

# MAT414 - Modern Algebra

**Miraj Samarakkody**

Tougaloo College

03/24/2025

# Cyclic Groups

Theorem 4.2 -  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Let  $a$  be an element of order  $n$  in a group and let  $k$  be a positive integer. Then  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

# Cyclic Groups

Theorem 4.2 -  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Let  $a$  be an element of order  $n$  in a group and let  $k$  be a positive integer. Then  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Proof steps:

We let  $d = \gcd(n, k)$

- In the first part, we have to prove  $\langle a^k \rangle \subseteq \langle a^{\gcd(n,k)} \rangle$  and  $\langle a^{\gcd(n,k)} \rangle \subseteq \langle a^k \rangle$

# Cyclic Groups

Theorem 4.2 -  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Let  $a$  be an element of order  $n$  in a group and let  $k$  be a positive integer. Then  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Proof steps:

We let  $d = \gcd(n, k)$

- ▶ In the first part, we have to prove  $\langle a^k \rangle \subset \langle a^{\gcd(n,k)} \rangle$  and  $\langle a^{\gcd(n,k)} \rangle \subset \langle a^k \rangle$
- ▶ Let  $d = \gcd(n, k)$

# Cyclic Groups

Theorem 4.2 -  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Let  $a$  be an element of order  $n$  in a group and let  $k$  be a positive integer. Then  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Proof steps:

We let  $d = \gcd(n, k)$

- ▶ In the first part, we have to prove  $\langle a^k \rangle \subset \langle a^{\gcd(n,k)} \rangle$  and  $\langle a^{\gcd(n,k)} \rangle \subset \langle a^k \rangle$
- ▶ Let  $d = \gcd(n, k)$
- ▶ Write  $d = ns + kt$  for some integers  $s, t$

# Cyclic Groups

Theorem 4.2 -  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Let  $a$  be an element of order  $n$  in a group and let  $k$  be a positive integer. Then  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|a^k| = n/\gcd(n, k)$

Proof steps:

We let  $d = \gcd(n, k)$

- ▶ In the first part, we have to prove  $\langle a^k \rangle \subset \langle a^{\gcd(n,k)} \rangle$  and  $\langle a^{\gcd(n,k)} \rangle \subset \langle a^k \rangle$
- ▶ Let  $d = \gcd(n, k)$
- ▶ Write  $d = ns + kt$  for some integers  $s, t$
- ▶ Here we show that  $|a^d| = n/d$  and then  $|a^k| = n/d$ .

## Example 5

For  $|a| = 30$ , find  $\langle a^{26} \rangle$  and  $|a|^{26}$ .

## Example 5

For  $|a| = 30$ , find  $\langle a^{17} \rangle$  and  $|a|^{17}$ .



## Example 5

For  $|a| = 30$ , find  $\langle a^{18} \rangle$  and  $|a|^{18}$ .

# Corollary 1

## Orders of Elements in Finite Cyclic Groups

In a finite cyclic group, the order of an element divides the order of the group.

## Corollary 2

Criterion for  $\langle a^i \rangle = \langle a^j \rangle$  and  $|a^i| = |a^j|$

Let  $|a| = n$ . Then  $\langle a^i \rangle = \langle a^j \rangle$  if and only if  $\gcd(n, i) = \gcd(n, j)$ ,  
and  $|a^i| = |a^j|$  if and only if  $\gcd(n, i) = \gcd(n, j)$ .

## Corollary 3

### Generators of Finite Cyclic Groups

Let  $|a| = n$ . Then  $\langle a \rangle = \langle a^j \rangle$  if and only if  $\gcd(n, j) = 1$ , and  $|a| = |\langle a^j \rangle|$  if and only if  $\gcd(n, j) = 1$ .

## Corollary 4

### Generators of $\mathbb{Z}_n$

An integer  $k$  in  $\mathbb{Z}_n$  is a generator of  $\mathbb{Z}_n$  if and only if  $\gcd(n, k) = 1$ .

## Example

Find all generators of the cyclic group  $U(50)$ .