

A Glimpse at Algebraic Combinatorics

Travis McVoy

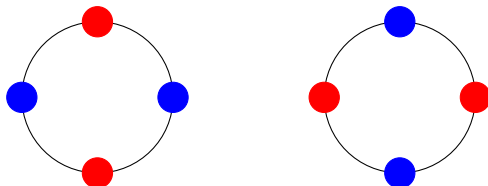
May 13, 2023

Contents

1	Background and Motivation	2
1.1	The Dihedral Group	2
1.2	Group Actions and Homomorphisms	4
1.3	Cosets and Lagrange's Theorem	9
1.4	Orbits	10
2	Counting Necklaces and Bracelets	12
2.1	Stabilizers	12
2.2	Orbit Theorems	13
3	Concluding Remarks	14
	References	16

1 Background and Motivation

Our goal in this paper is to count **combinatorial necklaces** and **bracelets**. We can think of a necklace as a circular collection of beads in which there are n beads and k possible colors the beads could be. We consider two necklaces to be the same if, via rotation, we can make the two necklaces identical. For a visual, see two identical necklaces below:



The question, then, is how many distinct necklaces (up to symmetry) can we form with n beads and k colors?

As for bracelets, the rules are quite similar. A bracelet is like a necklace, only we restrict not only cyclic rotations but also reflections. That is, if we can make two bracelets identical via some combination of rotations and reflections, then they are not distinct. Again, we wish to know how many bracelets there are up to symmetry given that we have n beads and k colors. We start with the necessary background knowledge.

1.1 The Dihedral Group

While I do assume some familiarity with the Dihedral Group, it will be useful to rely on polygons and their symmetries as tools while building intuition around various group theoretic concepts. Consequently, I think some proofs and examples of some of the more important properties of D_n are well deserved. We recall from Dummit & Foote that a symmetry of a regular n -gon is, “any rigid motion of the n -gon which can be effected by taking a copy of the n -gon, moving this n -gon in any fashion in 3-space and then placing the copy back on the original so it exactly covers it.” We can generalize “moving in any fashion” via rotations and reflections.

Imagine we inscribe a regular n -gon inside the unit circle such that the first vertex is at $(0,1)$, the second vertex is to the left of vertex 1, and so on. Then, rotating the n -gon simply moves the vertices along the circle. In particular, rotations that preserve symmetry are rotations of $\frac{2\pi}{n}$ radians, which we will denote as r . We can rotate in either the clockwise or counter clockwise direction, but it will be helpful to be consistent so let r be in the counter-clockwise direction. It should be clear that an n -gon has n rotations that preserve symmetry. Similarly, it's fairly easy to convince oneself that a regular n -gon also has n reflections. If n is odd, the reflections are about the line formed between a vertex and the origin. Since there are n vertices and no such line passes through two vertices at

once, there are n reflections. If n is even, there are $n/2$ reflections about lines formed by opposite vertices and $n/2$ reflections about perpendicular bisectors of opposite edges. We can be certain about the existence of lines through opposite vertices/edges when n is even because opposite vertices are separated by π radians. With that, we have shown that $|D_n|$ is indeed $2n$, but there is still a little work to do to build intuition around generalized polygon. Specifically, we would like to know why one reflection can generate the remaining $n - 1$ reflections when combined with rotations. In our examination of reflections, we may use whatever reflection we like, but for simplicity, we will denote f as the action that reflects (flips) the polygon about the line formed between vertex 1 (which may or may not be in its identity position) and the origin.

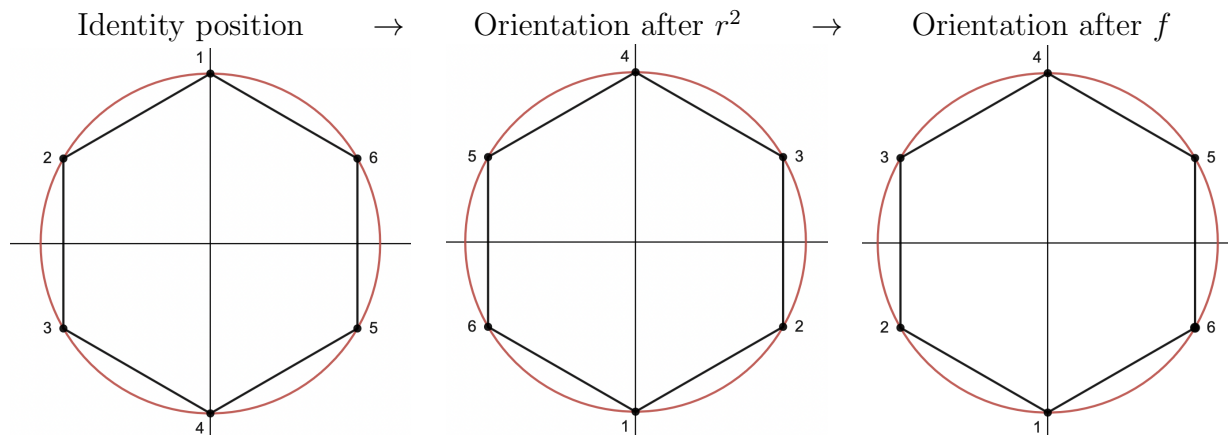
Suppose we wish to use our r and f to reflect a hexagon about the horizontal axis. As before, we inscribe the hexagon in the unit circle and let $(1,0)$ be vertex 1 and then fill in the remaining vertices by incrementing in the counterclockwise direction. Then, the reflection about the horizontal axis applies the following mapping of the vertices

$$1 \rightarrow 4 \quad 2 \rightarrow 3 \quad 3 \rightarrow 2 \quad 4 \rightarrow 1 \quad 5 \rightarrow 6 \quad 6 \rightarrow 5.$$

We can achieve that symmetry by first rotating 1 to 4, and then checking to see if we need to reflect to properly orient 2. After rotating, 2 will be at 5, but from above we see 2 goes to 3. So, we apply a reflection (send 2 from 5 to 3) and find that reflecting the hexagon about the horizontal axis from the identity position is given by

$$r^3 f = (123456)(123456)(123456)(26)(35) = (14)(23)(56).$$

We can confirm our work with some visual inspection:



In general, for any given symmetry of an n -gon we may obtain the symmetry by considering the resulting orientation of the polygon. Namely, we notice that the positions of 1 and 2 fix every other vertex (as we could define 3's position by considering 2, 4's position by considering 3, and so on). We can then think of a "symmetry algorithm" to obtain any desired symmetry of the polygon as a two step process. We first rotate 1 to the

desired position. From there, we reflect about 1 and the origin to orient 2 (if necessary). To conclude our review of the dihedral group, we consider six important properties:

- i) r, r^2, \dots, r^i are distinct for $0 \leq i \leq n$.
- ii) $|f| = 2$.
- iii) $f \neq r^i$ for any i .
- iv) $fr^i \neq fr^j$ if $j \neq i$ and $j, i \in \{x : 0 \leq x \leq n\}$
- v) $rf = fr^{-1}$
- vi) $r^i f = fr^{-i}$ for all $0 \leq i \leq n$

The first and second properties are obvious (but still important!) and will not be proven. We can provide an informal proof of property three by noticing that at least one vertex is fixed (one vertex if n odd, two vertices if n even) in f but no vertex is fixed in r^i . Property four is also obvious. If we reflect and then apply a rotation, that is clearly not the same as reflecting and applying a different rotation. Property five is the first that isn't immediately clear. A rather gimmicky way of proving property five is to notice that rf is just a reflection. Therefore, $(rf)^2 = 1$ so

$$rfrf = 1 \quad \Rightarrow \quad frf = r^{-1} \quad \Rightarrow \quad rf = fr^{-1}.$$

A similar argument can be applied to property six. These six properties together are very powerful. They allow us to simplify otherwise arduous expressions like $(fr^4)(fr^3)$. Notice that

$$(fr^4)(fr^3) = f(r^4f)r^3 = f(fr^{-4})r^3 = r^{-1}.$$

At this point, we have reviewed enough of the dihedral Group to make use of it—which we will do right away when we think about *group actions*.

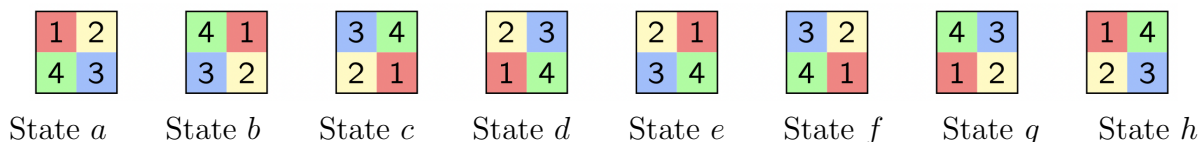
1.2 Group Actions and Homomorphisms

Before working through formal definitions and the like we will examine an intuitive approach to group actions. We can informally think of a group action as a group G permuting a set S of states or configurations. For example, we could interpret the permutation group S_{52} as the collection of all possible ways to shuffle a deck of cards. Notice, though, the subtle difference between actions themselves and the results they have on states.

Consider $1 \in S_{52}$. Let's suppose the standard ordering of a new deck of cards is all Clubs followed by all Hearts followed by all Spades followed by all Diamonds and each suit is ordered Ace, 2, 3, ... 10, Jack, Queen, King. The element $1 \in S_{52}$ is *not* the standard

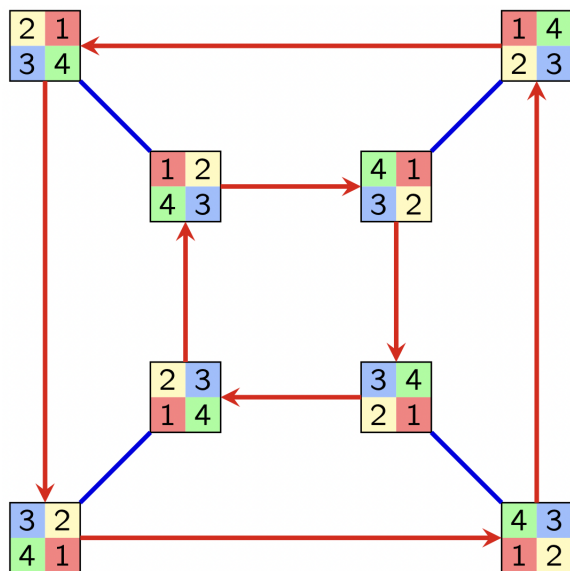
ordering, but rather, the action of not shuffling the cards, regardless of what order they may currently be in. Similarly, $r \in D_4$ is not a state but rather an action we can apply to a state. To emphasize the idea, consider the 8 states of a square:

Source: Prof. Macauley's Slides



If we so choose, we could let state a be the “identity state” (default state prior to any actions) but we don't have to. We could just as easily let the state b be the identity state. If that were the case, letting r be a 90° rotation counter clockwise would make state a correspond to result of applying r to state b .

It is a decent exercise to think about how actions and states interact and how the interactions shift if we choose different identity states or redefine our actions. For convenience, I've included a Cayley graph. The red arrows denote rotations whereas the blue arrows represent reflections about the horizontal axis.



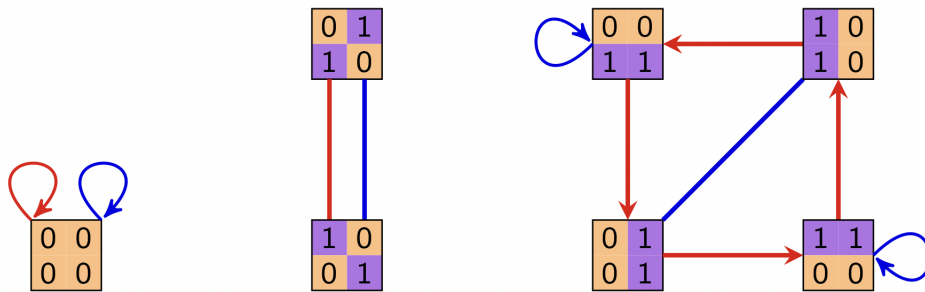
Source: Prof. Macauley's Slides

The astute reader may have noticed that so far, in our examples of actions there has been a bijection between actions and states. This is not always the case. Consider a set of seven “binary squares”:

$$S = \left\{ \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 0 & 0 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 1 & 1 \\ \hline 0 & 0 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 0 & 1 \\ \hline 0 & 1 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 1 & 1 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 1 & 0 \\ \hline 1 & 0 \\ \hline \end{array} \right\}$$

Source: Prof. Macauley's Slides

Let f be a horizontal flip and r a 90° rotation counter clockwise. Then, if we number the states from left to right we see that state 1 is unchanged by both rotation and reflection. Applying a rotation or reflection to state 2 results in state 3 and vice versa. States 4-7 are slightly more involved. States 4 and 6 are unchanged by reflection whereas states 5 and 7 interchange with each other after reflection. We can reach all four states (4-7) via rotation starting from any of the four states. A concise summary of all of the above is contained in what one might call an "action graph". In the graph below, let blue denote reflection, red rotation. Let directed arrows represent an action with an order greater than two and let loops denote an action that leaves the state unchanged. We then have:

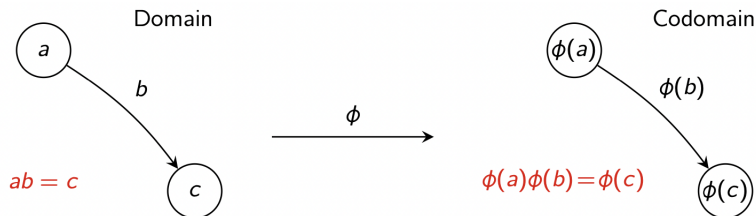


Source: Prof. Macauley's Slides

We now wish to start generalizing what we've learned about group actions. To do so, we will need to briefly examine *homomorphisms*.

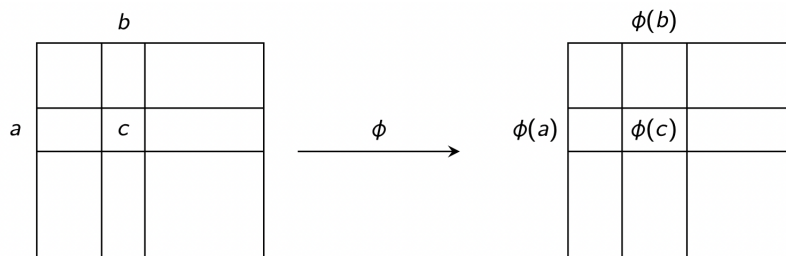
Definition. A homomorphism is a function ϕ from a group G to some other group G' such that for all $g_1, g_2 \in G$ we have $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$.

We can yet again use Cayley graphs to strengthen our intuition. When we discuss homomorphisms and group structure, we can think of two similar looking Cayley graphs, like so:



Source: Prof. Macauley's Slides

We can see the same idea in a multiplication table:



Source: Prof. Macauley's Slides

Proposition.

- i. If we let 1_G denote the identity in G and 1_H denote the identity in H , then $\phi(1_G) = 1_H$.
- ii. $\phi(g^{-1}) = \phi(g)^{-1}$.

Proof. For proof of the mapping from identity to identity, pick any $g \in G$ and first observe that

$$\phi(1_G)\phi(g) = \phi(1_G \cdot g) = \phi(g) = 1_H \cdot \phi(g).$$

Next, notice that $\phi(g) \in H$ and H is a group so $\phi(g)$ must have an inverse. We can therefore use right multiplication to cancel $\phi(g)$ and get $\phi(1_G) = 1_H$ as desired.

To prove the mapping of inverses, we again take any $g \in G$ and then observe that

$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1_G) = 1_H.$$

We see that $\phi(g)\phi(g^{-1}) = 1_H$ which immediately implies $\phi(g^{-1}) = \phi(g)^{-1}$. We will wrap up our brief considerations of homomorphisms with some examples. A few familiar homomorphisms are

- i. $\phi : V_4 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$
- ii. $\phi : D_3 \rightarrow S_3$
- iii. $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$

where V_4 is the Klein group and \mathbb{Z}_n denotes the integers reduced mod n . Notice that in the above, iii. is *not* bijective. Bijective homomorphisms are quite special and are called isomorphisms. If a group H is isomorphic to a group G , we immediately know the structure of H as the isomorphism tells us H is a structural copy of G . We don't really need isomorphisms to count necklaces, so that's all we will really say about them. To count necklaces, we are interested in homomorphisms and their role in group actions.

So far, we have only discussed group actions from an intuitive perspective, but we've actually already implicitly discussed the formal definition. Notice that we've been thinking of group actions as actions that permute states.

We can think of this homomorphism almost like a shuffle button. For every element in G there is a corresponding button that performs a type of shuffling. The idea of the homomorphism is that performing shuffle a and then performing shuffle b is equivalent to another shuffle button, either ab or ba . The ambiguity of the ab vs. ba button is due to the distinction between left and right actions. So long as we do not mistakenly right something false, the difference is not particularly important. Just as there is left multiplication and right multiplication, there are left actions and right actions. We may use either to achieve our goals.

Recall that a binary operation $*$ is defined such that it maps a Cartesian product between two sets to another set. In this way, $*$ gives us a rule for "multiplying" elements in sets. We can think of a group action in a similar manner.

Definition. A group action is a mapping $* : G \times X \rightarrow X$ where G is a group and X is a set. We say the group action is well defined if the mapping has the properties that $ex = x$ for all $x \in X$ and $(g_1g_2)x = g_1(g_2x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

If the above properties hold, we call X a G -set. We now connect our intuitive thinking to the formal definition.

Theorem. Let X be a G -set. For each $g \in G$, the function $\sigma_g : X \rightarrow X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X . Also, the map $\phi : G \rightarrow S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

Proof. We first show that σ_g is a 1-1 map of X onto itself. Notice that for $x_1, x_2 \in X$, if $\sigma_g(x_1) = \sigma_g(x_2)$ then $gx_1 = gx_2$. Similarly, $g^{-1}(gx_1) = g^{-1}(gx_2)$ so clearly, $x_1 = x_2$ and σ_g is 1-1. Via our properties of a G -set, we have $\sigma_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = ex = x$. We have now shown that σ_g is onto, so it is in fact a map from X to itself, and therefore, a permutation. We must now demonstrate that ϕ is a homomorphism. To do so, we must show that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. That is, we must show that the permutations $\phi(g_1g_2)$ and $\phi(g_1)\phi(g_2)$ both have an $x \in X$ that map to the same element. Using function composition and the properties from our definition of a group action, we have

$$\begin{aligned}\phi(g_1g_2)(x) &= \sigma_{g_1g_2}(x) = (g_1g_2)x = g_1\sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x)) \\ &= (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\sigma_{g_1g_2})(x) = (\phi(g_1)\phi(g_2))(x).\end{aligned}$$

One of particularly important byproducts of group actions is the concept of *orbits*. Orbits will be one of the integral parts of our method for counting necklaces and bracelets. First, though, it will be helpful to review cosets.

1.3 Cosets and Lagrange's Theorem

In reviewing cosets, we aim to set up the beginning of our examination of orbits and using orbits to count. To do so, all we really need is to show that cosets partition a group and that the order of cosets of certain groups are fairly easy to characterize using Lagrange's Theorem. Also, we will note that we focus solely on right cosets for convenience.

Definition. A partition of a set S is a collection of disjoint S_i such that the union of all S_i is S itself.

Definition. A right coset is the set $Ha = \{ha : h \in H\}$ obtained from a subgroup H of a group G where the representative a is in G .

Proposition. Let N be any subgroup of G . The set of right cosets of N in G form a partition of G . Furthermore, for all $u, v \in G$, $Nu = Nv$ if and only if $u^{-1}v \in N$. Also, $Nu = Nv$ if and only if u and v are representatives of the same coset.

Proof. Since N is a subgroup, the identity is in N . Therefore, $g = 1 \cdot g \in N$ for all $g \in G$ so

$$G = \bigcup_{g \in G} Ng.$$

We must now show that distinct cosets have empty intersections. We do so by showing that if two cosets intersect, they must be the same. Consider some Nu and Nv and let

$$Nu \cap Nv \neq \emptyset.$$

Now consider some $x \in Nu \cap Nv$. Notice that

$$x = nu = mv \quad \text{for some } n, m \in N.$$

If we multiply nu and mv on the left by n^{-1} we get

$$u = n^{-1}mv = m_1v$$

where $m_1 = n^{-1}m \in N$. Observe that for any $t \in N$ we have

$$tu = t(m_1v) = (tm_1)v \in Nv.$$

Hence, $Nu \subseteq Nv$. We can do all the above again and interchange u and v to show $Nv \subseteq Nu$. Thus, $Nu = Nv$ so two cosets with a nonempty intersection are actually the same set. We have now shown that cosets do partition a group as the union of all cosets does indeed get the original group and all distinct cosets are disjoint.

Now that we have proven cosets partition G , we need to prove Lagrange's Theorem. Before we do, though, we need to do a little preparation. Namely, we must show that given a subgroup H , all cosets of H in G have the same order. We will do so using a bijection.

Proposition. Let H be a subgroup of G . Then, for all g in G define a map $\lambda : H \rightarrow Hg$ by $\lambda(h) = hg$. It follows that λ is bijective so $|H| = |Hg|$.

Proof. We start by demonstrating that λ is 1-1. Suppose that $\lambda(h_1) = \lambda(h_2)$ for $h_1, h_2 \in H$. Then, we have $h_1g = h_2g$ and by right cancellation $h_1 = h_2$. To see λ is onto, notice that every element of Hg has the form hg for some $h \in H$ so λ is onto and we are done.

We may now state and prove Lagrange's Theorem.

Theorem. Let G be a finite group and let H be a subgroup of G . Then $|H|$ divides $|G|$.

Proof. Suppose that H has n distinct subsets. From our previous work, we know all the cosets of H in G are the same size and that the distinct cosets partition G . That is, we have

$$G = Hk_1 \cup Hk_2 \cup \cdots \cup Hk_n$$

and

$$\begin{aligned} |G| &= |H| + \cdots + |H| \\ &= n \cdot |H| \end{aligned}$$

so indeed, $|H|$ divides $|G|$. A particularly important result from Lagrange's theorem is that of the index, denoted $[G : H]$.

Definition. We define the index $[G : H] = |G|/|H|$ to be the number of right cosets of H in G .

Though I won't formally prove it, none of the ideas we just discussed are unique to right cosets. We could have just as easily proven everything with left cosets if we desired to do so. Now that we are armed with our knowledge of cosets, we may finally begin our examination of orbits.

1.4 Orbits

We start with an equivalence relation.

Theorem. Let X be a G -set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists a $g \in G$ such that $gx_1 = x_2$. Then \sim is an equivalence relation on X .

Proof. Clearly, \sim is reflexive as $1 \cdot x = x$ for all $x \in X$. Suppose that $x_1 \sim x_2$. To see that \sim is symmetric we observe that $x_1 \sim x_2$ implies $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = x_1$ so $g^{-1}x_2 = x_1$ which shows $x_2 \sim x_1$. For transitivity, suppose that $x_1 \sim x_2$ and $x_2 \sim x_3$. Then $g_1x_1 = x_2$ and $g_2x_2 = x_3$ for some $g_1, g_2 \in G$. Multiplying $g_1x_1 = x_2$ on the left by g_2 , we see that $(g_2g_1)x_1 = g_2x_2 = x_3$ so $x_1 \sim x_3$.

We can define an orbit via the equivalence relation we just proved.

Definition. Let X be a G -set. Each cell in the partition of the equivalence relation described in the previous theorem is an orbit in X under G . If $x \in X$, the cell containing x is called the orbit of x . We call this cell Gx .

To be clear, when we think about a partition we think about a collection of sets. Each set is what the definition above is referring to with the word “cell”. An example may provide some clarity.

Consider the permutation in S_8 denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

We find the orbit of an x in $\{1, 2, 3, 4, 5, 6, 7, 8\}$ we simply apply σ repeatedly. For instance, if we wanted to find the orbit of 2 we would get

$$2 \rightarrow 8 \rightarrow 2 \rightarrow 8 \rightarrow 2 \rightarrow \dots$$

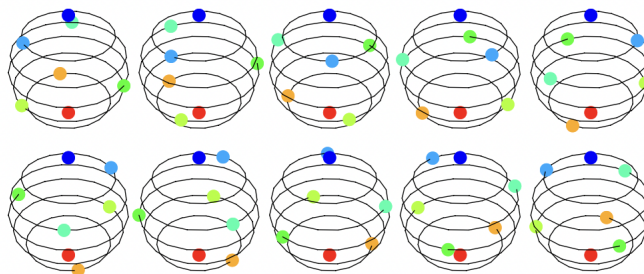
whereas the orbit of 1 would be

$$1 \rightarrow 3 \rightarrow 6 \rightarrow 1 \rightarrow 3 \rightarrow 6 \rightarrow \dots$$

and the orbit of 4 would be

$$4 \rightarrow 7 \rightarrow 5 \rightarrow 4 \rightarrow 7 \rightarrow \dots$$

We now say the orbit of 2 is $\{2, 8\}$, the orbit of 1 is $\{1, 3, 6\}$, and the orbit of 4 is $\{4, 5, 7\}$. It is perhaps a little more clear why they are called, “orbits”. When we repeatedly apply an action, we will eventually repeat (assuming the finite case—we will not consider the abstract algebra of infinite objects). We can think of this sort of like a circular motion in which we start at a point and travel through all possible points we can reach given some pre-defined jump (action). Then, the path we trace out is (very) loosely analogous to an actual orbit. Hence, orbits effectively tell us if a specific element can “reach” another element via a group action. To visualize this reaching idea, we look at a photo from WolframAlpha:



We can think of the various circular rings (no pun intended) to be the sets that denote orbits. So, the permutation in our example would have 3 circular rings because it has 3 orbits. Then, hopping along (applying σ to an element to get to another element in the orbit) the ring is allowed, but hopping from ring to ring (applying σ such that we get from an element in one orbit to an element in another) isn't. We have now covered a lot of background material and we have yet to count anything. How do we eventually tie everything together?

Recall that a group action is (informally) a group G that shuffles the states/configures of the elements of a set X . We may think about states as permutations, if we so choose. And, in fact, if we want to count items, more often than not permutations are very, very important. In this case, we want to count one permutation for every n permutations that are the same via symmetry. We can use orbits to do that by noticing that if G is say, the subgroup $H = \langle r \rangle$ of D_n then the orbit containing r^k tells us how many states (permutations) we can reach via the action of r^k on a given state. The question, then, is how do we count orbits?

2 Counting Necklaces and Bracelets

To count orbits, we will need to prove two theorems: The Orbit-Stablizer Theorem and Burnside's Lemma. Ideally, we'd also prove Pólya's Enumeration Theorem, but I don't see that as plausible given my remaining time. We will start with some terminology.

2.1 Stabilizers

Definition. A stabilizer is an element in the group G of a group action that fix some $x \in X$. That is, g is a stabilizer if and only if $gx = x$.

The simplest example of a stabilizer is the identity. There are nontrivial examples. Recall the binary squares we looked at earlier:

$$S = \left\{ \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 0 & 0 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 1 & 1 \\ \hline 0 & 0 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 0 & 1 \\ \hline 0 & 1 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 1 & 1 \\ \hline \end{array} , \begin{array}{|c|c|} \hline 1 & 0 \\ \hline 1 & 0 \\ \hline \end{array} \right\}$$

Source: Prof. Macauley's Slides

We can see that f , the reflection about the horizontal axis, does not alter the fourth square, so f is a stabilizer of the fourth square (and the sixth). If we were to examine stabilizers in full for this example, we may see a pattern.



Source: Prof. Macauley's Slides

Notice that the set of all stabilizers for a given state is a subgroup of D_4 . This is not a coincidence.

Proposition. For any G -set X , the set of stabilizers g such that $gx = x$ for some $x \in X$ is a subgroup of G .

Proof. Recall that a group action is a homomorphism and in particular, it is a permutation $\sigma : X \rightarrow X$ with a mapping $\phi : G \rightarrow S_X$ such that $\phi(g) = \sigma_g$ and $\phi(g)(x) = gx$. Using the subgroup criterion, we must show that there is an identity, inverses exist, and multiplication is closed. The identity isn't too bad (as we saw earlier). Since $\phi(1)(x) = 1 \cdot x = x$, we see that the identity of G is a stabilizer. For inverses, suppose that $\phi(g)(x) = x$. Then we must show $\phi(g^{-1})(x) = x$ as well. Notice that

$$x = \phi(1)(x) = \phi(g^{-1}g)(x) = \phi(g^{-1})\phi(g)(x) = \phi(g^{-1})(x).$$

For closure, we must show that if $\phi(g)(x) = x$ and $\phi(h)(x) = x$ then $\phi(gh)(x) = x$. Observe that

$$\phi(gh)(x) = \phi(g)\phi(h)(x) = \phi(g)(x) = x.$$

With that, we are ready to look at the Orbit-Stabilizer theorem.

2.2 Orbit Theorems

Theorem. Let X be a G -set and let $x \in X$. Then $|Gx| = [G : G_x]$ where Gx is the orbit of x and G_x is the stabilizer group for x . And, in particular, if $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.

Proof. Effectively we want to find a bijection between Gx and the left cosets of G_x in G .

To do that, we first let x_1 be in Gx . It follows that there exists some $g_1 \in G$ such that $g_1x = x_1$. Now, let $\gamma(x_1)$ be the left coset g_1G_x in G . Then, let some $g_2x = x_1$ so that $g_1x = g_2x$ and $g_1^{-1}(g_1x) = g_1^{-1}(g_2x)$ which implies $x = (g_1^{-1}g_2)x$. Hence, $g_1^{-1}g_2 \in G_x$ so $g_2 \in g_1G_x$ and finally, $g_1G_x = g_2G_x$. Consequently, γ is well defined.

We now show that γ is 1-1, consider some x_1, x_2 in Gx such that $\gamma(x_1) = \gamma(x_2)$. We can see that there exists $g_1, g_2 \in G$ such that $x_1 = g_1x$ and $x_2 = g_2x$ so $g_2 \in g_1G_x$. It follows, then, that $g_2 = g_1g$ for some $g \in G_x$ which means $x_2 = g_2x = g_1(gx) = g_1x = x_1$. Therefore, γ is 1-1.

We conclude the proof by demonstrating that each left coset of G_x in G is of the form $\gamma(x_1)$ for some x_1 in the cell Gx . First, let g_1G_x be a left coset. Then if $g_1x_1 = x_1$ we see that $\gamma(x_1) = g_1G_x$. We have now shown that γ is a bijective map from G_x to both the left and right cosets of G_x in G so $|Gx| = [G : G_x]$. Finally, observe that if $|G|$ is finite, we have from Lagrange's Theorem $|G| = |G_x| \cdot [G : G_x]$ which implies $|Gx|$ is a divisor of $|G|$.

Our final theorem will be that of Burnside's Lemma.

Theorem. Let G be a finite group and X a finite G -set. If r is the number of orbits in X under G , then $r \cdot |G| = \sum_{g \in G} |X_g|$ where X_g denotes the subset of elements X left fixed by g .

With Burnside's Lemma, we can (finally) do some counting.

Suppose we have 7 different colored beads. How many ways can we make a bracelet? A bracelet has rotational and reflective symmetry so we let $G = D_7$ and apply Burnside's Theorem. Without accounting for symmetry, there are clearly $7!$ ways we can arrange the beads. So, we are considering what happens when D_7 acts on a set X of $7!$ possible arrangements. So we have

$$7! \cdot \frac{1}{14} = 360$$

possible bracelets.

References

- [1] *A First Course in Abstract Algebra* by John Fraleigh
- [2] *Abstract Algebra* by Dummit and Foote
- [3] *Abstract Algebra: Theory and Applications* by Thomas Judson
- [4] *Visual Group Theory* by Nathan Carter
- [5] [Prof. Prof. Macauley's Slides and Lecture Videos](#)
- [6] *Abstract Algebra: A First Course* by Dan Saracino