TOPICS IN PERMUTATION GROUPS

A SHORT SEMINAR SERIES

JOSHUA WISCONS

Contents

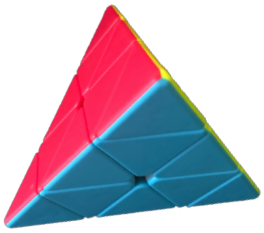
These (in progress!) notes are being prepared for a six-part seminar series on permutation groups in Spring 2022 at California State University, Sacramento. The seminar is meant to be casual, example driven, hopefully fun, and accessible to anyone having completed a first course in linear algebra, though exposure to groups will help.

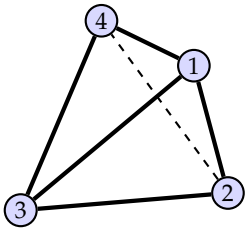
Date: April 11, 2022.

1. A First Example

Let's start by exploring symmetries of a familiar object. We'll also introduce notation as we go.

Example 1. Consider a regular tetrahedron, like the Pyraminx (pictured below). One way to represent the various symmetries is to consider how each symmetry permutes the vertices, so let's label them as follows





Let Tetra denote the collection of *all* symmetries of this object and Tetra$^+$ denote just the *rotational* symmetries. We will view each element of Tetra (and Tetra$^+$) as a permutation of the set $\{1, 2, 3, 4\}$. The collection of *all* permutations of $\{1, 2, 3, 4\}$ will be denoted Sym(4), so with this notation we have Tetra$^+ \subseteq$ Tetra $\subseteq$ Sym(4). Let's pause to define and introduce notation for Sym(X) generally.

Definition. Let X be a set. The **symmetric group** on X, denoted Sym(X), is the set of all permutations of X. When $X = \{1, 2, \ldots, n\}$, we write Sym(n) in place of Sym(X). We also adopt the following notation.

- The identity permutation will be denoted id_X (or just id), so $\mathrm{id}_X(x) = x$ for all $x \in X$.
- For $\sigma, \tau \in \mathrm{Sym}(X)$, $\sigma\tau$ denotes composition of σ and τ, so $\sigma\tau(x) = \sigma(\tau(x))$ for all $x \in X$.
- For $\sigma \in \mathrm{Sym}(X)$ and $n \in \mathbb{N}$, σ^n denotes the composition of σ with itself n-times, and σ^{-n} denotes the composition of σ^{-1} with itself n-times.

We may refer to $\sigma\tau$ as the *product* of σ and τ, but in Sym(X) this means composition.

Let's resume our investigation of the tetrahedron, and list some elements of Tetra$^+$. As we do, we'll introduce additional notation for writing permutations.

If we hold the top vertex 1, we can rotate the remaining ones by 120° to obtain the permutation γ defined via $\gamma(1) = 1$, $\gamma(2) = 3$, $\gamma(3) = 4$, and $\gamma(4) = 2$. We occasionally write permutations in two-line notation as below; the top row lists the inputs while the bottom lists the corresponding outputs.

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

More often, we will write permutations in so-called (disjoint) cycle notation, which will be "defined" via various examples. Writing γ using cycle notation yields $\gamma = (234)$. This is read left to right and indicates that a given number is mapped by γ to the number immediately to the right, cycling back to the beginning when the rightmost parenthesis is encountered. We can picture this as $2 \to 3 \to 4 \to 2$. Any number not appearing (like 1

in this case) is left fixed by the permutation. Because of the cyclical nature of this notation, there are various ways to write γ in this notation: $\gamma = (234) = (342) = (423)$.

Let's look for more symmetries. If we continue to hold the top vertex and rotate 120° again (for a total of 240°), we have the permutation $\gamma^2 = \gamma\gamma$. In two line notation,

$$\gamma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix},$$

and in cycle notation, $\gamma^2 = (243)$. Yet another rotation by 120°, returns the shape to the starting configuration, so $\gamma^3 = \mathrm{id}$. Also note, that we could have initially rotated by −120°, which is the inverse of γ (i.e. γ^{-1}), but this does not yield a new permutation since $\gamma^{-1} = (432) = (243) = \gamma^2$.

Now, this time, let's hold vertex 2, and rotate by 120°. Depending on your point of view, there are two options, but one of them is $\delta = (134)$. And rotating in the same direction by another 120°, yields $\delta^2 = (143)$. We can further consider holding the vertex 3 or 4 while rotating. So far, we've found the following rotational symmetries of the tetrahedron:

$$\{\mathrm{id}, (234), (243), (134), (143), (124), (142), (123), (132)\} \subseteq \textsc{Tetra}^+.$$

There are more. Imagine the line ℓ connecting the midpoint of the edge $\{1, 4\}$ (from vertex 1 to 4) with the midpoint of the edge $\{2, 3\}$ (from vertex 2 to 3); then let α be the rotation of the tetrahedron by 180° about the line ℓ. In two-line notation, we find that

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

and in cycle notation, we have $\alpha = (14)(23)$. Performing 180° rotations about the other two lines that connect pairs of "opposite edges", we find that $\textsc{Tetra}^+$ also contains (12)(34) and (13)(24). So now we have that

$$\left\{ \begin{matrix} \mathrm{id}, (12)(34), (13)(24), (14)(23), \\ (234), (243), (134), (143), (124), (142), (123), (132) \end{matrix} \right\} \subseteq \textsc{Tetra}^+.$$

What else could be in $\textsc{Tetra}^+$? Well, Sym(4) contains 12 more permutations that we have not encountered yet. Six of the remaining permutations move only two vertices while fixing the others, e.g. $\tau = (12)$; these permutations are called **transpositions** (since they transpose two numbers and leave the remaining unaltered). Now, τ does represent a symmetry of the tetrahedron, namely *reflection* through the plane that contains the edge $\{3, 4\}$ and is orthogonal to the edge $\{1, 2\}$. However, τ is not a *rotational* symmetry because a nontrivial rotational symmetry can only fix a vertex that is on the axis of rotation, and due to the structure of the tetrahedron, at most one vertex can lie on an axis of rotation that produces a symmetry. Similarly, we find that the other transpositions are in $\textsc{Tetra}$ but *not* $\textsc{Tetra}^+$, so

$$\{(12), (13), (14), (23), (24), (34)\} \subseteq \textsc{Tetra} - \textsc{Tetra}^+.$$

The only permutations in Sym(4) we have not yet considered are the so-called 4-cycles, such as $\sigma = (1234)$. Notice that $\sigma \in \textsc{Tetra}$ since $\sigma = (12)(23)(34)$, so it can be realized by performing three reflections in a row. However, σ is not a rotational symmetry. To see this, note that any rotation that moves vertex 2 to 3 and vertex 3 to 4 must have an axis of rotation orthogonal to *both* of the edges $\{2, 3\}$ and $\{3, 4\}$, implying that the axis of rotation runs through vertex 1, so 1 would have to remain fixed. Thus, σ is not a rotational symmetry.

Similarly, we see that each 4-cycle is in Tetra but *not* Tetra$^+$. In conclusion, we've found

$$\text{Tetra} = \text{Sym}(4)$$
$$\text{Tetra}^+ = \left\{ \begin{matrix} \text{id}, (12)(34), (13)(24), (14)(23), \\ (234), (243), (134), (143), (124), (142), (123), (132) \end{matrix} \right\}$$

Incidentally, although we already knew that the composition of any two symmetries of the tetrahedron was another symmetry, we can now directly verify that the composition of any two *rotational* symmetries is another *rotational* symmetry (e.g. $\gamma\delta = (234)(134) = (14)(23) = \alpha$).

2. Permutation groups

In this section, we'll formally introduce permutation groups and the related notion of group actions. We'll also see more examples (in addition to Tetra and Tetra$^+$); this includes the important family of alternating groups as well as the symmetry group of a cube. The section concludes with a couple of fundamental concepts in the study of permutation groups: orbits and stabilizers.

Definition. Let X be a set. A subset $G \subseteq \text{Sym}(X)$ is called a **subgroup** of $\text{Sym}(X)$ if all of the following hold:

- [closure under the identity] $\text{id} \in G$;
- [closure under composition] if $\alpha, \beta \in G$, then $\alpha\beta \in G$;
- [closure under inverses] if $\alpha \in G$, then $\alpha^{-1} \in G$.

In this case, we say G is a **permutation group** on X.

Example 2. As can be seen from Example 1, Tetra and Tetra$^+$ can both be viewed as permutation groups on $\{1, 2, 3, 4\}$.

2.1. The alternating group.

Recall that an element $\tau \in \text{Sym}(X)$ of the form $\tau = (ij)$ is called a transposition (for any $i \neq j \in X$). Let's explore how to decompose a given permutation into a product (i.e. composition) of transpositions.

Example 3. Consider the permutation $\alpha = (12345)$. After computing various products of transpositions, one might notice that α can be written as $\alpha = (12)(23)(34)(45)$ or $\alpha = (15)(14)(13)(12)$ or something else. Since $(ij)(ij) = \text{id}$ for each transposition (ij), one sees that there are a lot of ways to write α as a product of transpositions; for example, $\alpha = (12)(23)(34)(45)(12)(12)$ or $\alpha = (67)(12)(23)(34)(45)(67)$ (assuming in the latter case that we are working in $\text{Sym}(n)$ for $n \geq 7$).

What about the permutation $\beta = (12345)(6789)$? We can decompose β similar to before by treating each of the cycles (12345) and (6789) separately: $\beta = (12)(23)(34)(45)(67)(78)(89)$. And again, there are many ways to decompose β into a product of transpositions.

Abstracting our technique in the previous example, we get the following result; the proof is left as an exercise. In group-theoretic parlance, it says that each finite symmetric group is *generated* by its transpositions.

Lemma. *Every permutation in* $\text{Sym}(n)$ *can be written as a product of transpositions.*

Definition. Let $\sigma \in \text{Sym}(n)$. We call σ an **odd** permutation if it can be written as a product of an odd number of transpositions. Similarly, we call σ an **even** permutation if it can be written as a product of an even number of transpositions.

Looking back to Example 3, the permutation α was even; while β was odd. Notice that although there were several ways to write α as a product of transpositions, *every* way we came up with used an even number. It turns our that this was no coincidence.

Lemma. *Every permutation in* $\mathrm{Sym}(n)$ *is either even or odd, but not both.*

Proof idea. One first observation to make is that it suffices to prove id is (even but) not odd. Indeed, suppose we know that id is not odd. Towards a contradiction, assume an arbitrary σ is both even and odd. Then we can write $\sigma = \tau_1 \cdots \tau_k = \rho_1 \cdots \rho_\ell$ where k is even, ℓ is odd, and each τ_i and each ρ_j is a transposition. This implies $\mathrm{id} = \sigma\sigma^{-1} = \tau_1 \cdots \tau_k \rho_\ell^{-1} \cdots \rho_1^{-1}$. As the inverse of a transposition is itself, $\mathrm{id} = \tau_1 \cdots \tau_k \rho_\ell \cdots \rho_1$, implying that id is odd (since k is even and ℓ is odd), a contradiction.

So, it remains to show id is not odd. This is where most of the effort is, and we will simply refer out—sorry! A quick search of the internet will turn up various proofs of this lemma, but one nice (and detailed) outline of the proof can be found in Dana Ernst's abstract algebra book, see [Ern21, Theorem 4.103]. □

Notice that composing two even permutations results in another even permutation. Moreover, the previous "proof" discussed that id is even, and it also indicated that a permutation has the same parity as its inverse. Combining this, we arrive at the following fundamental theorem-definition.

Theorem. *Let* $\mathrm{Alt}(n)$ *denote the collection of all even permutations in* $\mathrm{Sym}(n)$*. Then* $\mathrm{Alt}(n)$ *is a subgroup of* $\mathrm{Sym}(n)$*; it is called the* ***alternating group****.*

Example 4. A concise summary of Example 1 is that if we view the elements of Tetra as permutations of $\{1, 2, 3, 4\}$, then $\mathrm{Tetra} = \mathrm{Sym}(4)$ and $\mathrm{Tetra}^+ = \mathrm{Alt}(4)$.

Note that, technically, the elements of Tetra operate on the entire tetrahedron, not just the vertices. Thus Tetra is not literally equal to Sym(4), so it is more precise to use the language of isomorphisms and write $\mathrm{Tetra} \cong \mathrm{Sym}(4)$ and $\mathrm{Tetra}^+ \cong \mathrm{Alt}(4)$. But in general, we won't much worry about this.

2.2. **One group, many actions.** When analyzing a permutation group G on some set X, it is important to keep in mind that G may very well also permute other sets, and simultaneously studying the various "actions" of G can be quite advantageous. For example, Tetra is first and foremost acting on the points of $\mathbb{R}^3$ (in a way that preserves the tetrahedron); however, the way we studied Tetra was via its action on the *vertices* of the tetrahedron. However, Tetra also permutes the *edges* of the tetrahedron as well as the *faces* and various other related sets of objects.

Let's formalize the notion of an "action", and then see how to leverage this idea with an example.

Remark. In what follows, we will occasionally use a phrase like "let G be a group." This can be taken to mean that G is a permutation group on some set X, but we don't care what X is. The point is that sometimes we only want to focus on how the elements of the group G interact with each other as opposed to how they permute the elements of X. If you've encountered the definition of an abstract group, then you could alternatively interpret "let G be a group" as "let G be an abstract group."

Definition. Let G be a group. We say G **acts** on a set Y if each $g \in G$ defines a function $Y \to Y : y \mapsto g \cdot y$ in such a way that

(1) for all $g, h \in G$ and all $y \in Y$, $g \cdot (h \cdot y) = (gh) \cdot y$, and
(2) for all $y \in Y$, $\mathrm{id} \cdot y = y$.

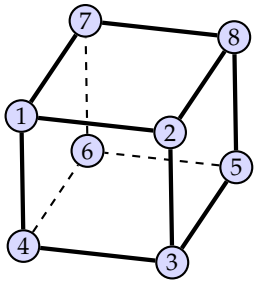
We say the action is **faithful** if the only element of G satisfying $g \cdot y = y$ for all $y \in Y$ is id.

In reading the definition, one should think of the notation $g \cdot y$ as $g(y)$. In what follows, we will often use the notation $g \cdot y$ in place of $g(y)$ for permutation groups too.

Remark. If G acts on a set Y, then the definition implies that each element of G can be viewed as a *permutation* of Y. However, it is possible for different elements of G to represent the same permutation of Y. (We'll see this in a later example.)

Now, if the action is faithful, then it can be shown that different elements of G always act as different permutations of Y, so in this case, we can view G as a permutation group on Y (even though G may also be a permutation group on some other set X). Technical note: the sentence "we can view G as a permutation group on Y" really means that "G is isomorphic to a permutation group on Y".

Example 5. Let's work out the symmetries of a cube like Rubik's Revenge (pictured below). Let Cube denote the collection of all symmetries of the cube, and let Cube$^+$ denote the rotational symmetries. As in Example 1, Cube as acts *faithfully* on the 8 vertices of the cube, so after labeling the vertices (as below), we may view Cube as a subgroup of Sym(8).



Note that Cube also acts faithfully on the 6 faces as well as on the 12 edges, so we could have instead chosen to label the faces or edges to view Cube as a subgroup of Sym(6) or Sym(12). However, for now, let's think in terms of the action on the vertices.

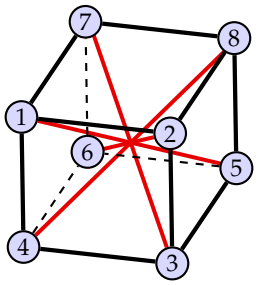
Rotating clockwise by 90° around the axis running through the centers of faces $\{1, 2, 3, 4\}$ and $\{5, 6, 7, 8\}$, we get the permutation $\alpha = (1234)(5678)$. Performing α twice (i.e. rotation about the same axis by 180°) yields the permutation $\alpha^2 = (13)(24)(57)(68)$. A third application of α results in $\alpha^3 = (1432)(5876)$, and $\alpha^4 = \mathrm{id}$. Performing similar rotations around the axes running through the center of the other two pairs of opposite faces, yields 6 more rotational symmetries, bringing our total thus far to 10: id, 3 of "shape" (13)(24)(57)(68), and 6 of "shape" (1234)(5678).

And there are more. Consider holding a pair of antipodal vertices, like 1 and 5. Let D_1 denote the diagonal line (running through the interior of the cube) connecting 1 and 5. Rotating the cube by 120° clockwise around D_1 gives the permutation $\gamma = (247)(683)$, and rotating by 240° (or −120°), yields $\gamma^2 = (274)(638)$. Considering the remaining three diagonals as well, we add 8 permutations of shape (247)(683) to our list of rotational symmetries, bringing our total thus far to 18.

And there are still more: we can rotate by 180° around the axis connecting the midpoint of opposite edges of the cube. For example, rotating about the line connecting the midpoints of edges $\{1, 4\}$ and $\{5, 8\}$ yields the permutation $\beta = (14)(58)(26)(37)$. This produces 6 more

rotational symmetries (including β) of shape (14)(58)(26)(37), and our total is now 24. Have we found all rotational symmetries? We could indeed construct a direct argument that we have found them all, but just having a complete list of the symmetries is not the end of the story. We typically also want to know more about the "structure" of the group itself.

To better understand Cube$^+$, let's change our point of view slightly. Perhaps we've noticed something about how the symmetries treat antipodal (i.e. opposite) vertices. For example, once we know where a given symmetry sends the vertex 1, we automatically know where 5 must be sent. In short, any symmetry of the cube (rotational or not), must move a pair of antipodal vertices to a (perhaps same) pair of antipodal vertices. This can be used to show that Cube acts on the 4 diagonals of the cube (pictured below).



Let's use the notation D_i for the diagonal line connecting vertex i to $i+4$ (so D_i connects vertices that are equal modulo 4). Our comment before is that Cube acts on the set $\mathcal{D} = \{D_1, D_2, D_3, D_4\}$. However, the action of Cube is *not* faithful on $\mathcal{D}$. Indeed, there is a very special reflection that takes each vertex to the antipodal vertex; let's call this antipodal reflection ρ. Then ρ fixes every diagonal, so ρ and id have the same action on $\mathcal{D}$. However, Cube$^+$ does act faithfully on $\mathcal{D}$: one can argue geometrically that the only rotational symmetry fixing all four diagonals is the identity. Thus, we may view Cube$^+$ as a subgroup of Sym($\{D_1, D_2, D_3, D_4\}$). To simplify notation, let's forget about the D, and just label the diagonals $1, 2, 3, 4$. In doing so, we may now view Cube$^+$ as a subgroup of Sym(4). Let's revisit some of the symmetries from before and see how they permute the diagonals.

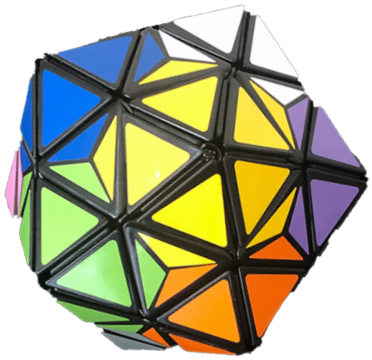
Symmetry	Permuting the vertices	Permuting the diagonals
α	(1234)(5678)	(1234)
α^2	(13)(24)(57)(68)	(13)(24)
γ	(247)(683)	(243)
β	(14)(58)(26)(37)	(14)
$\rho \notin$ Cube$^+$	(15)(26)(37)(48)	id

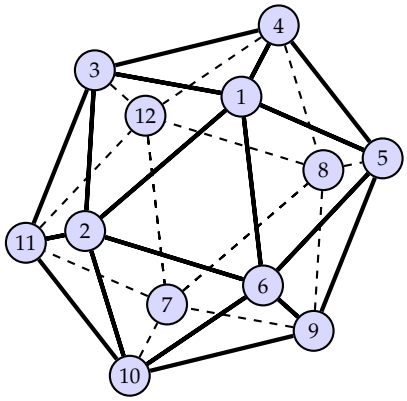
Now, remember that we found 24 rotational symmetries. If we view Cube$^+ \subseteq$ Sym(4) (permuting the diagonals), then as $|\text{Sym}(4)| = 24$, it must be that Cube$^+ =$ Sym(4). And this gives a nice description of Cube$^+$ as realizing all possible permutations of the 4 diagonals (in a way that different elements of Cube$^+$ represent different permutations of the diagonals).

And what about Cube? It turns out that if $\tau \in$ Cube, then either $\tau \in$ Cube$^+$ or $\tau = \sigma\rho$ for some $\sigma \in$ Cube$^+$ (with ρ the antipodal reflection). In other words, every symmetry of the cube is either a rotational symmetry (which we understand in terms of how it permutes the diagonals) or it is a composition of a rotational symmetry with the antipodal reflection. Moreover, for each $\sigma \in$ Cube$^+$, $\sigma\rho = \rho\sigma$, which (in group theoretic notation) implies that Cube $=$ Cube$^+ \times \{\text{id}, \rho\} \cong \text{Sym}(4) \times \mathbb{Z}_2$.

2.3. **Orbits and stabilizers.**

Example 6. Let's look at the symmetries of a regular icosahedron. (The Rubik-esque version of this is the Dogic pictured below.) Let Icosa^+ denote the set of rotational symmetries. Notice that Icosa^+ acts faithfully on the 12 vertices of the icosahedron, so after labeling the vertices (as below), we can view Icosa^+ as a subgroup of Sym(12).





This time, we'll just try to count the number of symmetries in Icosa^+ and leave the determination of which permutations are in Icosa^+ (and Icosa) as an exercise. Let $\sigma \in \text{Icosa}^+$ denote an arbitrary rotational symmetry. In two-line notation, σ has the form

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & 12 \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(12) \end{pmatrix}$$

To count Icosa^+, let's count the possible ways we can fill in the bottom row of the two-line notation for σ. Notice that there are rotations taking vertex 1 to any other vertex (including 1), so there are 12 possibilities for $\sigma(1)$.

Now assume that we have chosen $\sigma(1)$; how many possibilities remain for $\sigma(2)$? Notice that when counting the possibilities for $\sigma(2)$, the actual value of $\sigma(1)$ does not matter, so without loss of generality, we may assume that $\sigma(1) = 1$, i.e. σ fixes 1. Since 2 is connected to 1 by an edge and σ fixes 1, $\sigma(2)$ must also be connected to 1 by an edge, and we see that there are 5 possibilities for $\sigma(2)$, which correspond to rotations of the icosahedron about the line connecting 1 to its antipodal vertex 7.

Thus far, we found that there are 12 possibilities for $\sigma(1)$, and that once given $\sigma(1)$, there are 5 possibilities for $\sigma(2)$. Now assume that we know $\sigma(1)$ and $\sigma(2)$. What about $\sigma(3)$? Let's keep assuming that $\sigma(1) = 1$. Also, when counting possibilities for $\sigma(3)$, it does not matter which of the 5 vertices we choose for $\sigma(2)$, so let's assume that $\sigma(2) = 2$ (again without any loss of generality). But if σ fixes the vertices 1 and 2, then the axis of rotation for σ passes through the edge $\{1, 2\}$. However, the only rotation fixing an edge of the icosahedron is the identity, meaning that the only choice for $\sigma(3) = 3$ and in fact that $\sigma(k) = k$ for all $k \geq 3$.

In summary, there are 12 possibilities for $\sigma(1)$, from which 5 possibilities remain for $\sigma(2)$, and then only one choice remains for each $\sigma(k)$ with $k \geq 3$. Thus, $|\text{Icosa}^+| = 60$.

In Example 6, we encountered the need to discuss all possible vertices to which Icosa^+ can take vertex 1. This is an important concept for all permutation groups, and so we give it a name: the *orbit* of 1 under Icosa^+. We also had need to consider all symmetries in

Icosa$^+$ that fixed the vertex 1. This is an equally important concept that we also name: the *stabilizer* of 1 in Icosa$^+$. Here are the proper definitions.

Definition 2.1. Let G act on X, and let $y \in X$.

- The **orbit of** y **under** G is defined by $\mathrm{Orb}_G(y) = \{x \in X \mid x = g \cdot y \text{ for some } g \in G\}$.
- The **stabilizer of** y **in** G is defined by $G_y = \{g \in G \mid g \cdot y = y\}$.

When considering stabilizers of stabilizers, we use notation G_{y_1,y_2} in place of $(G_{y_1})_{y_2}$.

Example 7. Let's revisit Example 6 and record our findings using the language of orbits and stabilizers. Set $G = \text{Icosa}^+$.

We first found that $\mathrm{Orb}_G(1) = \{1, 2, \ldots, 12\}$. In fact, no matter which vertex k we choose, $\mathrm{Orb}_G(k) = \{1, 2, \ldots, 12\}$. Thus, G has only one orbit on the vertices, consisting of them all.

Next, instead of studying orbits with respect to G, we changed to considering the stabilizer G_1. Here we found that $\mathrm{Orb}_{G_1}(2) = \{2, 3, 4, 5, 6\}$. We could also ask where G_1 could take vertices other than 2. Since G_1 fixes 1, $\mathrm{Orb}_{G_1}(1) = \{1\}$. As G_1 also fixes the antipodal vertex 7, $\mathrm{Orb}_{G_1}(7) = \{7\}$. There are various other vertices to consider, and, for example, $\mathrm{Orb}_{G_1}(8) = \{8, 9, 10, 11, 12\}$. Here is the complete list of orbits of G_1:

$$\{1\}, \{7\}, \{2, 3, 4, 5, 6\}, \{8, 9, 10, 11, 12\}.$$

Finally, we considered the stabilizer $G_{1,2}$. This time we found that $G_{1,2}$ must fix every vertex, so for each vertex k, $\mathrm{Orb}_{G_{1,2}}(k) = \{k\}$.

On thing to notice in Example 7 is how the orbits of G_1 *partitioned* the set $\{1, 2, \ldots, 12\}$ (into non-overlapping pieces). Of course, the same is trivially true of the orbits of G since there was only one orbit. This observation about the orbits partitioning the set being acted upon is true in general.

Lemma. *Let G act on X. Then each $x \in X$ is contained in one and only one orbit of G.*

Proof. Each $x \in X$ is contained in the orbit $\mathrm{Orb}_G(x)$ since $x = \mathrm{id} \cdot x$ for id the identity permutation. Next, suppose some $z \in X$ is contained in both $\mathrm{Orb}_G(x)$ and $\mathrm{Orb}_G(y)$ for some $x, y \in X$. To prove the lemma, we want to show that this implies that the two orbits are actually the same, i.e. that $\mathrm{Orb}_G(x) = \mathrm{Orb}_G(y)$. Since $z \in \mathrm{Orb}_G(x) \cap \mathrm{Orb}_G(y)$, there exist $h_1, h_2 \in G$ such that $h_1 \cdot x = z = h_2 \cdot y$. Pictorially,

$$x \xrightarrow{h_1} z \xleftarrow{h_2} y.$$

Let's prove $\mathrm{Orb}_G(x) \subseteq \mathrm{Orb}_G(y)$. Choose $a \in \mathrm{Orb}_G(x)$. By definition of $\mathrm{Orb}_G(x)$, there exists $h_3 \in G$ such that $h_3 \cdot x = a$, so our picture becomes

$$a \xleftarrow{h_3} x \xrightarrow{h_1} z \xleftarrow{h_2} y.$$

To show $a \in \mathrm{Orb}_G(y)$, we need to find some $g \in G$ such that $g \cdot y = a$ (pictorially: $a \xleftarrow{g} y$). The key thing to remember is that G represents a permutation group, so G is closed under inverses and compositions. Thus, $h_1^{-1} \in G$, so also $h_3 h_1^{-1} h_2 \in G$. Let $g = h_3 h_1^{-1} h_2$. Then

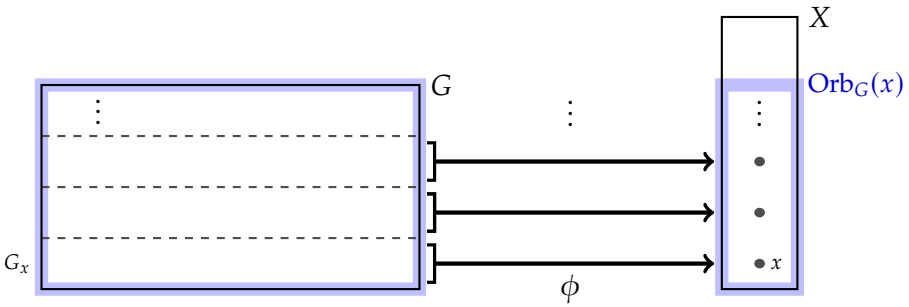
$$g \cdot y = h_3 h_1^{-1} h_2 \cdot y = h_3 h_1^{-1} \cdot z = h_3 \cdot x = a,$$

so $a \in \mathrm{Orb}_G(y)$. The proof that $\mathrm{Orb}_G(y) \subseteq \mathrm{Orb}_G(x)$ is similar. □

Returning to Example 6, note that not only did we consider orbits and stabilizers, but we also combined information about the two in order to count the size of the set being acted upon. The next theorem formalizes that process. In the statement of the theorem we use the notation $|A|$ to denote the cardinality (i.e. the "size") of the set A.

Theorem. *Let G act on X, and let $x \in X$. Then $|G| = |\mathrm{Orb}_G(x)| \cdot |G_x|$.*

Proof. We define a function $\phi : G \to \mathrm{Orb}_G(x)$ via $\phi(g) = g \cdot x$, so $g \cdot x = y \iff \phi(g) = y$. By definition of $\mathrm{Orb}_G(x)$, ϕ maps *onto* $\mathrm{Orb}_G(x)$, but ϕ is not likely one-to-one. For example, every element of G_x maps to x. Here is a picture.



For a given $g \in G$, let's count the number of $h \in G$ such that $\phi(g) = \phi(h)$. Notice that

$$\phi(g) = \phi(h) \iff g \cdot x = h \cdot x \iff x = g^{-1}h \cdot x \iff g^{-1}h \in G_x \iff h \in gG_x,$$

where we use the notation gG_x to denote the set $\{ga \mid a \in G_x\}$. So, counting the number of h such that $\phi(g) = \phi(h)$ is the same as determining the cardinality of gG_x. Now notice that for all $a, b \in G_x$,

$$ga = gb \iff a = g^{-1}gb \iff a = b,$$

which tells us that counting the number of $ga \in gG_x$ is the same as counting the number of $a \in G_x$. Thus, $|gG_x| = |G_x|$, and crucially, this does *not* depend on the choice of g. So each "fiber" in the picture above has the same size, which is $|G_x|$.

We conclude that for every $y \in \mathrm{Orb}_G(x)$, there are precisely $|G_x|$-many elements of G that map to y. Thus, $|G| = |\mathrm{Orb}_G(x)| \cdot |G_x|$. □

Example 8. Let's revisit Example 6 yet again. Set $G = \mathrm{Icosa}^+$.

The previous theorem says that $|G| = |\mathrm{Orb}_G(1)| \cdot |G_1|$. Since we know that $\mathrm{Orb}_G(1) = \{1, 2, \ldots, 12\}$, we get that $|G| = 12 \cdot |G_1|$.

We can now apply the same theorem to G_1 to get that $|G_1| = |\mathrm{Orb}_{G_1}(2)| \cdot |G_{1,2}|$, so as $\mathrm{Orb}_{G_1}(2) = \{2, 3, 4, 5, 6\}$, $|G_1| = 5 \cdot |G_{1,2}|$. Combining with what we've already learned, we get that $|G| = 12 \cdot 5 \cdot |G_{1,2}|$.

And finally, we also know that $G_{1,2}$ must fix every vertex, but the only element of G fixing all vertices is the identity. Thus, $G_{1,2} = \{\mathrm{id}\}$, so $|G_{1,2}| = 1$. Thus, $|G| = 12 \cdot 5 \cdot 1 = 60$.

3. Degrees of symmetry

Which would you say is "more symmetric": a regular tetrahedron or a cube? Why? A first thought may be that an object is more symmetric if it has more symmetries. With that point of view, a cube would be more symmetric than a tetrahedron since our work in Examples 1 and 5 implies that $|\textsc{Cube}| = 48 > 24 = |\textsc{Tetra}|$. However, this approach seems to privilege the cube simply because it has more vertices.

Let's work towards another approach to measuring symmetry. We saw that there is a symmetry taking any vertex of the tetrahedron to any other, and the same is true for a cube. But now, what if we ask about pairs of vertices. Notice that any two vertices of a tetrahedron can be simultaneously moved to any other two vertices. However, the same is *not* true for the cube: a pair of antipodal vertices can never be simultaneously moved to a pair of non-antipodal vertices. And this difference suggests that we might view the tetrahedron as being more symmetric than the cube. Let's formalize this idea.

Notation. For X a set, X^n denotes the set of all n-tuples with entries from X, and $X^{(n)}$ denotes the subset of X^n consisting of tuples with distinct entries, i.e.

$$X^{(n)} = \{(x_1, \ldots, x_n) \in X^n \mid x_i \neq x_j \text{ for all } i \neq j\}.$$

For example, $(1, 2, 3, 2) \notin \mathbb{Z}^{(4)}$ because of the repeated 2, but $(1, 2, 3, 7) \in \mathbb{Z}^{(4)}$ as there is no repetition in the coordinates.

Remark. If G acts on X, then G acts coordinatewise on both X^n and $X^{(n)}$ via the rule

$$g \cdot (x_1, \ldots, x_n) = (g \cdot x_1, \ldots, g \cdot x_n).$$

The main reason for looking at the action of G on X^n or $X^{(n)}$ is to study how a group element g *simultaneously* acts on $x_1, \ldots, x_n$ instead of simply studying how g acts on single elements of X. This better captures relationships between $x_1, \ldots, x_n$ (similar to how pairs of vertices on a cube might be antipodal or not).

Definition. We say that an action of G on X is **transitive** if G has only one orbit on X. More generally, we say the action is **k-transitive** if G has only one orbit on $X^{(k)}$ (with respect to the coordinatewise action).

Example 9. Let's revisit Examples 1 and 5 through the lens of k-transitivity.

The comment above that any two (distinct) vertices of a tetrahedron can be moved to any other two (distinct) vertices is stating that the action of Tetra on the vertices of the tetrahedron is 2-transitive. In fact, such pairs of vertices can be moved using a rotation, so Tetra$^+$ also acts 2-transitively on the vertices. And more is true: Tetra infact acts 4-transitively on the vertices.

As for the cube, Cube and Cube$^+$ act transitively on the vertices, but neither act 2-transitively. However, Cube$^+$ does act 4-transitively on the four diagonals of the cube.

Example 10. If $X = \{1, \ldots, n\}$, then it is fairly straightforward to verify that $\mathrm{Sym}(n)$ acts n-transitively on X, and it is ever so slightly less-straightforward to check that the action of $\mathrm{Alt}(n)$ is $(n-2)$-transitive but not $(n-1)$-transitive.

3.1. **Affine and projective linear groups.** Although we have seen some (and are about to see more) examples of **multiply transitive** actions (i.e. k-transitive actions for $k \geq 2$), it turns our that this is relatively rare, and it becomes even rarer to find k-transitive actions as k increases, which is to say that highly symmetric objects are rare.

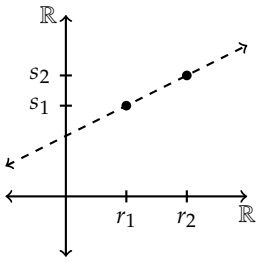
Example 11. Let's take a look at a particular group of permutations on $\mathbb{R}$. Specifically, we will consider the set of invertible (affine) linear functions:

$$\mathrm{AGL}_1(\mathbb{R}) = \left\{ f \in \mathrm{Sym}(\mathbb{R}) \mid f(x) = mx + b \text{ for some } m, b \in \mathbb{R} \text{ with } m \neq 0 \right\}.$$

It can be checked that $\mathrm{AGL}_1(\mathbb{R})$ satisfies the necessary closure axioms to be a permutation group on $\mathbb{R}$. Let's determine how transitive this action is.

Is the action transitive? Yes it is. For all $r, s \in \mathbb{R}$, the translation $f(x) = x + (s - r)$ is in $\mathrm{AGL}_1(\mathbb{R})$ and $f(r) = s$, so $\mathrm{AGL}_1(\mathbb{R})$ has a single orbit on $\mathbb{R}$.

What about 2-transitivity? Let's consider $(r_1, r_2), (s_1, s_2) \in \mathbb{R}^{(2)}$. We need to determine if there exists $f \in \mathrm{AGL}_1(\mathbb{R})$ such that $f(r_1, r_2) = (s_1, s_2)$, which would mean $f(r_1) = s_1$ and $f(r_2) = s_2$. If we graph the points (r_1, s_1) and (r_2, s_2) (remembering that $r_1 \neq r_2$ and $s_1 \neq s_2$ by definition of $\mathbb{R}^{(2)}$), we have something like the following:



The function representing the line connecting the two points will take r_1 to s_1 and r_2 to s_2, which is what we want, so the action is indeed 2-transitive.

Could it be 3-transitive? If it were, there would have to be some $f \in \mathrm{AGL}_1(\mathbb{R})$ such that $f(0, 1, 2) = (0, 1, 3)$, meaning that $f(0) = 0$, $f(1) = 1$, and $f(2) = 3$. Writing $f(x) = mx + b$, $f(0) = 0$ implies $b = 0$, and then $f(1) = 1$ implies $a = 1$. Thus f is the identity function $f(x) = x$, but then there is no way that $f(2) = 3$. So no, the action is not 3-transitive.

In Example 11, we considered the group of invertible linear functions from $\mathbb{R}$ to $\mathbb{R}$, but we used very little specific knowledge of $\mathbb{R}$. For example, we would have reached the same conclusion for invertible linear functions from $\mathbb{Q}$ to $\mathbb{Q}$. As such, we will define $\mathrm{AGL}_1(F)$ where F is any field; roughly, a **field** is a mathematical structure with "well-behaved" notions of addition and multiplication, as well as additive and multiplicative inverses. Examples of fields include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, but not $\mathbb{Z}$ because of the lack of multiplicative inverses for most elements. There are also examples of finite fields like $\mathbb{Z}_p$; here $\mathbb{Z}_p$ represents (congruence classes of) the integers with arithmetic performed modulo a prime number p.

Definition. For F a field, we define

$$\mathrm{AGL}_1(F) = \left\{ f \in \mathrm{Sym}(F) \mid f(x) = mx + b \text{ for some } m, b \in F \text{ with } m \neq 0 \right\}.$$

Remark. Essentially the same proof we gave in Example 11 shows that, for any field F, $\mathrm{AGL}_1(F)$ acts 2-transitively on F. Moreover, if $|F| \geq 4$, then the action is *not* 3-transitive.

The group $\mathrm{AGL}_1(F)$ can be generalized in (at least) a couple of ways. One way is to directly adapt the definition to give functions from the vector space F^n to itself by considering functions $f(x) = mx + b$ where m is an $n \times n$ matrix and b an n-vector.

Definition. For F a field, let $\mathrm{GL}_n(F)$ denote the set of all *invertible* $n \times n$ matrices with entries from F, and define

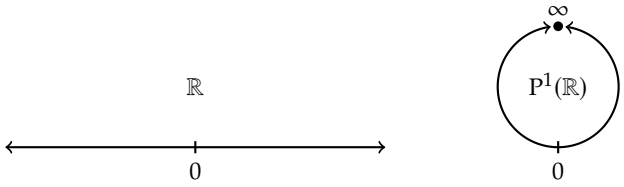
$$\mathrm{AGL}_n(F) = \left\{ f \in \mathrm{Sym}(F^n) \mid f(\bar{x}) = A\bar{x} + \bar{b} \text{ for some } A \in \mathrm{GL}_n(F) \text{ and some } \bar{b} \in F^n \right\}.$$

We refer to $\mathrm{AGL}_n(F)$ as the **affine general linear group** of degree n.

Remark. We won't explore $\mathrm{AGL}_n(F)$ much here, but it's worth mentioning that—just like $\mathrm{AGL}_1(F)$—each permutation group in this family (for all choices of n and F) acts 2-transitively on the vector space F^n, and provided $|F| \geq 4$, the action is not 3-transitive.

Let's now take a look at another way to generalize the construction of $\mathrm{AGL}_1(F)$. This time we will encounter a family of permutation groups that are typically 3-transitive but not 4-transitive.

Example 12. In Example 11, we looked at certain functions on the line $\mathbb{R}$; this time we will work with the projective line $\mathrm{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$. Right now, ∞ is just another symbol we are adding to the set $\mathbb{R}$, but we can think of $\mathrm{P}^1(\mathbb{R})$ as a circle where ∞ connects the positive and negative "ends" of the real line together.



We now define the so-called **factional linear transformations** of the projective line:

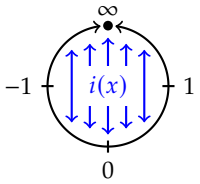
$$\mathrm{PGL}_2(\mathbb{R}) = \left\{ f \in \mathrm{Sym}(\mathrm{P}^1(\mathbb{R})) \mid f(x) = \frac{ax+b}{cx+d} \text{ for } a,b,c,d \in \mathbb{R} \text{ with } ad - bc \neq 0 \right\}.$$

In order for a function of the form $f(x) = \frac{ax+b}{cx+d}$ to be fully defined on $\mathrm{P}^1(\mathbb{R})$, we need to make sense of a couple values; set

$$f(-d/c) = \infty$$
$$f(\infty) = \begin{cases} \frac{a}{c} & \text{if } c \neq 0 \\ \infty & \text{if } c = 0. \end{cases}$$

The input $-d/c$ results in the denominator of $f(x)$ being 0, so $f(-d/c) = \infty$ can be thought of via the arithmetic $r/0 = \infty$ for each nonzero $r \in \mathbb{R}$. One way to make sense of $f(\infty)$ is to think of $\lim_{x\to\infty} f(x)$; this leads to $f(\infty) = a/c$, which is reasonably interpreted as ∞ in the case when $c = 0$.

Note that $\mathrm{AGL}_1(\mathbb{R}) \subset \mathrm{PGL}_2(\mathbb{R})$ by using $c = 0$ and $d = 1$ in the definition above. Moreover, every element of $\mathrm{AGL}_1(\mathbb{R})$ fixes ∞, and in fact, $\mathrm{AGL}_1(\mathbb{R})$ is equal to the stabilizer of ∞ in $\mathrm{PGL}_2(\mathbb{R})$. Also note that the "inversion" function $i(x) = \frac{1}{x} \in \mathrm{PGL}_2(\mathbb{R})$. If we scale the circle above so that -1 and 1 are the endpoints of the horizontal diameter, then the function $i(x)$ can be viewed as a reflection over that diameter (with $i(0) = \infty$ and $i(\infty) = 0$).



We now work to show that $\mathrm{PGL}_2(\mathbb{R})$ acts 3-transitively on $\mathrm{P}^1(\mathbb{R})$. Set $G = \mathrm{PGL}_2(\mathbb{R})$ and $X = \mathrm{P}^1(\mathbb{R})$.

Let's first prove that the action is transitive. We'll do this by showing that $r \in \mathrm{Orb}_G(\infty)$ for every $r \in X$ (implying that G has only on orbit on X). If $r = \infty$, then $r \in \mathrm{Orb}_G(\infty)$ since $\infty = \mathrm{id}(\infty)$ (where $\mathrm{id}(x) = x$). Suppose now that $r \neq \infty$; then $r \in \mathbb{R}$. Since $\mathrm{AGL}_1(\mathbb{R})$ is transitive on $\mathbb{R}$, there exists an $f \in \mathrm{AGL}_1(\mathbb{R}) \subset G$ such that $f(r) = 0$. And then, with $i(x)$

the inversion function defined above, we find that $i \circ f(r) = i(0) = \infty$, which shows that $r \in \mathrm{Orb}_G(\infty)$.

To show G acts 3-transitively, we will show that $(r_1, r_2, r_3) \in \mathrm{Orb}_G(0, 1, \infty)$ for every $(r_1, r_2, r_3) \in X^{(3)}$. Since we have shown G acts transitively on X, there exists $f \in G$ such that $f(r_3) = \infty$; thus $f(r_1, r_2, r_3) = (s_1, s_1, \infty)$ for some $s_1, s_2 \in X$. Because r_1, r_2, r_3 are all distinct and f is a one-to-one, s_1, s_2, ∞ are all distinct. In particular, $s_1, s_2 \in \mathbb{R}^{(2)}$, so by 2-transitivity of $\mathrm{AGL}_1(\mathbb{R})$, there exists $g \in \mathrm{AGL}_1(\mathbb{R})$ such that $g(s_1, s_2) = (0, 1)$. As mentioned before, the elements of $\mathrm{AGL}_1(\mathbb{R})$ fix ∞, so $g(\infty) = \infty$. Pictorially,

$$\begin{array}{ccccc} & f & & g & \\ r_1 & \to & s_1 & \to & 0 \\ r_2 & \to & s_2 & \to & 1 \\ r_3 & \to & \infty & \to & \infty \end{array}$$

Thus, $g \circ f(r_1, r_2, r_3) = (0, 1, \infty)$, so $(r_1, r_2, r_3) \in \mathrm{Orb}_G(0, 1, \infty)$ as desired.

Might the action be 4-transitive? If so, there would be an $f \in G$ such that $f(0, 1, \infty, 2) = (0, 1, \infty, 3)$. Since $f(\infty) = \infty$, we find that $f \in \mathrm{AGL}_1(\mathbb{R})$, so then (as we saw before) $f(0) = 0$ and $f(1) = 1$ imply that f is the identity function. But then there is no chance that $f(2) = 3$. So the action is not 4-transitive.

As with our exploration of $\mathrm{AGL}_1(\mathbb{R})$, our work with $\mathrm{PGL}_2(\mathbb{R})$ used very few specific properties of $\mathbb{R}$, and we are again able to define $\mathrm{PGL}_2(F)$ for F any field.

Definition. For F a field, we define $\mathrm{P}^1(F) = F \cup \{\infty\}$ and

$$\mathrm{PGL}_2(F) = \left\{ f \in \mathrm{Sym}(\mathrm{P}^1(F) \mid f(x) = \frac{ax + b}{cx + d} \text{ for } a, b, c, d \in F \text{ with } ad - bc \neq 0 \right\},$$

where

$$f(-d/c) = \infty \text{ and } f(\infty) = \begin{cases} \frac{a}{c} & \text{if } c \neq 0 \\ \infty & \text{if } c = 0. \end{cases}$$

Remark. Our work in Example 12 easily generalizes to show that, for any field F, $\mathrm{PGL}_2(F)$ acts 3-transitively on $\mathrm{P}^1(F)$; the action is *not* 4-transitive provided $|\mathrm{P}^1(F)| \geq 5$ (or equivalently, if $|F| \geq 4$).

To be continued. . .

References

[Ern21] Dana C. Ernst. An inquiry-based approach to abstract algebra. Available at https://github.com/dcernst/IBL-AbstractAlgebra, 2021.

Department of Mathematics and Statistics, California State University, Sacramento, Sacramento, CA 95819, USA

Email address: joshua.wiscons@csus.edu