# Counting Symmetries with Group Actions

Anlong Chua
canlong@mit.edu

Chase Vogeli
cpvogeli@mit.edu

November 2019

**Abstract**

How many ways can you arrange colored beads on a necklace? We'll attack this problem and similar problems using group theory, which is the mathematical language that describes the concept of symmetry. Specifically, we introduce Burnside's Lemma, a tool that lets us count configurations of geometric figures that are preserved under symmetry.

## 1 What is a group?

Groups often arise in nature as the set of symmetries of various objects. Consider for example a regular pentagon:

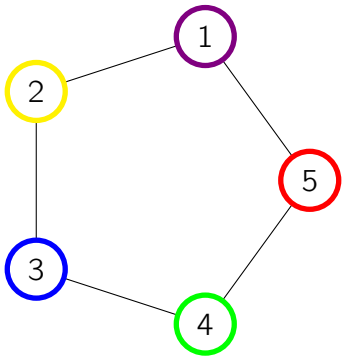



Figure 1: A regular pentagon.

What are some symmetries of this pentagon? For example, one can rotate the pentagon counter-clockwise by 72°.

In the same way, rotation of the pentagon by any multiple of 72° is a symmetry. Another type of symmetry is reflection.

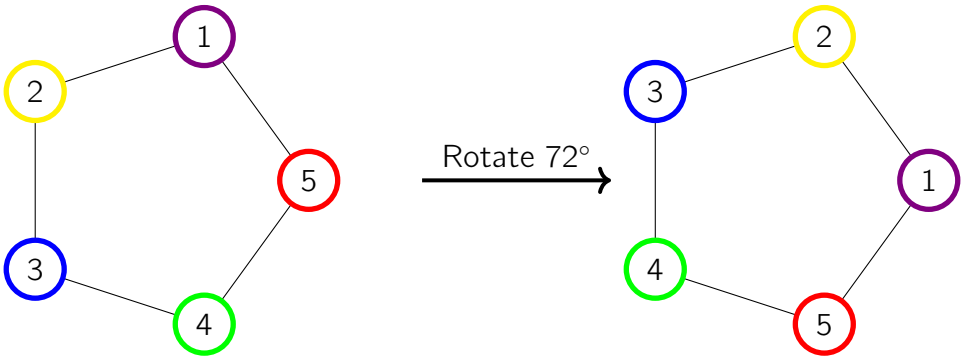



Figure 2: Counterclockwise rotation by 72°.

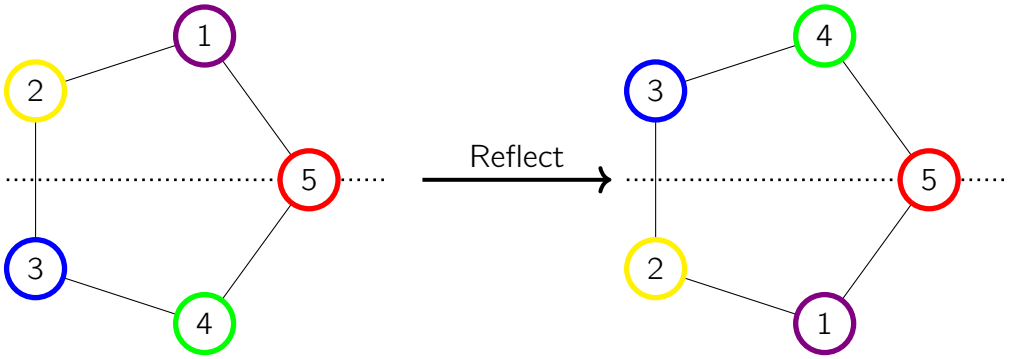



Figure 3: Reflection about an axis of symmetry.

Above, we reflected across the perpendicular line containing the vertex (5) (red), but we could just as well have reflected across the perpendicular line containing any other corner. In this way, we have described 10 different symmetries of the pentagon: 5 rotations, and 5 reflections. This set of symmetries is known as the *dihedral group*, often denoted $D_5$.

What is special about this set of symmetries? For one, the composition of any two symmetries is another symmetry. For example rotation followed by reflection across the dotted line is the same as reflection across the dotted line.

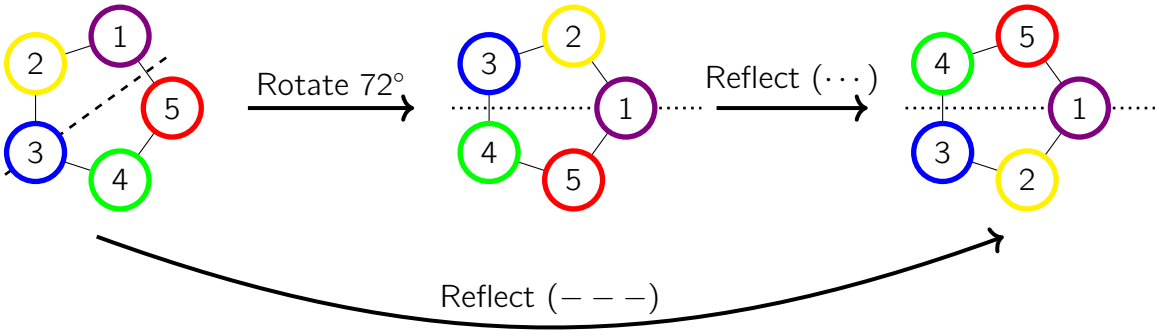



Figure 4: A composition of symmetries is a symmetry.

Another important property is the existence of an *identity*. For us, this is the rotation by 0°: this operation leaves the pentagon unchanged. The final important property is the existence of *inverses*: for any symmetry, there exists another symmetry that "undoes" the first. For example, rotation counterclockwise by 72°, which is equivalent to rotation clockwise by 288°, undoes rotation clockwise by 72°. Together, these properties are the defining axioms of a group.

We'll state the formal definition of a group for completeness only - feel free to ignore it, as we won't need it for the rest of the class!

**Definition 1.1**

A **group** is a set $G$ together with an associative binary operation $\cdot : G \times G \to G$ that has an identity and inverses.

Don't be alarmed by the technical-looking definition! When faced with an abstract algebraic structure, think of a concrete example to help unwind the definition. In our case, $G = D_5$ and the binary operation is simply composition of symmetries.

# 2 Groups act on objects

In practice, mathematicians study groups by studying their *actions* on other objects. A group action on a collection of objects essentially assigns, for each element of the group, a transformation of each object into another object in the collection.

In our case, the group $D_5$ comes with a natural action on the regular pentagon. To be precise, it acts on the set of vertices of the pentagon. For example, the "rotate by 72° element" sends vertex (1) (violet) to vertex (2) (yellow) and so on (see Fig. 2). If we do not distinguish the vertices, this action is pretty boring - nothing really distinguishes the collection of vertices we started out with from the set we ended up with. However, things get more interesting if we are allowed to label vertices of the pentagon.

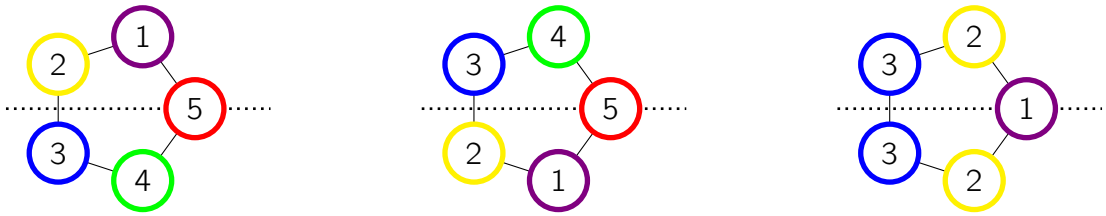



Figure 5: Examples of labelings of vertices of the pentagon.

To be precise, $D_5$ takes labeled pentagons to other labeled pentagons. This action is interesting because a given element of $D_5$ might not transform two different labeled pentagons in the same

way. For example, in Fig. 5, reflection across the dotted line transforms the first two pentagons into each other, while it keeps the third unchanged. The third labeled pentagon is known as a "fixed point" of the action.

**Definition 2.1**

Let $G$ be a group acting on some collection of objects. Let $g \in G$. A fixed point of $g$ is an object that $g$ leaves unchanged.

Notice that the property of being a fixed point depends not just on the object, but on the group element. For example, notice that while the third pentagon in Fig. 5 is fixed by the reflection, it is not fixed by any rotation.

Given a labeled pentagon, how many different labeled pentagons can one obtain by applying the $D_5$ action? Interestingly, this number also depends on the labeling under consideration.

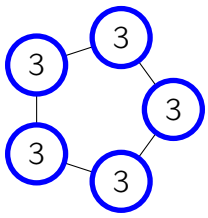



Figure 6: This labeled pentagon has only 1 element in its orbit.

For example, no matter how one might rotate or reflect the pentagon in Fig. 6, it is impossible to obtain a different labeling. On the other hand, the following labelings can be obtained by reflecting and rotating the third labeled pentagon in Fig. 5:

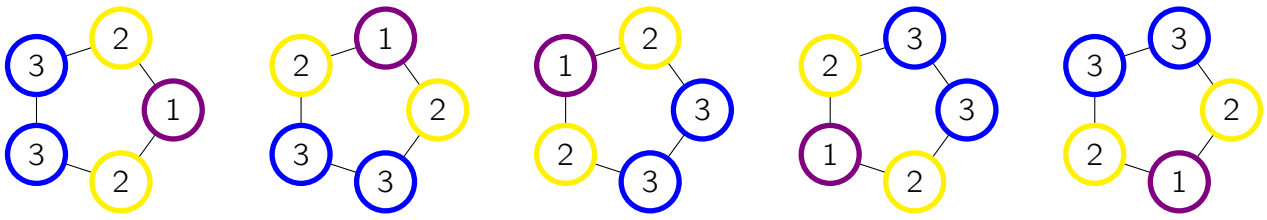



Figure 7: An orbit.

**Definition 2.2**

The **orbit** of an object under a group action is the set of elements obtained by applying various elements of the group.

**Note 2.3**

An important observation is that orbits *partition* the collection of objects being acted on. By this, we mean that every object is in **exactly one** orbit. For completeness, we include a proof of this statement.

*Proof.* If $x, y, z$ are objects, with $y$ and $z$ sharing an orbit with $x$, by definition, there exist group elements $g_1, g_2$ such that $g_1 x = y$ and $g_2 x = z$. Then $g_2 g_1^{-1} y = z$, showing that $y$ and $z$ share the same orbit. □

## 2.1 Burnside's Lemma

Given Note 2.3, it makes sense to speak of the number of partitions formed by the orbits of objects within the collection. Often, this number has a combinatorial interpretation; we shall see an example of this in Section 3. Burnside's Lemma is a tool that allows us to (relatively) easily compute this number.

**Lemma 2.4** (Burnside)

Let $G$ be a group acting on a collection of objects, and let $|G|$ denote the size of the group. Then

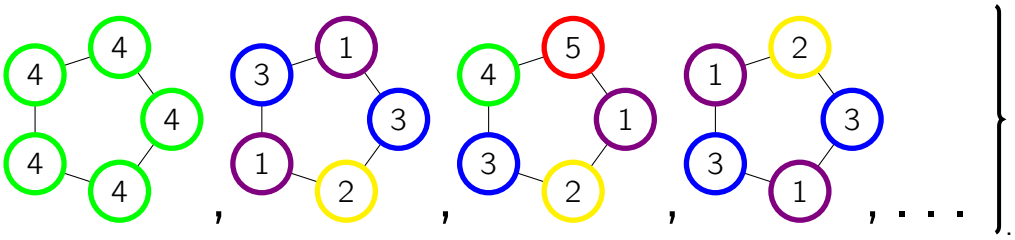
$$\#\text{ orbits} = \frac{1}{|G|} \sum_{g \in G} \#\text{ fixed points of } g.$$

Burnside's lemma says that the number of orbits is equal to the average number of fixed points each element of the group has. In our case, $|D_5| = 10$. A proof of Burnside's Lemma is included for completeness in Section 6.

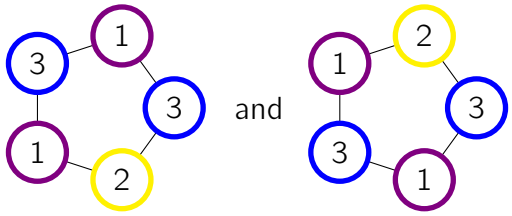
# 3 Counting necklaces with Burnside's Lemma

We turn to the problem of counting necklaces. Suppose you have $n$ different colors of beads at your disposal and you want to make a necklace with five beads. It's possible to work through this with any number of beads, but we'll focus on the case of five beads right now.

It's not immediately clear how to attack this problem, so let's start with something that we can easily count: how many necklaces are there, taking into account the orientation of necklaces. Let $S$ be the set of all such necklaces. The set $S$ then looks like

$S =$ 


It's straightforward to see that $S$ has $n^5$ many elements, but this isn't a satisfactory answer. To see why, the necklaces




are distinct elements of $S$, but you probably wouldn't call these necklaces distinct in real life! Indeed, you can rotate necklaces and turn necklaces over in real life, so this needs to be reflected in our counting. We need a notion of "sameness" of elements of $S$.

This is where group actions come into play! The key idea is that we instead of counting labeled pentagons, we need to be counting the orbits of labeled pentagons under the action of the group $D_5$. Indeed, each necklace corresponds to an orbit of labeled pentagons, which contains all of the various orientations of said necklace. As discussed in the last section, our tool for counting orbits is Burnside's lemma, Lemma 2.4.

Following Burnside's lemma, to compute the number of orbits, we need to compute the average number of fixed points of the elements of the group $D_5$. We'll compute the number of fixed points for each element in $D_5$, and then take the average. We treat the three types of elements in $D_5$—the identity, the rotations, and the reflections—separately.

**The identity symmetry** This is the easiest case. It is not hard to convince yourself that the identity element of $D_5$ fixes *every* labeled pentagon in $S$. Therefore, the number of fixed points is the size of $S$, which we saw to be $n^5$.

**The rotations** We next turn to the symmetries of $D_5$ which are given by rotations. The non-trivial rotations are the rotations by 72°, 144°, 216°, and 288°. We don't consider rotation by 360°, because this is actually the identity symmetry!

Suppose that a labeled pentagon is fixed by a rotation. Let's specifically consider the case of a clockwise 72° rotation, as depicted in Fig. 8. Then, color $a$ is the same as color $b$, color $b$ is the

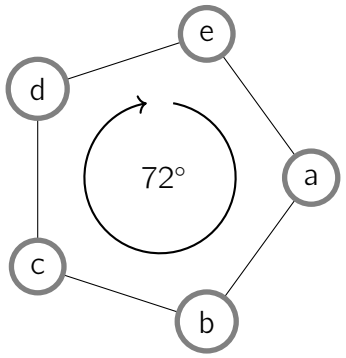



Figure 8: A 72° rotation.

same as color $c$, color $c$ is the same as color $d$, color $d$ is the same as $e$, and color $e$ is the same as color $a$. Thus, this necklace consists of beads of the same color! The idea is the same for the other angles. Since there are $n$ colors of beads at our disposal, there are $n$ necklaces that are fixed by a rotation.

**Note 3.1**

For necklaces with 5 beads, it is the case that the fixed points of a rotation must have all beads of the same color. This isn't the case for every length of necklace, though! For instance, is this the case for necklaces with 6 beads? Can you figure out for what type of number $n$, it is the case that fixed points of rotations of necklaces with $n$ beads must have all beads the same color?

**The reflections** Lastly, we consider the reflections in $D_5$. There are five reflections, one going through each vertex of the pentagon. Suppose that a labeled pentagon is fixed by a reflection. Then, the vertex which the axis lies on can be any color, and the remaining four vertices split into two pairs which must be the same color, as shown in the figure below.

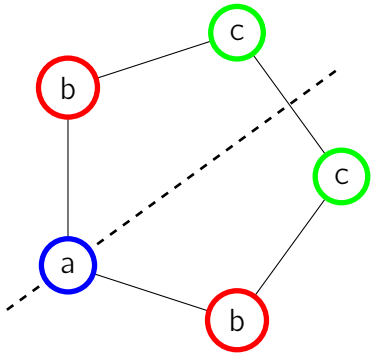



Figure 9: A fixed point of a reflection.

We see that a fixed point of a reflection is determined by the three colors: the color of the vertex

lying on the axis of reflection and the colors of the two other pairs of vertices. Thus, a reflection fixes $n^3$ labeled polygons.

**Note 3.2**

That the fixed points of reflections are determined by 3 colors also doesn't hold for necklaces of any length. Can you find a relationship between the number of beads $n$ and the number of fixed points of a reflection?

At this point, we've found the number of fixed points of each element in $D_5$! To summarize: there is one identity transformation fixing $n^5$ labeled pentagons, 4 rotations fixing $n$ labeled pentagons, and 5 reflections fixing $n^3$ labeled pentagons. If we plug this information into Burnside's lemma, Lemma 2.4, we have proved the following:

**Theorem 3.3** (Orbits of $D_5$ on labeled pentagons)

The number of orbits of the action of $D_5$ on the set $S$ of all labeled pentagons is

$$\#\text{ orbits} = \frac{n^5 + 4n + 5n^3}{10}$$

This is the result we were looking for! It tells us how many orbits, and thus, how many different necklaces there are under symmetry. Let's take our new formula for a test drive, and make sure that it makes sense by computing some simple cases.

Suppose that we only have one color of bead, so $n = 1$. Using Theorem 3.3, we see that there are

$$\frac{1^5 + 4 \cdot 1 + 5 \cdot 1^3}{10} = \frac{10}{10} = 1$$

possible necklaces. This lines up with what we would expect!

Let's move on to a slightly less trivial case, but one small enough where we can still write it out explicitly. Suppose we have two colors of beads, so $n = 2$. Using Theorem 3.3, we see that there are

$$\frac{2^5 + 4 \cdot 2 + 5 \cdot 2^3}{10} = \frac{32 + 8 + 40}{10} = \frac{80}{10} = 8$$

possible necklaces. It's not too difficult to draw all 8 necklaces; we do so in Fig. 10.

# 4 Fermat's Little Theorem

A slight modification of our counting technique from Section 3 allows us to prove Fermat's Little Theorem, which is a fundamental result in number theory. For example, it is an important building

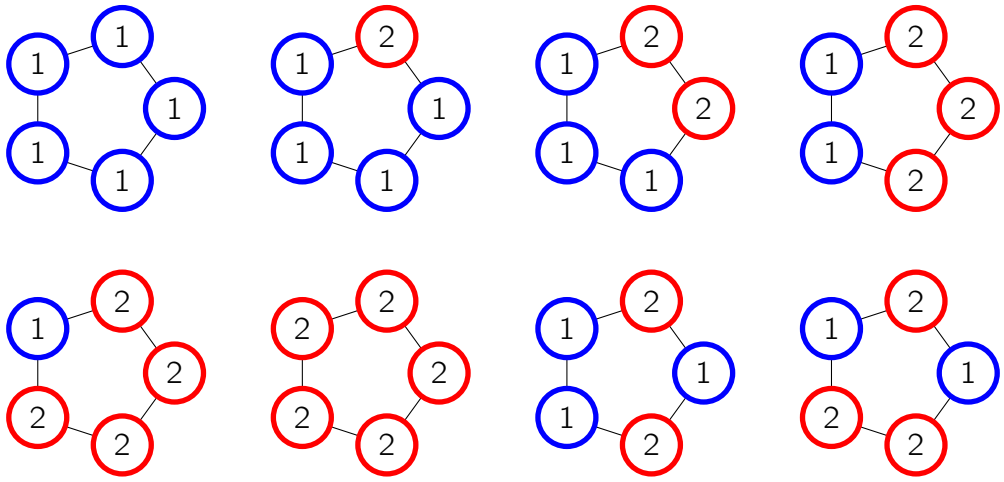



Figure 10: The 8 necklaces which possible to make with 5 beads with 2 colors.

block of the Miller-Rabin primality test.

**Theorem 4.1** (Fermat's Little Theorem)
Let $p$ be a prime number, and $n$ a positive integer. Then $n^p - n$ is an integer multiple of $p$.

Recall our set-up: we had a necklace of 5 beads, each of which could take on $n$ different colors. In addition, we had the group $D_5$ which acts by reflections and rotations. We'll make two modifications in our proof: first, we will consider necklaces with $p$ beads, and we will consider only the group of *rotations* of this necklace. Notice that in the case $p = 5$, our rotations were by multiples of $360°/5 = 72°$, so now our rotations will be in multiples of $360°/p$ - in other words, we now consider $p$ different rotations.

To apply Lemma 2.4, we need to calculate the number of fixed necklaces for each rotation. Notice that the rotation by $0°$ fixes everything; this element has $n^p$ fixed necklaces. On the other hand, all other rotations fix only necklaces where all beads have the same color

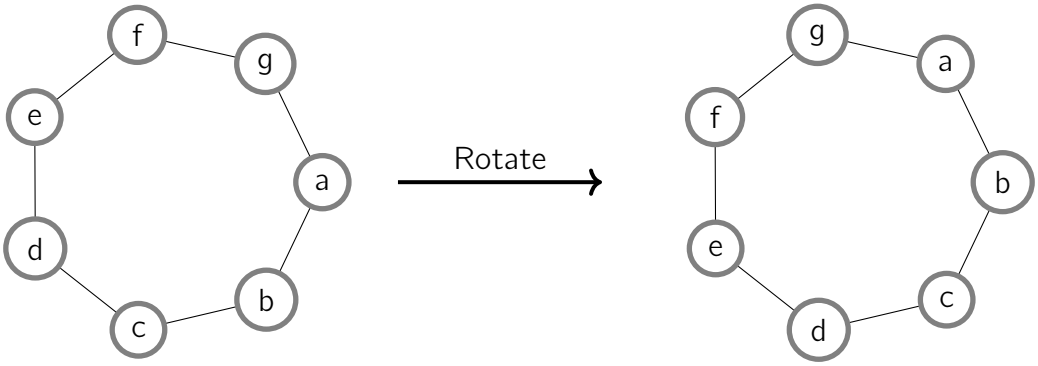



Figure 11: If this necklace were fixed by the rotation, then we must have $a = b$ and $b = c$ and ...

**Note 4.2**

As a thought experiment, think about why the statement above may not hold when $p$ is not prime! (This is related to Note 3.1.)

Therefore, Lemma 2.4 tells us that

$$\#\text{ orbits} = \frac{1}{|G|}\sum_{g\in G}\#\text{ fixed points of } g = \frac{1}{p}(n^p + (p-1)n).$$

Now, the trick is to notice that the number of orbits is an *integer*! This means that $n^p + (p-1)n$ is an integer multiple of $p$. Since $np$ is an integer multiple of $p$, this means that $n^p - n$ must also be an integer multiple of $p$!

# 5 What's next?

We hope that you've enjoyed learning about groups! If you want to learn more, *Visual Group Theory* by Nathan Carter is an accessible starting point. It contains many illustrations and is useful for building intuition. Another good first introduction to group theory is found in *A Book of Abstract Algebra* by Charles Pinter. The standard undergraduate-level text for group theory is the excellent *Algebra* by Michael Artin, which is a comprehensive and more theoretical treatment of the material.

# 6 A proof of Burnside's Lemma

Recall the statement of Burnside's Lemma:

**Lemma 6.1** (Burnside)

Let $G$ be a group acting on a collection of objects, and let $|G|$ denote the size of the group. Then

$$\#\text{ orbits} = \frac{1}{|G|}\sum_{g\in G}\#\text{ fixed points of } g.$$

Before proving the lemma, we need a preliminary result.

**Proposition 6.2**

Let $G$ be a finite group acting on a set $S$. For any $s \in S$, let $O(s)$ be the orbit of $s$. Let $\mathbf{1}\{T\}$ be the function that is equal to 1 if the statement $T$ is true, and 0 if $T$ is false. Then

$$\sum_{g \in G} \mathbf{1}\{g \cdot s = s\} = \frac{|G|}{|O(s)|}$$

*Proof.* Let $F(s) = \{g \in G \mid g \cdot s = s\}$. Then $|F(s)| = \sum_{g \in G} \mathbf{1}\{g \cdot s = s\}$. Let $s' \in O(s)$. By definition, there is some $h \in G$ such that $h \cdot s = s'$. For any $g \in F(s)$, we also have

$$h \cdot g \cdot s = h \cdot s = s'.$$

Conversely, if $h'$ is another group element such that $h' \cdot s = s'$, then $h^{-1}h' \cdot s = h^{-1}s' = s$ so $h^{-1}h' \in F(s)$. As such, for every $s' \in O(s)$, there are exactly $|F(s)|$ many elements in $|G|$ that take $s$ to $s'$. Since every element of $G$ takes $s$ to some other $s' \in O(s)$, it follows that $|F(s)| = \frac{|G|}{|O(s)|}$. □

*Proof of Burnside's Lemma (6.1).* Let $G$ be a finite group acting on a set $S$. Then

$$\begin{aligned}
\frac{1}{|G|} \sum_{g \in G} \#\text{ fixed points of } g &= \frac{1}{|G|} \sum_{g \in G} \sum_{s \in S} \mathbf{1}\{g \cdot s = s\} \\
&= \frac{1}{|G|} \sum_{s \in S} \sum_{g \in G} \mathbf{1}\{g \cdot s = s\} \\
&= \frac{1}{|G|} \sum_{s \in S} \frac{|G|}{|O(s)|}, \text{ by Proposition 6.2} \\
&= \sum_{s \in S} \frac{1}{|O(s)|} \\
&= \#\text{ orbits.}
\end{aligned}$$

□