OCTOBER 12 NOTES

1. 4.2: Groups acting on themselves by left multiplication, Cayley's Theorem

In this section, we will consider a special case of group actions: when a group G acts on itself. The most natural action we have is G acts on G by left multiplication: for $g \in G$ and $a \in G$, $g \cdot a = ga$.

We can actually generalize all of this to a group acting on a set of cosets, instead of just a group acting on itself. If H is a subgroup of G, then G acts by left multiplication on the set of left cosets of H by $g \cdot aH = gaH$.

We can then use group actions to prove strong statements about the structure of groups.

Corollary 1.1. If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal. For example, if $|G|$ is even, any subgroup of index 2 is normal.

Proof. Suppose $H \leq G$ and $[G : H] = p$. Let $\pi_H : G \to S_A$ be the permutation representation of the left multiplication action of G on the set A of cosets of H. Because H has p cosets, A has p elements, so $S_A = S_p$. Let $K = \ker \pi_H$. We claim that $K \leq H$: if $k \in K$, then $k(aH) = aH$ for any $aH \in A$, because multiplication by k acts as the identity permutation. But, this implies $kaa^{-1} \in H$, so $k \in H$. So, $K \leq H$. Let $q = [H : K]$. Then, $[G : K] = [G : H][H : K] = pq$. Because $G/K \cong \pi_H(G)$ is isomorphic to a subgroup of S_p, $pq = |G/K|$ must divide $|S_p| = p!$. Therefore, $q \mid p!/p = (p-1)!$. However, we assumed that p was the *smallest* prime dividing the order of G, and q also divides $|G|$, so all of the prime factors of q must be greater than p. Bcause $q \mid (p-1)!$ all of whose prime factors are less than p, we must have $q = 1$. Therefore, $[H : K] = 1$ so $H = K$, so $H = \ker \pi_H$ and H is normal. □

Example 1.2. Because $[S_n : A_n] = 2$, A_n is a normal subgroup of S_n.

2. 4.3: Groups acting on themselves by conjugation and the class equation

In this section, we consider a different action of G on itself: G acts on G by $g \cdot a = gag^{-1}$. We leave it as an exercise to verify that this is an action.

Definition 2.1. This action is called **conjugation**. If $a, b \in G$, such that $b = gag^{-1}$ for some $g \in G$, we say a and b are **conjugate**. The **conjugacy classes** of G are the orbits of this action, i.e. the sets of all conjugate elements.

Example 2.2. If G is abelian, then for any $g, a \in G$, $gag^{-1} = a$, so this is the trivial action. The associated permutation representation is the trivial function $\phi : G \to S_G$. Because this is not injective for non-trivial G, this action is **not faithful**.

For any non-trivial group G, this action is **not transitive** because $\mathcal{O}_1 = \{b \in G \mid b = g1g^{-1} = 1\} = \{1\}$. So, $\mathcal{O}_1 \neq G$.

For any group G and $a \in G$, $\mathcal{O}_a = \{a\}$ if and only if $gag^{-1} = a$ for all $g \in G$, if and only if $a \in Z(G)$.

Definition 2.3. Two subsets S and T of G are **conjugate** if there exists some $g \in G$ such that $T = gSg^{-1} = \{gsg^{-1} \mid s \in S\}$.

We can explicitly describe when two subsets are conjugate: by definition, the stabilizer of any subset S is $G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$ is the normalizer of S, and if $S = \{a\}$ is just one element, then $G_a = C_G(a)$ is the centralizer of a. By the *orbit-stabilizer theorem*, we know the number of different orbits of an element or subset is equal to the index of its stabilizer. Therefore:

Proposition 2.4. *The number of conjugates of a subset S in G is $[G : N_G(S)]$ and the number of conjugates of an element $a \in G$ is $[G : C_G(a)]$.*

This allows us to prove another very important result, the **class equation**.

Theorem 2.5. *Let G be a finite group and $g_1, \ldots, g_n$ be representatives of distinct conjugacy classes of G not contained in the center of G. Then,*

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(g_i)].$$

Proof. Because the conjugacy classes are orbits of the group action, they partition G, i.e.

$$|G| = \sum_{j=1}^{r} \mathcal{O}_{a_j}$$

where a_j are representatives of the different orbits. By above, we know $|\mathcal{O}_{a_j}| = 1$ if and only if $a_j \in Z(G)$, and for $a_j \notin Z(G)$, $|\mathcal{O}_{a_j}| = [G : C_G(a_j)]$. So,

$$|G| = \sum_{a_j \in Z_(G)} 1 + \sum_{a_j \notin Z(G)} [G : C_G(a_j)]$$

and renaming the $a_j \notin Z(G)$ as g_i, we see

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(g_i)].$$

□

Note that *every summand on the right side is a divisor of* $|G|$, and by definition the elements $[G : C_G(g_i)]$ must be *less than* $|G|$. This will be very important.

Example 2.6. In $G = S_3$, the conjugacy classes are: $\{1\}$ (this is the only element in the center of G), $\{(12), (13), (23)\}$ (we can write $(13) = (132)(12)(132)^{-1}$, for example) and $\{(123), (132)\}$.

The class equation then says:

$$6 = 1 + 2 + 3.$$

Your book goes in depth studying the conjugagcy classes in S_n. Because we are short on time, we just state the relevant result here:

Proposition 2.7. *Two elements in S_n are conjugate if and only if they have the same cycle type.*

How do we use the class equation? Here are some examples.

Theorem 2.8. *If p is a prime number and G is a group with $|G| = p^n$ for some $n \geq 1$, then $|Z(G)| > 1$.*

Proof. By the class equation, we know

$$|G| = |Z(G)| + \sum [G : C_G(g_i)]$$

but the numbers on the right side must all divide $|G| = p^n$. Also, $[G : C_G(g_i)] > 1$ be definition, so $p \mid [G : C_G(g_i)]$ for each i. As $p \mid |G|$, this implies $p \mid |Z(G)|$. Because $|Z(G)| \geq 1$, this implies $|Z(G)| \geq p$ and hence $Z(G)$ is non-trivial. □

Corollary 2.9. If $|G| = p^2$ for some prime p, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. In particular, G is abelian.

Proof. Since $Z(G) \neq \{1\}$ by the previous theorem, then $G/Z(G)$ has order 1 or p, so it must be cyclic. By a homework problem, this implies that G is abelian. If G has an element of order p^2, then $G \cong \mathbb{Z}_{p^2}$ because it is cyclic. Now suppose every element has order $< p^2$, so every non-identity element has order p. Choose $x \in G$ and $y \in G - \langle x \rangle$ both of order p. Then, $\langle x, y \rangle$ is strictly larger than $\langle x \rangle$, but $|\langle x \rangle| = p$ so we must have $G = \langle x, y \rangle = \{x^a y^b \mid a, b \in \mathbb{Z}_p\}$ because G is abelian. Consider the homomorphism $\phi : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ given by $(a, b) \mapsto x^a y^b$. One can check that this is the desired isomorphism. □

We can also use the class equation to prove the simplicity of A_5.

Proposition 2.10. *If $H \leq G$ is a normal subgroup, then H is a union of conjugacy classes of G.*

Proof. We must show that if $x \in H$, then for any $y \in \mathcal{O}_x$, $y \in H$. Suppose then that $x \in H$. Then, $y = gxg^{-1} \in \mathcal{O}_x \in gHg^{-1}$ by definition, but H is normal, so therefore $y \in H$. □

Theorem 2.11. *For $n \geq 5$, A_n is simple.*

Proof. We provide an outline of the proof, with some details left to check.

Step 1: For $n \geq 5$, A_n is generated by 3-cycles, i.e. $A_n = \langle (a_i a_j a_k) \mid i \neq j \neq k \in \{1, \ldots, n\} \rangle$. Try this as an exercise!

Step 2: All 3-cycles are conjugate in A_n for $n \geq 5$. Try this! You could do this by computing sizes of centralizers or directly: given (123) and $(a_i a_j a_k)$, find something that conjugates one to another.

Step 3: Let N be a non-trivial normal subgroup of A_n. Show that N contains a 3-cycle. This is the most computationally challenging part, and one way to do it is to: prove it for A_5 using the class equation (e.g. if N did not contain a 3 cycle, it would be a union of other conjugacy classes, but these cannot add up to a divisor of 60), and then use induction on n to prove it in general.

Then, because N contains a 3-cycle and it is normal, by Step 2, it must contain all 3-cycles, and by Step 1, it must be all of A_n, so A_n has no nontrivial normal subgroups. □

You may take a look at Section 4.6 for an alternative approach.