Applications of Group Actions

Ishita Goluguri and Christina Li

November 25, 2019

1 Introduction

In this paper, we explore some fascinating applications of group actions, a microcosm of the tools used to analyze symmetries in group theory. To do this, we begin with an introduction to group theory, developing the necessary tools we need to interrogate group actions. We begin by discussing the definition of a group and group actions, and simple examples of both, such as the group of symmetries of a square and this group's action upon a vertex. We proceed to then define both an orbit and a stabilizer, and prove the Orbit-Stabilizer Theorem, which is central to proving Burnside's Lemma. Subsequently, we exemplify how Burnside's Lemma can help us solve combinatorial problems. Namely, we compute the number of distinct colorings of a geometric pattern and the number of distinct necklaces that can be made with colored beads by utilizing Burnside's Lemma. Finally, we discuss another application of group actions, the Sylow Theorems, which are essential to the classification of groups. We prove these theorems using the conjugation group action as well as other relevant definitions.

2 Groups and Group Actions

Definition 2.1. A *group* is a set G together with a binary operation $\circ\colon G \times G \to G$ such that the following conditions hold:

(i) *Closure:* For all $g, h \in G$, the element $g \circ h$ is a uniquely defined element of G.

(ii) *Associativity:* For all $f, g, h \in G$, we have

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

(iii) *Identity:* There exists an *identity* element $e \in G$ such that

$$e \circ g = g \text{ and } g \circ e = g$$

for all $g \in G$.

(iv) *Inverse:* For each $g \in G$. there exists an *inverse* element $g^{-1} \in G$ such that

$$g \circ g^{-1} = e \text{ and } g^{-1} \circ g = e.$$

We will usually simply write gh for the composition $g \circ h$.

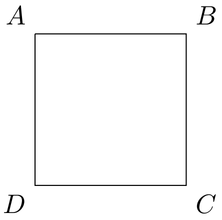
Definition 2.2. The *order* of a group G is its cardinality. In other words, it is the number of elements in G. The order of G is denoted $|G|$.

Example 2.3. The *dihedral group*, D_n, is the group of symmetries of a regular n-gon. The dihedral group of a square is denoted D_4, and defined as such:

$$D_4 = \{e, r_1, r_2, r_3, s_1, s_2, s_3, s_4\},$$

where

r_1 : clockwise rotation by 90°
r_2 : clockwise rotation by 180°
r_3 : clockwise rotation by 270°
e : clockwise rotation by 360°
s_1 : reflection across x-axis
s_2 : reflection across y-axis
s_3 : reflection across $y = x$ or BD
s_4 : reflection across $y = -x$ or AC.



Definition 2.4. A *subgroup* of a group G is a subset of G such that it itself is a group under the operation in G.

Definition 2.5. A group G *acts* on a set S when there is a map $G \times S \to S$ (written $(g, s) \mapsto gs$) such that the following conditions hold for all $s \in S$.

(i) *Associativity*: For $g, h \in G$ and $s \in S$,

$$g(hs) = (gh)s$$

(ii) *Identity*: The action of the identity of G on every $s \in S$ gives s, in other words,

$$es = s.$$

Example 2.6. The dihedral group D_4 acts upon the vertices of a square. Let us denote the vertices clockwise as A, B, C, and D. Any element in the dihedral group takes one vertex to another.

For example, $r_1 \cdot A = B$

(i) The group action is associative. $(d_1, (d_2, v_1)) \mapsto v_2$ where v_1, v_2 are vertices and $d_1, d_2 \in D_4$

(ii) The action of the identity of G on s gives s.

$$(e, s) \mapsto ese^{-1} = s.$$

Definition 2.7 (Set Multiplication)**.** Given set S and element x, we define multiplication of S and x by $Sx = \{sx \colon s \in S\}$.

Definition 2.8. Let H be a subgroup of a group G. The *right cosets* of H are the sets $Hg = \{hg : h \in H\}$ for each $g \in G$.

For any element $h \in H$, we have $Hh = H$ by the closure property of groups and subgroups.

Example 2.9. Let H be a subgroup of a group G. Let K be the set of right cosets of H. In other words, $K = \{Hg \colon g \in G\}$. For group G, there exists a group action $\theta \colon G \times K \to K$ which takes (g, k) to kg^{-1}. The map of this group action becomes $\{kg^{-1} \colon k \in K\}$. Alternatively, this can be written as Kg^{-1} using our definition of set multiplication. This is a right coset of K. Going back to our original definition, K is the set of right cosets of H in the form Hg. Thus, the right cosets of K are also right cosets of H and therefore, the set of right cosets of K is equal to K. The image of the map is K.

(i) *Associativity*: For $g, h \in G$ and $k \in K$,

$$h \cdot (g \cdot k) = h \cdot kg^{-1} = kg^{-1}h^{-1} = k(hg)^{-1} = (hg) \cdot k$$

(ii) *Identity*: The action of the identity of G on any $k \in K$ gives k, in other words,

$$e \circ k = ke = k.$$

Example 2.10. Let $S = G$ and let G act on itself by conjugation. For $g \in G$ and $s \in S$, the group G acts upon S by conjugation by $(g, s) \mapsto gsg^{-1}$.

We can see that conjugation satisfies the two requirements for a group action:

(i) The group action is associative. For $g, h \in G$ and $s \in S$,

$$g \circ (h \circ s) = g(h \circ s)g^{-1} = g \cdot (h \cdot s \cdot h^{-1}) \cdot g^{-1} = (g \cdot h) \cdot s \cdot (g \cdot h)^{-1} = (g \cdot h) \circ s \ ,$$

(ii) The action of the identity of G on s gives s.

$$(e, s) \mapsto ese^{-1} = s.$$

3 Orbit-Stabilizer Theorem

Throughout this section we fix a group G and a set S with an action of the group G. In this section, the group action will be denoted by both $g \cdot s$ and gs.

Definition 3.1. The *orbit* of an element $s \in S$ is the set

$$\text{orb}(s) = \{g \cdot s \mid g \in G\} \subset S.$$

Theorem 3.2. *For $y \in \text{orb}(x)$, the orbit of y is equal to the orbit of x.*

Proof. For $y \in \text{orb}(x)$, there exists some $g_1 \in G$ such $g_1x = y$. We can also write this as $x = g_1^{-1}y$ by left-multiplication with g^{-1}. For $z \in \text{orb}(y)$, there exists some $h \in G$ such that $hy = z$. By substituting $gx = y$ into the equation, we get $ghx = z$. By closure, $gh \in G$, so $z \in \text{orb}(x)$ and $\text{orb}(x) \subseteq \text{orb}(y)$.

Similarly, for $w \in \text{orb}(x)$ where $w \neq y$, there exists some $g_2 \in G$ such that $g_2x = w$. Substituting $x = g_1^{-1}y$, we see that $g_2g_1^{-1}y = w$. By closure, $g_2g_1^{-1} \in G$ so $w \in \text{orb}(y)$ and $\text{orb}(x) \subseteq \text{orb}(y)$.

Since $\text{orb}(x) \subseteq \text{orb}(y)$ and $\text{orb}(y) \subseteq \text{orb}(x)$, $\text{orb}(y) = \text{orb}(x)$. □

Definition 3.3. The *stabilizer* of an element $s \in S$ is the set

$$\text{stab}(s) = \{g \in G \colon g \cdot s = s\}$$

Theorem 3.4. *For any element $s \in S$, the stabilizer $\text{stab}(s) \subset G$ is a subgroup of G.*

Proof. We check all the group properties.

(i) *Closure:* Let $g, h \in \text{stab}(s)$. Then,

$$g \cdot h \cdot s = g \cdot (h \cdot s) = g \cdot s = s.$$

Therefore, $g \cdot h \in \text{stab}(s)$.

(ii) *Identity:* For identity $e \in G$, we have $e \cdot s = s$. Therefore, $e \in \text{stab}(s)$.

(iii) *Inverse:* Let $g \in \text{stab}(s)$. Then $g \cdot s = s$. Left-multiplication by g^{-1} gives $e \cdot s = s = g^{-1} \cdot s$. Therefore, $g^{-1} \in \text{stab}(s)$.

□

Theorem 3.5 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group acting on a set S. Then, for any $s \in S$,*

$$|G| = |\operatorname{orb}(s)| \cdot |\operatorname{stab}(s)|$$

Proof. For every $x \in \operatorname{orb}(s)$, define $H_x = \{g \in G \colon gs = x\}$. We know that H_x and H_y are disjoint whenever $x, y \in \operatorname{orb}(s)$ and $x \neq y$ because if $g \in H_x \cap H_y$, then $x = gs = y$.

For each $x \in \operatorname{orb}(s)$, the set H_x is a subset of G. Hence the union $\bigcup_{x \in \operatorname{orb}(s)} H_x$ is a subset of G.

If $g \in G$, then we have $gs = x$ for some $x \in S$, which gives us that $x \in \operatorname{orb}(s)$ and hence, that $g \in H_x$. Thus,

$$G \subseteq \bigcup_{x \in \operatorname{orb}(s)} H_x.$$

$$G = \bigcup_{x \in \operatorname{orb}(s)} H_x, \text{ so } |G| = \sum_{x \in \operatorname{orb}(s)} |H_x|$$

Note that $s \in \operatorname{orb}(s)$ and H_s is the stabilizer of s. We will now show that $|H_x| = |H_s|$ by creating a bijective map between the two.[1]

Let $h \in \operatorname{stab}(s)$ and pick some $g \in H_x$. Define a map $\varphi : \operatorname{stab}(s) \longrightarrow H_x$ by $h \mapsto gh$

We must prove this is a bijection. To prove it is injective, assume that $\varphi(a_1) = \varphi(a_2)$ for $a_1, a_2 \in \operatorname{stab}(s)$. We will show that $a_1 = a_2$.

$$\varphi(a_1) = ga_1, \varphi(a_2) = ga_2 . ga_1 = ga_2$$

Left-multiplying by g^{-1} gives $a_1 = a_2$.

To see that φ is surjective, let $h \in H_x$ and consider the element $g^{-1}h$. Now, $gs = x$ as $g \in H_x$, implying that $g^{-1}x = s$ (by left multiplication by g^{-1}. Since $hs = x$, we can substitute for x in the equation, getting $g^{-1}hs = s$. Thus, $g^{-1}h \in \operatorname{stab}(s)$. Furthermore, $g(g^{-1}h) = h$.

Our map is both surjective and injective, so we know it is bijective. Since φ is bijective, we see that

$$|G| = \sum_{x \in \operatorname{orb}(s)} |H_y| = \sum_{x \in \operatorname{orb}(s)} |\operatorname{stab}(s)| = |\operatorname{orb}(s)| \cdot |\operatorname{stab}(s)|.$$ □

4 Burnside's Lemma

Once again, let G be a group acting on a set S.

Definition 4.1. For an element $g \in G$, a *fixed point* of a set S is an element $s \in S$ such that $gs = s$. In other words, s is unchanged by the group operation. We denote the set of points in S fixed by g as $\operatorname{fix}(g)$.

Definition 4.2. For a group G that acts on set S, let S/G be the set of orbits of S.

Theorem 4.3 (Burnside's Lemma)**.** *For a finite group G that acts on a finite set S, we have*

$$|S/G| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{fix}(g)|.$$

[1] Recall that two functions are bijective if and only if each element in the domain corresponds to exactly one element in the range.

Proof. We write the sum $\sum_{g\in G}|\operatorname{fix}(g)|$ as a sum over all the elements of S:

$$\begin{aligned}\sum_{g\in G}|\operatorname{fix}(g)| &= \sum_{g\in G}|\{s\in S : gs = s\}| \\ &= |\{(g,s) : g\in G, s\in S, gs = s\}| \\ &= \sum_{s\in S}|\{g\in G : gs = s\}|.\end{aligned}$$

The stabilizer of s is $\{g\in G : gs = s\}$, so we make the substitution to get

$$\sum_{g\in G}|\operatorname{fix}(g)| = \sum_{s\in S}|\{g\in G : gs = s\}| = \sum_{s\in S}|\operatorname{stab}(s)|.$$

We can write $|S/G|$ as a similar sum. Since $|\operatorname{orb}(s)|$ represents the size of the orbit for s, each s in the orbit contributes $\frac{1}{|\operatorname{orb}(s)|}$ to the total sum for that orbit. Thus, if the sum of all the s in a given orbit always equals to 1, then the total sum of $\sum_{s\in S}\frac{1}{|\operatorname{orb}(s)|}$ equals the total number of orbits, $|S/G|$. So, we have

$$|S/G| = \sum_{s\in S}\frac{1}{|\operatorname{orb}(s)|}.$$

By the Orbit-Stabilizer theorem, we can rewrite this as

$$|S/G| = \sum_{s\in S}\frac{1}{|\operatorname{orb}(s)|} = \sum_{s\in S}\frac{1}{\frac{|G|}{|\operatorname{stab}(s)|}} = \sum_{s\in S}\frac{|\operatorname{stab}(s)|}{|G|} = \frac{1}{|G|}\sum_{s\in S}|\operatorname{stab}(s)|.$$

Since $\sum_{s\in S}|\operatorname{stab}(s)| = \sum_{g\in G}|\operatorname{fix}(g)|$, we substitute and get

$$|S/G| = \frac{1}{|G|}\sum_{g\in G}|\operatorname{fix}(g)|,$$

as desired. □

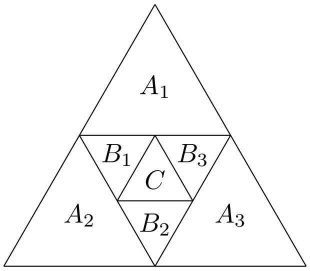
5 Applications of Burnside's Lemma

Burnside's Lemma can be applied to a variety of counting problems.

5.1 Coloring Problems

Burnside's Lemma can be used to solve problems about the number of ways to color various geometric patterns.

Example 5.1 (triangles with n colors)**.** We compute the number of distinct colorings of the regions of equilateral triangular tile below, up to rotation and reflection, with n colors. The group of symmetries of the triangle is D_3. The order of D_3 is 6.



We investigate fix(g), the number of colorings fixed under each group element $g \in D_3$.

The identity fixes every coloring. Since there are 7 regions and n colors, $\text{fix}(e) = n^7$.

For a coloring to be fixed under rot 120°, each of the regions A_n and B_n must be the same color, while C can be any color. Thus, $\text{fix}(\text{rot}\,120°) = n^3$. Similarly, $\text{fix}(\text{rot}(-120°)) = n^3$.

There are three group elements that reflect across a line of symmetry of the triangle. Without loss of generality, let us consider the group element that reflects across the line of symmetry from the top most vertex to the midpoint of the side opposite to it. We call this group element ref. For the coloring to be fixed under ref, regions A_2 and A_3 must be the same, as well as regions B_1 and B_3. The other regions can be any color. Thus, $\text{fix}(\text{ref}) = n^5$.

Since the number of colorings is equal to the number of orbits of D_3, we can use Burnside's Lemma to get

$$\text{Number of colorings} = \frac{1}{|D_3|}\sum_{g\in D_3} |\,\text{fix}(g)| = \boxed{\frac{1}{6}(n^7 + 3n^5 + 2n^3)}.$$

Example 5.2 (triangles with a fixed set of colors)**.** We compute the number of distinct colorings of the regions of equilateral triangular tile in 5.1 so that there are four blue regions and three green regions.

We investigate fix(g), the number of colorings fixed under each group element $g \in D_3$ using methods similar to those employed in Example 5.1:

$$\begin{array}{lr} e: & \text{fix}(e) = \binom{7}{4} = 35 \\ \text{rot}\pm 120°: & 2\cdot\text{fix}(\text{rot}\,120°) = 2\cdot 2 = 4 \\ 3\,\text{ref}: & 3\cdot\text{fix}(\text{ref}) = 3\cdot 7 = 21 \end{array}$$

Since the number of colorings is equal to the number of orbits of D_3, we can use Burnside's Lemma to get

$$\text{Number of colorings} = \frac{1}{|D_3|}\sum_{g\in D_3} |\,\text{fix}(g)| = \frac{35+4+21}{6} = \boxed{10}.$$

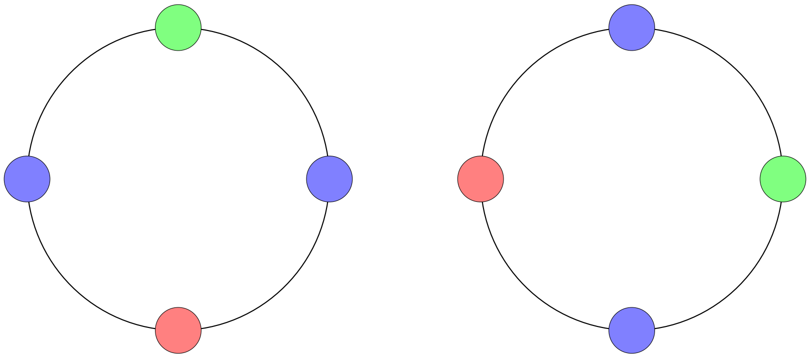
5.2 Necklace Problems

Burnside's Lemma can also be used to solve problems about the number of unique necklaces that can be made using various colors and numbers of beads. In the following, we let C be a set of *colors* that we are allowed to use for our necklaces.

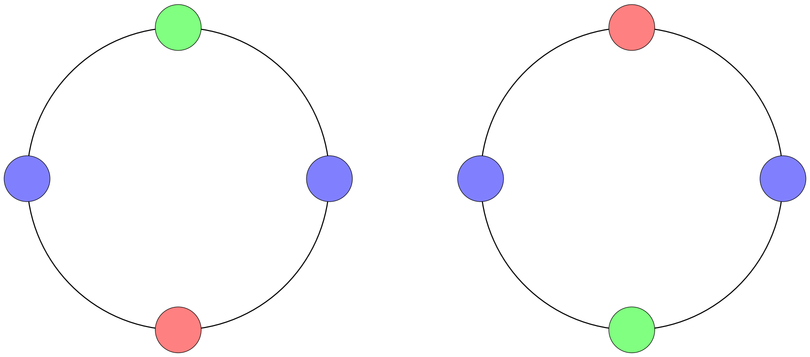
Definition 5.3. Let C be a set. A *necklace* with colors in C is a finite sequence $x_1 \dots x_n$ of elements of C. We say two necklaces are the same if one is a *rotation* $x_i x_{i+1} \dots x_{n+i-1}$ or *reflection* $x_{2i}x_{2i-1}x_{2i-2}\dots x_{2i-n}$ of the other, taking subscripts mod n.

Definition 5.4. A *bead* is a color on a necklace.

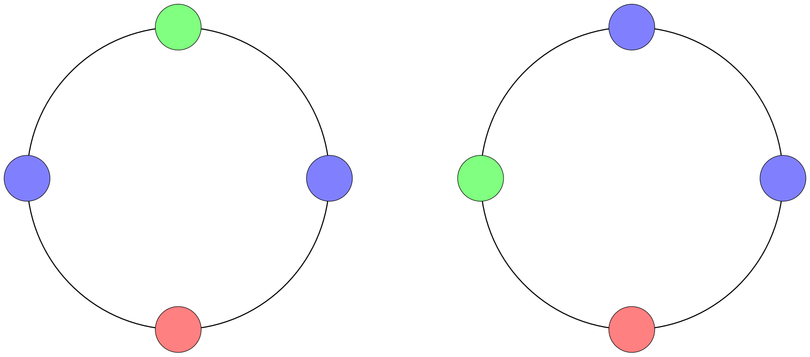
Example 5.5 (when necklaces are the same)**.** We investigate when necklaces are the same.



The two necklaces above are the same, as they are rotations of another.



The two necklaces above are the same, as they are each reflections of another.



The two necklaces above are *not* the same, as no sequence of rotations and reflections will turn one into another.

Example 5.6 (necklaces with n colors)**.** We compute the number of distinct necklaces with 6 beads and n possible colors for each bead. The group of symmetries of a 6-bead necklace is D_6. The order of D_6 is 12.

We investigate $\text{fix}(g)$, the number of necklaces fixed under each group element $g \in D_6$. For a necklace to be fixed under the group element $\text{rot}\,60°$, the second bead must be the same color as the first bead, the third the same as the second, the fourth the same as the third, and so on. Thus, all of the beads on the necklace must be the same color, so $\text{fix}(\text{rot}\,60°) = n$. Using similar methods to find $\text{fix}(g)$ for the rest of the group elements, we have

$$\begin{array}{lr} e: & \text{fix}(e) = n^6 \\ \text{rot}\,\pm 60° : & 2 \cdot \text{fix}(\text{rot}\,60°) = 2n \\ \text{rot}\,\pm 120° : & 2 \cdot \text{fix}(\text{rot}\,120°) = 2n^2 \\ \text{rot}\,180° : & \text{fix}(\text{rot}\,180°) = n^3 \\ \text{ref}(3): & 3 \cdot \text{fix}(\text{ref}) = 3n^4 \\ \text{ref}(3): & 3 \cdot \text{fix}(\text{ref}) = 3n^3 \end{array}$$

Since the number of necklaces is equal to the number of orbits of D_6, we can use Burnside's Lemma to get

$$\text{Number of necklaces} = \frac{1}{|D_6|} \sum_{g \in D_6} |\,\text{fix}(g)| = \boxed{\frac{1}{12}(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n)}.$$

Example 5.7 (necklaces with a fixed set of beads)**.** We compute the number of distinct necklaces with 2 red beads, 2 green beads, and 2 blue beads. As in Example 5.4, the group of symmetries of a 6-bead necklace is D_6, which has order 12.

We investigate fix(g), the number of necklaces fixed under each group element $g \in D_6$, using methods similar to those employed in Example 5.6:

$$\begin{array}{lr} e: & \operatorname{fix}(e) = \binom{6}{2\ 2\ 2} = 90 \\ \operatorname{rot} \pm 120^\circ: & 2 \cdot \operatorname{fix}(\operatorname{rot} 120^\circ) = 0 \\ \operatorname{rot} 180^\circ: & \operatorname{fix}(\operatorname{rot} 180^\circ) = 6 \\ \operatorname{rot} \pm 60^\circ: & 2 \cdot \operatorname{fix}(\operatorname{rot} 60^\circ) = 0 \\ \operatorname{ref}(6): & 6 \cdot \operatorname{fix}(\operatorname{ref}) = 6 \cdot 6 = 36 \end{array}$$

Since the number of necklaces is equal to the number of orbits of D_6, we can use Burnside's Lemma to get

$$\text{Number of necklaces} = \frac{1}{|D_6|} \sum_{g \in D_6} |\operatorname{fix}(g)| = \frac{1}{12}(90 + 6 + 36) = \boxed{11}.$$

Definition 5.8. *Euler's totient function* (denoted $\varphi(n)$) computes the number of integers less than n that are relatively prime to n (or equivalently, the number of integers a such that $gcd(a, n) = 1$). We can evaluate $\varphi(n)$ for some n by finding the product of the reciprocal of each of its prime factors subtracted from one.

If $n = p_1 \ldots p_m$ then

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right).$$

Example 5.9 (necklaces with a variable number of beads and colors)**.** We compute an expression for the number of necklaces with n beads and k colors.

Let us consider the rotation group for n beads, which has order n. If we have n beads then the elements of the rotation group are rotations by $2\pi r/d$ radians for d that divides n and r relatively prime to d. Now, we compute the size of the fixed set for a rotation by r/d of a circle. If we have a rotation r/d, then every bead that is congruent modulo n/d must be the same color. This gives us n/d possible colors to choose from.

From Burnside's Lemma, the number of necklaces fixed under rotations would be

$$\frac{1}{n} \sum_{d|n} \sum_{\substack{1 \le r \le d \\ \gcd(r,d)=1}} k^{n/d}.$$

Since $\varphi(d)$ represents the number of integers relatively prime to n that are less that n, we can rewrite the expression for fixed necklaces (necklaces that can't be flipped) as

$$\frac{1}{n} \sum_{d|n} \varphi(d) k^{n/d}.$$

If we have reflections and n is odd, then the fixed set of each reflection is $k^{1+\lfloor n/2 \rfloor} = k^{(n+1)/2}$. The size of the rotation and reflection group is $2n$ because there are n rotations and n reflections. Summing together the fixed sets for both rotations and reflections, we get the total number of necklaces.

If n is odd, the total number of necklaces is

$$\boxed{\frac{1}{2n} \left(\sum_{d|n} \varphi(d) k^{n/d} + n k^{(n+1)/2} \right)}.$$

If n is even, the fixed sets are $k^{n/2}$ if the line of reflection does not pass through any beads or $k^{(n+2)/2}$ if the line of reflection passes through two beads. There are $n/2$ lines that don't pass through any beads and $n/2$ lines that pass through two beads. Thus, the total number of necklaces if n is even is

$$\boxed{\frac{1}{2n} \left(\sum_{d|n} \varphi(d) k^{n/d} + \frac{n}{2} k^{n/2} + \frac{n}{2} k^{(n+2)/2} \right)}.$$

6 Sylow Theorems

In this section, we use p to refer to a chosen prime. Reference 4 (Algebra by Michael Artin) was used for much of the proofs of the Sylow Theorems.

Definition 6.1. The orbit of $h \in H$ under conjugation by a group G is the set of conjugate subgroups gHg^{-1} with $g \in G$.

Definition 6.2. The stabilizer of H under conjugation by G is called the *normalizer* and is denoted by $N(H)$:

$$N(H) = \{g \in G | gHg^{-1} = H\}$$

Remark 6.3. Lagrange's theorem, a proof of which can be found in [3], states that for a finite group G and H a subgroup of G, the order of H is a factor of the order of G. This implies that Sylow p-subgroups of a group G are in fact maximal p-subgroups of G.

Definition 6.4. A finite group is a *p-group* if it has order p^n for some positive integer n.

Definition 6.5. The Sylow p-subgroups of a group is the maximal subgroup of order p^n for a chosen prime number p and where n is a positive integer.

Corollary 6.6. *Every element in a Sylow p-subgroup has order p^m for some prime p and whole number m.*

Proof. The order of an element divides the order of the whole group. Therefore, the order of any element in a finite Sylow p-subgroup must be p^m such that $m < n$.

□

Definition 6.7. Let group G have order $p^e m$ such that $p \nmid m$. A *Sylow p-group* of group G is a subgroup H of order p^e.

Theorem 6.8 (First Sylow Theorem)**.** *A finite group whose order is divisible by a prime p contains a Sylow p-subgroup.*

Proof. Let S be the set of subsets of G of size p^e. G acts upon S by left multiplication. The number $|S|$ is the binomial coefficient

$$\binom{p^e m}{p^e} = \frac{p^e m}{p^e} \times \frac{p^e m - 1}{p^e - 1} \times \cdots \times \frac{p^e m - k}{p^e - k} \times \cdots \times \frac{p^e m - p^e + 1}{1}$$

For each term, $p^e m - k \equiv p^e - k (mod p)$, so the numerator and denominator contain the same number of factors of p. Therefore, $p \nmid |S|$.

Let $U \in S$ be a subset of size p^e such that $p \nmid |\operatorname{orb}(U)|$. Let $H = \operatorname{stab}(U)$.

By Orbit Stabilizer Theorem, we can write that $|U| = |\operatorname{orb}(U)| \times |\operatorname{stab}(U)|$. We know that $|U| = p^e$ and p does not divide $|\operatorname{orb}(U)|$, so p^e divides $|H|$.

We can partition U into right cosets of H of the form Hu for $u \in U$, and we can write this as

$$U = \bigcup_{u \in U} Hu$$

Since $|U| = p^e$, $|Hu|$ divides p^e. Because $|Hu| = |H|, |H|$ divides p^e. Therefore, $|H| = p^e$, and we have found a Sylow p-subgroup.

□

Theorem 6.9 (Second Sylow Theorem)**.** *All Sylow p-subgroups are conjugate.*

Proof. Given Sylow p-subgroups H and K of G, G acts on $S = gH$ by left multiplication such that

(i) there is an element of S stabilized by H

(ii) it is transitive: for any $s_1, s_2 \in S$, there is a g with $s_2 = gs_1$.

Then, K operates on S. Since $p \nmid |S| = m$, there is an orbit with size relatively prime to p. Furthermore, since the size of that orbit divides $|K| = p^e$, said orbit size is 1.

Let K fix $H' = gH$. We get $K \subseteq \text{stab}(gH)$. Let $gHg^{-1} = \{ghg^{-1} : h \in H\}$. Since $\text{stab}_G H = H$, we have $\text{stab}_G H = gHg^{-1}$. Thus, $K \subseteq gHg^{-1}$, and $|K| - |gHg^{-1}| = p^e$. So, $K = gHg^{-1}$, as desired. □

Definition 6.10. Let G be a group. A subgroup $H \subset G$ is *normal* if for all $g \in G$ we have $gHg^{-1} \in H$. Alternatively, we can write this as $gH = Hg$.

Corollary 6.11. *If a group G has a normal Sylow p-subgroup H, then H is the only Sylow p-subgroup of G.*

Proof. By the second Sylow theorem, we can get all Sylow p-subgroups of a given group by looking at the conjugates of one Sylow p-subgroup.

Let $g \in G$. For all g, $gHg^{-1} = H$, so H is only conjugate to itself. thus, H is the only Sylow p-subgroup of G. □

Theorem 6.12 (Third Sylow Theorem)**.** *The number of Sylow p-subgroups is* $1 \pmod p$.

Proof. Let H be a Sylow p-subgroup of G. Both G and H act upon the Sylow p-subgroups of G by conjugation. Let us partition the set of Sylow p-subgroups into their orbits under conjugation by H. By the Orbit Stabilizer theorem, the size of each orbit divides $|H| = p^e$, so each orbit has either size 1, or size p^n for some positive $n < e$.

Orbits of size p^n contribute $0 \pmod p$ to the number of Sylow p-subgroups of G, so it suffices to show that H only fixes H under conjugation, and thus, the size of its orbit is equal to 1. To show this, let's assume that H also fixes a different Sylow p-subgroup, K.

H is in the normalizer of K, or $H \in N(K)$. Both H and K are Sylow p-subgroups of $N(K)$, but K is a normal subgroup of $N(K)$. By 6.11, K is the only Sylow p-subgroup of G, so $H = K$. □

7 Acknowledgements

We would like to thank Peter Haine and the MIT PRIMES Circle program, as well as our mentor, Maya Sankar. In addition, we would like to thank our parents for supporting us and driving us to MIT every week.

References

[1] Jenny Jin. Analysis and Applications of Burnside's Lemma. 2018.

[2] Rahbar Virk. The Orbit-Stabilizer Theorem.

[3] Camilla and David Jordan. *Groups.* Modular Mathematics. Newnes, 1994.

[4] Micheal Artin. *Algebra.* 2011.