The Mathematics of the Rubik’s Cube

A Group-Theoretic View

Ali Jafari
Isfahan University of Technology

Fall 2025

Introduction

The Rubik's Cube was invented in 1974 by Hungarian architect and professor Ernő Rubik. Originally called the *Magic Cube*, it was designed as a teaching tool to explain three-dimensional geometry. It became an international craze after its global release in 1980, and since then has inspired mathematicians, computer scientists, and puzzle enthusiasts worldwide.

Goal of This Talk

In this talk, we will explore the **Rubik's Cube as a mathematical structure**, specifically as an example of a **group** in abstract algebra.

The aim is not to find the fastest or most efficient algorithms for solving the cube, but rather to understand the **algebraic principles and symmetries** that govern its behavior.

Through this perspective, we can see how concepts such as *permutations, subgroups, and commutators* naturally arise from the simple act of twisting a cube.

Notation

To describe cube moves precisely, we use standard notation:

- U — Rotate the **Up** face clockwise
- U' — Rotate the Up face counterclockwise
- $D, D', L, L', R, R', F, F', B, B'$ — other faces
- $U2$ means a 180-degree turn of the Up face
- Example: $RUR'U'$ is a common move sequence

Each move represents a **permutation** of the cube's smaller pieces (cubies). Combining moves corresponds to composing permutations — the core of group theory.

Bounds on Solving a Rubik’s Cube

The **number of possible positions** of a standard Rubik’s Cube is approximately 43 quintillion (4.3×10^{19}).

Mathematicians have long asked: *“What is the minimal number of moves required to solve any scrambled cube?”*

- 1981 — Morwen Thistlethwaite proved it can be solved in at most 52 moves.
- 1995 — The bound was improved to 29 moves.
- 2010 — Using Google’s computing power, it was shown that any cube can be solved in at most **20 moves**.

This minimal number (20) is now called **God’s Number**. It represents the “diameter” of the cube group — the largest distance between any two states.

Motivation

Before abstract algebra, mathematicians encountered many structures with similar properties:

- Integers $(\mathbb{Z}, +)$ — closed, associative, with identity 0, and inverses (negatives)
- Nonzero real numbers $(\mathbb{R}^\times, \times)$ — multiplicative group
- Symmetries of a geometric object — composition of transformations

These examples suggested that an underlying algebraic structure was shared among them. This realization led to the **abstract definition of a group**.

Definition of a Group

A **group** is a set G equipped with a binary operation $*$ satisfying the following properties:

1. **Associativity:** For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
2. **Identity element:** There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
3. **Inverse element:** For each $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Basic Theorems about Groups

Theorem 1. The identity element of a group is unique. *Proof:* Suppose e and e' are both identity elements. Then $e = e * e' = e'$.

Theorem 2. Every element in a group has a unique inverse. *Proof:* Suppose a^{-1} and b^{-1} are both inverses of a. Then $a^{-1} = a^{-1} * (a * b^{-1}) = (a^{-1} * a) * b^{-1} = e * b^{-1} = b^{-1}$.

Theorem 3. The cancellation law holds: If $a * b = a * c$, then $b = c$.

Remarks

- Groups can be **abelian** (commutative) or **non-abelian**.
- Many puzzles and symmetry operations — including the Rubik's Cube — form non-abelian groups.
- The abstract definition allows us to study structure, not just numbers or shapes.

This abstraction is the foundation for understanding the cube's mathematical behavior.

The Rubik's Cube as a Group

To view the Rubik's Cube as a group, we consider each legal move (rotation of one face) as an element of a set G. The set G together with the operation "performing one move after another" forms a mathematical structure.

Definition
Let G be the set of all possible configurations of the Rubik's Cube obtained by legal moves. Define the operation $*$ such that $a * b$ means performing move a followed by move b. Then $(G, *)$ is a group if the following properties hold:

Closure

Closure: If a and b are two legal move sequences, their composition $a * b$ is also a legal sequence.

Example

If $a = R$ (rotate the right face) and $b = U$ (rotate the upper face), then $a * b = RU$ is also a valid move on the cube.

Thus, the set of all move sequences is **closed** under composition.

Associativity

Associativity: For any move sequences $a, b, c \in G$,

$$(a * b) * c = a * (b * c)$$

This means that the order of performing moves in pairs does not matter, as long as the total sequence remains the same.

Example:

$$((R)(U))D = R(UD)$$

Both correspond to performing R, then U, then D.

Identity Element

Identity: There exists an element $e \in G$ such that for all $a \in G$,

$$e * a = a * e = a$$

In the case of the Rubik's Cube, the identity move is doing nothing — the solved cube itself.

$$e = \text{“no move”}$$

Inverse Element

Inverse: For every move sequence $a \in G$, there exists an inverse sequence a^{-1} such that:

$$a * a^{-1} = a^{-1} * a = e$$

Example: If $a = R$, then $a^{-1} = R'$ (a counter-clockwise rotation of the same face).

$$R * R' = e$$

Thus, every move has a well-defined inverse.

Conclusion: Cube Group

Therefore, the set of all cube configurations with composition of moves forms a **group**, often denoted as $\mathcal{G}_{\text{Rubik}}$.

$$\mathcal{G}_{\text{Rubik}} = (G, *)$$

- Identity element: no move
- Inverse: reverse moves
- Operation: move composition
- Closed and associative

This group captures the deep algebraic structure behind the Rubik's Cube puzzle.

Non-Commutativity in the Rubik’s Cube

One of the most important properties of the Rubik’s Cube group is that it is **non-abelian**:

$$a * b \neq b * a$$

in general.

Example:

$$R * U \neq U * R$$

- Performing R (right face) then U (upper face) gives a different result from doing U then R.
- This shows that the order of operations matters.

If all moves commuted, solving the cube would be trivial — algorithms based on move sequences would not change anything.

Why Non-Commutativity Matters

The fact that moves do not commute allows us to build **commutator sequences**, which change some pieces while leaving others fixed. This is the foundation of most cube-solving algorithms.

Example:

$$[R, U] = RUR'U'$$

This sequence changes only a few cubies while restoring most of the cube, enabling controlled manipulation.

Thus, non-commutativity is not a bug — it's the key to solving the puzzle!

Commutators

Definition: Given two elements a, b in a group, the **commutator** is defined as:

$$[a, b] = aba^{-1}b^{-1}$$

It measures how far the group is from being abelian.

Commutators are used to move or swap a few pieces without disturbing most of the cube.

Commutators are the mathematical foundation for building localized cube algorithms.

Commutator Example 1: Rotating Two Corners

To twist two corners in opposite directions:

$$X = F' \, D \, F \, L \, D \, L' \qquad Y = U$$

Then:

$$[X, Y] = X \, Y \, X^{-1} \, Y^{-1}$$

Expanding gives:

$$(F' \, D \, F \, L \, D \, L')(U)(L \, D' \, L' \, F' \, D' \, F)(U')$$

Effect: rotates the top front left corner clockwise and the top front right corner counterclockwise without disturbing the rest of the cube.

Using Commutators to Move Cubies

Observation: If two moves X and Y affect only a few of the same cubies, then they almost commute.

Therefore, the commutator

$$XYX^{-1}Y^{-1}$$

usually changes only a small number of cubies.

This makes commutators useful when the cube is almost solved, because they let us move only a few specific cubies without disturbing the rest.

Example: A Three–Cycle from a Commutator

Fact:
If exactly one cubie is moved by both X and Y, and no other cubie is affected by both moves, then the commutator

$$XYX^{-1}Y^{-1}$$

is a **three–cycle**. It moves three cubies a, b, c in a cycle:

$$a \mapsto b, \quad b \mapsto c, \quad c \mapsto a,$$

and leaves everything else fixed.

How to check this:

- a is the cubie moved by both X and Y.
- b is the cubie that Y moves to a.
- c is the cubie that X moves to a.

Commutator Example 2: Cycling Three Corners

To cycle three corners on the upper layer:

$$X = L\,D\,L' \qquad Y = U$$

Then:

$$[X, Y] = X\,Y\,X^{-1}\,Y^{-1}$$

Expanding gives:

$$(L\,D\,L')U(L\,D'\,L')U'$$

Conjugation

Definition: For $g, h \in G$, the **conjugate** of h by g is:

$$ghg^{-1}$$

Intuition: Conjugation means applying a move pattern, rotating the cube's perspective, performing a sequence, and then undoing the rotation.

Example:

$$R(UR'U')R'$$

This "wraps" a simple algorithm inside another move, repositioning its effect to another part of the cube.

Conjugation is fundamental for generalizing algorithms to affect different cube layers.

Cycling Three Top Corners while preserving orientation

Let

$$X = FLF^{-1}, \quad Y = R^2, \quad Z = F^2.$$

The only cubie moved by both X and Y is the front bottom right corner. Therefore, the commutator $[X, Y]$ is a three-cycle of corners.

We can check that it cycles the *top front right*, *front bottom right*, and *front bottom left* corners.

Z moves the latter two corners to the top layer. Hence, the conjugate

$$Z[X, Y]Z^{-1} = F'LF'R^2FL'F'R^2F^2$$

cycles three corners on the top layer.

Commutators and Conjugation in Algorithms

Commutator = small controlled change. **Conjugation** = same change, different location.

In the Beginner's Method:

- Use commutators to fix corner orientation.
- Use conjugation to repeat that same effect on other corners.

In Advanced Methods:

- Full algorithms are often combinations of multiple conjugated commutators.
- Example: a PLL algorithm is a conjugate of a short commutator pattern.

These two algebraic tools make modern cube-solving algorithms possible.

Summary

- The Rubik’s Cube group is **non-abelian**.
- Non-commutativity allows algorithmic manipulation of specific pieces.
- **Commutators** control small local changes.
- **Conjugation** lets us “move” an algorithm to another location on the cube.

These operations form the algebraic foundation of solving methods such as the Fridrich (CFOP) and beginner’s method.

Subgroups of the Cube Group

Definition: A subset $H \subseteq G$ is a **subgroup** of G if it is itself a group under the same operation.

In the Rubik's Cube, subgroups naturally appear when we restrict our moves.

Examples:

- $H_1 = \langle R \rangle$: rotations of the right face.
- $H_2 = \langle U, D \rangle$: rotations of the upper and down faces.
- $H_3 = \langle R, U \rangle$: a common 2-generator subgroup.

Each subgroup represents all positions reachable by using only the given moves.

Finite Nature of Generated Subgroups

Claim: Every subgroup generated by a finite set of Rubik's Cube moves is **finite**.

Reasoning:

- The Rubik's Cube group G is finite.
- Any subgroup $H \leq G$ is therefore also finite.
- Consequently, any sequence of moves in H must eventually repeat a previous configuration.

Conclusion: No matter what moves you apply within a generated subgroup, after finitely many moves the cube returns to a previous state.

Lagrange’s Theorem

- **Theorem:** If H is a subgroup of a finite group G, then the order of H divides the order of G.
- **Implication:** For any element $g \in G$, the size of the subgroup $\langle g \rangle$ generated by g divides $|G|$.
- Useful for studying subgroups generated by Rubik’s Cube moves.

Subgroups Generated by Moves

Generators	Size	Factorization
U	4	2^2
U, RR	14400	$2^6 \cdot 3^2 \cdot 5^2$
U, R	73483200	$2^6 \cdot 3^8 \cdot 5^2$
RRLL, UUDD, FFBB	8	2^3
Rl, Ud, Fb	768	$2^8 \cdot 3$
RL, UD, FB	6144	$2^{10} \cdot 3$
FF, RR	12	$2^2 \cdot 3$
FF, RR, LL	96	$2^5 \cdot 3$
FF, BB, RR, LL, UU	663552	$2^{13} \cdot 3^4$
LLUU	6	$2 \cdot 3$
LLUU, RRUU	48	$2^4 \cdot 3$
LLUU, FFUU, RRUU	82944	$2^{13} \cdot 3^4$
LLUU, FFUU, RRUU, BBUU	331776	$2^{12} \cdot 3^4$
LUlu, RUru	486	$2 \cdot 3^5$

Observations from Lagrange's Theorem

- The sizes of subgroups always divide the total order of the Rubik's Cube group, $|G| = 4.3.10^{19}$ approximately.
- Combining more generators usually produces a larger subgroup.
- Factorization helps to quickly check divisibility and subgroup structure.
- Useful for algorithm design: knowing the subgroup order tells us how many states are reachable using specific moves.

Permutation

Definition: A **permutation** of a set X is a bijection from X to itself.

Example: If $X = \{1, 2, 3\}$, one permutation is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

which sends $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$.

Rubik’s Cube as a Subgroup of S_{48}

- Label the 48 movable stickers of the cube.
- Each legal cube move corresponds to a permutation of these stickers.
- The set of all legal moves forms a **group** G:

$$G \leq S_{48}$$

- G is a **subgroup** of the symmetric group on 48 elements.

Cycles and Order of a Permutation

- Any permutation can be written as a product of **disjoint cycles**.
- **Order** of a permutation σ is the smallest n such that $\sigma^n = \mathrm{id}$.
- Example: $\sigma = (1\,2\,3)(4\,5)$ has order $\mathrm{lcm}(3, 2) = 6$.

Parity of a Permutation

- A permutation is **even** if it can be written as a product of an even number of transpositions.
- Otherwise, it is **odd**.
- Example: $(1\,2\,3) = (1\,3)(1\,2)$ is even.
- The Rubik's Cube group only allows **even permutations** of corners and edges.

Group Homomorphism

Definition: A function $\phi : G \to H$ between groups is a **homomorphism** if

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \quad \forall g_1, g_2 \in G$$

Example: The map from the Rubik's Cube group to the corner permutation group is a homomorphism, because composition of moves respects the cube's structure.

Why a Single Swap is Impossible

Key idea: Every legal move on the Rubik's Cube induces an *even* permutation on the cubies.

We see this using the sign homomorphism:

$$\mathrm{sgn} : S_{20} \to \{\pm 1\}.$$

- A face quarter-turn cycles 4 corners (a 4-cycle) and 4 edges (another 4-cycle).
- A 4-cycle has sign $(-1)^{4-1} = -1$.
- The product of two 4-cycles has sign

  $$(-1) \cdot (-1) = +1.$$

  So every quarter-turn is even.
- A half-turn is a product of four transpositions → also even.

Conclusion: Every generator of the cube group is even, so every legal cube move is an even permutation.

The Parity Obstruction

Since all face moves are even permutations, the whole cube group satisfies

$$G \subseteq A_{20}.$$

Important fact
A **single swap of two cubies** is a transposition, and a transposition is an *odd* permutation.

$$\mathrm{sgn}(\text{transposition}) = -1.$$

Therefore:

- A single swap (of two edges or two corners) is not in G.
- No sequence of legal moves can perform such a swap.

Result: *You cannot switch only two cubies on a Rubik's Cube.*

Edge Orientation Invariant

Each edge cubie has two possible orientations. Define

$$\omega(e) = \begin{cases} 0, & \text{if edge } e \text{ is correctly oriented,} \\ 1, & \text{if edge } e \text{ is flipped.} \end{cases}$$

Let the total edge orientation be

$$\Omega = \sum_{e=1}^{12} \omega(e) \pmod{2}.$$

Key fact: A face turn does not flip edges. It only permutes them, so all $\omega(e)$ remain unchanged.

Therefore: Every legal cube move preserves Ω.

Why a Single Edge Flip Is Impossible

Starting from a solved cube,

$$\Omega = 0.$$

Since every legal move preserves Ω, every reachable configuration also has

$$\Omega = 0.$$

Consequence
A configuration with exactly one flipped edge has

$$\Omega = 1,$$

so it cannot be reached by legal Rubik's Cube moves.

Result: *Edges can only be flipped in pairs. A single edge flip is impossible.*

Why a Single Corner Cannot Rotate

- Let $o(C_1), \ldots, o(C_8)$ be corner orientations.
- Any legal move keeps:

$$\sum_{i=1}^{8} o(C_i) \equiv 0 \pmod 3$$

- Trying to twist only one corner changes the sum to 1 or 2 modulo 3
- Contradiction! ⍰

Why a Single Corner Cannot Rotate

- Let $o(C_1), \ldots, o(C_8)$ be corner orientations.
- Any legal move keeps:

$$\sum_{i=1}^{8} o(C_i) \equiv 0 \pmod 3$$

- Trying to twist only one corner changes the sum to 1 or 2 modulo 3
- Contradiction! ⍰

Conclusion: A single corner rotation is impossible.

Naive Count of Cube Configurations

- Corners: 8! permutations × 3^8 orientations
- Edges: 12! permutations × 2^{12} orientations
- Total naive configurations:

$$8! \cdot 3^8 \cdot 12! \cdot 2^{12}$$

- Many of these arrangements are **impossible on a real cube!**

Constraints of the Cube

- **Corner orientation:** sum must be divisible by 3 → only 1/3 of corner orientations valid
- **Edge orientation:** sum must be divisible by 2 → only 1/2 of edge orientations valid
- **Permutation parity:** corner permutation parity = edge permutation parity → only 1/2 of permutation arrangements valid

Conclusion: Only $1/12$ of all theoretical sticker arrangements are achievable on a real cube

Mathematical Implications

- The cube demonstrates how abstract algebraic structures model physical puzzles.
- It connects group theory, combinatorics, and computer algorithms.
- It provides a real-world example of non-commutativity and finite group actions.

Research on the cube has led to progress in:

- Algorithm optimization and symmetry reduction.
- Computational group theory (using GAP, Magma, etc.).
- Educational tools for teaching algebraic thinking.

Conclusion

- The Rubik's Cube is not just a puzzle—it is a **mathematical structure**.
- Group theory provides the language to describe and solve it.
- Concepts like closure, inverses, commutators, conjugation, and parity appear naturally and have practical meaning.
- The study of the cube beautifully connects **theory** and **practice**.

"Mathematics reveals the hidden symmetry behind every twist."

Follow-up Sessions

The topics covered in this presentation can be extended in follow-up sessions, for example:

- Commutators in the Rubik's Cube Group
- Algorithms and strategies for solving the Rubik's Cube

These sessions can explore deeper group-theoretic properties and practical solving techniques.

References

- The Mathematics of the Rubik’s Cube: Introduction to Group Theory and Permutation Puzzles, MIT SP.268 https://web.mit.edu/sp.268/www/rubik.pdf
- Rubik’s Cube, Wikipedia https://en.wikipedia.org/wiki/Rubik
- The Mathematics of Rubik’s Cube, Michael Hutchings, UC Berkeley https://math.berkeley.edu/ hutching/rubik.pdf