14th Lecture: 23/2

Group Actions on Sets. The notion of a group acting on a set generalises the notion of a group itself. This more general viewpoint has, for example, some combinatorial applications.

Definition 14.1. Let G be a group and S a set. A *(right) action* of G on S is a map

$$S \times G \to G,$$
$$(s,\, g) \mapsto sg$$

satisfying the following two axioms:
(1) $s1_G = s \;\forall\, s \in S$
(2) $s(gh) = (sg)h \;\forall\, g,\, h \in G,\, \forall\, s \in S$.

Remark 14.2. One could just as well define group actions from the left. As usual, the important thing is to remain consistent in any calculation.

We denote by π_g the map $s \mapsto sg$.

Proposition 14.3. *Let the group G act on the set S. Then*
(i) For every $g \in G$, π_g is a permutation of S.
(ii) The map $g \mapsto \pi_g$ is a group homomorphism from G to G_S, the group of permutations of S.

PROOF: (i) I claim that the map π_g is invertible with inverse $\pi_{g^{-1}}$. This follows from axioms (1) and (2). For let $s \in S$. Then

$$s(\pi_g \pi_{g^{-1}}) = (\pi_{g^{-1}} \circ \pi_g)(s) = (sg)g^{-1} \overset{(2)}{=} s(gg^{-1}) = s1_G \overset{(1)}{=} s.$$

(ii) Call this map ϕ. That ϕ is a group homomorphism also follows from axiom (2), since for any $s \in S$ and $g,\, h \in G$:

$$s(\phi(gh)) = s(\pi_{gh}) = s(gh) \overset{(2)}{=} (sg)h$$
$$= (s\pi_g)\pi_h = (\pi_h \circ \pi_g)(s) = s(\pi_g \pi_h) = (s)\phi(g)\phi(h).$$

In other words, $\phi(gh) = \phi(h) \circ \phi(g) = \phi(g)\phi(h)$ as functions on S, v.s.v.

Definition 14.4. If the map ϕ in Proposition 14.3 is injective, then G is said to act *faithfully* on S. In that case, $\phi(G)$ is a subgroup of G_S. We say that ϕ is an *embedding* of G into G_S.

Theorem 14.5. (Cayley's Theorem for Groups) *Any group can be embedded into the group of permutations on some set.*

PROOF: Let G be a group. Then G acts on itself, considered as a set, by right-multiplication. In other words, we interpret sg as multiplication in the group, for all $s,\, g \in G$. It is clear that this is indeed a group action:

Axiom (1) is equivalent to 1_G actually being an identity element for G.

Axiom (2) is equivalent to the group operation being associative.
More significantly, this action is faithful. For if π_g is the identity map, then for all $s \in G$ we have $s = sg \Rightarrow s^{-1}(sg) = s^{-1}s \Rightarrow g = 1$. Hence, the map ϕ in this case embeds G into the group of permutations of G itself, considered as just a set.

Remark 14.6. Cayley's theorem explains wht the notion of group action on a set generalises the notion of group itself. It is also of conceptual importance in that it says that every group can be considered as a group of permutations (on some set), hence that permutation groups, strictly speaking, cover *all* groups. Whether or note this latter viewpoint is useful depends on the problem at hand.

We now begin the build up to the fundamental *combinatorial* result about group actions on sets, Theorem 14.14 below. From now on, so we don't have to constantly repeat ourselves in definitions and results, G is a group acting from the right on a set S.

Definition 14.7. For s in S, the *G-orbit* of s is the subset sG of S given by

$$sG = \{sg : g \in G\} = \{s' \in S : \exists\, g \in G \text{ with } sg = s'\}.$$

Proposition 14.8. *The G-orbits partition S. In other words, if $s_1,\ s_2 \in S$ then either $s_1G = s_2G$ or $s_1G \cap s_2G = \phi$.*

PROOF: Suppose $s_1G \cap s_2G \neq \phi$. Then there exist $g_1,\ g_2 \in G$ such that $s_1g_1 = s_2g_2 \Rightarrow s_2 = (s_1g_1)g_2^{-1} = (s_1)g_1g_2^{-1}$. Now let s_2g be an arbitrary element of s_2G. Then $s_2g = (s_1g_1g_2^{-1})g = (s_1)g_1g_2^{-1}g \in s_1G$. Thus, $s_2G \subseteq s_1G$. A similar argument shows that $s_1G \subseteq s_2G$, hence $s_1G = s_2G$, v.s.v.

Remark 14.9. Proposition 14.8 is a generalisation of Proposition 9.10 or, more precisely, of the equivalent version of Prop. 9.10 for left cosets. In the latter case, we have a subgroup H of a group G acting on G by right multiplication. The H-orbits then correspond to the left cosets of H in G. Proposition 9.10 itself is a special case of the equivalent version of Prop. 14.8 for left actions.

Definition 14.10. For $s \in S$, the *stabilizer* of s is the subgroup $\text{Stab}_G(s)$ of G given by

$$\text{Stab}_G(s) = \{g \in G : sg = s\}.$$

Note that $\text{Stab}_G(s)$ is indeed a subgroup of G since
(a) $s = sg = sh \Rightarrow (s)gh = (sg)h = sh = s$
(b) $s1 = s$
(c) $s = sg \Rightarrow sg^{-1} = (sg)g^{-1} = s1 = s$.

Proposition 14.11. *If G is a finite group and S a finite set then, for any $s \in S$,*

$$|sG| = \frac{|G|}{|\mathit{Stab}_G(s)|}. \tag{14.1}$$

PROOF: Let $H := \text{Stab}_G(s)$. As already noted, H is a subgroup of G. I claim that there is a 1-1 correspondence between the elements of sG and the right cosets of H in

G, given by $sg \mapsto Hg$, which will immediately imply (14.1). We need to show that this map from elements in the orbit of s to cosets of H has three properties:

Well-definedness: If $sg_1 = sg_2$ then we need to have $Hg_1 = Hg_2$. But $sg_1 = sg_2 \Rightarrow s = s1 = (sg_1)g_1^{-1} = (sg_2)g_1^{-1} \Rightarrow g_2g_1^{-1} \in H \Leftrightarrow Hg_2 = Hg_1$, v.s.v.
Injectivity: Basically, just run the above argument backwards:

$$Hg_1 = Hg_2 \Rightarrow g_2g_1^{-1} \in H \Rightarrow (s)g_2g_1^{-1} = s \Rightarrow sg_2 = sg_1.$$

Surjectivity: Trivial. Any right coset is of the form Hg for some $g \in G$, and will thus be the image of sg.

Remark 14.12. Proposition 14.11 can be considered a generalisation of Theorem 9.13.

Definition 14.13. For $g \in G$, the *fixed point set* of g, denoted $F_g(S)$, is the subset of S given by

$$F_g(s) = \{s \in S : sg = s\}.$$

Theorem 14.14. (Burnside's Lemma) *For any action by a finite group G on a finite set S one has*

$$\#\, G\text{-orbits in } S = \frac{1}{|G|} \sum_{g \in G} |F_g(S)|. \tag{14.2}$$

PROOF: Start by turning (14.1) upsidedown. So for any $s \in S$,

$$\frac{1}{|sG|} = \frac{1}{|G|} \cdot |\mathrm{Stab}_G(s)|.$$

Now sum over all $s \in S$ to get

$$\sum_{s \in S} \frac{1}{|sG|} = \frac{1}{|G|} \sum_{s \in S} |\mathrm{Stab}_G(s)|. \tag{14.3}$$

First consider the LHS of (14.3). When we sum over the elements in a fixed orbit, then each such element will contribute $1/t$ to the sum, where t is the size of the orbit. Hence, summing over the elements in a single orbit will in total contribute 1 to the sum. It follows that the entire sum is just the number of G-orbits in S. Hence, in order to prove (14.2), it remains to show that

$$\sum_{s \in S} |\mathrm{Stab}_G(s)| = \sum_{g \in G} |F_g(S)|. \tag{14.4}$$

This is proven by noting that both sides count the same thing, just in two different ways. Namely, both sides count the number of pairs $(s,\, g) \in S \times G$ such that $sg = s$.

For, on the one hand, if we first fix $s \in S$, then there are $|\mathrm{Stab}_G(s)|$ possibilities for g. Then summing over all s yields the LHS of (14.4).

On the other hand, if we first fix $g \in G$, then there are $|F_g(S)|$ possibilities for s. Then summing over all $g \in G$ yields the RHS of (14.4).

Remark 14.15. This idea of *counting pairs* in two different ways by projecting first onto one or the other coordinate is a general combinatorial principle which arises in many settings (see Demo5). This explains why Burnside's Lemma is considered a

combinatorial result. The example below is perhaps the best-known application of the Lemma.

In applications, one is interested in counting the number of orbits for some group action on a set, and Burnside's Lemma is useful if it turns out to be easier to count the sizes of sets of fixed points. In this sense, Burnside's Lemma is analogous to the Inclusion-Exclusion principle, where one is interested in counting the size of some union of sets, but it turns out to be easier to count sizes of intersections instead.

Example 14.16. (The Necklace Problem) Let $n,\ k$ be positive integers. A *necklace* consists of n beads arranged on a circular string, each of which is in one of k available colors. Let $\mathcal{N}(n,\ k)$ denote the number of different necklaces one can make from n beads and k colors. When we say "different" we are taking account of the fact that we don't distinguish between two arrangements of beads if one can be obtained from the other by just "moving the necklace around".

To make this question precise, we imagine the necklace as being a regular n-gon with the beads as its vertices. Let $S = S_{n,\,k}$ be the set of all n-tuples $(c_1,\ c_2,\ \ldots,\ c_n)$, where each $c_i \in \{1,\ 2,\ \ldots,\ k\}$. In other words, we number the vertices of the n-gon from 1 to n and number the available colors from 1 to k so that the elements of $S_{n,\,k}$ correspond to all possible arrangements of colored beads. This is before we take account of whether two arrangements are different necklaces or not. For the latter, we let $G = G_n$ be the group of symmetries of a regular n-gon. This group acts on the set $S_{n,\,k}$, for any k. Thus, two necklaces are considered different if they lie in different G-orbits, so $\mathcal{N}(n,\ k)$ is the number of G-orbits and we can use Burnside's Lemma to compute it:

$$\mathcal{N}(n,\ k) = \frac{1}{|G_n|} \sum_{g \in G_n} |F_g(S_{n,\,k})|. \tag{14.5}$$

Now the group of symmetries of a regular n-gon is a well-known object. It is called the *dihedral group* of order n and usually denoted D_n. Earlier in the course, we have already encountered $D_3 \cong S_3$, the symmetry group of an equilateral triangle, and D_4, the symmetry group of a square.

The group D_n contains two types of geometrical transformations:
(a) rotations by a mulltiple of $2\pi/n$
(b) reflection in one of n lines through the centerpoint of the n-gon.

Denote a $2\pi/n$ rotation by a and a reflection by b. Then D_n has the presentation

$$D_n = < a,\ b : a^n = b^2 = 1,\ b^{-1}ab = a^{-1} > .$$

The last commutator identity needs to be checked, but that's not important here. What matters is that D_n has size $2n$ and consists of the following elements

$$D_n = \{1\} \cup \{a^i : 1 \le i \le n-1\} \cup \{a^i b : 0 \le i \le n-1\},$$

where every element in the second subset is a rotation and every elöement in the third subset is a reflection. Substituting into (14.5) we get

$$\mathcal{N}(n,\ k) = \frac{1}{2n}\left(|F_1| + \sum_{i=1}^{n-1} |F_{a^i}| + \sum_{i=0}^{n-1} |F_{a^i b}|\right). \tag{14.6}$$

Identity: The identity element in G fixes every element of S (this applies to any group action, by Axiom (1)). Thus $|F_1| = |S| = |S_{n,\,k}| = k^n$.
Reflections: Here things are simplest when n is odd. In that case, every reflection is in a line through one of the vertices of the n-gon and the midpoint of the opposite side. A reflection thus fixes $k^{(n+1)/2}$ configurations of colored beads, since the colors can be chosen arbitrarily for the nodes on one side of the line, including the node on the line itself, and then the colors on the opposite nodes must match these. So, if n is odd, we have $|F_{a^i b}| = k^{(n+1)/2}$. I will leave it as an exericse for you to work out the answer when n is even (or see Homework 3, Exercise 3).
Rotations: Here things get trickier, because it turns out that the number of configurations fixed by a rotation of $2\pi i/n$ depends on GCD$(i,\, n)$. See Homework 3 for further discussion. Here we just consider the simplest case, namely when n is prime. In that case, for a configuration to be left unchanged by a non-trivial rotation, all the beads must have the same color (more generally, this is true of a rotation through $2\pi i/n$ whenever GCD$(i,\, n) = 1$). Hence, $|F_{a^i}| = k$ for each i.

Substituting everything into (14.6), we get the following formula when $n = p$ is an odd prime:

$$\mathcal{N}(p,\, k) = \frac{1}{2n}\,(k^n + (n-1)k + n \cdot k^{(n+1)/2}).$$

In class, we specifically did the (smallest non-trivial) example $p = 5$, $k = 2$. Thus

$$\mathcal{N}(5,\, 2) = \frac{1}{10}\,(2^5 + 4 \cdot 2 + 5 \cdot 2^3) = 8.$$

So you can make 8 different necklaces from 5 beads, given two available colors.