Example .0.1

If H is a subgroup of G, then G acts on G/H via $g(g'H) = (gg')H$.

This gives a homomorphism $G \to \mathrm{Sym}(G/H)$.

$$G_H = \{g \in G \mid gH = H\} = H$$
$$G_{gH} = gHg^{-1}$$

This action is transitive (i.e., there's only one orbit). As $G/H = \mathcal{O}_H$.

Remark .0.1

The orbits $\{\mathcal{O}_s\}_{s \in S}$ form a partition of S.

Remark .0.2

Every transitive action of G on S is isomorphic to the left-multiplication action of G on G/G_s (for any $s \in S$).

Actions of G on sets S and T are isomorphic if there is a bijection $f : S \to T$ such that $gf(s) = f(gs)$.

G acts on G by conjugation:

$$g \cdot h = ghg^{-1}$$

This gives a homomorphism $G \to \mathrm{Aut}(G) \leq \mathrm{Sym}(G)$ as we've discussed before.

The kernel is exactly the center of G. We know that

$$G_h = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} \coloneqq C_G(h)$$

where $C_G(h)$ denotes the "centralizer of h in G." Then the center of G is $Z(G) = \bigcap_{h \in H} C_G(h)$, which is the same as the kernel $\bigcap_{h \in H} G_h$.

Applying orbit stabilizer gets us that

$$|\text{conjugacy class of } h \in G| = [G : C_G(h)]$$

A corollary, the size of the conjugacy class divides the size of the group. Since G is the (disjoint) union of its conjugacy classes, it follows that if we have representatives $h_1, \ldots, h_k$ of all the distinct conjugacy classes then

$$\sum_{i=1}^{k} [G : C_G(h_i)]$$

This is called the class equation of G.

Example .0.2

If $G = S_5$ then the representatives of conjugacy classes are

h_i	$C_G(h_i)$	size	$[S_5 : C_G(h_i)]$
(1)	S_5	120	1
(12)	$C_2 \times S_3$	12	10
(123)	$C_3 \times S_2$	6	20
(1234)	C_4	4	30
(12345)	C_5	5	24
(12)(34)	D_4	8	15
(12)(345)	$C_2 \times C_3$	6	20
			120

I. Sylow's Theorems and p-groups

Definition I.0.1

A p-group (if p is prime) is a group of order p^n for some $n > 0$.

Theorem I.0.1

Every p-group has nontrivial center.

Proof. The class equation tells us that

$$p^n = \sum_{i=1}^{k} [G : C_G(h_i)]$$

Where h_i are representatives of the distinct conjugacy classes in G. $h \in Z(G)$ if and only if $C_G(h) = G$ if and only if $[G : C_G(h)] = 1$ if and only if the conjugacy class of h is $\{h\}$.

Since $|G| = p^n$, $[G : C_G(h_i)]$ are all powers of p (since they divide $|G|$). This is then either one of a multiple of p. Modding out by p on both sides of the class equation gives:

$$0 \equiv |Z(G)| \mod p$$

Because $1 \in Z(G)$, we know the right hand side has at least one element. Therefore it has at leas tP elements because it is divisible by p. Thus there is more than one element in the center and we're done!

Proposition I.0.2

All groups of order p^2 (for p a prime) are abelian.

Proof. Note that $Z(G)$ is nontrival, so $|Z(G)| = p$ or $|Z(G)| = p^2$ by Lagrange's theorem. If $|Z(G)| = p^2$ then $Z(G) = G$ and we're done. Thus we just need to see that something goes wrong if $|Z(G)| = p$.

Take some element $g \in G \setminus Z(G)$, we know that g commutes with itself and commutes with $Z(G)$. Thus $C_G(g) \supseteq \langle Z(G), g \rangle \supsetneq Z(G)$. Because $|C_G(g)| \mid |G| = p^2$ and $|C_G(g)| > p$, we then know that $|C_G(g)| = p^2$. Thus $g \in Z(G)$. Contradiction!