Why is Algebra Important for Combinatorics?

Robin Truax

March 2021

Contents

1 Motivation

Often, when counting objects, we would like to count them "up to some symmetry". A classic example is counting the number of ways to choose m objects from a set of n objects. This is equivalent to counting the number of permutations of n objects, up to the symmetry that the ordering of the first m, and the last $n - m$, do not matter. This might sound like a convoluted restatement, but it's actually how we derive the formula for binomial coefficients.

How can we generalize this notion? We rely on the area of math most closely related to symmetry: group theory. In this post, you will learn how a powerful tool from group theory for counting things up to symmetry.

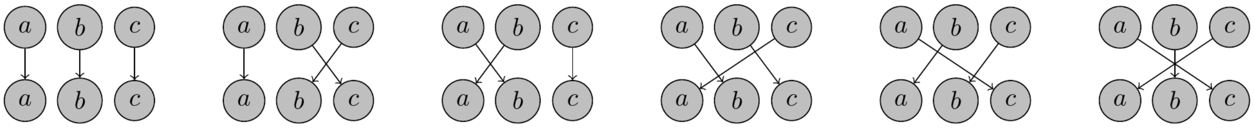
2 Group Actions

For this post, I'll assume you're familiar with the basics of group theory; that is, you know what a group is and basic things about them like subgroups, the index of a subgroup, and Lagrange's Theorem. However, I'll develop everything else from scratch. In this post, G is always a group, and X is a set which G acts on.

2.1 Definition

Definition 1 (Symmetric Group)**.** Given a set X, *the symmetric group on* X (denoted S_X) is the group of permutations on X. In particular, if $X = \{1, \ldots, n\}$, then we write S_n instead of S_X.

For example, if $X = \{a, b, c\}$, then S_X is the following set of 6 permutations:



Definition 2 (Group Action)**.** Formally, a *group action of G on X* is a homomorphism $\phi : G \to S_X$. Given $g \in G$ and $x \in X$, we write $g \cdot x$ to denote $\phi(g)(x)$.

This definition might be slightly opaque; despite its brevity, trying to understand a map whose output is another map can be quite difficult. Let's present an equivalent definition, just in case it helps.

Definition 3 (Group Actions with Operations)**.** A *group action of G on X* is an operation $\phi : G \times X \to X$, where we write $g \cdot x$ to abbreviate $\phi(g, x)$, satisfying the following two properties:

1. If e is the identity on G, $e \cdot x = x$.
2. If g and h are elements of G, $(gh) \cdot x = g \cdot (h \cdot x)$.

Problem 1. Demonstrate why these two definitions are the same. More precisely, show that any group action using the first definition gives a group action as defined by the second definition, and vice versa.

2.2 Examples and Properties

Example 1. The group S_X acts on the set X in a very natural way; a permutation $\phi \in S_X$ sends x to another element of X. Simply put, we can define $\phi \cdot x$ to be $\phi(x)$. This group action corresponds to the identity homomorphism $\iota : S_X \to S_X$.

Example 2. The group G acts on itself via the operation $g \cdot h = gh$.

Example 3. The group D_n acts on the vertices of a regular n-gon; since an element $d \in D_n$ corresponds to a rigid transformation of the regular n-gon, it sends a vertex of the n-gon to another vertex.

We will not use these definitions, but they are helpful to know in general.

Definition 4 (Faithful)**.** A group action $\phi : G \to S_X$ is called *faithful* if ϕ is injective; that is, if any two elements of G act differently on X.

Definition 5 (Transitive)**.** A group action of G on X is called *transitive* if, for any $x, y \in X$, there exists $g \in G$ with $g \cdot x = y$. In other words, a group action is transitive if it can move any element of X to any other element of X.

Problem 2. Which of the three examples are faithful? Which are transitive?

2.3 Orbits

Definition 6 (Orbits)**.** Suppose G acts on X. Then, define an equivalence relation $\sim$ on X by $x \sim y$ iff there exists $g \in G$ such that $g \cdot x = y$. This splits X into equivalence classes, which we call *orbits.* The set of all orbits is called the *orbit space*, and is denoted X/G.

Problem 3. Prove that $\sim$, as defined in the above definition, is indeed an equivalence relation.

For example, if a group action is transitive, then there is only one orbit, since $x \sim y$ for any $x, y \in X$.

Problem 4. Consider the group $G = S_m \times S_n$. Any pair (ϕ, ψ) for $\phi \in S_m$ and $\psi \in S_n$ can be identified with a permutation on $X = \{1, \ldots, m + n\}$, where ϕ acts on $\{1, \ldots, m\}$ and ψ acts on $\{m + 1, \ldots, m + n\}$. Therefore, G has a natural action on X. What are the orbits of this action?

2.4 Stabilizers

Definition 7 (Stabilizer)**.** Suppose G acts on X. Then, for any $x \in X$, the *stabilizer of* x (denoted G_x) is the subgroup of G composed of elements of G which fix x. In other words,

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

Problem 5. Prove that $G_x = \{g \in G \mid g \cdot x = x\}$ really is a subgroup of G for every $x \in X$.

Problem 6. Consider the action of $G = S_m \times S_n$ on $X = \{1, \ldots, m+n\}$ defined in the previous problem. What is the stabilizer of an element x of X? There will be two cases.

2.5 Fixed Points

Definition 8 (Fixed Points)**.** Suppose G acts on X. Then the set of elements of X fixed by a given element $g \in G$ is denoted X^g. That is,

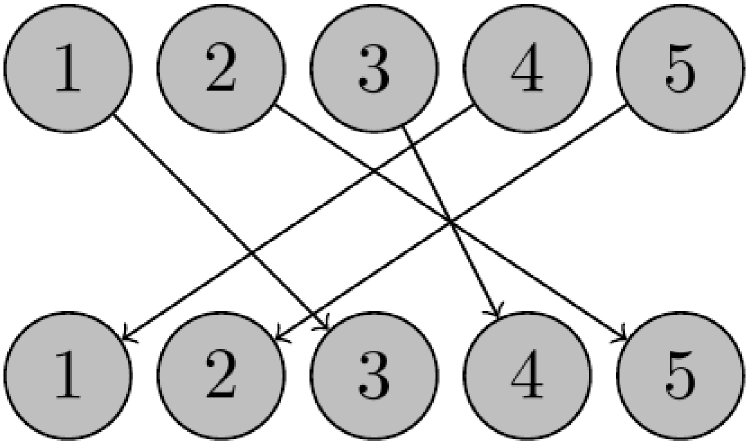
$$X^g = \{x \in X \mid g \cdot x = g\}.$$

Problem 7. What are the fixed points of the action in Example 2?

2.6 Cycles

Definition 9 (Cycles)**.** Suppose G acts on X. Then, take an element $g \in G$. Now, define an equivalence relation $\sim$ on X via $x \sim y$ if $g^n \cdot x \sim y$ for some $n \in \mathbb{Z}$. Then, equivalence class under this relation is defined to be a *cycle of* g. In other words, the action of g partitions X into *cycles of* g, as follows.

This concept can be quite difficult (although it is invaluable for later computation), so here is an example. Let S_5 act on the set $\{1, \ldots, 5\}$ in the obvious way. Then, let σ be the permutation



Then, there are two cycles of σ: $\{1, 3, 4\}$ and $\{2, 5\}$. Can you see why?

3 Theorems about Group Actions

Next, we'll develop two key results about group actions, that help us reframe questions in useful ways. The first result, called the Orbit-Stabilizer Theorem, is not only useful in combinatorics, but is key in group theory in general (for example, it is used to develop the class equation). The second result, Burnside's Lemma, has a proof so simple it seems almost trivial, but provides a change of perspective that trivializes difficult combinatorial problems.

3.1 The Orbit-Stabilizer Theorem

Theorem 1 (The Orbit-Stabilizer Theorem)**.** *Suppose G acts on a finite set X. For any $x \in X$, let $\mathcal{O}_x$ be the orbit containing x. Then the index of the stabilizer of x is the size of the orbit of x. That is,*

$$[G : G_x] = |\mathcal{O}_x|.$$

Proof. Consider the map $\phi : G \to \mathcal{O}_x$ given by $g \mapsto g \cdot x$. Notice that this map is surjective. We will show that each coset of G_x corresponds to a unique element of the orbit. To see why, suppose that y is a given element of $\mathcal{O}_x$. Then, there exists some $g \in G$ with $y = g \cdot x$. Now suppose that $h \in G$ is such that $y = g \cdot x = h \cdot x$. Then,

$$(g^{-1}h) \cdot x = g^{-1} \cdot (h \cdot x) = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = x$$

But this means that $g^{-1}h \in G_x$, or in other words that $h \in gG_x$. Therefore, the set of elements of G which map x to y are a coset of G_x. In other words, any coset of G_x uniquely corresponds to an element of $\mathcal{O}_x$. Yet there are $[G : G_x]$ cosets of G_x, and $|\mathcal{O}_x|$ elements of $\mathcal{O}_x$. Thus the result follows. □

Problem 8. Test the above theorem on the action defined in Problem 4 and 5. Does the theorem hold with your answers for the orbit and stabilizers of an element of $\{1, \ldots, m+n\}$?

3.2 Burnside's Lemma

Lemma 2 (Burnside's Lemma)**.** *Suppose that a finite group G acts on a finite set X. Then,*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

That is, the number of orbits can be computed by averaging the size of sets of fixed points.

Proof. Consider the following set of "invariant pairs":

$$I = \{(g, x) \mid g \cdot x = x\}.$$

We can count the size of this set in two different ways. Firstly, we can sum the size of X^g over all $g \in G$; this tells us that $|I| = \sum_{g \in G} |X^g|$. Secondly, we can sum the size of G_x over all $x \in X$; this tells us that $|I| = \sum_{x \in X} |G_x|$. Recall that, by the Orbit-Stabilizer Theorem, $|G_x| = \frac{|G|}{[G:G_x]} = \frac{|G|}{|\mathcal{O}_x|}$. Therefore,

$$\sum_{g \in G} |X^g| = |I| = \sum_{x \in X} \frac{|G|}{|\mathcal{O}_x|} = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}_x|}.$$

But notice that any given orbit $\mathcal{O}$ contributes a term $\frac{1}{|\mathcal{O}|}$ to the sum $\sum_{x \in X} \frac{1}{|\mathcal{O}_x|}$ a total of $|\mathcal{O}|$ times. Therefore, any given orbit contributes exactly $\frac{1}{|\mathcal{O}|} \cdot |\mathcal{O}| = 1$ to said sum. In other words, $\sum_{x \in X} \frac{1}{|\mathcal{O}_x|}$ simply counts the number of orbits of the action of G on X. Therefore, it is equal to $|X/G|$. Thus, as desired,

$$\sum_{g \in G} |X^g| = |G||X/G| \Rightarrow |X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

□

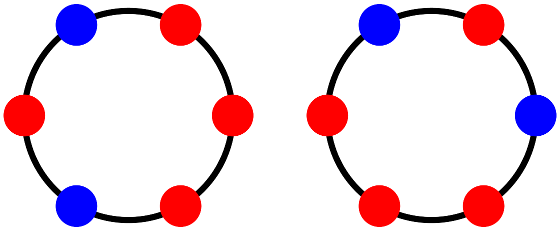
Instead of providing examples for Burnside's Lemma here, we'll discuss applications in the following section.

4 Examples

In general, Burnside's Lemma is helpful when we are trying to count objects up to some symmetry; we can view this as a problem of counting orbits of a symmetry group acting on all said objects. Following are two basic examples, and then a more involved one.

4.1 Enumerating Necklaces

Problem 9. Suppose that we have b types of beads and seek to make a necklace of n beads. Two necklaces are considered identical if they differ only by a rotation; that is, if the first necklace can be rotated until it looks identical to the second. For example, the following 6-bead necklaces are identical:



Discover a formula for the number of necklaces of n beads with b types of beads. Your formula's output should be a polynomial in b of degree n. Evaluate your formula for $n = 10$ and n prime.

Solution 9. Consider the set X of all b^n necklaces. These necklaces are operated on by the cyclic group C_n via rotation. More precisely, if c generates C_n, let c rotate the necklace by 1 bead, so c^m rotates the necklace by m beads. The number of non-equivalent necklaces is equal to the number of orbits of this action. Next, we'll apply Burnside's Lemma, which says that

$$|X/C_n| = \frac{1}{|C_n|}\sum_{g\in C_n}|X^g|$$

Now, $|C_n| = n$, so all we need to compute is how many necklaces are fixed by an element c^m of C_n. Notice that an element is fixed by c^m if and only if each bead has the same color as the bead m elements down. Yet this bead must be the same color as the bead m elements down from *it*, and so on. In other words, the action of g on an individual necklace partitions the necklace into $\gcd(m, n)$ cycles, and in each of these cycles, all the beads must have the same color. Thus, if $g = c^m$, then

$$|X^g| = b^{\gcd(m,n)} \Rightarrow \sum_{g\in C_n}|X^g| = \sum_{m=1}^{n} b^{\gcd(m,n)} \Rightarrow |X/C_n| = \frac{1}{n}\sum_{m=1}^{n} b^{\gcd(m,n)}.$$

Now, if $n = 10$, this is just a matter of evaluation. Explicitly,

$$|X/C_{10}| = \frac{1}{10}\sum_{m=1}^{10} b^{\gcd(m,10)} = \frac{1}{10}\left(b + b^2 + b + b^2 + b^5 + b^2 + b + b^2 + b + b^{10}\right) = \frac{1}{10}\left(b^{10} + b^5 + 4b^2 + 4b\right)$$

For example, if there are 4 types of beads, then there are $\frac{4^{10}+4^5+4(4^2)+4(4)}{10} = 104968$ distinct necklaces.

If n is a prime, on the other hand, $\gcd(m, n) = 1$ whenever $1 \leq m < n - 1$ and n if $m = n$. Thus,

$$|X/C_n| = \frac{1}{n}\sum_{m=1}^{n} b^{\gcd(m,n)} = \frac{1}{n}\left((n-1)b + b^n\right) = \frac{b^n + (n-1)b}{n}$$

4.2 Designing Dice

Let's look at another problem in the same vein.

Problem 10. Suppose that we have n colors with which to paint the sides of a cube. Say two colorings of a cube are equivalent if they differ by just a rotation; that is, if the first coloring can be rotated to give the second coloring. How many non-equivalent colorings of the cube are there?

Solution 10. Let X be the set of n^6 distinct colorings of the cube. X is acted upon by the group G of rotational symmetries of the cube. G has order 24, since a rotation of the cube amounts to choosing which of 6 faces will face "up", and then choose which of 4 rotations of the top face to choose. Therefore, all that remains is to compute $|X^g|$ for each element $g \in G$. While slightly tedious, this is not difficult. We begin by listing all the rotational symmetries of the cube:

Type	Axis	Order of Rotation	No. of elements
1	None	1	1
2	Face	2	3
3	Face	4	6
4	Edge	2	6
5	Vertex	3	8

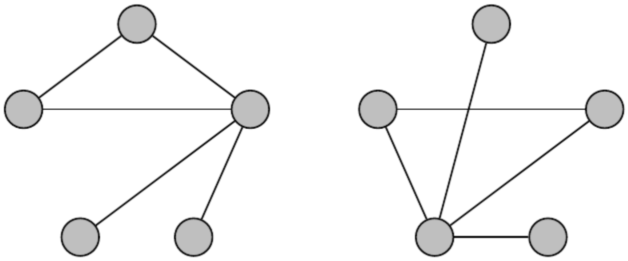
For any $g \in G$, a coloring $x \in X$ is fixed by g if and only if all faces in the same cycle of g have the same color. Thus, if $c(g)$ is the number of cycles of an element g acting on the cube, the number of fixed colorings is $n^{c(g)}$. We use this to create the next table:

Type	$c(g)$	$\|X^g\|$	No. of elements	Part of Sum
1	6	n^6	1	n^6
2	4	n^4	3	$3n^4$
3	3	n^3	6	$6n^3$
4	3	n^3	6	$6n^3$
5	2	n^2	8	$8n^2$

Therefore, $\sum_{g\in G} |X^g| = n^6 + 12n^3 + 3n^4 + 8n^2$, and indeed $|X/G| = \frac{n^6+12n^3+3n^4+8n^2}{24}$.

4.3 Counting Graphs

In graph theory, it is of interest to count the number of graphs on n vertices. This may seem initially simple: with n vertices, there are $\binom{n}{2}$ pairs of vertices, and so one might expect that there are $2^{\binom{n}{2}}$ graphs (since we have two choices for each pair of vertices: to have an edge or have no edge). However, some choices are redundant. For example, the following graphs are "the same" in some sense:



Both of them have the same structure. Explicitly, they both have a "root" vertex with connections to every other vertex, and one extra edge between two non-root vertices. If we could permute the vertices, we could shift one graph to the other. This leads to the following definition from graph theory:

Definition 10 (Isomorphic Graphs)**.** Suppose G and H are graphs with respective vertex sets $V(G)$ and $V(H)$. An isomorphism of graphs is a bijection $\phi : V(G) \to V(H)$ such that there is an edge between v and w in G if and only if there is an edge between $\phi(v)$ and $\phi(w)$ in H.

Problem 11. How many non-isomorphic graphs are there on 4 vertices?

Hint: Recall that there are $2^{\binom{4}{2}} = 2^6$ (possibly isomorphic) graphs on a set of 4 vertices. Let X be the set of these graphs, and let $G = S_4$ operate it by permuting its vertices. Then the number of orbits of this action is the number of non-isomorphic graphs on these vertices. Now, $|G| = 4! = 24$, so all that remains is to compute X^g for each g. You could do this in cases.

Problem 12. How many non-isomorphic graphs are there on n vertices?

We will not do this example here, as it takes a lot of computation. Instead, I leave it as an exercise for the reader, and reference here and here (clickable link) as places to learn more.