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 $< a^k > = < a^{\gcd(n,k)} >$ 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 $< a^k >=< a^{\gcd(n,k)} >$ 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 $< a^k >\supset< a^{\gcd(n,k)} >$

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 $d = nk$

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 $|a^d| = n/d$ and then $|a^k| = n/d$.