Lecture 21

Lagrange's Theorem and the class equation (applications of orbit-stabilizer)

21.1 Goals

1. Understand the statement of Lagrange's theorem.
2. Understand applications of Lagrange's theorem.
3. Understand the content of the class equation.
4. Understand applications of the class equation
5. Understand the notion of center.
6. Understand that any element $g \in G$ defines a subgroup generated by g.

21.2 Lagrange's Theorem

The orbit-stabilizer theorem tells us that, for finite groups, there is a big relationship between symmetries and divisibility. After all, if G exhibits symmetries of X (by specifying a group action of G on X) then sizes of orbits have to be divisors of $|G|$.

This theme continues. Here is one major application of the orbit-stabilizer theorem:

Theorem 21.2.1 (Lagrange's Theorem)**.** Let G be a finite group and H a subgroup. Then $|H|$ divides $|G|$.

Remark 21.2.2. One could ask for a converse: If d divides $|G|$, does there exists a subgroup of G with order d? The answer turns out to be no. For example, we can take $A_4 \subset S_4$ to be the following subgroup of order 12:

$$e, \qquad (12)(34), \qquad (13)(24), \qquad (14)(23),$$

$$(123), \qquad (132), \qquad (124), \qquad (142), \qquad (134), \qquad (143), \qquad (234), \qquad (243).$$

(Don't worry; the fact that this is a subgroup of S_4 is not at all obvious at this point.) Then 6 divides $|A_4| = 12$, but there is no subgroup of order 6 in A_4.

21.2.1 Any group acts on itself

To set up our proof of the theorem, let's first note that any group G acts on itself. Indeed, the multiplication map

$$G \times G \to G (g, h) \mapsto gh$$

is a group action by definition of group.

21.2.2 Any group action on a set results in a group action on the power set

Here is a fun, second observation: If G acts on a set, then G acts on the power set of that set. In other words, G acts on the set of all subsets:

Proposition 21.2.3. Suppose $G \times Y \to Y$ is a group action. Let $\mathcal{P}(Y)$ denote the set of all subsets of Y. Then the map

$$G \times \mathcal{P}(Y) \to \mathcal{P}(Y), \qquad (g, A) \mapsto gA := \{ga \,|\, a \in A\}$$

is a group action.

Remark 21.2.4. This is fairly straightforward to see in words: Fix a subset A of Y—this is just some collection of points in Y. Well, every g sends each of these points somewhere. In particular, applying g to each of these points, we'll get some (potentially new) subset of Y. We let gA denote this (potentially new) subset.

Remark 21.2.5. Note that, because the action of g is a bijection of Y, A and gA always have the same size.

Example 21.2.6. Let $G = S_n$ act on the set $Y = \underline{n}$. For concreteness, we will let $n = 4$. Then $\mathcal{P}(\underline{4})$, the set of all subsets of $\underline{4}$, has $2^4 = 16$ elements:

$$\begin{gathered}
\{\}, \\
\{1\}, \quad \{2\}, \quad \{3\}, \quad \{4\}, \\
\{1,2\}, \quad \{1,3\}, \quad \{1,4\}, \quad \{2,3\}, \quad \{2,4\}, \quad \{3,4\}, \\
\{1,2,3\}, \quad \{1,2,4\}, \quad \{1,3,4\}, \quad \{2,3,4\}, \\
\{1,2,3,4\}.
\end{gathered}$$

(Of course, you notice the pattern of 1, 4, 6, 4, 1—the number of subsets of a particular cardinality—as the $n = 4$th row in Pascal's triangle.)

Let me write what the element $g = (132)$ does to some of the elements of

$\mathcal{P}(\underline{4})$:

$$\begin{aligned}
g\{\} &= \{\} \\
g\{1\} &= \{3\} \\
g\{2\} &= \{1\} \\
g\{3\} &= \{2\} \\
g\{4\} &= \{4\} \\
g\{1,2\} &= \{1,3\} \\
g\{1,3\} &= \{2,3\} \\
g\{1,4\} &= \{3,4\} \\
g\{2,3\} &= \{1,2\} \\
g\{2,4\} &= \{1,4\} \\
g\{3,4\} &= \{2,4\} \\
g\{1,2,3\} &= \{1,2,3\} \\
g\{1,2,4\} &= \{1,3,4\} \\
g\{1,3,4\} &= \{2,3,4\} \\
g\{2,3,4\} &= \{1,2,4\} \\
g\{1,2,3,4\} &= \{1,2,3,4\}
\end{aligned}$$

Example 21.2.7. When G acts on itself, the induced action on $\mathcal{P}(G)$ has exactly two orbits of size one (i.e., exactly two fixed points): The subsets $\emptyset$ and G.

21.2.3

Thanks to the previous two observations, it makes to study the stabilizer of the subset H.

Lemma 21.2.8. Let $H \subset G$ be a subgroup, and let $G \times \mathcal{P}(G) \to \mathcal{P}(G)$ denote the action of a group G on its own power set. Then the stabilizer of H is H.

Proof. The notation can get confusing, so let's write $\mathbb{H}$ to mean an element of $\mathcal{P}(G)$ (i.e., H as a *subset* of G), and write H when we are trying to understand H as a subgroup of G. So we are setting out to show that $G_{\mathbb{H}} = H$.

(i) First, let me show that the stabilizer $G_{\mathbb{H}}$ is a subset of H. For this, suppose that

$$g\mathbb{H} = \mathbb{H}.$$

$g\mathbb{H} = \mathbb{H}$ means in particular that $g\mathbb{H} \subset \mathbb{H}$, so that for every $h \in \mathbb{H}$, we know that $gh \in \mathbb{H}$. In particular, there exists some $h' \in \mathbb{H}$ so that $gh = h'$. Thus,

$$g = h'h^{-1}.$$

By choice, $h, h' \in \mathbb{H} = H$; because subgroups are closed under inverse and multiplication, we conclude that $g \in H$. This shows $G_{\mathbb{H}} \subset H$.

(ii) Next, let me show that $H \subset G_{\mathbb{H}}$. This means that if $g \in H$, we must show that

$$g\mathbb{H} = \mathbb{H}.$$

First, $g\mathbb{H} \subset \mathbb{H}$. This is because if $g \in H$ and $h \in \mathbb{H} = H$, the definition of subgroup implies $gh \in H = \mathbb{H}$. On the other hand, if $h' \in \mathbb{H}$, define $h = g^{-1}h'$. Because g is assumed to be in H, we conclude that $h \in H$ as well. Moreover,

$$gh = gg^{-1}h' = h'$$

so $h' \in g\mathbb{H}$. This shows $\mathbb{H} \subset g\mathbb{H}$, concluding the proof that $\mathbb{H} = g\mathbb{H}$ when $g \in H$. In other words, $H \subset G_{\mathbb{H}}$.

Combining (i) and (ii), we see that $G_{\mathbb{H}} = H$. □

21.2.4 Proof of Lagrange's Theorem

Proof. We continue with the notation of Lemma 21.2.8. By the orbit-stabilizer theorem,

$$|G| = |G_{\mathbb{H}}| \times |G\mathbb{H}|.$$

By Lemma 21.2.8, we know that $G_{\mathbb{H}} = H$, so we see that the order of G is divisible by the order of H. □

21.3 Applications of Lagrange's Theorem

21.3.1 Review: Subgroup generated by an element

Before we see some applications, let's review some basics.

Recall that given a group G and an element $g \in G$, there is a *subgroup generated by* g. As a set, it is the collection of all elements

$$\{\dots g^{-2}, g^{-1}, e, g, g^2, \dots\} = \{g^n \mid n \in \mathbb{Z}\}.$$

Remark 21.3.1. A fancy way to think about this subgroup is as the image of the group homomorphism

$$\mathbb{Z} \to \mathbb{G}, \qquad n \mapsto g^n.$$

21.3.2 Groups of prime order

Here is one application of Lagrange's Theorem:

Proposition 21.3.2. If G is a group of prime order, G is cyclic. That is, G is isomorphic to the group $\mathbb{Z}/p\mathbb{Z}$. In particular, G is abelian.

Example 21.3.3. If you know that a group has order 13, then you know it is isomorphic to $\mathbb{Z}/13\mathbb{Z}$ (because 13 is prime).

There's a lot to digest here, but you probably feel that Proposition 21.3.2 is rather powerful. Just by knowing the size of a group, you know which group it is (up to isomorphism).

Remark 21.3.4. In general, a "goal" of the study of finite groups was to (i) Given n, have a list of all groups with order n, and (ii) given a group of order n, have a reasonable algorithm for deciding which group of order n it is.

This "goal" is more or less accomplished, but that does not mean that finite group theory is easy. This is because whether you can run an algorithm on a group is highly dependent on how a group is given to you. There is a lot of time in topology, for example, spent trying to decide whether a group of order 4 is cyclic, or is the Klein 4-group.

Proof of Proposition 21.3.2. Since G is a group of prime order, it has at least 2 elements. In particular, it contains an element g that does not equal the identity. Then the subgroup generated by g contains at least 2 elements, so does not have order 1.

On the other hand, by Lagrange's Theorem, any subgroup of G must have order 1 or order $|G|$. In particular, the subgroup generated by g must equal G.

This proves G is cyclic.

Further, by definition of the group generated by g, we conclude that we can write G concretely as

$$G = \{e, g, g^2, \ldots, g^{p-1}\}.$$

The assignment

$$\mathbb{Z}/p\mathbb{Z} \to G, \qquad a \mapsto g^a$$

is thus a group isomorphism. □

21.3.3 Orders of elements

Proposition 21.3.5. Let G be a finite group and $g \in G$ an element. Then the order of g divides the order of G.

Proof. The subgroup generated by g has order equal to the order of g. Now apply Lagrange's Theorem. □

21.4 Class equation and the conjugation action

What we've seen is that by being creative about our group actions, we can discover beautiful facts about groups. Here, let's apply orbit-stabilizer to the conjugation action.

21.4.1 Conjugation action

Remember that we have a canonical symmetry of a group, given by conjugation? Let's review. A group G acts on itself by multiplication, and by *conjugation*:

$$G \times G \to G, \qquad (g, h) \mapsto ghg^{-1}.$$

(In terms of the previous group action notation, $G = X$ and $h \in X$.) We won't want to write this action as "gh" because we'd confuse it with group multiplication. So we have introduced the notation of

$$C_g(h) = ghg^{-1}.$$

Although we've already seen this, let's review:

Proposition 21.4.1. Conjugation defines a group action of G on itself.

Proof. We need to show that $C_e(h) = h$ and that $C_{gg'}(h) = C_g(C_{g'}(h))$. Well,

$$C_e(h) = ehe^{-1} = ehe = h$$

and

$$C_{gg'}(h) = (gg')h(gg')^{-1} = gg'h(g')^{-1}g^{-1} = gC_{g'}(h)g^{-1} = C_g(C_{g'}(h)).$$

□

Example 21.4.2. The *orbit* of an element h (under the conjugation action) is the set

$$\{ghg^{-1} \,|g \in G\}.$$

This is by definition the conjugacy class of h. (Definition 19.4.11.)

This example leads immediately to the following:

Proposition 21.4.3. Assume G is a finite group and let $h \in G$. Then the size of the conjugacy class of h divides $|G|$.

Proof. By Example 21.4.2, the conjugacy class $Cl(h)$ of h is the orbit of a group action of G. Hence the orbit-stabilizer theorem says

$$|G| = |Cl(h)| \times |\text{stabilizer of } h \text{ (under conjugation)}|.$$

In particular, $|Cl(h)|$ divides $|G|$. □

The phrase "stabilizer of h (under conjugation)" is rather clunky. We thus give it a name:

Definition 21.4.4. Let G be a group and fix $h \in G$. The *centralizer* of h in G is the collection of those elements g for which $C_g(h) = h$. (In other words, the centralizer of h is the stabilizer of h under the conjugation action.)

Put another way, the centralizer of h is the set of all $g \in G$ satisfying

$$ghg^{-1} = h,$$

or equivalently,

$$gh = hg.$$

So, the final equivalent description of the centralizer you should know is that the centralizer of h is the set of all $g \in G$ commuting with h.

21.4.2 Centers

Let's study the conjugation action some more. For example, are there elements of $X = G$ that are fixed by the conjugation action?

Definition 21.4.5. Let $G \times X \to X$ be a group action. We say that $x \in X$ is a *fixed point* of the group action if, for every $g \in G$, $gx = x$.

Put another way, x is a fixed point if its orbit has size exactly 1.

Example 21.4.6. What would it mean for h to be a fixed point of the conjugation action? It would mean that for every $g \in G$, we have that

$$ghg^{-1} = h.$$

By multiplying on the right by g, the above equation is equivalent to

$$gh = hg.$$

In other words, h is a fixed point of the conjugation action if and only if h commutes with every element of G.

Example 21.4.7. e is a fixed point of the conjugation action, because

$$geg^{-1} = gg^{-1} = e.$$

And, sure enough, for every $g \in G$, we know $eg = ge$ (because both sides equal g).

"Commuting with every element of G" is an important property. We give a name to the set of all elements that satisfy this property:

Definition 21.4.8. Let G be a group. The *center* of G is the set of all elements $h \in G$ such that, for all $g \in G$, $gh = hg$. We often denote the center of G by Z.

So, the center is the collection of fixed points of the conjugation action. But the less obscure characterization (as elements that commute with all elements of G) gives rise to a nice property:

Proposition 21.4.9. The center of G is a subgroup of G.

Proof. We saw in Example 21.4.7 that e is in Z. It remains to show that Z is closed under multiplication and under inverses.

So suppose h and h' are in the center. Then for all $g \in G$, we have

$$g(hh') = (gh)h' = (hg)h' = h(gh') = h(h'g) = (hh')g.$$

So hh' commutes with all elements of G. This shows hh' is in the center.

If h is in the center, then for any $g \in G$, we have that $gh = hg$. Multiplying both sides by h^{-1} on the right and left, we find

$$h^{-1}g = gh^{-1}.$$

This shows that h^{-1} commutes with g. Because g was arbitrary, this shows h^{-1} is also in the center. □

21.5 The class equation

To prove the orbit-stabilizer theorem, we divided G into subsets of equal size.

But sometimes, it's useful to divide up the thing that G is action on—in other words, we can get information about an action by dividing X up into meaningful subsets. The *class equation* is a powerful equation—giving insight into the structure of non-abelian groups—obtained precisely by dividing $X = G$ up into its orbits.

21.5.1 A set as a union of its orbits

Given a group action $G \times X \to X$, let's observe that X is a union of its orbits. That is, we can write

$$X = O_1 \cup O_2 \cup \ldots \cup O_k$$

where the O_i are orbits of the group action. (For simplicity we've assumed there are finitely many orbits in the group action; namely, k of them; this assumption is automatic if X is a finite set.)

Moreover, two distinct orbits do not intersect each other, so we can turn unions of sets into summation of sizes:

$$|X| = |O_1| + |O_2| + \ldots + |O_k|.$$

21.5.2 When the action is the conjugation action

So, let's recall that an orbit of $X = G$ under the conjugation action is just a conjugacy class. By using the same trick of writing a set as a union of its orbits, we find that

$$G = Cl(h_1) \cup Cl(h_2) \cup \ldots \cup Cl(h_k).$$

Let me carefully say what I mean. I have chosen an h_i from each orbit O_i of the conjugation action. If $h_i \in O_i$, then $O_i = Cl(h_i)$ by Example 21.4.2.

Now, to organize things, let's divide orbits into two kinds of orbits: Those of size 1 (determined by fixed points of the action) and those of size ≥ 2:

$$G = \left(\bigcup_{\text{conjugacy classes } Cl(h_i) \text{ of size } 1} Cl(h_i) \right) \cup \left(\bigcup_{\text{conjugacy classes } Cl(h_j) \text{ of size } \geq 2} Cl(h_j) \right).$$

But we saw in Section 21.4.2 that the collection of elements h that are fixed by the conjugation action forms a subgroup: the center of G. In other words, we may re-write the above as

$$G = Z \cup \left(\bigcup_{\text{conjugacy classes } Cl(h_j) \text{ of size } \geq 2} Cl(h_j) \right)$$

where Z is the center of G.

Again by noting that none of the subsets in the union on the righthand side intersect, we may turn this union of subsets into a sum of sizes. This results in the following:

Theorem 21.5.1 (The class equation)**.** Let G be a finite group. Let $C_1, \ldots, C_k$ be its conjugacy classes of size ≥ 2. Then

$$|G| = |Z| + \sum_{i=1}^{k} |C_i|.$$

21.6 Applications of the class equation

Theorem 21.6.1. Let G be a group with order p^n. Then the center of G has more than 1 element.

In fact, by Lagrange's Theorem, the center must thus have size at least p; hence have size p, or p^2, or p^3... or p^{n-1}, or p^n (if G turns out to be abelian).

Proof. The class equation reads

$$|G| = Z + \sum_{i=1}^{k} |C_i|$$

where each $C_1, \ldots, C_k$ are the conjugacy classes of size at least 2. By the orbit-stabilizer theorem, we know that each $|C_i|$ is divisible by p (because $|C_i|$ is a factor of p^n, hence a power of p). So we must have

$$|Z| = |G| - \sum_{i=1}^{k} |C_i|$$

where the righthand side is made up of integers divisible by p. In particular, $|Z|$ must be divisible by p, meaning $|Z|$ has size at least p. □

21.7 Exercises

Exercise 21.7.1. Here is a fun application of the orbit-stabilizer theorem.

Theorem 21.7.2 (Cauchy's Theorem)**.** Let G be a finite group, and suppose p is a prime number dividing $|G|$. Then there exists an element of order p in G.

(a) Given p, let $G^p = G \times \ldots \times G$ be a product of p copies of G. Let $B \subset G \times \ldots \times G$ be the subset of elements $(g_1, \ldots, g_p)$ for which the product $g_1 g_2 \ldots g_p = e$.

Let $\mathbb{Z}/p\mathbb{Z}$ act on G^p as follows: Given $a \in \mathbb{Z}/p\mathbb{Z}$,

$$a \cdot (g_1, \ldots, g_p) = (g_{1-a}, \ldots, g_{p-a})$$

where $i - a$ is understood mod p.

Show that if $(g_1, \ldots, g_p) \in B$, then $a(g_1, \ldots, g_p) \in B$ for all $a \in \mathbb{Z}/p\mathbb{Z}$. (Hint: Conjugation by g_p.)

(This shows in particular that $\mathbb{Z}/p\mathbb{Z}$ acts on B.)

(b) By dividing B into its orbits, show that there must be at least *two* fixed points. (Hint: $(e, e, \ldots, e)$ is a fixed point of the $\mathbb{Z}/p\mathbb{Z}$ action. Further, $|B|$ is divisible by p, as are all the orbits that are not of size 1.)

(c) By examining what it means to be a fixed point of the $\mathbb{Z}/p\mathbb{Z}$ action, prove Cauchy's theorem.