Jonathan Lam
Mr. Ecsedy
AP Calculus BC p. 8
5 / 23 / 18

An Introduction to Group Theory through the Lens of the Rubik's Cube

Here are four observations:

1. Many mathematical operations produce a result that has the same form as its operands; i.e., the result comes from the same set as the operands.
2. Many binary mathematical operations disregard the way its elements are grouped.
3. Many mathematical operations have a unique "identity element." When performed on the identity element and some other element, this produces the other element.
4. Many mathematical operations have an inverse element for every possible input, so that applying the operation on the element and its inverse produces the identity element.

In fact, many mathematical operations have all four of these properties, so mathematicians decided to formalize them into a mathematical structure, consisting both of a *set* of elements and an operation (called the *group rule*) that together satisfy these conditions. The structure is called a *group*, and these four properties that must be obeyed by every group are called the *group axioms*. They are, in the order above, *closure*, *associativity*, (having an) *identity element*, and *invertibility*.

Take, for example, the addition operation over the set of integers. It follows all of the group axioms. Integers are closed over addition, because adding an integer to an integer always results in another integer. The order of grouping of elements for two numbers does not matter: $(2 + 2) + 3$ is equal to $2 + (2 + 3)$. The additive identity is zero; the additive inverse is the opposite of an integer.

Note that multiplication is not closed over integers, so the multiplication with integers is not a group. (Multiplication with real numbers is, however.) Note also that subtraction and division, while not considered valid operations (because they violate associativity), are simply the inverses of addition and multiplication. Therefore, when expressed in terms of addition and multiplication (and adjusting the group's sets as necessary to include additive and multiplicative inverses), these operations can be classified as groups. Another point to note is that *associativity* does not imply *commutativity*; i.e., changing the order of the terms may not create the same result. Groups that are commutative, such as addition and multiplication, are called *abelian groups*; others, such as the Rubik's cube group described later, are *non-abelian*.

Note that groups can be used to express much more abstract concepts than simple algebra. A higher-level example would be that of the Rubik's cube. Before going more in depth into the application of group theory to the Rubik's cube, some basic definitions need to be given:

Definition 1: *cubie*: a single, physical block on the Rubik's cube

Definition 1.1: *corner cubie*: one of eight cubies on the corner of the cube, with three stickers

Definition 1.2: *edge cubie*: one of twelve cubies on an edge of the cube, with two stickers

Definition 1.3: *center cubie*: one of six cubies on the center of a face; these do not get permuted or oriented, so they will be ignored in this discussion

Definition 2: *{ U, D, R, L, F, B }*: the set of possible single moves in a Rubik's cube in Singmaster notation, corresponding to clockwise turns of the up (top), down (bottom), right, left, front, and back faces

While it may not be immediately clear how the Rubik's cube might be expressed as a set (Set of cubies? Set of stickers? Set of moves?) It turns out that the Rubik's cube group (denoted (G,·) from here on) is an example of a permutation group, where the set is all possible permutations of moves. Each set of moves, or each possible position of the cube, is therefore represented by one element of the set. The number of items in the set, or cardinality of the underlying set of the group, denoted |G|, is the number of possible permutations of the Rubik's cube— |G| = 43,252,003,274,489,856,000. A Rubik's cube is non-abelian because changing the order of the moves does not produce the same permutation (otherwise solving it would become very easy by trial and error!).

One way, and perhaps the simplest way, to represent a group is through a permutation of moves necessary to get to a state of the cube from the solved state. This includes moves such as the group is by the permutation of moves. The set is a list of permutations generated by basic moves: { U, D, R, L, F, B }, until all possible states of the cube are exhausted. This means { E, U, D, R, L, F, B, U·U, U·D, U·R, U·L, … etc. }, where E is the empty move (the identity element) and the group rule is composition (·). Any legal state of the Rubik's cube can be represented by a sequence of moves. The problem with this notation is that it can have repetitions of the same state: for example, the element U·U·U·U is equivalent to E, and thus would be double-counted.

In fact, there are an infinite number of possible permutations (but only a finite number of possible states), so a more advanced notation should be used to denote the state of a cube.

The Rubik's cube is a *subgroup* of the *symmetric group* S_{48}, the permutations of the 48 non-center stickers on a Rubik's cube. Symmetric groups are permutation groups with all possible elements, but some permutation groups such as the Rubik's cube group have restrictions to prevent illegal combinations.

If all the stickers on a Rubik's cube could be freely permuted (which is clearly illegal — for example, a single corner cubie cannot have three stickers of the same color, which is possible with a total permutation), this would result in a symmetry group of S_{48}, which has a cardinality of 48!, or approximately 1.24*10^{61}. (Luckily for speedcubers and mathematicians alike,) Many of these permutations are illegal. If we restrict the permutations so that the stickers cannot be individually permuted freely, but rather the cubies themselves (the arrangements of stickers on each cubie remains constant), then we arrive at what is known as the Illegal Rubik's Cube Group, because even then some operations are illegal due to the symmetry of the Rubik's cube group. The set I of the Illegal Rubik's Cube Group is defined as:

$$I = (C_2^{12} \times S_{12}) \times (C_3^8 \times S_8)$$

$$|\, I \,| = 2^{12} \times 12! \times 3^8 \times 8! \approx 5.19 \times 10^{20}$$

The structure of I can be explained intuitively by thinking about the structure of the Rubik's cube, but it requires some other knowledge of cube theory . The cyclic group C_n describes a set of length n (cardinality n), and the symmetric group S_n denotes a symmetric group of n elements (cardinality n!). The first group here is C_2^{12} , which can be written $(C_2)^{12}$, and represents the two orientations of an edge (normal or flipped) for each of the twelve edges. This group has cardinality 2^{12}. The second group is S_{12}, which represents the permutation of the twelve edges. This group has cardinality 12!. The same logic can be applied to the eight corners, which have three orientations each.

Lastly, the product of two groups is another group which is the Cartesian product (×) of their sets, and the cardinality of a product is the product of the cardinalities of the operands:

$$|\ g_1 \times g_2 \times g_3 \times \ldots | = | g_1 | \times | g_2 | \times | g_3 |\ \times \ldots$$

This allows for the calculation of the cardinality of the Illegal Rubik's Cube Group, which is the product of multiple other groups.

While this appears to make sense, there are still some further rules to govern the moves of Rubik's cubes. For example, the orientations of the first 11 edges determine the orientation of the last edge, and the same for the corners. Also, there must always be an even number of flips (the proof is not given here), so the size of G is halved from there.

$$G \ = \ (C_2^{11} \times S_{12}) \times (C_3^7 \times S_8) \div 2 = \{ \ (\ v, \ w, \ r, \ s \ ) \mid v \in C_3^7, \ r \in S_8, \ w \in C_2^{10}, \ s \in S_{12} \ \}$$

$$\mid G \mid = 2^{10} \times 12! \times 3^7 \times 8! \approx 4.33 \times 10^{19}$$

This is the full, legal Rubik's cube group and its cardinality.

Looking over the equations, especially the final, precise definition of the Rubik's cube group, shows that there is a heavy connection to sets. Group theory can, in fact, be considered a subfield of *set theory*, where the sets are bound only with binary operations that follow the group axioms (whereas set theoryeory studies sets without these limitations and with n-ary operations). But groups are specifically defined in such a way to highlight features of symmetry, where symmetry is used in the sense of "reversible transformations that preserve some kind of structure" (Berchenko-Kogan). This leads to many supporting theorems (not discussed here) that extend past regular set theory, such as Lagrange's theorem or Burnside's theorem, that deal with more specific applications of groups. For simplicity, only the definition of the Rubik's cube group and its cardinality (which can be explained with basic Set Theory) are discussed in this paper, but many more applications of the Rubik's cube group's *subgroups* (groups whose sets are subsets of another group) and *homomorphisms* (similar group structures) exist in a deeper knowledge of group theory; for instance to discover algorithms to solve certain states.

Another observation from this work is that group theory is not often used directly to solve algebraic problems, but that a group is often fitted, or associated with a mathematical or real-world object, and the resulting group's properties are studied. This is the case with the Rubik's cube, as it is difficult to immediately draw conclusions from the fascinating toy. Writing it as the product of smaller, more understandable groups allows mathematicians to break down its structure and properties.

Group theory has many applications with objects with symmetry in the real world. Most clear are symmetry groups, which deal with geometric transformations (not to be confused with symmetric groups, which are a type of permutation group). This has applications from determining the properties of lattice structures to the use of Lie groups in the Standard Model of physics. The earliest use for groups was in the late 19th century, when mathematicians were looking to solve polynomial equations with degree n > 4, realizing the symmetry of the roots and generalizing it to modern group theory. Other applications include computational group theory, which has applications with computer modeling and graphics to cryptography— the widespread RSA encryption uses a the symmetry of modular multiplication groups to its advantage.

Because of the ubiquity of structures that use non-transforming operations, both in mathematics and for physical objects, it makes sense to describe an algebraic structure that can be used to generalize and mimic this symmetry. It provides an abstract basis for symmetry that can be applied to many objects, but is still powerful enough to make quantitative observations about behaviors and patterns present in the group.

Jonathan Lam
Mr. Ecsedy
AP Calculus BC p. 8
5 / 23 / 18

Works Cited

Berchenko-Kogan, Yasha. “What is the point of group theory?” *Quora*. N.p., 21 Jul 2014. Web. <https://www.quora.com/What-is-the-point-of-group-theory>.

Works Consulted

“Abstract Algebra.” *Wikipedia,* Wikimedia Foundation., 14 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Abstract_algebra>.

“Alternating group.” *Wikipedia,* Wikimedia Foundation., 2 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Alternating_group>.

Biderman, Stella. “Importance of group action in abstract algebra.” *Mathematics Stack Exchange*. Stack Exchange Inc., Web. 10 Nov. 2017. Web. 25 May 2018. <https://math.stackexchange.com/questions/2514058/importance-of-group-action-in-abstract-algebra>.

Chen, Kenneth. “How do I calculate the combinations of a Rubik’s Cube?” *Quora*. N.p., 5 Mar. 2018. Web. 25 May 2018. <https://www.quora.com/How-do-I-calculate-the-combinations-of-a-Rubiks-Cube>.

“Classification of finite simple groups.” *Wikipedia*. Wikimedia Foundation, Inc., 25 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Classification_of_finite_simple_groups>.

Conrad, Keith. “Why is group theory important?” *KConrad UConn Math 216*. N.p., N.d. Web. 25 May 2018. <http://www.math.uconn.edu/~kconrad/math216/whygroups.html>.

“Direct product of groups.” *Wikipedia,* Wikimedia Foundation., 19 Dec. 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Direct_product_of_groups>.

[Dmitri]. “Fun applications of representations of finite groups.” *Mathoverflow*. Stack Exchange Inc., 10 Jan. 2014. Web. 25 May 2018. <https://mathoverflow.net/questions/11784/fun-applications-of-representations-of-finite-groups>.

Driscoll-Tombin, Geoffrey R. “What is the difference between group theory and set theory?” *Quora*, N.p., Web. 25 May 2018. <https://www.quora.com/What-is-the-difference-between-group-theory-and-set-theory>.

Ellinor, Andrew, et al. “Lagrange’s Theorem.” *Brilliant*. Brilliant.org, N.d. Web. 25 May 2018. <https://brilliant.org/wiki/lagranges-theorem/>.

“Finite group.” *Wikipedia*. The Wikimedia Foundation, Inc., 14 May 2018. <https://en.wikipedia.org/wiki/Finite_group>.

“Group (mathematics.”> *Wikipedia.* The Wikimedia Foundation, Inc., 10 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Group_(mathematics)>.

“Group theory.” *Wikipedia*. The Wikimedia Foundation, Inc., 16 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Group_theory>.

Gruber, Alexander. “Are there real world applications of finite group theory?” *Mathematics Stack Exchange*. Stack Exchange, Inc., 8 Mar. 2013. Web. 25 May 2018. <https://math.stackexchange.com/questions/324253/are-there-real-world-applications-of-finite-group-theory>.

“A Hamiltonian circuit for Rubik’s Cube.” *cuBer Bruce* . N.p., N.d. Web. 25 May 2018. <http://bruce.cubing.net/ham333/rubikhamiltonexplanation.html>.

“History of group theory.” *Wikipedia*. The Wikimedia Foundation, Inc., 28 Apr 2016. Web. <https://en.wikipedia.org/wiki/History_of_group_theory>.

“Identity element.” *Wikipedia*. The Wikimedia Foundation, Inc., 9 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Identity_element>.

“Inverse element.” *Wikipedia*. The Wikimedia Foundation, Inc., 19 Dec. 2017. Web. 255 May 2018. <https://en.wikipedia.org/wiki/Inverse_element>.

[Joe Z.] “Is it possible to use one sequence of moves to solve the Rubik’s cube from any position?” *Puzzling Stack Exchange*. 17 Nov. 2014. Stack Exchange Inc., Web. 25 May 2018. <https://puzzling.stackexchange.com/questions/4820/is-it-possible-to-use-one-sequence-of-moves-to-solve-the-rubiks-cube-from-any-p>.

“List of finite simple groups.” *Wikipedia*. The Wikimedia Foundation, Inc., 11 Apr. 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/List_of_finite_simple_groups>.

Liu, Yanxi. “Group Theory and Its Applications in Robotics, Computer Vision/Graphics, and Medical Image Analysis.” *Yanxi’s book chapter on Computational Symmetry.* N.p., 2005. Web. 25 May 2018. <http://www.cs.cmu.edu/~yanxi/newtest.htm>.

[MD XF]. “Determine the highest order of an element of a Rubik’s Cube group.” *Mathematics Stack Exchange*. Stack Exchange, Inc., 14 Aug. 2017. Web. 25 May 2018.

<https://math.stackexchange.com/questions/2392906/determine-the-highest-order-of-an-element-of-a-rubiks-cube-group>.

"Number theory." *Wikipedia*. The Wikimedia Foundation, Inc., 15 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Number_theory>.

"Order (group theory)." *Wikipedia*. The Wikimedia Foundation, Inc., 1 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Order_(group_theory)>.

"Parity of a permutation." *Wikipedia,* Wikimedia Foundation., 30 Mar. 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Parity_of_a_permutation>.

"permutation." *Planetmath.org*. PlanetMath.org, Ltd., N.d. Web. 25 May 2018. <http://planetmath.org/permutation>.

"Permutation Group." *Wolfram MathWorld,* Wolfram Research, Inc., 2018. Web. 25 May 2018. <http://mathworld.wolfram.com/PermutationGroup.html>.

Rietman, Edward A. et al. "Review and application of group theory to molecular systems biology." *BMC*, BioMed Central Ltd., 22 Jun. 2011. Web. 25 May 2018. <https://tbiomed.biomedcentral.com/articles/10.1186/1742-4682-8-21>.

"Rubik's Cube group." *Wikipedia*. The Wikimedia Foundation, Inc., 15 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Rubik%27s_Cube_group>.

"Semidirect product." *Wikipedia. The* Wikimedia Foundation., 20 May. 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Semidirect_product>.

"Simple group." *Wikipedia*. The Wikimedia Foundation, Inc., 17 May 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Simple_group>.

"Symmetric group." *Wikipedia*, The Wikimedia Foundation, Inc., 7 Apr. 2018. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Symmetric_group>.

"Symmetric Group." *Wolfram MathWorld*, Wolfram Research, Inc., 2018. Web. 25 May 2018. <http://mathworld.wolfram.com/SymmetricGroup.html>.

"Wreath product." *Wikipedia,* Wikimedia Foundation., 24 Nov. 2017. Web. 25 May 2018. <https://en.wikipedia.org/wiki/Wreath_product>.

Yao, Brian, et al. "Group Theory." *Brilliant*. Brilliant.org, N.d. Web. 25 May 2018. <https://brilliant.org/wiki/group-theory-introduction/>.

Scholarly articles specific to the Rubik's Cube Group in relation to Group Theory:

Chen, Janet. *Group Theory and the Rubik's Cube*. N.p., n.d. Web. 25 May 2018. <http://www.math.harvard.edu/~jjchen/docs/Group%20Theory%20and%20the%20Rubik's%20Cube.pdf>.

Daniels, Lindsey. *Group Theory and the Rubik's Cube*. Lakehead University, N.d. Web. 25 May 2018. <http://math.fon.rs/files/DanielsProject58.pdf>.

Davis, Tom. *Group Theory vis Rubik's Cube*. geometer.org, 6 Dec. 2006. Web. 25 May 2018. <http://www.geometer.org/rubik/group.pdf>.

Howell, Zeb. *Explorations of the Rubik's Cube Group*. N.p., 18 Apr. 2016. Web. 25 May 2018. <http://buzzard.ups.edu/courses/2016spring/projects/howell-rubiks-cube-ups-434-2016.pdf>.