MA294 Lecture

Timothy Kohl

Boston University

July 14, 2021

All Groups are Permutation Groups

This statement has to be qualified a bit, but basically we can take an arbitrary group G (which is not necessarily a permutation group itself) and 'represent it' as a group of permutations on some set, in a relatively natural way.

Specifically, for a given group G, we can view G itself as a set, which can be permuted like any other set.

This gives rise to the following important idea.

Definition

For G a finite group, the left regular representation is the function $\lambda : G \to Perm(G)$ defined by $\lambda(g)(h) = gh$ for each $h \in G$.

The reason $\lambda : G \rightarrow Perm(G)$ makes sense is that for each $g \in G$ and elements $h_1, h_2 \in G$ we have that $gh_1 = gh_2$ if and only if $h_1 = h_2$.

This means that if $G = \{h_1, h_2, \ldots, h_n\}$ then for $g \in G$ we get a re-arrangement, i.e. permutation in that $gh \in G$ for each $h \in G$ so $G = \{gh_1, gh_2, \ldots, gh_n\}$ where, by the above observation, $gh_i = gh_j$ implies $h_i = h_j$.

To give an example of how this works, suppose we have $G = \mathbb{Z}_3 = \{0, 1, 2\}$ where now, since G is 'additive', we have $\lambda(g)(h) = g + h$.

So now, consider $\lambda(1)$ where $\lambda(1)(0) = 1 + 0 = 1$, $\lambda(1)(1) = 1 + 1 = 2$ and $\lambda(1)(2) = 1 + 2 = 0$ which means we can write $\lambda(1)$ in cycle notation as

$$\lambda(1) = (0, 1, 2)$$

and similarly $\lambda(2) = (0, 2, 1)$ and $\lambda(0) = ()$

Recall that the trivial permutation is written in cycle notation as '()'.

This can also be done with non-abelian groups, such as D_3.

For our purposes, we will give a slightly different presentation of D_3 which, at first, looks a bit abstract.

Instead of 'rotations' and 'flips' we can think of the group in terms of 'equations' that the elements of the group must satisfy.

So let's define 'x' to have the property that $x^3 = 1$, similar to how we defined C_3 earlier as $\langle x \rangle$.

But let's introduce another variable/symbol which we'll denote by 't' which has the property that $t^2 = 1$.

So we can (in a way) view x as corresponding to the rotation r_{120} and t as corresponding to one of the flips, say f_1.

The other 'equation' we need is one which describes how x and t 'interact' with each other.

And since we're thinking about D_3 then we know that rotations and flips don't commute, and indeed, from the group table for D_3, we find that $r_{120} \circ f_1 = f_1 \circ r_{240}$.

So if we view 'x as r_{120} then $x^2 = r_{240}$, which means that x and t satisfy the equation

$$xt = tx^{-1}$$

where $x^{-1} = x^2$ which means our 'new' D_3 contains $\{1, x, x^2\}$ and $\{1, t\}$ which means, we are 'missing' two other elements, namely the two other flips.

However, we know from looking at the group table for D_3 that if one composes a rotation with a flip, one gets a *different* flip.

So in particular the other two 'flips' are actually tx and tx^2 which means our (abstract) D_3 (as a set) consists of $\{1, x, x^2, t, tx, tx^2\}$.

One also can use the rule $xt = tx^{-1}$ to multiply the elements in this set, for example:

$$\begin{aligned} tx \cdot t &= t(xt) \\ &= t(tx^{-1}) \\ &= t^2x^{-1} \\ &= x^{-1} \\ &= x^2 \end{aligned}$$

and so on which means we can actually compute a group table.

Let's consider the group table for this D_3.

$\cdot$	1	x	x^2	t	tx	tx^2
1	1	x	x^2	t	tx	tx^2
x	x	x^2	1	tx^2	t	tx
x^2	x^2	1	x	tx	tx^2	t
t	t	tx	tx^2	1	x	x^2
tx	tx	tx^2	t	x^2	1	x
tx^2	tx^2	t	tx	x	x	1

which is, of course, synchronous with the group table for D_3 although when presented geometrically, 'x' corresponds to a 120° rotation, 'x^2' a 240° rotation etc.

Note also that $|t| = |tx| = |tx^2| = 2$ and $|x| = |x^2| = 3$ and $|1| = 1$ of course.

Basically, we've established an isomorphism

$$\{r_0, r_{120}, r_{240}, f_1, f_2, f_3\}$$
$$\updownarrow$$
$$\{1, x, x^2, t, tx, tx^2\}$$

where the second version is a bit easier to deal with, notationally, and computationally in that it is succinctly presented in terms of what are called 'generators' and 'relations'.

$$\langle x, t \mid x^3 = 1, t^2 = 1, xt = tx^{-1} \rangle$$

Note, what would happen if we wrote down this 'presentation'

$$\langle x, t \mid x^3 = 1, t^2 = 1, xt = tx \rangle$$

instead? Is it the same group?

Now, we can compute $\lambda(x)$ for $D_3 = \{1, x, x^2, t, tx, tx^2\}$ just given:

$$\begin{aligned}
\lambda(x)(1) &= x \cdot 1 = x \\
\lambda(x)(x) &= x \cdot x = x^2 \\
\lambda(x)(x^2) &= x \cdot x^2 = 1 \\
\lambda(x)(t) &= x \cdot t = tx^2 \\
\lambda(x)(tx) &= x \cdot tx = t \\
\lambda(x)(tx^2) &= x \cdot tx^2 = tx
\end{aligned}$$

which can be represented in cycle notation as $(1, x, x^2)(t, tx^2, tx)$.

In a similar way, one can show that $\lambda(t) = (1, t)(x, tx)(x^2, tx^2)$.

There are two key observations about $\lambda : G \to Perm(G)$.

First, λ is a group homomorphism since
$\lambda(g_1g_2)(h) = g_1g_2h = g_1(g_2h) = \lambda(g_1)(\lambda(g_2)(h)) = (\lambda(g_1) \circ \lambda(g_2))(h)$.

Second, λ is one-to-one. If we compute $ker(\lambda)$ we find that $\lambda(g)(h) = h$ for all $h \in G$ implies that $gh = h$ which implies that $g = e$, that is $\lambda(g)$ is the identity permutation, only if $g = e$, so $ker(\lambda) = \{e\}$.

We also observe that if $|G| = n$ then, clearly
$Perm(G) \cong Perm(\{1, 2, \ldots, n\}) = S_n$.

This observation, together with the fact that λ is 1-1 yields the following theorem.

Theorem (Cayley)

If $|G| = n$ then there exists a subgroup of S_n isomorphic to G.

As $\lambda : G \to Perm(G) \cong S_n$ is one-to-one then $\lambda(G)$ is a subgroup of $Perm(G)$ that is isomorphic to G.

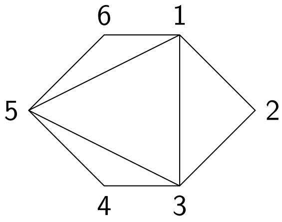
So what this implies is that S_n in some sense contains 'every group of order n' in that a group with n elements can be embedded in its group of permutations, and this group of permutations (of a set with n elements) is isomorphic to S_n.

Graph Automorphisms

Definition

A graph Γ consists of two sets, $V = \{v_1, \ldots, v_n\}$, **vertices** (or **nodes**) and **edges** $E = \{(v_i, v_j)\}$ which join different pairs of nodes.

For example:



A graph is a means of depicting a set of relationships that exists between different elements of the set of vertices.

A natural (although huge!) example of this is the internet, where the nodes are computers and edges are the existence (or non-existence) of connections between the computers.

Our examples will be small obviously, and in particular we are interested in ways to permute the vertices of the graph but not change the essential 'connectivity' of the graph.

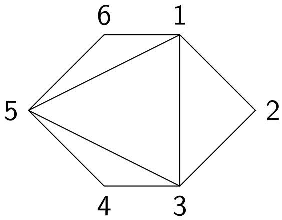
We'll make this definition precise in a moment.

To start with, we need a definition.

Definition

Given a graph $\Gamma = (V, E)$ the degree of any vertex v ($deg(v)$) is the number of edges connected to that vertex.

So for our first example:



we have $deg(v_1) = 4$, $deg(v_2) = 2$, $deg(v_3) = 4$, $deg(v_4) = 2$, $deg(v_5) = 4$, and $deg(v_6) = 2$.

Definition

A graph automorphism of a graph $\Gamma = (V, E)$ is an element $\sigma \in Perm(V)$ such that if v_i and v_j are connected by k edges, then $(\sigma(v_i)$ and $\sigma(v_j))$ are too.

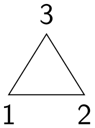
So for the example above, where $V = \{1, 2, 3, 4, 5, 6\}$ we can view the automorphism group as a subgroup of S_6, the question is, what are the elements of this group?

To begin with, we have the following very useful fact regarding degrees.

Proposition

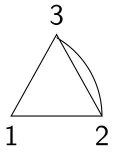
If $\Gamma = (V, E)$ and $\sigma \in Aut(\Gamma)$ is a graph automorphism, then for $v \in V$, $deg(\sigma(v)) = deg(v)$.

Before we look at our original example, let's look at some simpler ones.



Here $V = \{1, 2, 3\}$ and each node is connected to every other by one edge, so $Aut(\Gamma) = S_3$, since every permutation in S_3 preserves the connectivity of the edges.

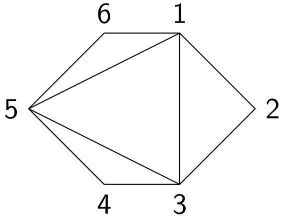
What if we modify this example slightly.



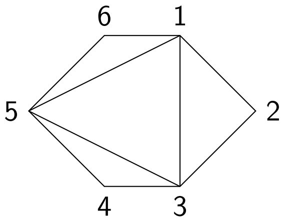
And we see now that $deg(v_2) = 3$ and $deg(v_3) = 3$ while $deg(v_1) = 2$ which means that if $\sigma \in Aut(\Gamma)$ then $\sigma(1) = 1$, which severely limits the possible choices for σ, in fact to just two.

That is $Aut(\Gamma) = \{(), (2,3)\}$ where, indeed, exchanging vertices 2 and 3 are still connected by two edges, even after we swap them.

So for this graph Γ



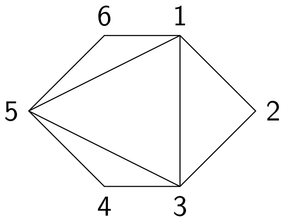
we have that $deg(v_1) = deg(v_3) = deg(v_5) = 4$, and $deg(v_2) = deg(v_4) = deg(v_6) = 2$, so if $i \in \{1,3,5\}$ then $\sigma(i) \in \{1,3,5\}$ and similarly if $i \in \{2,4,6\}$ then $\sigma(i) \in \{2,4,6\}$ too.



We will use the notation $a \leftrightarrow b$ to indicate vertices a and b are connected.

If $\sigma(1) = 3$ and $\sigma(3) = 1$ then since $1 \leftrightarrow 2$ and $3 \leftrightarrow 2$, we must have $\sigma(2) = 2$.

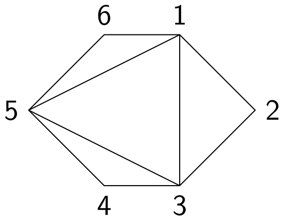
And since $deg(v_5) = 4$ then $\sigma(5) = 5$, and since $1 \leftrightarrow 6$ and $3 \leftrightarrow 4$ we must have $\sigma(4) = 6$ and $\sigma(6) = 4$, ergo $(1,3)(4,6) \in Aut(\Gamma)$.



Similarly, if $\sigma(1) = 5$ and $\sigma(5) = 1$ then $\sigma(3) = 3$ since $deg(v_3) = 4$.

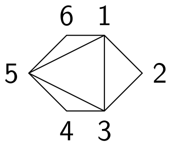
But since $1 \leftrightarrow 6$ and $5 \leftrightarrow 6$ we have $\sigma(6) = 6$, and since $1 \leftrightarrow 2$ and $5 \leftrightarrow 4$ we must have $\sigma(2) = 4$ and $\sigma(4) = 2$.

As such $(1,5)(2,4) \in Aut(\Gamma)$, and a similar argument involving the nodes 3 and 5 implies that $(3,5)(2,6) \in Aut(\Gamma)$.



Now suppose $\sigma(1) = 3$, $\sigma(3) = 5$ and $\sigma(5) = 1$ then since $1 \leftrightarrow 6$ and $1 \leftrightarrow 2$, and $3 \leftrightarrow 2$ and $3 \leftrightarrow 4$, and $5 \leftrightarrow 6$ and $5 \leftrightarrow 4$ we must also cyclically rotate the vertices $2, 4, 6$ in the same clockwise way as the vertices $1, 3, 5$.

As such $(1, 3, 5)(2, 4, 6) \in Aut(\Gamma)$, and similarly $(1, 5, 3)(2, 6, 4) \in Aut(\Gamma)$.



So we've established that $Aut(\Gamma)$ contains

$$\{(), (1,3)(4,6), (1,5)(2,4), (3,5)(2,6), (1,3,5)(2,4,6), (1,5,3)(2,6,4)\}$$

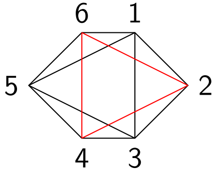
but does it contain any other elements?

No, because we were bound by the possibilities for where the nodes 1, 3, and 5 could be sent, and each such possibility forces the movements of $2, 4, 6$ so there are no more.

The last detail to consider is whether $Aut(\Gamma)$, equal to

$$\{(), (1,3)(4,6), (1,5)(2,4), (3,5)(2,6), (1,3,5)(2,4,6), (1,5,3)(2,6,4)\}$$

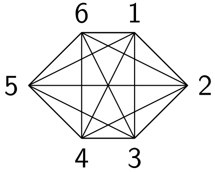
is isomorphic to something 'familiar'?
Yes, $Aut(\Gamma) \cong D_3$, and the idea is to look at the two 'triangles'



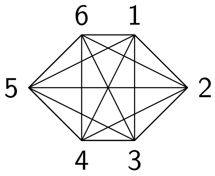
one of which is part of the graph $\{1, 3, 5\}$ and the other there by virtue of being attached to these, namely $\{2, 4, 6\}$,
i.e.$\{(), (1,3), (1,5), (3,5), (1,3,5), (1,5,3)\} \cong D_3$ and
$\{(), (4,6), (2,4), (2,6), (2,4,6), (2,6,4)\} \cong D_3$.

Complete Graphs

Here is a kind of 'extreme' example, although one which is actually pretty simple in a certain sense.



One sees that for each $v \in V = \{1, 2, 3, 4, 5, 6\}$ that $deg(v) = 5$ and, more to the point, each vertex is connected to every other vertex by an edge.



So for any $\sigma \in S_6$, one has that $\sigma(v_i)$ and $\sigma(v_j)$ are connected since v_i and v_j are connected.

As such $Aut(\Gamma)$ is all of S_6 and we have an example of a complete graph namely one for which each vertex is connected to every other vertex.

And for each n we have such a graph, and each has automorphism group equal to the entirety of S_n.

Orbits and Stabilizers

Symmetric groups also help us solve certain combinatorial (counting) problems. Let X be a finite set and $G \leq Perm(X)$ and define an equivalence relation $\sim$ on X as follows:

$$x \sim y \text{ if } g(x) = y \text{ for some } g \in G$$

Let's verify this is an equivalence.

- $x \sim x$ since $e(x) = x$ for $e \in G$ the identity element which fixes every element of X
- If $x \sim y$ then $g(x) = y$ for some $g \in G$, but then $x = g^{-1}(g(x)) = g^{-1}(y)$, i.e. $g^{-1}(y) = x$ so $y \sim x$
- If $x \sim y$ and $y \sim z$ then $g(y) = x$ and $g'(z) = y$ which means $g(g'(z)) = x$, i.e. $(g \circ g')(z) = x$ so $z \sim x$

Definition

For this equivalence relation, the equivalence classes are called the orbits with respect to the action of G on X.
Specifically, for $x \in X$, let $Gx = \{g(x) \mid g \in G\}$ where, if $G = \{g_1, \dots, g_n\}$ is literally $\{g_1(x), g_2(x), \dots, g_n(x)\}$

Note, it *is* possible that $g_i(x) = g_j(x)$ for two *distinct* elements $g_i, g_j \in G$, including the possibility that $g(x) = x$ for some $g \in G$ where $g \neq e$.

Example: $G = \{(), (1,2)(3,4,5), (3,5,4), (1,2), (1,2)(3,5,4), (3,4,5)\}$

- $G1 = \{1,2\}$
- $G2 = \{1,2\}$
- $G3 = \{3,4,5\}$
- $G4 = \{3,4,5\}$
- $G5 = \{3,4,5\}$

and we see here another phenomenon, namely that $Gx = Gy$ even when $x \neq y$.

Of particular importance for applications is the determination of $|Gx|$ for each $x \in X$.

Definition

For $G \leq Perm(X)$, and $x, y \in X$ let

$$G(x \to y) = \{g \in G \mid g(x) = y\}$$

and for $x = y$ we have

$$G(x \to x) = \{g \in G \mid g(x) = x\}$$

where $G(x \to x)$ is the stabilizer of x in G, which we also denote G_x.

Note, for any $x \in X$, we have $G_x \leq G$ since if $g_1, g_2 \in G_x$ then $(g_1 \circ g_2)(x) = g_1(g_2(x)) = g_1(x) = x$, and if $g(x) = x$ then $g^{-1}(g(x)) = g^{-1}(x)$, that is $x = g^{-1}(x)$ and thus $g^{-1} \in G_x$ too.

We observed that $G_x = G(x \to x)$ is a subgroup of G for each $x \in X$, so what about $G(x \to y)$ for $x \neq y$?

Theorem

Let $G \leq Perm(X)$ and let $h \in G(x \to y)$ then

$$G(x \to y) = hG_x$$

a left coset of G_x in G.

Proof.

If $g \in G_x$ and $h(x) = y$ then $(h \circ g)(x) = h(g(x)) = h(x) = y$ so that $h \circ g \in G(x \to y)$ so $hG_x \subseteq G(x \to y)$.

If $h \in G(x \to y)$ then $h = (h \circ e) \in hG_x$ since certainly $e \in G_x$ and so $G(x \to y) \subseteq hG_x$, so $G(x \to y) = hG_x$. □

As a consequence we have the following really fundamental fact about permutation groups, called the Orbit-Stabilizer Theorem.

Theorem

If $G \leq Perm(X)$ then $|Gx| = [G : G_x] = \frac{|G|}{|G_x|}$.

Proof.

The basic idea is that if $Gx = \{y_1, \ldots, y_m\}$ then $G(x \to y_i) \cap G(x \to y_j) = \emptyset$ for $i \neq j$ and $G(x \to y_i) = h_i G_x$ for distinct $\{h_1, \ldots, h_m\}$ where $G = h_1 G_x \cup h_2 G_x \cup \cdots \cup h_m G_x$.

But this says that 'm' which is $|Gx|$ is the same as the number of distinct cosets of G_x in G, that is $[G : G_x]$ where $[G : G_x] = \frac{|G|}{|G_x|}$. □

Example: $G = \langle (1,2)(3,4,5) \rangle =$
$\{(), (1,2)(3,4,5), (3,5,4), (1,2), (1,2)(3,5,4), (3,4,5)\}$

- $|G1| = 2 \leftrightarrow G_1 = \langle (3,4,5) \rangle \leftrightarrow [G : G_1] = \frac{6}{3} = 2$
- $|G3| = 3 \leftrightarrow G_3 = \langle (1,2) \rangle \leftrightarrow [G : G_3] = \frac{6}{2} = 3$

The main point of this theorem is that one may determine $|Gx|$ (which may not be easy to find) by using G_x which is generally easier to determine.

For a given $G \leq Perm(X)$ a related question that is also important is to find out how many distinct orbits there are.

For example, with $G = \langle(1,2)(3,4,5)\rangle$, we saw that $G1 = \{1,2\}$, $G2 = \{1,2\}$ while $G3 = \{3,4,5\}$, $G4 = \{3,4,5\}$, and $G5 = \{3,4,5\}$ as well.

Definition

For $G \leq Perm(X)$ and $g \in G$, let $F(g) = \{x \in X \mid g(x) = x\}$ which are the set of those elements of G which fix x.

Theorem (Frobenius)

For $G \leq Perm(X)$ the number of orbits of G on X is

$$\frac{1}{|G|}\sum_{g\in G}|F(g)|$$

which is a whole number.

Before exploring the proof, we should mention that this result is actually the tool that we will use for solving different combinatorial (counting) problems.

It is built on the Orbit-Stabilizer Theorem, but is different in that it actually tells us how many distinct orbits there are, which is actually a bit more mysterious than the size of the orbit of a particular element of x.

This theorem is telling us a *lot* about the action of G on X overall.

PROOF:
Consider the following subset of $G \times X$

$$E = \{(g, x) \mid g(x) = x\}$$

whose size we will compute in two different ways, and these two ways of counting will give us the statement of the theorem.

If $G = \{g_1, \ldots, g_n\}$ and $X = \{x_1, \ldots, x_r\}$ then $E = E_{g_1} \cup \cdots \cup E_{g_n}$ where

$$E_{g_i} = \{(g_i, x) \in G \times X \mid (g_i(x) = x\}$$

where the E_{g_i} are disjoint, and, for some g_i, potentially empty.
Moreover, it's clear that $E_{g_i} = F(g_i)$.

So we have that $|E| = \sum_{i=1}^{n} |F(g_i)|$.

Another way to view E is as follows:

$$E = E_{x_1} \cup E_{x_2} \cup \cdots \cup E_{x_r}$$

where $E_{x_j} = \{(g, x_j) \in G \times X \mid g(x_j) = x_j\}$ and so $|E_{x_j}| = |G_{x_j}|$ (!), so we have that

$$|E| = \sum_{j=1}^{r} |G_{x_j}|$$

So if $\{x_{11},\ldots,x_{1e_1}\}$, $\{x_{21},\ldots,x_{2e_2}\}$,...,$\{x_{t1},\ldots,x_{te_t}\}$ are the distinct orbits of G on X, namely t orbits, where the size of the i^{th} orbit is e_i.

As such $|Gx_{ij}| = e_i$ for $i = 1,\ldots,t$ and $j = 1,\ldots,e_t$, so $\frac{|G|}{|G_{x_{ij}}|} = e_i$ and so $|G_{x_{ij}}| = \frac{|G|}{e_i}$ for $i = 1,\ldots,t$.

Thus

$$\sum_{x\in X} |G_x| = e_1\frac{|G|}{e_1} + e_2\frac{|G|}{e_2} + \cdots + e_t\frac{|G|}{e_t}$$
$$= t|G|$$

and so... $\sum_{g\in G} |F(g)| = \sum_{x\in X} |G_x| = t|G|$ which means

$$t = \frac{1}{|G|}\sum_{g\in G} |F(g)|$$

as claimed. $\square$