

Group Theory

Rubik's Cube and the Permutation Group

Mohammed Alshamsi

2021004826

mo.alshamsi@aurak.ac.ae

Coding Club at the American University of Ras Al Khaimah

October 10, 2024



Introduction

- ▶ **Group Theory?** Study of groups (abstract algebraic structures)
- ▶ **Format?** You'll see the following:
 - ▶ Mathematical definitions with examples
 - ▶ Applications to Rubik's cubes
- ▶ **Why Math?** You'll learn new ways of reasoning, which will enable you to make more sophisticated software.
- ▶ **These Slides?** See our [GitHub](#) repository.
- ▶ **Coding Background?** Check GitHub or find a guide online. (We won't need it in this presentation.)

Any questions?



Outline

1 Review of Sets

- Set Basics
- Functions

2 Groups

- Group Definition
- Examples
- Some Properties of Groups

3 Integers modulo 12

- Subgroups
- Generating Sets
- Cosets

4 The Rubik's Cube Group

- Thistlethwaite's Algorithm



Review of Sets

Example (Familiar Sets)

$$\{0, 1, 2, 3, \dots\} = \mathbb{N} \quad \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}$$

$$\left\{ \frac{p}{q} : p, q \in \mathbb{Z} \right\} = \mathbb{Q}$$

Definition

Union: $A \cup B$, all elements that are in A or B

Intersection: $A \cap B$, all elements that are in A and B

Subtraction: $A - B$, all elements in A that are not in B

Subset: $B \subseteq A$, all elements of B are in A.

Functions

Definition (Function)

$f : X \rightarrow Y$, rule that assigns to each element of X exactly one element of Y .
This is denoted $f(x)$

Definition (Operation)

$* : X \times X \rightarrow X$, assigns to each **pair** of elements x, y from X an element of X .
This is denoted $x * y$

Groups

Definition (Group)

Set G and an operation $* : G \times G \rightarrow G$, where:

- 1 $*$ is associative; $(a * b) * c = a * (b * c)$
- 2 There is $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
- 3 For each $a \in G$ there is a^{-1} such that $a^{-1} * a = a * a^{-1} = e$

Example (\mathbb{Z} under addition)

- 1 Addition is associative; $(a + b) + c = a + (b + c)$
- 2 Identity element is 0
- 3 Every element's inverse is its negative

\mathbb{Z} is a group under addition!

Notational shortcut: ab instead of $a * b$.

Group Example

Example (Integers modulo 12)

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Operation: Clock arithmetic. $8 + 9 = 5 \pmod{12}$, for example.

- 1 Associativity?
- 2 Identity?
- 3 Inverses?

It's a group.

Groups

Theorem (Group Properties)

- ▶ Identity is unique
- ▶ Cancellation law: $ab = ac \implies b = c$, and $ba = ca \implies b = c$
- ▶ Exactly one inverse per element
- ▶ Inverse of ab is $b^{-1}a^{-1}$

Integers modulo 12

Definition (Subgroup)

A subgroup H of G is a subset of the group set of G , that is also a group under the same operation. " $H \leq G$ " means " H is a subgroup of G ".

Example (Subgroups of \mathbb{Z}_{12})

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} \quad \text{and} \quad \{0\}$$

$$\{0, 6\}$$

$$\{0, 4, 8\}$$

$$\{0, 3, 6, 9\}$$

$$\{0, 2, 4, 6, 8, 10\}$$

Basic Properties of Subgroups

Theorem (Basic Properties of Subgroups)

- A subgroup H of a group G always contains the identity.
- The inverse of any $h \in H$ is the same as in G , and is also a part of H .

Integers modulo 12

Definition (Generating Set)

Given a group G and a subset S of its group set.

The set of all possible combinations (under G 's operation) of the elements of S and their inverses, forms a subgroup of G .

S is the generating set of the subgroup, and the subgroup is denoted $\langle S \rangle$.

Example (Generators in \mathbb{Z}_{12})

1 generates \mathbb{Z}_{12} .

2 generates $\{0, 2, 4, 6, 8, 10\}$.

3 generates:

4 generates:

6 generates:

What is $\langle 5 \rangle$?

Cosets

Definition (Coset)

For each element g of G , there exists a (*right*) coset of H in G , defined as follows:

$$Hg = \{hg : h \in H\}$$

Example (Right Cosets in \mathbb{Z}_{12})

$\{1, 3, 5, 7, 9, 11\}$ is a coset of $\langle 2 \rangle$. We can denote it by $\langle 2 \rangle + 1$, $\langle 2 \rangle + 3$, et cetera.
(They're all the same coset!)

Cosets of $\langle 3 \rangle$ are $\langle 3 \rangle$ itself, $\langle 3 \rangle + 1$, and $\langle 3 \rangle + 2$.

Cosets of $\langle 4 \rangle$ are:

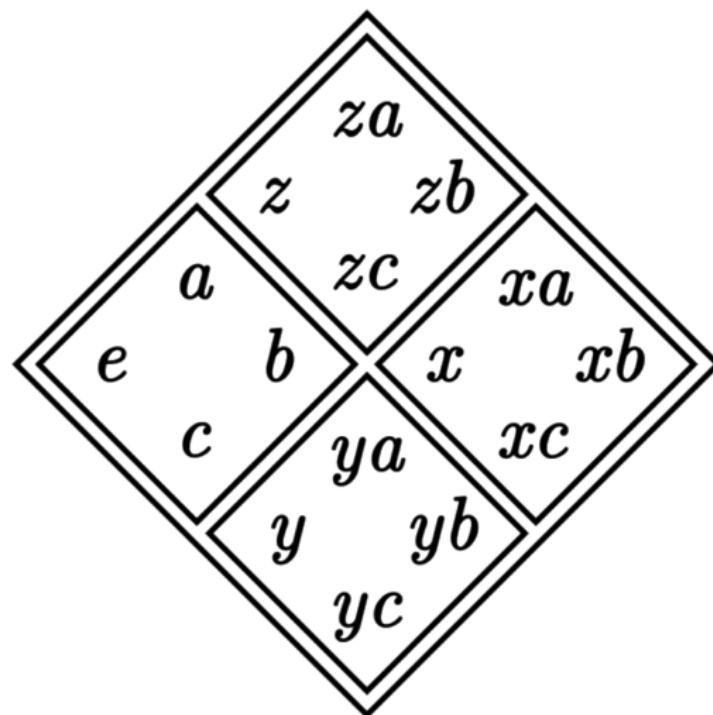
Cosets of $\langle 6 \rangle$ are:

Cosets

Theorem (Properties of Cosets)

- ▶ Hg_1 and Hg_2 , for any g_1 and g_2 , are either the same coset or are completely disjoint.
- ▶ All cosets of H , including H itself (He), are the same size.
- ▶ The union of all cosets of H produces the group set of G .
- ▶ (Lagrange's Theorem) The number of cosets, $(G : H)$, is equal to $\frac{|G|}{|H|}$.

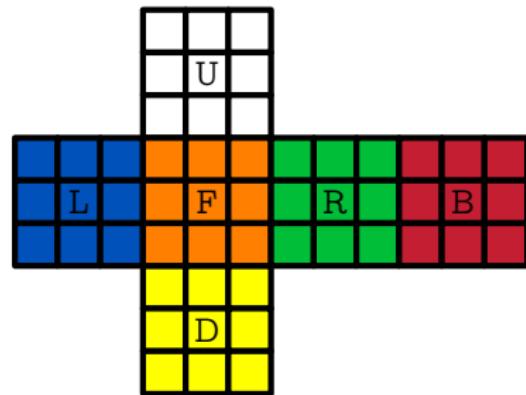
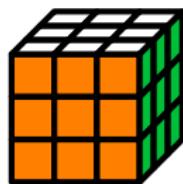
Cosets



(From [here](#).)

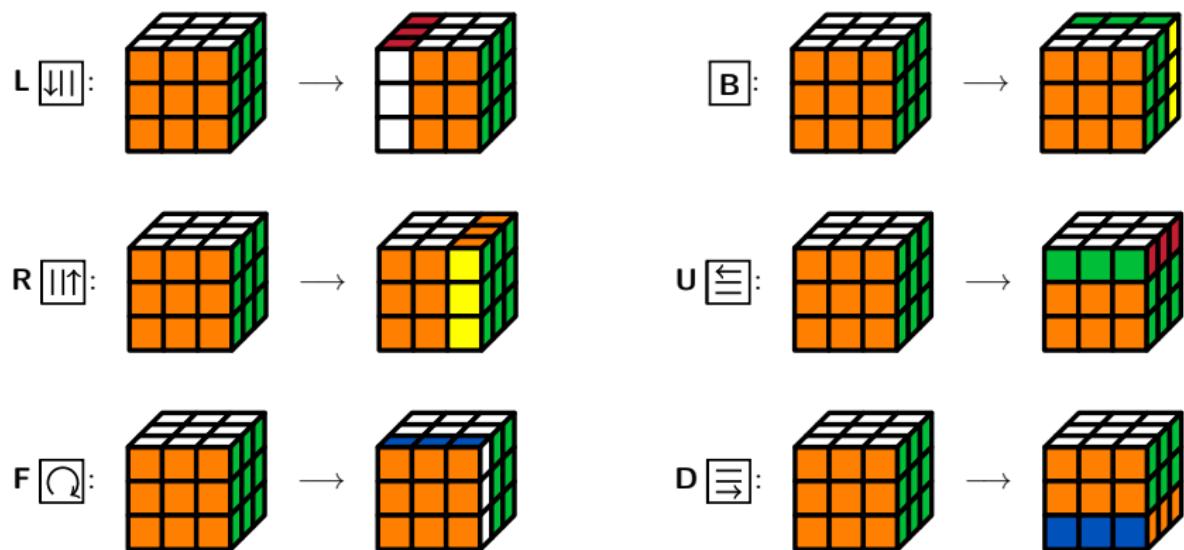
The Rubik's Cube

Here's a Rubik's Cube:



The Rubik's Cube Group

The group is generated by the following set of rotations:



This group has $2^{27}3^{14}5^37^211 = 43,252,003,274,489,856,000$ elements!

Nested Subgroups of the Rubik's Cube Group

The Rubik's Cube group G may be split into these subgroups:

$$G_0 = \langle L, R, F, B, U, D \rangle \quad |G_0| = 4.3 \times 10^{19}$$

$$G_1 = \langle L, R, F, B, U^2, D^2 \rangle \quad |G_1| = 2.1 \times 10^{16}$$

$$G_2 = \langle L, R, F^2, B^2, U^2, D^2 \rangle \quad |G_2| = 1.9 \times 10^{10}$$

$$G_3 = \langle L^2, R^2, F^2, B^2, U^2, D^2 \rangle \quad |G_3| = 6.6 \times 10^5$$

$$G_4 = \langle 1 \rangle \quad |G_4| = 1$$

G_{i+1} is a subgroup of G_i , and thus has cosets in G_i .

Definition (Coset Space)

The set of all right cosets of H in G is called its right coset space, and is denoted $H \setminus G$.

Thistlethwaite's Algorithm

$$G_4 \leq G_3 \leq G_2 \leq G_1 \leq G_0$$

Strategy: Traverse cosets in $G_{i+1} \setminus G_i$ to reach G_{i+1} . Repeat until G_4 reached.

- ▶ From G_0 to G_1 , we traverse a coset space of cardinality 2048, using all legal moves. Goal is to *orient* all the edges.
- ▶ $|G_2 \setminus G_1| = 1082565$. Goal is to orient all the corners.
- ▶ $|G_3 \setminus G_2| = 29400$. Goal is to correctly position the corners (which may lose orientation here), and put edges in their correct *slices*.
- ▶ $|G_4 \setminus G_3| = 663,552$. Goal is to re-orient the corners and position the edges, solving the cube.

Move choices are done using look-up tables.

Books on this Topic

There are others, but these two are in the library and I know they're good.

- *A Book of Abstract Algebra* by Charles Pinter
- *Algebra* by Michael Artin



That's All, Folks!

Thank you :)

(Full list of sources will be in the notes for this topic, coming soon)

Questions? Comments? Concerns?

