2009

The Group Theoretic Rubik's Cube

Ashley Cotten

The Group Theoretic Rubik's Cube

Abstract
Cyclic fads often boomerang our childhood toys, sending them back to us with renewed popularity during our adulthood. Recently, Rubik's Cube has made a startling comeback and is once again a staple in most toy stores. Invented by Erno Rubik in his hometown of Budapest, Hungary, the original \Magic Cube" was released in 1974. Upon its world debut in 1980, the toy named after this Hungarian architect became an instant classic. Over 350 billion Rubik's Cubes have been sold worlwide [sic] over the past 30 years, making it easily the top-selling puzzle toy in documented history.

This seemingly innocuous puzzle has frazzled countless children, and perhaps even more adults. The mathematical complexity of the Cube attracted group theorists and other mathematicians upon its release over three decades ago, and the many layers of its structure continue to intrigue the mathematics community. Most of us place emphasis on unscralmbing [sic] the Cube, solving the puzzle. Rather than focusing on the construction of algorithms or solutions to the Cube, we chose to take a group theoretic approach to analyzing this infamous toy. Here, treating Rubik's Cube as a group, we will examine subgroups of the Cube, particularly those constructed via semidirect products. These constructions aid us in describing the possible color arrangements of the Cube.

Degree Type
Open Access Senior Honors Thesis

Department
Mathematics

Keywords
Group theory, Rubik's Cube

THE GROUP THEORETIC RUBIK'S CUBE

By

Ashley Cotten

A Senior Thesis Submitted to the

Eastern Michigan University

Honors College

in Partial Fulfillment of the Requirements for Graduation

with Honors in Mathematics

Introduction

Cyclic fads often boomerang our childhood toys, sending them back to us with renewed popularity during our adulthood. Recently, Rubik's Cube has made a startling comeback and is once again a staple in most toy stores. Invented by Ernö Rubik in his hometown of Budapest, Hungary, the original "Magic Cube" was released in 1974. Upon its world debut in 1980, the toy named after this Hungarian architect became an instant classic. Over 350 billion Rubik's Cubes have been sold worlwide over the past 30 years, making it easily the top-selling puzzle toy in documented history.

This seemingly innocuous puzzle has frazzled countless children, and perhaps even more adults. The mathematical complexity of the Cube attracted group theorists and other mathematicians upon its release over three decades ago, and the many layers of its structure continue to intrigue the mathematics community. Most of us place emphasis on unscralmbing the Cube, solving the puzzle. Rather than focusing on the construction of algorithms or solutions to the Cube, we chose to take a group theoretic approach to analyzing this infamous toy. Here, treating Rubik's Cube as a group, we will examine subgroups of the Cube, particularly those constructed via semidirect products. These constructions aid us in describing the possible color arrangements of the Cube.

Rubik's Cube as a Group

To properly dissect the Cube, we must first understand the conventions of the Cube. Rather than labeling the Cube's six faces by their colors, we label the faces according to their orientation with respect to the user. That is, the faces are labeled front, right, left, up, down, and back with the front face directly facing the user. A labeling of the Cube's faces in which each face is abbreviated to its first letter is shown in Figure 1.

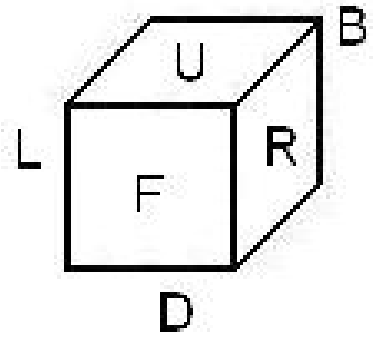

Figure 1: Labeling the Cube's faces.

A 90-degree, clockwise rotation of a face is denoted by the abbreviated label for the face being rotated, F, R, L, U, D, and B respectively. For example, a 90-degree, clockwise rotation of the up face is denoted U, and this rotation is shown below in Figure 2.

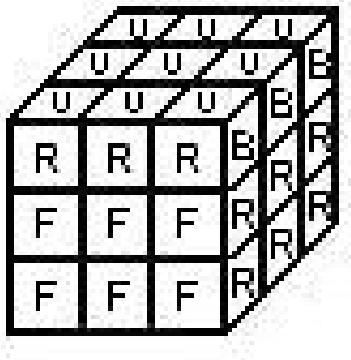

Figure 2: Rotation U.

Rubik's Cube is comprised of 27 smaller cubes called cubinos, forming a 3x3x3 cube of cubinos. Note that only 26 cubinos are exposed to form the six faces as one cubino is located directly in the Cube's center as its rotating mechanism, not belonging to any face, and hence cannot surface through any combination of face rotations. The 26 cubinos forming the faces can be divided into three categories. The 8 corner cubinos are the Cube's corners, with three distinct colors on their three exposed faces.

The 12 edge cubinos are the non-corner cubinos that form the edges of the Cube's faces, with two distinct colors on their two exposed faces. The 6 center cubinos form the centers of each of the Cube's faces and, with only one exposed face, display only one color. Figure 3 displays examples of each type of cubino. Since each face of the Cube is essentially a set of exposed cubino faces, called facelets, each face is composed of 9 facelets for a total of 54 facelets on the Cube.

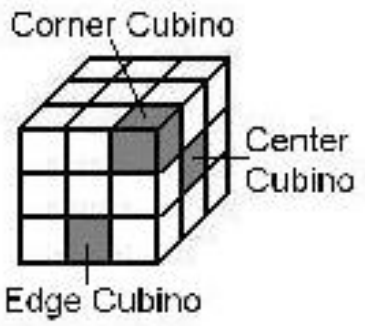

Figure 3: Corner, edge, and center cubinos.

To be considered a group, Rubik's Cube must adhere to certain properties. We first define the set of face rotations F, R, L, U, D, and B along with the multiplicative operation of producing these rotations sequencially as the group G. A group must meet three specific criteria: (1) its operation must be associative, (2) there must be an identity element, and (3) it must have an inverse property. Each of these is simple to check in G. Unlike the standard group-theoretic notation, when performing multiple rotations, the operations are listed from left to right as opposed to a right-to-left listing. Since the product of any two or more operations is simply performing these in sequence from left to right, $(FL)R = F(LR) = FLR$, and this operation is associative. The identity element E is the Cube in its original, clean state. Each element has a corresponding inverse - the 90-degree, counterclockwise rotation of the same face. That is, when we perform a 90-degree, clockwise rotation of any face followed by a 90-degree, counterclockwise rotation of the same face, or vice versa, we return

to the identity E. These inverses are denoted $F^{-1}, R^{-1}, L^{-1}, U^{-1}, D^{-1}$, and B^{-1}.

We may also make additional reductions to simplify notation. When multiplying an element with itself, rather than writing each separately, we may write that element to the second power. For example, instead of FF, we will write F^2. Note that we could similarly write $FFF = F^3$. Upon completing four 90-degree, clockwise rotations of one face, the face will have returned to its starting position. Thus, we say the order of each of these elements (F, R, L, U, D, B) is 4. Also note that three 90-degree, clockwise rotations of the same face produces the same permutation of facelets that a 90-degree, counterclockwise rotation of that face produces. Hence, $FFF = F^3 = F^{-1}$. Therefore, for any given face, using F as example, we will use E, F, F^2, and F^{-1} to denote the rotations of the face.

The aim of the Cube is to unscramble the colored faces so that each of the Cube's faces is homogeneous in color, called the clean state or the identity E. Hence, the 54 facelets act as our underlying set and are shuffled around the Cube by rotations of the Cube's faces. The movement of the facelets via face rotation is called a permutation. We will call the group of all possible permutations of the Cube's facelets the Rubik's group, $\Re$. To find the total order of this group is to find the total number of possible facelet arrangements. If all arrangements were possible, this group would be isomorphic to the symmetric group on 54 letters, Sym_{54}, the order of which is 54!. However, with each facelet limited in its permutations by the type of cubino it lies on, we know the order of $\Re$ must be less than that of Sym_{54}. That is, $|\Re| < |Sym_{54}| = 54! \approx 2.308 * 10^{71}$.

With an incredibly high upper bound on the order of $\Re$, it may be somewhat simpler to tackle the Cube piece by piece in the hopes of building up its total order. It is important to note that each type of cubino, despite permutation, remains essentially the same. That is, corner cubinos will always be corner cubinos, edges will remain

edges, and centers will always be centers. Thus, corners may only be permuted to other corners, edges to edges, and centers to centers. Hence, in this study of the cube, we will analyze each of these subgroups separately, beginning with the corner cubinos.

Group Theoretic Constructs

Before we can begin analyzing subgroups of Rubik's Cube, we must initially tackle a few vital group-theoretic constructs, the first of which is the semidirect product. Building this product requires two groups A and B along with a homomorphism g between A and the automorphism group of B. Assume that A and B are groups, and define a homomorphism $g : A \to Aut(B)$ where $Aut(B)$ is the group of all isomorphisms from B onto itself. That is, g sends an element $a \in A$ to an isomorphism $g_a : B \to B$. Given groups A and B and the homomorphism g, (A, g, B) denotes the semidirect system generated by these. To simplify notation, for all elements $a \in A$, let g_a denote the value of g at a, rather than $g(a)$. Note that g_a is itself a bijective function since it lies in $Aut(B)$, and g_a will take as input any element $b \in B$. Hence, for all $b \in B$, the value of g_a at b will be written $g_a(b)$. Also note that since g is a homomorphism, $g_a^{-1} = g_{a^{-1}}$.

If (A, g, B) is a semidirect system, then $B \rtimes A$ denotes the semidirect product of B and A. This semidirect product is a group under multiplication where the Cartesian product $B \times A$ is the underlying set and multiplication is defined as $(b, a)(b', a') = (bg_a(b'), aa')$ for all $(b, a), (b', a') \in B \times A$. We will prove that $B \rtimes A$ is a group by showing that its multiplication is associative, it has an identity, and it has an inverse property.

For the proof of associativity, let $(b, a), (b', a'), (b'', a'') \in B \times A$ where $b, b', b'' \in B$

and $a, a', a'' \in A$. We must show that

$$((b,a)\cdot(b',a'))\cdot(b'',a'') = (b,a)\cdot((b',a')\cdot(b'',a'')).$$

We will begin by evaluating the left hand side.

$$((b,a)\cdot(b',a'))\cdot(b'',a'') = (bg_a(b'),aa')\cdot(b'',a'') = (bg_a(b')g_{aa'}(b''),aa'a'')$$

Then, evaluating the right hand side:

$$(b,a)\cdot((b',a')\cdot(b'',a'')) = (b,a)\cdot(b'g_{a'}(b''),a'a'') = (bg_a(b'g_{a'}(b'')),aa'a'')$$

Note that since g is a homomorphism, $g_a(b'g_{a'}(b'')) = g_a(b')g_a(g_{a'}(b''))$. Also since g is a homomorphism, $g_a(g_{a'}(b'')) = (g_a \circ g_{a'})(b'') = g_{aa'}(b'')$. Hence, our right hand side becomes

$$(bg_a(b'g_{a'}(b'')),aa'a'') = (bg_ag_{aa'}(b''),aa'a'')$$

and our left and right hand sides are equivalent, proving associativity.

We must now prove the existence of the identity element, (e_B, e_A) where $e_B \in B$ and $e_A \in A$ are the identity elements of their respective groups. To prove this, we must show that for all $(b,a) \in B \times A$, $(b,a)(e_B,e_A) = (e_B,e_A)(b,a) = (b,a)$. We will first prove this for multiplication of the identity on the right. First,

$$(b,a)(e_B,e_A) = (bg_a(e_B), a\cdot id_A).$$

By definition of the group identity elements, for all elements $a \in A, a\cdot e_A = e_A \cdot a = a$, and similarly for all $b \in B$ with respect to e_B. Also note that since g is a homomorphism, it must send the identity element of its domain group to the identity

element of the group it maps onto. Therefore, $g_a(e_B) = e_B$, and

$$(bg_a(e_B), a \cdot e_A) = (b * e_B, a \cdot e_A) = (b, a).$$

For multiplication on the left, we begin

$$(e_B, e_A)(b, a) = (e_B * g_{e_A}(b), e_A \cdot a).$$

Note that g_{e_A} represents the identity bijection, sending each element $b \in B$ to itself. Hence, $g_{e_A}(b) = b$. Therefore,

$$(e_B * ge_A(b), e_A \cdot a) = (e_B * b, e_A \cdot a) = (b, a)$$

and the identity holds.

For each element contained in $B \times A$, its inverse must also lie in $B \times A$. The inverse element for any element $(b, a) \in B \times A$ is $(g_a^{-1}(b^{-1})), a^{-1})$ where $a^{-1} \in A$ and $g_a^{-1}(b^{-1}) \in B$ since A and B are groups and hence must contain each of their elements' inverses. To prove that $B \rtimes A$ is closed under inverses, we must show that for all $(b, a) \in B \times A$, $(b, a)(g_a^{-1}(b^{-1})) = (g_a^{-1}(b^{-1}))(b, a) = (e_B, e_A)$. We will first prove this for multiplication of the inverse on the right. First,

$$(b, a)(g_a^{-1}(b^{-1})), a^{-1}) = (bg_a(g_a^{-1}(b^{-1})), aa^{-1}).$$

Note that $g_a(g_a^{-1}(b^{-1})) = (g_a \circ g_a^{-1})(b^{-1}) = id_B(b^{-1}) = b^{-1}$ where id_B is the identity mapping in B. Therefore,

$$(bg_a(g_a^{-1}(b^{-1})), aa^{-1}) = (bb^{-1}, aa^{-1}) = (e_B, e_A).$$

For multiplication on the left, we begin

$$(g_{a^{-1}}(b^{-1}), a^{-1})(b, a) = (g_{a^{-1}}(b^{-1})g_{a^{-1}}(b), a^{-1}a).$$

Since g is a homomorphism, $g_{a^{-1}}(b^{-1})g_{a^{-1}}(b) = g_{a^{-1}}(b^{-1}b) = g_{a^{-1}}(e_B)$. Also note that $g_{a^{-1}}(e_B) = e_B$ since homormorphisms send the identity element of its domain group to the identity element it maps onto. Therefore,

$$(g_{a^{-1}}(b^{-1})g_{a^{-1}}(b), a^{-1}a) = (e_B, e_A).$$

Hence, the inverse property holds.

Example 1. To help solidify this concept, we first study an example of a semidirect product. Let $(Aut(\mathbb{Z}_3), g, \mathbb{Z}_3)$ be a semidirect system where $g : Aut(\mathbb{Z}_3) \to Aut(\mathbb{Z}_3)$ is just the identity homomorphism. We will examine the semidirect product $\mathbb{Z}_3 \rtimes Aut(\mathbb{Z}_3)$ and show that this is actually a group. Note that $\mathbb{Z}_3 = \{0, 1, 2\}$ forms a group under addition modulo 3 and $Aut(\mathbb{Z}_3)$, the set of all isomorphisms from $\mathbb{Z}_3$ to itself, forms a group under function composition. The isomorphisms in $Aut(\mathbb{Z}_3)$ are easily listed. The first is the identity, which we will simply call $id : \mathbb{Z}_3 \to \mathbb{Z}_3$. This sends each element in $\mathbb{Z}_3$ to itself. That is,

$$0 \to 0, 1 \to 1, 2 \to 2.$$

Since 0, the identity element in $\mathbb{Z}_3$, must be mapped to itself by isomorphism, the only other isomorphism in $Aut(\mathbb{Z}_3)$ must be what we will call $\phi : \mathbb{Z}_3 \to \mathbb{Z}_3$ with the following mapping:

$$0 \to 0, 1 \to 2, 2 \to 1.$$

Hence, $Aut(\mathbb{Z}_3) = \{id, \phi\}$, and we see that $Aut(\mathbb{Z}_3)$ is isomorphic to $\mathbb{Z}_2 = \{0, 1\}$, denoted $Aut(\mathbb{Z}_3) \cong \mathbb{Z}_2$. So the underlying set of our semidirect product is

$\mathbb{Z}_3 \times Aut(\mathbb{Z}_3) \cong \mathbb{Z}_3 \times \mathbb{Z}_2$. We will use this set and the multiplication outlined above to form the semidirect product group. However, we can fill in some additional information about our group multiplication. By the general definition, the multiplication is $(b, a)(b', a') = (bg_a(b'), aa')$ for all $(b, a), (b', a') \in B \times A$. For multiplication in $\mathbb{Z}_3 \rtimes Aut(\mathbb{Z}_3)$, since we know that the binary operation in $\mathbb{Z}_3$ is addition in modulo 3 $(+)$ and the binary operation in $Aut(\mathbb{Z}_3)$ is function composition $(\circ)$, our multiplication becomes $(a, \alpha)(b, \beta) = (a + \alpha(b), \alpha \circ \beta)$ for all $(a, \alpha), (b, \beta) \in \mathbb{Z}_3 \times Aut(\mathbb{Z}_3)$.

Rather than proving directly that $\mathbb{Z}_3 \rtimes Aut(\mathbb{Z}_3)$ is a group using the general proofs above, we will analyze the multiplication table of $\mathbb{Z}_3 \rtimes Aut(\mathbb{Z}_3)$. That is, we will study the results of all possible multiplications of elements within the underlying set $\mathbb{Z}_3 \times Aut(\mathbb{Z}_3)$. The table is shown below.

$\cdot$	$(0, id)$	$(1, id)$	$(2, id)$	$(0, \phi)$	$(1, \phi)$	$(2, \phi)$
$(0, id)$	$(0, id)$	$(1, id)$	$(2, id)$	$(0, \phi)$	$(1, \phi)$	$(2, \phi)$
$(1, id)$	$(1, id)$	$(2, id)$	$(0, id)$	$(1, \phi)$	$(2, \phi)$	$(0, \phi)$
$(2, id)$	$(2, id)$	$(1, id)$	$(1, id)$	$(2, \phi)$	$(0, \phi)$	$(1, \phi)$
$(0, \phi)$	$(0, \phi)$	$(2, \phi)$	$(1, \phi)$	$(0, id)$	$(2, id)$	$(1, id)$
$(1, \phi)$	$(1, \phi)$	$(0, \phi)$	$(2, \phi)$	$(1, id)$	$(0, id)$	$(2, id)$
$(2, \phi)$	$(2, \phi)$	$(1, \phi)$	$(0, \phi)$	$(2, id)$	$(1, id)$	$(0, id)$

This table directly resembles the multiplication table of Sym_3 when using the following mapping:

$$(0, id) \to (1\ 2\ 3) \quad (1, id) \to (3\ 1\ 2) \quad (2, id) \to (2\ 3\ 1)$$
$$(0, \phi) \to (2\ 1\ 3) \quad (1, \phi) \to (1\ 3\ 2) \quad (2, \phi) \to (3\ 2\ 1)$$

Hence, $\mathbb{Z}_3 \rtimes Aut(\mathbb{Z}_3) \cong Sym_3$ and is a group.

Example 2. Similarly, a semidirect product exists between $\mathbb{Z}_5$ and $Aut(\mathbb{Z}_5)$. Our semidirect system can be written $(Aut(\mathbb{Z}_5), h, \mathbb{Z}_5)$ where h is the homomorphism $h : Aut(\mathbb{Z}_5) \to Aut(\mathbb{Z}_5)$. Again, we can let h be the identity map. Also in line with

Example 1, we would like to show that $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$. Let $p \in Aut(\mathbb{Z}_5)$ be any isomorophism from $\mathbb{Z}_5$ to itself. Then we can construct the following mapping from $\mathbb{Z}_4$ to $Aut(\mathbb{Z}_5)$:

$\mathbb{Z}_4$	$Aut(\mathbb{Z}_5)$
0	$p \mapsto p$
1	$p \mapsto 3p$
2	$p \mapsto 4p$
3	$p \mapsto 2p$

This table can be used to verify that this is a homomorphism, that the identity element of $\mathbb{Z}_4$ is sent to the identity in $Aut(\mathbb{Z}_5)$, and that this homomorphism is bijective, thereby forming an isomorphism between $\mathbb{Z}_4$ and $Aut(\mathbb{Z}_5)$. Another way of seeing this isomorphism is by comparing the multiplication tables of both groups. Let $id, \psi_1, \psi_2, \psi_3$ be the mappings of $Aut(\mathbb{Z}_5)$ as listed above. That is, id maps p to p, ψ_1 maps p to $3p$, etc. Then the multiplication tables are as shown below.

$\mathbb{Z}_4$:

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

$Aut(\mathbb{Z}_5)$:

$\circ$	id	ψ_1	ψ_2	ψ_3
id	id	ψ_1	ψ_2	ψ_3
ψ_1	ψ_1	ψ_2	ψ_3	id
ψ_2	ψ_2	ψ_3	id	ψ_1
ψ_3	ψ_3	id	ψ_1	ψ_2

As we can see, the tables are identical when using the mapping from $\mathbb{Z}_4$ to $Aut(\mathbb{Z}_5)$ in the table above. Hence, we can deduce that $\mathbb{Z}_4 \cong Aut(\mathbb{Z}_5)$ and $\mathbb{Z}_5 \rtimes Aut(\mathbb{Z}_5) \cong \mathbb{Z}_5 \rtimes \mathbb{Z}_4$.

The last concept that must be mastered is the short exact sequence. To construct this, we need three groups, say K, G, and H. Also, let $f_1 : K \to G$ and $f_2 : G \to H$ be group homomorphisms. Then the sequence

$$0 \to K \xrightarrow{f_1} G \xrightarrow{f_2} H \to 0$$

is exact if $Ker(f_2) = Im(f_1)$ and $Ker(f_1) = \{id_K\}$ and $Im(f_2) = H$. The last two conditions are equivalent to the conditions that f_1 is injective and f_2 is surjective.

In previous examples, we were able to easily identify the semidirect products and the homomorphism linking the two groups of the semidirect system. For situations in which the semidirect product or the relation between these groups is harder to see, the construction of an exact sequence allows us to find these interactions.

Suppose that the sequence above is exact. Then a splitting is a homomorphism $\sigma : H \to G$ such that $f_2 \circ \sigma = id_H$ where id_H is the identity mapping in H. We claim that this splitting generates a function $\varphi : H \to Aut(K)$. Note that since f_1 is an injection and as a result $K \subset G$, $f_1(K)$ is a normal subgroup of G. Generally, since f_1 is an injection of K into a normal subgroup of G, when convenient, we will identity $f_1(K)$ with K. Hence, for any $g \in G, gKg^{-1} = K$. For any $h \in H$, $\sigma(h) = g$ for some $g \in G$. Therefore, $\sigma(h)K\sigma(h)^{-1} = K$ for any $h \in H$. This says that for each $h \in H$, we may define an automorphism $\varphi_h : K \to K$ by $\varphi_h(k) = \sigma(h)k\sigma(h)^{-1}$ for any $k \in K$, and this mapping from h to φ_h is the definition of $\varphi : H \to Aut(K)$. Using this definition, we may prove that $\varphi : H \to Aut(K)$ is a homomorphism. Let $h_1, h_2 \in H$, and keep in mind that σ is a homomorphism. Then, for any $k \in K$,

$$\varphi_{h_1h_2}(k) = \sigma(h_1h_2)k\sigma(h_1h_2)^{-1} = \sigma(h_1)\sigma(h_2)k\sigma(h_2)^{-1}\sigma(h_1)^{-1} = \varphi_{h_1}(\varphi_{h_2}(k)).$$

This function generated by the splitting creates the semidirect system (H, φ, K) which describes the semidirect product $K \rtimes_\varphi H$. Now, we claim that this semidirect product is isomorphic to G; that is, $K \rtimes_\varphi H \cong G$. To prove this, define the function $F : K \rtimes_\varphi H \to G$ by $F(k, h) = k\sigma(h)$ for any $(k, h) \in K \times H$. First note that F is a homomorphism. To show this, let $(k_1, h_1), (k_2, h_2) \in K \times H$. Then,

$$\begin{aligned} F(k_1, h_1) \cdot F(k_2, h_2) &= k_1\sigma(h_1)k_2\sigma(h_2) \\ &= k_1\sigma(h_1)k_2\sigma(h_1)^{-1}\sigma(h_1)\sigma(h_2) \end{aligned}$$

$$= k_1\varphi_{h_1}(k_2)\sigma(h_1h_2)$$
$$= F((k_1, h_1) * (k_2, h_2))$$

where $*$ denotes multiplication in $K \rtimes_\varphi H$. To prove that F is an isomorphism, we must also prove its injectivity and surjectivity.

To prove the surjectivity of F, let $g \in G$ and let $h = f_2(g)$. Note that $f_2(g\sigma(h^{-1})) = f_2(g)(f_2 \circ \sigma(h^{-1})) = f_2(g)id_H(h^{-1}) = f_2(g)h^{-1} = f_2(g)f_2(g)^{-1} = id_H$. Also, since $Ker(f_2) = Im(f_1)$, $g\sigma(h^{-1}) \in K$. Let us call this element $k = g\sigma(h^{-1})$. We must prove that for any element $(k, h) \in K \times H$, there exists a $g \in G$ such that $F(k, h) = g$. We see that

$$F(k, h) = k\sigma(h) = g\sigma(h^{-1})\sigma(f_2(g)) = g\sigma(f_2(g^{-1}))\sigma(f_2(g)) = g$$

and F is surjective.

Next, we must prove that F is injective. Suppose $F(k, h) = id_G$ where id_G is the identity mapping in G. Then $k\sigma(h) = e_G$ where e_G is the identity element in G. Therefore, $\sigma(h) = k^{-1} \in K$, and since $K = Ker(f_2)$, $\sigma(h) \in Ker(f_2)$. So we know that $f_2 \circ \sigma(h) = e_H$ where e_H is the identity element in H. Since $f_2 \circ \sigma(h) = id_H(h)$, $id_H(h) = e_H$. Therefore $h = e_H$. Applying σ to both sides of this, we find that $\sigma(h) = \sigma(e_H)$, and since σ is a homomorphism, $\sigma(h) = e_G$. We previously noted that $\sigma(h) = k^{-1}$. Hence, $k^{-1} = e_G$, which implies that $k = e_G$, and F is injective.

We now know that F is an isomorphism, and we can say that $K \rtimes_\varphi H \cong G$. Therefore, the construction of a short exact sequence allows us to describe the group in the center of the sequence as the semidirect product of the group to the left of it together with the group to the right. As we will see, this construction is exceedingly useful in building up and describing the group structure of Rubik's Cube.

Applications on the Cube

Though Example 1 from the previous section doesn't directly pertain to the Cube, the semidirect product formed by $\mathbb{Z}_5$ and $Aut(\mathbb{Z}_5)$ from Example 2 describes a 5-cycle subgroup of the corner cubinos. For simplification we will note that, as discussed in the previous section, $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$, the relevance of which will be discussed later. To see the representation of $\mathbb{Z}_5 \rtimes Aut(\mathbb{Z}_5) \cong \mathbb{Z}_5 \rtimes \mathbb{Z}_4$ on the Cube, we analyze the permutations of the corner cubinos of two adjacent faces. Let α be the clockwise rotation of one face of the Cube and β be the clockwise rotation of an adjacent face. Then the element $\alpha \circ \beta = \alpha\beta$ generates the 5-cycle of the corner cubinos shown below.

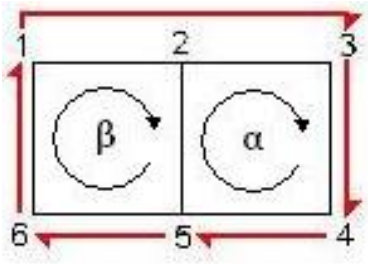

Figure 4: $\alpha\beta$

Note that of the 6 corner cubinos on these two faces, only 5 of the cubinos are permuted while one remains fixed. Since $\alpha\beta$ does not affect the fixed cubino at all, we can compose this element with itself as many times as we'd like - that is, we could perform this sequence of face rotations as many times as we'd like - and the fixed cubino will always remain fixed. To more readily see this as a 5-cycle, we may write this permutation in the following manner:

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

This states that the cubinos beginning in postitions 1 through 6 as listed in the

top row are permuted to the spots listed in the second row. For example, $\alpha\beta$ sends the cubino in position 1 to position 3, the cubino in position 3 to position 4, etc. This cycle is the written version of the diagram in Figure 4. We could also rewrite this cyle as (1 3 4 5 6)(2), symbolizing that the cubinos in positions 1, 3, 4, 5, and 6 are cycled amongst themselves in this order while the cubino in position 2 remains at 2. Since $\alpha\beta$ is composed of a disjoint 5-cycle and 1-cycle, the order of this cycle is 5, and $(\alpha\beta)^5 = id$ where id is the state in which all 6 corner cubinos remain fixed. The set of all powers of $\alpha\beta$, $\{(\alpha\beta)^n : n = 0, 1, 2, 3, 4 \text{ and } (\alpha\beta)^0 = id\}$, together with the operation of function composition creates a cyclic group written as $\langle\alpha\beta\rangle$. Note that this cyclic group is isomorphic to $\mathbb{Z}_5$ with the isomorphism mapping $n \in \mathbb{Z}_5$ to $(\alpha\beta)^n \in \langle\alpha\beta\rangle$ where $n = 0, ..., 4$.

From this, we can construct additional 5-cycles by conjugating the elements of $\langle\alpha\beta\rangle$ by powers of α and/or β. For example, let us conjugate on $\langle\alpha\beta\rangle$ by α. This generates the new underlying set $\alpha\langle\alpha\beta\rangle\alpha^{-1} = \{\alpha\gamma\alpha^{-1} : \gamma \in \langle\alpha\beta\rangle\}$, forming the cyclic group $\langle\alpha\alpha\beta\alpha^{-1}\rangle = \langle\alpha^2\beta\alpha^3\rangle$ of order 5 under function composition. Note that $\alpha^{-1} = \alpha^3$ since α denotes the rotation of a Cube face, making it an element of order 4. Below is the diagram for the generating element of this new cyclic group, $\alpha^2\beta\alpha^3$, with its new fixed point which is now the cubino in position 3.

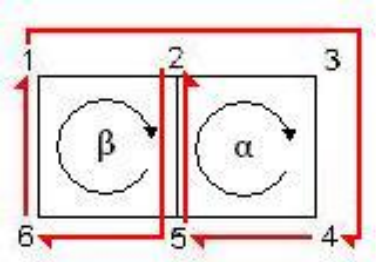

Figure 5: $\alpha^2\beta\alpha^3$

This cycle can be written as the permutation

$$\alpha^2\beta\alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 5 & 2 & 1 \end{pmatrix} = (1\ 4\ 5\ 2\ 6)(3).$$

Like $\langle\alpha\beta\rangle$, the cyclic group generated by $\alpha^2\beta\alpha^3$ is isomorphic to $\mathbb{Z}_5$ with an isomorphism mapping the elements $n \in \mathbb{Z}_5$ to the elements $(\alpha^2\beta\alpha^3)^n \in \langle\alpha^2\beta\alpha^3\rangle$ where $n = 0, ..., 4$. Through various conjugations on $\langle\alpha\beta\rangle$ like this one, we can generate additional 5-cycles each with different fixed points. That is, since there are 6 corner cubinos that could potentially be fixed, we can generate 6 cycles of order 5 which generate cyclic groups isomorphic to $\mathbb{Z}_5$ similar to this one.

Rather than creating these cyclic groups with unique fixed points, we will conjugate this element $\alpha^2\beta\alpha^3$ by varying degrees of β, which will leave the fixed point of $\langle\alpha^2\beta\alpha^3\rangle$ in tact since β does not affect the fixed cubino in position 3. Conjugation by β creates another 5-cycle, depicted as follows:

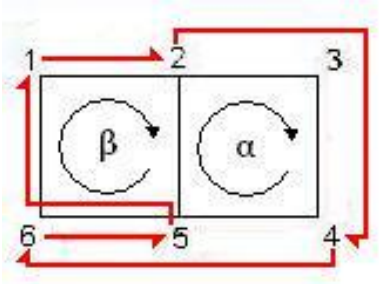

Figure 6: $\beta\alpha^2\beta\alpha^3\beta^{-1}$

Note that this cycle can be written as the permutation

$$\beta(\alpha^2\beta\alpha^3)\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 1 & 5 \end{pmatrix} = (1\ 2\ 4\ 6\ 5)(3).$$

We notice that this cycle is equivalent to $(\alpha^2\beta\alpha^3)^3 \in \langle\alpha^2\beta\alpha^3\rangle$. In fact, if we con-

jugate this element by varying degrees of β (β^0 through β^3 since β is of order 4), we produce all elements of the group $\langle \alpha^2\beta\alpha^3 \rangle$. We leave it to the reader to check the results of conjugating by the remaining degrees of β listed below.

To simplify notation, let $\tau = \alpha^2\beta\alpha^3$. Hence, τ is the generating element of the cyclic group $\langle \tau \rangle$ of order 5. Though we leave it to the reader to formally check these results, obtained by conjugating with various powers of β:

$$\beta^0\tau\beta^{-0} = \tau^1$$
$$\beta^1\tau\beta^{-1} = \tau^3$$
$$\beta^2\tau\beta^{-2} = \tau^4$$
$$\beta^3\tau\beta^{-3} = \tau^2$$

Note the pattern that arises: $\beta^a\tau^p\beta^{-a} = \tau^{3^a p}$ where $a \equiv 0 \text{mod} 4$, and $p \equiv 0 \text{mod} 5$. Note that we should say $\beta^a\tau^p\beta^{-a} = \tau^{p'}$ where $p' \equiv (3^a p) \text{mod} 5$ since τ is of order 5. These conjugations finally allow us to draw an isomorphism from $\mathbb{Z}_4$ to $Aut(\mathbb{Z}_5)$, $\varphi : \mathbb{Z}_5 \to Aut(\mathbb{Z}_5)$. To see this isomorphism, we construct a homomorphism $\varphi : \mathbb{Z}_4 \to Aut(\mathbb{Z}_5)$ defined by the following table:

$\mathbb{Z}_4$	$Aut(\mathbb{Z}_5)$
0	$p \mapsto p$
1	$p \mapsto 3p$
2	$p \mapsto 4p$
3	$p \mapsto 2p$
$\vdots$	$\vdots$
a	$p \mapsto (3^a p) mod 5$

This homomorphism is clearly bijective and, thus, is an isomorphism. Hence, we can say that $\mathbb{Z}_4 \cong Aut(\mathbb{Z}_5)$ and $\mathbb{Z}_5 \rtimes Aut(\mathbb{Z}_5) \cong \mathbb{Z}_5 \rtimes \mathbb{Z}_4$. Using the isomorphism φ, we construct the semidirect system $(\mathbb{Z}_4, \varphi, \mathbb{Z}_5)$. By the definition of mulplication for

a semidirect product, we know that for $(i, a), (i', a') \in \mathbb{Z}_5 \times \mathbb{Z}_4$

$$(i, a) \cdot (i', a') = (i * \varphi_a(i'), a \circ a').$$

By the definition of φ given above, $\varphi_a(i') = 3^a i'$. Also note that since the binary operation on both $\mathbb{Z}_5$ and $\mathbb{Z}_4$ is modular addition $(+)$, we know that both the operations given above ($*$ and $\circ$) are addition. Therefore,

$$(i, a) \cdot (i', a') = (i + 3^a i', a + a').$$

Now define X to be the set of all powers of τ composed with all powers of β. That is, $X = \{\tau^i \beta^a : i, a \in \mathbb{Z}\}$. Note that while i and a may be any integers, it is really only the residue classes of i mod 5 and a mod 4 that matter because of the orders of τ and β. We would first like to argue that X is a subgroup of $\langle \alpha, \beta \rangle$ which is the group comprised of all possible combinations of α and β. By Rotman [2], to show that X is a subgroup of $\langle \alpha, \beta \rangle$, we must prove that X is closed under mutiplication and under inverses.

To prove that X is closed under inverses, let $\tau^n \beta^m \in X$. We must show that its inverse $\beta^{-m} \tau^{-n} \in X$. We can show that this is in fact the inverse element of $\tau^n \beta^m$ by showing that their product is the identity. That is, we will show $(\tau^n \beta^m)(\beta^{-m} \tau^{-n}) = (\beta^{-m} \tau^{-n})(\tau^n \beta^m) = id$:

$$(\tau^n \beta^m)(\beta^{-m} \tau^{-n}) = \tau^n (\beta^m \beta^{-m}) \tau^{-n} = \tau^n (id \circ \tau^{-n}) = \tau^n \tau^{-n} = id$$
$$(\beta^{-m} \tau^n)(\tau^n \beta^m) = \beta^{-m} (\tau^{-n} \tau^n) \beta^m = \beta^{-m} (id \circ \beta^m) = \beta^{-m} \beta^m = id$$

Hence, $\beta^{-m} \tau^{-n}$ is in fact the inverse element on $\tau^n \beta^m$. To show that this inverse element is in X, we will rewrite it as $\beta^{-m} \tau^{-n} = \beta^{-m} \tau^{-n} \beta^m \beta^{-m} = (\beta^{-m} \tau^{-n} \beta^m) \beta^{-m}$. Note that by the definition of τ, $\beta^{-m} \tau^{-n} \beta^m$ is equivalent to some power of τ, say τ^p. Therefore, $\beta^{-m} \tau^{-n} = \tau^p \beta^m \in X$.

To prove that X is closed under multiplication, let $\tau^n\beta^m, \tau^{n'}\beta^{m'} \in X$. We must show that $(\tau^n\beta^m)(\tau^{n'}\beta^{m'}) \in X$. To prove this, we will rewrite this product as follows:

$$(\tau^n\beta^m)(\tau^{n'}\beta^{m'}) = \tau^n\beta^m\tau^{n'}\beta^{-m}\beta^{m+m'}$$

Note that $\beta^m\tau^{n'}\beta^{-m}$ can be rewritten as some power of τ, say τ^q. Then this product becomes

$$\tau^n\tau^q\beta^{-m}\beta^{m+m'} = \tau^{n+q}\beta^{m'}$$

and this product is in X.

Now, define a function $f : \mathbb{Z}_5 \rtimes \mathbb{Z}_4 \to X$ as a function that maps elements $(i, a) \in \mathbb{Z}_5 \times \mathbb{Z}_4$ to elements $\tau^i\beta^a \in X$. Since X describes the cycling corner cubinos, we aim to prove that this function f is a homomorphism to show that the cycle can be described as the semidirect product $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$.

We begin by proving that f is a homomorphism. Let $(i, a), (i', a') \in \mathbb{Z}_5 \times \mathbb{Z}_4$. By the definition of f and the definition of multiplication in $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$, we find

$$f(i, a) \cdot f(i', a') = \tau^i\tau^{\varphi_a i'}\beta^{a+a'} = \tau^{i+\varphi_a i'}\beta^{a+a'} = f((i, a) \cdot (i', a'))$$

and f is a homomorphism.

We must also prove that the kernel of f is trivial. That is, we need to check that nothing nontrivial in $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$ is sent to the identity $id \in X$. We will prove this by contradiction. Suppose $f(i, a) = \tau^i\beta^a = id$ where $i \not\equiv 0 \mod 4$ or $a \not\equiv 0 \mod 5$, i.e. $\tau^i \neq id$ or $\beta^a \neq id$. Then $\tau^i = \beta^{-a}$ which cannot happen because these cycles fix a different number of points; all powers of τ fix one point while β fixes two. Therefore, our kernel is trivial, and f is an injective homomorphism. Also, we know that the cardinality of $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$ is 20 and X can contain no more than 20 elements due to the orders of τ and β. Since the elements of $\mathbb{Z}_5 \rtimes \mathbb{Z}_4$ are unique and directly correspond

to the powers of τ and β, we see that f is surjective, making $f : \mathbb{Z}_5 \rtimes \mathbb{Z}_4 \to X$ an isomorphism.

Corner-Cubino Subgroup Construction

Now, with a better understading of semidirect products and their use for constructing subgroups, we aim to fully construct and analyze the corner-cubino subgroup of the Cube. For the sake of analyzing the corner cubinos alone, we will ignore the edge and center cubinos. The 8 corner cubinos of the standard Rubik's Cube are then, in essence, a 2x2x2 cube. The most we can hope to do is permute these 8 corners amongst themselves and rotate each cube on itself. The permutation of the 8 corners is isomorphic to the symmetric group on 8 letters, Sym_8, with order 8!. As stated previously, the corner cubinos each display three distinctly colored facelets, and thus each have three rotational orientations. These rotations are isomorphic to $\mathbb{Z}_3$, the set of integers under addition modulo 3. Hence, by rotation and permutation, the corner cubinos may generate at most $3^8 8!$ distinct facelet arrangements.

Assume for now that all permutations and rotations of the corner cubinos are possible. That is, imagine that we can take any corner cubino, remove it from the Cube, and place it back into the Cube in any other corner position in any rotation. We will call this group the "take-apart" group, T. Clearly, not all of these arrangements are plausible on the Cube, but understanding this "take-apart" group T will allow us to find the corner-cubino subgroup within this group.

To describe T, we must describe the permutation and color orientation of each of the corner cubinos. First, let us establish a numbering convention to aid in tracking the permutation and color orientation of the corner cubinos. Label each of the 8 corner positions, not the cubinos themselves, with the numbers 1 through 8. At each corner position, the position of each of the cubinos' facelets will be numbered 1

through 3, and the color orientation with the Cube in its clean state will be numbered clockwise as 1-2-3 with one number assigned to each of the cubino's facelets. That is, when the Cube is in its clean state, the numbering on each of the corner cubinos' facelets will line up with the numbering of the facelet positions. This also helps us track rotation of the corners. For example, if a corner cubino is rotated 120 degrees clockwise, then facelet 1 will be at position 2, facelet 2 will be at 3, and facelet 3 will be at 1. Thus, we now have a designated numbering for each corner position and the color orientation at each position.

The permutation of the 8 corner cubinos among these 8 positions is isomorphic to the symmetric group on 8 letters, Sym_8. Each of the corner cubinos have 3 possible color orientations. That is, each corner can be rotated clockwise 120 degrees to achieve new color orientations, and 3 rotations of any cubino will return it to its original orientation. Therefore, the color orientation on each of the corner cubinos is isomorphic to $\mathbb{Z}_3$ where each element of $\mathbb{Z}_3$ corresponds to the number of rotations on the cubino. To track the color orientations of all 8 corners at once, we describe the orientations as elements of $(\mathbb{Z}_3)^8$. These elements are octuples where each element of the ordered pair is the element of $\mathbb{Z}_3$ which describes the rotation on the corner cubino in that respective position. For example, the octuple $(0, 2, 1, 0, 2, 0, 1, 0) \in (\mathbb{Z}_3)^8$ states that the cubino in position 1 is in its original orientation, the cubino in position 2 has been rotated 240 degrees clockwise, etc. Note that $(\mathbb{Z}_3)^8$ only describes the rotation of the cubinos in each position without describing their permutations.

We may now construct an injective homomorphism $i : (\mathbb{Z}_3)^8 \to T$ where i sends each octuple of color orientations to the same cubino arrangement in T. We may also construct a surjective homomorphism $\pi : T \to Sym_8$ where π sends each of the cubino arrangements in T to the permutation in Sym_8 with corresponding cubino positions regardless of color orientation. Note that $Ker(\pi)$ contains all elements (cubino arrangements) in T that keep the cubino positions fixed but may rotate any

of them in any fashion. That is, $Ker(\pi) = (\mathbb{Z}_3)^8$. Also note that $Im(i) = (\mathbb{Z}_3)^8$ since i is an injection. Therefore, $Ker(\pi) = Im(i)$, and we can build the following exact sequence:

$$0 \to (\mathbb{Z}_3)^8 \xrightarrow{i} T \xrightarrow{\pi} Sym_8 \to 0.$$

From here, we create a splitting via the homomorphism $\sigma : Sym_8 \to T$ such that $\pi \circ \sigma = id_{Sym_8}$. On the cube, each element $x \in Sym_8$ sends each corner cubino to a distinct position but does not say how the cubino will be placed in this position. That is, x does not discern color orientation. Then σ maps an element $x \in Sym_8$ to the unique element in T which permutes the corner cubinos in the same fashion as x while preserving the orientation prescribed at each of the cubino's starting positions. This splitting generates a function $\varphi : Sym_8 \to Aut((\mathbb{Z}_3)^8)$. To get a better feel for the effects of φ, let $h \in Sym_8$ and let $k \in (\mathbb{Z}_3)^8$. Then the automorphism group $Aut((\mathbb{Z}_3)^8)$ sends each element $k \in (\mathbb{Z}_3)^8$ to some new color orientation via σ while keeping its position fixed. That is, k is mapped to $\sigma(h)k\sigma(h)^{-1} \in K$ where $\sigma(h)k\sigma(h)^{-1}$ sends each cubino to a new position by Sym_8, the numbering conventions at these new spots are applied by $(\mathbb{Z}_3)^8$, and the cubinos are then sent back to their original positions but now utilize the numbering convention of the positions they "visited." Therefore, φ maps $h \in Sym_8$ to the automorphism in $Aut((\mathbb{Z}_3)^8)$ with the aforementioned mapping, and as discussed in the previous section, φ is a homomorphism.

We now have the semidirect system $(Sym_8, \varphi, (\mathbb{Z}_3)^8)$ and, with it, the semidirect product $(\mathbb{Z}_3)^8 \rtimes Sym_8$. Thus, as proved in the previous section, $T \cong (\mathbb{Z}_3)^8 \rtimes Sym_8$. Now that we thoroughly understand the "take-apart" group in which all permutations and color orientations of the corner cubinos are possible, we can begin delving into T to find the actual corner-cubino subgroup which we will call C.

By construction, we know that $C \subseteq T$. Similarly to the "take-apart" group, to

analyze the corner-cubino subgroup C we must analyze its relationship between the permutation of the cubinos, Sym_8, and the color orientation on each of the 8 cubinos, $(\mathbb{Z}_3)^8$. First, we need to know if all permutations in Sym_8 are possible in C. As proved by Rotman [2], we know that any permutation in Sym_8 can be written as the product of two-cycles. Hence, we aim to prove that we can form a two-cycle flipping any two corner cubinos while leaving the other corners fixed.

Assume that the corner positions are labeled as follows:

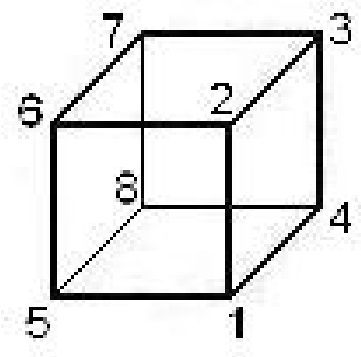

Figure 7: Numbering of the corner positions.

Assuming the faces of the Cube are labeled by the convention given in Figure 1, let ρ be the permutation that results from executing the following set of face rotations from left to right:

$$FLFL^{-1}F^2$$

As the reader can check, this permutation can be written as $\rho = (1\ 2)(6\ 8)$. Note that since ρ is the product of disjoint two-cycles, it is its own inverse; that is, $\rho = \rho^{-1}$ and $\rho \circ \rho = id$ where id is the permutation which leaves all corner cubinos fixed. We could also write the 90-degree clockwise rotation of the right face of the cube, R, as $R = (1\ 2\ 3\ 4)$. Conjugating this rotation R by ρ results in the following permutation,

which we will call κ.

$$\kappa = \rho R \rho^{-1} = \rho R \rho = (1\ 2)(6\ 8)(1\ 2\ 3\ 4)(1\ 2)(6\ 8) = (1\ 3\ 4\ 2)$$

We could also describe κ in terms of face rotations:

$$FLFL^{-1}F^2RFLFL^{-1}F^2$$

Now, if we compose the face rotation R by κ on the left and right, we find that

$$\kappa R \kappa = (1\ 3\ 4\ 2)(1\ 2\ 3\ 4)(1\ 3\ 4\ 2) = (1\ 2)(3)(4) = (1\ 2).$$

Therefore, the following set of face rotations produces a two-cycle of corner cubinos:

$$FLFL^{-1}F^2RFLFL^1F^2RFLFL^{-1}F^2RFLFL^1F^2.$$

While this may not be the simplest maneuver on the Cube, it proves that there exists a set of face rotations that produce a two-cycle of corner cubinos, leaving the other 6 corners fixed. By exhaustion, we can check that any two corners may be moved to the desired positions (corner positions 1 and 2) so that we may invoke $\kappa R \kappa$ and permute these two cubinos. Hence, the flip of any two corner cubinos is possible, and since all permutations may be written as the product of these two-cycles, all permutations in Sym_8 may be attained in C. Previously, we found that there is a surjection $\pi : T \to Sym_8$. Now, restricting the domain of this function to C, we note that $\pi/_C : C \to Sym_8$ is also a surjection since all permutations in Sym_8 are also present in C.

We now aim to study the relationship between C and $(\mathbb{Z}_3)^8$. Which cubino rotations are possible, and what restrictions are placed on rotation? Note that the splitting $\sigma : Sym_8 \to T$ was created without affecting color orientation on the cu-

binos. That is, σ puts cubinos in their standard orientation, so the entries of the octuples in $(\mathbb{Z}_3)^8$ that correpond to each permutation x sum to zero in $\mathbb{Z}_3$. Since $T \cong (\mathbb{Z}_3)^8 \rtimes Sym_8$, let $t \in T$ be defined as $t = (a, x)$ where $x \in (\mathbb{Z}_3)^8$ and $x \in Sym_8$. The isomorphism $F : (\mathbb{Z}_3)^8 \rtimes Sym_8 \to T$ maps (a, x) to $a\sigma(x)$. If the entries of the octuple a are all zeroes - that is, all corner cubinos are in their clean state color orientation - then the resulting $a\sigma(x)$ will also keep the cubinos in their original orientations.

Now assume that a is not the zero octuple. Note that the rotation of any individual face does not alter color orientation of the corner cubinos; that is, the entries in the octuples that describe these face rotations sum to zero in $\mathbb{Z}_3$. Hence, any combination of face rotations results in a permutation of facelets such the the entries in the octuple describing the resulting rotations in color orientation will sum to zero. Let $(a, x), (a', x') \in T \cong (\mathbb{Z}_3)^8 \rtimes Sym_8$. Then, by multiplication in the semidirect product, $F((a, x)(a', x')) = F(a\sigma(x)a'\sigma(x^{-1}), \sigma(x)\sigma(x^{-1}))$. On the cube, $a\sigma(x)a'\sigma(x^{-1})$ describes a situation in which a corner cubino is sent to a sent to a new position, the prescribed color orientation in this new position is applied, the cubino is sent back to its starting position, and then the color orientation of that original position is applied. That is, the color orientation of this permutation is the result of a and a', namely $a + a'$. Since a and a' both have entries which sum to zero, $a + a'$ sums to zero. This shows us that any real motion on the Cube must have a color orientation of the corner cubinos such that the entries in the describing octuple sum to zero in $\mathbb{Z}_3$.

Though we know that the rotation of the corners is restricted by the sum of zero mentioned above, we need to know if all such motions on the Cube are possible or if any other restrictions need to be made. Just as we proved that any two corner cubinos can be interchanged through motion on the Cube, the reader may prove that any four corners may be permuted to any four positions on the Cube. Using this, recall the permutation $\rho = (1\ 2)(6\ 8)$. This permutation also rotates the color orientation of

the four corners it permutes such that its corresponding element in $(\mathbb{Z}_3)^8$ is

$$(2, 2, 0, 0, 0, 1, 0, 1).$$

Since any four corners can be permuted to any other four, we could transplant these color orientations on any four corners. For example, we could generate a permutation such that its corresponding octuple is

$$(0, 1, 0, 0, 1, 0, 2, 0, 2).$$

If we add these rotations together as we did for $a + a'$ above, we find

$$(2, 2, 0, 0, 0, 1, 0, 1) + (0, 1, 0, 0, 1, 0, 2, 0, 2) = (2, 0, 0, 0, 1, 0, 0, 0).$$

Since we have previously proved that any two corners can be swapped and these two-cycles form all permutations in Sym_8, this orientation with one corner rotated 240 degrees and one corner rotated 120 degrees - again summing to zero in $\mathbb{Z}_3$ - can occur on any pair of corner cubinos. To help prove more generally that all permutations with color orientations such that the entries of the resulting octuple sum to zero are possible via motions on the Cube, let

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$$

be some element in $(\mathbb{Z}_3)^8$ such that $\sum_{i=1}^{8} a_i = 0$. This octuple describes the resulting color orientation of a motion on the Cube. We also know that we can construct the octuple $(-a_1, a_1, 0, 0, 0, 0, 0, 0)$ whose entries sum to zero. Combining these color orientations, we find

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) + (-a_1, a_1, 0, 0, 0, 0, 0, 0) = (0, a_1 + a_2, a_3, a_4, a_5, a_6, a_7, a_8).$$

Again, we know that we can construct a permutation with the color orientation octuple $(0, -a_1 - a_2, a_1 + a_2, 0, 0, 0, 0, 0)$. Combining the motion that generated the above sum with the motion that generates this octuple results in

$$\begin{aligned}(0, a_1 + a_2, a_3, a_4, a_5, a_6, a_7, a_8) + (0, -a_1 - a_2, a_1 + a_2, 0, 0, 0, 0, 0) \\ = (0, 0, a_1 + a_2 + a_3, a_4, a_5, a_6, a_7, a_8).\end{aligned}$$

We could continue this process, adding these additional motions until our octuple becomes

$$(0, 0, 0, 0, 0, 0, 0, a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8).$$

Since $\sum_{i=1}^{8} a_i = 0$, the entries of this octuple also sum to zero in $\mathbb{Z}_3$. Hence, any octuple $a \in (\mathbb{Z}_3)^8$ can be demonstrated on the Cube as long as the sum of its entries is zero.

We now know that any permutation in Sym_8 and any octuple in $(\mathbb{Z}_3)^8$ such that $\sum_{i=1}^{8} a_i = 0$ can be replicated on the corner cubinos of Rubik's Cube. However, since the elements of the corner-cubino subgroup C are ordered pairs containing an element from each of these groups, we need to know which octuples can be paired with which permutations. Let $(a, id) \in C$ where a is some octuple such that $\sum_{i=1}^{8} a_i = 0$ and id is the identity permutation in Sym_8 which fixes all corner cubinos. Every permutation $x \in Sym_8$ must be paired up with some octuple, say $a' \in (\mathbb{Z}_3)^8$, such that $\sum_{i=1}^{8} a'_i = 0$. That is, $(a', x) \in C$. Note that $a - a' \in (\mathbb{Z}_3)^8$ and $\sum_{i=1}^{8} (a - a')_i = \sum_{i=1}^{8} a_i - \sum_{i=1}^{8} a'_i = 0$. Therefore, $(a - a', id) \in C$. Then,

$$(a - a', id)(a', x) = (a - a' + id(a'), id \circ x) = (a - a' + a', x) = (a, x).$$

Therefore, any octuple a can be paired with any permutation x, and all combinations of the possible permutations and color orientations are obtainable on the Cube and, hence, in C.

With a firm understanding of the elements in C, we can now determine the order or C. Since the entries of the octuples in $(\mathbb{Z}_3)^8$ must sum to zero, once the first 7 entries have been chosen, the last entry is determined by the sum of others and, hence, has only one choice. Therefore, there are 3^7 ways of constructing these octuples. Since all permutations in Sym_8 are plausible, there are 8! permutations of the corner cubinos. Therefore, there are $3^7 8!$ elements in C. That is, there are $3^7 8! = 88,179,840$ facelet arrangements on the corner cubinos of Rubik's Cube.

Further Research

The edge-cubino subgroup which we will denote E can be described similarly to C. Ideally, the 12 edge cubinos can be permuted amongst themselves and the color orientation of the two distinct colors on each cubino can be written as elements of $\mathbb{Z}_2$. The permutation of the cubinos is given by Sym_{12}, and to describe the color orientation on all twelve cubinos simultaneously, we use elements of $(\mathbb{Z}_2)^{12}$ which are 12-entry ordered pairs with each entry being an element of $\mathbb{Z}_2$. By similar construction, we can build an exact sequence centered around the "take-apart" group for these edge cubinos, T_E as follows:

$$0 \to (\mathbb{Z}_2)^{12} \to T_E \to Sym_{12} \to 0$$

Therefore, we could construct another splitting $\sigma_E : Sym_{12} \to T_E$ and homomorphism $\varphi_E : Sym_{12} \to Aut((\mathbb{Z}_2)^{12})$ to form the semidirect product $(\mathbb{Z}_2)^{12} \rtimes Sym_{12}$. Thus, $T_E \cong (\mathbb{Z}_2)^{12} \rtimes Sym_{12}$. Again, the entries in the ordered pairs from $(\mathbb{Z}_2)^{12}$ that describe the orientations of the cubinos must sum to zero in $\mathbb{Z}_2$. From here, we deduce that there are $2^{11}12! = 980,995,276,800$ facelet arrangements on the edge cubinos of Rubik's Cube.

We may note that the center-cubino subgroup needs no examination and does not

affect the possible color arrangements of the Cube since color orientation is fixed and the centers cannot be permuted. Hence, further research should aim to fully describe the relationship between the corner- and edge-cubino subgroups, C and E. Preliminary research shows that the parity of the permutations in the two groups must line up for the move to exist on the Cube. That is, if $x \in C$ is an even permutation of corner cubinos together with some color orientation, the corresponding movement of the edge cubinos $y \in E$ must also be an even permutation paired with some color orientation. Similarly, an odd $x \in C$ must correspond to some odd $y \in E$. Though this should be formally proven, this restriction should cut the number of possible arrangements in half.

Analysis of the corner-cubino and edge-cubino subgroups, C and E, showed that the order of C is $3^7 8!$ and the order of E is $2^{11} 12!$. Hence, since the centers are insignificant to the number of facelet arrangements on the Cube, the total order of the Rubik's group, $\Re$, is the product of the orders of C and E divided by 2. Therefore, the order of $\Re$ is

$$\frac{3^7 8! * 2^{11} 12!}{2} \approx 4.32520033 * 10^{19}$$

and over 43 quintillion possible color combinations exist on Rubik's Cube.

Bibliography

[1] M. E. Larsen, *Rubik's Revenge: The Group Theoretical Solution*, The American Mathematical Monthly, 92 (1985) 381-90.

[2] J. J. Rotman, *A First Course in Abstract Algebra with Applications*, 3rd ed., Pearson Prentice Hall, Upper Saddle River, NJ, 2006.

[3] D. Singmaster, *Notes on Rubik's "Magic Cube"*, 5th ed., London, 1980.

[4] E. C. Turner and K. F. Gold, *Rubik's Groups*, The American Mathematical Monthly, 92 (1985) 617-629.

[5] M. Weinstein, *Examples of Groups*, Polygonal House, Washington, NJ, 2000.