Discrete Mathematics lecture notes 12-1

November 22, 2013

31. Permutation groups, stabilizers, and orbits

Symmetric groups are all well and good, but the presence of an adjective suggests that a more general notion is possible. In fact, we've already seen the abstract definition of a group, but we will not have need of that level of generality. Instead, we will examine those groups that live inside some symmetric group.[1]

Definition 1. A *subgroup* of Σ_n is a subset $G \subseteq \Sigma_n$ that satisfies

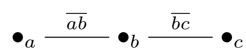
- for all $g, h \in G$, we have $g \circ h \in G$, and
- for all $g \in G$, we have $g^{-1} \in G$.

The first condition says that G is *closed under multiplication*, and the second the second that G is *closed under inversion.*

If G and H are both subgroups of Σ_n and $H \subseteq G$, we say G is a *subgroup of* G and write $H \leq G$.

For X a (finite, for us) set,[2] a *permutation group on* X is a subgroup $G \leq \Sigma_X$. We will often call G a *group of symmetries* of X.

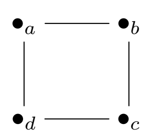
Example 2. Consider the figure[3] Γ below:



The labels on the dots and lines[4] are only to help us tell them apart. We think of Γ as consisting of two set: The set of vertices $V := \{a, b, c\}$ and the set of edges $E := \{\overline{ab}, \overline{bc}\}$. By definition, a *symmetry* of Γ is a pair (φ, η) where $\varphi : V \xrightarrow{\sim} V$ and $\eta : E \xrightarrow{\sim} E$ are bijections, subject to the constraint that if the endpoints of edge e are x and y, then the endpoints of edge $\eta(e)$ must be $\varphi(x)$ and $\varphi(y)$. This is is a roundabout way of saying that a symmetry is an action of picking up the graph turning it around, twisting it, reflecting it, but never tearing it or crushing to pieces together, then setting it back down in the original place.

It is easy to see that the bijection η of the edges is determined by φ.[5] This allows us to *identify* the group of symmetries G of Γ with a subgroup of $\Sigma_{\{a,b,c\}} \cong \Sigma_3$. If φ can't tear the edges, we clearly have to send b to itself (as it is the only vertex with two edges), but we can either leave a and c each fixed or swap each with the other. Thus, in cycle notation, $G = \{\mathrm{id}, (a\ c)\}$. Check that G is indeed closed under multiplication and inversion.

Example 3. We look now at a more complicated graph Ξ:



As in the previous example we're interested in the graph symmetries of Ξ are determined by where the vertices are sent, and so can be identified with a subgroup of $\Sigma_{\{a,b,c,d\}}$. Alternately, one could simply view Ξ as a square with labeled corners, and ask for the symmetries of that as a geometric object.[6]

[1]It turns out that this isn't really any less general: *Every* abstract group can appear as a subgroup of some (possibly infinite) symmetric group, though the utility of this observation is not absolute.

[2]In fact, we could just take $X = [n]$, but I want to now emphasize the fact that X is just a set without any *a priori* structure.

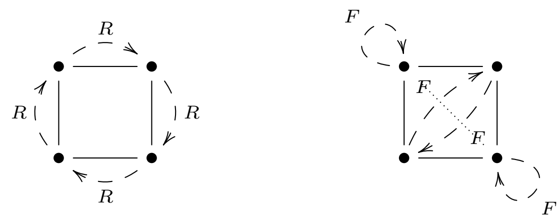
[3]This is an example of a combinatorial object called a *graph.*

[4]These are called *vertices* and *edges*, respectively.

[5]At least in this case. Can you draw a graph where this is not true?

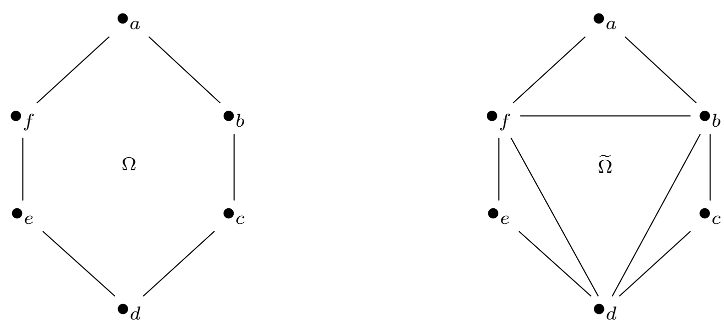
[6]There's a bit of a subtle point here: The symmetries of the square are *not* the same as those permutations of the corners that can be extended to a rigid motion on each of the sides; they are merely *determined* by such a corner-permutation. This is brushing up against the difference between equality vs. bijection of sets, or more accurately, equality vs. isomorphism of groups.

Consider the 90° clockwise rotation R and the flip about the dotted line F:



In cycle notation, we have $R = (a\ b\ c\ d)$ and $F = (b\ d)$. If e denotes the identity permutation, the group of symmetries of Ξ is, as a set $\{e, R, R^2, R^3, F, FR, FR^2, FR^3\}$. This is called the *dihedral group of order* 8, denoted D_8.[7] You should verify for yourself that D_8 is closed under multiplication and inversion, and that this is in fact the complete set of symmetries of Ξ.[8]

Example 4. Let Ω denote the regular hexagon, and $\widetilde{\Omega}$ the regular hexagon with a single inscribed equilateral triangle:



(Pretend they're regular.) Again, we can think of the groups of symmetries as living inside $\Sigma_{\{a,b,c,d,e,f\}}$, as each symmetry is determined by its action on the vertices. If G is the group of symmetries of Ω, then by analogy with the previous example we should have $G := D_{12}$, the dihedral group of order 12. G is generated[9] by the rotation $R = (a\ b\ c\ d\ e\ f)$ and the flip $F = (b\ f)(c\ e)$. Note $|D_{12}| = 12$, and we have the relations $R^6 = F^2 = \mathrm{id}$, $FRF = R^{-1} = R^5$.

However, not every element of G is a symmetry of $\widetilde{\Omega}$: The rotation R does not fix the triangle. If $\widetilde{G}$ is the symmetry group of $\widetilde{\Omega}$, you should check that $\widetilde{G} = \{\mathrm{id}, R^2, R^4, F, FR^2, FR^4\}$. Not in particular that there is no element of $\widetilde{G}$ that takes a to b.

The last sentence of the previous example is extremely important: Just because we're looking at a group of symmetries of some object doesn't mean the object itself is perfectly symmetric. This difference between points within the object is reflected by the nonexistence of symmetries taking one point to another, leading to the following

Definition 5. If G is a group of symmetries of the set X, an G*-orbit of* X is a subset $Y \subseteq X$ such that

- for all $y, y' \in Y$, there is some $g \in G$ such that $g(y) = y'$, and
- for all $x \in X$, if there exist $y \in Y$ and $g \in G$ such that $g(y) = x$, then $x \in Y$.

We will denote by $[x]_G$ the G-orbit containing the point $x \in X$.

[7] Warning: Some people call this group group D_4, as it is the group of symmetries of the regular 4-gon (a.k.a. square). In general, the group of symmetries of the regular n-gon would be called, using this alternate naming convention, D_n, but for us we'll label the dihedral groups by their orders.

[8] For instance, what about a flip through a vertical line? Where's that on our list of symmetries?

[9] In the sense discussed in the beginning of lecture notes 11-2; every element of G can be written as a product of copies of these two.

Exercise. Show that the notion of G-orbit above defined is equivalent to: A G-orbit is an equivalence class for the relation $\sim$ on X defined by $x \sim y$ iff there is some $g \in G$ such that $g(x) = y$.

In the above examples, Γ has two orbits ($\{a, b\}$ and $\{b\}$); Ξ and Ω each have one ($\{a, b, c, d\}$ and $\{a, b, c, d, e, f\}$, respectively), and $\widetilde{\Omega}$ has two ($\{a, c, e\}$ and $\{b, d, f\}$). The case where there is a single orbit is in some sense the atomic (i.e., indecomposable) one.

Definition 6. If X is a set and G a group of symmetries of X, then X is a *transitive G-set* if X has a single orbit under the action of G.

In other words, X is transitive one can move from any point of X to any other via an element of G.

We close with two notions that will play a major role in the next lecture.

Definition 7. Let X be a set and G a group of symmetries of X. For any point $x \in X$, the *stabilizer of x in G*, denoted $Stab_G(x)$ or G_x, is the subset of G defined by $G_x := \{g \in G | g(x) = x\}$.

In other words, the stabilizer of x in G is the set of points of G that fix (=stabilize) x.

Dually, we have

Definition 8. Let X be a set and G a group of symmetries of X. For an element $g \in G$, the *fixed point set of g in X*, denoted X^g, is the subset of X defined by $X^g := \{x \in X | g(x) = x\}$.

In other words, the fixed point set of g in X is the set of points of X that are stabilized (=fixed) by g.

Note the duality.

Proposition 9. *For any $x \in X$, the stabilizer G_x is a subgroup of G.*

Proof. We must show that G_x is closed under multiplication and inversion. If $g, h \in G_x$, then $g(x) = x = h(x)$, so that $(gh)(x) = g(h(x)) = g(x) = x$ and $gh \in G_x$. Similarly, to show that G_x is closed under inversion, we must have that if $g \in G_x$, then $g^{-1} \in G_x$. But $g^{-1}(x) = g^{-1}(g(x)) = (g^{-1}g)(x) = \mathrm{id}(x) = x$, from which the result follows. □

Important: $G_x \subseteq G$, $X^g \subseteq X$, and $[x]_G \subseteq X$. That is: The stabilizer of an element is a subset of G, while the fixed point sets and orbits are both subsets of X. Thus the previous proposition only makes sense for the stabilizer, where there is an induced multiplication induced by the ambient group G, and there is no dual version possible for either fixed point sets or orbits.[10]

[10] As with most claims that something is not possible, this is a lie. Except when we prove it, then it's true. Anyway, the point is that we can't dualize the last proposition *without* either more structure or a more general understanding of G-actions, leading to something called a groupoid. Cool stuff.