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. This is known as the *class equation* for the group G.

We are very easily able to apply the class equation to prove certain properties about p-groups.

Proposition: Let G be a nontrivial p-group. Then, G has a nontrivial center.

Proof. Since $|Z(G)| \equiv |G|$ modulo p, and $|G| > 1$ is a power of p, we have $|Z(G)|$ is a multiple of p. Since $e_G \in Z(G)$, we know that $|Z(G)| \geq p$. □

> **Exercise:** Let p, q be prime numbers, and let G be a group of order pq. Prove that either G is commutative or the center of G is trivial.
>
> Conclude that every group of order p^2 is commutative.

> **Solution:** From the class equation, we know that
>
> $$pq = |Z(G)| + \sum_{a \in A} [G : Z_G(a)].$$
>
> If $|Z(G)| = pq$, then G is abelian.
>
> Suppose toward contradiction that, without loss of generality, $|Z(G)| = p$. Then, $|G/Z(G)| = q$, meaning $G/Z(G)$ is cyclic, so G is abelian, so $Z(G) = G$. $\perp$
>
> Since, in any p-group, $|Z(G)| \geq p$, we must have that $Z(G) = G$, so G is abelian.

Example. Let G be a group of order 6. What are the possibilities for its class formula?

In general, if G is commutative, the class formula doesn't say much — in this case, it says $6 = 6$.

If G is not commutative then its center is trivial ($6 = 2 \times 3$), so we have $6 = 1 + \cdots$. Specifically, the $\cdots$ refers to the sizes of the conjugacy classes, which must be smaller than 6, greater than 1, and divide 6. Thus, we have

$$6 = 1 + 2 + 3$$

as the only possible class equation for a noncommutative group with six elements.

Note that normal subgroups are unions of conjugacy classes.[I] If H is a normal subgroup, and $a \in H$ with $b = gag^{-1}$ conjugate to a, we must have $b \in gHg^{-1} = H$.

Furthermore, every subgroup must have the identity and its size must divide the order of the group; therefore, a noncommutative group of order 6 cannot have any subgroup of order 2, since 2 cannot be written as a sum of orders of conjugacy classes including the center.

Definition. Let $A \subseteq G$ be a subset, $g \in G$ an element. The *conjugate* of A is the subset gAg^{-1}; the map $a \mapsto gag^{-1}$ is a bijection between A and gAg^{-1}.

Definition. Let $A \subseteq G$ be a subset. The *normalizer* $N_G(A)$ is its stabilizer under conjugation. The *centralizer* of A is the subgroup $Z_G(A) \subseteq N_G(A)$ that fixes each element of A.

Therefore, $g \in N_G(A)$ if and only if $gAg^{-1} = A$, and $g \in Z_G(A)$ if and only if $gag^{-1} = a$ for all $a \in A$. If $A = \{a\}$, then $N_G(A) = Z_G(A) = Z_G(a)$. However, in general, $Z_G(A) \subsetneq N_G(A)$.

If H is a subgroup of G, then every conjugate gHg^{-1} of H is also a subgroup of G; all conjugate subgroups have the same order.

Lemma: Let $H \subseteq G$ be a group. Then, the number of subgroups conjugate to H equals the index $[G : N_G(H)]$ of the normalizer of H in G.

Proof. Considering the group's self-action of conjugation, this follows from the orbit-stabilizer theorem. □

Corollary: If $[G : H]$ is finite, then the number of subgroups conjugate to H is finite and divides $[G : H]$.

Proof.

$$[G : H] = [G : N_G(H)][N_G(H) : H].$$

□

A useful fact is that if H and K are subgroups of G such that $H \subseteq N_G(K)$ — i.e., that $gKg^{-1} = K$ for all $g \in H$ — then conjugation by $g \in H$ gives an automorphism of K. Thus, there is a set function

$$\gamma \colon H \to \mathrm{Aut}(K).$$

Exercise: Let H and K be subgroups of G with $H \subseteq N_G(K)$. Verify that the function $\gamma \colon H \to \mathrm{Aut}(K)$ defined by conjugation is a homomorphism of groups, and $\ker(\gamma) = H \cap Z_G(K)$, where $Z_G(K)$ is the centralizer of K.

Solution: Let $a, b \in H$. Then,

$$\begin{aligned}
\gamma(ab^{-1}) &= (ab^{-1})K(ab^{-1})^{-1} \\
&= ab^{-1}Kba^{-1} \\
&= (aKa^{-1})(b^{-1}Kb) \\
&= (aKa^{-1})(bKb^{-1})^{-1} \\
&= \gamma(a)\gamma(b)^{-1}.
\end{aligned}$$

The kernel of γ consists of all those elements of H that map to $\mathrm{id} \colon K \to K$ — i.e., those that map to the central-

[I] This is used to show that A_5 is simple, for those of us studying for qualifiers.

izer of K. Therefore, $\ker(\gamma)$ consists of $H \cap Z_G(K)$.

The Sylow Theorems

The Sylow Theorems are a collection of theorems that concern p-subgroups of a certain finite group G. The first of the theorems says that G contains p-groups of all sizes allowed by Lagrange's theorem.

Theorem (Cauchy's Theorem)**:** Let G be a finite group, and let p be a prime divisor of $|G|$. Then, G contains an element of order p.

We can show the abelian case as an exercise.

Exercise: Suppose G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove there exists an element of order p.

Solution: Let $g \in G$. Then, $\langle g \rangle \subseteq G$ is a cyclic subgroup, meaning that it is of order k, where k divides $|G|$. Assuming $k \geq 2$, we may write $k = p_1^{e_1} \cdots p_n^{e_n}$, where p_i are prime. Then, for some prime q such that q divides k, we may take the prime subgroup $\langle h \rangle \coloneqq \left\langle g^{k/q} \right\rangle$.

Now, if $q = p$, we are done; else, we may take $G/\langle h \rangle$, which has order $|G|/q$, and since $p \neq q$, we may commence with the same process on $G/\langle h \rangle$.

However, we can also show the general case.

Proof. Let S be the set of ordered p-tuples of elements of G, $(a_1, \ldots, a_p)$, such that $a_1 \cdots a_p = e$. Then, $|S| = |G|^{p-1}$, as we may choose $a_1, \ldots, a_{p-1}$ arbitrarily, and select a_p to be the inverse of $a_1 \cdots a_{p-1}$.

Since p divides the order of S, it divides the order of G. Note that if $a_1, \ldots, a_p = e$, then

$$a_2 \cdots a_p a_1 = e,$$

as a_1 is a left-inverse to $a_2 \cdots a_p$, so it is a right inverse. Therefore, we may act $\mathbb{Z}/p\mathbb{Z}$ on S by taking $[m]$ to act on $(a_1, \ldots, a_p)$ yielding $(a_{m+1}, \ldots, a_p, a_1, \ldots, a_m)$; this yields an element of S.

Thus, by the general class equation, we have $|Z| \equiv |S| \equiv 0$ modulo p, where Z is the set of fixed points of the action.

In particular, fixed points are p-tuples of the form $(a, \ldots, a)$; note that $Z \neq \varnothing$, since $(e, \ldots, e) \in Z$. Thus, there is some element in Z of the form $(a, \ldots, a)$ with $a \neq e$.

In particular, this means there is $a \in G$ with $a \neq e$ and $a^p = e$. □

Corollary: If p is a prime divisor of $|G|$, and N is the number of cyclic subgroups of order p, then $N \equiv 1 \mod p$.

Proof. Since $|Z|$ in the proof of Cauchy's theorem is congruent to 0 modulo p, we must have $|Z| = mp$ for some $m \geq 1$. Now, since $e_G \in Z$ but e_G is not of order p, we must have $mp - 1$ elements of order p in G.

Since it takes $p - 1$ elements of order p to yield a cyclic subgroup of order p, we thus have $N = \frac{mp-1}{p-1} \equiv \frac{-1}{-1} = 1 \mod p$. □

Exercise: Let G be a group. A subgroup H of G is called *characteristic* if $\varphi(H) \subseteq H$ for all automorphisms φ of G.

(a) Prove that characteristic subgroups are normal.

(b) Let $H \subseteq K \subseteq G$, with H characteristic in K and K normal in G. Prove that H is normal in G.

(c) Let G, K be groups, and suppose G contains a single subgroup H isomorphic to K. Prove that H is normal in G.

(d) Let K be a normal subgroup of a finite group G, and assume $|K|$ and $|G/K|$ are relatively prime. Prove that K is characteristic in G.

Solution:

(a) Since conjugation is an automorphism, we have $gHg^{-1} \subseteq H$ for each $g \in G$, meaning H is normal.

(b) Since K is normal in G, K is preserved under conjugation by elements of G, so conjugation by elements of G is an automorphism of K. Thus H is preserved by conjugation of elements in G, so H is normal in G.

(c) Let $\varphi\colon G \to K$ be a surjective homomorphism such that $\varphi(H) \cong K$. Then,

$$\begin{aligned}\varphi\big(gHg^{-1}\big) &= \varphi(g)\varphi(H)\varphi(g)^{-1} \\ &= K,\end{aligned}$$

so $gHg^{-1} = H$, meaning H is normal.

(d) Let $|K|$ and $|G/K|$ be relatively prime.

Using part (c) of the exercise, we can see that if there is only one cyclic subgroup H of order p, then that subgroup must be normal.

Definition. A group G is called *simple* if the only normal subgroups of G are $\{e\}$ and G.

Applications of the Sylow Theorems