19 Group Actions on G

19.1 Conjugation

Today, we will discuss the special case of group actions where the set S is G itself. We've seen the power of studying orbits and stabilizers and how they can help us understand groups of symmetries. One attempt is to just directly apply the group action on G:

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto gx. \end{aligned}$$

However, this isn't particularly interesting. The action is transitive, and thus there is only one orbit and the stabilizers are all trivial.

We instead define a different group action on itself, **conjugation**. It takes

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto gxg^{-1}, \end{aligned}$$

conjugating x by g. One can check that it satisfies the axioms of a group action. We have some special names for the orbit and stabilizer under conjugation.

Definition 19.1
The orbit of an element under conjugation is

$$C(x) \coloneqq \text{Orbit}(s) = \{gxg^{-1} : g \in G\},$$

and is called the **conjugacy class** of x.

Definition 19.2
The stabilizer of an element under conjugation is

$$Z(x) \coloneqq \text{Stab}_G(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} \leq G.$$

It is called the **centralizer** of x in G, and it is a subgroup of G.

From before, for *any* $x \in G$, we have

$$|G| = |C(x)| \cdot |Z(x)|,$$

and we also have the **class equation**, which states that

$$|G| = |C_1| + \cdots + |C_k|,$$

since the conjugacy classes partition G, and additionally, each $|C_i|$ divides $|G|$ from the counting formula.

Student Question. *Are the conjugacy classes related to cosets, like we saw how left cosets of a subgroup partitioned a group?*

Answer. *No, in general the conjugacy classes won't have the same size like cosets do. We'll be seeing exactly what this equation looks like for different examples in the next few lectures.*

Another related set, which we saw in homework before is the center of a group.

Definition 19.3
The **center** of G is

$$\{Z \coloneqq x \in G : xg = gx, g \in G\}.$$

Other facts:

- $C(x) = \{x\}$ is equivalent to $Z(x) = G$ and also $x \in Z$, the center of G.

  So if we had an abelian group, then the center would be the whole group, and the class equation would be just the sum of a bunch of 1s.

- For any $x \in G$, we have that $Z \leq Z(x)$ since the center commutes with all elements. Also, since x commutes with itself, $\langle x \rangle \leq Z(x)$. This fact is a lower bound on the order of $Z(x)$, so it gives us the upper bound $|C(x)| \leq |G|/\operatorname{ord}(x)$.
- For all $x \in G$, conjugation preserves order: $\operatorname{ord}(x) = \operatorname{ord}(gxg^{-1})$. This is true because conjugation defines an automorphism of our group. If $x^k = e$, then $e = gx^kg^{-1} = (gxg^{-1})^k$ so $x^k = e$ is equivalent to $(gxg^{-1})^k = e$.

Student Question. *Why is conjugation an automorphism?*

Answer. *We can just show that conjugation satisfies the homomorphism property, that it preserves products: $gxyg^{-1} = gxg^{-1}gyg^{-1}$. Conjugation is a homomorphism and in fact an isomorphism from G to itself. Since it is an automorphism of G, elements that are conjugate to each other will have the same properties with respect to order; whether or not they commute; and so on.*

All we have done so far is take observations about these definitions, and the class equation comes from our work on group actions from last week.

Example 19.4
What does the class equation say for D_5? The order of the group is $|D_5| = 10$. It is equal to

$$D_5 = \{e, x, x^2, x^3, x^4, y, xy, x^2y, x^3y, x^4y\}.$$

One of the properties of reflections is that conjugating x by y gives $yxy^{-1} = x^4$. Let's figure out the conjugacy class of all the elements. The identity commutes with everything, so its conjugacy class is $C(e) = \{e\}$.

Now let's look at the reflection y. From our facts above about the centralizer, we know that $\langle y \rangle \leq Z(y) \leq D_5$. Then $Z(y)$ must be at least 2, and it must divide 10, so 2 and 10 are our only possibilities. However, not every element in D_5 commutes with y, so $|Z(y)| = 2$, and thus $|C(y)| = 5$. In fact, every reflection is conjugate to every other reflection: $C(y) = \{\text{all reflections}\}$.

The conjugacy class of x is at least x, and it is also at least $\{x, x^4\}$. It cannot be more, because the order must divide 10 and we only have 4 elements left to partition. Then we have $C(x) = \{x, x^4\}$ and similarly $C(x^2) = \{x^2, x^3\}$.

So we have $10 = 1 + 5 + 2 + 2$. The center corresponds to the elements that are in its own conjugacy class, so the center of D_5 is $\{e\}$.

Notice that the conjugacy classes have very different sizes; they partition the group in a very different way from cosets.

Since the group was small, we could have just brute forced and directly calculated the conjugacy classes for every element. However, looking at these divisibility facts is powerful and can handle more complicated and larger groups.

Student Question. *The conjugacy classes seem to contain x^{-1}; is that always true?*

Answer. *In the example, it was specifically true because $yxy^{-1} = x^4$. However, in general it isn't true. For example, in the integers, 5 and -5 are inverses, but not conjugate to each other.*

19.2 p-groups

By studying the class equation, it is possible to gain some information about a general class of groups, p-groups.

Definition 19.5
G is a p-group for a prime p if $|G| = p^e$ for some $e \geq 0$.

There exists a group of any order simply by taking the abelian cyclic group of that order.

Example 19.6
For example, we have a p-group for every $e \geq 0$ by taking C_p, C_{p^2}, C_{p^3}, and so on. Another example of a p-group is $C_p \times C_p \times \cdots \times C_p$.

Looking at a subgroup of 3×3 matrices also provides an example of a p-group.

Example 19.7
A more interesting group is the set of matrices

$$\begin{pmatrix} 1 & \star & \star \\ & 1 & \star \\ & & 1 \end{pmatrix} \leq GL_3(\mathbb{F}_p),$$

which has order p^3.

By looking at the class equation modulo p, the following theorem holds.

Theorem 19.8
Every p-group has non-trivial center.[a]

[a] There are elements of the center that are not the identity.

Example 19.9
For $G = D_4$, $|G| = 8 = 2^3$. The class equation says $8 = 1 + 1 + 2 + 2 + 2$, so the center has size 2 (since there are two 1's in the class equation.)

Proof. The class equation for G states that

$$|G| = |C_1| + \cdots + |C_k|,$$

which is

$$p^e = (1 + \cdots + 1) + (p + \cdots + p) + (p^2 + \cdots + p^2) + \cdots + (p^{e-1} + \cdots + p^{e-1}),$$

since the order of the conjugacy class must divide the order of G.

Recall that the sizes of the center, $|Z|$ is exactly the number of 1s in the class equation. Then the equation taken modulo p gives

$$0 = |Z| \bmod p,$$

which implies that p divides $|Z|$, since $|Z| \geq 1$ because at least the identity e is in Z. So $|Z| \geq p$, and then the center is nontrivial. □

This theorem is interesting because we get some nontrivial information about the group *just* from the size of the group, by using the class equation and looking at the numerics.

Example 19.10
Take the upper triangular matrices of the form

$$\begin{pmatrix} 1 & \star & \star \\ & 1 & \star \\ & & 1 \end{pmatrix} \leq GL_3(\mathbb{F}_p).$$

What is the center of the group? We want

$$\begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ & 1 & x \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & x & y \\ & 1 & x \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix}$$

for all x, y, z. This happens exactly when $a = c = 0$ and b can be anything. So $|Z| = p$, since there are p possibilities for b.

The example above was a group of order p^3 having center of size p, so it demonstrates that there is not a better theorem where the center always has size p^2, or something.

However, we can say a little more about the specific case of $|G| = p^2$.

Corollary 19.11
If $|G| = p^2$, then G must be abelian.[a]

[a] Earlier on, we stated that if p were prime, then G must be cyclic; now we get from p^2 that G is abelian, although not necessarily cyclic.

Proof. We have

$$\{e\} \lneq Z \leq G.$$

We want to show that $|Z| = p^2$, because that implies that $Z = G$ and then G is abelian. We already know that p divides $|Z|$, and that $|Z| \geq p$, so the only two possibilities are p and p^2. Assume for the sake of contradiction that $|Z| = p$. Then, pick $x \in G \setminus Z$ that is not in the center. Then, $Z \lneq Z(x)$; $Z(x) \neq Z$ because $x \in Z(x)$ but $x \notin Z$.

Then there exists $x \in Z(x)$ such that $x \notin Z$. Thus if $|Z| = p$, the only possibility is that $|Z(x)| = p^2$ since $Z(x)$ is a subgroup. However, this implies that $Z(x) = G$, but then $x \in Z$, which is a contradiction. □

The issue here is that p^2 is just not very big, so there is not very much room for a lot to happen. We can even classify exactly what groups of size p^2 look like.

Corollary 19.12
Given a group G such that $|G| = p^2$, G must be isomorphic to either C_{p^2}, the cyclic group of size p^2, or $C_p \times C_p = \{(a, b) : a, b \in C_p\}$.

Proof. We can split this up into two cases.

- **Case 1.** If there exists $a \in G$ with $\text{ord}(a) = p^2$, then $\langle a \rangle = G$, since $\langle a \rangle$ has size p^2, and thus must be the entire group G.
- **Case 2.** Otherwise, every element $a \neq e$ has order p, since it must divide p^2 and cannot be p^2 since we already considered that case. We claim that G being abelian such that every $x \neq e$ has order p comes from considering it as a vector space V over $F = \mathbb{F}_p$

  What is the dimension of this mystery vector space? The group G has size p^2, so it has dimension p. So $V = F \oplus F$, implying that $G = C_p \times C_p$. Here, we are forgetting the vector space structure and just thinking about it as a group with respect to addition.

The addition structure is already implicit from the structure on G. To turn G into a vector space, we only need to define how to scale $g \in G$ by $\overline{n} \in \mathbb{F}_p$, and then check the vector space axioms. Let $\overline{n} \cdot g = \overbrace{g + \cdots + g}^{\text{n times}}$ This is well-defined because $\text{ord}(g) = p$, so it only matters what $\overline{n}$ is modulo p. We have figured out a way to turn the group into a vector space. Since any two vector spaces of the same dimension are isomorphic to each other as vector spaces; in particular, they are isomorphic to each other as abelian groups.

□

All of this is gravy from what we were supposed to discuss this week, but it is helpful to see these examples.