GROUP THEORY OF THE RUBIK'S CUBE

NICHOLAS FLACH

1. Abstract

In this paper, we explore some of the basic topics in group theory and their applications to the Rubik's cube. We define concepts such as cyclic groups, generators, homomorphisms, kernel, direct product and semi-direct product, among others. We then talk about the Rubik's cube, outlining some core properties and some fascinating results. We define the Illegal Rubik's Cube Group and the Legal Rubik's Cube Group and find the order of both. This covers the total number of positions of the Rubik's cube. Finally, we delve into the $2 \times 2 \times 2$ Rubik's cube.

Contents

2. Introduction

In 1974, Hungarian design teacher Ernö Rubik designed a 3D color puzzle he called the Magic Cube. A few years later, a toy company began mass-producing the puzzle, giving it the new name of the Rubik's Cube. The puzzle was a massive success. It only took two years to reach 100 million sales [Mus21]. The Rubik's Cube became a common household item. In the following decades, it became more than just a simple puzzle. Many people began timing themselves solving the cube and pushing for faster times. On October 18, 2004, the World Cube Association was founded, and they began organizing and running official competitions where people

Date: July 10, 2022.

could compete in all sorts of timed events, such as simply solving the Rubik's cube, to solving the $2 \times 2 \times 2$ cube, the $4 \times 4 \times 4$, $5 \times 5 \times 5$, $6 \times 6 \times 6$, $7 \times 7 \times 7$, various other non-cubic twisty puzzles such as the skewb, pyraminx, and megaminx, and even solving the Rubik's cube blindfolded [WCA22].

As a monolith in the puzzle solving community, the Rubik's cube naturally solidified itself in the world of mathematics. Countless mathematicians began to realize the fascinating discoveries that can be found when math is applied to the wonderful puzzle. Despite not needing math to be able to solve the Rubik's Cube, their symbiosis is undeniable, and one of the best ways to consider the Rubik's cube mathematically is through the lens of group theory.

3. Background

Group theory, as the name suggests, is the study of groups.

Definition 3.1. Groups are sets that have a binary operation (let's call it $*$), which maps members of the set to other members of the set. However, there are also some additional restrictions on a set and operation for them to be defined as a group. They must satisfy three properties:

(1) A group must have closure, which means that if $a, b \in G$, then $a * b \in G$.
(2) The operation $*$ must be associative. In mathematical terms, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ for all $g_1, g_2, g_3 \in G$
(3) The group must have an element $e \in G$ that maps all elements to themselves. In mathematical terms, $e * g = g$ and $g * e = g$ for all $g \in G$. This element is called the unit element, or the identity.
(4) Each element in the group must have an inverse. An inverse maps an element to the unit element. In mathematical terms, $g * g^{-1} = e$, and $g^{-1} * g = e$.

Now that we have covered what a group is, let's talk about more group theory terminology. One of the most important types of groups (when it comes to the Rubik's cube) is a cyclic group. A cyclic group is a group where $G = \{g^n | n \in \mathbb{Z}\}$. Essentially, multiplying one element with itself $|G|$ times gives you all elements in the group. This special element g is called a generator, as it generates the group. A common notation to describe a cyclic group and its generator is $G = \langle g \rangle$.

Example 3.1. The group $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ under addition modulo 5 is a cyclic group that can be generated by the element 1.

The element 1 is a generator, and can of course be written as 1^1. The next element, 2, can be written as $1^2 = 1 + 1 \pmod 5 = 2 \pmod 5$. Note that 1^2 denotes the group operation $*$ rather than multiplication. The group operation is addition modulo 5, so $1^2 = 1 * 1 = 1 + 1 \pmod 5$. Similarly, the next element, 3, can be written as $1^3 = 1 + 1 + 1 \pmod 5 = 3 \pmod 5$. The rest follow a the same pattern: $1^4 = 1+1+1+1 \pmod 5 = 4 \pmod 5$, $1^5 = 1+1+1+1+1 \pmod 5 = 0 \pmod 5$. As shown, every element in $\mathbb{Z}_5$ can be written as a power of 1, making it a cyclic group with generator 1. Also note that 2, 3, and 4 work as generators of this group as well.

Example 3.2. Let $H = \{1, 3, 7, 9\}$ be a group under multiplication modulo 10. The group H is cyclic and can be generated by 3.

The element 3 can of course be written as $3^1 = 3$. Then $3^2 = 3 \cdot 3 \pmod{10} = 9 \pmod{10}$. Similarly, $3^3 = 3 \cdot 3 \cdot 3 \pmod{10} = 7 \pmod{10}$. Finally, $3^4 = 3 \cdot 3 \cdot 3 \cdot 3 \pmod{10} = 1 \pmod{10}$. As shown, each element in H can be written as a power of 3, meaning H is a cyclic group that can be generated by 3.

Definition 3.2 (Subgroup)**.** Let H be a subset of a group G. Then H is a subgroup of G if H can be a group with the same operation as G.

Definition 3.3 (Normal Subgroup)**.** Let H be a subgroup of G. H is a normal subgroup of G if, for each $a \in G$, $a^{-1}Ha = H$.

Moving on, there are a few common groups that are important to know.

Definition 3.4 (Symmetric Group)**.** The symmetric group, denoted S_n, is the group of all permutations of n objects.

This concept appears in many scenarios. For example, imagine you have 10 books on a bookshelf. The group describing all of the different ways to arrange the 10 books is S_{10}. An interesting property of these permutations is that they can be written as a combination of cycles flipping only two elements. If a permutations can be written as a combination of an odd number of these cycles, it is called an odd permutation. Similarly, if it can be written as a combination of even number of these cycles it is called an even permutation.

Definition 3.5 (Alternating Group)**.** The alternating group, denoted A_n, is the subgroup of S_n containing only even permutations.

Example 3.3. Let X be the set $\{1, 2, 3\}$. We can use this set to visualize S_3 and A_3.

$$S_3 = \{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\},$$
$$A_3 = \{(1, 2, 3), (2, 3, 1), (3, 1, 2)\}.$$

Definition 3.6 (Homomorphism)**.** Let ϕ be a function from a group G_1 to a group G_2. We call ϕ a homomorphism if it preserves the group operation, meaning

$$\phi(a * b) = \phi(a) * \phi(b)$$

for all $a, b \in G_1$.

Definition 3.7 (Isomorphism)**.** An isomorphism is a homomorphism that is one to one and onto.

Definition 3.8 (Automorphism)**.** An automorphism is a isomorphism of a group to itself: $\phi : G \to G$.

Definition 3.9 (Kernel)**.** Let G_1 and G_2 be groups. Additionally, let there be a homomorphism $\phi : G_1 \to G_2$. The kernel, denoted $\ker(\phi)$, is the set of all elements in G_1 that map to the identity element of G_2.

Definition 3.10 (Direct Product)**.** The direct product between two groups G_1 and G_2, denoted

$$G_1 \times G_2,$$

is the group of all ordered pairs (g_1, g_2), $g_1 \in G_1$, $g_2 \in G_2$ under the operation $(g_1, g_2) * (g_1', g_2') = (g_1 * g_1', g_2 * g_2')$.

Definition 3.11 (Semi-Direct Product)**.** The semi-direct product between two subgroups G_1 and G_2, denoted

$$G_1 \rtimes G_2,$$

is the group $A = G_1G_2$ where $G_1 \cap G_2 = e_A$ and G_1 is a normal subgroup of A.

Example 3.4. $S_n = A_n \rtimes C_2$

The group A_n is the group of all even permutations. The group C_2 is the cyclic group of order 2. This group has many realizations of it. Let's look at the group generated by the swapping of the first two elements of a set. The identity of this group is the cycle that changes nothing, and the only other element is the one that swaps the first two elements of a set. Keep in mind this group is C_2. This group either adds another 2-swap, or doesn't. Since A_n contains all even permutations, adding another 2-swap makes the permutation odd, and not adding one keeps it even. That covers all possible permutations of n elements, which is S_n. Thus, $S_n = A_n \rtimes C_2$.

Definition 3.12 (Wreath Product)**.** Let G be a group, X be the finite set $\{1, 2, 3, \ldots t\}$, and H be a group acting on X. Let G^t denote 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 through its action on X.

4. The Rubik's Cube

Let's begin by defining a notation for the moves of the Rubik's cube. Let F denote a 90 degree clockwise turn of the front side of the cube. Let B denote a 90 degree clockwise turn of the back side of the cube, viewed from the back side. Let U denote a 90 degree clockwise turn of the top side of the cube, viewed from the top. Let R denote the same turn of the right side, L for the left side, and D for the bottom side.

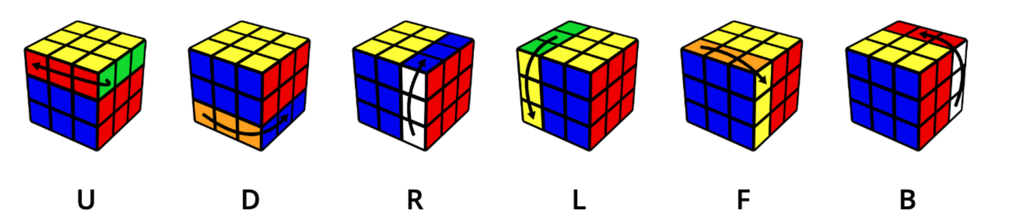


Figure 1. Standard Move Notation, image from [Wan].

Let's also define slice moves M, E, and S:

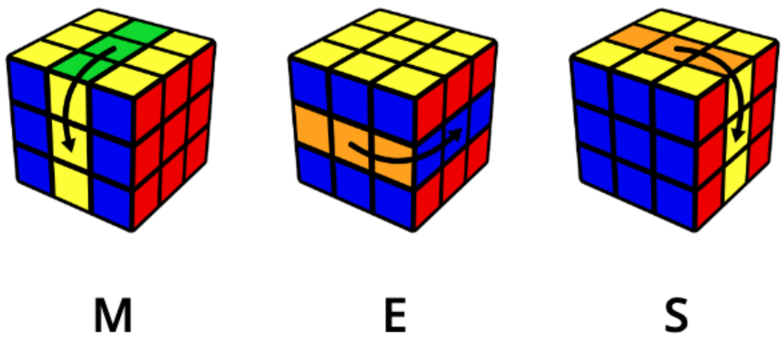
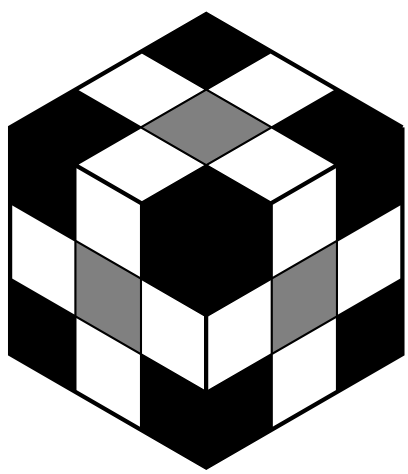


Figure 2. Slice Moves, image from [Wan].

Now we can begin to look at the Rubik's cube as a group. Let's define the pieces with three facets as corners, the pieces with two facets as edges, and the pieces with one facet as centers. In the diagram below, the black pieces are corners, the white pieces are edges, and the gray pieces are centers.

Figure 3. Edges, Corners, and Centers



Differentiating between the types of pieces is extremely important, as they are never interchangeable. In other words, a corner can never be moved to the position of an edge, and an edge can never be moved into the position of a corner. They can be analyzed almost separately except for some constraints they must follow that will be covered later.

Remark. The centers of the Rubik's cube never move.

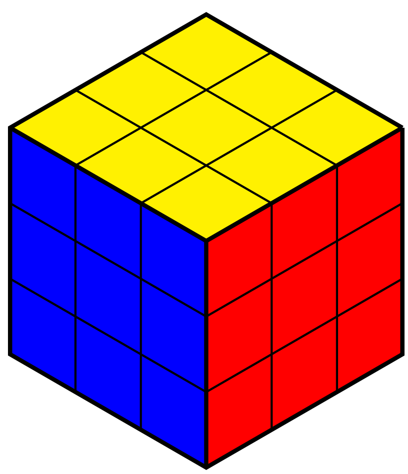
They may rotate with each move, but are never actually moved into a new position, and their color never changes. The only moving pieces are edges and corners.

Note that slice moves do not actually move the centers, because every slice move can be thought of as turning two opposite sides, and then rotating the entire cube. So, each slice move is composed of two standard moves, which do not move centers.

Now, in order to be able to reference each facet of the cube, let each corner be referred to using three letters, and each edge referred to using two letters. To know what each letter means, let the top face be U for up, the right face be R for right, the left face be L for left, and back face be B for back, the bottom face be D for down, and the front face be F for front. The first of the two or three letters is simply the face the facet is on, and then the second letter or second two letters provide information about where on that face the facet is. This is best understood through examples. For these examples, refer to the diagram below, and imagine that you are viewing the cube with the blue face on the front and the yellow face on top. Let's start with edges examples, then corners.

(1) The yellow facet of the blue and yellow edge can be referred to as UF
(2) The yellow facet of the red and yellow edge can be referred to as UR
(3) The red facet of the red and green edge can be referred to as RB (note that green is opposite of blue on the standard Rubik's cube)
(4) The blue facet of the blue and red edge can be referred to as FR

Figure 4. The Rubik's Cube



Now that naming edges might be more understandable, here are some examples of corners using the same diagram.

(1) The yellow facet of the yellow, red, and blue corner is UFR
(2) The blue facet of the blue, white, and red corner is FDR (note that white is opposite of yellow, and is the bottom face here)
(3) The red facet of the yellow, red, and blue corner is RUF

Now that you know more about how we can describe the cube, let's move into defining the Rubik's cube as a group. Let's differentiate between the Illegal Rubik's Cube Group and the Legal Rubik's Cube Group.

Definition 4.1 (Illegal Rubik's Cube Group)**.** The Illegal Rubik's Cube Group is the set of all possible permutations of the corner and edge pieces of the cube given that one is allowed to take it apart and place each piece where desired.

Remark. The Illegal Rubik's Cube Group satisfies all of the conditions of a group, and is therefore a group, not merely a set.

Definition 4.2 (Legal Rubik's Cube Group)**.** The Legal Rubik's Cube Group is the set of all possible permutations of the cube achieved solely through turning the faces of the cube.

Remark. The Legal Rubik's Cube Group also satisfies all of the conditions of a group, and is therefore a group, not merely a set.

Remark. The Legal Rubik's Cube Group is a subgroup of the Illegal Rubik's Cube Group.

Proof. Any turn on the cube can also be accomplished by taking apart the cube and placing each piece on the turned side 90 degrees away from its original position, so every permutation of the cube in the Legal group is also in the Illegal group. ■

To begin to delve into these groups, let's start with the larger Illegal Group.

Proposition 4.1. *The order of the Illegal Rubik's Cube Group is* $2^{12} \cdot 12! \cdot 3^8 \cdot 8! = 519,024,039,293,878,272,000$.

Proof. Since there are 12 edges on the cube, there are 12! different ways to permute them. After permutation, each edge has 2 orientations. So, the total number of positions of the edges is $12! \cdot 2^{12}$. For corners, there are 8, so there are 8! ways to permute them. A corner can be rotated 3 times before it returns to its original position, so each of the 8 corners has 3 possible orientations. This means there are a total of $8! \cdot 3^8$ ways to permute the corners. Thus the total possible permutations of the Illegal Rubik's Cube Group is $12! \cdot 2^{12} \cdot 8! \cdot 3^8$. ■

Now that we have shown the order of this group, let's define its group structure using the same logic from calculating the order.

Proposition 4.2. *The Illegal Rubik's Cube is* $(C_2^{12} \wr S_{12}) \times (C_3^8 \wr S_8)$.

Proof. Since there are 12 edges, on the cube, we can write the ways to position them as the set S_{12}. There are two ways to orient each edge, which can be written mathematically as the set C_2, or, for all 12 edges, C_2^{12}. To factor in both, we can write $C_2^{12} \wr S_{12}$. Similarly, for the 8 corners, we can write the ways to position them as S_8. There are 3 unique orientations of each corner, which can be represented by C_3, or C_3^8 for all 8 corners. We know that we must describe all of the permutations of both the edges and corners in the Illegal group, so we can write this as a direct product of the group containing all of the edge permutations and the group containing all of the corner permutations, which is $(C_2^{12} \wr S_{12}) \times (C_3^8 \wr S_8)$. ■

Now, in order to move from this definition to a definition of the Legal Rubik's Cube Group, we must find a way to filter out all of the positions unreachable by regular turns. There are many different examples of such positions. For example, if a cube is reassembled so that all pieces are solved except a single edge is flipped, shown in Figure 5, there is no way to solve this through regular turns. Also, if one corner is twisted while the rest of the cube is solved, shown in figure 6, there is no way to solve this through regular turns either. But how do we know?

Figure 5. One Edge Flip

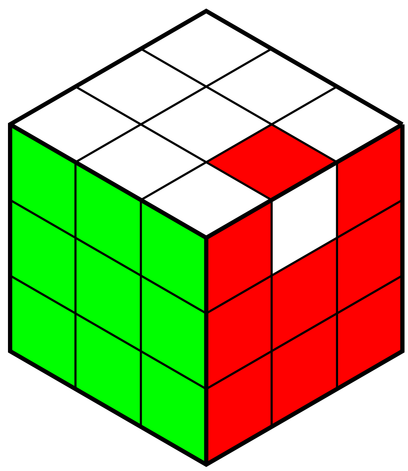
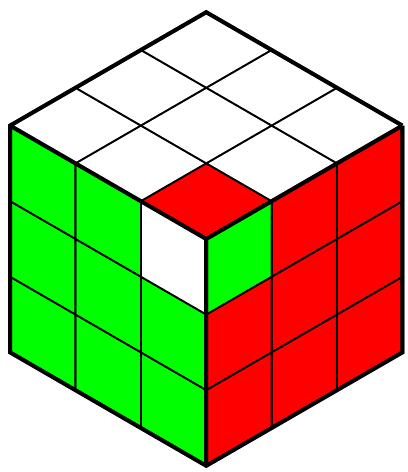


Figure 6. One Corner Twist

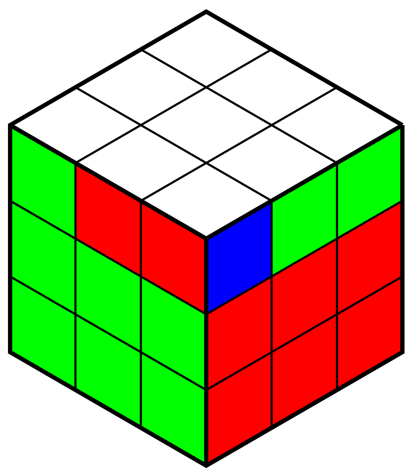


In order to mathematically delineate between solvable and unsolvable positions, a fundamental theorem is needed. Before getting to this theorem, we must prove three important lemmas.

Lemma 4.3. *It is possible to swap any two corners and two edges solely through turns.*

Proof. Let $g \in G$ be the sequence of moves $RUR^{-1}F^{-1}RUR^{-1}U^{-1}R^{-1}FR^2U^{-1}R^{-1}U^{-1}$. This sequence of moves swaps the UR and UF edge as well as the UFR and UBR corners, as shown in the diagram below.

Figure 7. UF and UR swapped, and UFR and UBR swapped

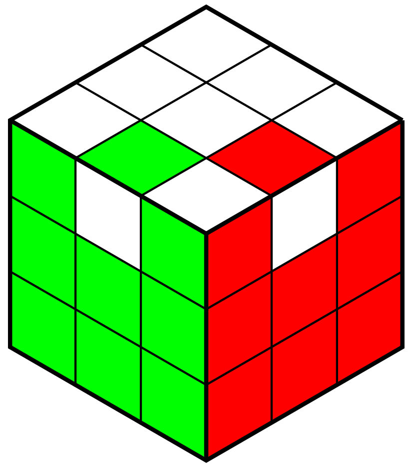


In order to swap any two edges and two corners, one can use a sequence of moves to set up the cube into the position where the two edges that need to be flipped are in the UF and UR position, and the two corners are in the UFR and UBR position, then execute the sequence of moves above, then undo the sequence of setup moves. ■

Lemma 4.4. *Any two edges on the cube can be flipped solely through turns.*

Proof. Let $g \in G$ be a sequence of moves that flips two edges, UF and UR. The move sequence $g = R^{-1}FRU^{-1}M^{-1}U^2MU^{-1}SR^{-1}F^{-1}RS^{-1}$ accomplishes this job, resulting in this position:

Figure 8. UF and UR flipped

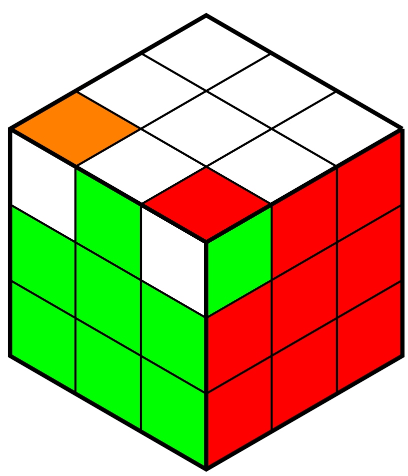


Now, in order to flip any two edges, simply hold the cube so that one flipped edge is in the UF position. There are countless ways to flip this edge and one other around the cube, but the easiest way to comprehend is to simply move the other flipped edge to the UR position in a way that does not effect the UF edge, then execute the sequence of moves g, then undo the moves used to get the second flipped edge to UR. This flips any two edges on the cube. ■

Lemma 4.5. *It is possible (solely through turns) to rotate any two corners such that one is rotated clockwise and the other counterclockwise.*

Proof. Let $g \in G$ be the set of moves $R^{-1}DRD^{-1}R^{-1}DRU^{-1}R^{-1}D^{-1}RDR^{-1}D^{-1}RU$. This move set rotates the UFR corner clockwise and the UFL corner counterclockwise. In other words, it solves this position of the cube:

Figure 9. UFR and UFL Corner Twist



Knowing that this position is solvable, it follows that any two opposite direction corner twists can be solved. Simply hold the cube so that the corner that needs to be twisted clockwise is in the UFR position, then turn the sides of the cube to move the second corner into the UFL position, then execute the sequence of moves to twist UFR clockwise and UFL counterclockwise, and then undo the moves used to place the second corner in the UFL position. ■

Now that these lemmas have been proven, let's move on to the theorem.

Theorem 1 (First Fundamental Theorem of Cube Theory [Dan14]). Let $v \in C_3^8$, $r \in S_8$, $w \in C_2^{12}$, and $s \in S_{12}$ be the four variables that describe a position of the cube. The position is achievable solely through turns if and only if:

(1) $sgn(s) = sgn(r)$
(2) $w_1 + w_2 + w_3 + \ldots + w_{12} = 0 \pmod 2$
(3) $v_1 + v_2 + v_3 + \ldots + v_8 = 0 \pmod 3$

Proof. To start, we need to show that conditions 1, 2, and 3 are satisfied by each turn of the Rubik's Cube.

The first constraint is satisfied because each turn of a face is a 4-cycle of the corners and of the edges, which is an odd permutation. So, each turn is a permutation of the corners and edges of the same parity, meaning the parities are always equal.

The second constraint ensures that there's always an even number of flipped edges. To prove that this is always true, let the facets of each edge be labeled arbitrarily with a 0 and a 1, such that one facet of the edge is labeled 1 and the other is labeled 0. If a turn of the cube moves a 0 onto a 1 or a 1 onto a 0, we can consider that edge as being flipped. If a 1 moves to a 1 or a 0 moves to a 0, we can consider the edge as not getting flipped. With every move, since there are 4 edges being cycled, there will be a total of $0, 2$, or 4 edge flips. Thus, with any sequence of moves, $w_1 + w_2 + w_3 + \ldots + w_{12} = 0 \pmod 2$.

The third constraint serves a similar purpose, but for the corners. We have three possible orientations of the corners. Let's label each facet of the corners with a $0, 1$, or 2, so that each corner has one facet with each labeling. With each move of the cube, if a number increases by $1 \pmod 3$, we can consider it a clockwise twist, and if it increases by $2 \pmod 3$, we can consider it a counterclockwise twist, and if it increases by $0 \pmod 3$, it doesn't change orientation. Imagine one turn of the cube. Let a_1, a_2, a_3, and a_4 be the numbers on the facets of the corners that are on the face being turned. With each corner being moved to the position adjacent to it, the total change in the numbers would be

$$(a_4 - a_3) + (a_3 - a_2) + (a_2 - a_1) + (a_1 - a_4) = 0 \pmod 3.$$

This gives the third constraint in this theorem.

Since this theorem is an if and only if statement, the converse must also be proven. The converse is that, if all three conditions of the theorem are true for a position, that position is solvable. Through lemmas 4.3, 4.4, and 4.5, we know that we can flip any two edges, twist any two corners in opposite directions, and swap any two edges with each other as long as we also swap two corners. These three operations of the cube are enough to solve any position. In other words, the Legal Rubik's Cube Group is generated by these three operations. ■

Moving on, we have the Second Fundamental Theorem of Cube Theory, which outlines criteria for determining if a specific permutation is achievable through turns.

Theorem 2 (The Second Fundamental Theorem of Cube Theory [Dan14]). A change in the pieces position is achievable through turns if and only if:

(1) The total number of even edge and corner cycles is even.
(2) There is an equal number of corners rotated clockwise and corners rotated counterclockwise.
(3) The number of reorienting edge cycles is even.

A proof can be found in [Dan14].

Now that we have outlined the most fundamental theorems, we have conditions to describe the Legal Rubik's Cube Group by viewing the Illegal Group and applying our restrictions.

By the second condition in the First Fundamental Theorem, the parity of the edges must be even. In other words, if we know the position of 11 edges, then there is only one possibility for the last one. So, instead of using C_2^{12} to represent the edge positioning, we can use C_2^{11}. This is because the orientations of the corners can be expressed with only 11 data values as the 12^{th} becomes obsolete. Similarly, due to the third condition of the First Fundamental Theorem, if there are 7 corners with a known position, there is only one option for the placement of the last corner. Thus, we can reduce the C_3^8 to C_3^7. So, we are now at an intermediate step, let's call it $G_0 = (C_2^{11} \rtimes S_{12}) \times (C_3^7 \rtimes S_8)$. This only factors in the second two constraints of the first fundamental theorem, but does not factor in the first, so it is incomplete. That is why this group is an intermediate step; we must first factor in the first constraint before reaching the Legal group. This first constraint tells us $sgn(s) = sgn(r)$. In other words, the parity of the edge permutation must be equal to the parity of the corner permutation. This means that if we know that a certain position's edge parity, we also know its corner parity. This further reduces the group by a factor of C_2. However, we cannot simply write $G = (C_2^{10} \rtimes S_{12}) \times (C_3^7 \rtimes S_8)$. The factor of C_2 needs to be removed from the corners and edges equally, not just the edges. So, we must deal with this condition in another way:

Proposition 4.6. *Let $(v, r, w, s), v \in C_3^8$, $r \in S_8$, $w \in C_2^{12}$, and $s \in S_{12}$ be four variables that define a position of the cube. Additionally, let's define a homomorphism $\phi : G_0 \to \{-1, 1\}$, where*

$$\phi(v, r, w, s) = sgn(r)sgn(s).$$

Then the Legal Rubik's Cube Group is $G = ker(\phi)$. [Dan14]

Proof. Think of this as splitting G_0 in half, as half of the group G_0 maps to 1 and half to -1. To define the legal group, we want to keep the half of G_0 with equal parity. The kernel of ϕ is the group of all elements of G_0 that map to the identity element of $\{-1, 1\}$, and the identity element of $\{-1, 1\}$ is 1. Note that if the parity of the corners is equal to the parity of the edges, $\phi(v, r, w, s) = 1$, meaning that $ker(\phi)$ is the group of all elements of G_0 that have equal parity of edge and corner permutations, which now takes into account all 3 constraints of the first fundamental theorem. Thus, we now have a group G that consists of all elements in the illegal group that are achievable through turns of the faces of the cube. In other words, we have our legal group. ■

Proposition 4.7. *The order of the Legal Rubik's Cube Group is* $|G| = \frac{1}{2} \cdot |G_0| = 2^{10} \cdot 12! \cdot 3^7 \cdot 8! = 43,252,003,274,489,856,000$.

Proof. Given $G = H_1 \times H_2$, we know that $|G| = |H_1| \cdot |H_2|$. ■

That massive number is the total number of positions of the Rubik's cube. This number is exactly $\frac{1}{12}$ of the order of the Illegal Rubik's Cube Group, which means:

Corollary 4.8. *If one took apart and reassembled the cube, there is a* $\frac{1}{12}$ *chance of it being solvable solely through turns.*

Proof. Taking apart and reassembling the cube is equivalent to choosing a random element in the the Illegal Rubik's Cube Group. Since the Legal group is a subgroup of the illegal group, and the order of the legal group is $\frac{1}{12}$ that of the illegal group, there is a $\frac{1}{12}$ chance that a random element in the illegal group is also in the legal group. ■

One can observe that the Legal Rubik's Cube Group is non-abelian. Imagine a cube in the solved state, with white on the top and green on the front. Performing the moves RU leaves the position in Figure 10, whereas the moves UR leave the position in Figure 11, which are clearly not the same. Thus, this group is non-abelian.

Figure 10. *RU*

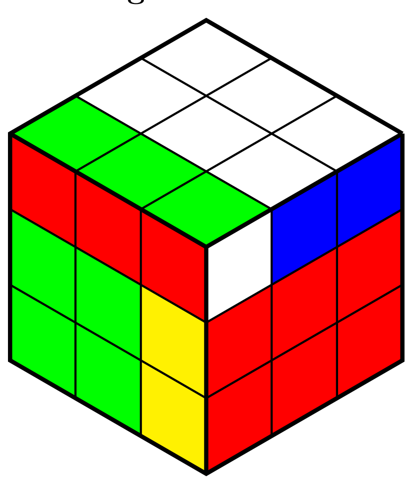
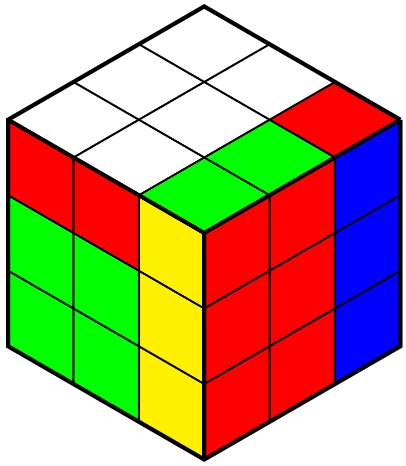


Figure 11. UR



4.1. **Commutators.** A commutator is an important part of group theory that measures commutativity. While commutators have many applications, they are particularly relevant to the Rubik's cube, as they were how people first figured out how to solve the cube when it was released. On the cube, the commutator can cycle 3 pieces without affecting any other pieces. The immediate benefit of this is that, once a piece is solved, it can be left in its solved state while other pieces are being solved, thus making the entire cube solvable. Commutators' ability to affect only 3 pieces at a time make them particularly useful in the world of solving a cube blindfolded. Trying to do so by memorizing the colors of the cube and attempting to solve it as one would without a blindfold is nearly impossible. Instead, top blindfold solvers encode the solution of the cube in letters and solve it using commutators. To uncover this powerful tool, let's look at what a commutator is in group theory.

Definition 4.3 (Commutator)**.** Let $a, b \in G$ where G is a group. A commutator is the product $a * b * a^{-1} * b^{-1}$.

To begin to dissect this, notice that if the last two elements in the product were reversed, we would get the identity element for every a and b. However, the change in order means that we only get the identity in special cases of a and b. This also means we can have a sense of how commutative a group G is by how close or far we are from the identity element.

In terms of the Legal Rubik's Cube Group, $a, b \in G$ denote sequences of moves. For a commutator on the cube, first the sequence of moves a is executed, then the sequence of moves b, then the inverse of a is executed, and then the inverse of b.

Example 4.1. Take the simple commutator that cycles the three edges UF, FR, and LF. Let G be the Legal Rubik's Cube group, and $a, b \in G$. We can define $a = RUR^{-1}$ and $b = E$. Note that this means $a^{-1} = RU^{-1}R^{-1}$ and $b^{-1} = E^{-1}$. So, the commutator $aba^{-1}b^{-1} = RUR^{-1}ERU^{-1}R^{-1}E^{-1}$. This sequence of moves cycles the three edges UF, FR, and LF.

Example 4.2. Let's look at the commutator that cycles the three corners UFR, UFL, and RDF. Take $a, b \in G$ such that $a = R^{-1}D^{-1}R$, $b = U^{-1}$. So, the commutator $aba^{-1}b^{-1} = R^{-1}D^{-1}RU^{-1}R^{-1}DRU$, which cycles three corners.

5. The $2 \times 2 \times 2$ Rubik's Cube

After learning some of the fascinating results that can be found from analyzing the $3 \times 3 \times 3$ Legal Rubik's Cube Group, one might wonder how these concepts apply to other Rubik's puzzles. To begin, let's take a look at the $2 \times 2 \times 2$ Rubik's cube. To approach representing it as a group, we must consider that the $2 \times 2 \times 2$ Rubik's cube only has corners. Unlike on a $3 \times 3 \times 3$ Rubik's cube, there are no pieces that do not move. There are no centers. Thus, we will have to worry about overcounting. Imagine a certain permutation of the cube. If you then rotate the entire cube without turning any of the sides, you get a permutation that is not any different from the first one. So, in counting, we must avoid this.

Remark. For every permutation, there are $6 \cdot 4 = 24$ different appearances of that permutation in the group of all $2 \times 2 \times 2$ permutations.

This means, if we want to only count unique $2 \times 2 \times 2$ permutations, we must divide the total number by 24. Another way to deal with this is to fix a corner in place, and not allow it to move at all, including any re-orientations (twistings) of it. We keep it completely fixed, and that way we are able to view the permutations of the other 7 corners relative to that fixed corner. Now this corner takes the place of centers on a $3 \times 3 \times 3$ cube, in that it acts as a reference for the position of other pieces. This is the same as saying we look at the subgroup of the cube generated by turning 3 adjacent sides, as turning 3 adjacent sides leaves exactly one corner unaffected.

Proposition 5.1. *The Illegal* $2 \times 2 \times 2$ *Group is* $C_3^7 \times S_7$.

Proof. The setup outlined above gives 7 corners to permute, as the 8^{th} is fixed. Each of the 7 corners then has 3 different orientations. Mathematically, this can be written as $C_3^7 \times S_7$, where the S_7 describes the position of corners disregarding orientation, and the C_3^7 represents the 3 possible orientations of the 7 moving corners. ■

Proposition 5.2. *The order of the* $2 \times 2 \times 2$ *illegal group is* $|C_3^7 \times S_7| = 3^7 \cdot 7! = 11,022,480$.

Proof. This follows from the previous proposition and the fact that $|G_1 \times G_2| = |G_1| \cdot |G_2|$ for any two groups G_1, G_2. ■

To move from the $2 \times 2 \times 2$ illegal group to the legal group, we can consider the First Fundamental Theorem of Cube Theory. However, this theorem applies to the $3 \times 3 \times 3$ Rubik's cube, so we must change our scope to make it compatible. Since we fix one corner of the $2 \times 2 \times 2$ in place, the overall cube will also have a fixed orientation like the $3 \times 3 \times 3$ with its centers. Additionally, the $2 \times 2 \times 2$ can be visualized as a $3 \times 3 \times 3$ with irrelevant edges. In other words, the rules pertaining to the corners still apply to the $2 \times 2 \times 2$ cube, but the rules of edges need not be considered.

Proposition 5.3. *The* $2 \times 2 \times 2$ *legal group can be defined as* $C_3^6 \times S_7$.

Proof. By constraint 3 in Theorem 1, the sum of the orientations of each corner must end in the original position, or in mathematical terms, $v_1 + v_2 + v_3 + \ldots + v_8 = 0 \pmod 3$. This means that if we were given the position and orientation of 6 corners (and that of the fixed corner), we know the position and orientation of the last one, and thus it is no longer new information, and we can reduce the illegal group by a factor of C_2 in order to achieve the legal group of $C_3^6 \times S_7$. ■

Proposition 5.4. *The order of the* $2 \times 2 \times 2$ *legal group is* $|C_3^6 \times S_7| = 3^6 \cdot 7! = 3,674,160$.

Proof. This follows from the previous proposition and the fact that $|G_1 \times G_2| = |G_1| \cdot |G_2|$ for any two groups G_1, G_2. ■

This means there are $3,674,160$ possible positions of the $2 \times 2 \times 2$ cube.

5.1. **The two-generator group.** The two-generator group of the $2 \times 2 \times 2$ is the subgroup of the legal group that is generated through turning only two adjacent sides. This leaves two corners unchanged, instead of one. For example, if you turned only the right face with R moves or R^{-1} moves and the up face with U and U^{-1} moves, the bottom left two corners stay in the same position. This subgroup can be written as $G = \langle R, U \rangle$ as it is generated by these two moves. Now, let's look at a subgroup H of this group, where H looks at all of the positions in G that only change the orientation of the corners, but not their actual position. In other words, we look at all of the possible ways to rotate some corners using R, R^{-1}, U and U^{-1}.

Lemma 5.5. *H is an abelian, normal subgroup of G of order* 3^5.

Proof. First, think of a corner's orientation as the group $\mathbb{Z}_3$ under addition. Let's say a corner's solved state is the number 0, then if it gets rotated clockwise its number increases by 1 (mod 3), and if it gets rotated counterclockwise its number decreases by 1 (mod 3). This way, using a simple integer, we can represent the corner's orientation. Since addition modulo 3 is commutative, then H is abelian. To prove normality of the H, let $h \in H$ and $g \in G$. Note that g is some sequence of moves that scrambles the cube, and g^{-1} then solves it from that scrambled state. Also, note that h is some sequence of moves that only affects the orientation of the corners, as it is part of H. So, the overall effect of the moves ghg^{-1} would scramble the cube, then change the orientation of some corners, then resolve it but with some corners' orientations being off. Thus, the only change in the end was with the orientations, meaning $ghg^{-1} \in H$. Therefore, H is a normal subgroup of G. To look at the order, we must consider that there are 6 corners that could have any of 3 orientations. Now, as mentioned earlier, the rules of the first fundamental theorem pertaining to the corners still apply for the $2 \times 2 \times 2$ cube. So, by constraint 3, $v_1 + v_2 + v_3 + \ldots + v_6 = 0 \pmod 3$. This means that, if we know the orientation of 5 corners, the last is already determined from that information. Therefore, the orientation of 5 of the corners is enough information to fully describe each $h \in H$, meaning the order of H is $|H| = 3^5$. ■

The subgroup H also has some other more interesting properties. Delving into them requires knowledge of not only groups, but fields, and other mathematical concepts not discussed in this paper. Further discussion of the subgroup H can be found at [Ben].

6. A Final Note on the $3 \times 3 \times 3$ Rubik's Cube

Another fascinating result that I would like to end on is that of the minimum number of moves needed to solve any position of the Rubik's cube. This was proven by [RKDD13] to be 20 moves in the half turn metric which is 26 moves in the quarter turn metric. Both of these metrics count 90 degree turns of a face as one move, but the half turn metric counts a 180 degree turn of a face as one move whereas the quarter turn metric counts it as two moves. Most use the half turn metric and I would encourage the reader to do the same, as it simply measures any turn of one face as one move.

While I will not go through the full proof of this fascinating result, I will both encourage the reader to read its proof at [RKDD13] and provide an overview of their method. The general idea is that they wanted to put every position of the Rubik's cube in the computer and let the computer calculate the minimum number of moves to solve each position. However, the total of $43,252,003,274,489,856,000$ positions of the cube is simply too large for the computer. The way to fit the entire cube into the computer involves defining a subgroup H of the Legal Rubik's Cube Group, $H = \langle U, D, R2, F2, L2, B2 \rangle$. The $2,217,093,120$ cosets of this subset, all of order $19,508,428,800$, cover the entire legal group. Note that the product of these two numbers is the total number of positions of the cube, so this does cover all positions. They then removed repeated positions and were able to cut down the subgroups enough to the point where the computer was enough to prove this amazing result of 20 moves.

7. Further Questions

Although the $3 \times 3 \times 3$ Rubik's cube has been explored in depth, many other types of Rubik's cubes have not. Other $n \times n \times n$ Rubik's cubes for $n \in \mathbb{Z}, n > 3$ are much less explored, and there is a lot more to be found out about them. Additionally, non cube-shaped Rubik's cubes such as the pyraminx, megaminx, square-1, clock, skewb, ivy cube, Redi cube, the $3 \times 3 \times 2$ cube, the $3 \times 3 \times 1$ cube, and so on, provide interesting grounds for exploration. For example, what are the illegal and legal groups of these puzzles? What is the minimum number of moves to return these puzzles to the solved state from any position? What is the order of the illegal and legal groups of these puzzles? What is the element of highest order in these groups? There is a lot to discover.

Additionally, even the original $3 \times 3 \times 3$ Rubik's cube has more to offer. A fascinating unanswered question pertaining to this cube is that of the minimum number of moves between two different positions of the cube. While many have pondered on the question of the minimum number of moves needed to take a cube from a scrambled state to the solved state, it is not yet known how to calculate the minimum number of moves between two arbitrary permutations of the cube in the legal group. It is left to the reader to explore.

8. Acknowledgements

I would like to thank the Euler Circle for mentoring and advice on how to write a paper, as well as for plenty of insightful math talks. Specifically, thanks to Simon Rubinstein-Salzedo for running the program and Emma Cardwell for mentoring the paper-writing process.

References

[Ben] William Brad Benjamin. Algebra of the 2x2x2 rubik's cube.
[Dan14] Lindsey Daniels. Group theory and the rubik's cube, 2014.
[Mus21] Rubik's cube, Nov 2021.
[RKDD13] Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge. The diameter of the rubik's cube is twenty, Feb 2013.
[Wan] Dylan Wang. Rubik's cube move notation.
[WCA22] World cube association, Jun 2022.