UMASS AMHERST MATH 411 SECTION 2, FALL 2009, F. HAJIR

PROBLEM SET 7

1. SYMMETRIES OF THE CUBE

Hold a cube in space. Consider the configurations of the cube that occupy exactly the same region in space. How many such configurations are there? Let us fix the original configuration as our base point. A movement of the cube which takes it from its original configuration to any other configuration is called a (rigid) symmetry of the cube. Thus, the set of symmetries of the cube, call it G_{cube}, is in one-to-one correspondence with the set of configurations. What we are asking then, is the determine the size of the set of symmetries of the cube. Clearly, the set of symmetries of the cube is a group under composition: the composition of two symmetries is another one, every symmetry has an inverse (reverse the motions), and the do-nothing symmetry is the identity symmetry.

It isn't too hard to convince someone that there are only finitely many possible configurations. Namely, a cube has 12 edges, and any symmetry of the cube permutes the edges. Moreover, if two symmetries permute the 12 edges in exactly the same way, then clearly the two symmetries are identical. Since there are at most 12! permutations of the edge set E, there are at most 12! possible permutations of the cube. In other words, there is a one-to-one map $G_{\text{cube}} \hookrightarrow \text{Perm}(E)$, so $|G_{\text{cube}}| \leq |\text{Perm}(E)| = 12!$. Note that this map is even a homomorphism of groups.

It takes a bit more work to identify $|G_{\text{cube}}|$ exactly. First, let us note that $|G_{\text{cube}}| \neq 12!$. This would happen only if every possible permuation of the 12 edges actually occurs as a rigid symmetry of the cube. This is clearly impossible! For example, if two edges, call them e_{12} and e_{23} meet at a vertex v_2, then under every rigid symmetry $\varphi \in G_{\text{cube}}$, $\varphi(e_{12})$ and $\varphi(e_{23})$ have to meet (and they have to meet at $\varphi(v_2)$). So, not all permutations of the edge set arise from rigid symmetries of the cube.

Now, a cube has 8 vertices, so by the same argument as above, we get $G_{\text{cube}} \hookrightarrow \text{Perm}(V)$, where V is the set of vertices of the cube, giving us $|G_{\text{cube}}| \leq 8!$. This is an improvement, but it's still a big overestimation, as can be seen by sitting with a cube and moving it around. It has a bunch of symmetries but not as many as 8!!. (Here the first "!" means factorial, the second "!" means "EXCLAIM!").

Well, going from edges to vertices gave an improvement, since there are fewer vertices. Now, let's see, a cube has six faces (the squares). Does that help? Let F be the set of faces of the cube.

PROBLEM 1. Use the action of G_{cube} on F to prove that $|G_{\text{cube}}| \leq 720$. Be sure to explain why the map $G_{\text{cube}} \to \text{Perm}(F)$ is injective.

We can try to improve on this estimate as follows. There are three pairs of opposite faces in the cube. If two faces are opposite in the original configuration, they they will remain opposite (not touching) under any rigid symmetry. Therefore, we have a map $G_{\text{cube}} \to \text{Perm}(\overline{F})$ where $\overline{F}$ is the set of pairs of opposite faces.

PROBLEM 2. Since $|\overline{F}| = 3$, $|\text{Perm}(\overline{F})| = 3! = 6$. Does the above argument prove that $|G_{\text{cube}}| \leq 6$? Does that seem reasonable? [Spend a moment twisting a cube around; do you see any subgroups of order 4 for example?] What can you say about the kernel of the map $G_{\text{cube}} \to \text{Perm}(\overline{F})$? Can you determine its order exactly? If so, using the First Isomorophism Theorem, can you determine $|G_{\text{cube}}|$?

Returning to the action of the symmetry group of the cube on the set of its vertices, note that under any symmetry, diagonally opposed vertices must remain diagonally opposed. In fact, imagine the space diagonals that connect pairs of diagonally opposed vertices (corners) of a cube. They meet at the very center of course and there are four of them (half as many as there are vertices). Any rigid symmetry of the cube permutes these 4 diagonals. Let D be the set of the space diagonals of the cube.

PROBLEM 3. By twisting a cube around, convince yourself that the map $G_{\text{cube}} \to \text{Perm}(D)$ is injective: the only symmetry that sends each of the four diagonals to itself is the identity. Now convince yourself that any preassigned permutation of the 4 diagonals can be achieved via a rigid symmetry of the cube. Hence the map $G_{\text{cube}} \to \text{Perm}(D)$ is surjective as well. Therefore, we expect $G_{\text{cube}} \xrightarrow{\sim} S_4$ has order 24. We'll discuss a more rigorous proof later.

2. Group Actions

Suppose X is a set. Recall that $\text{Perm}(X)$ is the set of bijective maps from X to X; it is a group under composition of maps. If G is a group, a *left action* of G on X is a group homomorphism

$$\sigma : G \to \text{Perm}(X),$$

sending $g \mapsto \sigma_g$. We say that G *acts on* X *on the left via* σ. Thus, a left action of G on X is simply a rule that assigns to each $g \in G$ a permuation $\sigma_g : X \xrightarrow{\sim} X$ of X, i.e. a bijective map sending $x \in X$ to $\sigma_g(x) \in X$. It is very convenient to suppress the homomorphism σ from the notation and write simply $g.x = \sigma_g(x)$, remembering all the while two rules which codify the fact that σ is a homomorphism, namely

- $e.x = x$ for all $x \in X$ (where e is the identity element of G),
- $(a * b).x = a.(b.x)$ for all $a, b \in G$ and $x \in X$.

These can also be written as $\sigma_e(x) = x$ and $\sigma_{ab}(x) = \sigma_a(\sigma_b(x))$.

Note that these rules also entail $\sigma_{a^{-1}}(x) = \sigma_a^{-1}(x)$. Here σ_a^{-1} means the inverse function of σ_a, i.e. $\sigma_a(\sigma_{a^{-1}}(x)) = \sigma_e(x) = x$.

We say that the action of G on X is *faithful* if the map $\sigma : G \to \text{Perm}(X)$ is injective. Equivalently, the action of G on X is faithful if given $g \neq g' \in G$, there exists $x \in X$ such that $g.x \neq g'.x$.

We say that the action of G on X is *transitive* if given any pair x, y of elements of X, there exists $g \in G$ such that $y = g.x$.

The Stabilizer and the Orbit

We continue with the notation above, so X is a set and G acts on the left on X via σ. Given $x \in X$, there are two important "sub-thingies" associated to x, one is a sub*set* of X, the other is a sub*group* of G: We define the *orbit of* x by

$$\mathcal{O}(x) = \mathcal{O}_G(x) = \{g.x | g \in G\}.$$

Clearly, $\mathcal{O}(x) \subset X$. It is the set of all points to which x is carried via the action of G on X. We also define the *stabilizer* of x by

$$G_x = \mathrm{Stab}(x) = \mathrm{Stab}_G(x) = \{g \in G | g.x = x\}.$$

PROBLEM 4. Prove that G_x is a subgroup of G.

Let us make a very simple observation. If $G_x = G$, then $\mathcal{O}(x) = \{x\}$. Qualitatively, if the stabilizer of x is "big," then the orbit of x is small. This is true more generally in a very precise way. Namely, we have

The See-Saw Principle of Group Actions: If a finite group G acts on a set X, then for every $x \in X$, $|G_x| \cdot |\mathcal{O}(x)| = |G|$.

Let us just point out a few examples of this (other than $G_x = G$).

Suppose $G = S_4$ acting on the set $X = \{1, 2, 3, 4\}$. If $x = 1$, then G_x is isomorphic to the set of all permutation sof $\{2, 3, 4\}$ which has order 6 of course, so $|G_x| = 6$. Note that $\mathcal{O}(x) = X$ which has order 4, and $4 * 6 = 24$ is indeed the cardinality of G.

PROBLEM 5. Though we haven't yet proved it, use the See-Saw Principle to prove that the group of symmetries of a regular n-gon ($n \geq 3$ is a fixed integer) has order $2n$. Hint: Consider the stab and orb of a fixed vertex.

Splitting Principle of Group Actions

When a group G acts on a set X, it induces an equivalence relation on X in a very natural way, namely, $x \sim y$ if and only if there exists $g \in G$ such that $g.x = y$.

PROBLEM 6. Use the axioms of a group action to verify that this definition does give an equivalence relation on X.

Recall that an equivalence relation on X is no more and no less than a partition of X.

PROBLEM 7. Show that under the defintion above, the partition of X to which the action of G on X gives rise is simply the set of G-orbits of elements of X.

PROBLEM 8. Suppose X is finite. Let $\mathrm{Orb}(G, X)$ be the set of G-orbits of elements of X. Use Problem 7 to show that

$$|X| = \sum_{A \in \mathrm{Orb}(G,X)} |A|.$$

Proof of the See-Saw Principle

First let us restate it in a slightly more general form: If G acts on the left on X and $x \in X$, then the cardinality of the orbit of x equals the index of the stabilizer of x in G, i.e.

$$|\mathcal{O}(x) = [G : G_x].$$

How do we get our previous See-Saw from this one? Easy, by Lagrange, if G is finite, then $|G|/|G_x| = [G : G_x]$. So how do we prove the above See-Saw Principle (it is Theorem 2.71 in the book). Let's give a bijection ψ from the set G/G_x to the set $\mathcal{O}(x)$ as follows. Any coset K of G_x is of the form $K = gG_x$. We put $\psi(K) = g.x$. Note that we made a choice of representative for K, so our first task (as usual) is to make sure that our map is well-defined. So, if $K = gG_x = g'G_x$, then $g' \in gG_x$, so $g' = ga$ for some $a \in G_x$. Hence $g'.x = (ga).x = g.(a.x) = g.x$ since $a.x = x$ by virtue of the fact that $a \in G_x$ is in the stabilizer of x. So, we have a well-defined map $\psi : G/G_x \to \mathcal{O}(x)$ sending $gG_x \mapsto g.x$. Why is this map injective? Suppose $g'.x = g.x$ for some $g, g' \in G$. Then $g^{-1}(g'.x) = g^{-1}(g.x)$ i.e. $(g^{-1}g').x = e.x = x$ which means that $g^{-1}g' \in G_x$, i.e. $gG_x = g'G_x$. Thus, if $\psi(K) = \psi(L)$, then $K = L$. Why is ψ surjective? Well, if $y \in \mathcal{O}(x)$, then $y = g.x$ for some $g \in G$ by definition of the orbit of x, so $y = \psi(gG_x)$. This completes the proof that $\psi : G/G_x \to \mathcal{O}(x)$ is a bijection.

Note the fabulous consequence:

When a finite group acts on a set, the sizes of the orbits are divisors of the order of the group.

3. Actions of a group on itself

If G is a group, there are two very natual actions of G the group on G the set, namely translation and conjugation. These actions descend (**always** in the first case, **sometimes** in the second case) to actions on quotients of G. Both of these actions are extremely important in group theory. Indeed, everything we have done in this course can be understood in terms of these two actions.

Action by translation

Let G be a group and let H be a subgroup of G; let $X = G/H$ be the set of left cosets of H in G. Keep in mind the "trivial" case where $H = \{e\}$, in which case G/H can be identified with G itself, since each coset of H consists of exactly one element of G.

The group G acts on G/H by translation. Namely, for each $g \in G$, and each $x \in G/H$ (for which we can write $x = aH$ for some $a \in G$), we define $g.x = gx = gaH$.

PROBLEM 9. Verify that this gives a well-defined action of G on G/H. Give a definition of the underlying map $\sigma : G \to \mathrm{Perm}(G/H)$ which codifies the action of G on G/H and verify that σ is a homomorphism. Verify that this action of G on G/H is transitive.

The conjugation action of G on itself

Suppose G is a group. Recall that for each $g \in G$, the map $c_g : G \to G$ given by $c_g(a) = gag^{-1}$ is an isomorphism of G (Problem set n where $3 \le n \le 5$). The conjugation action of G on G is given by the map $G \to \mathrm{Perm}(G)$ sending g to c_g.

PROBLEM 10. Verify that $G \to \mathrm{Perm}(G)$ sending g to c_g is a homomorphism, thereby checking that G acts on G via conjugation.

If $x \in G$, then under the conjugation action of G, the orbit of x is given by $\mathcal{O}(x) = \{gxg^{-1} | g \in G\}$. The orbits of G under the conjugation action are called the *conjugacy classes of* of G; some people use the notation x^G for the conjugacy class in G of the element x. In other words, a conjugacy class of G is a subset of G of the form $x^G = \{gxg^{-1} | g \in G\}$ where x is a fixed element of G. By a previous homework problem, the elements of a conjugacy class all have the same order. [Warning: just because two elements of a group G have the same order, one cannot conclude that they are conjugate; example: consider an abelian group!]

PROBLEM 11. Show that In an abelian group, every conjugacy class has exactly one element in it. Show that every non-trivial group has at least two conjugacy classes.

We have discussed the orbit of a point under the conjugation action, what about its stabilizer? Under the conjugation action, we have

$$G_x = \{g \in G | gxg^{-1} = x\}.$$

The set $C_G(x) = \{g \in G | gx = xg\}$ is called the *centralizer of* x *in* G. It is the set of elements of G that commute with G. We have $G_x = C_G(x)$ for the conjugation action.

PROBLEM 12. Prove that for $x \in G$, the size of the conjugacy class of x in G is the index of the centralizer of x in G, i.e.

$$|x^G| = [G : C_G(x)].$$

In particular, if G is finite, then $|x^G|$ is a divisor of $|G|$.

Recall that $Z(G) = \{g \in G | ga = ag \text{ for all } a \in G\}$ is the set of all elements of G that commute with every element of G. We've already seen that $Z(G)$ is a subgroup of G.

PROBLEM 13. Prove that $Z(G)$ is normal in G.

PROBLEM 14. Prove that if $x \in G$, then $|x^G| = 1$ if and only if $x \in Z(G)$.

PROBLEM 15. Prove the CLASS EQUATION for a finite group G, namely, if $C_0, C_1, \ldots, C_t$ are the conjugacy classes of G, then

$$|G| = |C_0| + |C_1| + \cdots |C_t|.$$

Rephrase the class equation in terms of the center and centralizers of elements of G.

PROBLEM 16. Prove that every normal subgroup H of a group G is a union of conjuacy classes of G, one of which is the trivial conjugacy class $\{e\}$.

PROBLEM 17. Suppose G acts on X. If $\mathcal{O}(x) = \mathcal{O}(y)$, show that $G_y = gG_xg^{-1}$ where $y = g.x$.

Suppose G acts on X. For each $g \in G$, let $\mathrm{Fix}(g) = \{x \in X | g.x = x\}$ be the subset of X consisting of those elements on which g acts trivially.

PROBLEM 18. If G is a group acting on a finite set X and there are N orbits, then

$$N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$