

## Unit 6: Algebraic Structures

### Topic 2: Cyclic Group

# Outline

- 1 Cyclic group
- 2 Lagrange' Theorem
- 3 Consequences of Lagrange's Theorem
- 4 Problems

## Cyclic group

### Definition

A group  $G$  is called cyclic if there is an element  $a$  in  $G$  such that  $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ . Such an element  $a$  is called a generator of  $G$ .

## Cyclic group

### Definition

A group  $G$  is called cyclic if there is an element  $a$  in  $G$  such that  $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ . Such an element  $a$  is called a generator of  $G$ .

### Remark

*If  $G$  is finite group of order  $n$ , then  $G$  is cyclic if and only if  $G$  has an element of order  $n$ .*

# Outline

- 1 Cyclic group
- 2 Lagrange' Theorem**
- 3 Consequences of Lagrange's Theorem
- 4 Problems

## Lagrange' Theorem

### Theorem (Lagrange's Theorem)

*The order of a subgroup of a finite group divides the order of the group.*

# Outline

- 1 Cyclic group
- 2 Lagrange' Theorem
- 3 Consequences of Lagrange's Theorem
- 4 Problems

## Lagrange's Theorem and Cyclic group

### Theorem

*Every subgroup of a cyclic group is cyclic. If  $|\langle a \rangle| = n$ , then the order of any subgroup of  $\langle a \rangle$  is a divisor of  $n$ ; and, for each divisor  $k$  of  $n$ , the group  $\langle a \rangle$  has exactly one subgroup of order  $k$ , namely,  $\langle a^{\frac{n}{k}} \rangle$ .*



## Consequences of Lagrange's Theorem

- The order of each element of a finite group divides the order of the group.

## Consequences of Lagrange's Theorem

- The order of each element of a finite group divides the order of the group.
- If  $G$  is a cyclic group of order  $n$  with generator  $a$ , then  $a^k$  is also a generator of  $G$  if and only if  $\gcd(k, n) = 1$ .

## Consequences of Lagrange's Theorem

- The order of each element of a finite group divides the order of the group.
- If  $G$  is a cyclic group of order  $n$  with generator  $a$ , then  $a^k$  is also a generator of  $G$  if and only if  $\gcd(k, n) = 1$ .
- A group of prime order is always cyclic.

# Outline

- 1 Cyclic group
- 2 Lagrange' Theorem
- 3 Consequences of Lagrange's Theorem
- 4 Problems

## Problems

### Problems:

- 1 Suppose  $G = \langle a \rangle$  and  $|a| = 20$ . How many subgroups does  $G$  have? List a generator for each of these subgroups.

## Problems

### Problems:

- 1 Suppose  $G = \langle a \rangle$  and  $|a| = 20$ . How many subgroups does  $G$  have? List a generator for each of these subgroups.
- 2 If  $g$  is a generator of the cyclic group  $U(49)$ , then find all generators of this group.

Thank You

*Any Question!!!*