MTHSC 412 Section 3.4 – Cyclic Groups

Kevin James

Definition

If G is a cyclic group and $G =< a >$ then a is a *generator* of G.

Definition

If G is a cyclic group and $G =< a >$ then a is a *generator* of G.

Example

1. $\mathbb{Z}$ is a cyclic group and can be generated by 1 or -1.

Definition

If G is a cyclic group and $G =< a >$ then a is a *generator* of G.

Example

1. $\mathbb{Z}$ is a cyclic group and can be generated by 1 or -1.
2. The group $G = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \leq S_4$ is cyclic and $G =< (1,2,3,4) >$.

Definition

If G is a cyclic group and $G =< a >$ then a is a *generator* of G.

Example

1. $\mathbb{Z}$ is a cyclic group and can be generated by 1 or -1.
2. The group $G = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \leq S_4$ is cyclic and $G =< (1,2,3,4) >$.
   Also, $G =< (1,4,3,2) >$.

Definition

If G is a cyclic group and $G =< a >$ then a is a *generator* of G.

Example

1. $\mathbb{Z}$ is a cyclic group and can be generated by 1 or -1.
2. The group $G = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \leq S_4$ is cyclic and $G =< (1,2,3,4) >$.
   Also, $G =< (1,4,3,2) >$.

Fact

If a is a generator of G, then so is a^{-1} (or $-a$ if we are using additive notation).

Theorem

Let $a \in G$. If $a^n \neq e$ for all $n \in \mathbb{Z}$, then $a^p \neq a^q$ for all $p \neq q \in \mathbb{Z}$ and G is infinite.

Theorem

Let $a \in G$. If $a^n \neq e$ for all $n \in \mathbb{Z}$, then $a^p \neq a^q$ for all $p \neq q \in \mathbb{Z}$ and G is infinite.

Corollary

If G is a finite group and $a \in G$, then there exists $n \in \mathbb{N}$ such that $a^n = e$.

Theorem

Let $a \in G$. If $a^n \neq e$ for all $n \in \mathbb{Z}$, then $a^p \neq a^q$ for all $p \neq q \in \mathbb{Z}$ and G is infinite.

Corollary

If G is a finite group and $a \in G$, then there exists $n \in \mathbb{N}$ such that $a^n = e$.

Example

S_3 is a finite group. For each element $\sigma \in S_3$ find the positive integer n such that $\sigma^n = e$.

Theorem

Let $a \in G$ and suppose that $a^k = e$ for some $k \in \mathbb{Z}$. Then there is a smallest positive integer m such that $a^m = e$ and

1. $< a >$ *has order* m *and* $< a > = \{a^0 = e = a^m, a, a^2, \ldots, a^{m-1}\}$.
2. $a^r = a^s$ *if and only if* $r \equiv s \pmod{m}$.

Definition

The *order* of an element $a \in G$ is defined by $o(a) = | < a > |$.

Definition

The *order* of an element $a \in G$ is defined by $o(a) = |<a>|$.

Fact

If $a \in G$ and $o(a)$ is finite then $o(a)$ is the least positive integer m such that $a^m = e$.

Theorem

Suppose that G is cyclic and $G =< a >$. If $H \leq G$, then either

1. $H =< e >$, *or*
2. *If* $H \neq< e >$, *then* $H =< a^k >$ *where* k *is the least positive integer such that* $a^k \in H$.

Theorem

Suppose that G is cyclic and $G =< a >$. If $H \leq G$, then either

1. $H =< e >$, *or*
2. *If* $H \neq< e >$, *then* $H =< a^k >$ *where* k *is the least positive integer such that* $a^k \in H$.

Corollary

Any subgroup of a cyclic group is cyclic.

Theorem

Suppose that $G =< a >$ is cyclic of order n. If $m \in \mathbb{Z}$ and $d = (m, n)$ then $< a^m > = < a^d >$.

Theorem

Suppose that $G = \langle a \rangle$ *is cyclic of order* n. *If* $m \in \mathbb{Z}$ *and* $d = (m, n)$ *then* $\langle a^m \rangle = \langle a^d \rangle$.

Fact

Suppose that $G = \langle a \rangle$ *is cyclic of order* n *and that* $d \mid n$. *Then* $o(a^d) = |\langle a^d \rangle| = n/d$.

Theorem

Suppose that $G =< a >$ *is cyclic of order* n*. If* $m \in \mathbb{Z}$ *and* $d = (m, n)$ *then* $< a^m > = < a^d >$.

Fact

Suppose that $G =< a >$ *is cyclic of order* n *and that* $d|n$*. Then* $o(a^d) = | < a^d > | = n/d$.

Corollary

Let $G =< a >$ *be a cyclic group of order* n*. The distinct subgroups of* G *are the groups* $< a^k >$ *where* k *is a positive divisor of* n*.*

Example

Suppose that $G = \mathbb{Z}_{10}$.
Note that $G = < 1 >$ is cyclic of order 10. So, the distinct subgroups are:

1. $< 0 >= \{0\}$ which has order 1.
2. $< 5 >= \{0, 5\}$ which has order 2.
3. $< 2 >= \{0, 2, 4, 6, 8\}$ which has order 5, and
4. $< 1 >= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ which has order 10.

Example

Suppose that $G \leq S_6$ is the cyclic group generated by $(1,2,3,4,5,6)$. That is,

$$G = \{e, (1,2,3,4,5,6), (1,3,5)(2,4,6), (1,4)(2,5)(3,6), (1,5,3)(2,6,4), (1,6,5,4,3,2)\}$$

The distinct subgroups are:

Example

Suppose that $G \leq S_6$ is the cyclic group generated by $(1,2,3,4,5,6)$. That is,

$$G = \{e, (1,2,3,4,5,6), (1,3,5)(2,4,6), (1,4)(2,5)(3,6), (1,5,3)(2,6,4), (1,6,5,4,3,2)\}$$

The distinct subgroups are:

1. $< e >$ which has order 1,
2. $< (1,2,3,4,5,6)^3 > = < (1,4)(2,5)(3,6) > = \{e, (1,4)(2,5)(3,6)\}$ which has order 2,
3. $< ((1,2,3,4,5,6)^2 > = < (1,3,5)(2,4,6) > = \{e, (1,3,5)(2,4,6), (1,5,3)(2,6,4)\}$ which has order 3, and
4. $G = < (1,2,3,4,5,6) >$ which has order 6.

Theorem

Let $G = < a >$ be a cyclic group of order n. Then a^m is a generator of G if and only if $(m, n) = 1$.

Theorem

Let $G = \langle a \rangle$ be a cyclic group of order n. Then a^m is a generator of G if and only if $(m, n) = 1$.

Example

1. Suppose that $G = \langle a \rangle$ is a cyclic group of order 9. Then the generators of G are

$$a, a^2, a^4, a^5, a^7, a^8.$$

Theorem

Let $G =< a >$ be a cyclic group of order n. Then a^m is a generator of G if and only if $(m, n) = 1$.

Example

1. Suppose that $G =< a >$ is a cyclic group of order 9. Then the generators of G are
$$a, a^2, a^4, a^5, a^7, a^8.$$
2. The generators of $\mathbb{Z}_{10}$ are 1,3,7, and 9.