Abstract

We discuss the nuances of the conjugation action in groups, and use it to prove the Sylow theorems. We then use the Sylow theorems to classify the nature of groups of a particular order.

Introduction to Conjugation

Every transitive left-action of a group on a set S is, up to isomorphism, left-multiplication on the set of left-cosets of $G/\operatorname{Stab}_G(a)$, where $\operatorname{Stab}_G(a)$ denotes the stabilizer subgroup of $a \in S$. Furthermore, the number of elements of a finite orbit of $a \in O_a$ is the index of $\operatorname{Stab}_G(a)$ — this is the much celebrated *orbit-stabilizer theorem.*

Note that from the orbit-stabilizer theorem, we can partition S into a formula involving the conjugacy classes. Since every element of s is either in an orbit or is in the set

$$Z \coloneqq \{a \in S \mid g \cdot a = a \text{ for all } g \in G\},$$

we calculate

$$\begin{aligned} |S| &= |Z| + \sum_{a \in A} |O_a| \\ &= |Z| + \sum_{a \in A} [G : \operatorname{Stab}_G(a)], \end{aligned}$$

where A is a system of representatives for the orbits. This is *a* class formula for the action of G on S.

The power of this class formula is that when G is finite, $[G : \operatorname{Stab}_G(a)]$ always divides G, which is a very strong constraint when we know something about $|G|$.

Proposition: Let $|G| = p^n$ be a group that acts on a finite set S, and let Z be the set of fixed points for the action. Then, $|Z| \equiv |S|$ modulo p.

Proof. Since each summand of the form $[G : \operatorname{Stab}_G(a)]$ is a number larger than 1 and a power of p, each $[G : \operatorname{Stab}_G(a)]$ is congruent to 0 mod p. □

Definition (Conjugation Action)**.** Let G be a group. The *conjugation action* of G on itself is defined by $\rho \colon G \times G \to G$, where

$$\rho(g, a) = gag^{-1}.$$

This map is equal to a particular group homomorphism $\sigma \colon G \to \operatorname{Sym}(G)$.

Definition (Center)**.** The *center* of G, denoted $Z(G)$, is the subgroup $\ker(\sigma) \subseteq G$. Concretely, it is

$$Z(G) = \{g \in G \mid ga = ag \text{ for all } a \in G\}.$$

Note that $Z(G)$ is always a normal subgroup, and all elements of $Z(G)$ commute with each other. Furthermore, a group G is abelian if and only if $Z(G) = G$.

Lemma: Let G be a finite group, and suppose $G/Z(G)$ is cyclic. Then, G is commutative.

Proof. Write $Z \coloneqq Z(G)$, and suppose G/Z is cyclic. Then, there is some $g \in G$ such that $\langle gZ \rangle = G/Z$. For all $a \in G$, there is some integer r such that

$$aZ = g^r Z,$$

meaning there exists some $z \in Z$ such that $a = g^r z$. Similarly, we write $b = g^s w$ for some $w \in Z$ and integer s. However, this means

$$ab = (g^r z)(g^s w)$$

$$\begin{aligned} &= g^{r+s}zw \\ &= (g^s w)(g^r z) \\ &= ba, \end{aligned}$$

where we use the fact that z and w commute with every element of G. □

Definition. Let $a \in G$. The *centralizer* of a, denoted $Z_G(a)$, is the stabilizer of a under conjugation. Concretely,

$$Z_G(a) = \{g \in G \mid ga = ag\},$$

or the set of elements of G that commute with a.

Note that $Z(G) \subseteq Z_G(a)$ for all $a \in G$, and that

$$Z(G) = \bigcap_{a \in G} Z_G(a).$$

Definition. The *conjugacy class* of $a \in G$ is the orbit $[a]$ of a under conjugation.

The Class Equation

What we call *the* class equation is generally the class formula for conjugation.

Definition. Let G be a finite group. Then,

$$|G| = |Z(G)| + \sum_{a \in A} [G : Z_G(a)],$$

where A is a family of representatives of conjugacy classes in G.

The Sylow Theorems

Applications of the Sylow Theorems