Cyclic groups and subgroups

Kevin James

Definition

A group H is cyclic if it can be generated by one element, that is if $H = \{x^n \quad | \quad n \in \mathbb{Z}\} =< x >$.

Definition

A group H is <u>cyclic</u> if it can be generated by one element, that is if $H = \{x^n \mid n \in \mathbb{Z}\} = < x >$.

Note

A cyclic group typically has more than one generator.

1. If $H =< x >$, then $H =< x^{-1} >$ also.
2. $\mathbb{Z} =< 1 >=< -1 >$. There are no other generators of $\mathbb{Z}$.
3. The generators of the cyclic group $(\mathbb{Z}/11\mathbb{Z})^*$ are 2,6,7 and 8.

Proposition

Suppose that $H = < x >$*. Then* $|H| = |x|$*. More precisely,*

1. *If* $|H| = n < \infty$ *then* $x^n = 1$ *and* $1, x, x^2, \ldots, x^{n-1}$ *are distinct.*
2. *If* $|H| = \infty$*, then* $x^n \neq 1$*,* $\forall n \in \mathbb{Z}$ *and for* $a, b \in \mathbb{Z}$*,* $x^a = x^b \Rightarrow a = b$*.*

Proposition

Suppose that $H = < x >$. *Then* $|H| = |x|$. *More precisely,*

1. *If* $|H| = n < \infty$ *then* $x^n = 1$ *and* $1, x, x^2, \ldots, x^{n-1}$ *are distinct.*
2. *If* $|H| = \infty$, *then* $x^n \neq 1$, $\forall n \in \mathbb{Z}$ *and for* $a, b \in \mathbb{Z}$, $x^a = x^b \Rightarrow a = b$.

Proposition

Suppose that G *is a group and that* $x \in G$. *If* $x^m = 1$ *and* $x^n = 1$ *then* $x^{(m,n)} = 1$ *as well. In particular, if* $x^m = 1$ *for some* $m \in \mathbb{Z}$, *then* $|x|$ *divides* m.

Theorem

Any two cyclic groups of the same order are isomorphic. More precisely,

1. *If* $0 \leq n < \infty$ *and if* $< x >$ *and* $< y >$ *are cyclic groups of order* n*, then the map* $\phi :< x > \to < y >$ *defined by* $\phi(x^k) = y^k$ *is a well defined isomorphism.*
2. *If* $< x >$ *is an infinite cyclic group, then the map* $\phi : \mathbb{Z} \to < x >$ *defined by* $\phi(k) = x^k$ *is a well defined isomorphism.*

Theorem

Suppose that G is a group, $x \in G$ and that $0 \neq a \in \mathbb{Z}$.

1. *If $|x| = \infty$, then $|x^a| = \infty$.*
2. *If $|x| = n$ then $|x^a| = \frac{n}{(a,n)}$.*

Theorem

Suppose that G is a group, $x \in G$ and that $0 \neq a \in \mathbb{Z}$.

1. *If $|x| = \infty$, then $|x^a| = \infty$.*
2. *If $|x| = n$ then $|x^a| = \frac{n}{(a,n)}$.*

Proposition

Suppose that $H =< x >$.

1. *If $|x| = \infty$, then $H =< x^a >$ if and only if $a = \pm 1$.*
2. *If $|x| = n$, then $H =< x^a >$ if and only if $(a, n) = 1$. In particular, the number of generators of H is $\phi(n)$.*

Theorem

Let $H = < x >$ be a cyclic group.

1. *Every subgroup of H is cyclic. More precisely, if $K \leq H$ then $K = < x^d >$ where d is the smallest positive integer for which $x^d \in K$.*
2. *If $|H| = \infty$, then we have $< x^m > = < x^{-m} >$ and for $0 \leq a < b < \infty$, $< x^a > \neq < x^b >$. Thus the non-trivial subgroups of H are in 1-1 correspondence with the positive integers $1, 2, \ldots$.*
3. *If $H = n < \infty$, then for each $a|n$, letting $n = ak$ we have $| < x^k > | = a$. Further, $< x^m > = < x^{(n,m)} >$. Thus the subgroups of H are in 1-1 correspondence with the positive divisors of n.*