

# Counting Colorings Cleverly

by Zev Chonoles

## How many ways are there to color a shape?

Of course, the answer depends on the number of colors we're allowed to use. More fundamentally, the answer depends on when we call two colorings "the same". We're usually interested in calling two colorings the same if we can rotate one to look like the other. For a complicated shape, it might be difficult to understand all of its possible rotations, and to classify the colorings which each rotation preserves.

Before we can tackle our problem, we need to understand rotation and symmetry.

## Groups and Symmetries

As is standard, I'll use capital letters for sets, e.g.  $X$ . The cardinality of a set  $X$  will be denoted  $|X|$ .

A **group** is a set  $G$  with a single operation  $\star$ , that is associative, has an identity, and has inverses. That is,

- For any  $g, h, k \in G$ ,  $(g \star h) \star k = g \star (h \star k)$ .
- There exists an  $e \in G$  such that  $e \star g = g \star e = g$  for all  $g \in G$ .
- For any  $g \in G$ , there exists an  $h \in G$  such that  $g \star h = h \star g = e$ .

Be aware that we sometimes omit the group operation in writing, so that  $gh$  would represent  $g \star h$ , for example.

Also note that we did not require that the operation of a group be commutative.

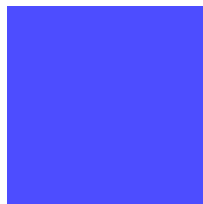
Are the integers  $\mathbb{Z}$  with  $+$  a group? Yes. What about  $\mathbb{Z}$  with  $\times$ ? No; many elements don't have inverses.

Groups show up everywhere in mathematics. Often, they are composed of functions instead of numbers. For example, given a "shape"  $A$ , we can define its **symmetry group** to be

$$\text{Sym}(A) = \{\text{reversible ways of mapping the shape to itself}\}.$$

If we were going to use fancier words, we might say that these maps are automorphisms of  $A$ .

As an example, let's consider a square  $S$ :



What are some of the elements of  $\text{Sym}(S)$ ?

- Translation in some direction? No, the square is ending up somewhere else.
- Rotation by  $45^\circ$ ? No, again the square is not being mapped to itself.
- Rotation by  $90^\circ$ ? Yes, this is in  $\text{Sym}(S)$ .
- Flipping it about its vertical axis? Yes, this is in  $\text{Sym}(S)$ .

Now, for any shape  $A$ , what is the operation on  $\text{Sym}(A)$ ? Composition of mappings. If  $f$  and  $g$  are in  $\text{Sym}(A)$ , then  $f \circ g$ , the mapping from  $A$  to itself defined by doing  $g$ , then doing  $f$ , is reversible because  $f$  and  $g$  are, and therefore  $f \circ g \in \text{Sym}(A)$ .

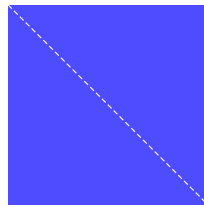
What is the identity for this operation? The identity function, i.e. the mapping that “does nothing”.

What is the inverse of an  $f \in \text{Sym}(A)$ ? The mapping that undoes  $f$ , which exists because we assumed that  $f$  was reversible.

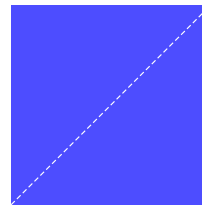
What are all of the elements of  $\text{Sym}(S)$ ?

$$\text{Sym}(S) = \{\text{id}, \text{rot}_{90}, \text{rot}_{180}, \text{rot}_{270}, \text{flip}_h, \text{flip}_v, \text{flip}_d, \text{flip}_s\}$$

where  $\text{flip}_d$  and  $\text{flip}_s$  refer to flipping about the *dexter* (right) and *sinister* (left) diagonals, respectively:



*dexter*



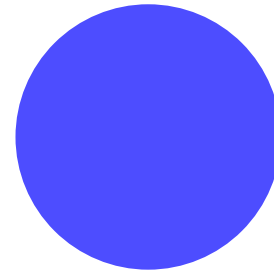
*sinister*

We usually refer to  $\text{Sym}(S)$ , the group of symmetries of a square, as  $D_8$ .

What about  $\text{Sym}(A)$  for the following shapes  $A$ :



(a)



(b)



(c)

(a)  $\text{Sym}(A) = \{\text{id}, \text{rot}_{180}, \text{flip}_h, \text{flip}_v\}$

(b)  $\text{Sym}(A) = \{\text{rot}_\theta \text{ for any } \theta \in [0, 360), \text{flip} \circ \text{rot}_\theta \text{ for any } \theta \in [0, 360)\}$

(c)  $\text{Sym}(A) = \{\text{id}\}$

As you can see, the more symmetries a shape has, the larger its symmetry group is.

## Group Actions

Let's generalize from groups rearranging shapes, to having groups rearrange arbitrary sets.

What exactly do we mean by this?

If  $G$  is a group and  $X$  is a set, then we say that  $\rho$  is an **action** of  $G$  on  $X$  when it is an assignment, to each  $g \in G$ , of a permutation  $\rho_g : X \rightarrow X$  (i.e. a bijective function from  $X$  to itself). This assignment must satisfy:

- The permutation corresponding to the identity element  $e \in G$  doesn't do anything. More precisely, we must have that  $\rho_e : X \rightarrow X$  is the identity function,  $\rho_e(x) = x$  for all  $x \in X$ .
- For any  $g, h \in G$ , the permutation corresponding to  $gh$  must equal the one obtained by applying the permutation corresponding to  $g$ , then applying the permutation corresponding to  $h$ . More precisely, for any  $g, h \in G$ , we must have  $\rho_{gh} = \rho_h \circ \rho_g$ .

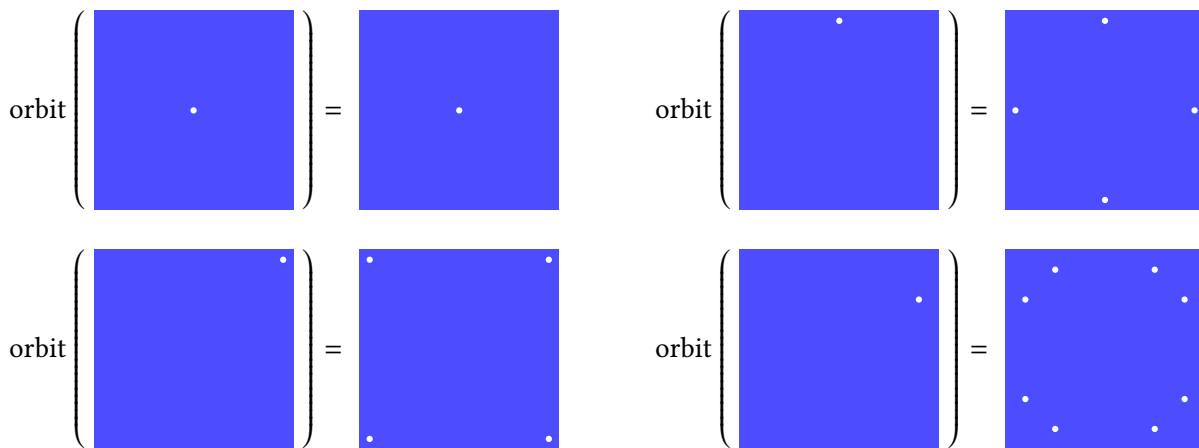
Note that we didn't require that distinct elements of  $G$  be assigned to distinct permutations of  $X$ . For any group  $G$  and any set  $X$ , we can assign the identity function of  $X$  to every  $g \in G$ , and this defines a perfectly valid action of  $G$  on  $X$ .

Recall our earlier example of  $D_8$ , the symmetry group of a square. We can define an action by letting  $G = D_8$  and  $X = \{\text{vertices of } S\}$ , and then for any  $g \in G$ , we let  $\rho_g$  be the permutation of  $X$  that sends a vertex of the square to wherever the symmetry  $g$  sends it. We could similarly consider actions of  $G$  on  $X = \{\text{edges of } S\}$ , or even  $X = \{\text{all points of } S\}$ .

Given an action  $\rho$  of a group  $G$  on a set  $X$ , we define the **orbit** of  $x \in X$  to be

$$\text{orbit}(x) = \{\text{elements of } X \text{ that } G \text{ can send } x \text{ to}\} = \{\rho_g(x) \mid g \in G\}.$$

For example, consider the action of the group  $G = D_8$  on the set  $X = \{\text{all points of } S\}$ . For four different choices of  $x$ , here is what  $\text{orbit}(x)$  looks like:



The following is a simple, but very important, theorem about orbits:

**Theorem.** Suppose we have an action  $\rho$  of a group  $G$  on a set  $X$ . For any  $x, y \in X$ , either  $\text{orbit}(x) = \text{orbit}(y)$ , or  $\text{orbit}(x)$  and  $\text{orbit}(y)$  are disjoint (i.e. they have no elements in common).

*Proof.* If  $\text{orbit}(x)$  and  $\text{orbit}(y)$  have no elements in common, then we are done, so suppose that  $z \in \text{orbit}(x)$  and  $z \in \text{orbit}(y)$  for some  $z \in X$ . Then by definition,

$$z \in \text{orbit}(x) = \{\rho_g(x) \mid g \in G\}, \quad z \in \text{orbit}(y) = \{\rho_g(y) \mid g \in G\},$$

so that there is some  $g \in G$  such that  $z = \rho_g(x)$ , and some  $h \in G$  such that  $z = \rho_h(y)$ . Then

$$\rho_{gh^{-1}}(x) = \rho_{h^{-1}}(\rho_g(x)) = \rho_{h^{-1}}(z) = \rho_{h^{-1}}(\rho_h(y)) = \rho_{hh^{-1}}(y) = \rho_e(y) = y,$$

so that  $y \in \text{orbit}(x)$ . By a similar argument,  $x \in \text{orbit}(y)$ .

Because we can “get to”  $y$  from  $x$ , any element of  $X$  we can get to from  $y$  we can also get to from  $x$ , so that  $\text{orbit}(y) \subseteq \text{orbit}(x)$ . To be precise, if  $w \in \text{orbit}(y)$ , then  $w = \rho_k(y)$  for some  $k \in G$ , and hence

$$w = \rho_k(y) = \rho_k(\rho_{gh^{-1}}(x)) = \rho_{gh^{-1}k}(x) \in \text{orbit}(x).$$

By a similar argument,  $\text{orbit}(x) \subseteq \text{orbit}(y)$ . Thus, we must have  $\text{orbit}(x) = \text{orbit}(y)$ . □

Given an action  $\rho$  of a group  $G$  on a set  $X$ , we define the **stabilizer** of  $x$  to be

$$\text{stab}(x) = \{\text{elements of } G \text{ that don't move } x\} = \{g \in G \mid \rho_g(x) = x\}.$$

Note that for any  $x \in X$ , the orbit of  $x$  is a subset of  $X$ , while the stabilizer of  $x$  is a subset of  $G$  (people seem to often get confused about this point).

When  $\rho_g(x) = x$  for some  $g \in G$  and  $x \in X$ , we usually say that  $g$  stabilizes  $x$ , or alternatively that  $g$  fixes  $x$ .

It should be clear to everyone that the identity element  $e \in G$  is in  $\text{stab}(x)$  for every  $x$ , because  $\rho_e : X \rightarrow X$  is the identity function of  $X$ .

Returning to our example of  $G = D_8$  acting on the set  $X = \{\text{all points of } S\}$ , note that

$$\begin{array}{cc} \text{stab} \left( \begin{array}{c} \text{blue square with dot in center} \end{array} \right) = \left\{ \text{id, rot}_{90}, \text{rot}_{180}, \text{rot}_{270}, \right. \\ \left. \text{flip}_h, \text{flip}_v, \text{flip}_d, \text{flip}_s \right\} & \text{stab} \left( \begin{array}{c} \text{blue square with dot at top center} \end{array} \right) = \{\text{id, flip}_v\} \\ \\ \text{stab} \left( \begin{array}{c} \text{blue square with dot at top right corner} \end{array} \right) = \{\text{id, flip}_s\} & \text{stab} \left( \begin{array}{c} \text{blue square with dot at bottom right corner} \end{array} \right) = \{\text{id}\} \end{array}$$

Hopefully, you are noticing a certain inverse relationship between orbits and stabilizers: specifically,

$$\begin{array}{l} \text{most } g \in G \text{ don't move } x \text{ (i.e., } \text{stab}(x) \text{ is big)} \iff x \text{ doesn't go many places (i.e., } \text{orbit}(x) \text{ is small)} \\ \text{most } g \in G \text{ do move } x \text{ (i.e., } \text{stab}(x) \text{ is small)} \iff x \text{ goes lots of places (i.e., } \text{orbit}(x) \text{ is big)} \end{array}$$

Intuitively, this is clear. In fact, in this example, in every case we had  $8 = |\text{orbit}(x)| \cdot |\text{stab}(x)|$ . This inverse relationship holds in general, and it is known as the

**Orbit-Stabilizer Theorem.** Suppose we have an action  $\rho$  of a group  $G$  on a set  $X$ . Then for any  $x \in X$ ,

$$|G| = |\text{orbit}(x)| \cdot |\text{stab}(x)|.$$

This is another immensely important theorem, but I'll put off the proof to the end so we can get right to applying it. Hopefully the example with the square  $S$  will suffice to convince you for now.

Our key result is

**Burnside's Lemma.** Suppose we have an action  $\rho$  of a finite group  $G$  on a finite set  $X$ . Then

$$\text{number of orbits of } \rho = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

where

$$\text{Fix}(g) = \{\text{elements of } X \text{ which } g \text{ doesn't move}\} = \{x \in X \mid \rho_g(x) = x\}.$$

To rephrase this statement,

$$\text{number of orbits of } \rho = \text{average number of elements fixed by a } g \in G.$$

*Proof of Burnside's Lemma.* Let  $n = |G|$  and  $m = |X|$ , and label the elements of  $G$  and the elements of  $X$  as  $g_1, g_2, \dots, g_n$  and  $x_1, \dots, x_m$  respectively. Expanding out the meaning of the sum,

$$\sum_{g \in G} |\text{Fix}(g)| = |\text{Fix}(g_1)| + \dots + |\text{Fix}(g_n)|.$$

Note that for any  $g_i$ ,

$$|\text{Fix}(g_i)| = \left| \{\text{solutions } (h, y) \text{ to } \rho_h(y) = y \text{ where } h = g_i\} \right|.$$

Because we are adding over every element of  $G$ , we end up counting every solution to  $\rho_h(y) = y$ :

$$\sum_{g \in G} |\text{Fix}(g)| = |\text{Fix}(g_1)| + \dots + |\text{Fix}(g_n)| = \left| \{\text{solutions } (h, y) \text{ to } \rho_h(y) = y\} \right|.$$

But we can now break this up according to the value of  $y$ :

$$\sum_{g \in G} |\text{Fix}(g)| = \left| \{\text{solutions } (h, y) \text{ to } \rho_h(y) = y \text{ where } y = x_1\} \right| + \dots + \left| \{\text{solutions } (h, y) \text{ to } \rho_h(y) = y \text{ where } y = x_m\} \right|$$

For any  $x_i \in X$ , we clearly have that

$$\left| \{\text{solutions } (h, y) \text{ to } \rho_h(y) = y \text{ where } y = x_i\} \right| = |\{h \in G \mid \rho_h(x_i) = x_i\}| = |\text{stab}(x_i)|,$$

so that

$$\sum_{g \in G} |\text{Fix}(g)| = |\text{stab}(x_1)| + \dots + |\text{stab}(x_m)| = \sum_{x \in X} |\text{stab}(x)|.$$

This is the critical step, so to really emphasize it, I'll explain it another way:

$$\begin{aligned} & \sum_{g \in G} |\text{Fix}(g)| = |\text{Fix}(g_1)| + \dots + |\text{Fix}(g_n)| \\ &= \left| \left\{ \begin{array}{c} \text{first element of } X \text{ which } g_1 \text{ doesn't move} \\ \vdots \\ \text{last element of } X \text{ which } g_1 \text{ doesn't move} \end{array} \right\} \right| + \dots + \left| \left\{ \begin{array}{c} \text{first element of } X \text{ which } g_n \text{ doesn't move} \\ \vdots \\ \text{last element of } X \text{ which } g_n \text{ doesn't move} \end{array} \right\} \right|. \end{aligned}$$

Thus, we list out the elements of  $X$  which are fixed by  $g_1$ , then those fixed by  $g_2$ , etc. How many times does a given  $x \in X$  appear altogether? The element  $x$  occurs one time for each  $g \in G$  which fixes  $x$ , so the element  $x$  is counted a total of  $|\text{stab}(x)|$  times. Therefore,

$$\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |\text{stab}(x)|.$$

Now applying the orbit-stabilizer theorem,

$$\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |\text{stab}(x)| = \sum_{x \in X} \frac{|G|}{|\text{orbit}(x)|} = |G| \sum_{x \in X} \frac{1}{|\text{orbit}(x)|}.$$

Every  $x \in X$  is an element of at least one orbit, because  $x \in \text{orbit}(x)$ , and by our earlier theorem, two orbits  $\text{orbit}(x)$  and  $\text{orbit}(y)$  are either identical or disjoint. Thus, we can group the elements of  $X$  by which orbit they are in; in fancier terms, the orbits form a partition of  $X$ . Labeling the different orbits  $\text{orbit}_1, \text{orbit}_2, \dots, \text{orbit}_k$ , we have that

$$\begin{aligned} \sum_{g \in G} |\text{Fix}(g)| &= |G| \sum_{x \in X} \frac{1}{|\text{orbit}(x)|} = |G| \left( \sum_{x \in \text{orbit}_1} \frac{1}{|\text{orbit}(x)|} + \dots + \sum_{x \in \text{orbit}_k} \frac{1}{|\text{orbit}(x)|} \right) \\ &= |G| \left( \sum_{x \in \text{orbit}_1} \frac{1}{|\text{orbit}_1|} + \dots + \sum_{x \in \text{orbit}_k} \frac{1}{|\text{orbit}_k|} \right) = |G| \left( \frac{|\text{orbit}_1|}{|\text{orbit}_1|} + \dots + \frac{|\text{orbit}_k|}{|\text{orbit}_k|} \right) \\ &= |G| \cdot \underbrace{(1 + \dots + 1)}_{\text{number of orbits of } \rho} = |G| \cdot (\text{number of orbits of } \rho) \end{aligned}$$

and therefore

$$\text{number of orbits of } \rho = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|. \quad \square$$

## Counting Colorings

Let's consider a cube  $C$ , and let  $G = \text{Sym}(C)$ . With the assistance of the orbit-stabilizer theorem, it is not hard to show that  $G$  has 24 elements.

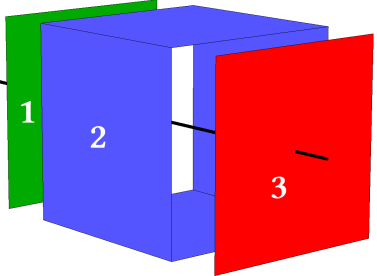
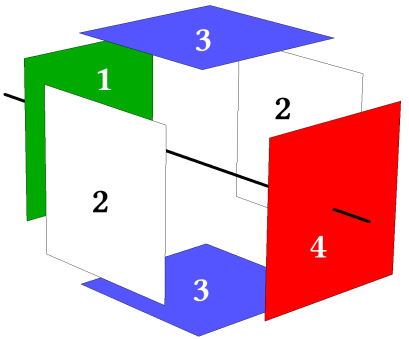
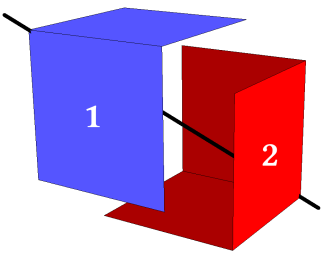
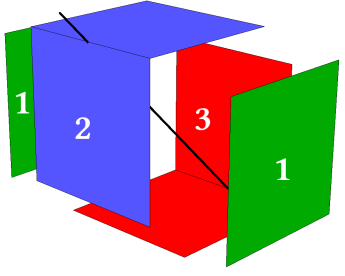
The set  $X = \{\text{all colorings of } C \text{ with } n \text{ colors}\}$  clearly has  $n^6$  elements in it, because a cube has 6 faces.

There is an action  $\rho$  of  $G$  on  $X$ , where  $\rho_g$  takes a coloring  $x$  and sends it to the coloring produced by applying the symmetry  $g$  to the colored cube  $x$ . Now, some colorings will be fixed by some symmetries; for example, a coloring that uses the same color on every face will be fixed by every  $g \in G$ . By considering how each symmetry moves the cube, we can figure out exactly how many colorings are fixed by each element of  $G$ . In other words, we can calculate  $|\text{Fix}(g)|$  for every  $g \in G$ .

Two elements of  $X$  are in the same orbit of  $\rho$  precisely when one can be rotated to look like the other, so an orbit represents a class of colorings that are the same up to rotation. Applying Burnside's lemma, our knowledge of  $|\text{Fix}(g)|$  for every  $g \in G$  will let us determine the number of orbits of  $\rho$ , i.e. the number of colorings of the cube, when considered up to rotations.

As an example of the kind of reasoning we use, note that there are 6 distinct  $90^\circ$  face rotations - we can rotate any of the 6 faces  $90^\circ$  clockwise (and rotating a face  $90^\circ$  counterclockwise is the same as rotating the opposite face  $90^\circ$  clockwise, so we aren't missing any).

Suppose, for example, that we are rotating the right face  $90^\circ$  clockwise. Then the right face is sent to itself, as is the left face, but the top, back, bottom, and front are permuted amongst each other. In order for a coloring  $x \in X$  to be fixed by this element of  $G$ , the colors of the right and left faces can be chosen independently, but we must choose the same color for the top, back, bottom, and front. Thus, there are  $n \cdot n \cdot n = n^3$  colorings that are fixed by this element of  $G$ .

Type of rotation	Number of such rotations	Number of colorings fixed by such rotations	Picture
identity	1	$n^6$	
90° face rotations	6	$n^3$	
180° face rotations	3	$n^4$	
120° vertex rotations	8	$n^2$	
180° edge rotations	6	$n^3$	

This implies that

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| = \frac{1}{24} (n^6 + 6n^3 + 3n^4 + 8n^2 + 6n^3) = \frac{n^6}{24} + \frac{n^4}{8} + \frac{n^3}{2} + \frac{n^2}{3}$$

is the number of orbits of the action of  $G = \text{Sym}(C)$  on the set  $X = \{\text{all colorings of } C \text{ with } n \text{ colors}\}$ . Therefore, this is the number of colorings of a cube  $C$  with  $n$  colors, up to rotation.

As an illustration of just how many colorings are really equivalent up to rotation:

Number of colors $n$	Number of colorings of a cube, up to rotation $\frac{n^6}{24} + \frac{n^4}{8} + \frac{n^3}{2} + \frac{n^2}{3}$	Number of colorings of a cube $n^6$
1	1	1
2	10	64
3	57	729
4	240	4096
5	800	15625
6	2226	46656

Incidentally, the same kind of reasoning about a dodecahedron will show that the number of colorings of a dodecahedron using  $n$  colors, up to rotation, is

$$\frac{n^{12}}{60} + \frac{n^6}{4} + \frac{11n^4}{15}.$$

## Proof of the Orbit-Stabilizer Theorem

For the sake of completeness, here is a full proof of the orbit-stabilizer theorem.

**Orbit-Stabilizer Theorem.** Suppose we have an action  $\rho$  of a group  $G$  on a set  $X$ . Then for any  $x \in X$ ,

$$|G| = |\text{orbit}(x)| \cdot |\text{stab}(x)|.$$

*Proof.* For any  $y \in \text{orbit}(x)$ , we define

$$\text{move}(x, y) = \{\text{elements of } G \text{ that move } x \text{ to } y\} = \{g \in G \mid \rho_g(x) = y\}.$$

Because  $y \in \text{orbit}(x)$ , we know that  $\text{move}(x, y)$  is non-empty; at least one  $g \in G$  moves  $x$  to  $y$ .

If  $h \in \text{move}(x, y)$  for some  $y \in \text{orbit}(x)$ , then for any  $g \in \text{stab}(x)$ , we clearly have that  $gh \in \text{move}(x, y)$ , because

$$\rho_{gh}(x) = \rho_h(\rho_g(x)) = \rho_h(x) = y.$$

Thus, for any  $y \in \text{orbit}(x)$  and  $h \in \text{move}(x, y)$ , we can define a function  $\phi : \text{stab}(x) \rightarrow \text{move}(x, y)$  by  $\phi(g) = gh$ . If we then define  $\psi : \text{move}(x, y) \rightarrow \text{stab}(x)$  by  $\psi(g) = gh^{-1}$ , it is clear that  $\phi$  and  $\psi$  are inverses, because

$$\phi(\psi(g)) = \phi(gh^{-1}) = (gh^{-1})h = g(h^{-1}h) = ge = g,$$

$$\psi(\phi(g)) = \psi(gh) = (gh)h^{-1} = g(hh^{-1}) = ge = g.$$

Therefore  $\phi$  is a bijection. Because there is a bijection between  $\text{stab}(x)$  and  $\text{move}(x, y)$  for any  $y \in \text{orbit}(x)$ , we can conclude that for any  $y \in \text{orbit}(x)$ ,

$$|\text{stab}(x)| = |\text{move}(x, y)|.$$



Each  $g \in G$  is in at least one set  $\text{move}(x, y)$ , because each  $g \in G$  moves  $x$  to some  $y \in \text{orbit}(x)$ , namely  $y = \rho_g(x)$ .

For two distinct  $y, z \in \text{orbit}(x)$ , the sets  $\text{move}(x, y)$  and  $\text{move}(x, z)$  are disjoint, i.e. they have no elements in common; this is clear because any  $g \in G$  cannot both move  $x$  to  $y$ , and *also* move  $x$  to  $z$ .

Thus, we can group the elements of  $G$  according to which  $y \in \text{orbit}(x)$  they send  $x$  to; in fancier terms, the sets  $\text{move}(x, y)$  form a partition of  $G$ . Therefore,

$$|G| = \sum_{y \in \text{orbit}(x)} |\text{move}(x, y)| = \sum_{y \in \text{orbit}(x)} |\text{stab}(x)| = |\text{orbit}(x)| \cdot |\text{stab}(x)|.$$

□