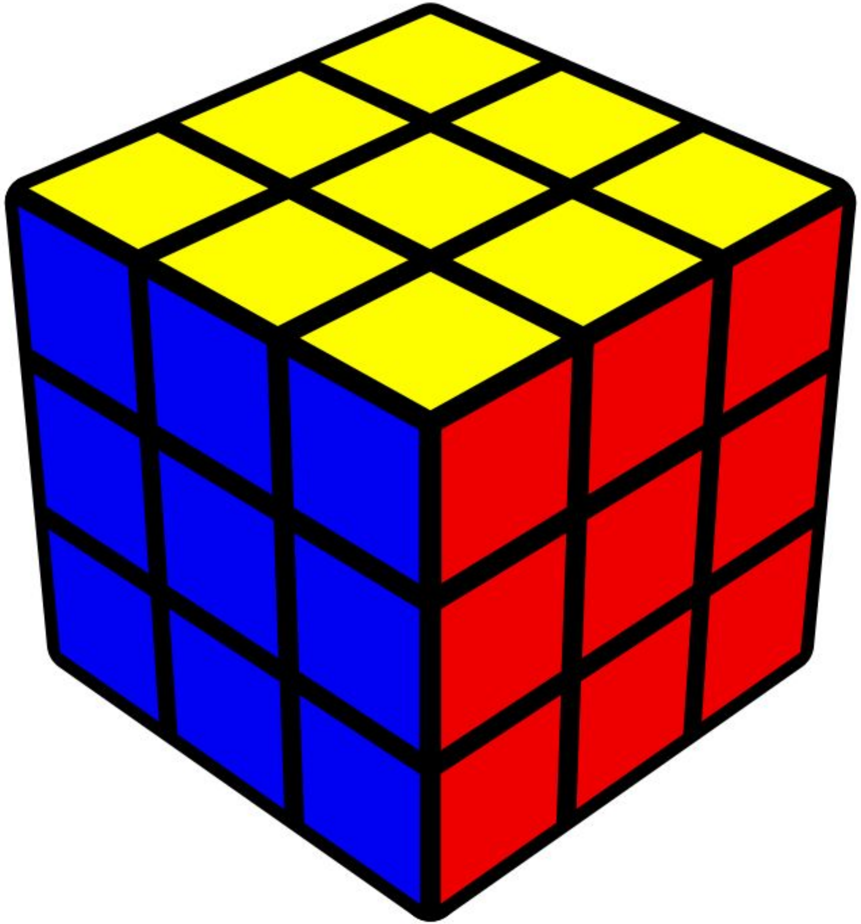
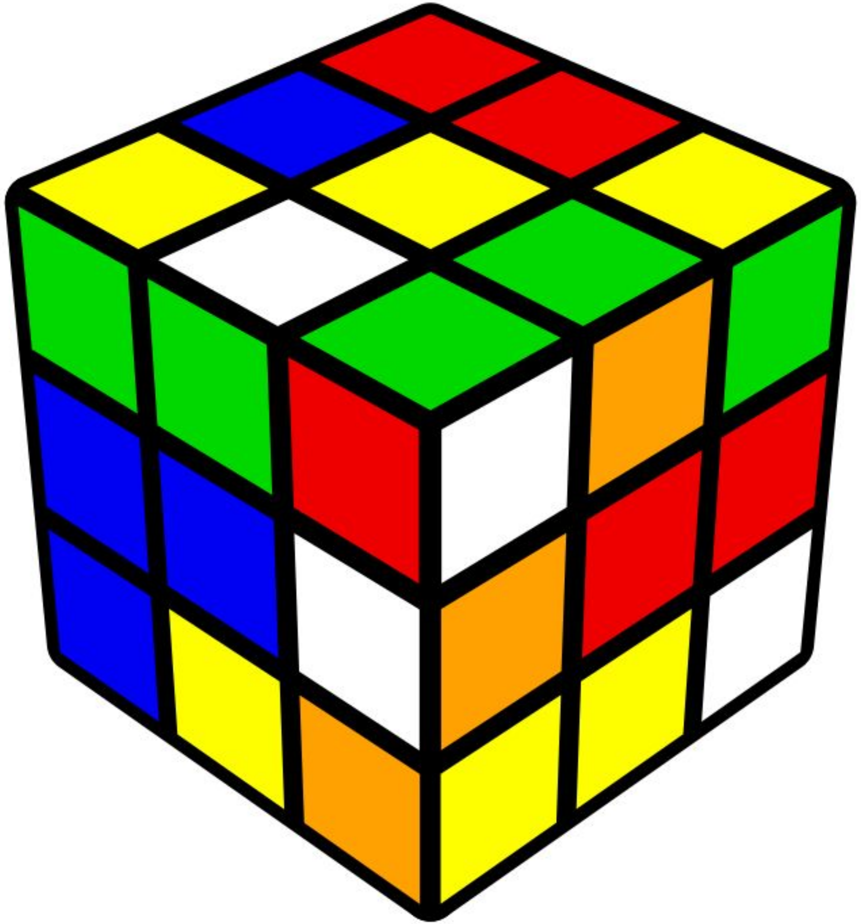
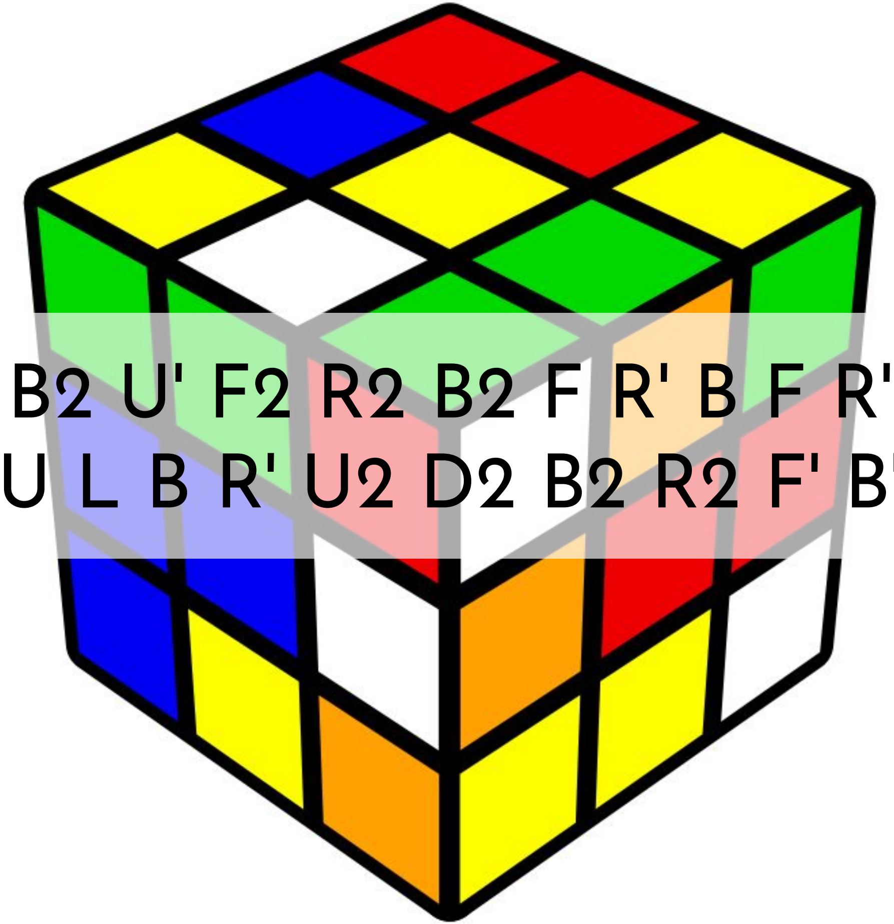


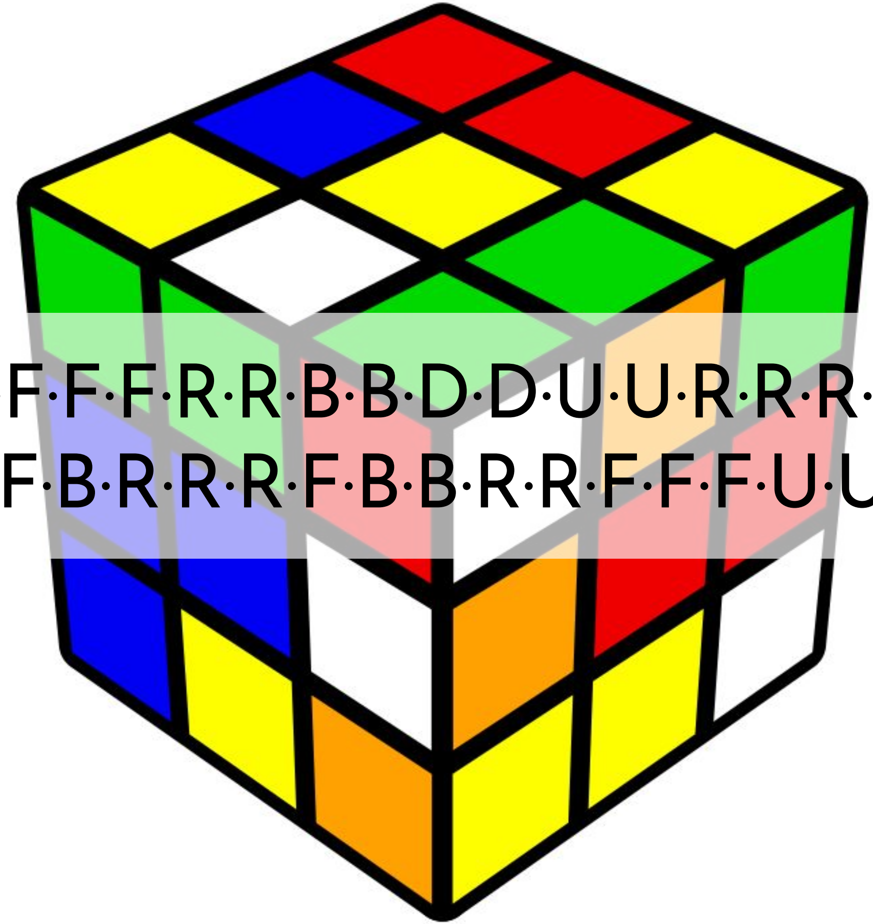
jonlam



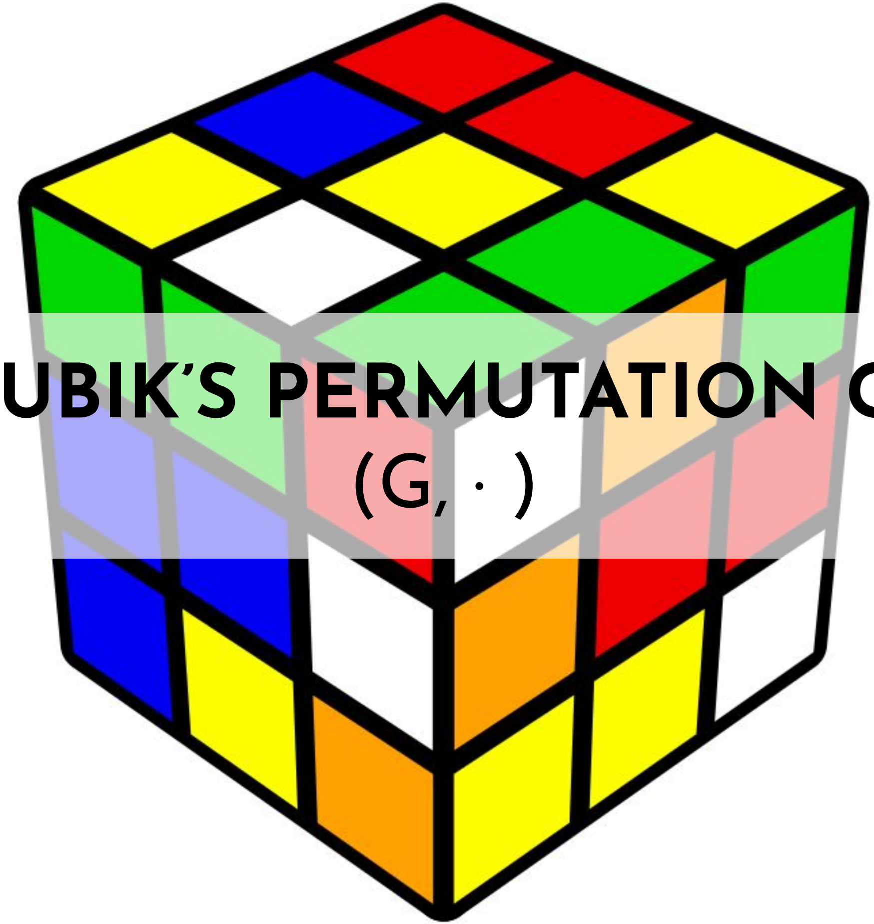
jonlam



B2 U' F2 R2 B2 F R' B F R'
U L B R' U2 D2 B2 R2 F' B'



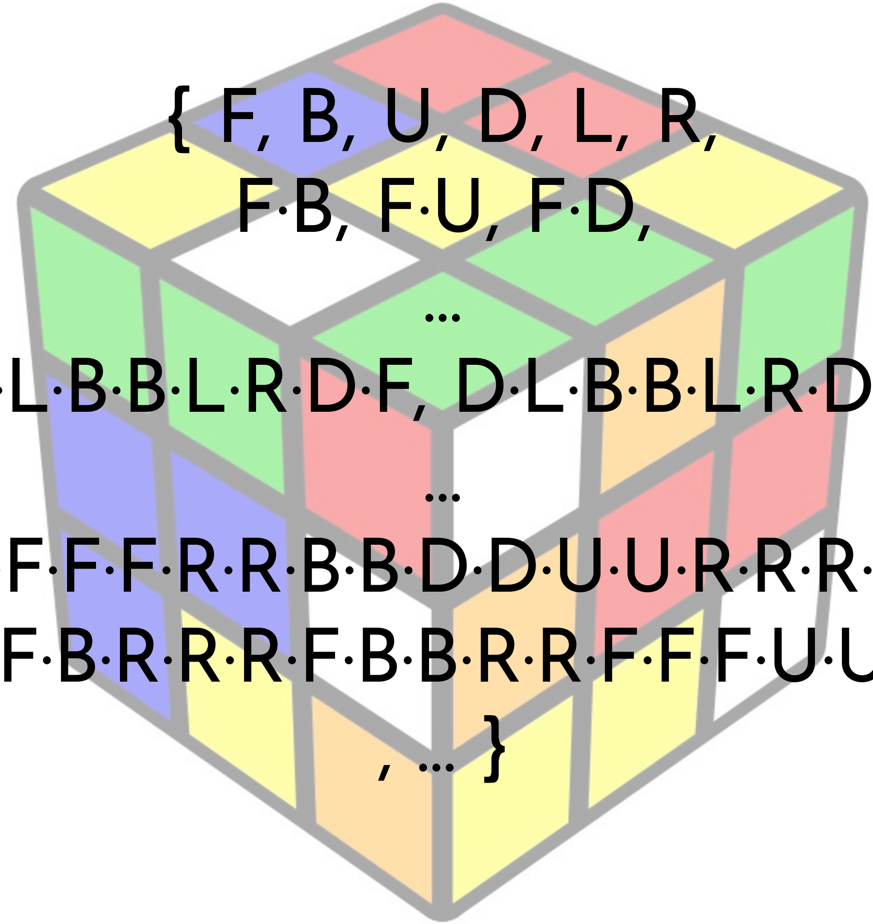
B·B·B·F·F·F·R·R·B·B·D·D·U·U·R·R·R·B·L·U·
R·R·R·F·B·R·R·R·F·B·B·R·R·F·F·F·U·U·U·B·B



THE RUBIK'S PERMUTATION GROUP

$(G, \cdot\ )$

jonlam



{ F, B, U, D, L, R,

F·B, F·U, F·D,

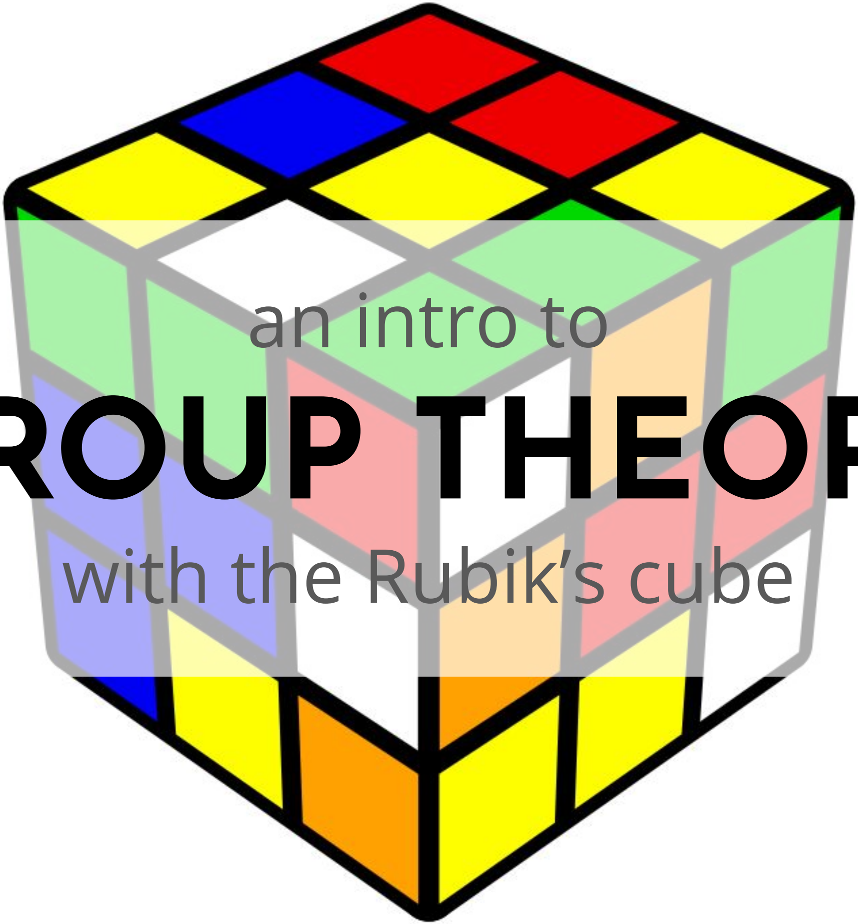
…

D·L·B·B·L·R·D·F, D·L·B·B·L·R·D·B,

…

B·B·B·F·F·F·R·R·B·B·D·D·U·U·R·R·R·B·L·U·
R·R·R·F·B·R·R·R·F·B·B·R·R·F·F·F·U·U·U·B·B

, … }



an intro to

GROUP THEORY

with the Rubik’s cube

by jonlam

NOTICE

This falls under abstract algebra, a part of mathematics unfamiliar to us. I understand very little and am going to try to cover much information in little time. If anything is unclear, please ask right away. I'll try my best to answer.

WHAT IS A GROUP?

A group is the combination of a set and a group law that obey the group axioms.

WHAT IS A GROUP?

A group is the combination of a set and a group law that obey the group axioms.

SET: a list of elements

$\mathbb{P}$ = { 2, 3, 5, 7, 11, ... }

Z = { ... -3, -2, -1, 0, 1, 2, 3, ... }

WHAT IS A GROUP?

A group is the combination of a set and a group law that obey the group axioms.

SET: a list of elements

ℙ = { 2, 3, 5, 7, 11, ... }

Z = { ... -3, -2, -1, 0, 1, 2, 3, ... }

GROUP LAW: a binary operation (acts on two elements of a set **a** and **b**):

a **+** b

a **mod** b

Generic notation: a ***** b

(looks like multiplication, because multiplication is an example of a group!)

jonlam

GROUP AXIOMS

CLOSURE: applying the operation to two elements of the set produces another element of the set

GROUP AXIOMS

CLOSURE: applying the operation to two elements of the set produces another element of the set

ASSOCIATIVITY: different groupings of elements do not change the result (don’t confuse with commutativity!)

GROUP AXIOMS

CLOSURE: applying the operation to two elements of the set produces another element of the set

ASSOCIATIVITY: different groupings of elements do not change the result (don’t confuse with commutativity!)

IDENTITY ELEMENT: there is a unique “identity” element **e** in the set that results in the other operand when the operation is performed

GROUP AXIOMS

CLOSURE: applying the operation to two elements of the set produces another element of the set

ASSOCIATIVITY: different groupings of elements do not change the result (don't confuse with commutativity!)

IDENTITY ELEMENT: there is a unique "identity" element **e** in the set that results in the other operand when the operation is performed

INVERSE ELEMENT: for every element **a** in a group, there is an inverse element **b** in the set such that **a * b = e**

EXAMPLE: ADDITION OVER INTEGERS

GROUP: (Z, +)
SET: Z,
GROUP RULE: +

CLOSURE: adding two integers results in an integer

ASSOCIATIVITY: grouping of addition doesn’t affect the result

IDENTITY ELEMENT: the identity is the unique element 0 (a + 0 = a)

INVERSE ELEMENT: the inverse of an element a is -a (a + (-a) = 0) then...

WHY STUDY AND FORMALIZE GROUPS?

“Group theory studies **symmetry**. There are symmetries everywhere.

Not only is there is symmetry in everyday life, there are symmetries in molecules, physical laws, crystals, formulae, music, and so forth. The symmetries get increasingly complicated, and an understanding of the symmetries gives insight into real properties of these objects.

I want to note that group theory studies **symmetry in the very broad sense of "reversible transformations that preserve some kind of structure"**. While being reflected in a mirror and remaining unchanged is the usual idea of symmetry, swapping x and y in $x^3+y^3+z^3$ is also symmetry in this broader sense, as is transposing a piece of music a half-step down.”

Source: Yasha Berchenko-Kogan, Math postdoc (Quora answer to “What is the point of group theory?”)

EXAMPLE: TURNS OVER THE RUBIK'S CUBE

GROUP: (G, ·)
SET: G,
GROUP RULE: · (composition)

CLOSURE: performing moves one after another results in another move

ASSOCIATIVITY: grouping of symmetries doesn't affect the result

IDENTITY ELEMENT: the identity is the empty permutation E (no moves)

INVERSE ELEMENT: the inverse of an element a is the reverse permutation, denoted a'

EXAMPLE: RUBIK'S CUBE (extended)

A MORE PRECISE SET: $G = \{ (v, r, w, s) \mid v \in C_3{}^7, r \in S_8, w \in C_2{}^{10}, s \in S_{12} \}$

where: v is the orientations of the corner cubies

r is the permutations of the corner cubies

w is the orientations of the edge cubies

s is the permutations of the edge cubies

EXAMPLE: RUBIK'S CUBE (extended)

A MORE PRECISE SET: $G = \{ (v, r, w, s) \mid v \in C_3^{\,7}, r \in S_8, w \in C_2^{\,10}, s \in S_{12} \}$

where: v is the orientations of the corner cubies

r is the permutations of the corner cubies

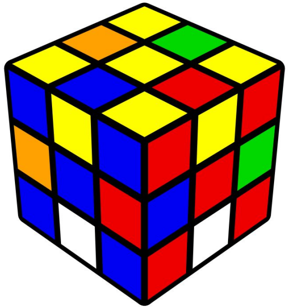
w is the orientations of the edge cubies

s is the permutations of the edge cubies

Example: Superflip

v = (1)(2)(3)(4)(5)(6)(7)

w = (1)(2)(3)(4)(5)(6)…(11)



r = (0, 0, 0, 0, 0, 0, 0, 0)

s = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)

jonlam

EXAMPLE: RUBIK'S CUBE (extended)

A MORE PRECISE SET: $G = \{ (v, r, w, s) \mid v \in C_3^{7}, r \in S_8, w \in C_2^{10}, s \in S_{12} \}$

where: v is the orientations of the corner cubies

r is the permutations of the corner cubies

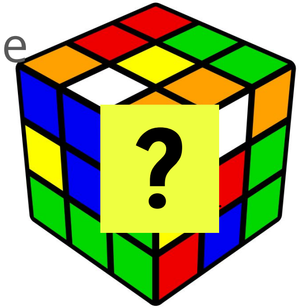
w is the orientations of the edge cubies

s is the permutations of the edge cubies

Example: Random scramble

v = (1423)(587)(6)

w = (1 12 5 7)(6 3 2 4) …



r = (0, 1, 1, 0, 2, 1, 0, 2)

s = (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)

EXAMPLE: RUBIK'S CUBE (extended)

A MORE PRECISE SET: $G = \{ (v, r, w, s) \mid v \in C_3^{\,7}, r \in S_8, w \in C_2^{\,10}, s \in S_{12} \}$

where: v is the orientations of the corner cubies

r is the permutations of the corner cubies

w is the orientations of the edge cubies

s is the permutations of the edge cubies

- The **cardinality** (order) of a group, denoted |G|, is the length of its set
  - $|G| = 43{,}252{,}003{,}274{,}489{,}856{,}000 = (12! * 2^{11} * 8! * 3^7) / 2$
  - Cardinalities for sets can be finite or *transfinite*

EXAMPLE: RUBIK'S CUBE (extended)

- The **order** of an element is how many times the group rule is applied to itself to attain the identity element
    - E.g.: U'·R'·U·R has order 6, because it takes six times to get back to E
    - E.g.: E has order 1 by definition

EXAMPLE: RUBIK'S CUBE (extended)

- The **order** of an element is how many times the group rule is applied to itself to attain the identity element
  - E.g.: U'·R'·U·R has order 6, because it takes six times to get back to E
  - E.g.: E has order 1 by definition
- A **subgroup** S_S of a group S is a group such that every element of S_s's set exists in S's set
  - E.g.: The permutation subgroup C_P changes positions of cubies but maintains orientations
  - E.g.: The orientation subgroup C_O changes orientation of cubies but maintains positions
  - E.g.: The Rubik's cube group G is a subgroup of the symmetry group S_{48}

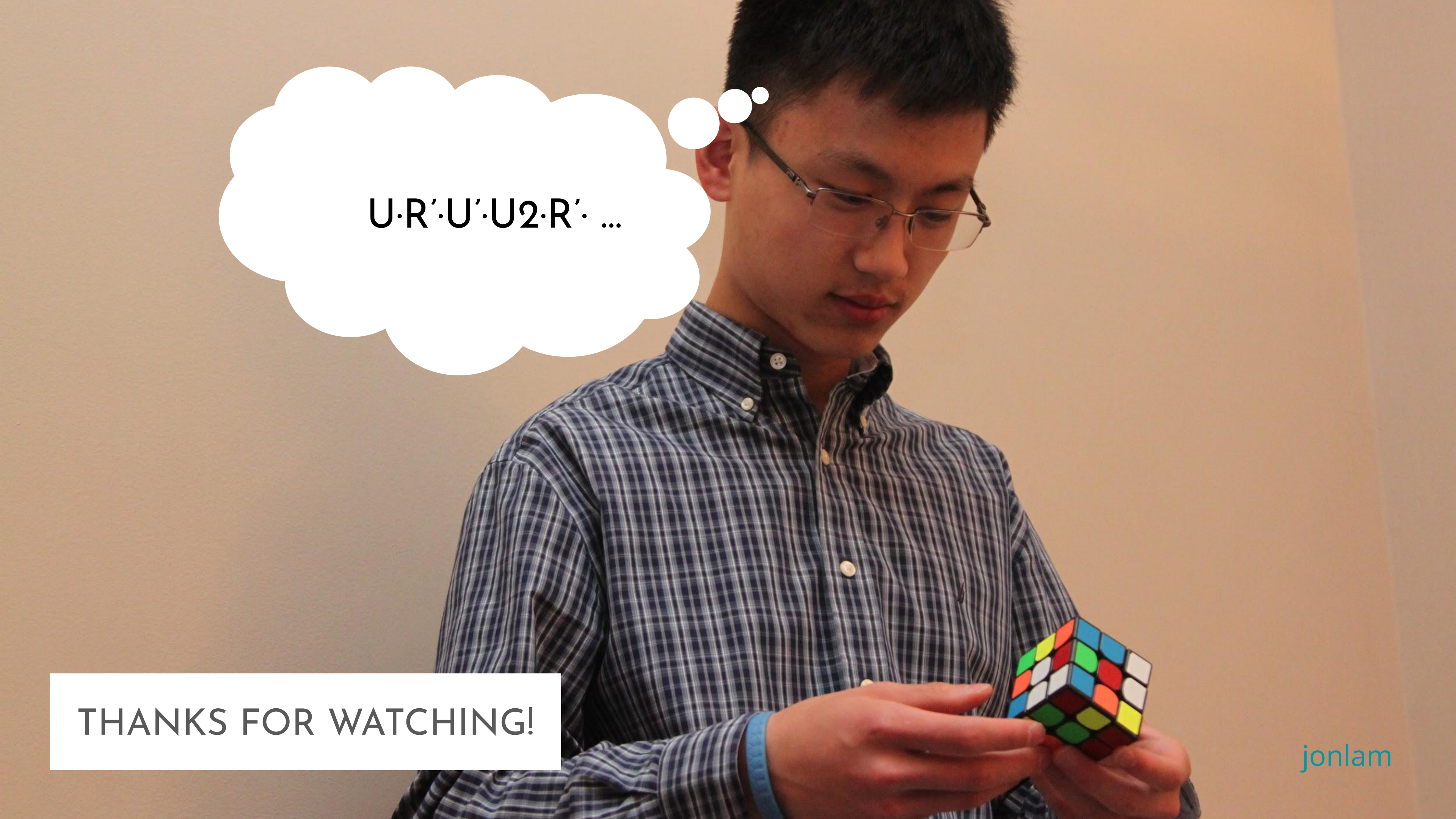
EXAMPLES OF GROUP APPLICATIONS

Model / Associate mathematical objects with groups, then *study* the properties of the groups.

- Permutation groups → polynomials, combinatorics, puzzles
- Lie groups → mechanical laws of physics
- Galois groups → solvability of higher-order polynomials
- the Fundamental group → mathematical topology
- Geometric group theory → algebraic geometry, number theory
- Computational group theory → cryptography, algorithmic approaches

RECENT / CURRENT ACTIVITY

- The classification of finite simple groups (i.e., groups that are finite and cannot be broken down into smaller groups), until 2004.
- Used to model and advance the knowledge in:
  - computer graphics
  - cryptography (multiplicative group modulo n in RSA)
  - elementary particle physics
  - the Standard Model
  - special relativity


U·R′·U′·U2·R′· ...
THANKS FOR WATCHING!
jonlam

WORKS CONSULTED

General sources:

"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>.

WORKS CONSULTED (cont'd.)

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>.

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>.

WORKS CONSULTED (cont'd.)

[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/>.

WORKS CONSULTED (cont'd.)

"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>.

WORKS CONSULTED (cont'd.)

"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>.

Jha, Raghav Govind. "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 (cont'd.)

[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>.

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>.

WORKS CONSULTED (cont'd.)

[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>.

"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>.

WORKS CONSULTED (cont'd.)

"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>.

WORKS CONSULTED (cont'd.)

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

"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>.

jonlam

WORKS CONSULTED (cont'd.)

“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/>.

WORKS CONSULTED (cont'd.)

<u>Scholarly articles specific to the Rubik's Cube Group in relation to Group Theory:</u>

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>.

WORKS CONSULTED (cont'd.)

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>.

<u>Images</u>:

Cube Rider API: http://cube.crider.co.uk/visualcube.php