Cyclic Groups

**Definition** A group $G$ is called *cyclic* if there is an element $a \in G$ such that the cyclic subgroup generated by $a$ is the entire group $G$. In other words,

$$G = \{a^n : n \in \mathbb{Z}\}.$$ 

Such an element $a$ is called a *generator* of $G$.

Note that a cyclic group is abelian. On the other hand, a group which is abelian is not necessarily cyclic.

**Examples and Non-Examples**

1) $\mathbb{Z}_n$

2) $S_3$

3) $\mathbb{Z}$

4) $\mathbb{R}$

5) $\mathbb{Z} \times \mathbb{Z}$

6) $\mathbb{Z}_{19}^\times$
**Theorem:** Suppose \( G \) is cyclic and \( a \in G \) is a generator of \( G \). If \( G \) is an infinite group, then there is an isomorphism \( \varphi: G \to \mathbb{Z} \) determined completely by \( \varphi(a) = 1 \). If \( G \) is finite with order \( n \), then there is an isomorphism \( \varphi: G \to \mathbb{Z}_n \) determined completely by \( \varphi(a) = [1]_n \).

How can a finite abelian group not be cyclic? Suppose \( G \) is an abelian group of order \( n \). By Lagrange’s theorem \( a^n = e \) for any element \( a \) of \( G \). But that doesn’t mean that the order of \( a \) is \( n \); it only means that the order of \( a \) divides \( n \).

For example, consider the following three groups of order 8: \( \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \text{and} \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \). The first is cyclic (and has \( \phi(8) = 4 \) elements of order 8, i.e., 4 generators). The second has no elements of order 8, though it does have 2 elements of order 4. The third has the identity and 7 elements of order 2.

Suppose \( G \) is an abelian group of order 6. Then \( G \) must be cyclic. In particular, \( \mathbb{Z}_6^\times \) is cyclic. Recall why this is so. First, there can’t be more than one element of order 2, since two such elements in an abelian group give us a subgroup of order 4 (an impossibility here by Lagrange’s Theorem). Second, there are an even number of elements of order 3. By Lagrange’s Theorem, we’re led to a couple of possibilities: either there is an element of order 2 \( \cdot 3 \) and \( G \) is cyclic, or there is an element of order 2 and an element of order 3, and their product has order \( 2 \cdot 3 \) so that \( G \) is cyclic once more.

The above argument works exactly the same for abelian groups of order \( 2p \), where \( p \) is an odd prime number. Thus, if \( G \) is an abelian group of order \( 2p \), then \( G \) must be cyclic. In particular, \( \mathbb{Z}_p^\times \) is cyclic.

Suppose \( G \) is an abelian group of order 12. Then \( G \) may not be cyclic. Is \( \mathbb{Z}_13^\times \) cyclic?
**Definition:** Suppose $G$ is a group. Suppose there is some positive integer $n$ such that $a^n = e$ for all elements $a$ of $G$. Then the smallest such $n$ is called the *exponent* of $G$.

**Examples**
1) $\mathbb{Z}_9$

2) $\mathbb{Z}_3 \times \mathbb{Z}_3$

3) A direct product of infinitely many copies of $\mathbb{Z}_2$.

4) $S_4$

**Note:** If $G$ is a finite group, then $g^{\phi(G)} = e$ for all $g \in G$ by Lagrange’s Theorem, so the exponent of $G$ is no larger than the order of $G$ (though it may be smaller).