# Cyclic Groups and Generators

**Definition**

A **cyclic group** $G$ is one in which every element is a power of a particular element, $g$, in the group. That is, every element of $G$ can be written as $g^n$ for some integer $n$ for a multiplicative group, or as $ng$ for some integer $n$ for an additive group. In this case, we write $G = \langle g \rangle$ and say $g$ is a **generator** of the group $G$.

Note that cyclic groups may have more than one generator. In fact, it's possible that every element of the group generates the entire group, or that only one element can be named as a generator.

**Example** $\mathbb{Z}$ is a cyclic group (under addition) generated by 1, since every integer can be written as an integer multiple of 1. It is also generated by $-1$. However, 2 is not a generator of $\mathbb{Z}$, since the set generated by 2 would include all even integers, but no odd integers.

The following theorem holds for any group $G$, not just cyclic groups, and says that every element of every group can be used to generate a cyclic group:

**Theorem 1**

If $g$ is an element of a group $G$, then $\langle g \rangle$ is a subgroup of $G$.

**Theorem 2**

If $g$ is an element of a group $G$, then $|g| = |\langle g \rangle|$. That is, the order of the element is equal to the order of the cyclic subgroup generated by that element.

**Example** The order of 3 in $\mathbb{Z}_{12}$ is 4, since $(4)(3) \equiv 0$ mod 12, and $\langle 3 \rangle = \{0, 3, 6, 9\}$ so the order of the subgroup generated by 3 is also 4.

**Definition**

If $G$ is a group and $S$ is a subset of $G$, then $\langle S \rangle$ is called the **subgroup generated by** $S$, and is defined to be the smallest subgroup of $G$ that contains $S$.

Note that $\langle S \rangle$ is NOT necessarily the group generated by powers of the elements in $S$.

**Theorem 3**

If $G$ is a finite cyclic group with order $n$, the order of every element in $G$ divides $n$.

**Theorem 4**

The generators of $\mathbb{Z}_n$ are the integers $g$ such that $g$ and $n$ are relatively prime.

**Theorem 5** (Fundamental Theorem of Cyclic Groups)

Every subgroup of a cyclic group is cyclic. Moreover, if a cyclic group $G$ is finite with order $n$:

1. the order of any subgroup of $G$ divides $n$.
2. for each (positive) divisor $k$ of $n$, there is exactly one subgroup of $G$ with order $k$.

The simplest way to find the subgroup of order $k$ predicted in part 2 of the theorem above is to find a generator $g$ of the group. The subgroup of order $k$ will be the subgroup generated by the element $g^{n/k}$. In additive groups, the subgroup of order $k$ is generated by $(n/k)g$.

**Theorem 6**

Let $G$ be a cyclic group with generator $g$ and order $n$. If $m < n$, then the order of the element $g^m$ in $G$ is $\dfrac{n}{\gcd(m,n)}$.

**Example** We'll find the order of 18 in $\mathbb{Z}_{30}$, which has order 30 and generator 1. Since (in multiplicative notation) $18 = 1^{18}$, then

$$|18| = \frac{30}{\gcd(18,30)} = \frac{30}{6} = 5$$