Math 116 Professor: Padraic Bartlett

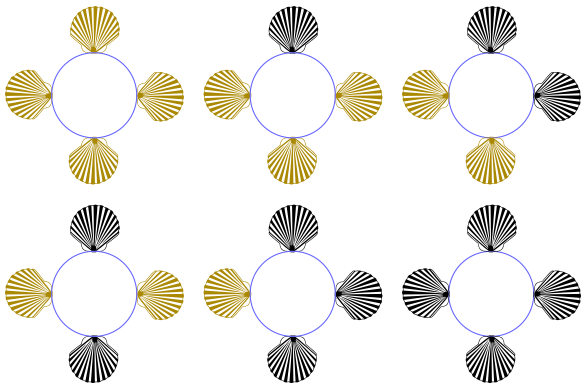
Lecture 5: Burnside's Lemma and the Pólya Enumeration Theorem

Weeks 8-9 *UCSB 2015*

We finished our Möbius function analysis with a question about seashell necklaces:

Question. Over the weekend, you collected a stack of seashells from the seashore. Some of them are tan and some are black; you have tons of each color.

You want to arrange them in a necklace! You consider two necklaces to be the same if one can be rotated so that it is the other (you don't allow flips, though, because then your seashells would be backwards.) For example, here are all of the distinct necklaces you can make with four shells:



How many different necklaces on n shells can you make, for any n?

We answered this problem by performing Möbius inversion on the divisor poset; however, at the time, many of you noted that there seemed to be a different connection to group theory here, and in specific to the idea of **groups** and **group actions**! Many of you have seen some of these ideas before (the idea of a group, if nothing else, is something you've likely seen in Math 8!) However, it may have been a while, so we review these ideas here:

1 Groups and Group Actions

1.1 Groups: Basic Definitions

Definition. A **group** is a set G along with some operation $\cdot$ that takes in two elements and outputs another element of our group, such that we satisfy the following properties:

- **Identity**: there is a unique identity element $e \in G$ such that for any other $g \in G$, we have $e \cdot g = g \cdot e = g$.

  In other words, combining any group element g with the identity via our group operation does not change g! You know many objects like this: if we work with the real numbers $\mathbb{R}$ and think of addition as our group operation, then 0 is our identity, as $0 + x = x$ for any x. Similarly, if we consider the real numbers again but take our operation to be multiplication, then 1 is our identity, as $1 \cdot x = x$ for any x.

- **Inverses**: for any $g \in G$, there is a unique g^{-1} such that $g \cdot g^{-1} = g^{-1}g = e$.

  In other words, if we start at any group element g, we can always find something to combine with g using our group operation to get back to the identity! Again, you know several objects like this: with $\mathbb{R}$ and addition, the inverse of any number x is just its negative $-x$, while if we consider the set of nonzero real numbers and multiplication, the inverse for any x is just $1/x$.

- **Associativity**: for any three $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

  In other words, the order in which we group combinations together doesn't matter, as long as the sequence that we have those objects grouped together in does not change! I.e. we can combine a with $b \cdot c$, or first find $a \cdot b$ and then combine that with c. Again, most of the natural operations you're familiar with (addition, multiplication) are associative: it is perhaps more interesting to point out some things that are nonassociative. For example, exponentiation is a nonassociative operation: $2^{(3^4)} = 2^{81} \approx 2.41 \cdot 10^{24}$, while $(2^3)^4 = 8^4 = 4096$.

It bears noting that this does not say that $a \cdot b = b \cdot a$: that is a different property, called **commutativity**, and is not a property that groups need to have (as we will show in the examples!) Groups that are commutative are called **abelian groups**, after the mathematician Niels Henrik Abel.

We list a number of examples of groups, as well as some nonexamples. Here, we don't give formal proofs that any of these objects are groups; instead, we list them rapid-fire to give you a list of examples to think about in your head! (If you're interested, you can prove that any of these objects satisfy the claimed properties, though!)

Example. As noted above, the real numbers with respect to addition, which we denote as $\langle \mathbb{R}, + \rangle$, is a group: it has the identity 0, any element x has an inverse $-x$, and it satisfies associativity.

Nonexample. The real numbers with respect to multiplication, which we denote as $\langle \mathbb{R}, \cdot \rangle$, is **not** a group: the element $0 \in \mathbb{R}$ has no inverse, as there is nothing we can multiply 0 by to get to 1!

Example. The nonzero real numbers with respect to multiplication, which we denote as $\langle \mathbb{R}^\times, \cdot \rangle$, is a group! The identity in this group is 1, every element x has an inverse $1/x$ such that $x \cdot (1/x) = 1$, and this group satisfies associativity.

Example. The integers with respect to addition, $\langle \mathbb{Z}, + \rangle$ form a group!

Nonexample. The integers with respect to multiplication, $\langle \mathbb{Z}, \cdot \rangle$ do not form a group: for example, there is no integer we can multiply 2 by to get to 1.

Nonexample. The natural numbers $\mathbb{N}$ are not a group with respect to either addition or multiplication. For example: in addition, there is no element $-1 \in \mathbb{N}$ that we can add to 1 to get to 0, and in multiplication there is no natural number we can multiply 2 by to get to 1.

Example. $GL_n(\mathbb{R})$, the collection of all $n \times n$ invertible real-valued matrices, is a group under the operation of matrix multiplication. Notice that this group is an example of a **nonabelian** group, as there are many matrices for which $AB \neq BA$: consider $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ versus $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Example. $SL_n(\mathbb{R})$, the collection of all $n \times n$ invertible real-valued matrices with determinant 1, is also a group under the operation of matrix multiplication; this is because the property of being determinant 1 is preserved under taking inverses and multiplication for matrices.

These examples are all great, but they're not really what I'm interested in for this class. Instead, I want to focus on examples of **finite** groups! In the next section, we study examples of these groups in more depth than above, and explain more about why they form a group.

1.2 Finite Groups

Definition. The object $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$ is defined as follows:

- Your set is the numbers $\{0, 1, 2, \ldots n-1\}$.
- Your addition operation is the operation "addition mod n," defined as follows: we say that $a + b \equiv c \mod n$ if the two integers $a + b$ and c differ by a multiple of n.

  For example, suppose that $n = 3$. Then $1 + 1 \equiv 2 \mod 3$, and $2 + 2 \equiv 1 \mod 3$.
- Similarly, our multiplication operation is the operation "multiplication mod n," written $a \cdot b \equiv c \mod n$, and holds whenever $a + b$ and c differ by a multiple of n.

  For example, if $n = 7$, then $2 \cdot 3 \equiv 6 \mod 7$, $4 \cdot 4 \equiv 2 \mod 7$, and $6 \cdot 4 \equiv 3 \mod 7$.

This is a commutative group!

This is not the only way in which modular arithmetic can make a group:

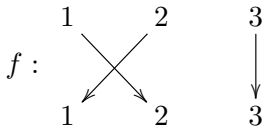
Example. $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, \ldots p-1\}$ is a commutative group with respect to the operation of multiplication mod p, if and only if p is a prime. (If you haven't proven this before; do it at home, or email me!)

There are other finite groups beyond those made out of modular arithmetic! In particular, there are several notable examples of **noncommutative** groups: we describe some of those here.

Example. The **symmetric group** S_n is the collection of all of the permutations on the set $\{1, \ldots n\}$, where our group operation is composition. In case you haven't seen this before:

- A **permutation** of a set is just a bijective function on that set. For example, one bijection on the set $\{1, 2, 3\}$ could be the map f that sends 1 to 2, 2 to 1, and 3 to 3.

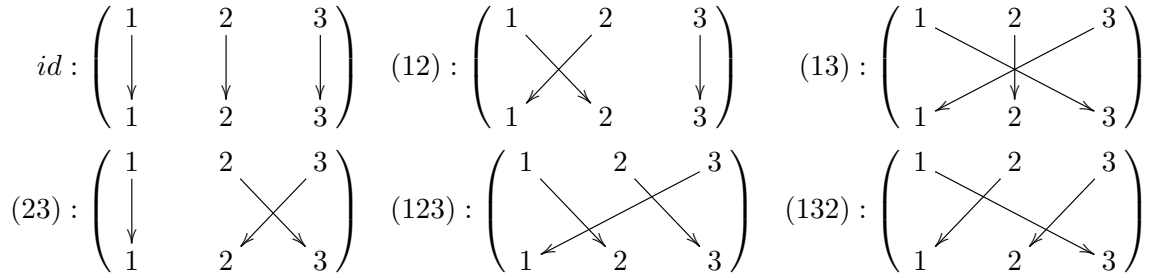
- One way that people often denote functions and bijections is via "arrow" notation: i.e. to describe the map f that we gave above, we could write



- This, however, is not the most space-friendly way to write out a permutation. A much more condensed way to write down a permutation is using something called **cycle notation**. In particular: suppose that we want to denote the permutation that sends $a_1 \to a_2$, $a_2 \to a_3$, $\ldots a_{n-1} \to a_n$, $a_n \to a_1$, and does not change any of the other elements (i.e. keeps them all the same.) In this case, we would denote this permutation using cycle notation as the permutation

$$(a_1 a_2 a_3 \ldots a_n).$$

To illustrate this notation, we describe all of the six possible permutations on $\{1, 2, 3\}$ using both the arrow and the cycle notations:



It's worth noting that some permutations need to be represented with multiple cycles. For example,

$$(143)(25) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix},$$

because 1 maps to 4, 4 maps to 3, and 3 maps to 1, giving us (143), and 2 maps to 5 maps to 2, giving us (25).

Because the composition of any two bijections is still a bijection, we have in particular that the composition of any two permutations is another permutation: so our group operation does indeed combine group elements into new group elements.

Composing any map f with the identity map $id(x) = x$ does not change the map f, so $id(x)$ is an identity element.

Associativity is doable to check: take any three bijections $f : C \to D, g : B \to C, h : A \to B$. We want to check that $(f \circ g) \circ h : A \to D$ is the same map as $f \circ (g \circ h) : A \to D$.

To do this, it suffices to show that they send the same elements to the same places, as this is exactly what it means for two functions to be equal. Take any $a \in A$, and notice that

$$((f \circ g) \circ h)(a) = (f \circ g)(h(a)) = f(g(h(a)))$$
$$(f \circ (g \circ h))(a) = (f(g(h(a)))) = f(g(h(a))).$$

So we satisfy associativity!

Finally, to see that we have inverses, notice that any bijection $f : X \to Y$ has an inverse function $f^{-1}Y \to X$ defined by

$$f^{-1}(y) = \text{ the unique } x \text{ such that } f(x) = y.$$

Notice that $f^{-1} \circ f(x) = x$ for any x: in other words, their composition is the identity! Therefore, any bijection has an inverse, and thus S_n is a group.

While the above work certainly shows that S_n is a group, it may not do a great job of giving us a feel for how to combine its elements. To do this, let's demonstrate a small yet useful property about S_n:

Definition. A permutation $\sigma \in S_n$ is called a **transposition** if we can write $\sigma = (ab)$, for two distinct values $a, b \in \{1, \dots n\}$.

Claim. We can write any $\sigma \in S_n$ as a product of transpositions.

Proof. To illustrate what our claim is, let's work it out for all of the elements of S_3. We first note that $(12), (13)$ and (23) are all trivially covered by this proposition, as they are themselves transpositions; as well, we can "trivially" write id as the product $(12)(12)$, amongst other things, as

$$id : \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix} \quad = \quad (12)(12) : \begin{pmatrix} 1 & 2 & 3 \\ \searrow\!\swarrow & & \downarrow \\ 1 & 2 & 3 \\ \searrow\!\swarrow & & \downarrow \\ 1 & 2 & 3 \end{pmatrix},$$

because both maps send 1 to 1, 2 to 2, and 3 to 3 (just follow the arrows!)

To work this out for (123) and (132) takes not much more work. Simply notice that to do the permutation (123), we could start with the swap 1 and 2, to get 1 to map to the right thing; from there, we currently have $2 \to 1$ and $3 \to 3$, when we want $2 \to 3$ and $3 \to 1$. Swapping 1 and 3 fixes these issues, and gives us the swap we want! Because function compositions are read right-to-left (because in $f(g(x))$, you apply g to x before applying f!), we would write this as (13)(12): and indeed, we can check that

$$(123) = \begin{pmatrix} 1 & 2 & 3 \\ & \searrow \quad \swarrow & \\ 1 & 2 & 3 \end{pmatrix} = (13)(12) = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \swarrow \quad \searrow & \downarrow \\ 1 & 2 & 3 \\ & \searrow \quad \swarrow \quad \searrow & \\ 1 & 2 & 3 \end{pmatrix}.$$

Using similar logic, we can see that (132) can be written as (12)(13):

$$(132) : \begin{pmatrix} 1 & 2 & 3 \\ & \swarrow \quad \searrow & \\ 1 & 2 & 3 \end{pmatrix} = (12)(13) = \begin{pmatrix} 1 & 2 & 3 \\ & \swarrow \quad \downarrow \quad \searrow & \\ 1 & 2 & 3 \\ & \swarrow \quad \searrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}.$$

This hopefully gives us a bit more of a feel for what we're doing here! Just to illustrate a tricker case, however, let's try a longer permutation: what about $\sigma = (12345) \in S_5$? Well: let's use similar logic to our earlier cases. We know that σ sends $1 \to 2$; so we can start with (12) as our first transposition. Now 1's going to the right place! If we consider 2, it's currently going to 1, when it should be going to 3. Therefore, if we follow up our first switch with (13), it will send 2 to 3, while not changing where 1 maps to (as we didn't touch its target from the first step, 2!)

This process continues: 3 is mapping to 1 now, and it should map to 4; so we should apply (14). Then, 4 is mapping to 1, and it should map to 5; so we apply (15). Now we have 5 mapping to 1, which is correct; in other words, all of our elements are mapping to

the right place! This is easily verified with a quick diagram:

$$(12345) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$(15)(14)(13)(12) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

In general, suppose we have any cycle $(a_1 a_2 \dots a_n)$. I claim that we can write this cycle as the product

$$(a_1 a_2 \dots a_n) = (a_1 a_n) \dots (a_1 a_4)(a_1 a_3)(a_1 a_2);$$

we prove this by induction. Our base case, when $n = 2$, is trivially true: so we move to our inductive step. Assume that our case holds for length-n cycles, and consider a cycle $(a_1 a_2 \dots a_n a_{n+1})$ of length $n + 1$.

So: consider the product $(a_1 a_{n+1})(a_1 a_n) \dots (a_1 a_4)(a_1 a_3)(a_1 a_2)$. We want to show that this permutation is precisely the cycle $(a_1 a_2 \dots a_n a_{n+1})$.

By induction, we know our product of transpositions is equal to $(a_1 a_{n+1})(a_1 a_2 \dots a_n)$. Consider where this permutation sends elements:

- If we look at any of the elements $a_k \in \{a_1, \dots a_{n-1}\}$, each a_k gets sent to a_{k+1} by the cycle $(a_1 a_2 \dots a_n)$; because none of the elements $a_2, \dots a_n$ are in the transposition $(a_1 a_{n+1})$, it does not interact further with any of these elements.
- If we look at a_n, it is sent to a_1 by the cycle $(a_1 a_2 \dots a_n)$; because a_1 is then sent to a_{n+1} by the transposition $(a_1 a_{n+1})$, in total we have that a_n is sent to a_{n+1}.
- Finally, a_{n+1} is not touched by the cycle $(a_1 a_2 \dots a_n)$, and is then sent to a_1 by the transposition $(a_1 a_{n+1})$.

In total, we have that each a_k is sent to a_{k+1}, with the exception of a_{n+1}, which is sent to a_1. In other words, our product of transpositions is precisely $(a_1 a_2 \dots a_n a_{n+1})$, as claimed.

Via cycle notation, we can write any permutation as some product of cycles: applying this result to each cycle in turn lets us write each permutation as a product of cycles, as claimed. □

It bears noting that a given permutation can be written as a product of transpositions in multiple ways: for example,

$$(123) = (13)(12) = (12)(23) = (12)(12)(12)(23),$$

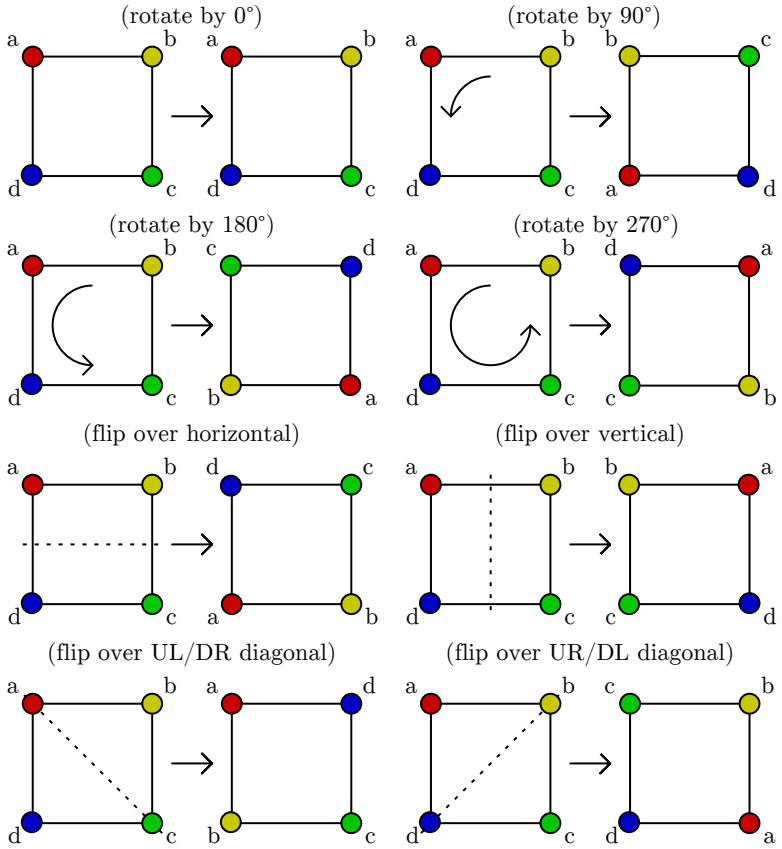
for example. However, you can prove that the **parity** of the number of transpositions needed to write any permutation is invariant:

Theorem. Take any permutation $\pi \in S_n$. Suppose that you can write π as a product of transpositions in two different ways; one that uses s transpositions, and another that uses t. Then either s, t are both odd, or s, t are both even.

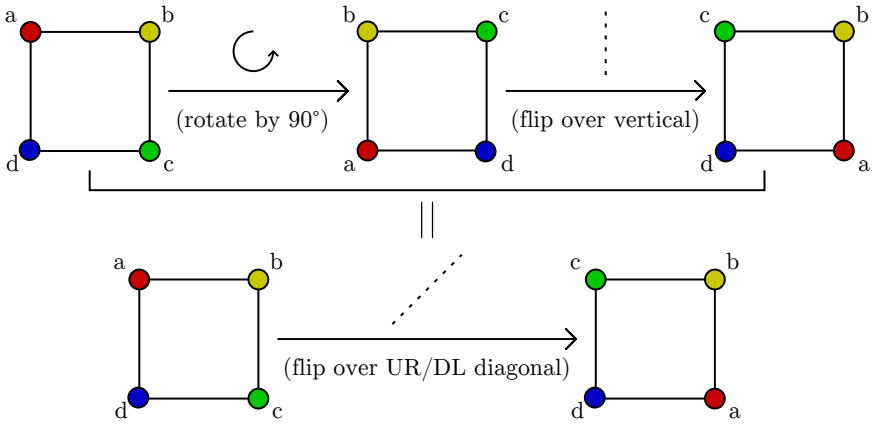
We leave this theorem for you to prove if you haven't seen it before!

Not all finite groups are as algebraic as S_n! Our last example, for instance, is beautifully geometric in nature:

Example. Consider a regular n-gon. There are a number of geometric transformations, or **similarities**, that we can apply that send this n-gon to "itself" without stretching or tearing the shape: i.e. there are several rotations and reflections that when applied to a n-gon do not change the n-gon. For example, given a square, we can rotate the plane by $0°, 90°, 180°$, or $270°$, or flip over one of the horizontal, vertical, top-left/bottom-right, or the top-right/bottom-left axes:



Given two such transformations f, g, we can compose them to get a new transformation $f \circ g$. Notice that because these two transformations each individually send the n-gon to itself, their composition also sends the n-gon to itself! Therefore composition is a well-defined operation that we can use to combine two transformations.



Notice that the trivial rotation by $0°$, when composed with any other map, does not change that map: so, under the operation of composition, rotation by $0°$ is an **identity**! Similarly, notice that performing the same flip twice in a row returns us back to the identity, so every flip has an **inverse** given by itself! (I.e. if f is a flip, $f \circ f = id$: i.e. $f = f^{-1}$.) As well, if we rotate by k degrees, rotating by $360 - k$ degrees results in a total rotation by 360: i.e. rotation by $0°$. So all rotations have inverses as well!

Finally, notice that because function composition is associative (as shown above!), this operation is **associative** as well. Consequently, the collection of all symmetries of a regular n-gon forms a group under the operation of function composition!

We call this last group D_{2n}, because it is the group of **order**[1] $2n$. Algebraists will usually use this terminology; geometers, however, will often write the same group as D_n, as they care about they object whose symmetries we are studying (a n-gon) more than the number of symmetries themselves ($2n$).

One particularly useful kind of group here is the idea of a **subgroup**:

1.3 Subgroups and Cosets

Definition. Take any group $\langle G, \cdot \rangle$, and a subset $H \subseteq G$. We say that H is a **subgroup** of G if the following three properties hold:

1. **Closure**: For any two elements $h_1, h_2 \in H$, $h_1 \cdot h_2$ is also in H.
2. **Identity**: The identity id of G is in H.
3. **Inverses**: If $h_1 \in H$, then h_1^{-1} is also in H.

Notice that any subgroup of a group is a group in its own right! This is because the associativity property is "inherited" from the larger group, and we've already checked all of the other properties for being a group.

[1] The **order** of a group is the number of elements in that group!

Examples. The set of even numbers is a subgroup of the integers under addition! This is because 0 is an even number (identity), the sum of any two even numbers is even (closure), and the additive inverse of any even number is also even (inverses.)

Conversely, the set of all odd numbers is not a subgroup of the integers under addition: because 0 is not odd, this subset does not satisfy the identity property!

The set of all powers of 2, $\{2^n \mid n \in \mathbb{Z}\}$ is a subgroup of the nonzero real numbers under multiplication! This is because $1 = 2^0$ (identity,) $2^n \times 2^m = 2^{n+m}$ (closure), and $2^n \cdot 2^{-n} = 2^0 = 1$ (inverses) all hold for this subgroup.

Conversely, the set of all even integers is not a subgroup of the nonzero reals under multiplication, as there is no multiplicative inverse for 2 in this set!

The set of all rotations, along with the identity is a subgroup of the group D_{2n} of symmetries of a n-gon: to see this, notice that we have the identity by definition, the inverse of rotating by θ is another rotation (by $2\pi - \theta$), and the composition of two rotations (by θ, φ) is just the rotation given by summing their angles ($\theta + \varphi$.)

Given the idea of a subgroup, a natural extension of this idea is the concept of **cosets**:

Definition. Suppose that $\langle G, \cdot \rangle$ is a group, $s \in G$ is some element of G, and H is a subgroup of G. We define the **left coset** of H corresponding to s as the set

$$Hs = \{sh \mid h \in H\}.$$

We will often omit the "left" part of this definition and simply call these objects cosets.

Example. Consider the group $G = \langle \mathbb{Z}, + \rangle$. One subgroup of this group is the collection of all multiples of 5: i.e.

$$H = \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\}$$

This subgroup has several left cosets:

- $s = 0$: this forms the coset

  $$0 + H = \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\},$$

  which is just H itself.

- $s = 1$: this forms the coset

  $$1 + H = \{\ldots -14, -9, -4, 1, 6, 11, 16 \ldots\}.$$

- $s = 2$: this forms the coset

  $$2 + H = \{\ldots -13, -8, -3, 2, 7, 12, 17 \ldots\}.$$

- $s = 3$: this forms the coset

  $$3 + H = \{\ldots -12, -7, -2, 3, 8, 13, 18 \ldots\}.$$

- $s = 4$: this forms the coset

$$4 + H = \{\ldots -11, -6, -1, 4, 9, 14, 19 \ldots\}.$$

Notice that this collection of cosets above is indeed the collection of **all** of the possible cosets of H within G: if we take any other element in $\mathbb{Z}$, like say 13, we'll get one of the five cosets above: i.e.

$$13 + H = \{\ldots -2, 3, 8, 13, 18 \ldots\} = 3 + H.$$

In general, $H + x = H + y$ for any $x \equiv y \mod 5$.

Example. Consider the group $G = \langle(\mathbb{Z}/7\mathbb{Z})^\times, \cdot\rangle$, i.e. the nonzero integers mod 7 with respect to the multiplication operation. This has the set

$$H = \{1, 6\}$$

as a subgroup (check this if you don't see why!)

This group has the following cosets:

- $s = 1$, which creates the cosets $H \cdot 1 = H$,
- $s = 2$, which creates the coset

$$2 \cdot H = \{2, 5\}.$$

- $s = 3$, which creates the coset

$$3 \cdot H = \{3, 4\}.$$

- $s = 4$, which creates the coset

$$4 \cdot H = \{4, 3\}.$$

  Notice that this coset is the same as $H \cdot 3$.

- $s = 5$, which creates the coset

$$5 \cdot H = \{5, 2\}.$$

  Notice that this coset is the same as $H \cdot 2$.

- $s = 6$, which creates the coset

$$6 \cdot H = \{6, 1\}.$$

  Notice that this coset is the same as H.

So, in total we have three distinct cosets!

Example. Consider the group S_3. This group has the subgroup

$$H = \{id, (123), (132)\}$$

as a subgroup. This subgroup has two possible distinct cosets:

- $id \cdot H = (123) \cdot H = (132) \cdot H$ are all the same coset, which is just H.
- $(12) \cdot H = (13) \cdot H = (23) \cdot H = \{(12), (13), (23)\}$.

Cosets have a number of remarkably useful properties:

Theorem. Take any finite group $\langle G, \cdot \rangle$ and any subgroup H.

1. For any $s \in G$, the left coset sH is equal to H if and only if $s \in H$.
2. Two cosets sH, tH are either completely identical or completely disjoint.
3. The various possible cosets of H **partition** G into a collection of disjoint subsets. (In particular, this proves that the number of elements in H must divide the number of elements in G.)
4. All cosets of H are the same size: i.e. $|sH| = |H|$ for any $s \in G$.
5. If there are k distinct cosets of H, then $k|H| = |G|$.

Proof. Take any group $\langle G, \cdot \rangle$ and any subgroup H. We prove these properties in order.

1. Take any $s \in G$. If $s \in H$, then because H is a subgroup we have that s^{-1} is in H, and therefore that for any $h \in H$ we have $s^{-1}h$ in H. Consequently, every member of H is in sH. As well, any member of sH is a product of two elements of H; therefore by closure, sH is a subset of H. Therefore we have proven that $Hs = H$, as claimed.

   Conversely, when $s \notin H$, we want to show that $sH \neq H$. But this is trivial: because H contains the identity, we know that $s = s \cdot id \in sH$, but $s \notin H$; so these are different sets.

2. Take any two cosets sH, tH. If they are not completely disjoint, then there is some element they share in common: in other words, there is some $h_1, h_2 \in H$ such that $sh_1 = th_2$. But this means that $t^{-1}s = h_1h_2^{-1}, s^{-1}t = h_1h_2^{-1}$, and therefore that $t^{-1}s, s^{-1}t$ are elements in H.

   So, take any $th_3 \in tH$. We can write $th_3 = t(t^{-1}s)(t^{-1}s)^{-1}h_3 = s(t^{-1}s)^{-1}h_3$; i.e. th_3 is an element of the form $s\cdot$ something in H! So $tH \subseteq sH$.

   Similarly, for any $sh_3 \in sH$, we can write $sh_3 = s(s^{-1}t)(s^{-1}t)^{-1}h_3 = t(s^{-1}t)^{-1}h_3$; i.e. sh_3 is of the form $t\cdot$ something in H! So $sH \subseteq tH$ as well, and we've proven our claim.

3. Simply notice that for any element $g \in G$, gH contains g; this is because the identity is in H, and therefore that $g \cdot id = g \in gH$. But this means that every element is in some coset: if we combine this with (2), we have that every element is in exactly one coset. But this is what it means to be a partition!

4. On one hand, we know that $sH = \{sh \mid h \in H\}$ means that we cannot have more elements in sH than we have in H, because we only get one element in Hs for each element of H. But if we ever had $sh_1 = sh_2$, we could multiply by s^{-1} on the left to get $h_1 = h_2$: consequently, we can conclude that we have exactly as many elements in sH as we do in H!

5. By point 3, the cosets of H partition G: that is, if we add up the sizes of all of our cosets, we will get the size of G. On the other hand, by point 4, all of these cosets are the same size; so the number of elements in all of our cosets is just $k|H|$. So we've proven our claim!

□

Point 5 has a very famous corollary, in the form of Lagrange's theorem:

Theorem. (Lagrange.) Let $\langle G, \cdot \rangle$ be a finite group, and H be any subgroup of G. Then the order of H divides the order of G.

1.4 Group Actions

Several of the groups we defined in these notes — S_n, D_{2n} — are interesting because they are groups defined by how they **act** on some outside object. For example, elements of S_n are permutations of the set $\{1, 2, \ldots n\}$; that is, they are defined by how they shuffle the elements of a set around. Similarly, elements of D_{2n} are symmetries of a n-gon; that is, they are defined by how they move the vertices of some n-sided shape around! This motivates us to introduce the idea of a **group action**:

Definition. A **group action** of a group $\langle G, \cdot \rangle$ on a set X is any map $\star : G \times X \to X$ that satisfies the following two properties:

1. **Identity**: If e is the identity in G, then for any $x \in X$, we have $e \star x = x$.

2. **Compatible with the group operation**: For any two elements $g, h \in G$ and any element $x \in X$, we have $g \star (h \star x) = (g \cdot h) \star x$.

The idea with this second operation is that it says that it doesn't matter whether we apply g, h one-by-one using $\star$ to x, or if we combine them first in G with $\cdot$ and then apply the result to x. In both cases we get the same thing!

We list several useful examples of group actions:

Example. Take the group S_n, and consider the following action of this group on the set $\{1, 2, \ldots n\}$: for any $\sigma \in S_n, k \in \{1, \ldots n\}$, set $\sigma \star k = \sigma(k)$. For example, if $\sigma = (123)$ and $k = 2$, we would say $\sigma(2) = 3$.

This is a group action! To see this, we just check our definition:

1. **Identity**: The identity of S_n is just the identity map id on $\{1, \ldots n\}$. Therefore, for any $k \in \{1, \ldots n\}$ we have $id \star k = id(k) = k$: so we satisfy the identity property!

2. **Compatible with the group operation**: Take any two permutations $\sigma, \varphi \in S_n$, and any $k \in \{1, \dots n\}$. Notice that $(\sigma \circ \varphi) \star (k) = \sigma(\varphi(k))$, and $\sigma \star (\varphi \star k) = \sigma \star (\varphi(k)) = \sigma(\varphi(k))$ is just the same thing; therefore we are compatible with our group's operation!

Example. Take the group D_{2n}, and consider the following way in which it acts on the set of vertices $\{v_1, \dots v_n\}$, listed in order, of a n-gon: if f is a symmetry of our n-gon, then we say that $f \star v_k$ is just $f(v_k)$. In other words, our action sends v_k to whatever vertex f maps v_k to. Show that this is a group action of D_{2n} on $\{v_1, \dots v_n\}$.

This is a group action! To see this, we just check our definition:

1. **Identity**: The identity of D_{2n} is just the identity map id on $\{v_1, \dots v_n\}$. Therefore, for any $k \in \{v_1, \dots v_n\}$ we have $id \star k = id(k) = k$: so we satisfy the identity property!

2. **Compatible with the group operation**: Take any two symmetries $f, g \in S_n$, and any $v_i \in \{v_1, \dots v_n\}$. Notice that $(f \circ g) \star (v_i) = f(g(v_i))$, and $f \star (g \star v_i) = f \star (g(v_i)) = f(g(v_i))$ is just the same thing; therefore we are compatible with our group's operation!

Example. For any group $\langle G, \cdot \rangle$, consider the following way in which G could act on **itself**: for any $g \in G, h \in G$, set $g \star h = g \cdot h$. This is a group action of G on G:

1. **Identity**: Suppose that the identity of G is e. Then, for any $g \in G$, we have $e \star g = e \cdot g = g$; so we satisfy the identity property!

2. **Compatible with the group operation**: Take any two elements $g, h \in G$, and any $k \in G$. Notice that $(g \cdot h) \star (k) = g \cdot h \cdot k$, and $g \star (h \star k) = g \star (h \cdot k) = g \cdot h \cdot k$ is just the same thing; therefore we are compatible with our group's operation!

2 Burnside's Lemma and Necklace Problems

2.1 Orbits, Stabilizers, and Fixed Points

It might seem like we've introduced an awful lot of notation for a relatively simple necklace problem; but if you look at the machinery we've assembled, it's all actually pretty natural. In our necklace problem, we have the following:

- A set given by all of the 2^n necklaces in two colors on n shells.
- A way for the group of rotational symmetries on a n-gon to **act** on this set; given any necklace, we act on it by a rotation by rotating that necklace!

From here, we want to know what are all of the elements that are "distinct" under these rotations. To make this more formal, consider the following definitions:

Definition. Suppose that X is a set and G is a group that acts on X by some operation $\star$. For any $x \in X$, make the following definitions:

- The **orbit** of x, denoted $Orb(x)$, is the collection of all elements in X that can be reached by starting at x and multiplying x by an appropriate element: that is,

$$Orb(x) = \{g \star x \mid g \in G\}.$$

- The **stabilizer** of x, denoted $Stab(x)$, is the collection of all elements in G that "don't move" x: that is,

$$Stab(x) = \{g \in G \mid g \star x = x\}.$$

- The **fixed points** of an element g, denoted $Fix(g)$ for any $g \in G$, is the collection of all of the elements of x "unmoved" by G: that is,

$$Fix(g) = \{x \in X \mid g \star x = x\}.$$

Notice the following properties:

Proposition. Take any group G acting on a set X. Then the sets $Orb(x)$ partition the set X; that is, every element of X is in some set $Orb(x)$, and for any $x, y \in X$, the sets $Orb(x), Orb(y)$ are either completely disjoint or identical.

Proof. The first property is easy to check. Let e denote the identity of our group G; then, for any $x \in X$, we have $e \star x = x$ by definition. But this means that $x \in Orb(x)$; so every $x \in X$ is in one of these sets.

For the second property: take any two sets $Orb(x), Orb(y)$. We claim that these two sets are either disjoint or identical; to prove this, we can simply look at the case where they are not disjoint and prove that they must be identical.

Let $z \in X$ be an element in both $Orb(x), Orb(y)$; then there are group elements $g_1, g_2 \in G$ with $g_1 \star x = g_2 \star y = z$. By compatibility, we can see that

$$x = e \star x = (g_1^{-1} \cdot g_1) \star x = g_1^{-1} \star (g_1 \star x) = g_1^{-1} \star (g_2 \star y) = (g_1^{-1} \cdot g_2) \star y,$$

and therefore that $x \in Orb(y)$. But this in particular means that for any $h \in G$, we have

$$h \star x = (h \cdot g^{-1} \cdot g_2) \star y;$$

i.e. **any** element in $Orb(x)$ is in $Orb(y)$! Similarly, we can solve for y in terms of x to get that for any $h \in G$,

$$(h \cdot g_2^{-1} \cdot g_1) \star x = h \star y,$$

and can similarly conclude that **any** element in $Orb(y)$ is in $Orb(x)$. □

Proposition. Take any group G acting on a set X. For any $x \in X$, the set $Stab(x)$ is a subgroup of G.

Proof. To check that a subset of a group is a subgroup, we just need to check three things:

- **Identity**: We need that the identity e of our group is in $Stab(x)$. This is by definition; for any $x \in X$, $e \cdot x = x$, and therefore $e \in Stab(x)$.
- **Closure**: For any $g, h \in Stab(x)$, we need $g \cdot h \in Stab(x)$. This is by compatibility; if $g, h \in Stab(x)$, then $g \star x = h \star x = x$, and therefore $(g \cdot h) \star x = g \star (h \star x) = g \star x = x$.
- **Inverses**: For any $g \in Stab(x)$, we need $g^{-1} \in Stab(x)$. This is also by compatibility; if $g \in Stab(x)$, then $g \star x = x$, and therefore $g^{-1} \star x = (g^{-1} \cdot g) \star x = e \star x = x$, so g^{-1} is also in $Stab(x)$.

□

In this sense, our necklace problem is a specific instance of the following problem: given a group G acting on a set X, how many **different** orbits are there? (I.e. how many "different" necklaces are there, given that an orbit of a necklace is just all of the things equivalent to that necklace under rotation?)

We answer this with the last two bits of algebra needed to solve our problem: the **Orbit-Stabilizer Theorem** and **Burnside's Lemma**!

2.2 Theorems!

Theorem. (Orbit-Stabilizer Theorem.) Let G be a finite group that acts on a set X, and take any element $x \in X$. Then

$$|G| = |Orb(x)| \cdot |Stab(x)|.$$

Proof. Let $G/Stab(x)$ denote the collection of all of the cosets of the subgroup $Stab(x)$ in G. For each coset K of $Stab(x)$, pick an "representative" element $g \in K$ in that coset; then we can write $K = g \cdot Stab(x)$ (this is because $K, g \cdot Stab(x)$ are two cosets that both contain g, and therefore must be equal by our results earlier.) This makes it easier to work with our cosets!

Consider the following function $f : G/Stab(x) \to Orb(x)$: for any coset $g \cdot Stab(x)$ with representative g, define

$$f(g \cdot Stab(x)) = g \star x.$$

I claim that f is a bijection. To see this, we just check injectivity and surjectivity:

- **Injectivity**: Suppose that $g \cdot Stab(x), h \cdot Stab(x)$ are two cosets that get mapped to the same element; then $g \star x = h \star x$. But this means that $(g^{-1} \cdot h) \star x = (g^{-1} \cdot g)x = e \star x = x$; i.e. that $g^{-1} \cdot h \in Stab(x)$. But this means that $g \cdot g^{-1} \cdot h = h \in gStab(x)$; that is, that $g \cdot Stab(x), h \cdot Stab(x)$ are not disjoint! Therefore they are the same. Consequently, we've proved injectivity, as we've shown that the only way for two cosets to map to the same element is if those two cosets were identical.
- **Surjectivity**: Take any $h \star x \in Orb(x)$. Because the cosets of $Stab(x)$ partition G, there is some coset $g \cdot Stab(x)$ with $h \in g \cdot Stab(x)$.

  But this just means that $h = g \cdot k$ for some $k \in Stab(x)$; consequently, we have that $h \star x = (g \cdot k) \star x = g \star (k \star x) = g \star x = f(g \cdot Stab(x))$. So we map to $h \star x$, and are therefore surjective!

Therefore, we have that the number of cosets of $Stab(x)$ is the same size as the number of elements in $Orb(x)$. But by our work earlier, we know that the number of cosets is just $|G|/|Stab(x)|$; combining gives us

$$|G| = |Orb(x)| \cdot |Stab(x)|,$$

as claimed. □

Theorem. (Burnside's[2] Lemma.) Let G be a finite group acting on a set X. Let k denote the number of distinct orbits of elements of X under this action, and let $\Omega_1, \ldots \Omega_k$ denote these k different orbits. Then

$$k|G| = \sum_{g \in G} |Fix(g)|.$$

Proof. Consider the set S of all pairs (g, x) where g fixes x: that is,

$$S = \{(g, x) \mid g \star x = x\}.$$

If we group pairs (g, x) by their first element, we can see that for a fixed $g \in G$ the number of pairs (g, x) with $g \star x = x$ is just the number of elements $x \in X$ that are fixed by G: that is, we have

$$|S| = \sum_{g \in G} |\{x \mid g \star x = x\}| = \sum_{g \in G} |Fix(g)|.$$

On the other hand, if we group pairs (g, x) by their second element, we can see that for a fixed $x \in X$ the number of pairs (g, x) where $g \star x = x$ is just the number of elements $g \in G$ that fix x: that is,

$$|S| = \sum_{x \in X} |Stab(x)|.$$

If we split X apart into its k disjoint orbits $\Omega_1, \ldots \Omega_k$, we have

$$|S| = \sum_{i=1}^{k} \sum_{x \in \Omega_i} |Stab(x)|.$$

By the orbit-stabilizer result earlier, we know that $|Stab(x)| = \frac{|G|}{|\Omega_i|}$, for any x in the orbit Ω_i; so we actually have

$$|S| = \sum_{i=1}^{k} \sum_{x \in \Omega_i} \frac{|G|}{|\Omega_i|} = |G| \sum_{i=1}^{k} \sum_{x \in \Omega_i} \frac{1}{|\Omega_i|}.$$

[2]Often known as the Cauchy-Frobenius lemma, or "the lemma that is not Burnside's," as Burnside did not prove this result; he simply cited it and attributed it to Frobenius in a book he wrote on finite groups. History!

But, for any Ω_i, the sum

$$\sum_{x \in \Omega_i} \frac{1}{|\Omega_i|} = 1,$$

as we're just adding up the quantity $\frac{1}{|\Omega_i|}$ a total of $|\Omega_i|$-many times! So we actually have

$$|S| = |G| \sum_{i=1}^{k} 1 = k|G|.$$

Combining this with our first result, we have

$$k|G| = \sum_{g \in G} |Fix(g)|,$$

as claimed.

□

2.3 Applications

We start by using this machinery to solve our necklace problem:

Question. Take any prime number n. Suppose we look at the set X of all 2^n necklaces on n shells, where each shell is either black or white; denote this collection as the set

$$X = \{(s_1, \ldots s_n) \mid s_i \in \{W, B\}\}.$$

Let the group $\langle \mathbb{Z}/n\mathbb{Z}, + \rangle$ act on this set by saying that for any $a \in \mathbb{Z}/n\mathbb{Z}$, we have

$$a \star (s_1, \ldots s_n) = (s_{1+a}, s_{2+a}, \ldots s_{n+a}),$$

where the arithmetic in the subscripts above is calculated mod n. (So, for example, $1 \star (s_1, s_2, s_3)$ would be (s_2, s_3, s_1).)

How many necklaces are distinct under this action; in other words, how many different orbits exist for this group action?

Answer. By Burnside's lemma, we have

$$k|G| = \sum_{g \in G} |Fix(g)|,$$

where k is the number of orbits (i.e. what we want to find,) and $|G| = |\mathbb{Z}/n\mathbb{Z}| = n$. So it suffices to understand the sets $|Fix(g)|$, for all $g \in G$.

Notice that necklaces in X come in two different kinds:

- Some necklaces — specifically, two necklaces, the all-white and all-black necklaces — have all of their shells the same color. These necklaces are fixed by every element of G, as they are the same under any rotation.

- Other necklaces have shells of different colors. I claim that these necklaces are not fixed by any element of G other than the identity element (i.e. 0) To see why, take any necklace $(s_1, \ldots s_n)$, and any element $a \neq 0 \in \mathbb{Z}/n\mathbb{Z}$ such that $a \star (s_1, \ldots s_n) = (s_1, \ldots s_n)$.

  Then, for any k, we have

$$\begin{aligned}(s_1, \ldots s_n) = a \star (s_1, \ldots s_n) &= a \star a \star (s_1, \ldots s_n) \\ &= a \star a \star a \star (s_1, \ldots s_n) \\ &\ldots \\ &= \overbrace{a \star a \star \ldots \star a}^{k \text{ times}} \star (s_1, \ldots s_n) \\ &= (\overbrace{a + a + \ldots + a}^{k \text{ times}}) \star (s_1, \ldots s_n) \\ &= (k \cdot a) \star (s_1, \ldots s_n).\end{aligned}$$

  But n is a prime number, and $a \neq 0$; so, in the **multiplicative** group $\langle (\mathbb{Z}/n\mathbb{Z})^\times, \cdot \rangle$, a has an inverse element; call it $a^{-1} \in \mathbb{Z}/n\mathbb{Z})^\times$. Then, for any $b \in \mathbb{Z}/\mathbb{Z}$, if we let $k = ba^{-1}$, we have

$$\begin{aligned}(s_1, \ldots s_n) &= (ba^{-1}a) \star (s_1, \ldots s_n) \\ &= (b) \star (s_1, \ldots s_n) \\ &= \star(s_{1+b}, \ldots s_{n+b}).\end{aligned}$$

  In other words, we have $s_1 = s_{1+b}$ for any b; i.e. every shell in our necklace is the same!

This means that the $|Fix(g)|$ sets come in two different kinds:

- $g = 0$. The identity fixes every element in X by assumption; so $|Fix(0)| = 2^n$, the set of all of our necklaces.
- $g \neq 0$. Then, as shown above, there are only two necklaces that g fixes; so $|Fix(g)| = 2$.

Therefore,

$$kn = \sum_{g \in G} |Fix(g)| = |Fix(0)| + \sum_{g \neq 0 \in \mathbb{Z}/n\mathbb{Z}} |Fix(g)| = 2^n + \sum_{g \neq 0 \in \mathbb{Z}/n\mathbb{Z}} 2 = 2^n + 2(n-1),$$

and therefore that the number of distinct orbits is

$$\frac{2^n + 2(n-1)}{n}.$$

Success!

We turn here to a problem you will likely remember from our first class:

Question. Suppose that you have a set of n different postcards, out of which you want to choose k. In how many ways can you do this, if you don't care about the order in which you picked your cards?

Answer. So, on one hand, we already know the answer here: it's $\binom{n}{k}$. To show this at the time, though, we had to do something fairly odd with equivalence classes (or indeed when we studied this again with generating functions, we had to find some recurrence relations!) Some people asked at the time if there was a connection here between our answer and the idea of "quotient groups," and at the time I said that something close to that held; what I meant at the time was "use Burnside's lemma," and that's what we'll do here!

Specifically: let's unimaginatively label our n postcards $\{1, 2, \dots n\}$ Let X consist of all of the ways to order our set of n postcards; there are $n!$ elements in X, as we've proven in many ways in this class.

To select k postcards, then, we can simply choose any ordering from X and take the first k postcards in that ordering! So the elements of X correspond to way to pick out k postcards, where we care about the ordering of what we choose and what we do not choose. How can we get from here to our desired counting problem, where we don't care about the ordering of what we choose or the ordering of what we don't choose?

We start, as always, with a few definitions. Given two groups G, H, define their **direct product** as follows:

Definition. Given two groups $\langle G, \cdot \rangle$, $\langle H, \cdot \rangle$ we define their **direct product** $\langle G \times H$, as follows:

- The set: $G \times H = \{(g, h) \mid g \in G, h \in H\}$.
- The operation: for any $(g_1, h_1), (g_2, h_2) \in G \times H$, set $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$, where the operations inside the parentheses come from the original groups G, H.

It's not hard to check that this satisfies the properties of being a group; do so if you're curious!

For this problem, I specifically want to consider the cartesian product $G = S_k \times S_{n-k}$; that is, the group of all permutation (σ, π), where $\sigma \in S_k$, $\pi \in S_{n-k}$. This group acts on our set X of postcard-orderings as follows: for any postcard ordering $P = (p_1, \dots p_n) \in X$, define $(\sigma, \pi) \star P$ as the ordering given by using σ to permute the first k postcards, and using π to permute the remaining $n - k$ postcards. In symbols, we write this as

$$(\sigma, \pi) \star (p_1, p_2, \dots p_k, p_{k+1}, \dots p_n) = (p_{\sigma(1)}, p_{\sigma(2)}, \dots p_{\sigma(k)}, p_{k+\pi(1)}, p_{k+\pi(2)}, \dots p_{k+\pi(n-k)}).$$

We like this group action because it captures exactly what we meant by "we don't care about the ordering:" given any two orderings $P_1, P_2 \in X$, we consider P_1, P_2 to be the "same" ways to pick out k postcards if they have the same first k elements in some order: in other words, we consider P_1 and P_2 to be the same if there is some reorderings (σ, π) of P_1's cards that yields P_2!

So, our problem is now a Burnside's lemma problem: we have a set X and a group G acting on X, and we want to count the number of elements that are distinct under action by G; i.e. the number of distinct orbits of X under this group action. Therefore, it suffices to understand the fixed points of our group elements under our group action! This is pretty simple:

- The identity, as always, fixes everything: so $|Fix(id)| = n!$, the number of elements in X.
- Any other group element, however, fixes nothing! This is not hard to see; take any pair of permutations $(\sigma, \pi) \neq (id, id)$. One of σ, π must not be the identity; therefore, when it acts on any ordered set of postcards, it will shuffle those cards around (and in particular send that ordered set to something different!) So $|Fix(g)| = 0$ for any non-identity element g.

Applying Burnside's lemma gives us the following: the number of distinct orbits of X under action by G, i.e. the number of ways to choose k cards out of n without caring about the order, is just

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}|Fix(g)| &= \frac{1}{|S_k \times S_{n-k}|}\left(|Fix(0)| + \sum_{g\neq 0\in\mathbb{Z}/n\mathbb{Z}}|Fix(g)|\right)\\ &= \frac{1}{k!(n-k)!}\cdot\left(n! + \sum_{g\neq 0\in\mathbb{Z}/n\mathbb{Z}} 0\right)\\ &= \frac{n!}{k!(n-k)!}.\end{aligned}$$

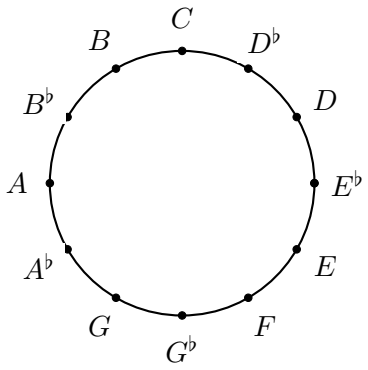
So we've answered our question.

We close by studying one last example of Burnside's lemma: counting chords!

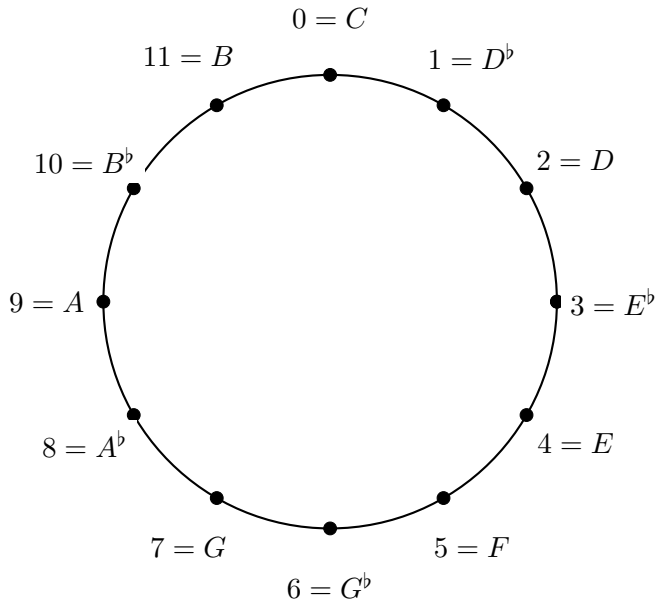
Question. Consider the standard Western musical scale of tones, where we consider two tones to be equivalent if they differ by an octave: that is, consider the tones

$$C, D\flat, D, E^\flat, E, F, G^\flat, G, A^\flat, A, B^\flat, B$$

arranged in a circle as follows:



We can identify these tones with the group $\mathbb{Z}/12\mathbb{Z}$ as follows:



A **triad** in this sense is any chord (i.e. subset of our tones) made out of three distinct tones; i.e. it is any ordered triple of three distinct elements of $\mathbb{Z}/12\mathbb{Z}$. In music, we often consider two triples to be "equivalent" if one can be translated (musically, the word here is **transposed**) to become another; i.e. we consider

$$(C, E, G) = (0, 4, 7) \text{ and } (F, A, C) = (5, 9, 0) = (0 + 5, 4 + 5, 7 + 5) \mod 12$$

to be "equivalent" because if we are only capable of discerning relative pitch, the spaces between these notes are all equal!

Similarly, we often consider two triples to be equivalent if the tones of one can be permuted to become the notes of the other: i.e. we consider

$$(C, E, G) = (0, 4, 7) \text{ and } (G, C, E) = (7, 4, 0)$$

to be equivalent because if all three tones are sounded simultaneously these two chords are indistinguishable. (Musically, such chords are said to be **inversions** of each other.)

How many distinct musical triads are there, given that we consider two triads to be equivalent if one can be transformed into the other under translation and permutation?

Answer. If we phrase this as a Burnside's lemma-styled problem, the answer here is relatively easy to determine!

Let X be the set of all unordered distinct triples of elements from $\mathbb{Z}/12\mathbb{Z}$. It is not hard to see that $|X| = \binom{12}{3}$, as we are just considering all of the ways to pick out three tones from a set of 12 tones without caring about the ordering.

This is almost an answer to our question: it counts all of the triads up to inversions (i.e. permutations.) So, to finish our problem, we just need to deal with translation as well!

To do this, we simply consider the group action of $G = \mathbb{Z}/12\mathbb{Z}$ on our set of triples, where for any $k, a, b, c \in \mathbb{Z}/12\mathbb{Z}$, we have

$$k \star \{a, b, c\} = \{a + k, b + k, c + k\},$$

where our addition is done mod 12.

This is a group action; moreover, we consider two triads in X equivalent if and only if one can be translated into the other via our group action, so determining the number of distinct orbits here will answer our question about the number of different triads!

As before, we consider the elements of our group case-by-case:

- As always, the identity $0 \in \mathbb{Z}/12\mathbb{Z}$ fixes everything, so we have $|Fix(0)| = |X| = \binom{12}{3}$.
- If we consider translation by 4, we have that $\{a, b, c\}$ is a fixed point if and only if

  $$4 \star \{a, b, c\} = \{a + 4, b + 4, c + 4\} = \{a, b, c\}.$$

  In particular, this forces our set to be of the form $\{a, a+4, a+8\}$ after some thought, and implies that there are precisely four such triples – $\{0, 4, 8\}, \{1, 5, 9\}\{2, 6, 10\}, \{3, 7, 11\}$. So $|Fix(4)| = 4$.
- By completely identical reasoning, $|Fix(8)| = 4$ as well!
- For any other translation, I claim that there are no fixed points. In fact, we can prove a stronger claim:

  Lemma. Suppose that we are working in a d-tone system (i.e. in $\mathbb{Z}/d\mathbb{Z}$,) and studying n-tuples of tones.

  Suppose that $A = \{a_1, \dots a_n\}$ is an unordered n-tuple of tones, and $k \in \mathbb{Z}/d\mathbb{Z}$ is such that $k \star A = A$. Then $k \cdot n$ is a multiple of d.

  Proof. If $k \star A = A$, then if $a_i \in A$, we must have that $a_i + k$ is in $k \star A$, and therefore in A itself. Repeating this logic tells us that $a_i + mk \in A$ for any m, provided that (as always) we do our arithmetic mod d. Notice that we get precisely $d/gcd(k, d)$-many distinct elements via this operation, as we get a repeat precisely when mk is a multiple of d for the first time.

  Take any $a_1 \in A$, and let $A_1 = \{a_1 + mk \mid m \in \mathbb{N}\}$. If A_1 is all of A, stop; otherwise, there is some other a_2 still in A not in A_1. Define $A_2 = \{a_2 + mk \mid m \in \mathbb{N}\}$. Notice that A_1, A_2 have no elements in common, as $a_1 + mk = a_2 + m'k \Rightarrow a_1 + (m - m')k = a_2$, and we would have then had a_2 in A_1.

  Repeat this process until we can't go any further. This gives us a bunch of sets $A_1, \dots A_l$, each of size $d/gcd(d, k)$.

  Because we have n elements in A, we must also have n elements in $k \star A$; therefore we have

  $$l \cdot \frac{d}{gcd(d, k)} = n \Rightarrow l \cdot d \cdot \frac{k}{gcd(d, k)} = kn.$$

$\frac{k}{gcd(d,k)}$ is always an integer, as it is k divided by some of its factors; so the LHS above is two integers times d. Therefore the RHS is a multiple of d, and we've proven our claim! □

Therefore, in any d-tone system where we're picking out n-tuples of tones, the only value k in $\mathbb{Z}/d\mathbb{Z}$ where we can possibly have fixed points are when kn is a multiple of d. In particular, for our problem here, we are considering $n = 3$-tuples of tones; so the only possible fixed points are when $3k$ is a multiple of 12; i.e. when $k = 0, 4, 8$! So no other group elements have fixed points in this problem; i.e. $|Fix(g)| = 0$ for $g \neq 0, 4, 8$.

Therefore, by Burnside's lemma, the number of distinct orbits (i.e. number of distinct triads) is

$$\frac{1}{|G|}\sum_{g\in G}|Fix(g)| = \frac{1}{12}\left(|Fix(0)| + |Fix(4)| + |Fix(8)|\right) = \frac{\binom{12}{3} + 4 + 4}{12} = \frac{228}{12} = 19.$$

(Similar methods can enumerate all of the different 4-tuples of tones, or in general all of the n-tuples for any n; try it if you're interested!)