Group Theory and the Rubik's Cube

Janet Chen

A Note to the Reader

These notes are based on a 2-week course that I taught for high school students at the Texas State Honors Summer Math Camp. All of the students in my class had taken elementary number theory at the camp, so I have assumed in these notes that readers are familiar with the integers mod n as well as the units mod n.

Because one goal of this class was a complete understanding of the Rubik's cube, I have tried to use notation that makes discussing the Rubik's cube as easy as possible. For example, I have chosen to use right group actions rather than left group actions.

Introduction

Here is some notation that will be used throughout.

$\mathbb{Z}$	the set of integers $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$
$\mathbb{N}$	the set of positive integers $1, 2, 3, \ldots$
$\mathbb{Q}$	the set of rational numbers (fractions)
$\mathbb{R}$	the set of real numbers
$\mathbb{Z}/n\mathbb{Z}$	the set of integers mod n
$(\mathbb{Z}/n\mathbb{Z})^\times$	the set of units mod n

The goal of these notes is to give an introduction to the subject of group theory, which is a branch of the mathematical area called algebra (or sometimes abstract algebra). You probably think of algebra as addition, multiplication, solving quadratic equations, and so on. Abstract algebra deals with all of this but, as the name suggests, in a much more abstract way! Rather than looking at a specific operation (like addition) on a specific set (like the set of real numbers, or the set of integers), abstract algebra is algebra done without really specifying what the operation or set is. This may be the first math you've encountered in which objects other than numbers are really studied!

A secondary goal of this class is to solve the Rubik's cube. We will both develop methods for solving the Rubik's cube and prove (using group theory!) that our methods always enable us to solve the cube.

References

Douglas Hofstadter wrote an excellent introduction to the Rubik's cube in the March 1981 issue of *Scientific American*. There are several books about the Rubik's cube; my favorite is *Inside Rubik's Cube and Beyond* by Christoph Bandelow. David Singmaster, who developed much of the usual notation for the Rubik's cube, also has a book called *Notes on Rubik's 'Magic Cube,'* which I have not seen.

For an introduction to group theory, I recommend *Abstract Algebra* by I. N. Herstein. This is a wonderful book with wonderful exercises (and if you are new to group theory, you should do lots of the exercises). If you have some familiarity with group theory and want a good reference book, I recommend *Abstract Algebra* by David S. Dummit and Richard M. Foote.

1. Functions

To understand the Rubik's cube properly, we first need to talk about some different properties of functions.

Definition 1.1. *A function or map f from a domain $\mathcal{D}$ to a range $\mathcal{R}$ (we write $f : \mathcal{D} \to \mathcal{R}$) is a rule which assigns to each element $x \in \mathcal{D}$ a unique element $y \in \mathcal{R}$. We write $f(x) = y$. We say that y is the image of x and that x is a preimage of y. Note that an element in $\mathcal{D}$ has exactly one image, but an element of $\mathcal{R}$ may have 0, 1, or more than 1 preimage.*

Example 1.2. We can define a function $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2$. If x is any real number, its image is the real number x^2. On the other hand, if y is a positive real number, it has two preimages, $\sqrt{y}$ and $-\sqrt{y}$. The real number 0 has a single preimage, 0; negative numbers have no preimages. ❖

Functions will provide important examples of groups later on; we will also use functions to "translate" information from one group to another.

Definition 1.3. *A function $f : \mathcal{D} \to \mathcal{R}$ is called one-to-one if $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$ for $x_1, x_2 \in \mathcal{D}$. That is, each element of $\mathcal{R}$ has at most one preimage.*

Example 1.4. Consider the function $f : \mathbb{Z} \to \mathbb{R}$ defined by $f(x) = x + 1$. This function is one-to-one since, if $x_1 \neq x_2$, then $x_1 + 1 \neq x_2 + 1$. If $x \in \mathbb{R}$ is an integer, then it has a single preimage (namely, $x - 1$). If $x \in \mathbb{R}$ is not an integer, then it has no preimage.

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not one-to-one, since $f(1) = f(-1)$ but $1 \neq -1$. Here, 1 has two preimages, 1 and -1. ❖

Definition 1.5. *A function $f : \mathcal{D} \to \mathcal{R}$ is called onto if, for every $y \in \mathcal{R}$, there exists $x \in \mathcal{D}$ such that $f(x) = y$. Equivalently, every element of $\mathcal{R}$ has at least one preimage.*

Example 1.6. The function $f : \mathbb{Z} \to \mathbb{R}$ defined by $f(x) = x + 1$ is not onto since non-integers do not have preimages. However, the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 1$ is onto.

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not onto because there is no $x \in \mathbb{Z}$ such that $f(x) = 2$. ❖

Exercise 1.7. *Can you find a ...*

1. *... function which is neither one-to-one nor onto?*
2. *... function which is one-to-one but not onto?*
3. *... function which is onto but not one-to-one?*
4. *... function which is both one-to-one and onto?*

Definition 1.8. *A function $f : \mathcal{D} \to \mathcal{R}$ is called a bijection if it is both one-to-one and onto. Equivalently, every element of $\mathcal{R}$ has exactly one preimage.*

Example 1.9. The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 1$ is a bijection. ❖

Example 1.10. If $\mathcal{S}$ is any set, then we can define a map $f : \mathcal{S} \to \mathcal{S}$ by $f(x) = x$ for all $x \in \mathcal{S}$. This map is called the identity map, and it is a bijection. ❖

Definition 1.11. *If $f : \mathcal{S}_1 \to \mathcal{S}_2$ and $g : \mathcal{S}_2 \to \mathcal{S}_3$, then we can define a new function $f \circ g : \mathcal{S}_1 \to \mathcal{S}_3$ by $(f \circ g)(x) = g(f(x))$. The operation $\circ$ is called composition.*

Remark 1.12. *One usually writes $(g \circ f)(x) = g(f(x))$ rather than $(f \circ g)(x) = g(f(x))$. However, as long as we are consistent, the choice does not make a big difference. We are using this convention because it matches the convention usually used for the Rubik's cube.*

Exercises

1. Which of the following functions are one-to-one? Which are onto?

   (a) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2 + 1$.
   (b) $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2 + 1$.
   (c) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 3x + 1$.
   (d) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x + 1$.

2. Suppose $f_1 : S_1 \to S_2$ and $f_2 : S_2 \to S_3$ are one-to-one. Prove that $f_1 \circ f_2$ is one-to-one.

3. Suppose $f_1 : S_1 \to S_2$ and $f_2 : S_2 \to S_3$ are onto. Prove that $f_1 \circ f_2$ is onto.

4. Let $f_1 : S_1 \to S_2$, $f_2 : S_2 \to S_3$, and $f_3 : S_3 \to S_4$. Prove that $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$.

5. Let S be a set.

   (a) Prove that there exists a function $e : S \to S$ such that $e \circ f = f$ and $f \circ e = f$ for all bijections $f : S \to S$. Prove that e is a bijection. S.

   (b) Prove that, for every bijection $f : S \to S$, there exists a bijection $g : S \to S$ such that $f \circ g = e$ and $g \circ f = e$.

6. If $f : \mathcal{D} \to \mathcal{R}$ is a bijection and $\mathcal{D}$ is a finite set with n elements, prove that $\mathcal{R}$ is also a finite set with n elements.

2. Groups

Example 2.1. To get an idea of what groups are all about, let's start by looking at two familiar sets.

First, consider the integers mod 4. Remember that $\mathbb{Z}/4\mathbb{Z}$ is a set with 4 elements: 0, 1, 2, and 3. One of the first things you learned in modular arithmetic was how to add numbers mod n. Let's write an addition table for $\mathbb{Z}/4\mathbb{Z}$.

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

Now, we're going to rewrite the addition table in a way that might seem pretty pointless; we're just going to use the symbol $*$ instead of $+$ for addition, and we'll write $e = 0$, $a = 1$, $b = 2$, and $c = 3$. Then, our addition table looks like

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Let's do the same thing for $(\mathbb{Z}/5\mathbb{Z})^\times$, the set of units mod 5. The units mod 5 are 1, 2, 3, and 4. If you add two units, you don't necessarily get another unit; for example, $1 + 4 = 0$, and 0 is not a unit. However, if you multiply two units, you always get a unit. So, we can write down a multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$. Here it is:

$\cdot$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Again, we're going to rewrite this using new symbols. Let $*$ mean multiplication, and let $e = 1$, $a = 2$, $b = 4$, and $c = 3$. Then, the multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$ looks like

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Notice that this is exactly the same as the table for addition on $\mathbb{Z}/4\mathbb{Z}$!

Why is it interesting that we get the same tables in these two different situations? Well, this enables us to translate algebraic statements about addition of elements of $\mathbb{Z}/4\mathbb{Z}$ into statements about multiplication of elements of $(\mathbb{Z}/5\mathbb{Z})^\times$. For example, the equation $x + x = 0$ in $\mathbb{Z}/4\mathbb{Z}$ has two solutions, $x = 0$ and $x = 2$. With our alternate set of symbols, this is the same as saying that the equation $x * x = e$ has solutions $x = e$ and $x = b$. If we translate this to $(\mathbb{Z}/5\mathbb{Z})^\times$, this says that the solutions of $x \cdot x = 1$ in $(\mathbb{Z}/5\mathbb{Z})^\times$ are $x = 1$ and $x = 4$. That is, 1 and 4 are the square roots of 1 in $(\mathbb{Z}/5\mathbb{Z})^\times$, which is exactly right!

In mathematical language, we say that $\mathbb{Z}/4\mathbb{Z}$ with addition and $(\mathbb{Z}/5\mathbb{Z})^\times$ with multiplication are "isomorphic groups." The word "isomorphic" means roughly that they have the same algebraic structure; we'll get into this later. For now, let's just see what a "group" is. ❖

Definition 2.2. *A group $(G, *)$ consists of a set G and an operation $*$ such that:*

1. *G is closed under $*$. That is, if $a, b \in G$, then $a * b \in G$.*

   Examples:

   - *$\mathbb{Z}/4\mathbb{Z}$ is closed under $+$; after all, we wrote down the addition table, which tells us how to add any two elements of $\mathbb{Z}/4\mathbb{Z}$ and get another element of $\mathbb{Z}/4\mathbb{Z}$. Similarly, $(\mathbb{Z}/5\mathbb{Z})^\times$ is closed under multiplication.*
   - *$\mathbb{Z}$ is closed under $+$: if $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$. Similarly, $\mathbb{Z}$ is also closed under $-$.*
   - *$\mathbb{R}$ is closed under multiplication: if we multiply two real numbers, we get a real number.*
   - *The set of negative numbers is not closed under multiplication: if we multiply two negative numbers, we get a positive number.*

2. *$*$ is associative. That is, for any $a, b, c \in G$, $a * (b * c) = (a * b) * c$.*

   Examples:

   - *Addition and multiplication are associative.*
   - *Subtraction is not associative because $a - (b - c) \neq (a - b) - c$.*

3. *There is an "identity element" $e \in G$ which satisfies $g = e * g = g * e$ for all $g \in G$.*

   Examples:

   - *For $(\mathbb{Z}/4\mathbb{Z}, +)$, 0 is an identity element because $g = 0 + g = g + 0$ for any $g \in \mathbb{Z}/4\mathbb{Z}$. For $((\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$, 1 is an identity element because $g = 1 \cdot g = g \cdot 1$ for any $g \in (\mathbb{Z}/5\mathbb{Z})^\times$.*
   - *For $(\mathbb{Z}, +)$, 0 is an identity element because $g = 0 + g = g + 0$ for any $g \in \mathbb{Z}$.*
   - *For $(\mathbb{R}, \cdot)$, 1 is an identity element because $g = 1 \cdot g = g \cdot 1$ for any $g \in \mathbb{R}$.*

4. *Inverses exist; that is, for any $g \in G$, there exists an element $h \in G$ such that $g * h = h * g = e$. (h is called an inverse of g.)*

   Examples:

   - *Using the addition table for $\mathbb{Z}/4\mathbb{Z}$, we can find inverses of all the elements of $\mathbb{Z}/4\mathbb{Z}$. For instance, we can see from the table that $1 + 3 = 3 + 1 = 0$, so 3 is the inverse of 1. Similarly, since the table for $(\mathbb{Z}/5\mathbb{Z})^\times$ is identical, all elements of $(\mathbb{Z}/5\mathbb{Z})^\times$ have inverses.*
   - *For $(\mathbb{Z}, +)$, the inverse of $n \in \mathbb{Z}$ is $-n$ because $n + (-n) = (-n) + n = 0$.*
   - *For $(\mathbb{R}, \cdot)$, not every element has an inverse — namely, 0 does not have an inverse. However, if $x \neq 0$, then $\frac{1}{x}$ is an inverse of x because $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$.*

Example 2.3.

1. $(\mathbb{Z}/4\mathbb{Z}, +)$ and $((\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$ are groups. In fact, as we said earlier, these should be thought of as the "same" group, but we won't go into this until later.
2. $(\mathbb{Z}, +)$ is a group. However, $(\mathbb{Z}, -)$ is not a group because subtraction is not associative.
3. $(\mathbb{R}, \cdot)$ is not a group since 0 does not have an inverse under multiplication. However, $(\mathbb{R} - \{0\}, \cdot)$ is a group.
4. The set of negative numbers is not closed under multiplication, so the set of negative numbers with multiplication is not a group.
5. We can construct a group $(G, *)$ where G is a set with just one element. Since G must have an identity element, we will call this single element e. To define the group operation $*$, we just need to say what $e * e$ is. There is only one choice since G has only one element: $e * e$ must be e. This defines a group which is called the trivial group. As you might guess, the trivial group isn't very interesting.
6. Soon, we will see how to make the moves of a Rubik's cube into a group!

❖

The examples of groups we have seen so far all have another special property: for every $g, h \in G$, $g * h = h * g$; that is, the $*$ operation is commutative. This is *not* true of all groups. If it is true of $(G, *)$, we say $(G, *)$ is abelian. We will soon see examples of nonabelian groups.

Now, we will prove two important properties of groups.

Lemma 2.4. *A group has exactly one identity element.*

Proof. Let $(G, *)$ be a group, and suppose e and e' are identity elements of G (we know that G has at least one identity element by the definition of a group). Then, $e * e' = e$ since e' is an identity element. On the other hand, $e * e' = e'$ since e is an identity element. Therefore, $e = e'$ because both are equal to $e * e'$. □

Lemma 2.5. *If $(G, *)$ is a group, then each $g \in G$ has exactly one inverse.*

Proof. Let $g \in G$, and suppose g_1, g_2 are inverses of G (we know there is at least one by the definition of a group); that is, $g * g_1 = g_1 * g = e$ and $g * g_2 = g_2 * g = e$. By associativity, $(g_1 * g) * g_2 = g_1 * (g * g_2)$. Since g_1 is an inverse of g, $(g_1 * g) * g_2 = e * g_2 = g_2$. Since g_2 is an inverse of g, $g_1 * (g * g_2) = g_1 * e = g_1$. Therefore, $g_2 = g_1$. □

In general, we write the unique inverse of g as g^{-1}. However, if we know that the group operation is addition, then we write the inverse of g as $-g$.

Exercises

1. Which of the following are groups? Prove your answer.
   (a) $(\{\pm 1\}, \cdot)$
   (b) $(S, +)$, where S is the set of non-negative integers $\{0, 1, 2, 3, \ldots\}$
   (c) $(2\mathbb{Z}, +)$, where $2\mathbb{Z}$ is the set of even integers
   (d) $(\mathbb{Z}, \cdot)$
   (e) $(\mathbb{Z}, ?)$ where $a?b$ is defined to be $a + b - 1$.
   (f) $(\mathbb{Q} - \{0\}, \cdot)$
   (g) $(\mathbb{R}, \bigstar)$ where $a \bigstar b$ is defined to be $(a - 1)(b - 1)$.
   (h) $(G, \circ)$ where G is the set of bijections from some set $\mathcal{S}$ to itself and $\circ$ denotes composition of functions.

2. Let $(G, *)$ be a group and $a, b, c \in G$. Prove:
   (a) If $a * b = a * c$, then $b = c$.
   (b) If $b * a = c * a$, then $b = c$.

   That is, we can cancel in groups.

3. If $(G, *)$ is a group and $g \in G$, prove that $(g^{-1})^{-1} = g$.

4. If $(G, *)$ is a group and $g, h \in G$ such that $g * h = e$, prove that $h * g = e$. (That is, if $g * h = e$, then h is the inverse of g and g is the inverse of h.)

5. If $(G, *)$ is a group and $g, h \in G$ such that $g * h = h$, prove that g is the identity element of G.

6. Let $(G, *)$ be a finite group; that is, $(G, *)$ is a group and G has finitely many elements. Let $g \in G$. Prove that there exists a positive integer n such that $g^n = e$ (here, g^n means $g * g * \cdots * g$ with n copies of g). The smallest such integer n is called the order of g.

7. Find the order of 5 in $(\mathbb{Z}/25\mathbb{Z}, +)$. Find the order of 2 in $((\mathbb{Z}/17\mathbb{Z})^\times, \cdot)$.

8. If $(G, *)$ is a group in which $g * g = e$ for all $g \in G$, show that $(G, *)$ is abelian.

9. If $(G, *)$ is a group where G has 4 elements, show that $(G, *)$ is abelian.

10. Let $(G, *)$ be a finite group. Prove that there is a positive integer n such that $g^n = e$ for all $g \in G$. (This is different from Problem 6 in that you need to show that the same n works for all $g \in G$.)

11. Let G be a set and $*$ be an operation on G such that the following four properties are satisfied:

    (a) G is closed under $*$.
    (b) $*$ is associative.
    (c) There exists $e \in G$ such that $g * e = g$ for all $g \in G$. (We call e a "right identity.")
    (d) For each $g \in G$, there exists $h \in G$ such that $g * h = e$. (We call h a "right inverse" of g.)

    Prove that $(G, *)$ is a group.

3. The Rubik's Cube and Subgroups

3.1. Cube notation

The Rubik's cube is composed of 27 small cubes, which are typically called "cubies." 26 of these cubies are visible (if you take your cube apart, you'll find that the 27th cubie doesn't actually exist). When working with the Rubik's cube, it's helpful to have a systematic way of referring to the individual cubies. Although it seems natural to use the colors of a cubie, it is actually more useful to have names which describe the locations of the cubies. The cubies in the corners are called, appropriately enough, "corner cubies." Each corner cubie has 3 visible faces, and there are 8 corner cubies. The cubies with two visible faces are called "edge" cubies; there are 12 edge cubies. Finally, the cubies with a single visible face are called "center cubies," and there are 6 center cubies.

Now, let's name the 6 faces of the Rubik's cube. Following the notation developed by David Singmaster, we will call them right (r), left (l), up (u), down (d), front (f), and back (b). The advantage of this naming scheme is that each face can be referred to by a single letter.

To name a corner cubie, we simply list its visible faces in clockwise order. For instance, the cubie in the upper, right, front corner is written urf. Of course, we could also call this cubie rfu or fur. Sometimes, we will care which face is listed first; in these times, we will talk about "oriented cubies." That is, the oriented cubies urf, rfu, and fur are different. In other situations, we won't care which face is listed first; in these cases, we will talk about "unoriented cubies." That is, the unoriented cubies urf, rfu, and fur are the same.

Similarly, to name edge and center cubies, we will just list the visible faces of the cubies. For instance, the cubie in the center of the front face is just called f, because its only visible face lies on the front of the cube.

We will also frequently talk about "cubicles." These are labeled the same way as cubies, but they describe the space in which the cubie lives. Thus, if the Rubik's cube is in the start configuration (that is, the Rubik's cube is solved), then each cubie lives in the cubicle of the same name (the urf cubie lives in the urf cubicle, the f cubie lives in the f cubicle, and so on). If you rotate a face of the Rubik's cube, the cubicles don't move, but the cubies do. Notice, however, that when you rotate a face of the Rubik's cube, all center cubies stay in their cubicles.

Finally, we want to give names to some moves of the Rubik's cube. The most basic move one can do is to rotate a single face. We will let R denote a clockwise rotation of the right face (looking at the right face, turn it 90° clockwise). Similarly, we will use the capital letters L, U, D, F, and B to denote clockwise twists of the corresponding faces. More generally, we will call any sequence of these 6 face twists a "move" of the Rubik's cube. For instance, rotating the right face counterclockwise is a move which is the same as doing R three times. Later in this lecture, we will describe a notation for these more complicated moves.

A couple of things are immediately clear. First, we already observed that the 6 basic moves keep the center cubies in their cubicles. Since any move is a sequence of these 6 basic moves, that means that every move of the Rubik's cube keeps the center cubies in their cubicles (for a formal proof, see the example after Proposition 4.9). Also, any move of the Rubik's cube puts corner cubies in corner cubicles and edge cubies in edge cubicles; it is impossible for a corner cubie to ever live in an edge cubicle or for an edge cubie to live in a corner cubicle. Using these two facts, we can start to figure out how many possible configurations the Rubik's cube has. Let's look, for instance, at the urf cubicle. Theoretically, any of the 8 corner cubies could reside in this cubicle. That leaves 7 corner cubies that could reside in the urb cubicle, 6 for the next corner cubicle, and so on. Therefore, there are $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 8!$ possible positionings of the corner cubies. Notice that a corner cubie can fit into its cubicle in 3 different ways. For instance, if a red, white, and blue cubie lies in the urf cubicle, either the red, white, or blue face could lie in the u face of the cubicle (and this determines where the other 2 faces lie). Since there are 8 corner cubies and each can lie in its cubicle in 3 different ways, there are 3^8 different ways the corner cubies could be oriented. Therefore, there are $3^8 \cdot 8!$ possible configurations of the corner cubies. Similarly, since there are 12 edge cubies, there are 12! positions of the edge cubies; each edge cubie has 2 possible orientations, giving 2^{12} possible orientations. So, there are

$2^{12} \cdot 12!$ possible configurations of the edge cubies, giving a total of $2^{12}3^8 8!12!$ possible configurations of the Rubik's cube. (This number is about 5.19×10^{20}, or 519 quintillion!)

Although these configurations are theoretically possible, that doesn't mean that these configurations could really occur. We will say that a configuration of the Rubik's cube is valid if it can be achieved by a series of moves from the starting configuration. It turns out that some of the theoretically possible configurations we have counted are actually not valid. Therefore, we have two goals:

1. Demonstrate that some configurations are not valid.
2. Find a set of moves that can take us from any valid configuration back to the start configuration.

3.2. Making the Rubik's Cube into a Group

We can make the set of moves of the Rubik's cube into a group, which we will denote $(\mathbb{G}, *)$. The elements of $\mathbb{G}$ will be all possible moves of the Rubik's cube (for example, one possible move is a clockwise turn of the top face followed by a counterclockwise turn of the right face). Two moves will be considered the same if they result in the same configuration of the cube (for instance, twisting a face clockwise by 180° is the same as twisting the same face counterclockwise by 180°). The group operation will be defined like this: if M_1 and M_2 are two moves, then $M_1 * M_2$ is the move where you first do M_1 and then do M_2.

Why is this a group? We just need to show the 4 properties in [PS 2, #11].

- $\mathbb{G}$ is certainly closed under $*$ since, if M_1 and M_2 are moves, $M_1 * M_2$ is a move as well.

- If we let e be the "empty" move (that is, a move which does not change the configuration of the Rubik's cube at all), then $M * e$ means "first do M, then do nothing." This is certainly the same as just doing M, so $M * e = M$. So, $(\mathbb{G}, *)$ has a right identity.

- If M is a move, we can reverse the steps of the move to get a move M'. Then, the move $M * M'$ means "first do M, then reverse all the steps of M." This is the same as doing nothing, so $M * M' == e$, so M' is the inverse of M. Therefore, every element of $\mathbb{G}$ has a right inverse.

- Finally, we must show that $*$ is associative. Remember that a move can be defined by the change in configuration it causes. In particular, a move is determined by the position and orientation it puts each cubie in.

  If C is an oriented cubie, we will write $M(C)$ for the oriented cubicle that C ends up in after we apply the move M, with the faces of $M(C)$ written in the same order as the faces of C. That is, the first face of C should end up in the first face of $M(C)$, and so on. For example, the move R puts the ur cubie in the br cubicle, with the u face of the cubie lying in the b face of the cubicle and the r face of the cubie lying in the r face of the cubicle. Thus, we write R(ur) = br.

  First, let's investigate what a sequence of two moves does to the cubie. If M_1 and M_2 are two moves, then $M_1 * M_2$ is the move where we first do M_1 and then do M_2. The move M_1 moves C to the cubicle $M_1(C)$; the move M_2 then moves it to $M_2(M_1(C))$. Therefore, $(M_1 * M_2)(C) = M_2(M_1(C))$.

  To show that $*$ is associative, we need to show that $(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3)$ for any moves M_1, M_2, and M_3. This is the same as showing that $(M_1 * M_2) * M_3$ and $M_1 * (M_2 * M_3)$ do the same thing to every cubie. That is, we want to show that $[(M_1 * M_2) * M_3](C) = [M_1 * (M_2 * M_3)](C)$ for any cubie C. We know from our above calculation that $[(M_1 * M_2) * M_3](C) = M_3([M_1 * M_2](C)) = M_3(M_2(M_1(C)))$. On the other hand, $[M_1 * (M_2 * M_3)](C) = (M_2 * M_3)(M_1(C)) = M_3(M_2(M_1(C)))$. So, $(M_1 * M_2) * M_3 = M_1 * (M_2 * M_3)$. Thus, $*$ is associative.

Therefore, $(\mathbb{G}, *)$ is indeed a group.

3.3. Subgroups

We calculated that there are around 519 quintillion possible configurations of the Rubik's cube (although these are not all valid). Trying to understand such a large number of configurations is no easy task! It is helpful to restrict the problem; for instance, instead of looking at all possible moves of the Rubik's cube, we might start out by looking at the moves which only involve twists of the down and right faces.

This is a general philosophy in group theory: to understand a group G, we should try to understand small pieces of it.

Definition 3.1. *A nonempty subset H of a group $(G, *)$ is called a subgroup of G if $(H, *)$ is a group.*

The advantage of studying subgroups is that they may be much smaller and, hence, simpler; however, they still have algebraic structure.

Example 3.2. A group is always a subgroup of itself. Also, the trivial group is a subgroup of any group. However, these subgroups aren't too interesting! ❖

Example 3.3. The set of even integers is a subgroup of $(\mathbb{Z}, +)$: after all, the even integers are certainly a subset of $\mathbb{Z}$, and we know from [PS 2, #1c] that $(2\mathbb{Z}, +)$ is a group. ❖

The following lemma often makes it easier to check if a subset is actually a subgroup.

Lemma 3.4. *Let $(G, *)$ be a group. A nonempty subset H of G is a subgroup of $(G, *)$ iff, for every $a, b \in H$, $a * b^{-1} \in H$.*

Proof. First, suppose H is a subgroup. If $b \in H$, then $b^{-1} \in H$ since $(H, *)$ is a group. So, if $a \in H$ as well, then $a * b^{-1} \in H$.

Conversely, suppose that, for every $a, b \in H$, $a * b^{-1} \in H$.

- First, notice that $*$ is associative since $(G, *)$ is a group.
- Let $a \in H$. Then, $e = a * a^{-1}$, so $e \in H$.
- Let $b \in H$, Then $b^{-1} = e * b^{-1} \in H$, so inverses exist in H.
- Let $a, b \in H$. By the previous step, $b^{-1} \in H$, so $a * (b^{-1})^{-1} = a * b \in H$. Thus, H is closed under $*$.

Therefore, $(H, *)$ is a group, which means that H is a subgroup of G. □

3.4. Simplifying Group Notation

It is common practice to write group operations as multiplication; that is, we write gh rather than $g * h$, and we call this the "product" of g and h. The statement "let G be a group" really means that G is a group under some operation which will be written as multiplication. We will also often write the identity element of G as 1 rather than e. Finally, we will use standard exponential notation, so g^2 means gg, g^3 means ggg, and so on.

In particular, we will do this with $(\mathbb{G}, *)$. That is, from now on, we will just call this group $\mathbb{G}$, and we will write the operation as multiplication. For instance, DR means the move D followed by the move R. The move which twists the right face counterclockwise by 90° is the same as a move twisting the right face clockwise three times, so we can write this move as R^3.

Exercises

1. If G is a group and $g, h \in G$, write $(gh)^{-1}$ in terms of g^{-1} and h^{-1}.

2. If A, B are subgroups of a group G, prove that $A \cap B$ is a subgroup of G.

3. Let G be a group and $Z(G) = \{z \in G : zx = xz \text{ for all } x \in G\}$. (This notation means that $Z(G)$ is the set of $z \in G$ such that $zx = xz$ for all $x \in G$.) Prove that $Z(G)$ is a subgroup of G. $Z(G)$ is called the center of G. If G is abelian, what is $Z(G)$?

4. Remember that $\mathbb{G}$ is the group of moves of the Rubik's cube. Prove that this group is not abelian. (Hint: pick two moves M_1 and M_2 and look at their commutator $[M_1, M_2]$, which is defined to be $M_1 M_2 M_1^{-1} M_2^{-1}$.)

5. Let C_1 and C_2 be two different unoriented corner cubies, and let C_1' and C_2' be two different unoriented corner cubicles. Prove that there is a move of the Rubik's cube which sends C_1 to C_1' and C_2 to C_2'. Since we are talking about unoriented cubies and cubicles, we only care about the positions of the cubies, not their orientations. (For example, if $C_1 = \mathsf{dbr}$, $C_2 = \mathsf{urf}$, $C_1' = \mathsf{dlb}$, and $C_2' = \mathsf{urf}$, then the move D sends C_1 to C_1' and C_2 to C_2'.)

6. Let G be a group and S be a subset of G. Let H be the set of all elements of G which can be written as a finite product of elements of S and their inverses; that is, H consists of all elements of the form $s_1 \cdots s_n$ where each s_i is either an element of S or the inverse of an element of S. Prove that H is a subgroup of G. We call H the subgroup of G generated by S and write $H = \langle S \rangle$. It is the smallest subgroup of G containing S (do you see why?).

7. If G is an abelian group, show that $\{a^2 : a \in G\}$ is a subgroup of G. Which part of your proof fails when G is not abelian?

8. Find all subgroups of $(\mathbb{Z}, +)$.

9. Let $(G, *)$ be a group and H be a nonempty finite subset of G closed under $*$. Prove that H is a subgroup of G. Is the statement still true if H is not required to be finite?

10. Try scrambling your Rubik's cube. How many cubies can you put in the right position? The right orientation?

11. Brainstorm a bit about what kind of strategy you should use to solve the Rubik's cube. Which cubies should you try to solve first? What kind of moves should you look for?

4. Generators

Let G be a group and S be a subset of G. In [PS 3, #6], we defined the subgroup $\langle S \rangle$. Now, we will give some properties of $\langle S \rangle$. First, let's look at the special case when $\langle S \rangle$ is just G.

Definition 4.1. *Let G be a group and S be a subset of G. We say that S generates G or that S is a set of generators of G if $G = \langle S \rangle$; that is, every element of G can be written as a finite product (under the group operation) of elements of S and their inverses.*

Example 4.2. Every element of $\mathbb{Z}$ can be written as a finite sum of 1's or -1's, so $\mathbb{Z}$ is generated by $\{1\}$. That is, $\mathbb{Z} = \langle 1 \rangle$. For the same reason, $\mathbb{Z} = \langle -1 \rangle$. Of course, it's also true that $\mathbb{Z} = \langle 1, 2 \rangle$. In general, there are many possible sets of generators of a group. ❖

Example 4.3. Every element of $\mathbb{Z}/4\mathbb{Z}$ can be written as a finite sum of 1's, so $\mathbb{Z}/4\mathbb{Z} = \langle 1 \rangle$.

Even though $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z}/4\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ are not equal! $\langle S \rangle$ only makes sense in the context of a given group. ❖

Example 4.4. Every element of $\mathbb{G}$ can be written as a finite sequence of turns of the Rubik's cube, so $\mathbb{G} = \langle \mathsf{D}, \mathsf{U}, \mathsf{L}, \mathsf{R}, \mathsf{F}, \mathsf{B} \rangle$. ❖

You might think of generators as being the "core" of the group; since every element of the group can be written in terms of the generators, knowledge about the generators can often be translated into knowledge about the whole group. We will make this more precise soon.

Definition 4.5. *A group G is cyclic if there exists $g \in G$ such that $G = \langle g \rangle$.*

Example 4.6. $\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ are cyclic. ❖

For finite groups, we can even relax the definition of generators slightly by leaving out the inverses of S. To prove this, we need a lemma.

Lemma 4.7. *Let G be a finite group and $g \in G$. Then, $g^{-1} = g^n$ for some $n \in \mathbb{N}$.*

Proof. If $g = e$, then there is nothing to show. So, suppose $g \neq e$. By [PS 2, #6], there exists a positive integer m such that $g^m = e$. Since $g \neq e$, $m \neq 1$, so $m > 1$. Let $n = m - 1 \in \mathbb{N}$. Then, $gg^n = g^m = e$, so g^n is the inverse of g by [PS 2, #4]. □

Lemma 4.8. *Let G be a finite group and S be a subset of G. Then, $G = \langle S \rangle$ iff every element of G can be written as a finite product of elements of S. (That is, the inverses of S are not necessary.)*

Proof. If every element of G can be written as a finite product of elements of S, then it is clear that $G = \langle S \rangle$.

Conversely, suppose $G = \langle S \rangle$. This means that every element of G can be written as a finite product $s_1 \cdots s_n$ where each s_i is either in S or the inverse of an element of S. The basic point of the proof is that the inverse of an element of S can also be written as a product of elements of S by the previous lemma. To make this completely rigorous, we will use induction on n.

Suppose $n = 1$. Either $s_1 \in S$ or $s_1^{-1} \in S$. If $s_1 \in S$, then s_1 is written as a product of a single element of S. If $s_1^{-1} \in S$, then s_1 can be written as a finite product of elements of S by Lemma 4.7. So, the base case is true.

Now, suppose the statement is true for all natural numbers smaller than n; we want to show that $s_1 \cdots s_n$ can be written as a finite product of elements of S. By the induction hypothesis, $s_1 \ldots, s_{n-1}$ and s_n can both be written as finite products of elements of S. Therefore, their product $s_1 \cdots s_n$ certainly can as well. □

Now, we will see how to translate properties of generators to the whole group.

Proposition 4.9. *Let G be a finite group and S be a subset of G. Suppose the following two conditions are satisfied.*

1. *Every element of S satisfies some property P.*
2. *If $g \in G$ and $h \in G$ both satisfy the property P, then gh satisfies the property P as well.*

Then, every element of $\langle S \rangle$ satisfies P.

Before we prove this, let's see how it might be used.

Example 4.10. Let $S = \{\mathsf{D}, \mathsf{U}, \mathsf{L}, \mathsf{R}, \mathsf{F}, \mathsf{B}\} \subset \mathbb{G}$. Then, every $M \in S$ satisfies the property "M keeps all center cubies in their cubicles." If $M_1, M_2 \in \mathbb{G}$ are such that they keep all center cubies in their cubicles, then $M_1 M_2$ certainly keeps all center cubies in their cubicles. Since $\mathbb{G} = \langle S \rangle$, the proposition says that every element of $\mathbb{G}$ keeps the center cubies in their cubicles.

This proposition is extremely useful for the Rubik's cube because it means we frequently only need to understand properties of the 6 basic moves rather than all 5×10^{20} possible moves. ❖

Now, let's prove Proposition 4.9.

Proof. By Lemma 4.8, any element of $\langle S \rangle$ can be written as $s_1 \cdots s_n$ where $n \in \mathbb{N}$ and each s_i is an element of S. We will prove the proposition by induction on n.

If $n = 1$, then $s_1 \in S$ satisfies property P by hypothesis.

Suppose inductively that $s_1 \cdots s_{n-1}$ satisfies property P. Then, the product $(s_1 \cdots s_{n-1})s_n$ is a product of two elements satisfying property P, so it satisfies property P as well. □

Exercises

1. If H is a subgroup of a group G, prove that $\langle H \rangle = H$.
2. If A is a subset of B, prove that $\langle A \rangle$ is a subgroup of $\langle B \rangle$. Is the converse true?
3. Let G be a nontrivial group (remember that the trivial group is the group with only one element, so a nontrivial group is a group with at least 2 elements). Suppose that the only subgroups of G are G and $\{1\}$. Prove that G is cyclic and finite, and prove that the number of elements in G is a prime number.
4. Prove that any subgroup of a cyclic group is cyclic.
5. Remember that $\mathbb{G}$ is the group of moves of the Rubik's cube, $\mathsf{D} \in \mathbb{G}$ is a clockwise twist of the down face, and $\mathsf{R} \in \mathbb{G}$ is a clockwise twist of the right face. Find the order of D, R, and DR (remember, DR is the move where you first do D, then R; for the definition of order, see [PS 2, #6]).
6. A group G is finitely generated if there exists a finite subset S of G such that $G = \langle S \rangle$.
   (a) Prove that every finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic.
   (b) Prove that $(\mathbb{Q}, +)$ is not finitely generated.

5. The Symmetric Group

When we found the number of possible configurations of the Rubik's cube, we used the fact that any move sends corner cubies to corner cubicles to deduce that there are 8! possible ways to position the corner cubies. In this section, we will lay down the mathematical foundation needed to understand these possibilities.

Rather than just looking at configurations of 8 cubies, we'll look at configurations of any n objects. We'll call these objects $1, 2, \ldots, n$, although these names are arbitrary. We can think of arranging these objects as putting them into n slots. If we number the slots $1, 2, \ldots, n$, then we can define a function $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ by letting $\sigma(i)$ be the number put into slot i.

Example 5.1. We can put the objects 1, 2, 3 in the order 3 1 2. Here, 3 is in the first slot, 1 is in the second slot, and 2 is in the third slot. So, this ordering corresponds to the function $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ defined by $\sigma(1) = 3$, $\sigma(2) = 1$, and $\sigma(3) = 2$. ❖

What can we say about σ?

Lemma 5.2. *σ is a bijection.*

Proof. Suppose $x \neq y$. Since a number cannot be in more than one slot, if $x \neq y$, slots x and y must contain different numbers. That is, $\sigma(x) \neq \sigma(y)$. Therefore, σ is one-to-one.

Any number $y \in \{1, 2, \ldots, n\}$ must lie in some slot, say slot x. Then, $\sigma(x) = y$. So, σ is onto. □

On the other hand, if $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is a bijection, then σ defines an arrangement of the n objects: just put object $\sigma(i)$ in slot i. So, the set of possible arrangements is really the same as the set of bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$. Therefore, instead of studying possible arrangements, we can study these bijections.

Definition 5.3. *The symmetric group on n letters is the set of bijections from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$, with the operation of composition. We write this group as S_n.*

Note that S_n is a group by [PS 2, #1h].

Let's do an example to make sure that the group operation is clear.

Example 5.4. Let $\sigma, \tau \in S_3$ be defined by $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$, $\tau(1) = 1$, $\tau(2) = 3$, and $\tau(3) = 2$. Then, $(\sigma\tau)(1) = \tau(3) = 2$, $(\sigma\tau)(2) = \tau(1) = 1$, and $(\sigma\tau)(3) = \tau(2) = 3$. ❖

5.1. Disjoint Cycle Decomposition

There is a more compact way of writing elements of the symmetric group; this is best explained by an example.

Example 5.5. Consider $\sigma \in S_{12}$ defined by

$$\begin{array}{cccccc} \sigma(1) = 12 & \sigma(2) = 4 & \sigma(3) = 5 & \sigma(4) = 2 & \sigma(5) = 6 & \sigma(6) = 9 \\ \sigma(7) = 7 & \sigma(8) = 3 & \sigma(9) = 10 & \sigma(10) = 1 & \sigma(11) = 11 & \sigma(12) = 8 \end{array}$$

We will write "$i \mapsto j$" ("i maps to j") to mean $\sigma(i) = j$. Then,

$$\begin{array}{l} 1 \mapsto 12,\ 12 \mapsto 8,\ 8 \mapsto 3,\ 3 \mapsto 5,\ 5 \mapsto 6,\ 6 \mapsto 9,\ 9 \mapsto 10,\ 10 \mapsto 1 \\ 2 \mapsto 4,\ 4 \mapsto 2 \\ 7 \mapsto 7 \\ 11 \mapsto 11 \end{array}$$

This data tells us what σ does to each number, so it defines σ. As shorthand, we write

$$\sigma = (1\ 12\ 8\ 3\ 5\ 6\ 9\ 10)\ (2\ 4)\ (7)\ (11).$$

Here, (1 12 8 3 5 6 9 10), (2 4), (7), and (10) are called cycles. When writing the disjoint cycle decomposition, we leave out the cycles with just one number, so the disjoint cycle decomposition of σ is $\sigma = (1\ 12\ 8\ 3\ 5\ 6\ 9\ 10)\ (2\ 4)$. ❖

Now, let's actually define what a cycle is.

Definition 5.6. *The cycle $(i_1\ i_2\ \cdots\ i_k)$ is the element $\tau \in S_n$ defined by $\tau(i_1) = i_2, \tau(i_2) = i_3, \ldots, \tau(i_{k-1}) = i_k, \tau(i_k) = i_1$ and $\tau(j) = j$ if $j \neq i_r$ for any r. The length of this cycle is k, and the support of the cycle is the set $\{i_1, \ldots, i_k\}$ of numbers which appear in the cycle. The support is denoted by $\operatorname{supp}\tau$. A cycle of length k is also called a k-cycle.*

Definition 5.7. *Two cycles σ and τ are disjoint if they have no numbers in common; that is,* $\operatorname{supp}\sigma \cap \operatorname{supp}\tau = \varnothing$.

Lemma 5.8. *Let $\sigma, \tau \in S_n$ be cycles. If σ and τ are disjoint, then $\sigma\tau = \tau\sigma$.*

Proof. Let $i \in \{1, \ldots, n\}$. Since $\operatorname{supp}\sigma \cap \operatorname{supp}\tau = \varnothing$, there are only two possibilities:

- $i \notin \operatorname{supp}\sigma$ and $i \notin \operatorname{supp}\tau$. In this case, $\sigma(i) = i$ and $\tau(i) = i$, so $(\sigma \circ \tau)(i) = \tau(i) = i$ and $(\tau \circ \sigma)(i) = \sigma(i) = i$.
- Otherwise, i is in the support of exactly one of σ and τ. We may suppose without loss of generality that $i \notin \operatorname{supp}\sigma$ and $i \in \operatorname{supp}\tau$. Then, $\sigma(i) = i$, so $(\sigma \circ \tau)(i) = \tau(i)$. On the other hand, $(\tau \circ \sigma)(i) = \sigma(\tau(i))$. Now, since $\tau(i) \in \operatorname{supp}\tau$ and $\operatorname{supp}\tau \cap \operatorname{supp}\sigma = \varnothing$, $\tau(i) \notin \operatorname{supp}\sigma$. Therefore, $\sigma(\tau(i)) = \tau(i)$. So, we again have $(\sigma\tau)(i) = (\tau\sigma)(i)$.

Therefore, $(\sigma\tau)(i) = (\tau\sigma)(i) = i$ for all i, which shows that $\sigma\tau = \tau\sigma$. □

Any $\sigma \in S_n$ can be written as a product (under the group operation, which is composition) of disjoint cycles. This product is called the disjoint cycle decomposition of σ. In our example, we gave a method for finding the disjoint cycle decomposition of a permutation.

We write the identity permutation as 1.

Example 5.9. S_2 consists of two permutations, 1 and (1 2). ❖

Example 5.10. Let $\sigma, \tau \in S_6$ be defined by

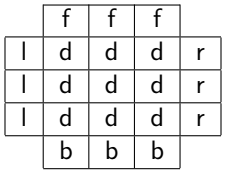
$$\begin{array}{llllll} \sigma(1) = 3 & \sigma(2) = 5 & \sigma(3) = 4 & \sigma(4) = 1 & \sigma(5) = 2 & \sigma(6) = 6 \\ \tau(1) = 5 & \tau(2) = 4 & \tau(3) = 3 & \tau(4) = 2 & \tau(5) = 1 & \tau(6) = 6 \end{array}$$

In cycle notation, $\sigma = (1\ 3\ 4)(2\ 5)$ and $\tau = (1\ 5)(2\ 4)$. Then, $\sigma\tau = (1\ 3\ 2)\ (4\ 5)$ and $\tau\sigma = (1\ 2)(3\ 4\ 5)$. We can also easily compute $\sigma^2 = (1\ 4\ 3)$ and $\tau^2 = 1$. ❖

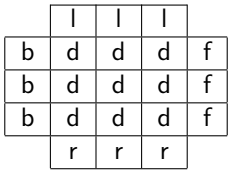
Definition 5.11. *If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, \ldots, n_r$ (including its 1-cycles), then the integers $n_1, \ldots, n_r$ are called the cycle type of σ.*

5.2. Rubik's Cube

We can write each move of the Rubik's cube using a slightly modified cycle notation. We want to describe what happens to each oriented cubie; that is, we want to describe where each cubie moves *and* where each face of the cubie moves. For example, if we unfold the cube and draw the down face, it looks like



If we rotate this face clockwise by 90° (that is, we apply the move D), then the down face looks like



So, D(dlf) = dfr because the dlf cubie now lives in the dfr cubicle (with the d face of the cubie lying in the d face of the cubicle, the l face of the cubie lying in the f face of the cubicle, and the f face of the cubie lying in the r face of the cubicle). Similarly, D(dfr) = drb, D(drb) = dbl, and D(dbl) = dlf. If we do the same thing for the edge cubies, we find D = (dlf dfr drb dbl)(df dr db dl).

Example 5.12. Check that the disjoint cycle decomposition of R is (rfu rub rbd rdf)(ru rb rd rf). ❖

Exercises

1. Let $\sigma, \tau \in S_5$ be defined as follows.

$$\begin{array}{lllll} \sigma(1)=3 & \sigma(2)=4 & \sigma(3)=5 & \sigma(4)=2 & \sigma(5)=1 \\ \tau(1)=5 & \tau(2)=3 & \tau(3)=2 & \tau(4)=4 & \tau(5)=1 \end{array}$$

   Find the cycle decompositions of each of the following permutations: σ, τ, σ^2, and $\tau^2\sigma$.

2. Let $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$. Find σ^2 and σ^3. What is the order of σ?

3. Suppose σ is a permutation with cycle type $n_1, \ldots, n_r$. What is the order of σ?

4. Let $\sigma = (1\ 2)$ and $\tau = (2\ 3)$. Find $\sigma\tau$ and $\tau\sigma$.

   (a) What is the order of $(1\ 2)(2\ 3)$? Does this agree with your answer to [PS 5, #3]?
   (b) For what n is S_n abelian?

5. Write all the elements of S_3, the symmetric group on 3 elements, using disjoint cycle notation.

6. Find all subgroups of S_3.

7. Remember that D, U, L, R, F, and B are defined to be clockwise twists of the down, up, left, right, front, and back faces, respectively. We showed in class that D has disjoint cycle decomposition (dlf dfr drb dbl)(df dr db dl) and that R has disjoint cycle decomposition (rfu rub rbd rdf)(ru rb rd rf). Write U, L, F, and B as products of disjoint cycles.

8. Let $a_1, \ldots, a_m$ be distinct elements of $\{1, \ldots, n\}$, and let $\sigma = (a_1\ a_2)(a_1\ a_3)(a_1\ a_4)\cdots(a_1\ a_m)$. Find the disjoint cycle decomposition of σ.

9. Show that S_n is generated by the set of 2-cycles in S_n.

10. Let $\tau \in S_n$, and let $a_1, \ldots, a_k)$ be distinct elements of $\{1, \ldots, n\}$. Prove that $\tau^{-1}(a_1\ a_2\ \cdots\ a_k)\tau = (\tau(a_1)\ \tau(a_2)\ \cdots\tau(a_k))$.

11. Let $\sigma, \sigma' \in S_6$ be defined by

$$\begin{aligned} \sigma &= (1\ 3\ 2)(4\ 6) \\ \sigma' &= (2\ 5\ 4)(1\ 6) \end{aligned}$$

Find $\tau \in S_6$ such that $\sigma' = \tau^{-1}\sigma\tau$.

12. Let $\sigma, \sigma' \in S_n$. Prove that σ and σ' have the same cycle type iff $\sigma' = \tau^{-1}\sigma\tau$ for some $\tau \in S_n$.

Note: Any element of the form $\tau^{-1}\sigma\tau$ is called a conjugate of σ, so this says that the conjugates of σ are exactly the elements of S_n with the same cycle type as σ.

13. Let H be the subgroup of $\mathbb{G}$ generated by D^2 and R^2; that is, $H = \langle \mathsf{D}^2, \mathsf{R}^2 \rangle$. How many elements does H have? Which of these elements might be helpful for solving the Rubik's cube?

14. Let $\sigma, \tau \in S_n$. Suppose $\operatorname{supp}\sigma \cap \operatorname{supp}\tau = \{x\}$; that is, x is the only number in $\{1, \ldots, n\}$ which appears in the cycle decomposition of both σ and τ. We define the commutator of σ and τ to be $\sigma\tau\sigma^{-1}\tau^{-1}$, and we write this as $[\sigma, \tau]$. Show that $\operatorname{supp}[\sigma, \tau]$ has at most 3 elements.

6. Configurations of the Rubik's Cube

As we said already, a configuration of the Rubik's cube is determined by four pieces of data:

- the positions of the corner cubies
- the positions of the edge cubies
- the orientations of the corner cubies
- the orientations of the edge cubies

The first can be described by an element σ of S_8 (i.e., the element of S_8 which moves the corner cubies from their start positions to the new positions). The second can be described by an element τ of S_{12}. Now, we will see how to understand the third and fourth. The basic idea is to fix a "starting orientation" and a systematic way of writing down how a given orientation differs from this starting orientation. Ths is mostly just a matter of notation.

We'll start with the corner cubies. Each corner cubie has 3 possible orientations, and we will number these orientations 0, 1, and 2. Let's explain what these numbers mean. Imagine that your Rubik's cube is in the start configuration. We are going to write a number on one face of each corner cubicle, as follows. Write:

1 on the u face of the ufl cubicle
2 on the u face of the urf cubicle
3 on the u face of the ubr cubicle
4 on the u face of the ulb cubicle
5 on the d face of the dbl cubicle
6 on the d face of the dlf cubicle
7 on the d face of the dfr cubicle
8 on the d face of the drb cubicle

So, each corner cubicle now has exactly one numbered face. Each corner cubie thus has one face lying in a numbered cubicle face. Label this cubie face 0. Going around the cubie clockwise, label the next face 1, and then label the final face 2.

Example 6.1. If we look straight at the down face and unfold the cube, the cubie faces look like this.

	f	f	f	
l	d	d	d	r
l	d	d	d	r
l	d	d	d	r
	b	b	b	

So, the cubicle numberings that we can see look like this:

	6		7	
	5		8	

Therefore, the cubie labels look like

	2		1	
1	0		0	2
2	0		0	1
	1		2	

❖

Now, each face of each corner cubie has a number on it. If the Rubik's cube is in any configuration, we will describe the orientations of the corner cubies like this: for any i between 1 and 8, find the cubicle face labeled i; let x_i be the number of the cubie face living in this cubicle face. We write x for the ordered 8-tuple $(x_1, \ldots, x_8)$. Notice that we can think of each x_i as counting the number of clockwise twists the cubie i is away from having its 0 face in the numbered face of the cubicle. But a cubie that is 3 twists away is oriented the same way as a cubie that is 0 twists away. Thus, we should think of the x_i as being elements of $\mathbb{Z}/3\mathbb{Z}$. So, x is an 8-tuple of elements of $\mathbb{Z}/3\mathbb{Z}$; we write $x \in (\mathbb{Z}/3\mathbb{Z})^8$.

Example 6.2. If the Rubik's cube is in the start configuration, each x_i is 0. We also write $x = 0$ to mean that each x_i is 0. ❖

Example 6.3. Let's see what the x_i are after we apply the move R to a cube in the start configuration. In the start configuration, the right hand face looks like this:

	u	u	u	
f	r	r	r	b
f	r	r	r	b
f	r	r	r	b
	d	d	d	

The cubicle numbers on this face are

	2		3	
	7		8	

Therefore, the labeling of the corner cubies looks like this:

	0		0	
2	1		2	1
1	2		1	2
	0		0	

If we rotate the right face of the cube by 90°, then the cubie faces look like

	1		2	
0	2		1	0
0	1		2	0
	2		1	

The cubies on the left face are unaffected by R, so $x_1 = 0$, $x_4 = 0$, $x_5 = 0$, and $x_6 = 0$. Now, we can see from our diagrams that $x_2 = 1$, $x_3 = 2$, $x_7 = 2$, and $x_8 = 1$. So, $x = (0, 1, 2, 0, 0, 0, 2, 1)$. ❖

We can do the same thing for the edge cubies. First, we label the edge cubicles as follows. Write:

1 on the u face of the ub cubicle
2 on the u face of the ur cubicle
3 on the u face of the uf cubicle
4 on the u face of the ul cubicle
5 on the b face of the lb cubicle
6 on the b face of the rb cubicle
7 on the f face of the rf cubicle
8 on the f face of the lf cubicle
9 on the d face of the db cubicle
10 on the d face of the dr cubicle
11 on the d face of the df cubicle
12 on the d face of the dl cubicle

Each edge cubie now has a face lying in a numbered cubicle face; label this cubie face 0, and label the other face of the cubie 1. Then, let y_i be the number of the cubie face in the cubicle face numbered i. This defines $y \in (\mathbb{Z}/2\mathbb{Z})^{12}$.

Thus, any configuration of the Rubik's cube can be described by $\sigma \in S_8$, $\tau \in S_{12}$, $x \in (\mathbb{Z}/3\mathbb{Z})^8$, and $y \in (\mathbb{Z}/2\mathbb{Z})^{12}$. So, we will write configurations of the Rubik's cube as ordered 4-tuples (σ, τ, x, y).

Example 6.4. The start configuration is (1, 1, 0, 0). ❖

Example 6.5. Pretend that your cube is in the start configuration. Let (σ, τ, x, y) be the configuration of the cube after we do the move [D, R], which is defined to be $\mathsf{DRD}^{-1}\mathsf{R}^{-1}$. We will write down σ, τ, x, and y.

We showed in class that D = (dlf dfr drb dbl)(df dr db dl) and R = (rfu rub rbd rdf)(ru rb rd rf). Therefore, D^{-1} = (dbl drb dfr dlf)(dl db dr df) and R^{-1} = (rdf rbd rub rfu)(rf rd rb ru). So,

$$[\mathsf{D}, \mathsf{R}] = (\mathsf{dlf\ dfr\ lfd\ frd\ fdl\ rdf})(\mathsf{drb\ bru\ bdr\ ubr\ rbd\ rub})(\mathsf{df\ dr\ br}) \tag{6.1}$$

(When writing this down, be very careful with the orientations.)

Remember that τ is an element of S_{12}; we think of it as a bijection from the set of 12 unoriented edge cubies to the set of 12 edge cubicles. It is defined like this: if C is an unoriented edge cubie in the start configuration, then $\tau(C)$ is the unoriented edge cubicle where C is living in the current configuration. Like any element of S_{12}, τ can be written in disjoint cycle notation.

In this particular example, [D, R] moves cubie df to cubicle dr, cubie dr to cubicle br, and cubie br to cubicle df. Therefore, τ = (df dr br).

Similarly, we think of σ as a bijection from the set of 8 unoriented corner cubies to the set of 8 unoriented corner cubicles. To find σ, we must figure out what [D, R] does to the *positions* of the corner cubies. Observe that [D, R] switches the positions of the cubies dfl and dfr, and it also switches the positions of drb and bru. Therefore, σ = (drb bru)(dfl dfr).

Recall that we defined x as follows. When the cube was in the start configuration, we numbered 8 cubicle faces like this:

1 on the u face of the ufl cubicle
2 on the u face of the urf cubicle
3 on the u face of the ubr cubicle
4 on the u face of the ulb cubicle
5 on the d face of the dbl cubicle
6 on the d face of the dlf cubicle
7 on the d face of the dfr cubicle
8 on the d face of the drb cubicle

We numbered each of the corresponding cubie faces 0. Starting from 0 on a corner cubie, we went clockwise

and labeled the other two faces 1 and 2. (For example, the u face of the ufl cubie is labeled 0, so the f face is 1 and the l face is 2.) Now that the cube is no longer in the start configuration, we define x_i to be the cubie face number in cubicle face i.

In the start position, all of the numbered cubicle faces have cubie faces numbered 0. Since the move $[\mathsf{D}, \mathsf{R}]$ does not affect cubies ufl, urf, ulb, or dbl, x_1, x_2, x_4, and x_5 must be 0. To find x_3, we want to see which cubie face is in the u face of the ubr cubicle. We can see from (6.1) that $[\mathsf{D}, \mathsf{R}]$ puts the b face of the drb cubie there; by our numbering scheme, the b face of the drb cubie is numbered 2; therefore, $x_3 = 2$. Similarly, $x_6 = 2$, $x_7 = 0$, and $x_8 = 2$. Therefore, the ordered 8-tuple x is $(0, 0, 2, 0, 0, 2, 0, 2)$.

Similarly, to define y, we first numbered 12 edge cubicle faces (when the cube was in the start configuration):

1 on the u face of the ub cubicle
2 on the u face of the ur cubicle
3 on the u face of the uf cubicle
4 on the u face of the ul cubicle
5 on the b face of the lb cubicle
6 on the b face of the rb cubicle
7 on the f face of the rf cubicle
8 on the f face of the lf cubicle
9 on the d face of the db cubicle
10 on the d face of the dr cubicle
11 on the d face of the df cubicle
12 on the d face of the dl cubicle

Then, we labeled the corresponding cubie faces 0 and the other edge cubie faces 1. Finally, we defined y to be the 12-tuple $(y_1, \ldots, y_{12})$ where y_i is the number in edge cubicle face i.

Since $[\mathsf{D}, \mathsf{R}]$ only affects the edge cubies df, dr, and br, we know right away that y_{11}, y_{10}, and y_6 are the only y_i that may be nonzero. Since $[\mathsf{D}, \mathsf{R}]$ puts the b face of the br cubicle in the d face of the df cubicle, $y_{11} = 0$. Similarly, y_{10} and y_6 are both 0. So, $y = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.

You might wonder why we bother to define configurations of the Rubik's cube this way, since it seems much easier to get the information directly from (6.1). The main reason is that writing σ, τ, x, and y separately allows us to recognize patterns more easily (and prove them!). ❖

Exercises

1. Suppose your Rubik's cube is in the configuration (σ, τ, x, y). If you apply the move D to the cube, it ends up in a new configuration (σ', τ', x', y'). Write x' and y' in terms of x and y. Do the same for the moves U, L, R, F, and B. Do you notice any patterns?

2. Write the commutator $[\mathsf{D}, \mathsf{R}]$ in disjoint cycle notation (be careful to keep track of the orientations of the cubies). What is the order of $[\mathsf{D}, \mathsf{R}]$? Can you find ...

   (a) ... a move which fixes the positions (but not necessarily orientations) of the back corner cubies and one front corner cubie?

   (b) ... a move which leaves 6 corner cubies fixed and switches the other 2?

   Try using these moves to put all the corner cubies in the right positions (but not necessarily orientations). What other useful moves can you get from $[\mathsf{D}, \mathsf{R}]$?

3. (a) In the subgroup $\langle \mathsf{D}, \mathsf{R} \rangle$ of $\mathbb{G}$, find a move which changes the orientations (but not positions) of two corner cubies without affecting any other corner cubies. Your move may do anything to edge

cubies. (Hint: compute a few elements of $\langle \mathsf{D}, \mathsf{R} \rangle$ and think about which powers of these elements are simplest. Then try to put some of these simple things together.)

(b) Find a move which changes the orientations of the cubies dbr and ufl but does not affect any other corner cubies.

7. Group Homomorphisms

In Example 2.1, we said that $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/5\mathbb{Z})^\times$ should be thought of as the same group. After all, they both have 4 elements, and addition in $\mathbb{Z}/4\mathbb{Z}$ behaves exactly the same way as multiplication in $(\mathbb{Z}/5\mathbb{Z})^\times$. In order to understand this, we really need a way to translate behavior from one group to another.

Let's take another look at Example 2.1. We observed in that example that the addition table for $\mathbb{Z}/4\mathbb{Z}$ and the multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$ were really the same. Essentially, if we replaced 0, 1, 2, and 3 in the addition table for $\mathbb{Z}/4\mathbb{Z}$ by 1, 2, 4, 3 (respectively), then we got the the multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$. Another way of thinking about this is that we really defined a function $f : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^\times$ by $f(0) = 1$, $f(1) = 2$, $f(2) = 4$, and $f(3) = 3$. This function had a special property, though, which was that it translated the addition table for $\mathbb{Z}/4\mathbb{Z}$ to the multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$.

How can we express this? Well, the idea is that, for every $a, b \in \mathbb{Z}/4\mathbb{Z}$, the term $a + b$ in the addition table for $\mathbb{Z}/4\mathbb{Z}$ should correspond to the term $f(a)f(b)$ in the multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$. That is, $f(a + b) = f(a)f(b)$ for all $a, b \in \mathbb{Z}/4\mathbb{Z}$. This condition expresses the fact that f "translates" the addition table for $\mathbb{Z}/4\mathbb{Z}$ to the multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$.

We can generalize this condition to any pair of groups.

Definition 7.1. *Let $(G, *)$ and $(H, \bigstar)$ be two groups. A homomorphism from G to H is a map $\phi : G \to H$ such that $\phi(a * b) = \phi(a) \bigstar \phi(b)$ for all $a, b \in G$.*

Example 7.2. We can define a map $\phi : \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^\times$ by taking $\phi(0) = 1$, $\phi(1) = 2$, $\phi(2) = 4$, and $\phi(3) = 3$. Using the addition table for $\mathbb{Z}/4\mathbb{Z}$ and the multiplication table for $(\mathbb{Z}/5\mathbb{Z})^\times$, we can check that $\phi(a+b) = \phi(a)\phi(b)$ for all $a, b \in \mathbb{Z}/4\mathbb{Z}$. Alternatively, observe that $\phi(x) = 2^x$ for all x, so $\phi(a+b) = 2^{a+b} = 2^a 2^b = \phi(a)\phi(b)$. ❖

Example 7.3. We can define a map $\phi_{\text{corner}} : \mathbb{G} \to S_8$ as follows. Any move in $\mathbb{G}$ certainly rearranges the corner cubies somehow; thus, it defines a permutation of the 8 unoriented corner cubies. That is, any $M \in \mathbb{G}$ defines some permtuation $\sigma \in S_8$. Let $\phi_{\text{corner}}(M) = \sigma$. That is, $\phi_{\text{corner}}(M)$ is the element of S_8 which describes what M does to the unoriented corner cubies. For example, we know that $[\mathsf{D}, \mathsf{R}]$ has disjoint cycle decomposition $(\mathsf{dlf\ dfr\ lfd\ frd\ fdl\ rdf})(\mathsf{drb\ bru\ bdr\ ubr\ rbd\ rub})(\mathsf{df\ dr\ br})$. Therefore, $\phi_{\text{corner}}(M) = (\mathsf{dlf\ dfr})(\mathsf{drb\ bru})$.

Similarly, we can define a homomorphism $\phi_{\text{edge}} : \mathbb{G} \to S_{12}$ by letting $\phi_{\text{edge}}(M)$ be the element of S_{12} which describes what M does to the 12 unoriented edge cubies. For example, $\phi_{\text{edge}}([\mathsf{D}, \mathsf{R}]) = (\mathsf{df\ dr\ br})$.

Finally, we can define a "cube" homomorphism $\phi_{\text{cube}} : \mathbb{G} \to S_{20}$, which describes permutations of the 20 unoriented edge and corner cubies. For example, $\phi_{\text{corner}}([\mathsf{D}, \mathsf{R}]) = (\mathsf{dlf\ dfr})(\mathsf{drb\ bru})(\mathsf{df\ dr\ br})$. ❖

Exercises

1. Let $\sigma \in S_5$ be defined by $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 1$, $\sigma(4) = 5$, and $\sigma(5) = 3$. Write σ as a product of 2-cycles in at least 3 different ways (this is possible by [PS 5, #9]). Do you notice any patterns in the ways you have written σ? How many 2-cycles did you use?

2. Let $\phi : (\mathbb{Z}, +) \to (\mathbb{R} - \{0\}, \cdot)$ be defined by $\phi(x) = 2^x$. Prove that ϕ is a homomorphism.

3. Find all homomorphisms $\phi : (\mathbb{Z}/4\mathbb{Z}, +) \to ((\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$.

4. (a) Find a move $M \in \mathbb{G}$ which switches the positions of the urf and bdl cubies without affecting any other corner cubies. What is $\phi_{\text{corner}}(M)$?

   Hint: Start with the move you found in [PS 6, #2b].

(b) Let C_1 and C_2 be any two distinct unoriented corner cubies. Prove that there is some move $M \in \mathbb{G}$ which switches the positions of C_1 and C_2 without affecting any other corner cubies. (Even if you didn't find the move in [PS 7, #4a], assume that such a move exists, and you should be able to do this proof!) What is $\phi_{\text{corner}}(M)$?

5. Let $\phi : (G, *) \to (H, \bigstar)$ be a homomorphism.

   (a) Let 1_G be the identity element of G and 1_H be the identity element of H. Prove that $\phi(1_G) = 1_H$.

   (b) Prove that $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$. (First make sure you understand exactly what this means!)

6. Let $\phi : (G, *) \to (H, \bigstar)$ be a homomorphism. The image of ϕ is defined to be the set $\operatorname{im}\phi = \{\phi(g) : g \in G\}$. Prove that $\operatorname{im}\phi$ is a subgroup of H.

8. The Sign Homomorphism

By [PS 5, #9], S_n is generated by the 2-cycles in S_n. That is, any permutation in S_n can be written as a finite product of 2-cycles. However, any given permutation of S_n can be written as a finite product of 2-cycles in infinitely many ways, so it seems like there is not much we can say about this product.

Some permutations in S_n can be written as a product of an even number of 2-cycles; we call these even permutations. Other permutations in S_n can be written as a product of an odd number of 2-cycles; we call these odd permutations. So far, there seems to be no reason that a permutation could not be both even and odd. However, it is in fact true that a permutation is either even or odd, but not both.

Unfortunately, a direct proof of this fact is rather messy; instead, we will give a proof which is relatively simple but uses an indirect trick.

Fix n, and let $p(x_1, \ldots, x_n)$ be a polynomial in the n variables $x_1, \ldots, x_n$.

Example 8.1. If $n = 1$, $p(x_1)$ is a polynomial in the variable x_1; that is, $p(x_1)$ looks like $a_m x_1^m + a_{m-1}x_1^{m-1} + \cdots + a_0$. So, $p(x_1)$ is a sum of terms that look like ax_1^i.

If $n = 2$, then $p(x_1, x_2)$ is a sum of terms that look like $ax_1^i x_2^j$.

In general, $p(x_1, \ldots, x_n)$ is a sum of terms that look like $ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$. ❖

If $\sigma \in S_n$, let p^σ be the polynomial defined by $(p^\sigma)(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. That is, we simply replace x_i by $x_{\sigma(i)}$.

Example 8.2. Suppose $n = 4$, $p(x_1, x_2, x_3, x_4) = x_1^3 + x_2x_3 + x_1x_4$, and $\sigma \in S_4$ has cycle decomposition $\sigma = (1\ 2\ 3)$. Then, $(p^\sigma)(x_1, x_2, x_3, x_4) = x_{\sigma(1)}^3 + x_{\sigma(2)}x_{\sigma(3)} + x_{\sigma(1)}x_{\sigma(4)} = x_2^3 + x_3x_1 + x_2x_4$. ❖

Lemma 8.3. *For any $\sigma, \tau \in S_n$, $(p^\sigma)^\tau = p^{\sigma\tau}$.*

This statement is easy to misinterpret, so before we give a proof, let's do an example.

Example 8.4. As in the previous example, let $n = 4$, $p(x_1, x_2, x_3, x_4) = x_1^3 + x_2x_3 + x_1x_4$, and $\sigma = (1\ 2\ 3)$. Let $\tau = (1\ 3)\ (2\ 4)$. We know that $p^\sigma = x_2^3 + x_3x_1 + x_2x_4$, so $(p^\sigma)^\tau = x_{\tau(2)}^3 + x_{\tau(3)}x_{\tau(1)} + x_{\tau(2)}x_{\tau(4)} = x_4^3 + x_1x_3 + x_4x_2$. On the other hand, $\sigma\tau = (1\ 4\ 2)$, so $p^{\sigma\tau} = x_{(\sigma\tau)(1)}^3 + x_{(\sigma\tau)(2)}x_{(\sigma\tau)(3)} + x_{(\sigma\tau)(1)}x_{(\sigma\tau)(4)} = x_4^3 + x_1x_3 + x_4x_2$. ❖

Now, we will prove Lemma 8.3.

Proof. By definition, $(p^\sigma)(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, so $[(p^\sigma)^\tau](x_1, \ldots, x_n) = p(x_{\tau(\sigma(1))}, \ldots, x_{\tau(\sigma(n))})$. Now, $\tau(\sigma(i)) = (\sigma\tau)(i)$, so $[(p^\sigma)^\tau](x_1, \ldots, x_n) = p(x_{(\sigma\tau)(1)}, \ldots, x_{(\sigma\tau)(n)}) = (p^{\sigma\tau})(x_1, \ldots, x_n)$. □

To prove our assertion about even and odd permutations, we will apply Lemma 8.3 to a specific polynomial, namely

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Example 8.5. If $n = 3$, $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. ❖

Lemma 8.6. *For any $\sigma \in S_n$, $\Delta^\sigma = \pm\Delta$.*

Example 8.7. If $\sigma = (1\ 3\ 2)$, then $\Delta^\sigma = (x_3 - x_1)(x_3 - x_2)(x_1 - x_2) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \Delta$.

On the other hand, if $\sigma = (1\ 2)$, then $\Delta^\sigma = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta$. ❖

Now, we will prove Lemma 8.6. As you might guess from the examples, the idea is to match terms of Δ with terms of Δ^σ. That is, for each term $x_i - x_j$ of the product for Δ, either $x_i - x_j$ or its negative appears in the product for Δ^σ.

Proof. By definition,

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j),$$

so

$$\Delta^\sigma = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

In order to show $\Delta^\sigma = \pm\Delta$, we must show two things. First, for each i and j with $1 \le i < j \le n$, we must show that either $x_{\sigma(i)} - x_{\sigma(j)}$ or its negative appears in Δ; that is, either $x_{\sigma(i)} - x_{\sigma(j)}$ or its negative has the form $x_k - x_\ell$ with $1 \le k < \mathrm{l} \le n$. Secondly, we must show that, for each i and j with $1 \le i < j \le n$, either $x_i - x_j$ or its negative appears in Δ^σ. Since Δ and Δ^σ have the same number of terms, these two statements together prove that the terms of Δ and Δ^σ match up.

To prove the first statement, all we need to show is that either $\sigma(i) < \sigma(j)$ or $\sigma(j) < \sigma(i)$; equivalently, we need to show that $\sigma(i) \neq \sigma(j)$ if $1 \le i < j \le n$. This is true because σ is one-to-one and $i \neq j$.

To prove the second statement, we need to show that either $x_i - x_j$ or its negative can be written as $x_{\sigma(k)} - x_{\sigma(\ell)}$ with $1 \le k < \ell \le n$. Since $\sigma \in S_n$, $\sigma^{-1} \in S_n$; in particular, σ^{-1} is also a bijection. Since $i \neq j$, $\sigma^{-1}(i) \neq \sigma^{-1}(j)$. Let k be the smaller of $\sigma^{-1}(i)$ and $\sigma^{-1}(j)$, and let ℓ be the larger. Then, $1 \le k < \ell \le n$, and $x_i - x_j$ is either $x_{\sigma(k)} - x_{\sigma(\ell)}$ or its negative. □

By Lemma 8.6, we can define a map $\epsilon : S_n \to \{\pm 1\}$ by $\sigma\Delta = \epsilon(\sigma)\Delta$. By Lemma 8.3, $\Delta^{\sigma\tau} = (\Delta^\sigma)^\tau = [\epsilon(\sigma)\Delta]^\tau = \epsilon(\sigma)\Delta^\tau = \epsilon(\sigma)\epsilon(\tau)\Delta$. Therefore, $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$. So, ϵ is a homomorphism. We call it the sign homomorphism.

We claimed at the beginning that $\epsilon(\sigma)$ had something to do with the number of 2-cycles in a product decomposition of σ. Now, we'll prove this.

Theorem 8.8. *If σ is a 2-cycle, then $\epsilon(\sigma) = -1$.*

Proof. First, let $\sigma = (1\ 2)$. We can write

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Now, let's write the terms where $i = 1$ or $i = 2$ separately. Then,

$$\begin{aligned} \Delta &= \prod_{1<j\le n} (x_1 - x_j) \prod_{2<j\le n} (x_2 - x_j) \prod_{3\le i<j\le n} (x_i - x_j) \\ &= (x_1 - x_2) \prod_{2<j\le n} (x_1 - x_j) \prod_{2<j\le n} (x_2 - x_j) \prod_{3\le i<j\le n} (x_i - x_j) \end{aligned}$$

Therefore,

$$\begin{aligned} \Delta^\sigma &= (x_{\sigma(1)} - x_{\sigma(2)}) \prod_{2<j\le n} (x_{\sigma(1)} - x_{\sigma(j)}) \prod_{2<j\le n} (x_{\sigma(2)} - x_{\sigma(j)}) \prod_{3\le i<j\le n} (x_{\sigma(i)-x_\sigma(j)}) \\ &= (x_2 - x_1) \prod_{2<j\le n} (x_2 - x_j) \prod_{2<j\le n} (x_1 - x_j) \prod_{3\le i<j\le n} (x_i - x_j) \\ &= -\Delta \end{aligned}$$

Thus, we have proved the statement for $\sigma = (1\ 2)$.

We could generalize the above argument to any 2-cycle, but there is an easier way! Let σ be any 2-cycle. By [PS 5, #12], σ is conjugate to $(1\ 2)$. That is, $\sigma = \tau(1\ 2)\tau^{-1}$ for some $\tau \in S_n$. Since ϵ is a homomorphism, $\epsilon(\sigma) = \epsilon(\tau)\epsilon(1\ 2)\epsilon(\tau)^{-1} = \epsilon(1\ 2) = -1$. □

Since ϵ is multiplicative, if $\epsilon(\sigma) = 1$, then σ must be a product of an even number of 2-cycles. Similarly, if $\epsilon(\sigma) = -1$, then σ must be a product of an odd number of 2-cycles. So, σ is even iff $\epsilon(\sigma) = 1$, and σ is odd iff $\epsilon(\sigma) = -1$.

Exercises

1. Let $\phi : (G, *) \to (H, \bigstar)$ be a homomorphism. If S is a subset of $\operatorname{im}\phi$, prove that $\langle S \rangle$ is a subgroup of $\operatorname{im}\phi$.

2. Prove that the homomorphism $\phi_{\text{corner}} : \mathbb{G} \to S_8$ is onto (equivalently, $\operatorname{im}\phi_{\text{corner}}$ is S_8). What does this tell you about the possible positions of the corner cubies?

3. Suppose your Rubik's cube is in the configuration (σ, τ, x, y). If you apply the move $M \in \mathbb{G}$ to the Rubik's cube, it ends up in a new configuration (σ', τ', x', y'). Prove that $\sigma' = \sigma\phi_{\text{corner}}(M)$ and $\tau' = \tau\phi_{\text{edge}}(M)$.

4. Let (σ, τ, x, y) be a configuration of the Rubik's cube. Prove that there is a move $M \in \mathbb{G}$ which puts all of the corner cubies in the correct positions.

5. Let $\phi : G \to H$ be a homomorphism and G' be a subgroup of G. Define a map $\phi' : G' \to H$ by $\phi'(g) = \phi(g)$. Prove that ϕ' is a homomorphism. We call this homomorphism the restriction of ϕ to G' and write $\phi' = \phi|_{G'}$.

6. Find all homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z}$. Which of these homomorphisms are isomorphisms?

7. Let G be a group and let $a \in G$. Define a map $\phi : G \to G$ by $\phi(g) = a^{-1}ga$. Is ϕ a homomorphism? Is ϕ an isomorphism?

8. Write DR^{-1} and $\mathsf{D}^{-1}\mathsf{R}$ in disjoint cycle notation. Can you use these to find a move which changes the orientations of two corner cubies without affecting any other corner cubies?

9. So far, we have only used twists of the 6 faces D, U, L, R, F, and B. Let $\mathsf{M_R}$ be a clockwise twist (looking at the right face) of the face between the left and right faces. Write $\mathsf{M_R}$, $\mathsf{M_RU}$, $\mathsf{M_RU}^{-1}$, $\mathsf{M_RU}^2$, and $\mathsf{M_R}{-}1\mathsf{U}^2$ in disjoint cycle notation. Use these to ...

   (a) ... find a move in $\mathbb{G}$ which cycles 3 edge cubies without affecting any other cubies.
   (b) ... find a move in $\mathbb{G}$ which changes the orientations of 2 edge cubies without affecting any other cubies.

   Note: Remember that we defined $\mathbb{G}$ to be the moves composed of sequences of $\mathsf{D}, \mathsf{U}, \mathsf{L}, \mathsf{R}, \mathsf{F}, \mathsf{B}$; that is, $\mathbb{G} = \langle \mathsf{D}, \mathsf{U}, \mathsf{L}, \mathsf{R}, \mathsf{F}, \mathsf{B} \rangle$. Therefore, $\mathsf{M_R}$ is not an element of $\mathbb{G}$, so you will have to rewrite your moves to make them elements of G.

10. Is it possible for the Rubik's cube to be in a configuration where exactly two cubies are in the wrong positions?

9. The Alternating Group

In the previous section, we defined what it meant for an element of S_n to be even or odd. Recall that $\sigma \in S_n$ is defined to be even if it can be written as a product of an even number of 2-cycles, and it is defined to be odd if it can be written as a product of an odd number of 2-cycles.

Example 9.1. (1 2)(1 3) is even since it is a product of two 2-cycles. (1 2) is odd since it is a product of one 2-cycle. ❖

We then proved that an element of S_n is either even or odd, but not both. The tool we used for this was the sign homomorphism. Remember that this was a homomorphism $\epsilon : S_n \to \{\pm 1\}$ such that $\epsilon(\sigma) = -1$ for any 2-cycle σ. Since the 2-cycles generate S_n, this property characterizes the homomorphism. In fact, the way ϵ was actually defined is no longer important!

Since ϵ is a homomorphism, $\epsilon(\sigma) = -1$ if σ is odd, and $\epsilon(\sigma) = 1$ if σ is even.

Example 9.2. $\epsilon((1\ 2)(1\ 3)) = 1$ and $\epsilon((1\ 2)) = -1$. ❖

Example 9.3. $\epsilon(1\ 6\ 3\ 4\ 2) = 1$ because $(1\ 6\ 3\ 4\ 2) = (1\ 6)(1\ 3)(1\ 4)(1\ 2)$ is even. ❖

Example 9.4. If σ is a k-cycle, then $\epsilon(\sigma) = (-1)^{k-1}$. After all, if σ is a k-cycle, then we can write $\sigma = (a_1\ a_2\ \ldots\ a_k) = (a_1\ a_2)(a_1\ a_3)\cdots(a_1\ a_k)$. ❖

The product of an even permutation and an odd permutation is odd. The product of two even permutations or two odd permutations is even. The inverse of an even permutation is even, and the inverse of an odd permutation is odd. Therefore, we can define a subgroup of S_n consisting of all the even permutations. This group is called the alternating group and is denoted A_n.

Example 9.5. If $M \in \mathbb{G}$ is a face twist (one of $\mathsf{D}, \mathsf{U}, \mathsf{L}, \mathsf{R}, \mathsf{F}, \mathsf{B}$), then $\phi_{\text{cube}}(M)$ is a product of two 4-cycles. A 4-cycle is odd, so a product of two 4-cycles is even. Therefore, $\phi_{\text{cube}}(M)$ is even. Since the face twists generate all of $\mathbb{G}$, this means that $\phi_{\text{cube}}(M)$ is even for all $M \in \mathbb{G}$. That is, $\phi_{\text{cube}}(M) \in A_{20}$ for all $M \in \mathbb{G}$. Another way of writing this is to say that $\operatorname{im}\phi_{\text{cube}}(M) \in A_{20}$.

Now, $\phi_{\text{cube}}(M) = \phi_{\text{corner}}(M)\phi_{\text{edge}}(M)$, so either $\phi_{\text{corner}}(M)$ and $\phi_{\text{edge}}(M)$ are both even, or they are both odd. That is, $\phi_{\text{corner}}(M)$ and $\phi_{\text{edge}}(M)$ have the same sign.

Suppose your cube is in the start configuration and you do the move M to it. Then, it ends up in a confiugration (σ, τ, x, y) where $\sigma = \phi_{\text{corner}}(M)$ and $\tau = \phi_{\text{edge}}(M)$. Therefore, we have proved that, if (σ, τ, x, y) is a valid configuration, then σ and τ have the same sign. ❖

Since A_n consists of all of the even elements of S_n, A_n can also be described as $\{\sigma \in S_n : \epsilon(\sigma) = 1\}$. This definition can be generalized to any homomorphism.

Definition 9.6. *The kernel of a homomorphism $\phi : G \to H$ is defined to be $\{g \in G : \phi(g) = 1_H\}$, and it is denoted by* $\ker\phi$. *That is,* $\ker\phi$ *is the preimage of 1_H in G.*

Example 9.7. The kernel of the homomorphism $\phi_{\text{cube}} : \mathbb{G} \to S_{20}$ consists of all moves of the Rubik's cube which do not change the positions of any of the cubies. That is, $\ker\phi_{\text{cube}}$ consists of all moves which only affect the orientations, not the positions, of cubies. As you can imagine, this is a useful set to understand: if you have put all the cubies in the right positions, you want to find moves that only affect the orientations of the cubies. ❖

Theorem 9.8. *If G and H are groups and $\phi : G \to H$ is a homomorphism, then* $\ker\phi$ *is a subgroup of G.*

Proof. By Lemma 3.4, it suffices to show that, if $g, h \in \ker \phi$, then $gh^{-1} \in \ker \phi$. So, let $g, h \in \ker \phi$. Then,

$$\begin{aligned} \phi(gh^{-1}) &= \phi(g)\phi(h^{-1}) \text{ since } \phi \text{ is a homomorphism} \\ &= \phi(g)\phi(h)^{-1} \text{ by [PS 7, \#5b]} \\ &= 1_H 1_H^{-1} \text{ since } g, h \in \ker \phi \\ &= 1_H \end{aligned}$$

Therefore, $gh^{-1} \in \ker \phi$. □

Example 9.9. The alternating group A_n is the kernel of $\epsilon : S_n \to \{\pm 1\}$. ❖

Exercises

1. Let $\sigma \in S_{10}$ be defined by $\sigma = (1\ 3)(2\ 4\ 6\ 9)(1\ 4\ 9)$. What is $\epsilon(\sigma)$? Is σ even or odd?
2. If $\sigma \in S_n$, prove that $\sigma^2 \in A_n$.
3. If $\sigma \in S_n$ has cycle type $n_1, \ldots, n_r$, what is $\epsilon(\sigma)$?
4. Prove that A_n is generated by the set of 3-cycles in S_n.
5. Prove that S_n is generated by $(1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n)$.
6. Find a move $M \in \mathbb{G}$ which changes the orientations of the cubies dfr and ulb without affecting any other corner cubies. What is $\phi_{\text{corner}}(M)$? What is a strategy for fixing the orientations of all corner cubies?

10. Group Actions

If the Rubik's cube is some configuration $\mathcal{C} = (\sigma, \tau, x, y)$, then doing a move $M \in \mathbb{G}$ puts the Rubik's cube in some new configuration. Let's write this new configuration as $\mathcal{C} \cdot M$.

Suppose the Rubik's cube starts in the configuration $\mathcal{C}$. If we do the move M_1, the configuration of the cube becomes $\mathcal{C} \cdot M_1$. If we then do another move M_2, the configuration becomes $(\mathcal{C} \cdot M_1) \cdot M_2$. On the other hand, what we have really done is started with the configuration $\mathcal{C}$ and applied the move $M_1 M_2$, so another way to write the new configuration is $\mathcal{C} \cdot (M_1 M_2)$. That is, we have just shown that $(\mathcal{C} \cdot M_1) \cdot M_2 = \mathcal{C} \cdot (M_1 M_2)$ for all configurations $\mathcal{C}$ and all moves $M_1, M_2 \in \mathbb{G}$.

If we do the empty move (the identity element e of $\mathbb{G}$), then the configuration does not change at all, so $\mathcal{C} \cdot e = \mathcal{C}$.

This is an example of a mathematical object called a "group action." Elements of a group (here, the elements are moves of the Rubik's cube) affect elements of some set (the set of configurations of the Rubik's cube). We have actually used group actions already; for instance, to understand S_n, we studied how elements of S_n affected the integers $1, \ldots, n$.

To give a formal definition, we first need some notation. If S_1 and S_2 are two sets, then $S_1 \times S_2$ is the set of ordered pairs (s_1, s_2) with $s_1 \in S_1$ and $s_2 \in S_2$.

Definition 10.1. *A (right) group action of a group $(G, *)$ on a (non-empty) set A is a map $A \times G \to A$ (that is, given $a \in A$ and $g \in G$, we can produce another element of A, which we write $a \cdot g$) satisfying the following two properties:*

1. *$(a \cdot g_1) \cdot g_2 = a \cdot (g_1 * g_2)$ for all $g_1, g_2 \in G$ and $a \in A$.*
2. *$a \cdot e = a$ for $a \in A$ (here, e is the identity element of G).*

This is a right action rather than a left action because we put the elements of the group on the right.

In the first condition, $a \cdot g_1 \in A$, so $(a \cdot g_1) \cdot g_2$ makes sense. On the other hand, $g_1 g_2 \in G$, so $a \cdot (g_1 g_2)$ also makes sense.

When we have a group action of G on a set A, we just say "G acts on A."

Example 10.2. The group $\mathbb{G}$ acts on the set of configurations (σ, τ, x, y) of the Rubik's cube (we allow both valid and invalid configurations). ❖

Example 10.3. S_n acts on the set $\{1, \ldots, n\}$. The group action is defined as follows: given $i \in \{1, \ldots, n\}$ and $\sigma \in S_n$, let $i \cdot \sigma = \sigma(i)$. To check that this really is a group action, observe that $i \cdot (\sigma\tau) = (\sigma\tau)(i) = \tau(\sigma(i)) = \tau(i \cdot \sigma) = (i \cdot \sigma) \cdot \tau$ and $i \cdot 1 = 1(i) = i$. ❖

Example 10.4. S_n acts on the set of polynomials in the variables $x_1, \ldots, x_n$; in fact, we used this action to prove the existence of the sign homomorphism. Namely, if $p(x_1, \ldots, x_n)$ was a polynomial, we defined a new polynomial p^σ by $p^\sigma(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. This was again a polynomial in the variables $x_1, \ldots, x_n$. We proved that $(p^\sigma)^\tau = p^{\sigma\tau}$, and it is clear that $p^1 = p$. Thus, if we define $p \cdot \sigma = p^\sigma$, we have a group action. ❖

Example 10.5. The group $(\mathbb{Z}, +)$ acts on the set $\mathbb{R}$ by $a \cdot g = g + a$ for $g \in \mathbb{Z}$ and $a \in \mathbb{R}$. After all,

$$\begin{aligned} (a \cdot g_1) \cdot g_2 &= (a \cdot g_1) + g_2 \\ &= (a + g_1) + g_2 \\ &= a + (g_1 + g_2) \\ &= a \cdot (g_1 + g_2) \end{aligned}$$

for all $g_1, g_2 \in \mathbb{Z}$ and $a \in \mathbb{R}$. Moreover, $a \cdot 0 = 0 + a = 0$ for all $a \in \mathbb{R}$. ❖

Example 10.6. Often, we are interested in the case when the set A is the group itself. In this case, we say

that the group acts on itself. For instance, we can define a group action as follows: for $g \in G$ and $a \in G$, define $a \cdot g = ag$, the normal group multiplication of a and g (check that this defines a group action). We call this the action of G on itself by right multiplication. ❖

Definition 10.7. *If G acts on a set A, then the orbit of $a \in A$ (under this action) is the set $\{a \cdot g : g \in G\}$.*

Example 10.8. $\mathbb{G}$ acts on the set of configurations of the Rubik's cube. The orbit of the start configuration under this action is exactly the set of valid configurations of the Rubik's cube. ❖

Example 10.9. In Example 10.5, we said that $(\mathbb{Z}, +)$ acts on the set $\mathbb{R}$ by $a \cdot g = g + 1$ for all $g \in \mathbb{Z}$ and $a \in \mathbb{R}$. Thus, the orbit of a is the set $\{a + g : g \in \mathbb{Z}\}$, or the set $\{\ldots, a-2, a-1, a, a+1, a+2, \ldots\}$. In particular, $a, a+1, a-1, \ldots$ all have the same orbit. There is a distinct orbit for each $a \in [0, 1)$. Therefore, we can think of the set of orbits as the interval $[0, 1)$. However, since the orbit of 0 is the same as the orbit of 1, we could also think of the set of orbits as $[0, 1]$ with 0 and 1 viewed as the same point. One way to visualize this is to imagine bending the interval $[0, 1]$ around so that 0 and 1 join — this forms a circle! Thus, it is natural to think of the set of orbits of this action as forming a circle. ❖

Definition 10.10. *If a group action has only one orbit, we say that the action is transitive (or that the group acts transitively).*

Example 10.11. $\mathbb{G}$ acts on the set of ordered pairs (C_1, C_2) of different unoriented corner cubies. After all, if C_1 and C_2 are two different unoriented corner cubies, applying a move $M \in \mathbb{G}$ sends these corner cubies to two different corner cubicles C_1' and C_2'. Then, we can define the group action by $(C_1, C_2) \cdot M = (C_1', C_2')$. (Check that this is a group action.) By [PS 3, #5], this action is transitive.

In the same way, $\mathbb{G}$ acts on the set of ordered triples (C_1, C_2, C_3) of different unoriented edge cubies. ❖

We often want to prove something about all elements of an orbit (for example, we might want to prove a statement about all valid configurations of the Rubik's cube). The following lemma can be useful in these situations.

Lemma 10.12. *Suppose a finite group G acts on a set A, and let S be a set of generators of G. Let P be a property such that the following is true:*

Whenever $a \in A$ satisfies P and $s \in S$, $a \cdot s$ also satisfies P.

Then, if $a_0 \in A$ satisfies P, every element in the orbit of a_0 also satisfies P.

Proof. Let's define a new property Q as follows: say $g \in G$ satisfies property Q when the following is true:

Whenever $a \in A$ satisfies P, $a \cdot g$ also satisfies P.

It suffices to show that every $g \in G$ satisfies property Q. After all, that would mean that, if $a_0 \in A$ satisfies P, then $a_0 \cdot g$ satisfies P for all $g \in G$, which is exactly what we want to show.

By hypothesis, every element of S satisfies property Q. By Proposition 4.9, all we need to show is that, if $g, h \in G$ both satisfy property Q, then gh satisfies property Q. So, suppose $g, h \in G$ both satisfy property Q. To show that gh also satisfies property Q, we want to show that, if $a \in A$ satisfies P, then $a \cdot gh$ also satisfies P.

Suppose $a \in A$ satisfies P. Since g satisfies property Q, $a \cdot g$ satisfies property P. Since h satisfies property Q, $(a \cdot g) \cdot h$ satisfies property P. However, by the definition of a group action, $(a \cdot g) \cdot h = a \cdot gh$. So, we have proved that, if $a \in A$ satisfies P, then $a \cdot gh$ satisfies P. That means that gh satisfies property Q, which finishes our proof. □

In the case of the Rubik's cube, we will often try to apply the above lemma to the action of the group $\mathbb{G}$ on the set A of configurations. In particular, if we let $S = \{\mathsf{D}, \mathsf{U}, \mathsf{L}, \mathsf{R}, \mathsf{F}, \mathsf{B}\}$ and a_0 be the start configuration, then we can use the lemma to prove things about all valid configurations of the Rubik's cube.

Exercises

1. Prove that the group $(n\mathbb{Z}, +)$ acts on $\mathbb{Z}$ by $a \cdot g = a + g$ for all $g \in n\mathbb{Z}$ and $a \in A$. What are the orbits of this action? How many different orbits are there? Does the set of orbits remind you of anything in number theory?

2. Let G be a group. Prove that G acts on G by $a \cdot g = g^{-1}ag$ for all $g \in G$ and $a \in G$. We say that "G acts on itself by conjugation."

3. By [PS 10, #2], S_n acts on S_n by $\tau \cdot \sigma = \sigma^{-1}\tau\sigma$ for all $\tau \in S_n$ and $\sigma \in S_n$. What are the orbits of this action? (You might want to first try to write out the orbits explicitly for $n = 3$.)

4. Let $\mathbb{R}^2$ be the usual xy-plane, which consists of ordered pairs (x, y) where $x, y \in \mathbb{R}$. Prove that the group $(\mathbb{R}, +)$ acts on $\mathbb{R}^2$ by $(x, y) \cdot r = (x + r, y)$ for $(x, y) \in \mathbb{R}^2$ and $r \in \mathbb{R}$. If $(x, y) \in \mathbb{R}^2$, find the orbit of (x, y). Can you describe the set of orbits geometrically?

5. Let $\mathbb{Z}^2$ be the set of ordered pairs (z_1, z_2) where $z_1, z_2 \in \mathbb{Z}$. We add two ordered pairs as follows: $(z_1, z_2) + (z_3, z_4)$ is defined to be $(z_1 + z_3, z_2 + z_4)$. Prove that $(\mathbb{Z}^2, +)$ is a group, and prove that this group acts on $\mathbb{R}^2$ by $(x, y) \cdot (z_1, z_2) = (x + z_1, y + z_2)$ for all $(x, y) \in \mathbb{R}^2$ and $(z_1, z_2) \in \mathbb{Z}^2$. Can you describe the set of orbits geometrically?

6. Let A be the set of ordered triples (C_1, C_2, C_3) where C_1, C_2, and C_3 are different unoriented edge cubies. In class, we explained how $\mathbb{G}$ acts on A. What does it mean (in terms of the Rubik's cube) to say that this action has only one orbit? Convince yourself that the action really has just one orbit.

7. If C_1, C_2, and C_3 are any three different unoriented edge cubies, prove that there is a move $M \in \mathbb{G}$ such that M does not affect any corner cubies and $\phi_{\text{edge}}(M) = (C_1\ C_2\ C_3)$.

8. Suppose your Rubik's cube is in a valid configuration (e, τ, x, y) (that is, all of the corner cubies are in the right positions). Prove that τ is even and that there is a move $M \in \mathbb{G}$ which puts all of the edge cubies in the right positions (without affecting the corner cubies).

11. Valid Configurations of the Rubik's Cube

Now, we will put everything we have learned together to give a characterization of the valid configurations of the Rubik's cube.

Theorem 11.1. *A configuration (σ, τ, x, y) is valid iff $\operatorname{sgn}\sigma = \operatorname{sgn}\tau$, $\sum x_i \equiv 0 \pmod 3$, and $\sum y_i \equiv 0 \pmod 2$.*

The rest of this section will be devoted to proving this theorem. First, we will show that, if (σ, τ, x, y) is valid, then $\operatorname{sgn}\sigma = \operatorname{sgn}\tau$, $\sum x_i \equiv 0 \pmod 3$, and $\sum y_i \equiv 0 \pmod 2$. In the process, we will prove some slightly more general facts that will be useful for proving the converse.

Recall that $\mathbb{G}$ acts on the set of configurations of the Rubik's cube. The valid configurations form a single orbit of this action. So, it makes sense that statements we make about valid configurations can be generalized to other orbits.

Lemma 11.2. *If (σ, τ, x, y) and (σ', τ', x', y') are in the same orbit, then $(\operatorname{sgn}\sigma)(\operatorname{sgn}\tau) = (\operatorname{sgn}\sigma')(\operatorname{sgn}\tau')$.*

Proof. By Lemma 10.12, it suffices to show that, if $(\sigma', \tau', x', y') = (\sigma, \tau, x, y) \cdot M$ where M is one of the 6 basic moves, then $(\operatorname{sgn}\sigma)(\operatorname{sgn}\tau) = (\operatorname{sgn}\sigma')(\operatorname{sgn}\tau')$. By [PS 8, #3], $\sigma' = \sigma\phi_{\text{corner}}(M)$ and $\tau' = \tau\phi_{\text{edge}}(M)$. Therefore, $(\operatorname{sgn}\sigma')(\operatorname{sgn}\tau') = (\operatorname{sgn}\sigma)(\operatorname{sgn}\phi_{\text{corner}}(M))(\operatorname{sgn}\tau)(\operatorname{sgn}\phi_{\text{edge}}(M))$. If M is one of the 6 basic moves, then $\phi_{\text{corner}}(M)$ and $\phi_{\text{edge}}(M)$ are both 4-cycles, so they both have sign -1. Thus, $(\operatorname{sgn}\sigma')(\operatorname{sgn}\tau') = (\operatorname{sgn}\sigma)(\operatorname{sgn}\tau)$. □

Corollary 11.3. *If (σ, τ, x, y) is a valid configuration, then $\operatorname{sgn}\sigma = \operatorname{sgn}\tau$.*

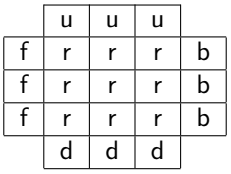
Proof. This is a direct consequence of Lemma 11.2 since any valid configuration is in the orbit of the start configuration $(1, 1, 0, 0)$. □

Lemma 11.4. *If (σ', τ', x', y') is in the same orbit as (σ, τ, x, y), then $\sum x'_i \equiv \sum x_i \pmod 3$ and $\sum y'_i \equiv \sum y_i \pmod 2$.*

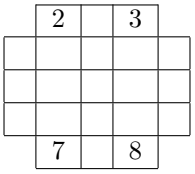
Proof. In light of Proposition 10.12, it suffices to show that, if $(\sigma', \tau', x', y') = (\sigma, \tau, x, y) \cdot M$ where M is one of the 6 basic moves, then $\sum x'_i \equiv \sum x_i \pmod 3$ and $\sum y'_i \equiv \sum y_i \pmod 2$. You should have done this in [PS 6, #1]. Here is a table showing what x' and y' are if $(\sigma', \tau', x', y') = (\sigma, \tau, x, y) \cdot M$ and M is one of the 6 basic moves. In each case, it is easy to check that $\sum x'_i \equiv \sum x_i \pmod 3$ and $\sum y'_i \equiv \sum y_i \pmod 2$.

M	x' and y'
D	$(x_1, x_2, x_3, x_4, x_8, x_5, x_6, x_7)$
	$(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_{10}, y_{11}, y_{12}, y_9)$
U	$(x_2, x_3, x_4, x_1, x_5, x_6, x_7, x_8)$
	$(y_4, y_1, y_2, y_3, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12})$
R	$(x_1, x_7 + 1, x_2 + 2, x_4, x_5, x_6, x_8 + 2, x_3 + 1)$
	$(y_1, y_7, y_3, y_4, y_5, y_2, y_{10}, y_8, y_9, y_6, y_{11}, y_{12})$
L	$(x_4 + 2, x_2, x_3, x_5 + 1, x_6 + 2, x_1 + 1, x_7, x_8)$
	$(y_1, y_2, y_3, y_5, y_{12}, y_6, y_7, y_4, y_9, y_{10}, y_{11}, y_8)$
F	$(x_6 + 1, x_1 + 2, x_3, x_4, x_5, x_7 + 2, x_2 + 1, x_8)$
	$(y_1, y_2, y_8 + 1, y_4, y_5, y_6, y_3 + 1, y_{11} + 1, y_9, y_{10}, y_7 + 1, y_{12})$
B	$(x_1, x_2, x_8 + 1, x_3 + 2, x_4 + 1, x_6, x_7, x_5 + 2)$
	$(y_6 + 1, y_2, y_3, y_4, y_1 + 1, y_9 + 1, y_7, y_8, y_5 + 1, y_{10}, y_{11}, y_{12})$

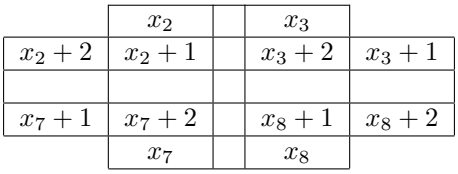
As an example, we'll see how to find x' when M is the move R. The cubicles of the right hand face look like this:



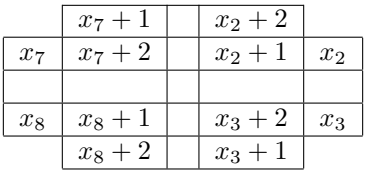
The cubicles are labeled like this:



Therefore, if the Rubik's cube is in the configuration (σ, τ, x, y), the cubies on the right face are labeled like this:



If we rotate this face by 90° clockwise, then the cubies look like:



Thus, $x' = (x_1, x_7+1, x_2+2, x_4, x_5, x_6, x_8+2, x_3+1)$. So, $\sum x_i' = \sum x_i + 6 \equiv \sum x_i \pmod 3$. □

Corollary 11.5. *If (σ, τ, x, y) is a valid configuration, then $\sum x_i \equiv 0 \pmod 3$ and $\sum y_i \equiv 0 \pmod 2$.*

Proof. This is a direct consequence of Lemma 11.4 since any valid configuration is in the orbit of the start configuration $(1, 1, 0, 0)$. □

Thus, we have proved one directon of Theorem 11.1. Now, we will prove the converse. Suppose $\operatorname{sgn}\sigma = \operatorname{sgn}\tau$, $\sum x_i \equiv 0 \pmod 3$, and $\sum y_i \equiv 0 \pmod 2$. We want to show that there is a series of moves which, when applied to (σ, τ, x, y), gives the start configuration; that is, if the Rubik's cube is in the configuration (σ, τ, x, y), it can be solved. The idea of the proof is basically to write down the steps required to solve the Rubik's cube. Thus, we will prove these four facts:

1. If (σ, τ, x, y) is a configuration such that $\operatorname{sgn}\sigma = \operatorname{sgn}\tau$, $\sum x_i \equiv 0 \pmod 3$, and $\sum y_i \equiv 0 \pmod 2$, then there is a move $M \in \mathbb{G}$ such that $(\sigma, \tau, x, y) \cdot M$ has the form $(1, \tau', x', y')$ with $\operatorname{sgn}\tau' = 1$, $\sum x_i' \equiv 0 \pmod 3$, and $\sum y_i' \equiv 0 \pmod 2$. That is, we can put all the corner cubies in the right positions.

2. If $(1, \tau, x, y)$ is a configuration with $\operatorname{sgn}\tau = 1$, $\sum x_i \equiv 0 \pmod 3$, and $\sum y_i \equiv 0 \pmod 2$, then there is a move $M \in \mathbb{G}$ such that $(1, \tau, x, y) \cdot M$ has the form $(1, \tau', 0, y')$ with $\operatorname{sgn}\tau' = 1$ and $\sum y_i' \equiv 0 \pmod 2$. That is, we can put all the corner cubies in the right orientations (and positions).

3. If $(1, \tau, 0, y)$ is a configuration with $\operatorname{sgn}\tau = 1$ and $\sum y_i \equiv 0 \pmod 2$, then there is a move $M \in \mathbb{G}$ such that $(1, \tau, 0, y) \cdot M$ has the form $(1, 1, 0, y')$ with $\sum y_i' \equiv 0 \pmod 2$. That is, we can put all the edge cubies in the right positions (without disturbing the corner cubies).

4. If $(1, 1, 0, y)$ is a configuration with $\sum y_i \equiv 0 \pmod 2$, then there is a move $M \in \mathbb{G}$ such that $(1, 1, 0, y) \cdot M = (1, 1, 0, 0)$. That is, we can solve the cube!

Before proving these, let's point out a useful fact. Suppose that (σ, τ, x, y) satisfies $\operatorname{sgn}\sigma = \operatorname{sgn}\tau$, $\sum x_i \equiv 0 \pmod 3$, and $\sum y_i \equiv 0 \pmod 2$. Then, Lemma 11.2 and 11.4 show that, for any (σ', τ', x', y') in the same orbit as (σ, τ, x, y), $\operatorname{sgn}\sigma' = \operatorname{sgn}\tau'$, $\sum x'_i \equiv 0 \pmod 3$, and $\sum y'_i \equiv 0 \pmod 2$. Thus, for example, in the first statement above, if we can prove that there is a move $M \in G$ such that $(\sigma, \tau, x, y) \cdot M$ has the form $(1, \tau', x', y')$, it is automatic that $\operatorname{sgn}\tau' = 1$, $\sum x'_i \equiv 0 \pmod 3$, and $\sum y'_i \equiv 0 \pmod 2$. Therefore, to finish the proof of Theorem 11.1, it suffices to prove the following four propositions.

Proposition 11.6. *If (σ, τ, x, y) is a configuration such that $\operatorname{sgn}\sigma = \operatorname{sgn}\tau$, $\sum x_i \equiv 0 \pmod 3$, and $\sum y_i \equiv 0 \pmod 2$, then the orbit of (σ, τ, x, y) contains some configuration of the form $(1, \tau', x', y')$.*

Proposition 11.7. *If $(1, \tau, x, y)$ is a configuration with $\operatorname{sgn}\tau = 1$, $\sum x_i \equiv 0 \pmod 3$, and $\sum y_i \equiv 0 \pmod 2$, then the orbit of $(1, \tau, x, y)$ contains some configuration of the form $(1, \tau', 0, y')$.*

Proposition 11.8. *If $(1, \tau, 0, y)$ is a configuration with $\operatorname{sgn}\tau = 1$ and $\sum y_i \equiv 0 \pmod 2$, then the orbit of $(1, \tau, 0, y)$ contains some configuration of the form $(1, 1, 0, y)$.*

Proposition 11.9. *If $(1, 1, 0, y)$ is a configuration with $\sum y_i \equiv 0 \pmod 2$, then the orbit of $(1, 1, 0, y)$ contains the start configuration $(1, 1, 0, 0)$.*

We will prove these in order. So, we want to first show that we can put all the corner cubies in the right positions.

Lemma 11.10. *The homomorphism $\phi_{\text{corner}} : \mathbb{G} \to S_8$ is onto.*

Proof. By [PS 5, #9], S_8 is generated by the set S of 2-cycles in S_8. It suffices to show that $S \subset \operatorname{im}\phi_{\text{corner}}$. After all, if $S \subset \operatorname{im}\phi_{\text{corner}}$, then $S_8 = \langle S \rangle \subset \langle \operatorname{im}\phi_{\text{corner}} \rangle$ by [PS 4, #2]. By [PS 7, #6], $\operatorname{im}\phi_{\text{corner}}$ is a group, so $\langle \operatorname{im}\phi_{\text{corner}} \rangle = \operatorname{im}\phi_{\text{corner}}$ by [PS 4, #1].

So, we want to show that every 2-cycle in S_8 is in the image of ϕ_{corner}. In [PS 6, #2b], you should have found a move which switches just 2 corner cubies and leaves the other corner cubies fixed. One such move is $M_0 = ([\mathsf{D}, \mathsf{R}]\mathsf{F})^3$, which has disjoint cycle decomposition $(\mathsf{dbr\ urb})(\mathsf{dr\ uf})(\mathsf{br\ rf})(\mathsf{df\ lf})$. Then, $\phi_{\text{corner}}(M_0) = (\mathsf{dbr\ urb})$. So, we at least know that $(\mathsf{dbr\ urb})$ lies in the image of ϕ_{corner}.

Let C_1 and C_2 be any pair of corner cubies. By [PS 3, #5], there exists a move $M \in \mathbb{G}$ which sends dbr to C_1 and urb to C_2. Let $\sigma = \phi_{\text{corner}}(M)$. Then, $\sigma(\mathsf{dbr}) = C_1$ and $\sigma(\mathsf{urb}) = C_2$. Since ϕ_{corner} is a homomorphism,

$$\begin{aligned}
\phi_{\text{corner}}(M^{-1}M_0M) &= \phi_{\text{corner}}(M)^{-1}\phi_{\text{corner}}(M_0)\phi_{\text{corner}}(M) \\
&= \sigma^{-1}(\mathsf{dbr\ urb})\sigma \\
&= (\sigma(\mathsf{dbr})\ \sigma(\mathsf{urb}))\text{by [PS 5, \#10]} \\
&= (C_1\ C_2)
\end{aligned}$$

Therefore, $(C_1\ C_2) \in \operatorname{im}\phi_{\text{corner}}$, which finishes the proof. □

Proof of Proposition 11.6. By Lemma 11.10, there exists a move $M \in \mathbb{G}$ such that $\phi_{\text{corner}}(M) = \sigma^{-1}$. By [PS 8, #3], $(\sigma, \tau, x, y) \cdot M = (1, \tau', x', y')$ for some $\tau' \in S_{12}$, $x' \in (\mathbb{Z}/3\mathbb{Z})^8$, and $y' \in (\mathbb{Z}/2\mathbb{Z})^{12}$. □

Next, we will prove Proposition 11.7. The basic idea for orienting all of the corner cubies correctly was to use moves which change the orientations of just 2 cubies. First, we must show that such moves exist.

Lemma 11.11. *If C_1 and C_2 are any two corner cubies, there is a move $M \in \mathbb{G}$ which changes the orientations (but not positions) of C_1 and C_2 and which does not affect the other corner cubies at all. Moreover, there is such a move M which rotates C_1 clockwise and rotates C_2 counterclockwise.*

Proof. As in the proof of Lemma 11.10, the point is to first find a single move M_0 which changes the orientations of 2 cubies and then conjugate M_0 to find other moves that change the orientations of 2 cubies. In [PS 6, #3], you should have found such a move; one possibility is $M_0 = (\mathsf{DR}^{-1})^3(\mathsf{D}^{-1}\mathsf{R})^3$, which has disjoint cycle decomposition $(\mathsf{dfr\ rdf\ frd})(\mathsf{drb\ rbd\ bdr})(\mathsf{df\ dr\ fr\ ur\ br\ db\ dl})$. Then, $\phi_{\text{corner}}(M_0) = 1$ and $\psi_{\text{corner}}(M_0) = (\mathsf{dbr\ rdb\ brd})(\mathsf{drf\ rfd\ fdr})$. So, if $C_1 = \mathsf{dbr}$ and $C_2 = \mathsf{drf}$, the lemma is true.

Now, we will conjugate this move. By [PS 3, #5], there exists $M \in \mathbb{G}$ which sends dbr to C_1 and drf to C_2. Let $M' = M^{-1}M_0M$. By applying [PS 5, #10] to find $\psi_{\text{corner}}(M')$, we see that M' changes the orientations of C_1 and C_2 and does not affect the other corner cubies. Specifically, M' rotates C_1 clockwise and rotates C_2 counterclockwise. □

Proof of Proposition 11.7. Suppose that the Rubik's cube is in a configuration where at least two corner cubies C_1 and C_2 have the wrong orientation. By Lemma 11.11, there is a move which rotates C_1 clockwise, rotates C_2 counterclockwise, and does not affect the other corner cubies. By applying this move once or twice, we can ensure that C_1 has the correct orientation. Since this move does not affect any corner cubies besides C_1 and C_2, the Rubik's cube now has one fewer corner cubie with an incorrect orientation. Doing this repeatedly, we end up with a configuration $(1, \tau', x', y')$ where there is at most one corner cubie with the incorrect orientation. That is, at least 7 of the x_i' are 0. By Lemma 11.4, $\sum x_i' \equiv \sum x_i \equiv 0 \pmod 3$, so it must be the case that the last x_i' is also 0, so the configuration of the Rubik's cube is $(1, \tau', 0, y')$. □

Next, we want to prove Proposition 11.9; that is, we want to fix the positions of the edge cubies. The idea of the proof is very similar to the one we used to prove Proposition 11.7. Recall that, in that case, we first proved that $\phi_{\text{corner}} : \mathbb{G} \to S_8$ is onto. In this case, we only want to use moves that don't affect the corner cubies, since we have already done a lot of work to get the corner cubies in the right positions and orientations. Therefore, instead of looking directly at ϕ_{edge}, we will look at the restriction of ϕ_{edge} to $\ker \psi_{\text{corner}}$ (see [PS 8, #5]).

Lemma 11.12. *The image of $\phi_{\text{edge}}|_{\ker \psi_{\text{corner}}} : \ker \psi_{\text{corner}} \to S_{12}$ contains A_{12}.*

Proof. By [PS 9, #4], A_{12} is generated by the set of 3-cycles in A_{12}. By the same argument as in the proof of Lemma 11.10, it suffices to show that every 3-cycle is in the image of $\phi_{\text{edge}}|_{\ker \psi_{\text{corner}}}$. As in the proof of Lemma 11.10, the strategy is to use conjugates of a single move to prove this.

You shoudl have found a move in [PS 8, #9a] that does not affect any corner cubies but cycles 3 edge cubies. One such move is $M_0 = \mathsf{LR}^{-1}\mathsf{U}^2\mathsf{L}^{-1}\mathsf{RB}^2$, which has disjoint cycle decomposition (ub uf db). Then, $M_0 \in \ker \psi_{\text{corner}}$, and $\phi_{\text{edge}}(M_0) = (\mathsf{ub}\ \mathsf{uf}\ \mathsf{db})$. By [PS 10, #6], if C_1, C_2, and C_3 are any 3 corner cubies, there is a move M of the Rubik's cube which sends ub to C_1, uf to C_2, and db to C_3. Then, by [PS 5, #10], $M' = M^{-1}M_0M$ has disjoint cycle decomposition $(C_1\ C_2\ C_3)$, so $M' \in \ker \psi_{\text{corner}}$ and $\phi_{\text{edge}}(M') = (C_1\ C_2\ C_3)$. Therefore, $(C_1\ C_2\ C_3) \in \operatorname{im} \phi_{\text{edge}}|_{\ker \psi_{\text{corner}}}$, which completes the proof. □

Remark 11.13. *In fact, the image of $\phi_{\text{edge}}|_{\ker \psi_{\text{corner}}} : \ker \psi_{\text{corner}} \to S_{12}$ is exactly A_{12}, which you can prove using Corollary 11.3.*

Now, Proposition 11.8 follows directly from Lemma 11.12. (The proof is exactly the same idea as the proof of Proposition 11.6.)

Finally, we must prove Proposition 11.9. This is quite similar to Proposition 11.7; first, we need an analog of Lemma 11.11.

Lemma 11.14. *If C_1 and C_2 are any two edge cubies, there is a move $M \in \mathbb{G}$ which changes the orientations (but not positions) of C_1 and C_2 and which does not affect the other cubies at all.*

Proof. In [PS 8, #9b], you should have found a move which switches the orientations of 2 edge cubies without affecting any other cubies. One such move is

$$\mathsf{LR}^{-1}\mathsf{FLR}^{-1}\mathsf{DLR}^{-1}\mathsf{BLR}^{-1}\mathsf{ULR}^{-1}\mathsf{F}^{-1}\mathsf{LR}^{-1}\mathsf{D}^{-1}\mathsf{LR}^{-1}\mathsf{B}^{-1}\mathsf{LR}^{-1}\mathsf{U}^{-1}$$

(this move is described more easily as $(\mathsf{M_RU})^4(\mathsf{M_RU}^{-1})^4$). Call this move M_0; it has disjoint cycle decomposition (fu uf)(bu ub). By [PS 10, #6], $\mathbb{G}$ acts transitively on the set of ordered triples (C_1, C_2, C_3) where C_1, C_2, and C_3 are different edge cubies. In particular, if C_1 and C_2 are any two different edge cubies, there exists $M \in \mathbb{G}$ sending uf to C_1 and ub to C_2. By [PS 5, #10], MM_0M^{-1} changes the orientations of C_1 and C_2 and does not affect the other cubies at all. □

Now, the argument we used to prove Proposition 11.7 proves Proposition 11.9 as well. This completes the proof of Theorem 11.1.

Remark 11.15. *Earlier, we calculated that there were* $2^{12}3^8 8!12!$ *possible configurations of the Rubik's cube; now, Theorem 11.1 tells us that only* $\frac{1}{12}$ *of those are valid. Of course, this means there are still more than* 4×10^{19} *valid configurations, no small number!*