Finite Groups

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

September 15, 2015

Groups

Definition

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

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

Commutative Groups

Definition

A group G is called a commutative group if its binary operation is commutative.

Commutative groups are also called abelian groups.

Examples

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

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.

Example

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ is a cyclic group with a generator 1

Group Isomorphism

Example

- $\mathbb{Z}_2 = \{0, 1\}$ is a group under modulo 2 addition
- $R = \{1, -1\}$ is a group under multiplication

$$
\begin{array}{ccc}
\mathbb{Z}_2 & \qquad & R \\
0 \oplus 0 = 0 & & 1 \times 1 = 1 \\
1 \oplus 0 = 1 & & -1 \times 1 = -1 \\
0 \oplus 1 = 1 & & 1 \times -1 = -1 \\
1 \oplus 1 = 0 & & -1 \times -1 = 1
\end{array}
$$

Definition

Groups G and H are isomorphic if there exists a bijection $\phi : G \to H$ such that

$$\phi(\alpha \star \beta) = \phi(\alpha) \otimes \phi(\beta)$$

for all $\alpha, \beta \in G$.

Cyclic Groups and $\mathbb{Z}_n$

Theorem

Every cyclic group G of order n is isomorphic to $\mathbb{Z}_n$

Proof.

Let h be a generator of G. Define $h^i = \underbrace{h \star h \star \cdots \star h}_{i \text{ times}}$.

The function $\phi : G \to \mathbb{Z}_n$ defined by $\phi(h^i) = i \bmod n$ is a bijection. $\square$

Corollary

Every finite cyclic group is abelian.

Subgroups

Definition

A nonempty subset S of a group G is called a subgroup of G if

- $\alpha + \beta \in S$ for all $\alpha, \beta \in S$
- $-\alpha \in S$ for all $\alpha \in S$

Example

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has subgroups

- $\{0\}$
- $\{0, 3\}$
- $\{0, 2, 4\}$
- $\{0, 1, 2, 3, 4, 5\}$

Lagrange's Theorem

Theorem
If S is a subgroup of a finite group G, then $|S|$ divides $|G|$.

Definition
Let S be a subgroup of a group G. For any $g \in G$, the set $S \oplus g = \{s \oplus g | s \in S\}$ is called a coset of S.

Example
$S = \{0, 3\}$ is a subgroup of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. It has cosets

$$S \oplus 0 = \{0, 3\}, \quad S \oplus 1 = \{1, 4\}, \quad S \oplus 2 = \{2, 5\},$$
$$S \oplus 3 = \{0, 3\}, \quad S \oplus 4 = \{1, 4\}, \quad S \oplus 5 = \{2, 5\}.$$

Lemma
Two cosets of a subgroup are either equal or disjoint.

Lemma
If S is finite, then all its cosets have the same cardinality.

Application of Lagrange's Theorem

Prove that $2^{p-1} = 1 \bmod p$ for any prime $p > 2$.

- Consider the group $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$ under the operation

$$a \odot b = ab \bmod p$$

- Consider the subgroup S generated by 2

$$\left\{2, 2^2, 2^3, \ldots, 2^{n-1}, 2^n = 1\right\}$$

- What can we say about the order of S?

Subgroups of Cyclic Groups

Example

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has subgroups $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$, $\{0, 1, 2, 3, 4, 5\}$

Theorem

Every subgroup of a cyclic group is cyclic.

Proof.

- If h is a generator of a cyclic group G of order n, then

$$G = \left\{h, h^2, h^3, \ldots, h^n = 1\right\}$$

- Every element in a subgroup S of G is of the form h^i where $1 \leq i \leq n$
- Let h^m be the smallest power of h in S
- Every element in S is a power of h^m

$\square$

Subgroups of Cyclic Groups

Example

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has subgroups $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$, $\{0, 1, 2, 3, 4, 5\}$

Theorem

If G is a finite cyclic group with $|G| = n$, then G has a unique subgroup of order d for every divisor d of n.

Proof.

- If $G = \langle h \rangle$ and d divides n, then $\langle h^{n/d} \rangle$ has order d
- Every subgroup of G is of the form $\langle h^k \rangle$ where k divides n
- If k divides n, $\langle h^k \rangle$ has order $\frac{n}{k}$
- If a subgroup has order d, it is equal to $\langle h^{n/d} \rangle$

$\square$

Number of Generators of a Cyclic Group

Examples

- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ has four generators $1, 2, 3, 4$
- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ has two generators $1, 5$
- $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$ has four generators $1, 3, 7, 9$

Theorem

A cyclic group of order n has $\phi(n)$ generators where

$$\phi(n) = \textit{No. of integers in } \{0, 1, \ldots, n-1\} \textit{ relatively prime to } n$$

Order of an Element in a Cyclic Group

Example

- $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$ has
  - four elements $1, 3, 7, 9$ of order 10
  - four elements $2, 4, 6, 8$ of order 5
  - one element 5 of order 2
  - one element 0 of order 1

Theorem

$$n = \sum_{d : d \mid n} \phi(d)$$

Summary

- Every cyclic group G of order n is isomorphic to $\mathbb{Z}_n$.
- If S is a subgroup of a finite group G, then $|S|$ divides $|G|$.
- Every subgroup of a cyclic group is cyclic.
- If G is a finite cyclic group with $|G| = n$, then G has a unique subgroup of order d for every divisor d of n.
- A cyclic group of order n has $\phi(n)$ generators.

Questions? Takeaways?