# Group Theory

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

January 21, 2026

# Groups

## Definition

A set $G$ with a binary operation $\star$ defined on it is called a group if

- the operation $\star$ is closed,
- the operation $\star$ is associative,
- there exists an identity element $e \in G$ such that for any $a \in G$

$$a \star e = e \star a = a,$$

- for every $a \in G$, there exists an element $b \in G$ such that

$$a \star b = b \star a = e.$$

## Example

- Modulo $n$ addition on $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

## Definition

A group is abelian if for all $a, b \in G$, we have $a \star b = b \star a$

# Cyclic Groups

## Definition

A finite group is a group with a finite number of elements. The order of a finite group $G$ is its cardinality.

## Definition

A cyclic group is a finite group $G$ such that each element in $G$ appears in the sequence

$$\{g, g \star g, g \star g \star g, \ldots\}$$

for some particular element $g \in G$, which is called a generator of $G$.

## Examples

- For an integer $n \geq 1$, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$
  - Operation is addition modulo $n$
  - $\mathbb{Z}_n$ is cyclic with generator 1
- For an integer $n \geq 2$, $\mathbb{Z}_n^* = \{i \in \mathbb{Z}_n \setminus \{0\} \mid \gcd(i, n) = 1\}$
  - Operation is multiplication modulo $n$
  - $\mathbb{Z}_n^*$ is cyclic if $n$ is a prime

# Subgroups

- **Definition:** If $G$ is a group, a nonempty subset $H \subseteq G$ is a *subgroup* of $G$ if $H$ itself forms a group under the same operation associated with $G$.
- Example: Consider the subgroups of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.
- **Lagrange's Theorem:** If $H$ is a subgroup of a finite group $G$, then $|H|$ divides $|G|$.
- Example: Check the cardinalities of the subgroups of $\mathbb{Z}_6$.
- **Corollary:** If a group has prime order, then every non-identity element is a generator.

# Fields

## Definition

A set $F$ together with two binary operations $+$ and $*$ is a field if

- $F$ is an abelian group under $+$ whose identity is called 0
- $F^* = F \setminus \{0\}$ is an abelian group under $*$ whose identity is called 1
- For any $a, b, c \in F$

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

## Definition

A finite field is a field with a finite cardinality.

# Prime Fields

- $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ where $p$ is prime
- $+$ and $*$ defined on $\mathbb{F}_p$ as

$$x + y = x + y \bmod p,$$
$$x * y = xy \bmod p.$$

- $\mathbb{F}_5$

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| * | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

- In fields, division is multiplication by multiplicative inverse

$$\frac{x}{y} = x * y^{-1}$$

# Characteristic of a Field

## Definition

Let $F$ be a field with multiplicative identity 1. The characteristic of $F$ is the smallest integer $p$ such that

$$\underbrace{1 + 1 + \cdots + 1 + 1}_{p \text{ times}} = 0$$

## Examples

- $\mathbb{F}_2$ has characteristic 2
- $\mathbb{F}_5$ has characteristic 5
- $\mathbb{R}$ has characteristic 0

## Theorem

*The characteristic of a finite field is prime*

# References

- Sections 9.1, 9.3 of *Introduction to Modern Cryptography*, J. Katz, Y. Lindell, 3rd edition
- Chapter 2 of *An Introduction to Bitcoin*, S. Vijayakumaran, `www.ee.iitb.ac.in/~sarva/bitcoin.html`