{aligned}$$

□

The wreath product can describe the group of operations in the Rubik's cube, and can help us understand how composing operations affects the position of the cube. Recall the two definitions of the semi-direct product:

Definition 3.3 (Inner definition of the semi-direct product). *Let G be a group. Let H_1 and H_2 be subgroups of G. Then G is the semi-direct product of H_1 and H_2 (i.e. $G = H_1 \rtimes H_2$) if the following 3 conditions are met:*

1. *$G = H_1 \, H_2$, that is, for all $g \in G$, g can be expressed uniquely as $g = h_1 h_2$, where $h_1 \in H_1$ and $h_2 \in H_2$.*
2. *$H_1 \cap H_2 = \{e\}$*
3. *$H_1 \lhd G$.*

Definition 3.4 (Outer definition of the semi-direct product). *Let H_1 and H_2 be groups. Construct a homomorphism $\varphi \colon H_2 \to Aut(H_1)$. Then the elements in the semi-direct product are $H_1 \rtimes_\varphi H_2 = \{(h_1, h_2) : h_1 \in H_1,\ h_2 \in H_2\}$. Multiplication between group elements is defined by $(h_1, h_2)(h_1', h_2') = (h_1 \cdot \varphi(h_2)h_1', h_2 h_2')$.*

Remark 3.4.3. *It is fairly straightforward to show that the semi-direct product multiplication in the outer definition satisfies the group properties of identity, inverses, closure, and associativity. This will be left to the reader.*

Remark 3.4.4. *It is worth checking that the inner and outer definitions are consistent. The outer semi-direct product $H_1 \rtimes_\varphi H_2$ has subgroups $\mathcal{H}_1 = \{(h_1, e) : h_1 \in H_1\}$ and $\mathcal{H}_2 = \{(e, h_2) : h_2 \in H_2\}$ isomorphic to H_1 and H_2 respectively. $\mathcal{H}_1$ and $\mathcal{H}_2$ satisfy the three conditions of the inner definition, so we see that an outer semi-direct product is an inner semi-direct product. Working in the other direction, note that for the inner semi-direct product we can define a homomorphism $\varphi \colon H_2 \to Aut(H_1)$ by conjugation: $\varphi(h_2)(h_1) = h_2 h_1 h_2^{-1}$. Then consider multiplication in $G = H_1 \rtimes H_2$:*

$$h_1 h_2 h_1' h_2' = h_1(h_2 h_1' h_2^{-1}) h_2 h_2' = (h_1 \varphi(h_2)(h_1'))(h_2 h_2').$$

The above multiplication follows the definition of outer semi-direct product multiplication. So we can define an isomorphism between $H_1 \rtimes H_2$ and $H_1 \rtimes_\varphi H_2$, by mapping $h_1 h_2 \in H_1 \rtimes H_2$ to $(h_1, h_2) \in H_1 \rtimes_\varphi H_2$. This shows that an inner semi-direct product is an outer semi-direct product.

Now, let us turn our attention to the wreath product, which is an extension to the semi-direct product.

Definition 3.5. *(Wreath product) Let G_1, G_2 be groups and let G_2 be a group acting on a finite set $X_2 = \{x_1, x_2, ..., x_m\}$. Let G_1^m denote the Cartesian product of G_1 with itself m times. Then the wreath product of G_1 with G_2 (denoted $G_1 \wr G_2$) is:*

$$G_1 \wr G_2 = G_1^m \rtimes_\varphi G_2$$

where $\varphi \colon G_2 \to Aut(G_1^m)$. G_2 acts on the elements in G_1^m in the same way as G_2 acts on X_2.

Example 3.5.1. *Consider $(\mathbb{Z}/2\mathbb{Z})^3 \wr S_3 = \{((a_1, a_2, a_3), \rho) : a_1, a_2, a_3 \in \mathbb{Z}/2\mathbb{Z}, \rho \in S_3\}$. Then $\rho \in S_3$ acts on $(\mathbb{Z}/2\mathbb{Z})^3$ in the same way that ρ acts on the set $\{1, 2, 3\}$ - that is, $\varphi(\rho)(a_1, a_2, a_3) = (a_{\rho^{-1}(1)}, a_{\rho^{-1}(2)}, a_{\rho^{-1}(3)})$. Thus we have*

$$\begin{aligned}((a_1, a_2, a_3), \pi)((b_1, b_2, b_3), \rho) &= ((a_1, a_2, a_3) + \varphi(\pi)((b_1, b_2, b_3), \pi\rho). \\ &= ((a_1, a_2, a_3) + (b_{\pi^{-1}(1)}, b_{\pi^{-1}(2)}, b_{\pi^{-1}(3)}), \pi\rho) \\ &= ((a_1 + b_{\pi^{-1}(1)}, a_2 + b_{\pi^{-1}(2)}, a_3 + b_{\pi^{-1}(3)}), \pi\rho)\end{aligned}$$

As we will soon see, the positions of the Rubik's cube under the composition of operations behave similarly to the multiplication defined in example 3.5.1.

4 Positions and Operations of the Rubik's Cube

Before we introduce the Rubik's cube group, we need to introduce a few more definitions to describe the sequence of changes a person will make to solve the cube.

Definition 4.1 (Manoeuvre)**.** *A manoeuvre is a finite sequence of basic moves, in which no consecutive layer moves act on the same layer. We write out the manoeuvre, left-to-right, as the sequence of base moves. In this paper, some manoeuvres will be labelled with a number, eg m_{100}. This corresponds to Bandelow's naming system for manoeuvres; see [2],*

Remark 4.1.5. *When we consider the Rubik's cube group, we can choose whether or not to include cube moves in a manoeuvre. In this paper, we will choose not to for simplicity. We can consider positions that can rotated into each other as essentially the same position, but just seen from the perspective of another observer.*

Definition 4.2 (Position)**.** *The position of a Rubik's cube is described by the location and orientation of each edge and corner cubie. A position can therefore be described as a 4-tuple $p = (\rho, \sigma, x, y)$.*
$\rho \in S_8$ (the permutation of corner cubies within 8 corner cubicles)
$\sigma \in S_{12}$ (the permutation of edge cubies within 12 edge cubicles).
$x = (x_1, x_2, ..., x_8)$ where $x_i = 0, 1, or\, 2$ (the orientation of each of the 8 corner cubie in the corner cubicles, with the corner cubicles labelled from 1 to 8 in a fixed way)
$y = (y_1, y_2, ..., y_{12})$ where $x_i = 0$ or 1 (the orientation of each of the 12 edge cubies in the cubicles, with the edge cubicles labelled from 1 to 12 in a fixed way, like an imaginary skin over the cube). We can consider x and y like coordinates.

Remark 4.2.6. *If we wanted to include cube moves, the position of the cube would be described by the 5-tuple $(\rho, \sigma, \tau, x, y)$, where $\tau \in S_6$ (permuting the face cubies in the 6 face cubicles).*

Definition 4.3 (Operation)**.** *An operation permutes cubies in their cubicles, and (possibly) permutes their orientation. Operations are written in cycle notation in terms of the cubicles. e.g. (+ufl, rub) tells us that a corner cubie in cubicle rub is right twisted as it moves to cubicle ufl, and the cubie in cubicle ufl does not change orientation when it moves to cubicle rub. + denotes that a corner cubie is right twisted when it enters a cubicle, and − denotes a corner cubie is left twisted. For edge cubies, there are only two orientations so an orientation change is always denoted +, e.g. (+uf)(+ur).*

Remark 4.3.7. *Note that operations are distinct from manoeuvres. Different manoeuvres can execute the same operation. For example, $m_5 = (R(U^2RF'D^2FR')^2R'$ and $m_{5c} = URU^2RU^2R'U'RU'R'U^2R'U^2RUR'$ are two distinct manoeuvres but carry out the same operation (+urf)(-ufl).*

5 The Group Structure of the Rubik's Cube

Let us discuss some more obvious groups of the Rubik's cube.

Definition 5.1. *(Illegal Rubik's Cube Operation Group) The illegal Rubik's Cube Group, G^*, is the set of all operations on the cube. This includes operations that involve taking apart and reassembling the cubies (but we are not allowed to rearrange the stickers on the facets).*

From the perspective of solving the cube (without taking it apart, of course), we particularly want to study the operations that can be carried out by a sequence of basic moves.

Definition 5.2. *(Legal Rubik's Cube Operation Group) The legal Rubik's cube group (abbrev. "Rubik's cube group"), G, is a subgroup of the illegal Rubik's cube group and is the set of all operations that can be executed by manoeuvres.*

We can similarly define the illegal and legal manoeuvre group, M^* and M respectively. We can also define the illegal and legal position group, P^* and P respectively.

We can derive some relations between these groups. For example, there exists a surjective (but not injective) homomorphism $\psi\colon M \to G$ which maps every manoeuvre to the operation it carries out. We can consider manoeuvres to be equivalent iff $\psi(m_a) = \psi(m_b)$.

There is a bijection between operations in G^* and positions in P^*; $\Psi : G^* \leftrightarrow P^*$, where $\Psi(p) = g\ I_P$. G^* is a group action of operations on the the set of positions, and each element in G^* is acts on the positions in P^* by definition uniquely. This bijection means that $p \in P$ iff $g \in G$.

6 The Fundamental Laws of Cubology

How do we determine whether $p \in P^*$ is also an element of P? The first fundamental law of cubology allows us to determine whether a position is in the same orbit as the start position I_p under the group action of G.

Theorem 6.1 (First Fundamental Law of Cubology)**.** *A position $p = (\rho, \sigma, x, y) \in P^*$ is also in P if and only if all three criteria is met:*

i $sgn(\rho) = sgn(\sigma)$

ii $x_1 + x_2 + ... + x_8 \equiv 0 \pmod 3$

iii $y_1 + y_2 + ... + y_{12} \equiv 0 \pmod 2$

Proof. **Showing that the three criteria are necessary conditions for a position to be legal**. It is quite clear that the three criteria hold for the start position. In addition, each basic move U, D, R, L, F, B creates an edge 4-cycle and a corner 4-cycle. Since 4-cycles are an odd permutation, $sgn(\rho) = sgn(\sigma)$ holds after every basic move. Thus $sgn(\rho) = sgn(\sigma)$ is invariant under manoeuvers, satisfying (i).

For basic moves R, L, F, B, for two x_i's, the coordinate value increases by 1 (mod 3) and for two x_i's, the coordinate value decreases by 1 (mod 3) and the other four coordinate values do not change, so $\sum_1^8 x_i \equiv 0 \pmod 3$ still holds. Basic moves U and D preserve the value of $\sum_{i=1}^8 x_i \pmod 3$. Thus $\sum_{i=1}^8 x_i \equiv 0 \pmod 3$ is invariant under all manoeuvres, satisfying (ii).

For each basic move, four coordinate values of y change by 1 (mod 2) and the other eight coordinate values are unchanged. Thus (iii) is satisfied.

Showing that the three criteria are sufficient conditions for a position to be legal. We will show that for any position p satisfying the three criteria, there exists a manoeuvre $\dot{M}$ acting on p such that $\dot{M}p = I_p$. WLOG, assume that $sgn(\rho) = sgn(\sigma) = 1$; if a position p' has $sgn(\rho) = sgn(\sigma) = -1$, then applying a basic move to p' will give a new position where $sgn(\rho) = sgn(\sigma) = 1$.

Firstly, we will show that we can always move the corner and edge cubies back into their starting cubicles. Consider any manoeuvre for a corner 3-cycle, for example $m_{100} = RB'RF^2R'BRF^2R^2$. m_{100} executes the operation

$$(ufl, urf, ubr) = (X_1, X_2, X_3)(X_4)(X_5)(X_6)(X_7)(X_8).$$

For brevity, the above operation will be simply referred to as (X_1, X_2, X_3). There exists a manoeuvre, denoted $\tilde{m}$, composed of at most two basic cube moves, which moves X_i (for $4 \leq i \leq 8$) to X_3 (we don't need to worry about making sure that $\tilde{m}$ preserves the positions the other cubies, so long as $\tilde{m}$ preserves X_1 and X_2). Then we can create a manoeuvre, M, that executes the corner 3-cycle (X_1, X_2, X_i) (keeping all other cubies fixed): $M = \tilde{m}\ m_{100}\ \tilde{m}'$. Thus we can create a manoeuvre that executes any edge 3-cycle of the form (X_1, X_2, X_i) for $3 \leq i \leq 8$. Since $\langle(X_1, X_2, X_i)\rangle$ is a group of all permutations in S_8 with $sgn(\rho) = 1$, there is an element in $\langle(X_1, X_2, X_i)\rangle$, namely m_C, that will move the corner cubies into the correct cubicle.

Next, we show that we can move the edge cubies into their starting positions after the corner cubies have been restored. $m_{510} = F^2UM_RU^2M_R'UF^2$ executes the operation $(uf, ul, ur) = (Y_1, Y_2, Y_3)$. There exists a manoeuvre, denoted $\hat{m}$, which moves a fixed cubie Y_i into the cubicle occupied by Y_3. By manoeuvre $\check{M} = \hat{m}\ m_{510}\ \hat{m}'$, we can create any operation of the form (Y_1, Y_2, Y_i). $\langle(Y_1, Y_2, Y_i)\rangle$ generates all permutations of edges in S_{12} such that $sgn(\sigma) = 1$, so there exists an element of $\langle(Y_1, Y_2, Y_i)\rangle$ where $M_E \, M_C \, p = I_p$.

At this point, corner and edge cubies have been restored their starting cubicles. We now show that it is possible to reorient cubies within their cubicles so that the cube returns to the start position. It follows from our proof that $\sum_{i=1}^{8} x_i \equiv 0 \pmod 3$ and $\sum_{i=1}^{8} y_i \equiv 0 \pmod 2$ is invariant under manoeuvres that there is a 1-to-1 correspondence between each right-twisted corner and each left-twisted corner, and that incorrectly oriented edges come in pairs.

By manoeuvre $m_{415b} = LFR'F'L'U^2RURU'R^2U^2R \rightarrow (+uf)(+ur)$, we can reorient pairs of edges. If the incorrectly oriented pair of edge cubies are not diagonally adjacent each other on the same face, then by repeatedly carrying out cube moves and carrying out m_{415b} on one correctly oriented and one incorrectly oriented cubie diagonally adjacent to each other on the same face, we can still eventually reorient the edge cubie (since we can get to any edge cubie by moving to diagonally adjacent cubies (that share the same face) only, without having to revisit any cubies).

By manoevre $m_5 = R(U^2RF'D^2FR')^2R' \rightarrow (+urf)(-ufl)$, we can reorient pairs of oppositely twisted corner cubies on the same long edge of the cube. Analogously, if the oppositely twisted pair of corner cubies do not share the same long edge of the cube, then we can still "chase around the cube" to reorient the aforementioned pair of corner cubies. This completes the argument. □

Corollary 6.1.1. *If you (perish the thought* [2]*) take apart the Rubik's cube and randomly reassemble the cubies, the probability that you will get a position where you can solve the cube using the basic moves is* $\frac{1}{12}$.

Proof. $|P^*| = 8! \cdot 3^8 \cdot 12! \cdot 2^{12}$ is the number of all illegal and legal positions. Criteria (i) of the first law halves $|P^*|$, because $|S_n| = 0.5|S_n|$; criteria (ii) reduces $|P^*|$ to a third, because we can freely choose the coordinate value of $x_1, ..., x_7$ but this determines x_8; criteria (iii) reduces $|P^*|$ by a quarter, because $y_1, ..., y_{11}$ determines y_{12}. Thus

$$|P| = 1/12 \cdot |P^*| \approx 4.3 \times 10^{19}.$$

□

The Second Fundamental Law of Cubology is really the First Fundamental Law in disguise.

Theorem 6.2 (Second Fundamental Law of Cubology)**.** *An operation is legal, if and only if the following three conditions are fulfilled:*

1. *The total number of cycles of even length (corner and edge cycles) is even.*
2. *The number of right-twisting corner cycles is equal to the number of left-twisting cycles in modulo 3.*
3. *The number of reorienting edge cycles is even.*

[2] In the cubing community, disassembling the Rubik's cube for any reason other than for lubricating the cube is considered a permanent badge of dishonour of the worst kind. Shame and guilt will forever follow you. You have been warned.

Proof. The bijection between P^* and G^* allows us to rename the results of the first law in terms of operations. $sgn(\rho) = sgn(\sigma)$ iff there are an even number of odd permutations in total in the operation, so criteria *(ii)* is equivalent to *(1.)*. It can be seen from the proof of the first law that criteria *(2.)* and *(3.)* are true iff criteria *(ii)* and *(iii)* is true respectively. □

Remark 6.0.8. *A position derived from a possible position, by reorienting a cubie, swapping the cubicles of two edge cubies, or swapping two corner cubies, is impossible.*

7 The Group Structure of the Rubik's Cube Revisited

Before we conclude this paper, we shall link the elements of G to wreath products.

Preposition 7.1. *The operations on the corner cubies can be described by $(C_3)^8 \wr S_8)$.*

Proof. Let $gI_p = (x, \rho)$ and $g^*I_p = (x^*, \rho^*)$ denote the positions of the corner cubies. Then consider carrying out operation g followed by operation g^* on the start position. After operation g, orientation of the corner cubies is given by x. Applying operation g^* will permute the cubies within the cubicle according to ρ^*, and will therefore permute the coordinate elements within x in the same way as ρ^* permutes the eight corner cubies. Then x^* will be added onto the permuted x. Thus,

$$\begin{aligned} g^*gI_p &= (x^* + \varphi(\rho^*)x, \rho^*\rho) \\ &= ((x_1^*, x_2^*, ..., x_8^*) + (x_{\rho*^{-1}(1)}, x_{\rho*^{-1}(2)}, ..., x_{\rho*^{-1}(8)}), \rho^*\rho) \\ &= ((x_1^* + x_{\rho*^{-1}(1)}, x_2^* + x_{\rho*^{-1}(2)}, ..., x_8^* + x_{\rho*^{-1}(8)}), \rho^*\rho) \end{aligned}$$

Notice how multiplication of operations works in the same way as multiplication in $(C_3)^8 \wr S_8)$, and how there is a bijection between the operations on corner cubies and elements in $(C_3)^8 \wr S_8)$. Thus operations on corner cubies can be described by $(C_3)^8 \wr S_8)$. □

Preposition 7.2. *The operations on the edge cubies can be described by $(C_2)^{12} \wr S_{12}$.*

Proof. In a similar vein, let $hI_p = (y, \sigma)$ and $h^*I_p = (y^*, \sigma^*)$ denote positions of edge cubies. Then composing operations h and h^* gives

$$\begin{aligned} h^*hI_p &= (y^* + \varphi(\sigma^*)y, \sigma^*\sigma) \\ &= (y_1^* + y_{\sigma*^{-1}(1)}, y_2^* + y_{\sigma*^{-1}(2)}, ..., y_{12}^* + y_{\sigma*^{-1}(12)}), \sigma^*\sigma) \end{aligned}$$

so the group of operations on the edge cubies is isomorphic to $(C_2)^{12} \wr S_{12}$. □

Preposition 7.3. *The illegal Rubik's cube operation group is $G^* = ((C_2)^{12} \wr S_{12}) \times (C_3)^8 \wr S_8)$*

Proof. This follows from definition 4.2 and the bijection between P and G. □

Let us also give one of many possible examples of how we can use our two shiny new fundamental laws of cubology to deduce some information about the subgroups of G.

Theorem 7.1. *The centre of the Rubik's cube group, $Z(G)$, consists of only the identity operation and the superflip operation, (+uf)(+ul)(+ub)(+ur)(+df)(+dl)(+db)(+dr) (+fl)(+lb)(+br)(+rf).*

Proof. Let $gI_P = (\rho, \sigma, x, y)$ for $g \in Z(G)$ and $g^*I_p = (\rho^*, \sigma^*, x^*, y^*)$ and for any $g^* \in G$. Since for $n \geq 3$, $Z(S_n) = \{e\}$ [3], $\rho = I_{S_8}$ and $\sigma = I_{S_{12}}$.
So we only need to show that

$$\begin{aligned}(I_{S_8}, I_{S_{12}}, x, y)(\rho^*, \sigma^*, x^*, y^*) &= (\rho^*, \sigma^*, x^*, y^*)(I_{S_8}, I_{S_{12}}, x, y)\\ (\rho^*, \sigma^*, x + x^*, y + y^*) &= (\rho^*, \sigma^*, x^* + x\rho^*, y^* + y\sigma^*).\end{aligned}$$

This amounts to showing that $x = \rho^* x$ for all $\rho^* \in S_8$ and $y = \sigma^* y$ for all $\sigma^* \in S_{12}$. For this to be true, we must have that $x_1 = x_2 = ... = x_8$ and that $y_1 = y_2 = ... = y_{12}$. The First Fundamental Law prevents $x_i = 1$ and $x_i = 2$. So $x_i = 0$, meaning that elements in the centre subgroup do not change corner cubie orientation. Thus, the only two options for elements in the centre group is for $y_i = 1$ (corresponding to the superflip) and for $y_i = 0$ (corresponding to the identity). □

Remark 7.0.9. *The centre group is very small, especially considering that $|G| = |P|$ is massive, as shown in corollary 6.1.1! This perhaps offers some explanation for why, without knowledge of standard algorithms used to solve the Rubik's cube, it is difficult to solve the cube; operations on the Rubik's cube are extremely non-commutative, and so the order in which operations are carried out matters a great deal.*

8 Concluding remarks and further questions

The topics covered in this paper just scratches the surface of the interesting structures that can be found in the Rubik cube. Although the Rubik's cube might seem like a quaint little toy, some structures in the Rubik's cube can actually have fairly deep links to other fields of mathematics, which the author invites the reader to explore. For example, we can find a subgroup of G which is isomorphic to the quaternion group:

$$\begin{aligned}1 &:= I_G\\ -1 &:= (+uf)(+ul)(+ub)(+ur)\\ i &:= (+ur, uf)(+ul, ub)\\ j &:= (+ul, uf)(+ub, ur)\\ k &:= (+uf, ub)(+ul, ur)\\ -i &:= i^{-1}\\ -j &:= j^{-1}\\ -k &:= k^{-1}.\end{aligned}$$

The above operations obey the quaternion rules $i^2 = j^2 = k^2 = -1$, $ij = (-1)ji = k$, $jk = (-1)kj = i$, $ki = (-1)ik = j$. Are there any more subgroups of G which are isomorphic to other interesting groups?

Even further afield, Bandelow's book hints at a most strange connection between the behaviour of corner cubies in G and elementary physical particles. From the First Fundamental Law, corner cubies can only be twisted in pairs in opposite directions, or twisted in triplets in the same direction. In a similar way, quarks and antiquarks can only exist

[3] Let $f \in S_n$. Then there exists $i \neq j$ such that $f(i) = k$ and there exists $j \neq k$ such that $f(k) = j$. We can then find an element in $g \in S_n$, where g(k)=k and g(i)=j. Then we have that $fg(i) = f(j) \neq k$, and $gf(i) = k$. Hence $fg(i) \neq gf(i)$.

as a quark-antiquark pair (the "meson"), or as a quark-triplet (the "baryon"), or as an antiquark-triplet (the "antibaryon"). The author has effectively zero understanding of elementary particle physics, but the author wonders whether there might be a group theoretical reason for this connection, and wonders whether the Rubik's cube exhibits symmetries that are intrinsic to the physical world. As Bandelow tentatively asks, "will the day come, when new elementary particles are looked for and actually found on the basis of the properties of our corner cubies?".

References

[1] D. Joyner, *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*, ser. Adventures in Group Theory. Johns Hopkins University Press, 2008, ISBN: 978-0-8018-9726-9. [Online]. Available: https://books.google.co.uk/books?id=iM0fco-_Ri8C.

[2] C. Bandelow, *Inside Rubik's Cube and Beyond*, ser. SpringerLink : Bücher. Birkhäuser Boston, 2012, ISBN: 978-1-4684-7779-5. [Online]. Available: https://books.google.co.uk/books?id=93bSBwAAQBAJ.

[3] L. Daniels, "Group theory and the rubik's cube," p. 28, 2014. [Online]. Available: https://www.lakeheadu.ca/sites/default/files/uploads/77/docs/Daniels_Project.pdf.

[4] L. Davidson, "12 things you didn't know about the rubik's cube, the world's best-selling toy," Jul. 17, 2015, ISSN: 0307-1235. [Online]. Available: https://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/11745738/12-things-you-didnt-know-about-the-Rubiks-Cube-the-worlds-best-selling-toy.html (visited on 05/29/2020).