Propositions about Conjugacy

Definition. Suppose that G is a group. Suppose that $a,\ b \in G$. We say that a and b are *conjugate in* G if there exists an element $g \in G$ such that $b = gag^{-1}$. We will write $a \sim_G b$ if a and b are conjugate in G.

1. The relation $\sim_G$ is an equivalence relation on the set G. Each equivalence class under this equivalence relation is called a *conjugacy class* in G.

2. If a and b are conjugate in G, then $|a| = |b|$.

3. A group G is abelian if and only if each conjugacy class in G consists of exactly one element.

4. An element $z \in G$ is in the center $Z(G)$ of G if and only if the set $\{z\}$ is a conjugacy class in G.

5. Suppose that G is a group and that $a \in G$. Define

$$C(a) \ = \ \{ \ g \in G \ \big| \ ga = ag \ \} \ .$$

The $C(a)$ is a subgroup of G (which is called the *centralizer of* a *in* G). Furthermore, the cardinality of the conjugacy class of a in G is equal to the index $[G : C(a)]$.

6. If G is a finite group, then the cardinality of every conjugacy class in G divides $|G|$.

7. (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

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

8. Suppose that G is a group and that 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.

Some Theorems about Finite Groups

1. Suppose that G is a group of order p, where p is a prime. Then $G \cong \mathbb{Z}_p$.

2. Suppose that G is a finite group and that $|G| = p^n$, where p is a prime and $n \geq 1$. Then $|Z(G)| = p^m$, where $m \geq 1$. Thus, $Z(G) \neq \{e\}$.

3. Let G be any group. Then $Z(G)$ is a normal subgroup of G. If $G/Z(G)$ is a cyclic group, then G is an abelian group (and therefore $Z(G) = G$).

4. Suppose that G is a group of order p^2, where p is a prime. Then G is abelian.

5. Suppose that G is a nonabelian group of order p^3, where p is a prime. Then $Z(G) \cong \mathbb{Z}_p$ and $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

6. Suppose that G is a group of order pq, where p and q are distinct primes. Assume that $q > p$ and that $q \not\equiv 1 \pmod{p}$. Then $G \cong \mathbb{Z}_{pq}$.

7. (Cauchy's Theorem.) Suppose that G is a finite group and that p is a prime which divides $|G|$. Then G contains at least one subgroup of order p. Thus, G has at least one element of order p. The number of elements of order p in G is a multiple of $p - 1$.