PROPERTIES OF CYCLIC GROUPS

1. Every subgroup of a cyclic group is cyclic.

2. Suppose G is an infinite cyclic group. Then, for every $m \geq 1$, there exists a unique subgroup H of G such that $[G : H] = m$.

3. Suppose G is a finite cyclic group. Let $m = |G|$. For every positive divisor d of m, there exists a unique subgroup H of G of order d.

4. If G is an infinite cyclic group, then G is isomorphic to the additive group $\mathbf{Z}$. If G is a finite cyclic group of order m, then G is isomorphic to $\mathbf{Z}/m\mathbf{Z}$.

5. Suppose that G is a finite cyclic group of order m. Let a be a generator of G. Suppose $j \in \mathbf{Z}$. Then a^j is a generator of G if and only if $gcd(j, m) = 1$.

CONJUGACY

Suppose that G is a group. If $a, b \in G$, then we will say that *"a is conjugate to b in G"* if there exists an element $x \in G$ such that $a = x^{-1}bx$. There is no standard notation, but we will simply write $a \sim_G b$ if a is conjugate to b in G. If G is understood, we may sometimes just write $a \sim b$.

1. The relation of conjugacy is an equivalence relation on G.

The equivalence classes are called the *"conjugacy classes"* of the group G. If $a \in G$, then the elements of its conjugacy class are called the *"conjugates"* of a in G.

2. Suppose that G is a group and H is a subgroup of G. Then H is a normal subgroup of G if and only if H is a union of conjugacy classes of G.

3. Suppose that G is a group and $a \in G$. Let $C(a)$ be the centralizer of a in G. Then the cardinality of the conjugacy class of a is the same as the cardinality of the right coset space $C(a)\backslash G$. In particular, if G is finite, then the number of conjugates of a in G is equal to the index $[G : C(a)]$.

4. Suppose $a, b \in G$, where G is a group. If a is conjugate to b in G, then a and b have the same order.

5. (The class equation) Suppose that G is a finite group. Let k denote the number of distinct conjugacy classes in G. Suppose that $a_1, ..., a_k$ are representatives of the distinct conjugacy classes of G. Then

$$|G| \; = \; \sum_{j=1}^{k} \; [G : C(a_j)].$$