MAT414 - Modern Algebra

Miraj Samarakkody

Tougaloo College

03/24/2025

Cyclic Groups

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

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

Cyclic Groups

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

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

Proof steps:

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

- In the first part, we have to prove $< a^k > \subset < a^{\mathrm{gcd}(n,k)} >$ and $< a^k > \supset < a^{\mathrm{gcd}(n,k)} >$

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 is a group and let k be a positive integer. Then $< a^k > = < a^{\gcd(n,k)} >$ and $|a^k| = n/gcd(n,k)$

Proof steps:

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

- In the first part, we have to prove $< a^k > \subset < a^{\gcd(n,k)} >$ and $< a^k > \supset < a^{\gcd(n,k)} >$
  - Let $d = nk$

Cyclic Groups

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

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

Proof steps:

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

- In the first part, we have to prove $< a^k > \subset < a^{\mathrm{gcd}(n,k)} >$ and $< a^k > \supset < a^{\mathrm{gcd}(n,k)} >$
  - Let $d = nk$
  - 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 is a group and let k be a positive integer. Then $< a^k >=< a^{\gcd(n,k)} >$ and $|a^k| = n/gcd(n,k)$

Proof steps:

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

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

Example 5

For $|a| = 30$, find $< a^{26} >$ and $|a|^{26}$.

Example 5

For $|a| = 30$, find $< a^{17} >$ and $|a|^{17}$.

Example 5

For $|a| = 30$, find $< a^{18} >$ 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

Criterian 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 $U(50)$.

Fundamental Theorem of Cyclic Groups

Theorem 4.3

Fundamental Theorem of Cyclic Group

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

Example

Suppose $G = \langle a \rangle$ and G has order 30. Find all the subgroups of G.

Corollary

Subgroups of $\mathbb{Z}_n$

For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.

Example 7

Write the list of subgroups of $\mathbb{Z}_{30}$.

Example 8

Find the generators of the subgroup of order 9 in $\mathbb{Z}_{36}$.

Euler Phi Function

Let $\phi(1) = 1$, and for any integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n.

Example

Write each $\phi(n)$ for $n \in \{1, 2, \ldots, 12\}$