Number Theory

Coding Club

Mohammed Alshamsi
2021004826
mo.alshamsi@aurak.ac.ae

American University of Ras Al Khaimah

September 23, 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

Example (Familiar Sets)

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

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

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)

$f : X \to Y$, rule that assigns to each element of X exactly one element of Y.

This is denoted $f(x)$

Definition (Operation)

$* : X \times X \to X$, 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 $* : G \times G \to G$, 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!

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? Yes.
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 $b^{-1}a^{-1}$

Extended Example: Integers modulo 12

Definition (Subgroup)

A subgroup of H is a subset of the group set of G that is also a group under the same operation.

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

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

Basic Properties of Subgroups

Theorem (Basic Properties of Subgroups)

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

Extended Example: 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 $\langle 3 \rangle + 1$ and $\langle 3 \rangle + 2$.

Cosets of $\langle 4 \rangle$ are:

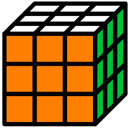
Cosets of $\langle 6 \rangle$ are:

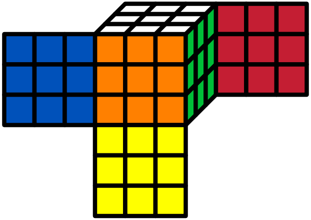
Properties of Cosets

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 $\frac{|G|}{|H|}$.

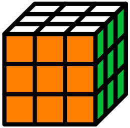
The Rubik's Cube Group

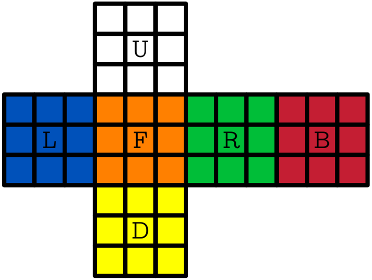




The Rubik's Cube

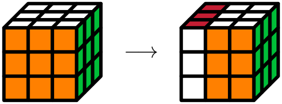
Here's a Rubik's Cube:

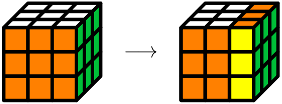


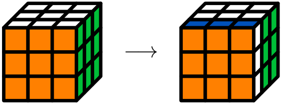


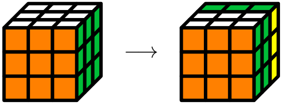
The Rubik's Cube Group

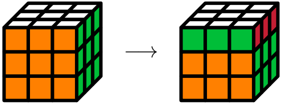
The cube is generated by the following set of rotations:

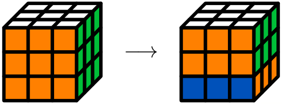
L :


R :


F :


B :


U :


D :


Singmaster Notation

Thistlethwaite's Algorithm