5-10-2016

Mathematics of the Rubik's Cube

Kara M. Dismuke
Loyola Marymount University, karadismuke@gmail.com

Mathematics of the Rubik's Cube

by

Kara Michel Dismuke

A thesis presented to the
Faculty of the Department of Mathematics
Loyola Marymount University

in partial fulfillment of the requirements
for Graduation with the Bachelor of Science Degree in Mathematics

May 9, 2016

Mathematics of the Rubik's Cube

Senior Thesis by

Kara Michel Dismuke

Alissa S. Crans, Thesis Director

Abstract

In choosing a topic for my thesis, I wanted to choose a topic that would be relatable to those outside of the math community without sacrificing mathematical integrity nor rigor. Thus, I chose the Rubik's Cube to be the lens through which I sought to view Group Theory. In taking this approach, while gaining a basic appreciation for the Rubik's Cube, we gain a better understanding of fundamental concepts like permutations, groups, commutativity, order, and generators. Even more, we apply the Cube to deeper concepts within Group Theory, namely those that revolve around the notion of a group action like orbit, stabilizer, kernel, and faithfulness. Throughout, we also make conjectures and prove certain theorems in order to enrich our understanding of these concepts and shed more light on the Cube. Overall, though I entered into this paper thinking that Group Theory would help me learn more about the Rubik's Cube, I now believe the Rubik's Cube is the perfect springboard by which anyone can learn more about Group Theory!

Thesis written by

Kara Michel Dismuke

Approved by

Alissa S. Crans, Thesis Director	Date
Suzanne Larson, Mathematics Department Chair	Date
Vandana Thadani, Honors Program Director	Date

Contents

CHAPTER 1

Rubik's Cube Fundamentals

1.1. Introduction to the Cube

Sodoku. Poker. Connect Four. Mastermind. Chess. Mathematics is no stranger to problems and games simple enough for the average person to understand, but difficult enough for the average person to easily solve or win. As it pertains to these types of challenges, I believe mathematics is the difference maker: it can transform problems that often frustrate and confuse into sources of intrigue and captivation. With this in mind, we proceed and take a closer look at the mathematical beauty of the classic puzzle: *the Rubik's Cube*.

1.1.1. The Stationary Cube. Let us first consider the cube in its solved state without any movement. We will use the word "cubie" to refer to one of individual cubes in the Rubik's Cube and use the word "cubicle" refer to the the cubby that each cubie can occupy. Thus, cubies can change location depending on movement, whereas cubicles remain in fixed positions.

We can further understand the Rubik's Cube by identifying, notating, and counting fundamental aspects of the stationary cube.

- 6 colors (red, blue, green, white, yellow, orange)
- 26 total cubies (and 26 total cubicles)
  - 12 "edge cubies": each has exactly 2 visible cubie faces (see Figure 1)
  - 8 "corner cubies": each has exactly 3 visible cubie faces (see Figure 2)
  - 6 "center cubies": each has exactly 1 visible cubie face (see Figure 3)
- 6 total faces (front, left, right, upper, down, back)
- 9 facelets (face(s) of a cubie) of each color for a total of 54 total facelets
  - 24 corner cubie facelets
  - 24 edge cubie facelets
  - 6 center cubie facelets

FIGURE 1.
edge cubie

FIGURE 2.
corner cubie

FIGURE 3.
center cubie

For the sake of clarity and consistency, we now specify the following notation: for cubicles we use **lowercase letter(s)** and for cubies we use **lowercase italicized letters**. Cubicle notation can be seen when considering, for example, the front right (edge) cubicle - is denoted by fr (or, equivalently, rf). Cubie notation can be seen when considering the left upper back (corner) cubie - denoted by: *lub* (or, equivalently, *lbu, bul, blu, ulb*, or *ubl*). The solved Cube represents the only case when all cubies are in their respective cubicles; so, for instance, in this caes, cubie *ldf* is in the cubicle ldf.

1.1.2. The Cube with Movement. For the simplest case possible, a "move" of the Rubik's Cube signifies a rotation of one of the 6 Rubik's Cube faces. We assume this rotation to be clockwise and in 90 degree increments, and identify such a rotation either F, L, R, U, D, B depending on which face is rotated (front, left, right, upper, down, and back, respectively). To be clear, taking the face F as example, F^2 would indicate a 180 degree clockwise rotation of the front face. F^3 would indicate a 270 degree clockwise rotation (which is equivalent to a 90 degree counterclockwise rotation F^{-1}) of the front face. F^4 would indicate a 360 degree clockwise rotation of the front face - which is equivalent to no movement of the front face at all.

Observe when we rotate the right face in any 90 degree increment, the center cubie does not move. We know, by definition, this is true of the center cubicle (and any cubicle for that matter); however, we see here that center cubies also remain fixed. Certainly, this is only true for the center cubies as the edge cubies and corner cubies move. However, equipped with this knowledge, we know then that to solve the cube, we must rotate edge cubies and corner cubies in such a way so as to match their colors to the color of the particular center cubie facelet (since the center cubies do not move). Certainly, we may need to use more than one move in a sequence, and so, we will refer to any possible sequence of move as a "process."

FIGURE 4.
Observe the center cubie of the front face (which is fixed) is white.

1.1.3. Home Positions. Consider the analogy of a home with regards to the cube in its solved state. Once the cubie is in its proper cubicle, then it is in its home location. Even more, once the cubie is in its proper cubicle and is properly oriented, then it is in both its home location and its home position. These, of course, are respective to the particular center cubies (depending on color). Note in the figure

above, the center cubie facelet of the front face is white. Thus, to get the cube in its solved state, all non-center cubies on the same face must also be white (i.e. they must return to their "white" home positions).

To further make this distinction, consider the following example.

EXAMPLE 1.1. Looking at the front face of the Cube, we observe we have 4 edge cubies, 4 corner cubies, and 1 center cubie. (Note, this is true of any and all of the 6 faces.) In the solved state, each of the 4 edge cubies (*fr, fu, fr, fd*) are in their respective cubicles (fr, fu, fr, fd). Additionally, in the solved state, each of the 4 corner cubies (*flu, fur, frd, fdl*) are in their respective cubicles (flu, fur, frd, fdl). And, of course, we also have, regardless of whether the cube is solved or not, that each center cubie is already in its center cubicle.

Referenced above in terms of the difference between home location and home position, we must acknowledge the fact that a cubie can be in its cubicle without being positioned correctly.

Recall the solved cube where white is our front face. We see in Figure 5 the front face (white), the left face (blue), and the upper face (red). As we look at the solved cube from a different angle (see Figure 6), we see the down face (orange) and the right face (green). Thus, we can assume that the back face is yellow.

Clearly, each of the cubies is in its cubicle; specifically with regards to the front face, we have *fr* is in fr, fu is in fu, *fr* is in fr, *fd* is in fd, *flu* is in flu, *flu* is in flu, *fur* is in fur, *frd* is in frd, *fdl* is in fdl, and, trivially, *f* is in f.

FIGURE 5.
Solved Cube

FIGURE 6.
Solved Cube seen from a different angle

Let us look more specifically at corner cubie *frd*, which we observe to be in the cubicle frd since the Cube is in its solved state. However, just because the cubie is in the cubicle (location is correct), does not mean it is positioned correctly within the cubicle. Consider Figures 7 and 8.

We see that after some rotations, the cube is no longer in its solved state. Where we have defined the front face by the center white cubie, we see that the cubies are not in the proper cubicles (i.e. are not in the home location). However, we see the cubie *frd* (which uniquely has one white facelet, one green facelet, and one orange facelet) that began in cubicle frd still retains its location (see Figures 7 and 8). However, clearly, the cubie is not in its proper position within the cubicle frd itself. Thus, it can be said that the cubie *frd* is in its home location, but not its home position.

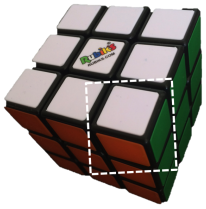


FIGURE 7.
Note the edge cubie: *frd* is in cubicle frd.

FIGURE 8.
Note the edge cubie: *frd* is **still** in cubicle frd.

Observe that for the Cube to be in its solved state, each cubie must be in its home location **and** its home position.

1.1.4. A Remark on Notation. Now that the various parts of the Rubik's Cube have been named and notation has been specified for cubie and cubicle, we must propose a notation by which we can communicate various moves/rotations of the cube. For an unsovled cube, we start with how to identify a cubie in a particular cubicle. Consider, the cubie *fdl* where the front facelet is white, the down facelet is orange (not shown), and the left facelet is blue and see that with a solved Cube, this cubie is in cubicle fdl (see Figure 9). After several movements of the cube, we ended up with the Cube as shown in Figure 10. We observe that the *fdl* cubie is no longer in cubicle fdl; instead, it is in cubicle ldb. Generally, since the piece in cubicle fdl is now (after several moves) in cubicle ldb. we can depict this as:

$$\text{fdl} \to \text{ldb}.$$

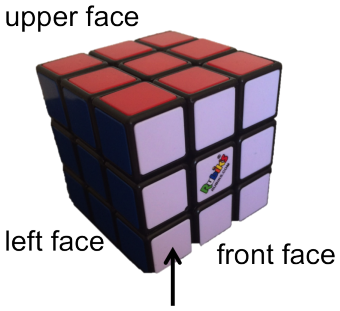


FIGURE 9.
Solved Cube

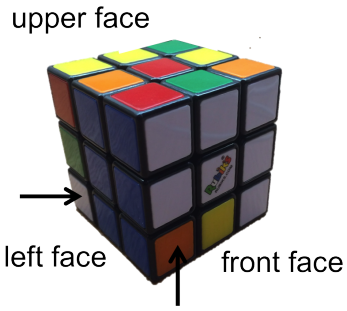


FIGURE 10.
Note that cubie *fdu* is not (located nor positioned) in cubicle fdu.

To express the movement of any cubie, we can write it in terms of the cubicles changing positions. Suppose we begin with the solved cube (see Figure 11) and perform an L^3 rotation. Figure 12 shows the result of this rotation. When we consider the particular cubie *fdl* and how it has been affected by this rotation, we see it moves from cubicle fdl to cubicle ufl. More generally, regardless of what cubie began in fdl, after an L^3 rotation, it will end up in cubicle ufl expressed as:

$$\text{fdl} \rightarrow \text{ufl: } L^3$$

FIGURE 11.
Solved Cube

FIGURE 12.
Note that cubie *fdu* is not (located nor positioned) in cubicle fdu.

Observe that notation precision comes into play again. Though we can express cubicle fdl as fdl, ldf, or dfl (following the clockwise convention), what we decide to name it following an L^3 rotation of the cubie in that cubicle affects what we call the cubicle that the cubie ends up in. Thus, in addition, to expressing the above rotation as fdl $\rightarrow$ ufl: L^3, we could also express it (equivalently) as:

$$\text{dlf} \rightarrow \text{flu: } L^3$$

or, as:

$$\text{lfd} \rightarrow \text{luf: } L^3 \quad .$$

However, in each, case we must be sure that we are precise so as to ensure that the facelets of the cubie are matched appropriately. In the case of fdl $\rightarrow$ ufl: L^3 as depicted in Figure 12, we see that the white facelet of cubie *fdl* goes from occupying the "f" part of the fdl cubicle to occupying the "u" part of the ufl cubicle. Similarly, the green facelet of *fdl* goes from occupying the "d" in fdl to "u" in ufl, and the orange facelet of *fdl* occupies the "l" position in both cubicles.

With all of this notation groundwork laid, we can consider the following example, with the understanding that a process is a sequence of moves carried out from left to right.

EXAMPLE 1.2. Consider a process UR^{-1}. We can describe what is going on by the movement of the cubies in particular cubicles. Recall, that for each individual move only affects 8 of the 26 cubies. Clearly, then, U affects all cubies on the upper face (excluding the center cubie) and R^{-1} affects all cubies on the right face (excluding the center cubie). Performing this process in order, (U then R^{-1}) we get a sequence

described by:

$$\begin{gathered}
\text{ufr} \to \text{ulf} \to \text{ulf} \\
\text{ur} \to \text{uf} \to \text{uf} \\
\text{uf} \to \text{ul} \to \text{ul} \\
\text{ufl} \to \text{ulb} \to \text{ulb} \\
\text{ul} \to \text{ub} \to \text{ub} \\
\text{fr} \to \text{fr} \to \text{dr} \\
\text{frd} \to \text{frd} \to \text{drb} \\
\text{dr} \to \text{dr} \to \text{br} \\
\text{rdb} \to \text{rdb} \to \text{rbu} \\
\text{rb} \to \text{rb} \to \text{ru} \\
\text{ubl} \to \text{urb} \to \text{fru} \\
\text{ub} \to \text{ur} \to \text{fr} \\
\text{ubr} \to \text{urf} \to \text{frd}
\end{gathered}$$

We observe that some cubies are affected by both rotations (the last three in the list) and some are only affected by one (the first ten in the list). Note that the cubies affected by none, we consider to be trivial and thus do not list.

Considering we have two face rotations (U and R^{-1}), we may wonder why there are only 13 movements and not 16. Because since the upper face and the right face share an edge, three cubies are affected by both movements (U and R^{-1}). Now, should we rotate faces opposite from each other on the cube (i.e. that have no cubies in common), such as R and L, then each rotation of either R or L affects 8 cubies. Thus, RL (or LR) would affect 16 cubies.

1.2. Rotating the Cube with Order

First, let us consider the following example in which we wish to restrict movement to edge cubies only.

EXAMPLE 1.3. Consider $L^2R^2U^2D^2F^2B^2$ as performed on the Cube in its solved state (see Figures 13 and 14).

FIGURE 13.
Start: Solved Cube

FIGURE 14.
After $L^2R^2U^2D^2F^2B^2$

Note that the white facelet of the front left upper (*ful*) cubie of Figure 13 has been marked with a black dot to help show the movement of the cubies (in which only edge cubies move).

This was a one-step process to obtain a Cube arrangement where only edge pieces moved. Recall that every odd number of times we repeat $L^2R^2U^2D^2F^2B^2$, we will get this arrangement. For every even number of times we repeat the process, the Cube will return to its original (solved) state.

DEFINITION 1.1. The **order of a process** on the Rubik's Cube is defined as the smallest number of times a process must be repeated before we return to our original state (i.e. the arrangement of the cube we started with). In the above example, we see that it takes us rotating the cube twice (with $L^2R^2U^2D^2F^2B^2$ as our process) to return to our original state (which, in this case, was the solved cube).

EXAMPLE 1.4. Now, suppose we wanted to find another process wherein only edge cubies move positions, but say we wanted this process to be of order 3.
Consider the process $RF^2B^2L^3F^2B^2$.

Observe (see Figures 15 and 16) for the front face, after carrying out the process once, the *fl* edge cubie is the only one that moves. (The back face (unseen) also only has one edge cubie that changes position.) For the left and upper faces, we see two edge cubies change positions (and the same is true for the right and down faces, though this is unseen in the figures).

When we carry out the process again (see Figure 17), we observe the same phenomena occurs (except this time the facelets of the moved edge cubies are of a different color).

And, lastly, when we carry out the process for a third time (see Figure 18), we find that we arrive back to the original cube, as desired.

FIGURE 15.
Start

FIGURE 16.
$RF^2B^2L^3F^2B^2$

FIGURE 17.
$(RF^2B^2L^3F^2B^2)^2$

FIGURE 18.
$(RF^2B^2L^3F^2B^2)^3$

Note that similar processes that only move edge cubies can be found of higher orders as can other processes of various orders, which, for example, may only move corner cubies.

CHAPTER 2

Introduction to Groups

Now that the Rubik's Cube groundwork has been laid, we may now proceed in laying the foundational aspects of group theory that we may then synthesize the two into a more collective whole.

2.1. Preliminaries

2.1.1. Permutations.

DEFINITION 2.1. Consider a set A. A **permutation** is function, $f : A \to A$ that is "one-to-one" and "onto". Recall for a function to be "one to one" we must have for all $a, b \in A$, $f(a) = f(b)$ implies $a = b$ and for a function to be "onto" we must have that for all $b \in A$, there exists $a \in A$ such that $f(a) = b$.

EXAMPLE 2.1. Consider the set $A = \{1, 2, 3, 4\}$. Let us define a function f, by $f(1) = 3$, $f(2) = 4$, $f(3) = 2$, and $f(4) = 1$. Per standard convention, then, we can express all elements of A with their respective outputs in an array:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

Note: This array represents one possible permutation of the set A.

More generally, for all $i_n \in A$ and a bijective function f, we can express a permutation in array form as

$$\begin{bmatrix} i_1 & i_2 & i_3 & ... & i_n \\ f(i_1) & f(i_2) & f(i_3) & ... & f(i_n) \end{bmatrix}$$

Notice that the first row of the array contains each element i_n of our set A. In the second row, each entry is an output, $f(i_n)$, of the element i_n (the input) that is directly above it (i.e. in the same column). Note that any array representing a permutation will have 2 rows and n columns (where n is the number of elements in A).

EXAMPLE 2.2. In the cases where we have more than one permutation to consider, we can compose the permutations in a single array. To do this, let us first consider the permutations X and Y:

$$X = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad Y = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$

To find the composite of the permutations X and Y, we first move "right to left" - beginning with Y and its first entry (in row 1): 1. Then we move "top to bottom" - observing $Y(1) = 1$. Then, continuing to move "right to left," we see $X((Y(1)) = X(1) = 2$. Following this same procedure, we get the following result for the composite,XY:

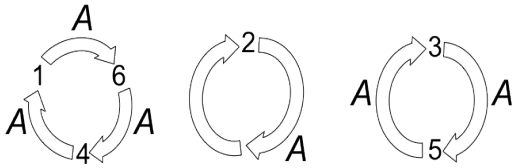
$$XY = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ X(Y(1)) & X(Y(2)) & X(Y(3)) \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}.$$

Another way of representing a particular permutation is through the use of cyclic notation. Cyclic notation is convenient because it expresses a permutation (and multiple cycles) in a more compact form. To understand this notation, let us consider the following example.

Example 2.3. Let A be the permutation:

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 5 & 1 & 3 & 4 \end{bmatrix}$$

To express this in cyclic notation, we would write (164)(2)(35). This short-hand notation represents the following behavior of the permutation:



We can understand this by thinking of the permutation as sending 1 to 6, 6 to 4, and 4 to 1, 2 to itself, 3 to 5 and 5 to 3. So, (164)(2)(35) is just one way of expressing this permutation in cyclic notation. Another, way would be (2)(416)(35), another would be (53)(2)(641), and yet another would be (35)(164) (with the underlying assumption that the permutation sends 2 to 2).

Generally, we call a "cycle" an **"m-cycle"** where m is the cycle length. So, from above, (14) would be a 2-cycle. Furthermore, recalling the permutation A from above, we can think of its 2-cycle (14) as sending 1 to 4 and 4 to 1 while fixing 2, 3, and 5 (as they are not in the cycle).

$$(14) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{bmatrix}$$

We can use the cyclic notation as we look to find products of permutations.

Example 2.4. Recall the permutation A from the previous example. Then define a new permutation B. We will find the composite, AB.

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 5 & 1 & 3 & 4 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 3 & 4 & 6 \end{bmatrix}$$

Rather than expressing the composite AB as (164)(2)(35)(1)(2)(354)(6), though this is accurate, we look for a "simpler" answer whereby we use *disjoint* cycles (i.e. where each cycle has no number in common). To do this, let us operate under the "right to left" convention of function composition used previously in this paper.

For example, moving right to left,

- **For 1:** 1 is fixed by (6), then is fixed by (354), then is fixed (2), then 1 is sent by (1) to 1, then is fixed by (35), then is fixed by (2), and then is sent by (164) to 6.
- **For 2:** 2 is fixed by (6), then is fixed by (354), then is sent by (2) to itself, then is fixed by (1), then is fixed by (35), then is sent by (2) to itself, and then is fixed by (164).
- **For 3:** 3 is fixed by (6) and then is sent by (354) to 5. Then, 5 is fixed by (2), then is fixed by (1), and then is sent by (35) to 3. Then, 3 is fixed by by (2) and then is fixed by (164).

We follow this procedure to obtain the product AB in disjoint cycle form as the array:

$$AB = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 5 & 1 & 4 \end{bmatrix}$$

In cyclic notation, then, AB= (1645)(2)(3), or, more simply, AB = (1645).

Notice here that this operation is **not** commutative. We found that AB = (1645). Solving for BA, we get BA = (1634). Clearly, then, $AB \neq BA$, and so, we know permutations do not (necessarily) commute.

We can apply this notion of permutations to the Rubik's Cube. Recall Example 1.2. Since there are only a finite number of cubicles (and thus repetitions must occur), we can also represent the process UR^{-1} by means of cycle representations (after repeated UR^{-1} rotations and noting that these cycles are disjoint):

(fu, lu, bu, rf, rd, rb, ru)(flu, lbu, urf)$_+$(bru, rdf, rbd)$_+$

We use the subscript $_+$ to communicate that we need to do a 120 degree clockwise rotation wherein the last piece returns to the first piece. So, for the cycle (flu, lbu, urf), we would expect urf to send us to flu upon a UR^{-1} movement. However, it sends us to ufl. So, we use $_+$ to indicate that the up face goes to the front face, the front face goes to the left face, and the left face goes to the up face - thus giving us flu, as desired.

2.2. Group Theory

We now turn from the notion of a permutation to the notion of a group, which, unsurprisingly, is the most fundamental concept in the field of Group Theory.

Let us begin by recalling the definition of a group.

Definition 2.2. Let G be a set with $a, b \in G$ and with a binary operation (denoted by *) that assigns to each ordered pair, (a, b) an element $a*b$ where $a*b \in G$. Then, G is a **group** if the following properties hold:

(1) *Closure*: For all $a, b \in G$, the product $a * b \in G$
(2) *Associativity*: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
(3) *Identity*: There exists $e \in G$ such that $a * e = a \in G$. (e is called the *identity element.*)
(4) *Inverses*: For all $a \in G$, there exists $b \in G$ such that $a * b = b * a = e^G$. (b is called the *inverse* of a.)

EXAMPLE 2.5. To illustrate this, let us consider the set $\mathbb{R}$ and prove $\mathbb{R}$ is a group under addition. So, let $G = \mathbb{R}$.

(1) *Closure*: The sum of any real numbers will be a real number. That is, the quantity $a + b \in G$, for all $a, b \in G$.
(2) *Associativity*: The order we add real numbers doesn't matter. That is, $(a + b) + c = a + (b + c)$, for all $a, b, c \in G$.
(3) *Identity*: 0 is the additive identity for the real numbers since adding 0 to a real number gives us that number. That is, $a + 0 = a$, for all $a \in G$.
(4) *Inverses*: Adding the "negative" of a real number to that real number gives us the identity element, 0. That is, for all $a \in G$, there exists $b \in G$ such that $a + b = 0$. This is true when $b = -a$ (i.e. when b is the inverse of a).

Thus, the set $\mathbb{R}$ is a group under addition!

EXAMPLE 2.6. Let us now consider a set that is not a group: the set $\mathbb{Z}$ with the operation of multiplication. So, let $G = \mathbb{Z}$.

(1) *Closure*: The product of any integers will be an integer. That is, the quantity $ab \in G$, for all $a, b \in G$.
(2) *Associativity*: The order we multiply integers doesn't matter. That is, $(ab)c = a(bc)$, for all $a, b, c \in G$.
(3) *Identity*: 1 is the multplicative identity for the integers since multiplying 1 to any integer gives us that integer. That is, $(a)(1) = a$, for all $a \in G$.
(4) *Inverses*: We want to find an integer such that we can multiply it by another integer to get the identity. That is, we want to find an element $b \in G$ such that, for all $a \in G, ab = 1$. However, this cannot be done. Without loss of generality, let $a = 3$. The only way to get $ab = 1$ is if $b = 1/3$. However, $1/3$ is not an integer. Thus, the inverse property does not hold.

Thus, the set $\mathbb{Z}$ is **not** a group under multiplication!

2.2.1. The Cube as a Group. Recall the definition of a group in Section 1.2 (see Definition 1.3). We want to show the Rubik's Cube is a group, and to do this, we let it be generated be the six moves: R, L, U, D, B, F, and we let our binary operation be a sequence of moves. Processes, composed of one move or multiple moves, are elements of our group.

(1) *Closure*: For any moves X and Y in the Rubik's Cube, the process XY produces a possible arrangement of the Cube. In other words, performing moves will never give us something other than a possible result in the Cube, and so, closure holds.

(2) *Associativity*: Let X, Y, and Z be elements of our Rubik's Cube group (i.e. they are moves R, L, U, D, F, or B). We want to show $(XY)Z = X(YZ)$. For the LHS, (XY) means rotating face X, then rotating face Y. Then to get to $(XY)Z$ we would rotate face Z. For the RHS, first we rotate face X, then we deal with (YZ) which requires we then rotate face Y and then after, we rotate face Z. Clearly, then, LHS= RHS and associativity holds.
(3) *Identity*: We want to find a possible move for a face of the cube that gives us back that same face. Clearly, this "move" would be either no move at all (0 degrees), or, equivalently, rotating the face in any multiple of 360 degrees (as the same permutation would result). This, then, is our identity element, I.
(4) *Inverses*: Let X be any move (R, L, U, D, F, or B). We aim to show that there exists another move, Y, whereby $XY = YX = I$. Upon being rotated 90 degrees in a clockwise fashion by means of X, to get back to the starting point we would undo X by rotating the face X acted upon by -90 degrees or some multiple of it. (Equivalently, some multiple of 270 degrees would yield the same permutation.)

2.2.2. More on The Inverse. Note that for processes to be equivalent, their inverse processes must be equivalent (and vis versa). For each process, there is more than one process which produces its inverse permutation (see Example 3.1).

Example 2.7. Suppose we start with the solved Cube and perform R. We want to find R^{-1} whereby we would return to the original state where all cubies are in their home positions and locations in the cubicles. Obviously, since R requires we rotate the right face 90 degrees clockwise, we can undo this by rotating the right face 90 degrees counterclockwise (i.e. perform R^{-1}). However, we could also rotate R 270 degrees clockwise (i.e. perform R^3) and obtain our desired result. Certainly, we can extend this logic should our process involve more than one step, and thus, we've shown there is not just one unique inverse to each process (regardless of the number of moves within the sequence of the process).

Additionally, we see that any permutation produced by a process followed by its inverse is the identity. Symbolically: $X(X^{-1}) = I$, where X is a legal move and I is the Identity (i.e. the arrangement that we began with before performing any moves).

2.2.2.1. *Inverses of Permutations.* To solidify our understanding of the notion of taking the inverse of a permutation, we will consider a few examples. However, before doing so, let's remind ourselves of the **socks and shoes principle**, which says the inverse of putting on socks then putting on shoes is taking off shoes and then taking off socks.

Example 2.8. Let A, B, C, D be legal moves of the Cube. Observe:
$(A,B)^{-1} = (B^{-1}, A^{-1}$ (or, equivalently, $(A^{-1}, B^{-1}))$
$(A,B,C)^{-1} = (C^{-1}, B^{-1}, A^{-1})$
$(A,B,C,D)^{-1} = (D^{-1}, C^{-1}, B^{-1}, A^{-1})$
Generally, $(X_1, X_2, X_3, ..., X_{n-1}, X_n)^{-1} = (X_n^{-1}, X_{n-1}^{-1}, ..., X_3^{-1}, X_2^{-1}, X_1^{-1})$

Example 2.9. Let A, B, C, D, and E be legal moves of the Cube. Suppose we wanted to find the inverse of the permutation with two disjoint cycles: (A,B)(C,D,E). Let's name the first cycle, (A,B), α and the second cycle, (C,D,E), β. So now we are looking at $\alpha\beta$. Finding the inverse of this, by the socks and shoes principle, we get:

$$(\alpha\beta)^{-1} = (\beta)^{-1}(\alpha)^{-1}.$$

Then,

$$(\beta)^{-1}(\alpha)^{-1} = (\mathrm{C,D,E})^{-1}(\mathrm{A,B})^{-1} = (\mathrm{E}^{-1},\mathrm{D}^{-1},\mathrm{C}^{-1})(\mathrm{B}^{-1},\mathrm{A}^{-1}).$$

So, altogether,

$$((\mathrm{A,B})(\mathrm{C,D,E}))^{-1} = (\mathrm{E}^{-1},\mathrm{D}^{-1},\mathrm{C}^{-1})(\mathrm{B}^{-1},\mathrm{A}^{-1}).$$

2.2.3. Groups and Commutativity. Anytime we are considering groups, the question of commutativity, or "Abelianness" arises.

Definition 2.3. A group, G, is called **Abelian** if $\forall a, b \in G, a * b = b * a$. Otherwise, we say G is non-Abelian.

As it pertains to the Rubik's Cube, we want to know whether or not any two moves commute. In other words, for any moves, X and Y, does $XY = XY$?

Assume we start with the Rubik's Cube in it solved state where we set the green face on the right, the blue face on the left, the red face is up, the orange face is down, the white face is in front, and the yellow face is in the back. Consider the following example.

Example 2.10. Consider the processes X and Y as being LR and $\mathrm{L}^{-1}\mathrm{R}^{-1}$, respectively. We want to see if commutativity holds; in other words, does XY=YX?

We see, XY = (LR)($\mathrm{L}^{-1}\mathrm{R}^{-1}$) and YX = ($\mathrm{L}^{-1}\mathrm{R}^{-1}$)(LR). Note that the processes X and Y only involve movement of cubies to/from the left face and right face of the cube as the other cubies are left unaffected. Further, observe that the left and right faces share no cubies and so movement of the left face has no impact on any cubies of the right face (and vis versa). Thus, we have that for this case, commutativity holds (i.e. XY=YX).

This example offers us insight into opposite faces of the cube. Certainly, we know the pairs of opposites are: left/right, upper/down, and front/back. However, since we know, the Cube consists solely of the colors red, blue, green, white, yellow, and orange, each color occupies a particular face at one time, and the center cubies do not move, we know that certain colors will always be opposite each other on the cube (as determined by the color of the center cubies).: white and yellow, blue and green, and red and orange.

Example 2.11. Now let us consider the following example of moving R (i.e. rotating the right face 90 degrees clockwise) and then U (i.e. rotating the upper face 90 degrees clockwise), and also, moving U and then R.

Clearly, these are not the same results. Thus, $RU \neq UR$, and so, the Rubik's Cube group is **non-Abelian**, even though sometimes, in certain cases, commutativity does hold. This is significant because it tells us the order in which we perform our moves matters (usually)!

FIGURE 1. Result of RU

FIGURE 2. Result of UR

2.2.3.1. *Commutators.* Even though, we've shown that the Rubik's Cube group as a whole is non-Abelian, it can be shown that certain elements (i.e. moves) within the group commute with one another. Certainly, we can see trivially that R and L commute, U and D commute, and F and B commute since neither pair shares any elements in common and so the order we perform the moves in does not change our final result.

In our previous discussions regarding the inverse, we showed that there exists an inverse for any possible move on the Cube, and that the inverse of cycles $\alpha\beta$ is $(\beta)^{-1}(\alpha)^{-1}$ So, considering the process BR, which we know does not commute, we see that the inverse is $R^{-1}B^{-1}$:

$$(BR)(BR)^{-1} = BR(R^{-1}B^{-1}) = I, \text{ where I is the identity.}$$

Implicitly, then, $B^{-1}R^{-1}$ is not the inverse of BR:

$$(BR)(B^{-1}R^{-1}) \neq I.$$

However, we need not dismiss $B^{-1}R^{-1}$. Rather, we can employ it in consideration of the process $BRB^{-1}R^{-1}$, in which we identify it as what is called a commutator. In general, for an arbitrary group G, we define:

DEFINITION 2.4. The **commutator subgroup** G' of a group G is the subgroup generated by the set $\{x^{-1}y^{-1}xy \mid x, y \in G\}$.

A commutator in the Rubik's Cube, denoted [X,Y] is any product that takes the form $XYX^{-1}Y^{-1}$ where X and Y are two elements of the group (i.e. moves on the Cube). The only time when $XYX^{-1}Y^{-1} = I$ is if the elements commute, and vis versa, if the elements commute, then we are guaranteed to have $XYX^{-1}Y^{-1} = I$.

DEFINITION 2.5. The **center**, $Z(G)$, of a group G is the subset of elements in G that commute with every element in G:

$$Z(G) = \{a \in G \mid ax = xa \ \forall \ x \in G\}.$$

THEOREM 2.1. *If a group $G = < a_1, a_2, \ldots, a_m >$ and x commutes with the product $a_1a_2\ldots a_m$ then $x \in Z(G)$.*

PROOF. We will show for all $h \in$ in G, $hx = xh$. Let $h \in G$ where $h = a_{t_1}a_{t_2}\ldots a_{t_k}$. Inducting on n, we proceed.

Base Case: When $k = 0$, there are no generators in our product. Thus, we are left with the empty set, which in this case, is the identity. So, $h = e_G$ and clearly, any element commutes with the identity:

$$e_G h = h e_G.$$

Inductive Step: Suppose we know the result for $k = n$. That is, x commutes with $h \in G$ such that h=$a_{t_1} a_{t_2} ... a_{t_n}$ (for some choice of t_i's). We aim to show that the result holds for $k = n + 1$, namely that x commutes with $h \in G$ where

$$h = a_{t_1} a_{t_2} ... a_{t_n} a_{t_{n+1}}.$$

For the sake of clarity, we can express h in the following way:

$$h = h' a_{t_{n+1}}, \text{ where } h' = a_{t_1} a_{t_2} ... a_{t_n}$$

By our inductive hypothesis, we know that x commutes with h'. By definition, $a_{t_{n+1}}$ is one of the a_k's, and so, is a generator of the group that we know commutes with x. Since h=h'$a_{t_{n+1}}$ and x commutes with both h' and $a_{t_{n+1}}$, then we get the following:

$$\begin{aligned} hx &= (h' \mathrm{a}_{t_{n+1}})x \\ &= h'(\mathrm{a}_{t_{n+1}} x) \\ &= h'(x \mathrm{a}_{t_{n+1}}) \\ &= (h'x)\mathrm{a}_{t_{n+1}} \\ &= (xh')\mathrm{a}_{t_{n+1}} \\ &= x(h' \mathrm{a}_{t_{n+1}}) \\ &= xh. \end{aligned}$$

Clearly, x and h commute, as desired. Thus, we've proven the result for $k = n + 1$ and the induction step is complete. Thus, we can now conclude, by the principle of induction, that if G is generated by {a_1,a_2,...,a_m} and x commutes with the product $a_1 a_2 ... a_m$ $(= h)$ then $x \in Z(G)$ (i.e. $xh = xh, \forall x \in G$). □

2.2.4. Order.

Definition 2.6. Generally, a **symmetric group** is defined as containing *all* possible permutations of a set A. It is expressed as S_n where n is the degree or number of elements. Each permutation in S_n is of the form:

$$Z = \begin{bmatrix} 1 & 2 & ... & n-1 & n \\ Z(1) & Z(2) & ... & Z(n-1) & Z(n) \end{bmatrix}$$

Let us look at the case when $n = 3$, that is, where there are three elements in our set. Let our set be A and let $A = 1, 2, 3$. Thus, we see the group S_3 consists of the following elements:

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

We can also represent these elements in cyclic notation:

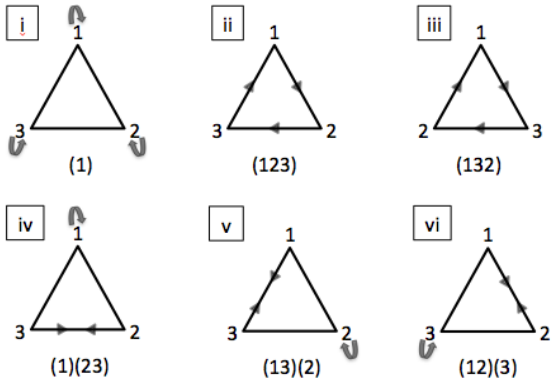
(1), (12), (23), (13), (123), (132).

Definition 2.7. The **order of a group** (also known as the cardinality) is defined as the number of elements in a group. We denote the order of a group, G, by $|G|$.

When we are dealing with S_n, we know there are n elements in our set. To find the order of the group, S_n, that is the number of elements (i.e. permutations) in our group, we again consider the generic permutation Z that has n elements:

$$Z = \begin{bmatrix} 1 & 2 & ... & n-1 & n \\ Z(1) & Z(2) & ... & Z(n-1) & Z(n) \end{bmatrix}$$

For $Z(1)$ there are n possible options $\{1, 2, ..., n-1, n\}$. For $Z(2)$, then, there are $n-1$ possible options (all the elements minus the one we chose previous (for Z(1)). This continues until finally for Z(n), we find that there is one possibility. Altogether, then, we see there are $n(n-1)...(2)(1) = n!$ possible elements of the set Z. Thus, more generally, the order of any symmetric group S_n is n!. This is why we have exactly 6 elements in S_3 (i.e. $|S_3| = 6$). These 6 elements can be found by considering a triangle, and its possible manipulations (i.e. rotations, reflections).



In addition to this notion of the order of a group, we also have the notion of the order of a particular element defined as follows.

Definition 2.8. The **order of an element x** in a group G, denoted $|x|$, is the smallest positive integer n such that $g^n = e_G$. Should no such integer exist, then the group has infinite order. See Example 2.12.

2.3. Generating a Group

Definition 2.9. For $a \in G$, we define $< a > = \{a^n \mid n \in \mathbb{Z}\}$. We call this the **subgroup generated by one element.**

Example 2.12. Consider $(123) \in S_3$. Then,

$$\begin{aligned} < (123) > &= \{(123), (123)^2, (123)^3, ...\} \\ &= \{(123), (123)(123), (123)(123)(123), ...\} \\ &= \{(123), (132), (1)\}. \end{aligned}$$

We are only left with three elements in the subgroup $< a >$ even though we take (123) to any and all powers, n where $n \in \mathbb{Z}$. This is the case because, when $n > 3$, we will be working with at least one of the permutations previously considered. For example, let us consider $(123)^5$.

$$\begin{aligned} (123)^5 &= (123)^2(123)^3 \\ &= (123)^2(1). \\ &= (123)(123) \end{aligned}$$

$$= (132)$$

Note, (132) is clearly one of the three elements originally generated by (123)).

For any group element, we can prove $< a >$ is a subgroup by using the Two-Step Subgroup Test, which says, for G, a group and H, a non-empty subset of G, if $ab \in H$ whenever $a, b \in G$ (H is closed under the operation) and if $a^{-1} \in H$ whenever $a \in H$ (H is closed under taking inverses), then H is a subgroup of G.

PROOF. We begin by observing $< a >$ is a non-empty subset of a group G (since $a^0 = e_G \in G$). Letting $x, y, \in < a >$, we proceed.

First, we need to show $xy \in < a >$. To do this, let us first express x as a^i and y as a^j (where $i, j \in \mathbb{Z}$). Thus, we have:

$$xy = a^i a^j = a^{(i+j)}$$

But, we know that $\mathbb{Z}$ is closed under addition, and so, $(i + j) \in \mathbb{Z}$. Thus, we have that $xy = a^{(i+j)}$ is an element of $< a >$, as desired.

Now, need to show $x^{-1} \in < a >$. To do this, again, let $x = a^i$ (where $i \in \mathbb{Z}$). We want then to show there exists an element $z \in < a >$ such that:

$$a^i z = e_G.$$

We can express the relationship this way because we know an element and its inverse yield the identity, and we know, by definition of a group, there always exists an identity element of a group, e_G. So then, let $z = a^{-i}$. We know that for any $i \in Z$, $-i \in Z$, and so, z is an element of $< a >$, as desired. □

We do not need, however, to limit ourselves to the consideration of a subgroup generated by only one group element.

DEFINITION 2.10. For $a, b \in G$, we define $< a, b > = \{a^n b^m \mid m, n \in \mathbb{Z}\}$, which we call the **subgroup generated by two elements.**

EXAMPLE 2.13. Letting (123) and (12) $\in S_3$. Then,

$$\begin{aligned} < (123), (12) > = &\{(123), (123)^2, (123)^3, (12), (12)^2, (123)(12), (12)(123), (123)^2(12), \\ &(12)(123)^2, (123)^3(12), (12)(123)^3, (123)(12)^2, (12)^2(123), \ldots\} \\ = &\{(123), (132), (1), (12), (1), (13), (23)\} \end{aligned}$$

We see that regardless of what powers we raise (123) and (12) to and regardless of how we compose them, <(123),(12)> has (exactly) 6 elements.

Further, these six elements are ones we have seen before as they are the exact elements of the S_3 group! Because of this, we say that the elements (123) and (12) **generate** the group S_3 (recall results of Section 2.2.4).

DEFINITION 2.11. More generally, if $< a >= G$, then we say a **generates** G. Similarly, if $< a, b >= G$, then we say a and b **generate** G.

THEOREM 2.2. *Lagrange's Theorem*
If G is a finite group and H is a subgroup of G. then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.

DEFINITION 2.12. First, we will need to introduce the notion of a coset, specifically the left coset. The **left coset of H in G containing a**, denoted aH, is the set $\{ah|h \in H\}$ where H is a subgroup of a group G and $a \in G$. We can express this equivalently as $Ha = \{ha|h \in H\}$ or as $aHa^{-1} = \{aHa^{-1}|h \in H\}$.

PROOF. Now we proceed by letting $a_1H, a_2H, ..., a_rH$ denote distinct left cosets of a subgroup H of a group G. For each, $a \in G$, $aH = a_iH$ for some i. By properties of cosets, we also have that $a \in aH$. So, each element of G is contained one of our a_iH cosets:

$$G = a_1H \cup a_2H \cup ... \cup a_rH \quad .$$

By properties of cosets, we also have that this union is disjoint. This gives us that the order of G (i.e. all the elements of G) is the sum of the orders of the cosets:

$$|G| = |a_1H| + |a_2H| + ... + |a_rH|.$$

Lastly, since each coset has the same number of elements in it as the subgroup (i.e. $|a_iH| = |H|$ for each i), we have that $|G| = r|H|$. That is, that the order of the subgroup H divides the order of the group G. □

As it pertains to order and generators, it will be helpful to show $|x| = | < x > |$, i.e. for an element of finite order n, the subgroup generated by that element also has order n (recall Definition 2.8).

THEOREM 2.3. *Generally, for an element x in a group G that has finite order, n, then $< x >= \{e, x, x^2, x^3, ..., x^{n-1}\}$ and $x^i = x^j$ if and only if n divides $i - j$.*

PROOF. Let $x \in G$ where G is a group.
To begin, assume $|x| = n$ where $n \in \mathbb{Z}^+$. First, we will show that this implies:

$$< x >= \{e, x, x^2, x^3, ..., x^{n-1}\}.$$

Let $x^k \in < x >$. By the division algorithm, we get:

$$k = qn + r \text{ where } 0 \leq r \leq n - 1.$$

Thus,

$$x^k = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = (e_G)x^r = x^r \quad .$$

This implies $x^k \in \{e_G, x, x^2, ..., x^{n-1}\}$ (since $0 \leq r \leq n - 1$). Therefore, we have now shown $< x >= \{e_G, x, x^2, ..., x^{n-1}\}$, as desired. In other words, $|x| = | < x > |$.
Now, we assume $x^i = x^j$ where $i, j \in \mathbb{Z}^+$. We want to show n divides $(i - j)$. To do this, let us multiply the equation, $x^i = x^j$ by x^{-j}. Then we see:

$$x^i x^{-j} = x^j x^{-j}$$
$$x^{i-j} = e_G.$$

Using the division algorithm again, we have there exists q, r such that $(i-j) = qn+r$ where $0 \leq r \leq n - 1$. Then,

$$e_G = x^{i-j} = (x^{qn})(x^r = (x^n)^q(x^r) = e_G x^r = e_G x^r = x^r \quad .$$

Since, by definition of order, n is the smallest positive integer such that $x^n = e_G$, we must get $r = 0$ so that we get our desired result: n divides $i - j$.
Lastly, it remains to be shown that if n divides $i - j$ then $x^i = x^j$. To do this, let us assume n does, in fact, divide $i - j$. That is, there exists an element p such that $(i - j) = mn$. Then,

$$x^{i-j} = x^{mn} = (x^n)^m = (e_G)^m = e_G.$$

From this, we get the following:

$$e_G = x^{i-j} = (x^i)(x^{-j})$$
$$(x^i)(x^{-j})(x^j) = (e_G)(x^j)$$
$$(x^i) = (x^j).$$

This is our desired result. And so, altogether, we have shown for an element x of finite n order, $|x| = | < x > | = n$ since $< x >= \{x, x^2, ..., x^{n-1}\}$, and we have shown $x^i = x^j$ if and only if n divides $i - j$. □

2.3.1. Generating on the Cube.

Example 2.14. Now, we can take this notion of a subgroup generated by one element and apply it the Rubik's Cube. Consider <U>.

$$<U> = \{I, U, U^2, U^3\}$$

Thus, | <U> | = 4 as there are only 4 unique elements generated by <U>.

Example 2.15. We can also consider a subgroup generated by two elements: $<U^2, D^2>$.

$$<U^2, D^2> = \{I, U^2, D^2, U^2D^2\}$$

Thus, $| <U^2, D^2> | = 4$ as there are only 4 unique elements generated by $<U^2,D^2>$.

Example 2.16. Consider now a subgroup generated by two elements that has more elements in it: $<U^2, D^2>$.

<U, D> =

{ I, U, U^2, U^3, D, D^2, D^3, UD, UD^2, UD^3, U^2D, U^2D^2, U^2D^3 U^3D, U^3D^2, U^3D^3 }

Thus, | <U, D> | = 16.

In all three of these examples, the order we perform the moves does not matter. For instance, RR^2=R^2R (Example 1.8), $U^2D^2 = D^2U^2$ (Example 1.10), and $U^3D^2 = D^2U^3$ (example 1.11). In each of these cases, because the moves share no cubies in common, the order we perform the moves does not matter. These are examples of commutative elements within the Rubik's Cube. We will discuss later whether this is always the case, that is, whether or not commutativity always holds for any moves of the Cube.

At this point, we may observe a pattern amongst these examples and consequently we might conjecture that:

Conjecture 2.1. *For all $x, y \in G$, if $xy = yx$, then $| < x, y > | = |x||y|$.*

For moves (i.e elements) U and U^2 of our Rubik's Cube group, let us consider $<U,U^2>$. First, note U and U^2 do commute. Then, recall we showed in Example 1.8 $|U| = 4$, and it can easily be seen that $|U^2| = 2$. Thus, $| <U,U^2> |=(4)(2)=8$. However, $<U,U^2>= \{I, U, U^2, U^3\}$, and so, $| <U,U^2> | = 4 \neq 8$.

This happens because <U> and $<U^2>$ have elements in common, and so, when we find $| < U, U^2 > |$ by finding the product $|U||U^2|$, we over-count. To better illustrate this, suppose <U> has x unique elements, $<U^2>$ has y unique elements, and, together, they have z elements in common. So $|U| = x + z$ and $|U^2| = y + z$. If we

were to calculate | <U,U^2> | by |U||U^2|, we'd be (incorrectly) counting the elements z twice. Thus, the only time our conjecture holds is when, z is zero - when the two sets have no elements in common. In other words, the results hold when the elements commute.

What we do see in this example, though, is that | <U,U^2> | = 4 divides $lcm(|U|,|U^2|) = 8$. So, let us amend our previous conjecture by issuing the following:

CONJECTURE 2.2. *For all $x, y \in G$, if $xy = yx$, then $| < x, y > |$ divides $lcm(|x|, |y|)$.*

PROOF. Let $g, h \in G$ where G is a group that is Abelian (see Definition 2.3). Suppose $|g| = m$ and $|h| = m$ where $m, n \in \mathbb{Z}^+$. We want to show $| < g, h > |$ divides $lcm(|g|, |h|) = lcm(m, n)$. For the sake of clarity and convenience, let $lcm(mn,) = x$. Now, we see the following two possible cases:

(1) $|g| \leq |h|$ (i.e. $m \leq n$) and, by the definition of lcm, x is a multiple of n.
(2) $|g| \geq |h|$ (i.e. $m \geq n$) and, by the definition of lcm, x is a multiple of m.

Without loss of generality, let us first consider Case 1. *So, want to show $| < g, h > |$ divides x.* To begin, we know

$$< g >=\{e_g, \text{ g, } g^1, \text{ } g^2, \text{ ..., } g^{(m-1)}\} \text{ and } < h >=\{e_h, \text{ h, } h^1, \text{ } h^2, \text{ ..., } h^{(n-1)}.\} .$$

Suppose a of the elements of $< g >$ are unique to $< g >$ and b elements of $< h >$ are unique to $< h >$. Then, suppose $< g >$ and $< h >$ have c elements in common where $0 \leq k \leq m$ (since $|g| = m$ and $|g| \leq |h|$). Thus,

$$| < g > | = a + c = m \text{ and } | < h > | = b + c = n.$$

To try to find $| < g, h > |$, we begin counting the unique elements of $< h >$ and $< g >$, namely, $a + b$. Then, we only need to count c, the elements in common, once. Let these c elements be contributed to by $< h >$ and not by $< g >$. So, we see:

$$| < g, h > | = (|g| - y)|h| = (a)(bc) = (m - y)n. .$$

Clearly, then, since $| < g, h > |$ is a multiple of n and x is a multiple of n, $| < g, h > |$ divides x, as desired. A similar argument can be made for Case 2, and so, altogether, we have shown for any elements g and h in some Abelian group, G where $|g| = m$ and $|h| = m$, $| < g, h > |$ divides $lcm(|g|, |h|)$. □

Note, that when G is not Abelian, this result does not hold as can be seen in the following counterexample.

EXAMPLE 2.17. Let R^2 and U^2 be the elements in our Cube group. Then,

<R^2>={I, R^2}, and so, | <R> |=2.
<U^2>={I, U^2}, and so, | <U> |=2.

When we perform R^2U2, we see that it was no until we performed the process six times, that we returned to the identity. Thus, $(R^2U^2)^6 = I$, and so, $|R^2U^2| = 6$.

Thus, $lcm($<R>, <U>$) = 2$, and clearly, | <R^2U2> |=6 does not divide 2. Thus, the conjecture does not hold for elements that do not commute (e.g. R^2 and U^2).

CHAPTER 3

Group Actions

Now, we can take a look at, what some mathematicians believe, is one of the most crucial results in Group Theory: the notion of group actions.

DEFINITION 3.1. Let G be a group and let X be a set. A **group action** of G on X is a function $f : G \times X \to X$ such that the following two properties are satisfied:

(1) $e \cdot x = x$, $\forall x \in X$
(2) $(gh) \cdot x = g \cdot (h \cdot x)$, $\forall\ g, h \in G$ and $x \in X$. (Note, gh represents the "product" of the elements g and h in G.)

EXAMPLE 3.1. Let $G = \mathbb{R}$. Then, let G act on the points in the plane $X = \mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$, where $r \in \mathbb{R}$ and $(x, y) \in X$.

PROOF. We need to show the two properties, (1) and (2), are satisfied.

(1) Let $(x, y) \in X$. Then,

$$\begin{aligned} e_G \cdot (x, y) &= (x + e_G y,\ y) \\ &= (x + (0)(y),\ y), \text{ (since } e_G = 0) \\ &= (x,\ y) \end{aligned}$$

(2) We want to show $(gh) \cdot (x, y) = g \cdot (h \cdot (x, y))$ for all $g, h \in G$ and for all $(x, y) \in X$. So, let $g, h \in G$ and $(x, y) \in X$. Then, consider the LHS and the RHS:

LHS:

$$\begin{aligned} (gh) \cdot (x, y) &= (g + h) \cdot (x, y) \\ &= (x + (g + h)y, y) \end{aligned}$$

RHS:

$$\begin{aligned} g \cdot (h \cdot (x, y)) &= g \cdot (h \cdot (x, y)) \\ &= g \cdot (x + hy, y) \\ &= (x + hry + gy,\ y) \\ &= (x + y(h + g), y) \\ &= (x + (g + h)y,\ y) \end{aligned}$$

We can do this last step because we have that associativity holds ($\mathbb{R}$ is a group), and we know that commutativity holds for $\mathbb{R}$ under addition. Clearly, then, LHS=RHS. Thus, we have that $\cdot$ is a group action of G on X. □

EXAMPLE 3.2. A group G acts on itself (i.e. the set X is also G) whereby G acts on G with the operation $(g \cdot x) = gxg^{-1}$, where $g, x \in G$.

PROOF. We need to show the two properties, (1) and (2), are satisfied.

(1) Let $x \in G$. Then,

$$\begin{aligned} e_G \cdot x &= (\mathrm{e}_G)x(\mathrm{e}_G)^{-1} \\ &= x \text{ (since } e_G\text{= 1 and } {e_G}^{-1} = e_G = 1). \end{aligned}$$

(2) We want to show $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h, x \in G$. So, let $g, h \in G$ and $x \in X$. Then, consider the LHS and the RHS:

LHS:

$$\begin{aligned} (gh) \cdot x &= (gh)x(gh)^{-1} \\ &= ghxh^{-1}g^{-1} \end{aligned}$$

RHS:

$$\begin{aligned} g \cdot (h \cdot x) &= g \cdot (hxh^{-1}) \\ &= g(hxh^{-1})g^{-1} \\ &= ghxh^{-1}g^{-1} \end{aligned}$$

Clearly, LHS=RHS. Thus, we have that $\cdot$ is a group action of G on G.

□

EXAMPLE 3.3. Let G =($\mathbb{R}$,+) and $r \in G$. Then, let G act on set X of functions $f(x)$ of a real variable by:

$$\textit{(i)}\ r \cdot f(x) = f(x + r)$$
$$\textit{(ii)}\ r \cdot f(x) = f(x)e^r$$

but **not** by:

$$\textit{(iii)}\ r \cdot f(x) = f(xe^r + r).$$

PROOF. For each, we need to show the two properties, (1) and (2), are satisfied. For *(i)*:

(1) Let $f(x) \in X$. Then,

$$\begin{aligned} e_G \cdot f(x) &= f(x + e_G) \\ &= f(x + 0) \text{ (since } e_G\text{=0)} \\ &= f(x) \end{aligned}$$

(2) We want to show $(gh) \cdot f(x) = g \cdot (h \cdot f(x))$ for all $g, h \in G$ and for all $f(x) \in X$. So, let $g, h \in G$ and $f(x) \in X$. Then, consider the LHS and the RHS:

LHS:

$$\begin{aligned} (gh) \cdot f(x) &= (g + h) \cdot f(x) \\ &= f(x + g + h) \end{aligned}$$

RHS:

$$\begin{aligned} g \cdot (h \cdot f(x)) &= g \cdot (f(x + h)) \\ &= f(x + h + g) \\ &= f(x + g + h) \end{aligned}$$

We can do this last step because we have that commutativity holds for $\mathbb{R}$ under addition. Clearly, then, LHS=RHS. Thus, we have that $\cdot$ is a group action of G on X.

For *(ii)*:

(1) Let $f(x) \in X$. Then,

$$\begin{aligned} e_G \cdot f(x) &= f(x)e^{e_G} \\ &= f(x)e^0 \text{ (since } e_G{=}0) \\ &= f(x) \end{aligned}$$

(2) We want to show $(gh) \cdot f(x) = g \cdot (h \cdot f(x))$ for all $g, h \in G$ and for all $f(x) \in X$. So, let $g, h \in G$ and $f(x) \in X$. Then, consider the LHS and the RHS:

LHS:

$$\begin{aligned} (gh) \cdot f(x) &= (g+h) \cdot f(x) \\ &= f(x)e^{g+h} \end{aligned}$$

RHS:

$$\begin{aligned} g \cdot (h \cdot f(x)) &= g \cdot (f(x)e^h) \\ &= (f(x)e^h)e^g \\ &= f(x)e^{h+g} \\ &= f(x)e^{g+h} \end{aligned}$$

We can do this last step because we have that commutativity holds for $\mathbb{R}$ under addition. Clearly, then, LHS=RHS. Thus, we have that $\cdot$ is a group action of G on X.

For *(iii)*:

(1) Let $f(x) \in X$. Then,

$$\begin{aligned} e_G \cdot f(x) &= f(xe^{e_G}{+}e_G) \\ &= f(xe^0{+}0) \text{ (since } e_G{=}0) \\ &= f(x) \end{aligned}$$

(2) We want to show $(gh) \cdot f(x) = g \cdot (h \cdot f(x))$ for all $g, h \in G$ and for all $f(x) \in X$. So, let $g, h \in G$ and $f(x) \in X$. Then, consider the LHS and the RHS:

LHS:

$$\begin{aligned} (gh) \cdot f(x) &= (g+h) \cdot f(x) \\ &= f(xe^{g+h} + g + h) \end{aligned}$$

RHS:

$$\begin{aligned} g \cdot (h \cdot f(x)) &= g \cdot (f(xe^h{+}h) \\ &= f((xe^h{+}h)(e^g) + g) \\ &= f(xe^{g+h}{+}he^g + g) \end{aligned}$$

But, for all $g, h \in G$ and for all $f(x) \in X$, we get: LHS $\neq$ RHS. Thus, we have that $\cdot$ is **not** a group action of G on X.

□

EXAMPLE 3.4. Let G be a group, let X be a set, and let $\cdot$ be an action of G on X. Let $g \in G$ and define a function by $\phi_g(x) = g \cdot x$ for all $x \in X$. We want to show ϕ_g is an permutation of X.

PROOF. Let G be a group and let X be a set. Suppose G acts on X by $\phi_g(x) = g \cdot x$ for all $x \in X$. For ϕ_g to be a permutation of X, ϕ_g must be a function from X to

itself that is both "one-to-one" and "onto." By definition of group action, we know a function maps elements from a set to the same set. Thus, we have that ϕ_g is a function from X to itself. Now, we need to show it is one-to-one and onto.

One-to-One: ϕ_g is one-to-one if for all $x, y \in X$, $\phi_g(x) = \phi_g(y)$ implies $x = y$.

Towards proving this, let $a, a' \in X$, let $g \in G$, and assume $\phi_G(a) = \phi_g(a')$. Then, we have: $\phi(a) = g \cdot a$ and $\phi_g(a') = g \cdot a'$. Thus, using our assumption, we have that $ga = ga'$. So, clearly then, $a = a'$, as desired.

Onto: ϕ_g is onto if for all $x \in X$, there exists $y \in X$ such that $\phi_g(y) = x$.

Towards proving this, let $b \in X$. We want to show there exists $a \in X$ such that,

$$\phi_g(a) = g \cdot a = b$$

Let $a = g^{-1}b$ where $g^{-1} \in G$. We know $a \in G$ and $g^{-1} \in G$ because G is a group (closure property and inverse property hold). Then, clearly,

$$\begin{aligned} \phi_g(a) &= g \cdot a \\ &= g \cdot (g^{-1}b) \\ &= (g \cdot g^{-1}) \cdot b \\ &= (e_G) \cdot b \\ &= b \end{aligned}$$

Thus, we have shown ϕ_g is a permutation of X where X is a set acted on by a group G such that $\phi_g \cdot (x) = gx$ for all $x \in X$. By proving this, we've shown a group action is a permutation and a permutation is a group action!

□

3.0.1. Equivalence Relation. Let a group, G, act on a set, X. Define a relation $\sim$ on X by $x \sim y$ if and only if $\exists$ a $g \in G$ whereby $g \cdot x = y$. We will show that $\sim$ is an equivalence relation - that is, we will show $\sim$ is reflexive, symmetric and transitive.

First, let f be an action of G on X where:

$$f : G \text{ x } X \to X$$

and let $f(g, x)$ be an element of the set denoted by $g \cdot x \ \forall \ g \in G$ and $x \in X$. We define $x \sim y$ by: $f(g, x) = y$ - that is, $g \cdot x = y$.

Is $\sim$ reflexive?

Let $a \in X$., and let $g = e_G$ where e_G is the identity element of G (since G is a group). Then,

$$g \cdot a = e_G \cdot a = a \quad .$$

Clearly, then $a \sim a$ and $\sim$ is reflexive.

Is $\sim$ symmetric?

Let $a, b \in X$. We assume $a \sim b$, and so, we have that there exists $g \in G$ such that $g \cdot a = b$. We need to show that $b \sim a$ - that is, there exists $h \in G$ such that $h \cdot b = a$.

Let $h = g^{-1}$ (where we know $g^{-1} \in G$ because of a group's "inverse" property). Then, we get the following:

$$h \cdot b = h \cdot (g \cdot a) = (hg) \cdot a = (g^{-1}g) \cdot a = e_G \cdot a = a.$$

Clearly, then $a \sim b$ and $b \sim a$, and so, $\sim$ is symmetric.

Is $\sim$ transitive?

Let $a, b, c \in X$. We assume $a \sim b$ and $b \sim c$. Thus, we have there exists $g \in G$

such that $g \cdot a = b$ and $\exists h \in G$ such that $h \cdot b = c$. We need to show that $a \sim c$ - that is, there exists $k \in G$ such that $k \cdot a = c$.

Let $k = hg$ (where we know $k \in G$ because of a group's "closure" property). Then, we get the following:

$$c = h \cdot b = h \cdot (g \cdot a) = (hg) \cdot a = k \cdot a$$

Clearly, then $a \sim b$, $b \sim c$, and $a \sim c$, and so, $\sim$ is transitive.

3.0.2. Transitive Group Action.

DEFINITION 3.2. The action of G on X is **transitive** if X is non-empty and for all pairs $x, y, \in G$, there exists an element $g \in G$ so that $g \cdot x = y$.

In Example 3.1, we showed $\cdot$ is an action of G on X where G acts on the plane $X = \mathbb{R}$ x $\mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$ where $r \in \mathbb{R}$ and $(x, y) \in X$. To show the action is transitive, we first let $x, y \in X$. That is, $x = (x_1, x_2) \in \mathbb{R}$ x $\mathbb{R}$ and $y = (y_1, y_2) \in \mathbb{R}$ x $\mathbb{R}$. Now, we ask: *does there exist an element $g \in G$ such that $g \cdot x = y$?*

To answer this, let $y = (x_1 + gx_2, x_2)$ where $g \in G$. Note, since closure for $\mathbb{R}$ holds under the operation of addition, $(x_1 + gx_2) \in \mathbb{R}$. Thus, we can let $(x_1 + gx_2) = y_1$ and $x_2 = y_2$, and so,

$$g \cdot x = (x_1 + gx_2, x_2) = y.$$

Therefore, *yes*, there exists an element $g \in G$ such that $g \cdot x = y$, and so, the action is transitive.

In Example 3.3, we showed f is an action of G on G where G acts on itself by $(g \cdot x) = gxg^{-}1$, where $g, x \in G$. To show the action is transitive, we begin by letting $x, y \in G$. Now, we ask: *does there exist an element $g \in G$ such that $g \cdot x = y$?*

To answer this, let $y = gxg^{-1}$ where y must be an element of G because G is a group, and so, closure holds and the inverse, g^{-1}, exists for some $g \in G$. Thus,

$$g \cdot x = gxg^{-1} = \text{y}.$$

Therefore, *yes*, there exists an element $g \in G$ such that $g \cdot x = y$, and so, the action is transitive.

In Example 4.4, we showed h is an action on G where G acts on a set of functions $f(x)$ of a real variable by: *(i)* $r \cdot f(x) = f(x + r)$ and *(ii)* $r \cdot f(x) = f(x)e^r$ where $r \in \mathbb{R}$ and $f(x) \in X$.

For *(i)*, to show the action is transitive, we begin by letting $a, b \in X$. That is, a is some function $s(x) \in X$ and b is some function $t(x) \in X$ (and where $x \in \mathbb{R}$). Now, we ask: *does there exist an element $g \in G$ such that $g \cdot a = b$?*

To answer this, let $b = t(x) = s(x + g)$, where $g \in G$. Since $G = \mathbb{R}$ is closed under addition, we have that $(x + g) \in \mathbb{R}$. Thus, we have:

$$g \cdot a = g \cdot (s(x)) = s(x + g) = t(x) = b.$$

Therefore, *yes*, there exists an element $g \in G$ such that $g \cdot a = b$, and so, the action is transitive.

For *(ii)*, to show the action is transitive, we begin by letting $a, b \in X$. That is, a is some function $s(x) \in X$ and b is some function $t(x) \in X$ (and where $x \in \mathbb{R}$). Now, we ask: *does there exist an element $g \in G$ such that $g \cdot a = b$?*

To answer this, let $b = t(x) = s(x)e^g$, where $g \in G$. Since $G = \mathbb{R}$ is closed under addition and multiplication, we have that $e^g \in \mathbb{R}$. Thus, we have:

$$g \cdot a = g \cdot s(x) = s(x)e^g = t(x) = b.$$

Therefore, *yes*, there exists an element $g \in G$ such that $g \cdot a = b$, and so, the action is transitive.

3.1. Stabilizers and Orbits

Let G be a group that acts on a set X.

DEFINITION 3.3. The **orbit of x** is the set $orb_G(x) = \{g \cdot x | g \in G\}$. The orbit is the set of the elements of our set X that we get from a group element acting on a particular element of X. We can think about the notion of the orbit as the trajectory. EXPLAIN MORE?

DEFINITION 3.4. The **stabilizer of x** is the set $stab_G(x) = \{g \in G | g \cdot x = x\}$. The stabilizer is the set of group elements that acts on a particular element of our set X in such a way that they do not change the element.

EXAMPLE 3.5. As it pertains to the Rubik's Cube, let us consider the subgroup <L > and find its orbit and stabilizer on the solved Cube. So, as it applies to the above definitions, G= <L> and x is the solved cube. We get the following:

$$orb_G(x) = \{\text{the results of performing I, L, L}^2\text{, and L}^3\}$$
$$stab_G(x) = \{\text{the result of performing I}\}$$

.

THEOREM 3.1. *The stabilizer is a subgroup of a group.*

PROOF. We begin by letting G be a group, letting G act on a set X, and letting S be a subset of G where $S = stab(x) = \{g \in G | g \cdot x = x\}$. Because S contains the identity element, we know it is non-empty, and so, we can proceed using the 2-Step Subgroup Test. Suppose a, b are stabilizers, i.e. $a, b \in S$. This means that for all $x \in X$, $a, b \in G$ such that $a \cdot x = x$ and $b \cdot x = x$.

First, we want to show ab is a stabilizer, i.e. $(a \cdot b) \in S$ such that $(a \cdot b) \cdot x = x$. Since, $a \cdot x = x$ and $b \cdot x = x$, we have:

$$\begin{aligned}(a \cdot b) \cdot x &= a \cdot (b \cdot x) \\ &= a \cdot x \\ &= x.\end{aligned}$$

Thus, S is closed under our operation.

Now, we need to show for all $s \in S$, there exists $s^{-1} \in S$. To do this, let $s \in S$, i.e. $s \in G$ such that $s \cdot x = x$. Since $s \in G$, where G is a group, we know there exists an $s^{-1} \in G$. Thus, we get the following:

$$\begin{aligned}s^{-1} \cdot x &= s^{-1} \cdot (s \cdot x) \\ &= (s^{-1} \cdot s) \cdot x \\ &= e_G \cdot x\end{aligned}$$

$$= x$$

Clearly, $s^{-1} \in S$, and so, S is closed under taking inverses. Altogether, then, we've shown that the stabilizer, S is a subgroup of G. □

EXAMPLE 3.6. Let us first consider the symmetric group, S_4 acting on a "set of numbered squares." We would expect the order to be 4! (see Definition 2.6), and that is exactly what we get: 24 elements in the group.

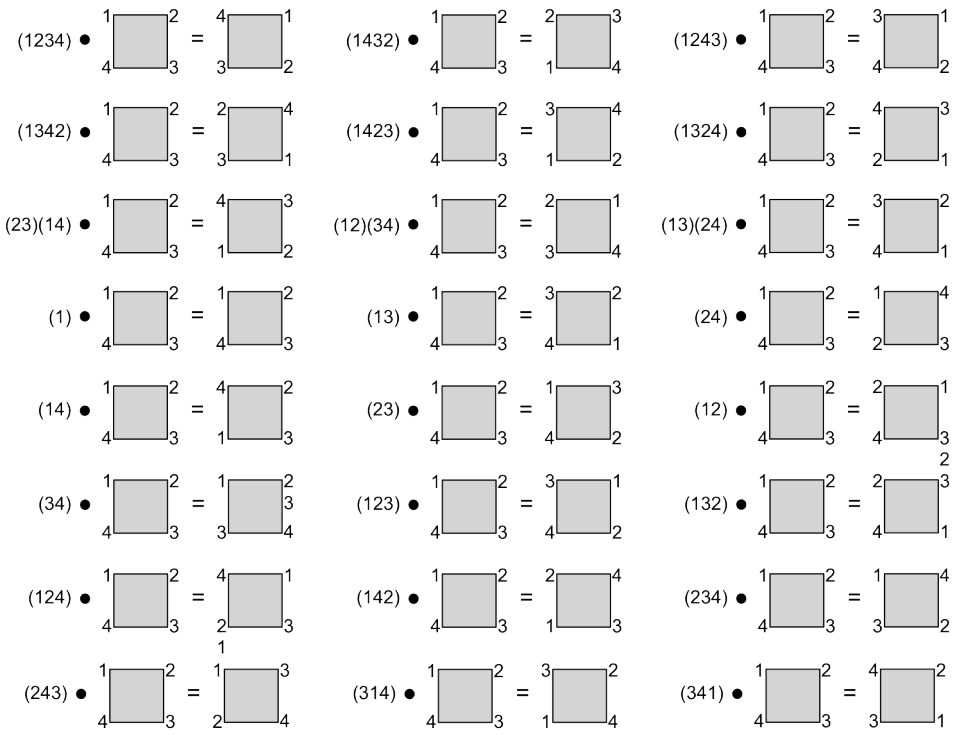


FIGURE 1. All elements of S_4

Rather, than considering the entire S_4 group, let us focus in on certain elements, namely those in the dihedral group of order 8.

DEFINITION 3.5. The **dihedral group** of order m contains m elements of S_n, namely the m of them which are symmetries of polygons. That is, they can be formed by rotations or flips.

D_8 is a subgroup of the group S_4. To see this, let consider D_8 as our group acting on a "dotted set of squares." We see that we have 8 group elements acting the square by either a rotation (by 0, 90, 180, or 270 degrees) or a flip (horizontal H, vertical V, diagonal D, diagonal D'):

Consider in our "set of dotted squares" the specific square, which we will call "Square 1":

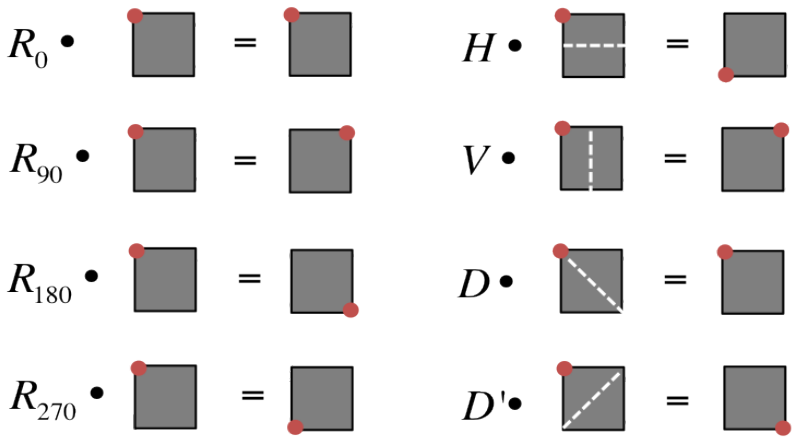


FIGURE 2. All elements of D_8

FIGURE 3. An element of our "set of dotted squares"

The orbit of Square 1 is the set of elements in our "set of dotted squares" we get after Square 1 was acted on by all elements of the group D_8. Not counting duplicates, we see that we get 4 (unique) elements of our set, and so,

$$|orb_{D_8}(\text{Square 1})|=4.$$

The stabilizer of Square 1 is the set of group elements that act on Square 1 without affecting it. Thus, $stab_{D_8}(\text{Square 1}) = \{R_0, D\}$, and so,

$$|stab_{D_8}(\text{Square 1})|=2.$$

This example illustrates a theorem of tremendous consequence within Group Theory, namely the Orbit-Stabilizer Theorem.

THEOREM 3.2. *Orbit Stabilizer Theorem*
Where G is a finite group of permutations of a set X, for any $x \in X$, we have:

$$|G| = |orb_G(x)||stab_G(x)|.$$

PROOF. First, recall the result of Lagrange's Theorem (see proof of Theorem 2.2), namely that $|G|/|stab_G(x)|$ gives us the number of distinct left cosets of $stab_G(x)$ in G. Thus, we can establish a one-to-one correspondence between these left cosets and the elements in the orbit of i. Let's call this correspondence C and define the relationship as the mapping the coset $\phi stab_G(x)$ to $\phi(x)$ under C. We need to show $\alpha stab_G(x) = \beta stab_G(x)$ implies $\alpha(x) = \beta(x)$. However, we have that $\alpha stab_G(x) =$

$\beta stab_G(x)$ implies $\alpha^{-1}\beta \in stab_G(x)$, and so, $(\alpha^{-1}\beta)(x) = x$, and consequently, $\beta(x) = \alpha(x)$. Not only does this show C to be well-defined, but it also shows that it is one-to-one. To show C is onto then, let $y \in orb_G(x)$, which gives us that $\alpha(x) = y$ for some $\alpha \in G$. Then, clearly, $C(\alpha stab_G(x)) = \alpha(x) = y$.

□

3.2. Kernels and Faithfulness

In addition to orbits and stabilizers, as it pertains to group actions we also have the notion of a kernel.

DEFINITION 3.6. The **kernel** of a group action where a group G acts on a set X is:

$$ker_G = \{g \in G \mid g \cdot x = x \ \forall x \in X\}$$

Thus, the kernel, unlike the stabilizer, is the set of group elements that fix every element $x \in X$.

DEFINITION 3.7. Furthermore, if and only if the only element in the kernel is the identity, then we say G **acts faithfully** on X.

To get a better understanding of these concepts, let us apply them to some examples we have considered previously.

(1) For Example 3.1, we first see that the stabilizer is not just the identity. (Consider for any element in the set X of the form $(x, 0)$ (i.e. when $y = 0$), all elements $g \in G$ will be in the stabilizer since $g \cdot (x, 0) = (x + g(0), y) = (x, y)$.) However, when we consider the kernel, we are finding elements which fix every element $(x, y) \in X$ and the only group element that does this is the identity. Thus, we conclude this action to be faithful.

(2) For Example 3.2, we (trivially) have the identity as a stabilizer. Since $e_G \in G$ and letting $x \in G$, we get:

$$\begin{aligned} e_G \cdot x &= e_G x {e_G}^{-1} = x \end{aligned}$$

However, we also have for $x \in G$,

$$\begin{aligned} x \cdot x &= xxx^{-1} \\ &= x(e_G) = x \\ &= x \end{aligned}$$

Additionally, we have for $x^{-1} \in G$,

$$\begin{aligned} x^{-1} \cdot x &= x^{-1}x(x^{-1})^{-1} \\ &= (e_G)x = x \end{aligned}$$

Since, $G = X$ in this example, x and x^{-1} are also elements of the kernel as they fix every element in X (i.e. in G), and so, this action does not act faithfully.

(3) For Example 3.5, when we are considering the group D_8 acting on our "set of dotted squares" we see that the only group element which fixes every element $xinX$ is the identity. As it pertains to the notion of the stabilizer, we saw in this example that $stab_{D_8}(\text{Square 1}) = R_0, D$ (where R_0 is taken to be the

identity). However the group element D does not fix every square in our 11set of dotted squares" as we can see if our dot was in, say, the upper right corner of the square (instead of the upper left corner). Thus, altogether, we can conclude this action is faithful.

THEOREM 3.3. *The kernel is a subgroup of a group G.*

PROOF. By the Two-Step Subgroup Test, let G be a group that acts on a set X. Where K is a non-empty subset of G, let $K = ker = \{g \in G \mid g \cdot x = x \ \forall x \in X\}$.

Suppose $a, b \in K$. This means that for any $x \in X$, we have $a \cdot x = x$ and $b \cdot x = x$. We want to show then that $ab \in K$, i.e. for all $x \in X$, $ab \cdot x = x$. Since we have $a \cdot x = x$ and $b \cdot x = x$, we get:

$$\begin{aligned} ab \cdot x &= a \cdot (b \cdot x) \\ &= a \cdot x \\ &= x \end{aligned}$$

Now, we need to show for an element $k \in K$, it's inverse $k^{-1} \in K$. That is, we want to show $k^{-1} \cdot x = x$. Where $k \in K$, we have for any $x \in X$,

$$k \cdot x = x$$

Since $k \in G$ and G is a group, we have that there exists $k^{-1} \in G$. Thus, we get the following:

$$\begin{aligned} k^{-1} \cdot x &= k^{-1} \cdot (k \cdot x) \\ &= (k^{-1} \cdot k) \cdot x \\ &= (e_G) \cdot x \\ &= (= x \end{aligned}$$

Clearly, then $k^{-1} \in K$, and so, K is closed under taking inverses, as desired. Altogether, then, we've shown that the kernel, K is a subgroup of a group G.

□

Bibliography

[1] Alexander F. Frey Jr. and David Singmaster. *Handbook of Cubik Math*. Lutterworth Press, Cambridge, England, 2010.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley Sons, Inc, Hoboken, New Jersey, 2004.

[3] John B. Fraleigh. *A First Course in Abstract Algebra, 8th ed.*. Addison Wesley, Boston, Massachusetts, 2009.

[4] Joseph A. Gallian. *Contemporary Abstract Algebra, 8th ed.*. Brooks Cole, Boston, Massachusetts, 2013.