An Introduction to Group Theory through Puzzles

Kevin Santos

University of Toronto

2021

Outline

Table of Contents

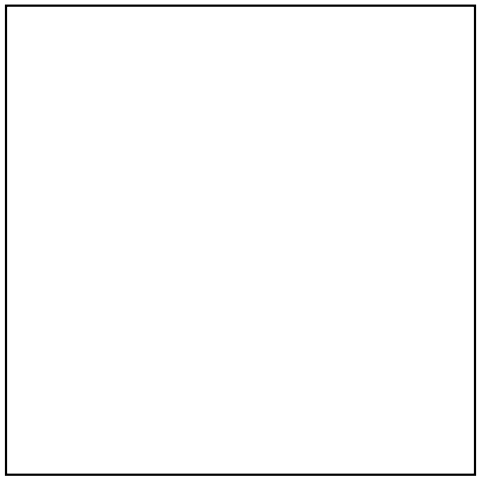
What is group theory?

A group is a set, along with a way of combining objects in the set, that fulfills certain properties.

Groups provide one of the main foundations for the field of algebra; they're an example of an **algebraic structure**.

Symmetries of the square

What are some of the symmetries of a square?



A symmetry can be thought of as a function mapping the square onto itself.

Combining symmetries

The set of all symmetries can be written:
$\{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

We can compose two symmetries to get another symmetry in the set.

$R_{90} \circ R_{180} =$

$V \circ V =$

$R_{270} \circ H =$

The dihedral group of order 4 (D_4)

$\circ$	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D	D'
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{90}	R_{180}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

Definition of a group

Definition

A **group** is a set G with an operation $\star$ such that the following properties hold for all elements a, b, c in G:

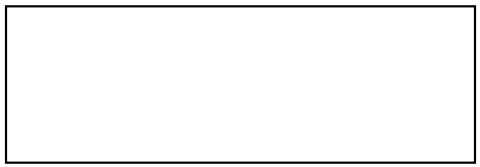
1. **Closure**: $a \star b$ is also an element in G
2. **Associativity**: $(a \star b) \star c = a \star (b \star c)$
3. **Identity**: There is an element e where $a \star e = e \star a = a$ for all a in G
4. **Inverses**: For each a in G, there is an element x in G where $a \star x = x \star a = e$

Note that we usually denote the operation by writing the two terms next to each other, when the operation is known or obvious: $a \star b = ab$

Familiar examples of groups: $(\mathbb{Z}, +)$, $(\mathbb{R}, \times)$
Example of a non-group: $(\mathbb{Z}, \times)$

The Klein 4-group

What if we instead look at the symmetries of a rectangle?



Using the previous notation, the set of symmetries is $\{R_0, R_{180}, H, V\}$

This set also forms a group with composition. This **subgroup** of D_4 has some nice properties!

The Klein 4-group

$\circ$	R_0	R_{180}	H	V
R_0	R_0	R_{180}	H	V
R_{180}	R_{180}	R_0	V	H
H	H	V	R_0	R_{180}
V	V	H	R_{180}	R_0

$+$	0	x	y	z
0	0	x	y	z
x	x	0	z	y
y	y	z	0	x
z	z	y	x	0

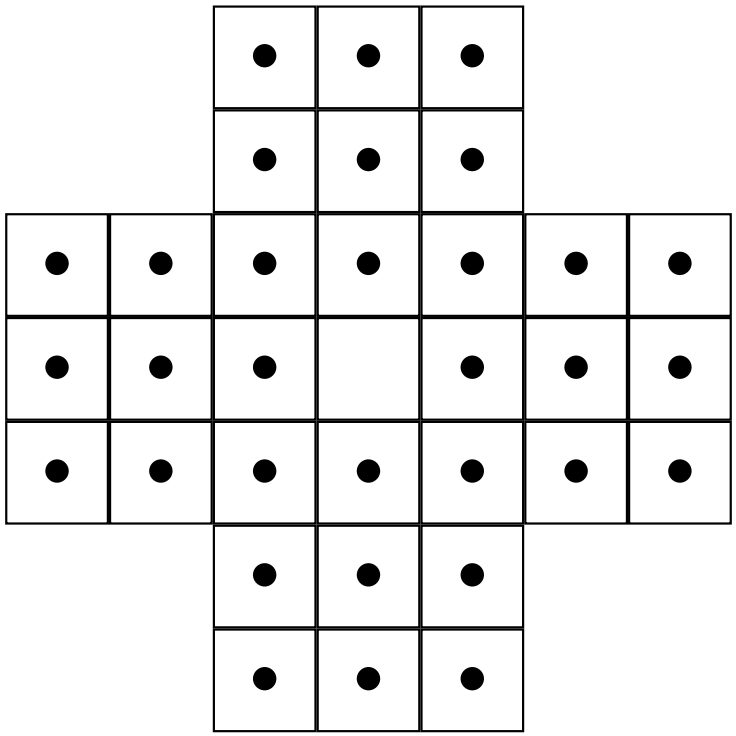
- Combining two different (non-identity) elements gives the third (non-identity) element.
- The operation is **commutative**. $x + y = y + x$. That means the group is **abelian**.
- Each element is its own inverse.
- By the above properties, $x + y + z = 0$.
- (Technically the Klein 4-group is isomorphic to the direct product $\mathbb{Z}/2 \oplus \mathbb{Z}/2$)

Table of Contents

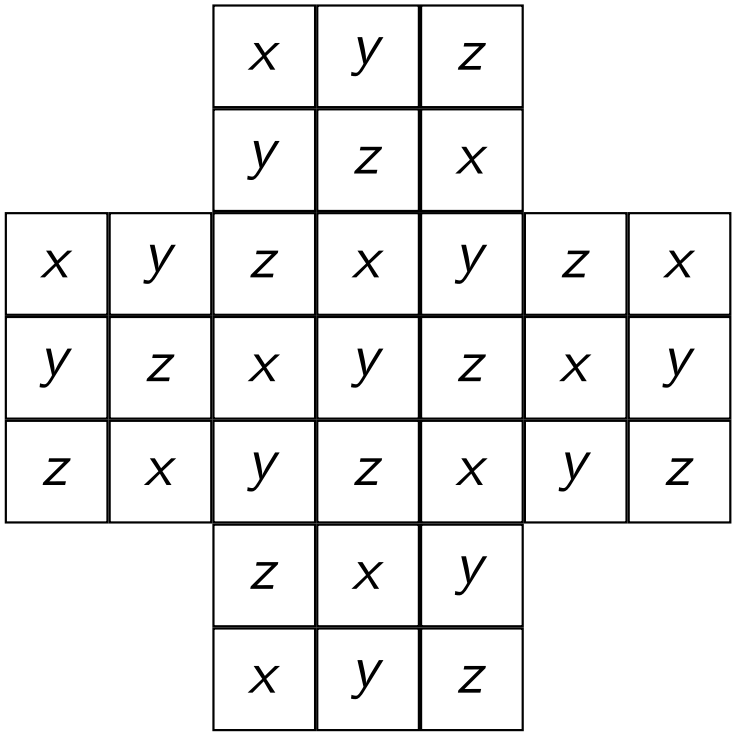
Peg solitaire

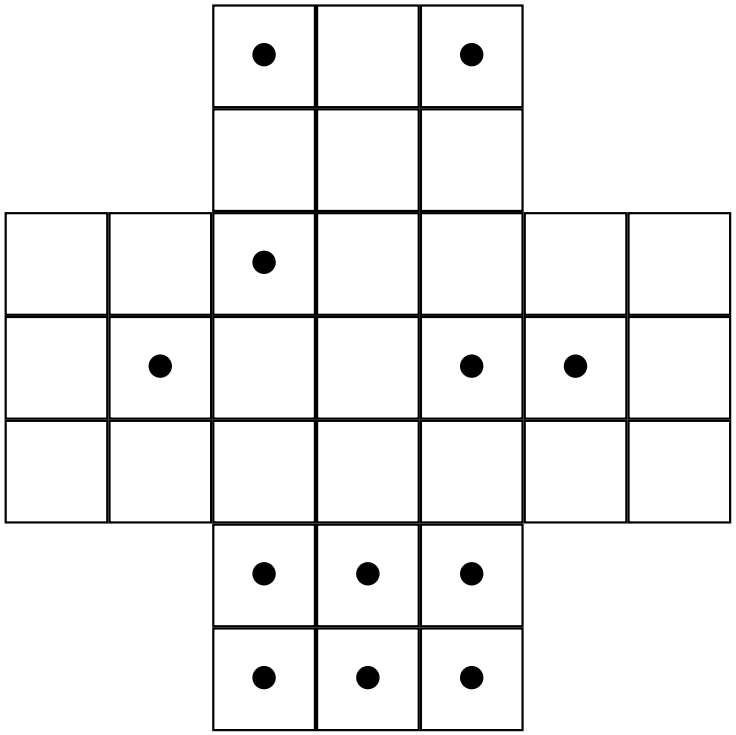
The objective of peg solitaire is to perform a series of moves so that you end up with only one peg left on the board. We eliminate a peg by using an adjacent peg to "jump" over it into an empty spot.

We can apply some group theory to determine the possible winning positions, or if it's even possible to win!



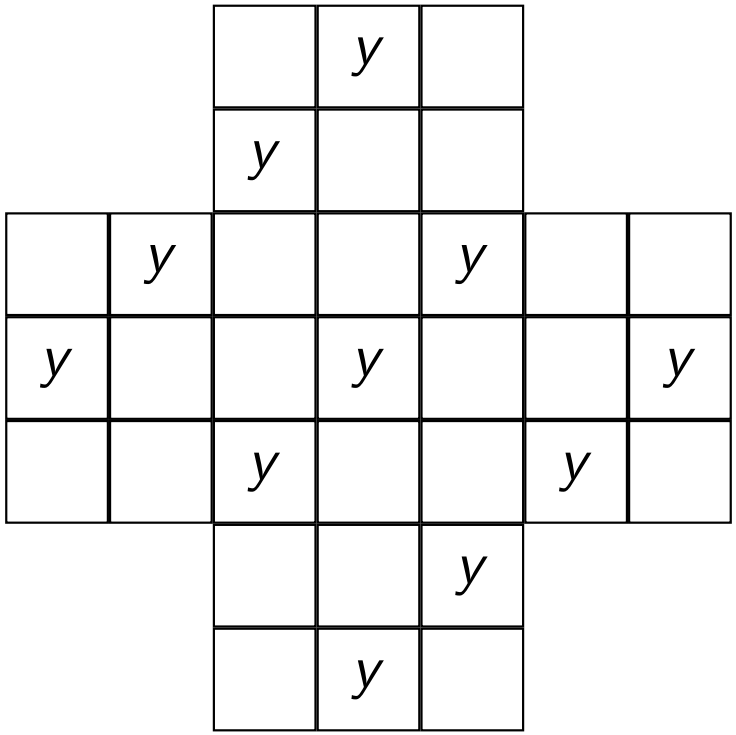
Labelling the board





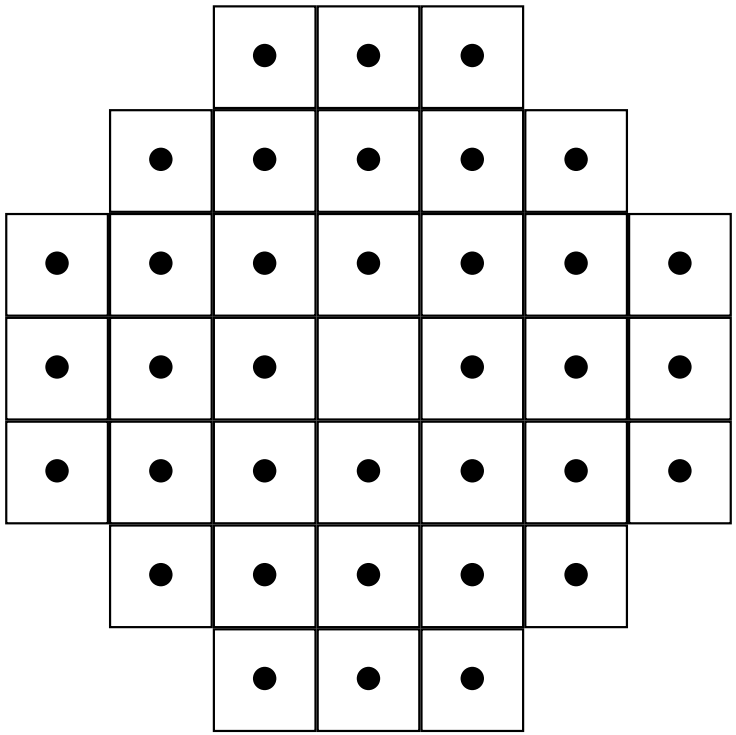
Possible winning end states

Since the initial configuration has a sum of y, and applying a move doesn't change the sum of the configuration, any achievable state must also sum to y.
That means that if we end up with one peg remaining, it must be on a square labelled y.

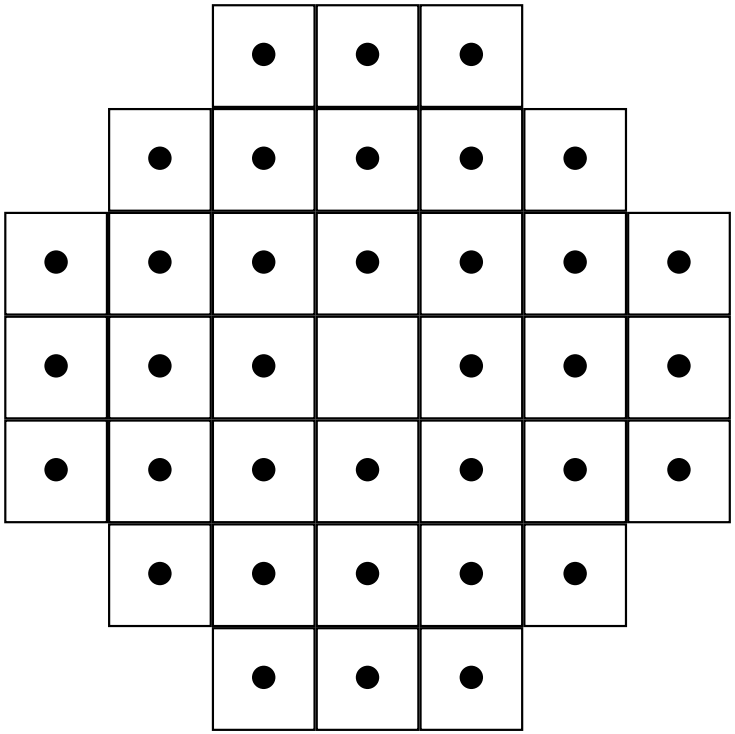


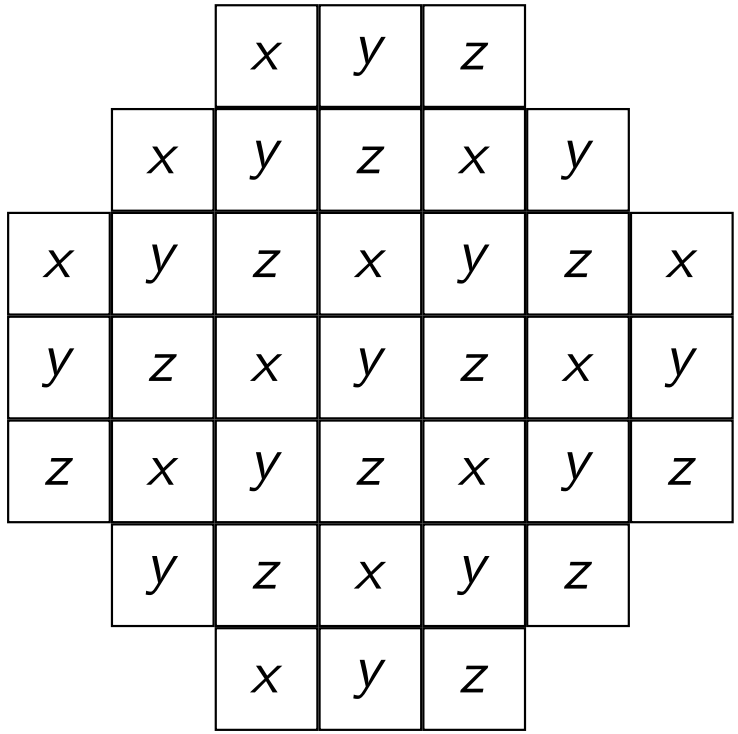
A different board

What if we alter the board slightly?



A different board





We can label the board like the original one, so that applying a move doesn't alter the configuration's sum. In this case, the sum of the initial arrangement is 0. But there's no way to have an arrangement with a single peg that also sums to 0, since no squares are labelled with 0.

Table of Contents

The 15 Puzzle

The original 15 puzzle was created and sold in the 1870s and became popular in America and Europe. The challenge was to start with the first configuration below and slide the tiles around to end up with the second configuration.

We want to use group theory to represent different configurations and moves.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

The original challenge

The original goal of the 15 puzzle was to apply a series of moves to the starting arrangement, and end up with the 14 and 15 tiles switched, with all the other tiles in their initial location.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Revisiting symmetries of the square

Permutations

Definition

A **permutation** on a set A is a function from A to A that is one-to-one and onto.

You may be familiar with permutations as "different arrangements of the objects in a set".

Different arrangements of a set can be realized as functions.

Representing permutations

Permutations can be represented using **cycle notation.**

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

$$\alpha =$$

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

$$\beta =$$

Permutation groups

Definition

The symmetric group of degree n, S_n, is the group of all permutations on the set $\{1, 2, 3, ..., n\}$

The operation on this group is the usual composition of functions.

(You can represent this in cycle notation and find the product of two cycles, but it's a bit involved, so I won't go into it here.)

Note the **identity** in the group is the identity permutation, i.e. the identity function on the set. It's written as (1).

Decomposing permutations

Every permutation can be written as a product of **2-cycles/transpositions**.

For example, $\alpha = (1432)$ can be rewritten $\alpha = (12)(13)(14)$

Parity of permutations

Similar to the natural numbers, any given permutation must be either even or odd.

Definition

A permutation α is **even** if it can be written as the product of an even number of 2-cycles/transpositions.
A permutation α is **odd** if it can be written as the product of an odd number of 2-cycles/transpositions.

From the previous example, take $\alpha = (1432) = (14)(13)(12)$.
α can be written as three 2-cycles, so α is odd.

Notating configurations of the 15 puzzle

We'll label each of the slots on the grid from 1-16.

We can identify which numbered tile is in which slot using a permutation that maps (tile number) $\mapsto$ (slot number)
(We'll label the "blank"/"empty" tile as the 16th tile.)

So the following configuration can be associated with the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 7 & 9 & 6 & 16 & 4 & 3 & 2 & 1 & 5 & 12 & 10 & 13 & 15 & 11 & 14 & 8 \end{bmatrix}$$

8	7	6	5
9	3	1	
2	11	14	10
12	15	13	4

The original challenge

The original goal of the 15 puzzle was to apply a series of moves to the starting arrangement, and end up with the 14 and 15 tiles switched, with all the other tiles in their initial location.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

No possible solution

Proof. (By contradiction) In each basic move of the puzzle, you exchange the positions of the blank space (tile 16) and another tile. The move where two tiles in position i and j are swapped (but all the other pieces are the same) can be described by the permutation $(i\,j)$.

The permutation for the starting position is the identity (1), while the permutation for the winning position is $(14\,15)$.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

No possible solution

If the puzzle were solvable, there would have to be some series of transpositions $\tau_1, \tau_2, ..., \tau_m$ so that

$$(14\,15) = \tau_m ... \tau_2 \tau_1 (1)$$

Since (1) is the identity, this can be rewritten

$$(14\,15) = \tau_m ... \tau_2 \tau_1$$

Note that the permutation (14 15) is odd—it can be written as 1 transposition, and 1 is odd.

No possible solution

$$(14\,15) = \tau_m \ldots \tau_2 \tau_1$$

Notice that in the two arrangements, the blank space is in the same spot. That means that after all the moves are applied, the empty space must have travelled up and down an equal number of times, and left and right an equal number of times. As well, each transposition changes the position of the blank space.

That means there must be an even number of transpositions on the right side. But $(14\,15)$ is an odd permutation. Therefore no solution is possible.

The 15 puzzle and the alternating group

It turns out that the set of even permutations in S_{16} form a group within themselves. Composing two even permutations results in an even permutation, like how adding two even numbers gives an even number. This **subgroup** of S_{16} is referred to as the alternating group A_{16}.

Consider the set of all possible arrangements of the puzzle where the blank space is in the lower right corner, i.e. permutations of the puzzle where the value of 16 is fixed. This set is exactly the alternating group A_{15}.

Table of Contents

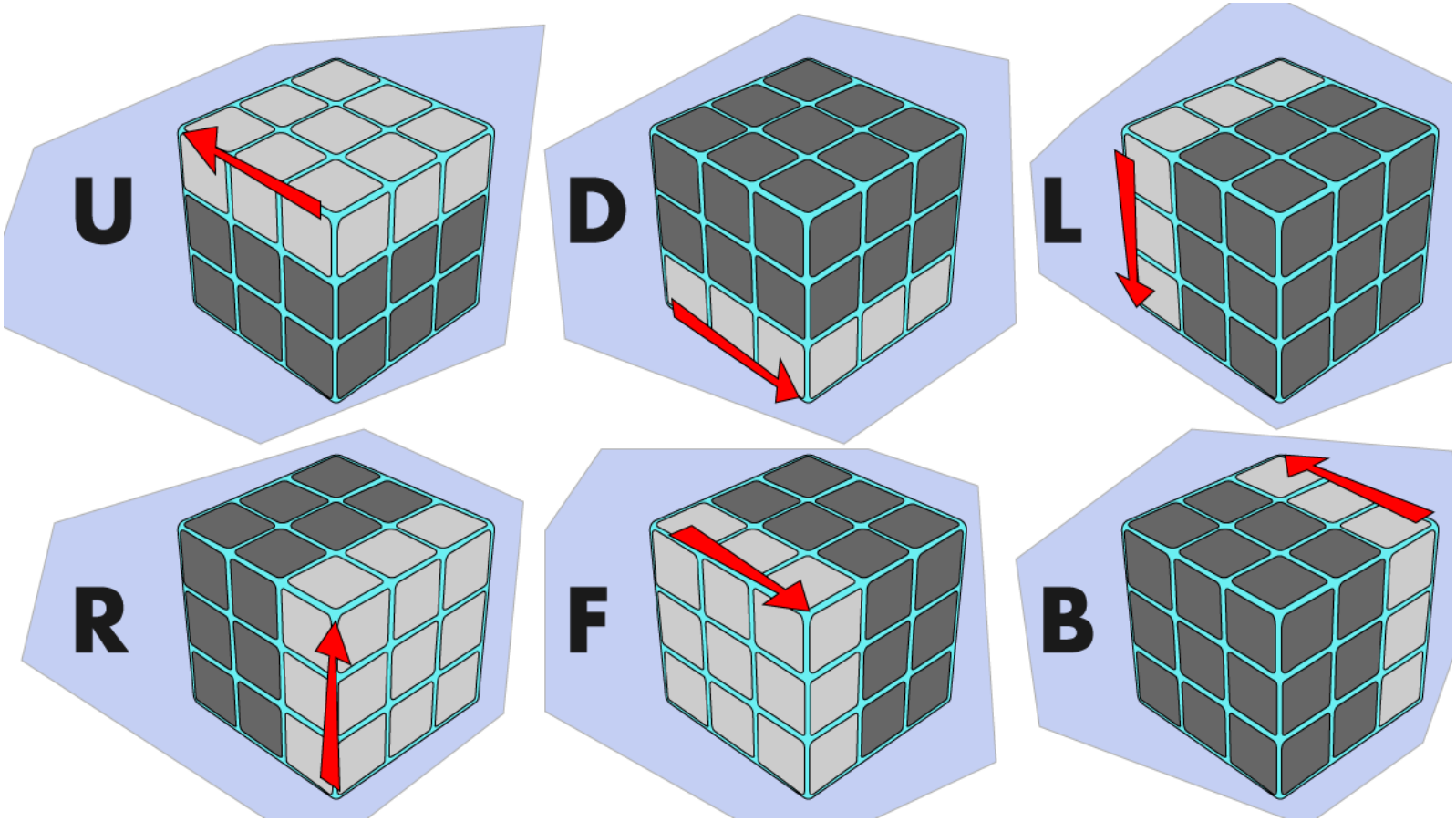
The Rubik's cube and God's number

We can use group theory to understand the different moves and configurations of the Rubik's cube.

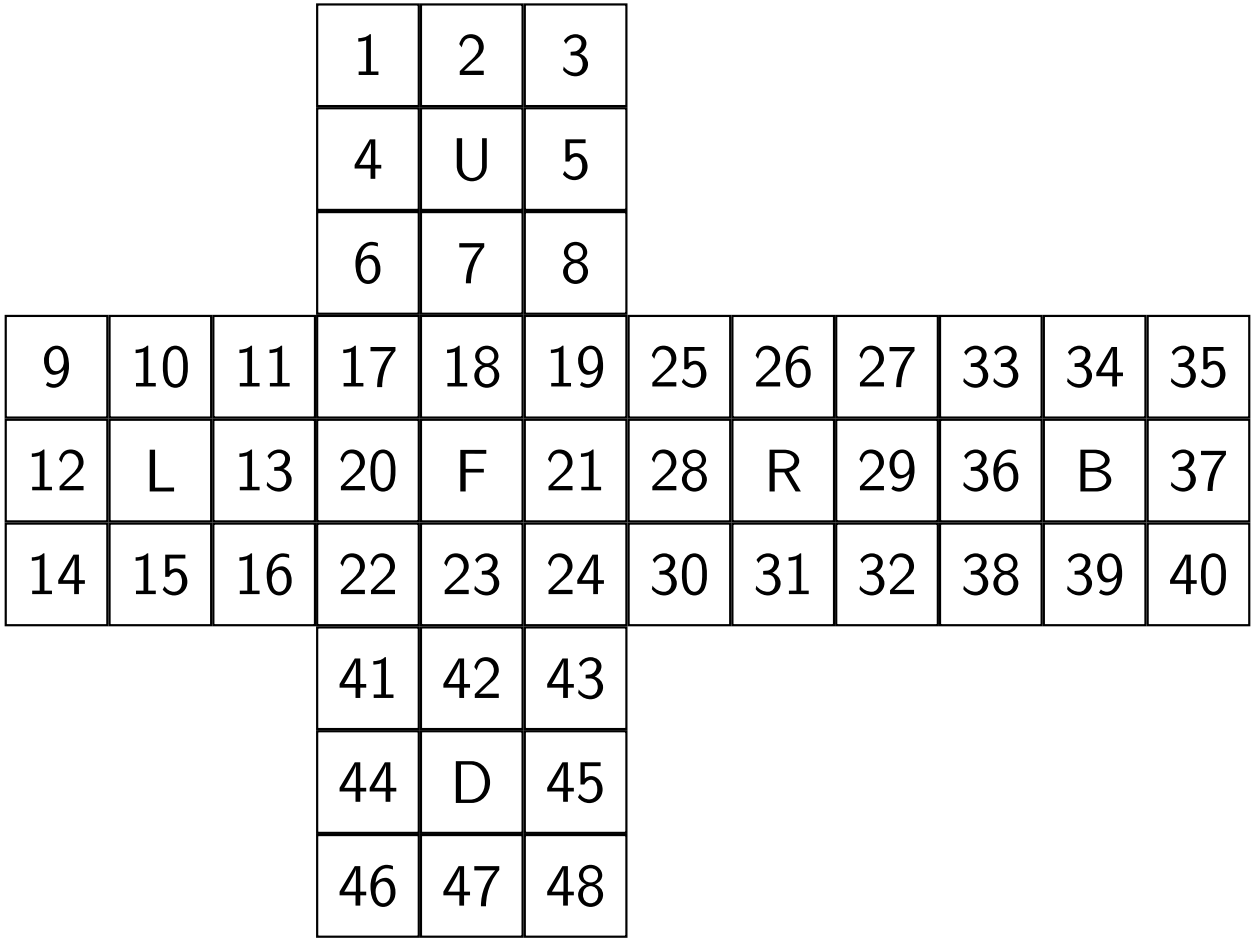
Mathematicians studying the cube wanted to determine **God's number**, the minimum number of moves required to solve a Rubik's cube.

Group theory was an important tool in the search for God's number.

Notating the Rubik's cube



Notating the Rubik's cube



Notating the Rubik's cube

$F = (17\ 19\ 24\ 22)(18\ 21\ 23\ 20)(6\ 25\ 43\ 16)(7\ 28\ 42\ 13)(8\ 30\ 41\ 11)$
$B = (33\ 35\ 40\ 38)(34\ 37\ 39\ 36)(3\ 9\ 46\ 32)(2\ 12\ 47\ 29)(1\ 14\ 48\ 27)$
$L = (9\ 11\ 16\ 14)(10\ 13\ 15\ 12)(1\ 17\ 41\ 40)(4\ 20\ 44\ 37)(6\ 22\ 46\ 35)$
$R = (25\ 27\ 32\ 30)(26\ 29\ 31\ 28)(3\ 38\ 43\ 19)(5\ 36\ 45\ 21)(8\ 33\ 48\ 24)$
$U = (1\ 3\ 8\ 6)(2\ 5\ 7\ 4)(9\ 33\ 25\ 17)(10\ 34\ 26\ 18)(11\ 35\ 27\ 19)$
$D = (41\ 43\ 49\ 46)(42\ 45\ 47\ 44)(14\ 22\ 30\ 38)(15\ 23\ 31\ 39)(16\ 24\ 32\ 40)$

These are all elements in S_{48}.

All arrangements of the Rubik's cube can be described as a product of all these moves.

The Rubik's cube group

The Rubik's cube group can be viewed as the subgroup of S_{48} generated by the six move permutations: $< F, B, L, R, U, D >$.
This isn't a very useful representation; we can narrow it down further.

Since the center square on each face is fixed, we can look at arrangements of the 8 corner pieces and 12 edge pieces.

The Rubik's cube group

Each of the 8 corner pieces has 3 possible configurations, which we can assign a number in $\mathbb{Z}/3 = \{0, 1, 2\}$.
Each of the 12 edge pieces has 2 possible configurations, which we can assign a number in $\mathbb{Z}/2 = \{0, 1\}$.
So we can denote an arrangement of the cube by a 4-tuple:
$(\alpha, \beta, \vec{v}, \vec{w}) \in S_8 \times S_{12} \times (\mathbb{Z}/3)^8 \times (\mathbb{Z}/2)^{12}$

The Rubik's cube group

But not all combinations of these elements are compatible with the Rubik's cube.

The permutations α and β need to have the same parity, i.e. they either need to both be even or both be odd.

As well, in the initial state of the cube, summing the configurations of the edge pieces and of the corner pieces gives 0. Applying a move doesn't change this overall sum. So the only possible choices for $\vec{v} = (v_1, ..., v_8) \in (\mathbb{Z}/3)^8$ and $\vec{w} = (w_1, ..., w_{12}) \in (\mathbb{Z}/2)^{12}$ are those where

$$\sum_{i=1}^{8} v_i = 0, \quad \sum_{i=1}^{12} w_i = 0$$

The order of the Rubik's cube group

Taking these considerations into account, we can represent the Rubik's cube group as

$$\Big\langle (\alpha, \beta, \vec{v}, \vec{w}) \in S_8 \times S_{12} \times (\mathbb{Z}/3)^8 \times (\mathbb{Z}/2)^{12} \mid sgn(\alpha) = sgn(\beta);\ \sum_{i=1}^{8} v_i = 0;\ \sum_{i=1}^{12} w_i = 0 \Big\rangle$$

The set of all configurations of the Rubik's cube forms a group of permutations of order 43,252,003,274,489,856,000.

God's number is 20 (!)

In 2010, Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge proved that God's Number for the Cube is exactly 20.

Date	Lower bound	Upper bound	Gap	Notes and Links
July, 1981	18	52	34	Morwen Thistlethwaite proves 52 moves suffice.
December, 1990	18	42	24	Hans Kloosterman improves this to 42 moves.
May, 1992	18	39	21	Michael Reid shows 39 moves is always sufficient.
May, 1992	18	37	19	Dik Winter lowers this to 37 moves just one day later!
January, 1995	18	29	11	Michael Reid cuts the upper bound to 29 moves by analyzing Kociemba's two-phase algorithm.
January, 1995	20	29	9	Michael Reid proves that the "superflip" position (corners correct, edges placed but flipped) requires 20 moves.
December, 2005	20	28	8	Silviu Radu shows that 28 moves is always enough.
April, 2006	20	27	7	Silviu Radu improves his bound to 27 moves.
May, 2007	20	26	6	Dan Kunkle and Gene Cooperman prove 26 moves suffice.
March, 2008	20	25	5	Tomas Rokicki cuts the upper bound to 25 moves.
April, 2008	20	23	3	Tomas Rokicki and John Welborn reduce it to only 23 moves.
August, 2008	20	22	2	Tomas Rokicki and John Welborn continue down to 22 moves.
July, 2010	20	20	0	Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge prove that God's Number for the Cube is exactly 20.

www.cube20.org

God's number is 20 (!)

"How did we solve all 43,252,003,274,489,856,000 positions of the Rubik's cube?

- *We partitioned the positions into 2,217,093,120 sets of 19,508,428,800 positions each.*
- *We reduced the count of sets we needed to solve to 55,882,296 using symmetry and set covering.*
- *We did not find optimal solutions to each position, but instead only solutions of length 20 or less.*
- *We wrote a program that solved a single set in about 20 seconds.*
- *We used about 35 CPU years to find solutions to all of the positions in each of the 55,882,296 sets."*

www.cube20.org

Further reading

- MATC01 (Groups and Symmetry) and MATD01 (Fields and Groups)
- Gallian — *Contemporary Abstract Algebra*
- www.cube20.org (documents the search for God's number)
- Berlekamp, Conway, Guy — *Winning Ways for your Mathematical Plays* (lots of fun applications of math in puzzles and games)

References

- Bialostocki, Arie. "An Application of Elementary Group Theory to Central Solitaire." *The College Mathematics Journal*, May 1998, Vol. 29, No. 3, pp. 208-212
- Rokicki, Tomas. "Twenty-Five Moves Suffice for Rubik's Cube." arxiv.org, Mar 2008. https://arxiv.org/abs/0803.3435
- Rokicki, Tomas. "God's Number is 20." www.cube20.org
- Conrad, Keith. "The 15-Puzzle (And Rubik's Cube)." Expository papers, math.uconn.edu. https://kconrad.math.uconn.edu/blurbs/grouptheory/15puzzle.pdf