

Group Theory and the Rubik's Cube

by
Lindsey Daniels

A project submitted to the Department of
Mathematical Sciences in conformity with the requirements
for Math 4301 (Honours Seminar)

Lakehead University
Thunder Bay, Ontario, Canada
copyright ©(2014) Lindsey Daniels

Abstract

The Rubik's Cube is a well known puzzle that has remarkable group theory properties. The objective of this project is to understand how the Rubik's Cube operates as a group and explicitly construct the Rubik's Cube Group.

Acknowledgements

I would like to thank my supervisors Dr. Adam Van Tuyl and Dr. Greg Lee for their expertise and patience while preparing this project.

Contents

Abstract	i
Acknowledgements	ii
Chapter 1. Introduction	1
Chapter 2. Groups	3
1. Preliminaries	3
2. Types of Groups	4
3. Isomorphisms	6
Chapter 3. Constructing Groups	9
1. Direct Products	9
2. Semi-Direct Products	10
3. Wreath Products	10
Chapter 4. The Rubik's Cube Group	12
1. Singmaster Notation	12
2. The Rubik's Cube Group	12
3. Fundamental Theorems of Cube Theory	16
4. Applications of the Legal Rubik's Cube Group	20
Chapter 5. Concluding Remarks	22
Chapter 6. Appendix	23
Bibliography	24

CHAPTER 1

Introduction

In 1974, Ernő Rubik invented the popular three dimensional combination puzzle known as the Rubik's Cube. The cube was first launched to the public in May of 1980 and quickly gained popularity. Since its launch, 350 million cubes have been sold, becoming one of the best selling puzzles [2]. By 1982, the cube had become part of the *Oxford English Dictionary* and a household name [5]. In 1981, David Singmaster published *Notes on Rubik's 'Magic Cube'* which was the first analysis of the Rubik's Cube, and provided an algorithm for solving it. Singmaster also introduced 'Singmaster Notation' for the different rotations of the cube [10]. Today, numerous methods for solving the cube exist.

When the cube was first introduced to the public, the focus was on solving the puzzle. Today, the Rubik's Cube is still popular; however, the focus has changed. Speed-cubing competitions are held through the World Cube Association, where participants attempt to solve the cube as fast as possible [2] (the current world record for solving the cube is 5.55 seconds [7]). There is also interest in finding the maximum number of minimum moves needed to put the cube into its solved state from any position. This number is called God's Number and in 2010 was determined to be 20 [9]. God's Number, however, does not say which twists and turns are needed to solve the cube, it merely states what the maximum number of moves is. The challenge for the solver is to find the 20 moves (or less) that are required [8].

Since its creation, the cube has been studied in a variety of fields such as computer science, engineering and mathematics. In mathematics, the Rubik's Cube can be described by Group Theory. The different transformations and configurations of the cube form a subgroup of a permutation group generated by the different horizontal and vertical rotations of the puzzle [2]. The solution to the cube can also be described by Group Theory [5]. Group Theory allows for the examination of how the cube functions and how the twists and turns return the cube to its solved state. This project will explore the construction of this permutation group, as well as the associated properties and theorems.

This project will follow the method of David Joyner's *Adventures in Group Theory: Rubik's Cube, Merlin's Machine and Other Mathematical Toys* to construct the Rubik's Cube Group. To begin, in Chapter 2, the preliminary properties of a group are reviewed. The different types of groups needed to construct the Rubik's Cube Group will be defined, as well as the First Group Isomorphism Theorem. Chapter 3 presents the three different products that are used in the Rubik's Cube Group. Some of the related properties of these products are also described. In Chapter 4, Singmaster Notation will be introduced

and the First and Second Fundamental Theorems of Cube Theory are presented. Here, the Rubik's Cube Group will be explicitly constructed. In Chapter 5 a short summary is provided, along with some possible extensions of this paper. Finally, in Chapter 6 an appendix of move sequences is provided.

CHAPTER 2

Groups

In this chapter, the definition of a group and some of the associated properties are reviewed. Several different types of groups are discussed, as well as the different isomorphism theorems.

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

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

$$\begin{aligned} * : G \times G &\rightarrow G \\ (g_1, g_2) &\mapsto g_1 * g_2. \end{aligned}$$

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 $a * a^{-1} = a^{-1} * a = e$ (*inverses*).

EXAMPLE 2.2. 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 $\frac{1}{2}$ since $2 * \frac{1}{2} = 1$, but $\frac{1}{2} \notin \mathbb{Z}$.

DEFINITION 2.3. The **order** of a group G , denoted $|G|$, is the number of elements in G .

DEFINITION 2.4. 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 2.5. 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 2.6. A group G is a **finite group** if $|G| < \infty$.

EXAMPLE 2.7. For each positive integer $n > 1$, $G = \mathbb{Z}_n$ is a finite group since $|G| = n$.

DEFINITION 2.8. Let G be a group and $H \subset G$. The set $aH = \{ah \mid h \in H\}$ for any $a \in G$ is a **left coset** of H in G . Likewise the set $Ha = \{ha \mid h \in H\}$ for any $a \in G$ is a **right coset** of H in G .

THEOREM 2.9 (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 2.10. Let G and H be finite groups and $H \subset G$. The **index** of H in G is $[G:H] = |G|/|H|$.

EXAMPLE 2.11. 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 $\{1, 3, 5\}$.

DEFINITION 2.12. Let G and H be groups and $H \subset G$. The subgroup H is a **normal** subgroup of G , denoted by $H \triangleleft G$, if, for each a in G , $a^{-1}Ha = H$ (or $aH = Ha$).

EXAMPLE 2.13. 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 $H \triangleleft G$.

LEMMA 2.14. *Let S_1, S_2, \dots, S_n denote finite sets. Then*

$$|S_1 \times S_2 \times \dots \times S_n| = |S_1| \cdot |S_2| \cdot \dots \cdot |S_n|.$$

PROOF. Let $S_1 \times S_2 \times \dots \times S_k = \{(s_1, s_2, \dots, s_n) \mid s_i \in S_i\}$. Now, there are $|S_1|$ choices for s_1 , $|S_2|$ choices for s_2 , $|S_3|$ choices for s_3 , and so on. By the multiplication principle:

$$|S_1 \times S_2 \times \dots \times S_k| = |S_1| \cdot |S_2| \cdot \dots \cdot |S_k|.$$

□

2. Types of Groups

Many special types of groups can be constructed. In this section, the relevant groups that will be needed to construct the Rubik's Cube Group are outlined.

DEFINITION 2.15. 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 2.16. If $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, then a cyclic subgroup would be $\langle 2 \rangle = \{0, 2, 4\}$.

DEFINITION 2.17. A **permutation** of a set G is a one-to-one and onto function from G to itself.

DEFINITION 2.18. A **cycle** is a permutation of the elements in a set $X = \{1, 2, 3, \dots, n\}$ such that $x_1 \mapsto x_2 \mapsto x_3 \mapsto \dots \mapsto x_1$ where $x_i \in X$.

DEFINITION 2.19. 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, the cycle is omitted from the cycle notation. Also, the identity permutation is denoted by (1) .

EXAMPLE 2.20. Take the set $X = \{1, 2, 3, 4\}$ and the permutation $\sigma : X \rightarrow X$ where $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 1$ and $\sigma(4) = 3$. As a cycle, σ is $1 \mapsto 2 \mapsto 4 \mapsto 3 \mapsto 1$ and the cycle notation is (1243) .

DEFINITION 2.21. A cycle $(x_1x_2\dots x_k)$ 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 2.22. 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 2.23. Consider the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$. 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 2.24. The **permutation group** of the set S is the set of all permutations of S that form a group under composition.

EXAMPLE 2.25. Let $T = \{1, 2, 3\}$. A permutation of T would be $\rho : T \rightarrow T$ where $\rho(1) = 2$, $\rho(2) = 3$, and $\rho(3) = 1$. The permutation can be written completely as $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ or in cycle notation $\rho = (123)$. The set of all permutations of T is

$$T_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

In cycle notation, $T_1 = \{(1), (23), (12), (123), (132), (13)\}$. The identity of T_1 is the permutation $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$.

DEFINITION 2.26. The permutation group of n elements, denoted S_n is called the **symmetric group**.

DEFINITION 2.27. The group of all even permutations, denoted A_n , is called the **alternating group**.

DEFINITION 2.28. Let G be a group and $H \triangleleft G$. Then the **factor group** is the group $G/H = \{aH \mid a \in G\}$ under the operation $(aH)(bH) = abH$ for $a, b \in G$.

EXAMPLE 2.29. If $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and $H = \{0, 2, 4\}$, then the factor group $G/H = \{a + H \mid a \in G\}$

$$= \{(0 + \{0, 2, 4\}), (1 + \{0, 2, 4\}), (2 + \{0, 2, 4\}), (3 + \{0, 2, 4\}), (4 + \{0, 2, 4\}), (5 + \{0, 2, 4\})\}$$

$$= \{\{0, 2, 4\}, \{1, 3, 5\}, \{2, 4, 0\}, \{3, 5, 1\}, \{4, 0, 2\}, \{5, 1, 3\}\}$$

$$= \{\{0, 2, 4\}, \{1, 3, 5\}\}.$$

3. Isomorphisms

One of the important concepts in group theory is understanding how to construct isomorphisms.

DEFINITION 2.30. A function ϕ from a group G to a group H is a **homomorphism** if ϕ preserves the group operation; that is, if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

EXAMPLE 2.31. Take $G = S_4$ and $H = \{1, -1\}$ under the operation multiplication. Define the map $\sigma : G \rightarrow H$ with $\sigma(a) = \begin{cases} 1 & a \text{ even} \\ -1 & a \text{ odd} \end{cases}$ for every $a \in G$.

To check that σ is a homomorphism, the 4 possible cases will be verified: a and b both even, a odd and b even, a even and b odd, a and b both odd. Also, recall that the product of two even functions is even, the product of two odd functions is even, and the product of an even function with an odd function is odd.

$$\text{If } a \text{ and } b \text{ are even, then } \phi(ab) = \phi(a)\phi(b) = (1)(1) = 1$$

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

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

$$\text{If } a \text{ and } b \text{ are odd, then } \phi(ab) = \phi(a)\phi(b) = (-1)(-1) = 1$$

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

DEFINITION 2.32. An **isomorphism** is a homomorphism $\phi : G \rightarrow H$ that is a one-to-one and onto. If such a function exists, then G is **isomorphic** to H and denote this by $G \cong H$.

EXAMPLE 2.33. Let $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$ both under the operation addition. Then $\phi : \mathbb{Z} \rightarrow 2\mathbb{Z}$ is an isomorphism where $\phi(a) = 2a$ for all $a \in \mathbb{Z}$.

DEFINITION 2.34. 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 2.35. Take G to be any group under the operation of addition. Then $\rho : G \rightarrow G$ is an automorphism where $\rho(a) = a$ for all $a \in G$.

DEFINITION 2.36. Let G and H be groups and let $f : G \rightarrow H$ be a homomorphism. Then the **kernel** of f is the set $\ker(f) = \{g \in G \mid f(g) = e_H\}$, where e_H is the identity element of H .

EXAMPLE 2.37. Take $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ where $a \mapsto a \pmod{n}$. The identity of \mathbb{Z}_n is 0. So $\ker(f) = \{a \in \mathbb{Z} \mid a = bn, b \in \mathbb{Z}\} = n\mathbb{Z}$.

LEMMA 2.38. Let $f : G \rightarrow H$ be a homomorphism for any two groups, G and H . Then $\ker(f)$ is a normal subgroup of G and $G/\ker(f)$ is a group.

PROOF. First, note that $\ker(f) \neq \emptyset$ since $e_G \mapsto e_H$ by properties of homomorphisms. Next, to show $\ker(f)$ is a subgroup of G , it is enough to show that if $a, b \in \ker(f)$ then $ab^{-1} \in \ker(f)$. Let $a, b \in \ker(f)$, then $f(a) = e_H$ and $f(b) = e_H$. So $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = e_H e_H^{-1} = e_H$. Thus, $ab^{-1} \in \ker(f)$.

Let $g \in G$ and $k \in \ker(f)$. Now, $\ker(f)$ is a normal subgroup of G since:

$$\begin{aligned} f(gkg^{-1}) &= f(g)f(k)(fg^{-1}) \text{ since } f \text{ is a homomorphism} \\ &= f(g)e_H f(g^{-1}) \text{ by definition of kernel and since } k \in \ker(f) \\ &= f(g)(f(g))^{-1} \\ &= e_H. \end{aligned}$$

So $gkg^{-1} \in \ker(f)$. By the definition of a normal subgroup, $\ker(f)$ is normal.

Finally, by definition of a factor group, $G/\ker(f)$ is a group. \square

THEOREM 2.39 (First Isomorphism Theorem of Groups). Let ϕ be a group homomorphism from G to H . Then the map from $G/\ker(\phi)$ to $\phi(G)$ defined by $g\ker(\phi) \rightarrow \phi(g)$ is an isomorphism. That is, $G/\ker(\phi) \cong \phi(G)$.

PROOF. Define a map

$$\begin{aligned} \rho : G/\ker(\phi) &\rightarrow \phi(G) \\ a\ker(\phi) &\mapsto \phi(a). \end{aligned}$$

For ρ to be an isomorphism, ρ must be well-defined, one-to-one, onto and a homomorphism.

First, ρ is well-defined. Suppose:

$$\begin{aligned} a\ker(\phi) = b\ker(\phi) &\iff ab^{-1} \in \ker(\phi) \text{ properties of cosets} \\ &\iff \phi(ab^{-1}) = e_H \text{ where } e_H \text{ is the identity of } H \\ &\iff \phi(a)\phi(b^{-1}) = e_H \text{ since } \phi \text{ is a homomorphism} \\ &\iff \phi(a)(\phi(b))^{-1} = e_H \text{ since } \phi \text{ is a homomorphism} \\ &\iff \phi(a) = \phi(b). \end{aligned}$$

So ρ is well-defined.

Second, ρ is one-to-one. Suppose:

$$\rho(a \ker \phi) = \rho(b \ker \phi).$$

Then, $\phi(a) = \phi(b)$ by mapping of ρ .

$$\text{So, } \phi(ab^{-1}) = e_H.$$

$$\implies ab^{-1} \in \ker \phi$$

$$\implies a \ker \phi = b \ker \phi.$$

Thus ρ is one-to-one.

Next, ρ is onto since if $b \in \phi(G)$, then there exists some $a \in G$ such that $\phi(a) = b$ and $\rho(a \ker \phi) = \phi(a) = b$.

Finally, ρ is a homomorphism.

$$\begin{aligned} \rho((a \ker \phi)(b \ker \phi)) &= \rho(ab \ker \phi) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) \text{ since } \phi \text{ is a homomorphism} \\ &= \rho(a \ker \phi)\rho(b \ker \phi). \end{aligned}$$

So ρ is a homomorphism and it follows that ρ is an isomorphism. \square

EXAMPLE 2.40. Take $\phi : S_4 \rightarrow \mathbb{Z}_2$ where $\phi(a) = \begin{cases} 0 & \text{if } a \text{ even} \\ 1 & \text{if } a \text{ odd} \end{cases}$. Then $\text{Im } \phi = \mathbb{Z}_2$.

Also note that the identity in \mathbb{Z}_2 is 0. Now, the kernel of ϕ is $\ker \phi = \{\text{all even permutations}\} = A_4$. By the First Isomorphism Theorem of Groups, $S_4/A_4 \cong \mathbb{Z}_2$.

CHAPTER 3

Constructing Groups

In this chapter, the construction of groups using direct products, semi-direct products, and wreath products will be examined.

The main sources for this chapter are [4] and [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 G_1 and G_2 is the set $G_1 \times G_2$ under the operation $(g_1, g_2) \cdot (g'_1, g'_2) = (g_1g'_1, g_2g'_2)$ for $g_1, g'_1, \in G_1$ and $g_2, g'_2 \in G_2$.

EXAMPLE 3.2. Let $G_1 = \mathbb{Z}_2$ and $G_2 = \mathbb{Z}_2$. Then

$$\begin{aligned} A &= G_1 \times G_2 \\ &= \mathbb{Z}_2 \times \mathbb{Z}_2 \\ &= \{(0, 0), (0, 1), (1, 0), (1, 1)\}. \end{aligned}$$

EXAMPLE 3.3. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) | x, y \in \mathbb{R}\}$ under addition. That is, if $a, b, c, d \in \mathbb{R}$, then $(a, b) + (c, d) = (a + c, b + d)$.

DEFINITION 3.4. Let G be a group and X be a set. Define a map $G \times X \rightarrow X$. Then the group G **acts** on X if the following happen:

- $ex = x$ for all $x \in X$
- $gx \in X$ for all $g \in G$ and $x \in X$
- $(mn)x = m(nx)$ for all $m, n \in G$ and $x \in X$

EXAMPLE 3.5. Let $G = S_4$ and $X = \{1, 2, 3, 4\}$. Some examples of G acting on X are:

- $[(12)(34)]2 = 1$.
- $[(1234)]3 = 4$.
- $[(132)(12)]2 = 3$.

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

- (1) $A = G_1 G_2$.
- (2) $G_1 \cap G_2 = e_A$ where e_A is the identity element of A .
- (3) $G_1 \triangleleft A$.

EXAMPLE 3.7. The group S_n can be written as a semi-direct product: $S_n = A_n \rtimes \langle(12)\rangle$. Note that $A_n \cap \langle(12)\rangle = e$. Now, for any $a \in S_n$ and $b \in A_n$, $aba^{-1} \in A_n$ since $\text{sgn}(b) = 1$ and for any $s \in \{-1, 1\}$, $\text{sgn}(aba^{-1}) = \text{sgn}(a)\text{sgn}(b)\text{sgn}(a^{-1}) = s^2 = 1$. But this means that aba^{-1} is even, and thus $aba^{-1} \in A_n$. So $A_n \triangleleft S_n \implies S_n \cong A_n \rtimes \langle(12)\rangle$.

EXAMPLE 3.8. The dihedral group (the group of reflections and rotations of a regular polygon with n sides) $D_n = \langle r, s \mid r^n = s^2 = e, sr = r^{-1}s \rangle$ can be expressed as a semi-direct product. Let $G_1 = \langle r \rangle$ where r are the rotations of order n and $G_2 = \langle s \rangle$ where s are the reflections of order 2. Now $G_1 \cap G_2 = e$ and $G_1 \triangleleft D_n$. So $G_1 \rtimes G_2 \cong D_n$.

3. Wreath Products

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

DEFINITION 3.9. Let X be a finite set, G a group and H a group acting on X . Fix a labelling of X , say $\{x_1, x_2, \dots, x_t\}$, 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 .

REMARK 3.10. 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 $(g_1, g_2, \dots, g_t)^h = (g_{1h}, g_{2h}, \dots, g_{th})$.

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

- (1) write H as a permutation group on n items.
- (2) make n copies of the group G .
- (3) 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 .

EXAMPLE 3.11. Let $G = \mathbb{Z}_m$, $H = S_n$ and $X = \{1, 2, 3, \dots, n\}$. Then the wreath product of G by H is $\mathbb{Z}_m^n \wr S_n$ where $\rho : S_n \rightarrow \text{Aut}(\mathbb{Z}_m^n)$ is defined by $\rho(\sigma)(x_1, x_2, \dots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$. The group $\mathbb{Z}_m^n \wr S_n$ is called the **generalized symmetric group**.

The wreath product just shuffles the elements of \mathbb{Z}_m^n according to the action from S_n . The result is a permutation of the original element. Hence, $\mathbb{Z}_m^n \wr S_n$ is called the generalized symmetric group.

EXAMPLE 3.12. Let $G = \mathbb{Z}_2$, $H = S_3$ and $X = \{1, 2, 3\}$. The wreath product of G by H is $\mathbb{Z}_2^3 \wr S_3$. The elements of the wreath product $\mathbb{Z}_2^3 \wr S_3$ are:

$$\{(0, 0, 0)\sigma, (1, 0, 0)\sigma, (0, 1, 0)\sigma, (0, 0, 1)\sigma, (1, 1, 0)\sigma, (0, 1, 1)\sigma, (1, 0, 1)\sigma, (1, 1, 1)\sigma\}$$

where $\sigma \in S_3$.

The wreath product permutes the factors of G according to the action h on X . So if $x \in G$, then the wreath product would take the components of g and shuffle them around according to the action h on the set X .

CHAPTER 4

The Rubik's Cube Group

The Rubik's Cube is a $3 \times 3 \times 3$ cube. The cube can be manipulated by rotating the faces of the cube. There are six faces, with each face composed of nine facets. On each face, the center facet is fixed, and is unmoveable. In total, there are $6 \cdot 9 = 54$ 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.

In this chapter, the Rubik's Cube Group will be defined. As well as some of the associated theorems and applications of the group.

The primary sources for this chapter are [5] and [1].

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 [10] 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.

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

It is noted that the clockwise turns are done as if the solver is looking at that particular face, and then turns the face in the clockwise direction. The inverse of each move would be the 90 degree rotation of the face counter-clockwise and denoted M_i^{-1} , where $M_i \in \{U, F, L, R, B, D\}$.

EXAMPLE 4.1. The combination FLU would result in the front face of the cube being rotated 90 degrees, then the left face by 90 degrees and finally the upper face 90 degrees. The inverse of FLU would be the move $U^{-1}L^{-1}F^{-1}$.

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 4.2. 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 Legal Rubik's Cube Group and the Illegal Rubik's Cube Group. The difference between the two being that the Illegal Rubik's Cube Group allows the solver to take the cube apart and rearrange the facets. In neither case is the solver allowed to remove the stickers from each facet. As expected, the Rubik's Cube Group is a subset of the Illegal Rubik's Cube group.

Now, not all of the permutations of S_{54} will be possible on the Rubik's Cube. The middle facet on each side of the cube is fixed and cannot be permuted to a different position on the cube. Furthermore, any 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. Hence, G is only a subset of S_{54} and not isomorphic to the full permutation group.

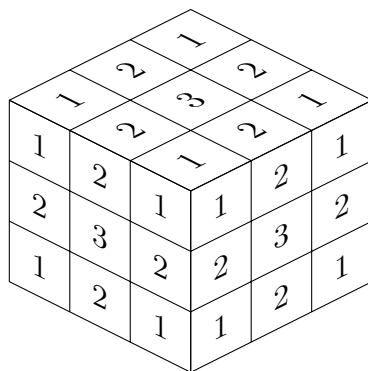


FIGURE 1. The different types of facets on a Rubik's Cube: 1 denotes the facets that make up corner cubes, 2 denotes facets that make up edge cubes and 3 denotes the fixed center cubes [6].

2.1. Corner Cubes. As shown in Figure 1, each corner cube consists of three facets. Now, there are a total of eight corner cubes on a Rubik's Cube and each of the facets that comprise the corner cube lie on three different sides of the cube.

As shown in Figure 2, facet A is on the upper face, facet B is on the left face, and facet C is on the front face. Now, it is possible to reorient the facets of a center cube: 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 . Moreover, since there are eight corner cubes, the orientation of any facet of

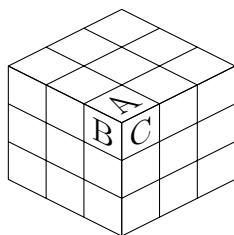


FIGURE 2. The 3 facets that make up a corner cube [6].

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 4.3. *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. \square

2.2. 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.

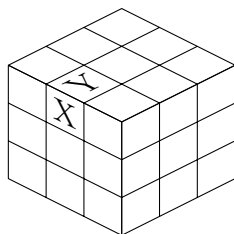


FIGURE 3. The 2 facets that make up an edge cube [6].

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 $C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_2 = C_2^{12}$.

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 4.4. *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. \square

2.3. Cube Position. From Lemma 4.3 any corner cube position can be expressed as a 8-tuple and from Lemma 4.4 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.

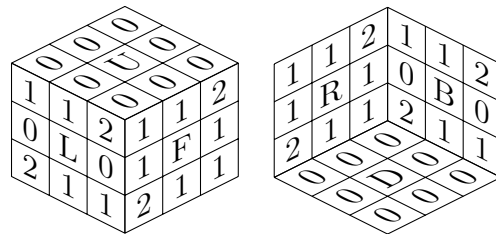
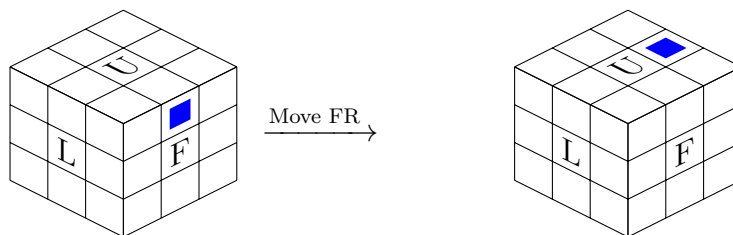


FIGURE 4. The fixed orientation markings, as denoted in [5], for the facets of the Rubik's Cube [6].

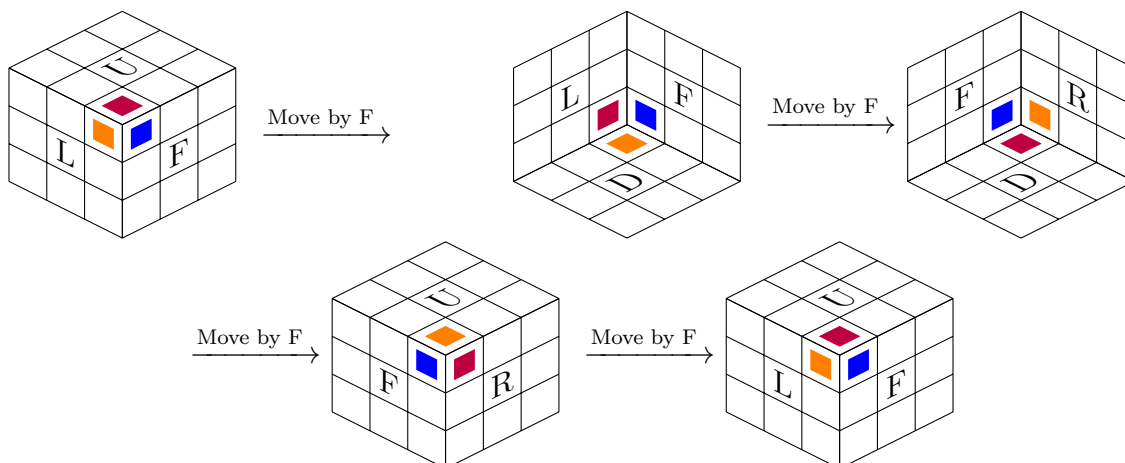
For any arbitrary facet, the position of the facet is assigned the corresponding number above. Even though the facets will be moving around the cube, the numbering system remains fixed.

EXAMPLE 4.5. Consider the top edge cube on the front face of the Rubik's Cube [6]. 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.



REMARK 4.6. With each turn, the edge cube's orientation number is changed by either $0 \pmod 2$ or $1 \pmod 2$.

EXAMPLE 4.7. Consider the cube below [6] and the upper, front and left face corner cube.



Tracking the blue facet, it begins with the number 1, then has number 2, number 1, number 2, and then back to number 1 to complete the cycle. Next, the purple facet starts with number 0, then goes to number 1, number 0, number 1, and then back to 0 to complete the cycle. Finally, the orange facet starts with number 2, then number 0, number 2, number 0, and then back to number 2.

REMARK 4.8. With each turn of the R, L, F or B face, the corner facet orientation number is changed by either $1 \pmod 3$ or $2 \pmod 3$. With each turn of the U or D face, the numbering remains unchanged ($0 \pmod 3$).

REMARK 4.9. The orientation number for any facet is determined by comparing the position of the facet on the Rubik's Cube to the fixed numbering shown in Figure 4.

2.4. 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 4.10. *The Illegal Rubik's Cube Group is $I = (C_2^{12} \wr 12) \times (C_3^8 \wr S_8)$.*

PROOF. This follows from Lemma 4.3, Lemma 4.4 and the definition of the direct product. \square

3. Fundamental Theorems of Cube Theory

To be able to distinguish between the legal and illegal Rubik's Cube Group, the First and Second 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. The illegal Rubik's Cube group allows the solver to take the cube apart and reassemble it. However, the cube may get reassembled in an arrangement that is not solvable. For example, putting 19 of the cubes back in the solved state and putting the last cube in upside down.

THEOREM 4.11 (First Fundamental Theorem of Cube Theory). [1]

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) $\text{sgn}(r) = \text{sgn}(s)$ (equal parity of permutations).
- (2) $v_1 + v_2 + v_3 + \dots + v_8 = 0 \pmod{3}$ (conservation of the total number of twists).
- (3) $w_1 + w_2 + w_3 + \dots + w_{12} = 0 \pmod{2}$ (conservation of the total number of flips).

PROOF. (\Rightarrow) Let $v \in C_3^8$, $r \in S_8$, $w \in C_2^{12}$, $s \in S_{12}$ and $g \in G$ where g is a move that rearranges the cube from the solved state to a state (v, r, w, s) . So g can be written as $g = M_1 M_2 \dots M_n$ where $M_i \in \{F, L, U, B, R, D\}$.

- (1) With each move a total of four edge cubes and four corner cubes are moved; that is, the same number of corner cubes are moved and the same number of edge cubes are moved. Note that each permutation is a 4-cycle, which is odd and has

$$\text{sgn} = -1. \text{ So for each } g: \text{sgn}(r) = \prod_{k=1}^n \text{sgn}(M_i) = \text{sgn}(s)$$

- (2) Note that if M_i is U or D , then v remains unchanged, since the all corner cubes remain on the same face. If M_i is R , L , F , or B , then two corner cubes are moved. One corner cube is moved down off the U face and one corner cube is moved up onto the U face. So, the components of v are either decreased by $1 \pmod{3}$ or increased by $1 \pmod{3}$, respectively. But this means that for any R , L , F , or B , $v_1 + v_2 + v_3 + \dots + v_8 = 1 \pmod{3} - 1 \pmod{3} = 0 \pmod{3}$. So $v_1 + v_2 + v_3 + \dots + v_8 = 0 \pmod{3}$ for any move g .
- (3) For each move g a total of four edge cubes will be reoriented. So $w_1 + w_2 + w_3 + \dots + w_{12} = 4 \pmod{2}$.

(\Leftarrow) Let $A = (v, r, w, s)$ and let A satisfy conditions (1), (2), and (3).

Condition (1) says that $\text{sgn}(s) = \text{sgn}(r)$. So there is equal parity of permutations. Thus the permutations of the corner cubes and edge cubes are either both even or both odd. Assume that $\text{sgn}(s) = \text{sgn}(r) = 1$; that is, the permutations are even. If the permutations are odd, simply apply one of the basic moves (B, F, L, U, R, D) and the new position will satisfy $\text{sgn}(s) = \text{sgn}(r) = 1$.

Now, consider the move for a corner 3-cycle. Take $M = RB^{-1}RF^2R^{-1}BRF^2R^2$ for example. The move M cycles the upper-front-left, upper-front-right, and upper-back-right corner cubes without changing the position of the other cubes. Denote the upper-front-left cube as a_1 , the upper-front-right cube as a_2 , and the upper-back-right cube as a_3 and denote the remaining corner cubes as a_4, a_5, a_6, a_7 and a_8 . For every a_i , from a_4, a_5, a_6, a_7, a_8 , there exists a move x from $\{B, F, L, U, R, D\}$ of at most two moves (that is, two of B, F, L, U, R, D) such that a_i is moved to the position of a_3 without changing the position of a_1 and a_2 . Now, apply the transformation xMx^{-1} . This move creates the 3-cycle (a_1, a_2, a_i) . This 3-cycle can be obtained for any of the a_i 's; that is, the 3-cycles (a_1, a_2, a_3) , (a_1, a_2, a_4) , (a_1, a_2, a_5) , (a_1, a_2, a_6) , (a_1, a_2, a_7) and (a_1, a_2, a_8) can all be obtained by the appropriate move x . But, this generates all the even permutations of the

corner cubes. Therefore, there exists an appropriate move x that will return all the corner cubes to their home positions.

Now, consider the move for an edge 3-cycle. Take the move $M^* = R^2UFB^{-1}R^2F^{-1}BUR^2$ (see appendix for diagram). The move M^* cycles the upper-front, upper-back and upper-right edge cubes without changing the position of any of the other cubes. Denote the upper-front cube as b_1 , the upper-back cube as b_2 and the upper-right cube as b_3 and denote the remaining edge cubes by $b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}$ and b_{12} . Likewise with the corner cubes, for any b_i from $b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12}$, there exists a move y from $\{B, F, L, U, R, D\}$ of at most 2 moves so that the edge cube b_i is moved to the position of b_3 without changing the position of b_1 and b_2 . Now, apply the transformation yM^*y^{-1} . This transformation creates the 3-cycle (b_1, b_2, b_i) . But using an appropriate choice for y , the 3-cycles $(b_1, b_2, b_3), (b_1, b_2, b_4), (b_1, b_2, b_5), (b_1, b_2, b_6), (b_1, b_2, b_7), (b_1, b_2, b_8), (b_1, b_2, b_9), (b_1, b_2, b_{10}), (b_1, b_2, b_{11}),$ and (b_1, b_2, b_{12}) . These generate all the even permutations of the edge cubes. Thus, there exists an appropriate move y that will return all of the edge cubes into their home positions.

All that is left to do is to reorient the cubes so that the facets are colour matched.

Condition (2) says that there is a conservation of total twists; that is, the number of clockwise twists is equal to the number of counterclockwise twists. This means there exists a move which twists exactly 2 corner cubes and preserves the orientation and position of all the other cubes, namely the move $M_1 = (R^{-1}D^2RB^{-1}U^2B)^2$ which twists the upper-front-right corner cube by 120 degrees and twists the bottom-down-left cube by -120 degrees. Note that the move M_1 can be modified to obtain a similar result for any 2 corner cubes. To begin to match the facets of the corner cubes, first twist any clockwise and counterclockwise pairs into their solved orientations. The remaining corner cube orientations will occur in triples since the corner cubes obey $\sum_{i=1}^8 v_i = 0 \pmod{3}$. So they will occur in either 3 clockwise twists or 3 counterclockwise twists. Call these 3 cubes $c_1, c_2,$ and c_3 . The remaining corner cubes can be solved by a sequence of corner twisting moves, say $M_1^* = L^{-1}D^2LBD^2B^{-1}UBD^2B^{-1}L^{-1}D^2LU^{-1}$ or a similar move for two of the remaining corner cubes that need reorienting. Now, M_1^* will solve one of the remaining corner cubes, say c_1 , and reorient the other corner cube, say c_2 , into the opposite position to the untouched corner cube, c_3 . That is, if c_3 needs to be solved by a clockwise twist then M_1^* will reorient c_2 to a position that needs a counterclockwise twist to be solved and vice versa. The remaining two cubes can be solved with the appropriate move M_1 . Thus all the corner cubes are in their solved states.

Condition (3) says that there is a conservation of total flips. Since $\sum_{i=1}^{12} w_i = 0$ is done mod 2, there is an even number of edge cubes that need to be flipped. But there exists a move that flips exactly 2 edge cubes and preserves the orientation and position of the remaining cubes. Take the move $M_2 = LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$. The move M_2 flips the upper-front edge cube and the upper-right edges cube, while leaving the position

and orientation off all the other cubes untouched. The move M_2 can be modified appropriately so that any 2 edges cubes can be flipped and the position and orientation of all the other cubes will be preserved. Since there are an even number of edge cubes, all the edge cubes are able to return to their solved orientations.

Thus A is a solvable position on the Rubik's Cube. So (v, r, w, s) is a possible arrangement of the Rubik's Cube. \square

The Second Fundamental Theorem of Cube Theory gives the criteria for legal moves on the Rubik's Cube.

THEOREM 4.12 (Second Fundamental Theorem of Cube Theory). [1]

An operation of the cube is possible if and only if the following are satisfied:

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

PROOF. (\Rightarrow) Let M be an operation on the cube that takes the cube from the solved state to position $g = (v, s, w, r)$, where $v \in C_3^8, r \in S_8, w \in C_2^{12}$, and $s \in S_{12}$.

- (1) By (1) of Theorem 4.11, $sgn(r) = sgn(s)$. But this means that the permutation is even. So the length of the edge and corner cycles is even.
- (2) For any move M , the corner cubes are moved either right, left or not at all. So the cycle changes the sum of v_i by 2, 1 or 0 (mod 3) respectively. By Theorem 4.11, $\sum_{i=1}^8 v_i = 0$ the number of right twists is equal to the number of left twists.
- (3) Note that an edge cycle only reorients if it is changed by an odd number; that is $w_j = 1$ for some $j = \{1, 2, 3, \dots, 12\}$. By Theorem 4.11, $\sum_{i=1}^{12} w_i = 0$. But this means that if one edge cycle is reorienting, then another edge cycle must be reorienting since the sum is zero. Thus, there must be an even number of reorienting edge cycles.

(\Leftarrow) Suppose that (1), (2), and (3) hold. By Theorem 4.11, there exists move M that takes the cube from the the solved state to the state g . There also exists move M^{-1} that takes the cube from the state g to the solved state. Now, by assumption M and M^{-1} satisfy (1), (2), and (3). But M and M^{-1} are both valid operations on the Rubik's Cube. Thus, if (1), (2), and (3) hold, then the operation is valid. \square

With the two fundamental theorems of cube theory, any possible position and operation on the Rubik's Cube can be defined. Also, the theorems eliminate the physically impossible arrangements and moves from the group.

4. Applications of the Legal Rubik's Cube Group

Using the criteria of the First and Second Fundamental Theorems of Cube Theory, the Illegal Rubik's Cube Group can be reduced to the group $G_0 = \{(v, r, w, s) | v \in C_3^8, r \in S_8, w \in C_2^{12}, \text{ and } s \in S_{12}\}$ where G_0 has the properties of Theorem 4.11 and Theorem 4.12.

By Lemma 4.10, the Illegal Rubik's Cube Group is defined to be $I = (C_2^{12} \wr S_{12}) \times (C_3^8 \wr S_8)$. However, by the conditions of Theorem 4.11, the group is double counting some positions of the facets. Condition (2) of Theorem 4.11 determines the position of the corner cubes, but note that once 7 of the corner cubes have their arrangement, the last cube's position would automatically be determined by the given formula. Likewise, condition (3) determines the orientation of the edge cubes. Once 11 edge cubes are given a position, the final edge cube is automatically determined by the formula. Condition (2) reduces the group by a factor of C_3 and condition (3) reduces the group by a factor of C_2 . By reducing I , the group G_0 is obtained.

Note that $G_0 \subset I$; however, G_0 is not quite the Rubik's Cube Group. Some additional reduction will be done to obtain the Rubik's Cube Group G .

THEOREM 4.13. *There exists an isomorphism:*

$$G_0 \cong (C_3^7 \wr S_8) \times (C_2^{11} \wr S_{12})$$

and

$$|G_0| = |S_8||S_{12}||C_2^{11}||C_3^7| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$$

PROOF. By Theorem 4.11, the First Isomorphism Theorem of Groups and the definition of semi-direct product $G_0 \cong (C_3^7 \wr S_8) \times (C_2^{11} \wr S_{12})$. By Lemma 2.14 $|G_0| = |S_8||S_{12}||C_2^{11}||C_3^7| = 8! \cdot 12! \cdot 2^{11} \cdot 3^7$. \square

Now, to obtain the Rubik's Cube Group G , G_0 must be further reduced. Condition (1) of Theorem 4.11 says that the number of even permutations is equal to the odd permutations. So G_0 must be further reduced by a factor of C_2 .

LEMMA 4.14. *The Rubik's Cube Group, G , can be expressed as $G = (C_3^7 \wr S_8) \times (C_2^{10} \wr S_{12})$.*

PROOF. This follows from Lemma 4.10 and Theorem 4.11. \square

COROLLARY 4.15. *The Rubik's Cube Group G is the kernel of the homomorphism*

$$\begin{aligned} \phi : G_0 &\rightarrow \{1, -1\} \\ (v, r, w, s) &\mapsto \text{sgn}(r)\text{sgn}(s). \end{aligned}$$

In particular, $G \subset G_0$ is normal of index 2 and

$$|G| = 8! \cdot 12! \cdot 2^{10} \cdot 3^7.$$

PROOF. Let $G_0 = (C_3^7 \wr S_8) \times (C_2^{11} \wr S_{12})$, $H = \{-1, 1\}$ and $\phi : G_0 \rightarrow H$ where $(\vec{v}, r, \vec{w}, s) \mapsto \text{sgn}(r)\text{sgn}(s)$. Then $\ker(\phi) = \{(v, r, w, s) \mid \phi(v, r, w, s) = e_H\}$, where $e_H = 1$. By Theorem 4.13 and the First Isomorphism Theorem of Groups $G_0/\ker(\phi) \cong G$, where $G = (C_3^7 \wr S_8) \times (C_2^{10} \wr S_{12})$. Next, by Lemma 2.14, $|G| = 8! \cdot 12! \cdot 2^{10} \cdot 3^7$ and $[G_0 : G] = \frac{(8! \cdot 12! \cdot 2^{11} \cdot 3^7)}{(8! \cdot 12! \cdot 2^{10} \cdot 3^7)} = 2$. \square

CHAPTER 5

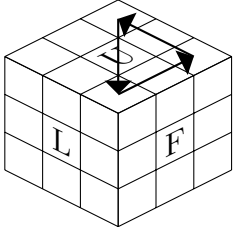
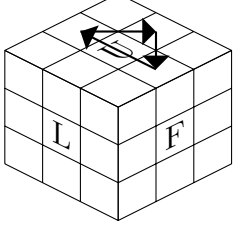
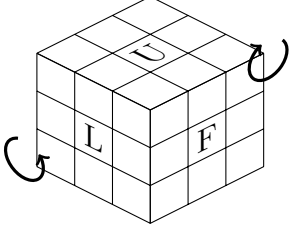
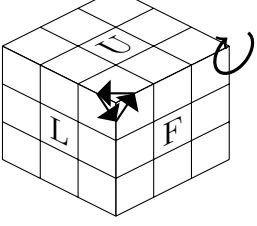
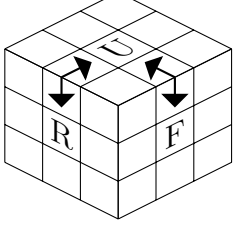
Concluding Remarks

This paper 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 $G = \langle R, B, L, U, F, D \rangle$, which is a subgroup of S_{54} . The First and Second Fundamental Theorems of Cube Theory were presented, which gave the criteria for all the possible arrangements and moves allowed on the cube. The fundamental theorems redefined the Rubik's Cube group to $G = (C_3^7 \wr S_8) \times (C_2^{10} \wr S_{12})$. Furthermore the group G was shown to be the kernel of the homomorphism of $G_0 = (C_3^7 \wr S_8) \times (C_2^{11} \wr S_{12}) \rightarrow \{-1, 1\}$.

The scope of this paper was restricted to the $3 \times 3 \times 3$ Rubik's Cube Group; however, the method developed in this project can be extended to describe the group structure of the $4 \times 4 \times 4$ and $5 \times 5 \times 5$ Rubik's Cube. Moreover, the algorithm for solving any of the 3 cubes can be describe in terms of group operations.

CHAPTER 6

Appendix

Move Sequence [1]	Diagram [6]
$RB^{-1}RF^2R^{-1}BRF^2R^2$	
$R^2UFB^{-1}R^2F^{-1}BUR^2$	
$(R^{-1}D^2RB^{-1}U^2B)^2$	
$R(U^2RF^{-1}D^2FR^{-1})^2R^{-1}$	
$LFR^{-1}F^{-1}L^{-1}U^2RURU^{-1}R^2U^2R$	

Bibliography

- [1] Brandelow, Christoph. *Inside the Rubik's Cube and Beyond*. Birkhäuser. (1982). 12, 17, 19, 23
- [2] Demaine, Erik D.; Demain, Martin L; Eisenstat, Sarah; Lubiw, Anna; Winslow, Andrew. Algorithms for Solving Rubik's cubes. *Lecture Notes in Computer Science*, **6942** (2011) 689-700. 1
- [3] Dummit, David S.; Foote, Richard M. *Abstract Algebra*. Prentice Hall. (1999). 9
- [4] Gallian, Joseph A. *Contemporary Abstract Algebra*. Brooks/Cole, Cengage Learning. (2010). 3, 4, 9
- [5] Joyner, David. *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and other Mathematical Toys*. John Hopkins University Press. (2008). 1, 3, 12, 15
- [6] Kottwitz, Steven. *Example: Sudoku 3D cube*. texexample.net. (2008). Link at <http://www.texample.net/tikz/examples/sudoku-3d-cube/> 13, 14, 15, 23
- [7] Reynolds, Tim. *World cube Association Official Results*. World Cube Organization. (2014). Link at <https://www.worldcubeassociation.org/results/regions.php> 1
- [8] Rokicki, Tomas. Twenty-Two moves suffice for Rubik's Cube. *Math Intelligencer*. **32, No. 1** (2010) 33-40. 1
- [9] Rokicki, Tomas; Kociemba, Herbert; Davidson, Morley; Dethridge, John. The diameter of the Rubik's Cube is twenty. *SIAM J. Discrete Math*, **27, No. 2** (2013) 1082-1105. 1
- [10] Singmaster, David. *Notes on Rubik's 'Magic Cube'*. Enslow Pub Inc. (1981). 1, 12