OCTOBER 5 NOTES

1. 3.5: Transpositions and the generation of S_n

Here, we list some facts about S_n that we will prove in the future. (This is a bit out of place; but we will list the relevant definitions/facts anyway.)

Definition 1.1. In S_n, a cycle of length 2 (one of the form (ab)) is called a **transposition**.

Proposition 1.2. *Every permutation can be written as a product of transpositions.*

Proof. We prove this for single cycles, as you can write any permutation as a product of disjoint cycles. If $\sigma = (a_1 a_2 \dots a_m)$, then

$$\sigma = (a_1 a_2 \dots a_m) = (a_1 a_m)(a_1 a_{m-1}) \dots (a_1 a_3)(a_1 a_2)$$

is a product of transpositions. □

Definition 1.3. If $\sigma \in S_n$ can be written as a product of an even number of transpositions, then σ is called an **even** permutation. If it can be written as an odd number of transpositions, then σ is an **odd** permutation.

The **sign** of a permutation is

$$\epsilon(\sigma) = \begin{cases} 1 & \sigma \text{ is even} \\ -1 & \sigma \text{ is odd} \end{cases}$$

One has to check that this is *well-defined*; i.e. that no permutation can be written as both an even and odd number of transpositions. Your book does this rigorously. Once that is done, we define the alternating group:

Definition 1.4. The **alternating group** A_n is the collection of all even permutations in S_n. Equivalently, if $\epsilon : S_n \to \{\pm 1\}$ is the homomorphism sending a permutation to its sign, $A_n = \ker \epsilon$.

Because A_n is the kernel of a homomorphism, it is a normal subgroup of S_n, and by the First Isomorphism Theorem, it has size $|A_n| = n!/2$.

2. 4.1: Group Actions and Permutation Representations

Finally, we recap some terminology about group actions.

Definition 2.1. If G acts on a nonempty set A, then the map $\sigma_g : A \to A$ given by $\sigma_g : a \mapsto g \cdot a$ is a permutation of A, and this induces a homomorphism $\phi : G \to S_A$ defined by $\phi(g) = \sigma_g$ called the **permutation representation.**

Definition 2.2.

(1) The **kernel** of an action of G on a set A is

$$\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$$

(equivalently, the kernel of the permutation representation ϕ). An action is **faithful** if its kernel is the identity.

(2) For any $a \in A$, the **stabilizer** of a is the set

$$G_a = \{g \in G \mid g \cdot a = a\}.$$

Note that by definition, for any $a \in A$, the kernel of the group action is contained in G_a.

We could 'reverse' these ideas: suppose G is a group and A is any set such that there exists a homomorphism $\phi : G \to S_A$. Then, we may define an action of G on A by $g \cdot a = \phi(g)(a)$. This is the content of the following:

Proposition 2.3. *For any group G and nonempty set A, there is a bijection between actions of G on A and homomorphisms $G \to S_A$.*

We then rephrase our definition of permutation representation as follows:

Definition 2.4. A **permutation representation** of G is any homomorphism G to the symmetric group S_A for some nonempty set A.

Finally, two more definitions on group actions arising from the following fact:

Proposition 2.5. *If G acts on a set A, then the relation defined by $a \sim b$ if $a = g \cdot b$ for some $g \in G$ is an equivalence relation.*

Proof. We check the properties: because $a = 1 \cdot a$ by definition of action, then $a \sim a$. If $a \sim b$, then $a = g \cdot b$, so $g^{-1} \cdot a = b$, so $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then $a = g_1 \cdot b$ and $b = g_2 \cdot c$ so $a = (g_1 g_2) \cdot c$ so $a \sim c$. Thus, this is an equivalence relation. □

Definition 2.6. If G is a group acting on a set A and $a \in A$, then the equivalence class of a, $\{g \cdot a \mid g \in G\}$, is called the **orbit** of a. The action is **transitive** if the orbit of a is all of A.

Proposition 2.7. *For any $a \in A$, the size of the orbit of a is $[G : G_a]$.*

Proof. Let $\mathcal{O}_a$ denote the orbit of a. Suppose $b \in \mathcal{O}_a$, i.e. $b = g \cdot a$ for some $g \in G$. Then, define a map $\mathcal{O}_a \to \{$ cosets of $G_a\}$ by $b = g \cdot a \mapsto gG_a$. This is surjective, since for any $g \in G$, $g \cdot a$ is by definition an element of $\mathcal{O}_a$. It is also injective: $g \cdot a = h \cdot a$ if and only if $hg^{-1} \in G_a$ if and only if $gG_a = hG_a$. Therefore, it is a bijection, so $|\mathcal{O}_a| = [G : G_a]$. □

For finite groups, this is usually referred to as the **Orbit-Stabilizer Theorem**, because by Lagrange's Theorem, it says $|G| = |\mathcal{O}_a||G_a|$, the size of the orbit times the size of the stabilizer.

3. 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 $a \in G$, $g \cdot a = ga$. What we will prove in this section is that (1) this action is transitive and faithful and (2) the associated permutation representation gives an injective map to S_G.

Let us see this in an example. Suppose $G = \langle x \mid x^3 = 1 \rangle = \{1, x, x^2\}$. What happens when we act by G on itself? For each $g \in G$, we move the elements of G around using the action. If $g = 1$, then we can compute $g \cdot a$ for all $a \in G$:

$$1 \cdot 1 = 11 = 1 \qquad 1 \cdot x = 1x = x \qquad 1 \cdot x^2 = 1x^2 = x^2.$$

If $g = x$, we can do the same thing:

$$x \cdot 1 = x1 = x \qquad x \cdot x = xx = x^2 \qquad x \cdot x^2 = xx^2 = 1.$$

Finally, for $g = x^2$, we get:

$$x^2 \cdot 1 = x^2 1 = x^2 \qquad x^2 \cdot x = x^2 x = 1 \qquad x^2 \cdot x^2 = x^2 x^2 = x.$$

What we see is that this action is transitive, because every element can move to every other element of the group, and it is faithful, because each group element acts in a different way.

What we are interested in now is the map to S_G. G has 3 elements, so this is just S_3. How do we get the map? We consider the induced permutation from each element of g: recall that the permutation representation is the map $\phi : G \to S_G$ given by $\phi(g) = \sigma_g$, where σ_g is the permutation of S_G given by $\sigma_g(a) = g \cdot a$.

We can explicitly determine each permutation σ_g: if $g = 1$, then $\sigma_1(a) = a$ for all $a \in G$, so σ_1 is the identity permutation. If $g = x$, then we see that σ_x moves 1 to x, x to x^2, and x^2 to 1 so 'cyclically rotates' the elements of G. Labeling the elements as $1, 2, 3$, this would be the permutation (123). Similarly, if $g = x^2$, then σ_{x^2} moves 1 to x^2, x to 1, and x^2 to x, so rotates the elements in the other direction. With the same labeling, this would be the permutation (132).

In summary, we have worked out the permutation representation: it is the map $G \to S_3$ sending 1 to 1, x to (123), and x^2 to (132).

Let us prove some general facts about this example.

Proposition 3.1. *The left multiplication action of G on itself is transitive, i.e. for any $a \in G$, $\mathcal{O}_a = \{b \in G \mid b = g \cdot a \text{ for some } g \in G\} = G$.*

Proof. Let $a \in G$. Let $b \in G$ be any element. We need to show that $b \in \mathcal{O}_a$. But, because $a, b \in G$, $g = ba^{-1} \in G$, and $g \cdot a = ga = ba^{-1}a = b$, so $b \in \mathcal{O}_a$ and we are done. $\square$

Proposition 3.2. *The left multiplication action of G on itself is faithful, i.e. for any $g_1 \neq g_2 \in G$, $\sigma_{g_1} \neq \sigma_{g_2}$.*

Proof. We prove the contrapositive. Assume that $\sigma_{g_1} = \sigma_{g_2}$. Then, for $a \in G$, $\sigma_{g_1}(a) = \sigma_{g_2}(a)$, so $g_1 a = g_2 a$. By the cancellation law, this implies that $g_1 = g_2$. $\square$

Now we can finally prove Cayley's Theorem. Recall a homework problem: if $\phi : G \to H$ is an injective homomorphism, then $G \cong \phi(G)$ and $\phi(G)$ is a subgroup of H.

Theorem 3.3 (Cayley's Theorem)**.** *Every group G is isomorphic to a subgroup of a symmetric group. If $|G| = n$, then G is isomorphic to a subgroup of S_n.*

Proof. Consider the left multiplication action of G on itself. We have already shown that the permutation representation $\phi : G \to S_G$ is a homomorphism, and by the previous proposition, ϕ is injective, so $G \cong \phi(G)$ and $\phi(G)$ is a subgroup of S_G. $\square$

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 $g \cdot aH = gaH$. In this case, generalizations of the previous propositions still hold; for example, the following is a theorem in Dummit and Foote.

Theorem 3.4. *Let G be a group and H a subgroup. Let G act by left multiplication on the set A of cosets of H in G with permutation representation π_H. Then:*

(1) G acts transitively on A
(2) the stabilizer of the coset $1H \in A$ is H
(3) the kernel of the action (kernel of π_H) is the largest normal subgroup of G contained in H.

Let us use the action to prove a theorem on normal subgroups!

Corollary 3.5. 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.