Square Coloring up to Rotations

An Introduction to Groups and Burnside's Lemma

Akash Dhiraj

Math Circle

Overview

The Plan

Big Question 1.

Consider a cube and 6 arbitrary, distinct colours. We'll colour the sides of our cube using these six colours. Suppose two colorings of our cube are considered the same if we can rotate one colored cube onto the other. How many such cubes exists? What if we swap 6 with n?

The Plan

Big Question 1.

Consider a cube and 6 arbitrary, distinct colours. We'll colour the sides of our cube using these six colours. Suppose two colorings of our cube are considered the same if we can rotate one colored cube onto the other. How many such cubes exists? What if we swap 6 with n?

Related Question 2 (AIME 1996).

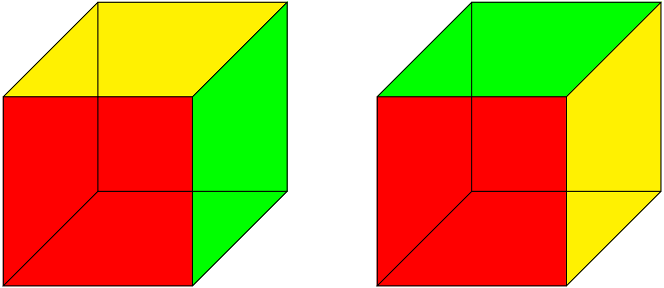
Two of the squares of a 7×7 checkerboard are painted yellow, and the rest are painted green. Two color schemes are equivalent if one can be obtained from the other by applying a rotation in the plane of the board. How many inequivalent color schemes are possible?

These problems motivate all further discussion. Broadly, there are two lines of attack for them: case bashing and case bashing with a bit of elegance. These lectures will be on this *bit of elegance*.

The Plan

Big Question 1.

Consider a cube and 6 arbitrary, distinct colours. We'll colour the sides of our cube using these six colours. Suppose two colorings of our cube are considered the same if we can rotate one colored cube onto the other. How many such cubes exists? What if we swap 6 with n?



(a) (b)

Figure: two of the same colorings (opposite sides are the same colour here)

Part 1

Groups: What are they?

Groups! What are they?

Definition 1 (Group).

A group is a set G with binary operation $\circ : G \times G \to G$, i.e. for $g, h \in G$, there is a well defined element $g \circ h \in G$, more commonly written as gh. Groups satisfy the following axioms:

Groups! What are they?

Definition 1 (Group).

A group is a set G with binary operation $\circ : G \times G \to G$, i.e. for $g, h \in G$, there is a well defined element $g \circ h \in G$, more commonly written as gh. Groups satisfy the following axioms:

(1) There exists $e \in G$ such that, for all $g \in G$, $e \circ g = g \circ e = g$. Such e is called the *identity element*.

Groups! What are they?

Definition 1 (Group).

A group is a set G with binary operation $\circ : G \times G \to G$, i.e. for $g, h \in G$, there is a well defined element $g \circ h \in G$, more commonly written as gh. Groups satisfy the following axioms:

(1) There exists $e \in G$ such that, for all $g \in G$, $e \circ g = g \circ e = g$. Such e is called the *identity element*.

(2) For all $g \in G$, we have a left and right *inverse* g^{-1}. I.e. $g \circ g^{-1} = g^{-1} \circ g = e$.

Groups! What are they?

Definition 1 (Group).

A group is a set G with binary operation $\circ : G \times G \to G$, i.e. for $g, h \in G$, there is a well defined element $g \circ h \in G$, more commonly written as gh. Groups satisfy the following axioms:

(1) There exists $e \in G$ such that, for all $g \in G$, $e \circ g = g \circ e = g$. Such e is called the *identity element*.

(2) For all $g \in G$, we have a left and right *inverse* g^{-1}. I.e. $g \circ g^{-1} = g^{-1} \circ g = e$.

(3) $\circ$ is *associative*. I.e for all $g, g', g'' \in G$, $g(g'g'') = (gg')g''$. Intuitively, this just means that it doesn't matter what order we do the operation $\circ$.

Groups! What are they?

Definition 1 (Group).

A group is a set G with binary operation $\circ : G \times G \to G$, i.e. for $g, h \in G$, there is a well defined element $g \circ h \in G$, more commonly written as gh. Groups satisfy the following axioms:

(1) There exists $e \in G$ such that, for all $g \in G$, $e \circ g = g \circ e = g$. Such e is called the *identity element*.

(2) For all $g \in G$, we have a left and right *inverse* g^{-1}. I.e. $g \circ g^{-1} = g^{-1} \circ g = e$.

(3) $\circ$ is *associative*. I.e for all $g, g', g'' \in G$, $g(g'g'') = (gg')g''$. Intuitively, this just means that it doesn't matter what order we do the operation $\circ$.

Example 2 (Prototypical).

$\mathbb{Z}$ is a group! Remember that the data of a group is both an operation and a set. We'll let our operation be standard addition.

The Integers Modulo n

Example 3 ($\mathbb{Z}/n\mathbb{Z}$).

Recall a special type of equivalence relation between the integers. We said $a \equiv b \pmod{n} \iff n$ divides $a - b$ when we started modular arithmetic.

The Integers Modulo n

Example 3 ($\mathbb{Z}/n\mathbb{Z}$).

Recall a special type of equivalence relation between the integers. We said $a \equiv b \pmod{n} \iff n$ divides $a - b$ when we started modular arithmetic. Now, we'll construct the group $\mathbb{Z}/n\mathbb{Z}$. Let n be a positive integer. The elements of our group will be sets of the form

$$a + n\mathbb{Z} = \{m \in \mathbb{Z} \mid m = a + kn, k \in \mathbb{Z}\}$$

for all integer a.

The Integers Modulo n

Example 3 ($\mathbb{Z}/n\mathbb{Z}$).

Recall a special type of equivalence relation between the integers. We said $a \equiv b \pmod{n} \iff n$ divides $a - b$ when we started modular arithmetic. Now, we'll construct the group $\mathbb{Z}/n\mathbb{Z}$. Let n be a positive integer. The elements of our group will be sets of the form

$$a + n\mathbb{Z} = \{m \in \mathbb{Z} \mid m = a + kn, k \in \mathbb{Z}\}$$

for all integer a. There can only be finitely many such sets. This is because there are only finitely many residues modulo n, and, if a and b differ by a multiple of n (i.e. $a \equiv b \pmod{n}$), then $a + n\mathbb{Z} = b + n\mathbb{Z}$.

The Integers Modulo n

Example 3 ($\mathbb{Z}/n\mathbb{Z}$).

Recall a special type of equivalence relation between the integers. We said $a \equiv b \pmod{n} \iff n$ divides $a - b$ when we started modular arithmetic. Now, we'll construct the group $\mathbb{Z}/n\mathbb{Z}$. Let n be a positive integer. The elements of our group will be sets of the form

$$a + n\mathbb{Z} = \{m \in \mathbb{Z} \mid m = a + kn, k \in \mathbb{Z}\}$$

for all integer a. There can only be finitely many such sets. This is because there are only finitely many residues modulo n, and, if a and b differ by a multiple of n (i.e. $a \equiv b \pmod{n}$), then $a + n\mathbb{Z} = b + n\mathbb{Z}$. Now for our operation. First, we'll call the operation $+$ as opposed to the usual $\circ$. Your intuition probably says $a + n\mathbb{Z} + b + n\mathbb{Z} = (a + b) + n\mathbb{Z}$. This is correct. However, we need to put in some work to show this actually makes sense.

The Integers Modulo n

Example 3 ($\mathbb{Z}/n\mathbb{Z}$).

Recall a special type of equivalence relation between the integers. We said $a \equiv b \pmod{n} \iff n$ divides $a - b$ when we started modular arithmetic. Now, we'll construct the group $\mathbb{Z}/n\mathbb{Z}$. Let n be a positive integer. The elements of our group will be sets of the form

$$a + n\mathbb{Z} = \{m \in \mathbb{Z} \mid m = a + kn, k \in \mathbb{Z}\}$$

for all integer a. There can only be finitely many such sets. This is because there are only finitely many residues modulo n, and, if a and b differ by a multiple of n (i.e. $a \equiv b \pmod{n}$), then $a + n\mathbb{Z} = b + n\mathbb{Z}$. Now for our operation. First, we'll call the operation $+$ as opposed to the usual $\circ$. Your intuition probably says $a + n\mathbb{Z} + b + n\mathbb{Z} = (a + b) + n\mathbb{Z}$. This is correct. However, we need to put in some work to show this actually makes sense.

Following my inner lazy mathematician, I'll use this as a PSET problem :)

Symmetric Group

I'll preface this example by noting that S_n is perhaps one of the most important finite groups. You'll see a few reasons for why in the PSET!

Example 4 (S_n).

Symmetric Group

I'll preface this example by noting that S_n is perhaps one of the most important finite groups. You'll see a few reasons for why in the PSET!

Example 4 (S_n).

We denote the symmetric group of degree n S_n. S_n consists of permutations of the set $X = \{1, 2, 3 \ldots, n\}$. A permutation of X is a bijective (one-one and onto) function $f : X \to X$. Naturally, our group operation shall be function composition.

Symmetric Group

I'll preface this example by noting that S_n is perhaps one of the most important finite groups. You'll see a few reasons for why in the PSET!

Example 4 (S_n).

We denote the symmetric group of degree n S_n. S_n consists of permutations of the set $X = \{1, 2, 3 \ldots, n\}$. A permutation of X is a bijective (one-one and onto) function $f : X \to X$. Naturally, our group operation shall be function composition. Two predominant notations for representing permutations exist. We'll start with *Row Notation*. Let's say $n = 5$, and we want to write the permutation f, where $f(1) = 1$, $f(2) = 3$, $f(3) = 2$, $f(4) = 5$, and $f(5) = 4$. Then, we'd write

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}.$$

Symmetric Group

I'll preface this example by noting that S_n is perhaps one of the most important finite groups. You'll see a few reasons for why in the PSET!

Example 4 (S_n).

We denote the symmetric group of degree n S_n. S_n consists of permutations of the set $X = \{1, 2, 3 \ldots, n\}$. A permutation of X is a bijective (one-one and onto) function $f : X \to X$. Naturally, our group operation shall be function composition. Two predominant notations for representing permutations exist. We'll start with *Row Notation*. Let's say $n = 5$, and we want to write the permutation f, where $f(1) = 1$, $f(2) = 3$, $f(3) = 2$, $f(4) = 5$, and $f(5) = 4$. Then, we'd write

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}.$$

More commonly, we use *cyclic notation*, where we write $f = (2, 3)(4, 5)$.

Symmetric Group

I'll preface this example by noting that S_n is perhaps one of the most important finite groups. You'll see a few reasons for why in the PSET!

Example 4 (S_n).

We denote the symmetric group of degree n S_n. S_n consists of permutations of the set $X = \{1, 2, 3 \ldots, n\}$. A permutation of X is a bijective (one-one and onto) function $f : X \to X$. Naturally, our group operation shall be function composition. Two predominant notations for representing permutations exist. We'll start with *Row Notation*. Let's say $n = 5$, and we want to write the permutation f, where $f(1) = 1$, $f(2) = 3$, $f(3) = 2$, $f(4) = 5$, and $f(5) = 4$. Then, we'd write

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}.$$

More commonly, we use *cyclic notation*, where we write $f = (2, 3)(4, 5)$.

I'll elaborate on how cyclic notation works in class with more examples.

Checking the Group Axioms of the Symmetric Group

(1) We hope to show that, for permutations $f, g : X \to X$, $f \circ g : X \to X$ is a permutation. Suppose $\exists x \in X$ such that $f \circ g(x) = f \circ g(x')$. Then,

$$f(g(x)) = f(g(x')) \implies g(x) = g(x') \implies x = x'$$

by the injectivity of f and g. We conclude $f \circ g$ is injective. Consider $x \in X$. By the surjectivity of f and g, $\exists y, z \in X$ such that $f(y) = x$ and $g(z) = y$. Then, $f \circ g(z) = x$, i.e. $f \circ g$ is surjective.

Checking the Group Axioms of the Symmetric Group

(1) We hope to show that, for permutations $f, g : X \to X$, $f \circ g : X \to X$ is a permutation. Suppose $\exists x \in X$ such that $f \circ g(x) = f \circ g(x')$. Then,

$$f(g(x)) = f(g(x')) \implies g(x) = g(x') \implies x = x'$$

by the injectivity of f and g. We conclude $f \circ g$ is injective. Consider $x \in X$. By the surjectivity of f and g, $\exists y, z \in X$ such that $f(y) = x$ and $g(z) = y$. Then, $f \circ g(z) = x$, i.e. $f \circ g$ is surjective.

(2) Our identity element is the permutation that fixes the elements of X. Call this function e. In row notation,

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Checking the Group Axioms of the Symmetric Group

(1) We hope to show that, for permutations $f, g : X \to X$, $f \circ g : X \to X$ is a permutation. Suppose $\exists x \in X$ such that $f \circ g(x) = f \circ g(x')$. Then,

$$f(g(x)) = f(g(x')) \implies g(x) = g(x') \implies x = x'$$

by the injectivity of f and g. We conclude $f \circ g$ is injective. Consider $x \in X$. By the surjectivity of f and g, $\exists y, z \in X$ such that $f(y) = x$ and $g(z) = y$. Then, $f \circ g(z) = x$, i.e. $f \circ g$ is surjective.

(2) Our identity element is the permutation that fixes the elements of X. Call this function e. In row notation,

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

(3) Consider a permuation $f \in S_n$ We'll define the inverse of f $g : X \to X$ such that $f(x) = y \implies g(y) = x$. Our function is well defined and bijective from the bijectivity of f.

Checking the Group Axioms of the Symmetric Group

(1) We hope to show that, for permutations $f, g : X \to X$, $f \circ g : X \to X$ is a permutation. Suppose $\exists x \in X$ such that $f \circ g(x) = f \circ g(x')$. Then,

$$f(g(x)) = f(g(x')) \implies g(x) = g(x') \implies x = x'$$

by the injectivity of f and g. We conclude $f \circ g$ is injective. Consider $x \in X$. By the surjectivity of f and g, $\exists y, z \in X$ such that $f(y) = x$ and $g(z) = y$. Then, $f \circ g(z) = x$, i.e. $f \circ g$ is surjective.

(2) Our identity element is the permutation that fixes the elements of X. Call this function e. In row notation,

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

(3) Consider a permuation $f \in S_n$ We'll define the inverse of f $g : X \to X$ such that $f(x) = y \implies g(y) = x$. Our function is well defined and bijective from the bijectivity of f.

(4) Function composition is associative. For $f, g, h \in S_n$ and $x \in X$, $f \circ (g \circ h)(x) = f(g(h(x))) = (f \circ g) \circ h(x)$.

Short Facts about Groups

(1) *Abelian* groups are groups where the operation is commutative.

Short Facts about Groups

(1) *Abelian* groups are groups where the operation is commutative.

Fun Fact 1.

These groups are named after the mathematician Niels Henrik Abel. He did a lot of neat things. Of particular note is his proof that no polynomials of degree greater than 4 have a solution in terms of radicals!

Short Facts about Groups

(1) *Abelian* groups are groups where the operation is commutative.

Fun Fact 1.

These groups are named after the mathematician Niels Henrik Abel. He did a lot of neat things. Of particular note is his proof that no polynomials of degree greater than 4 have a solution in terms of radicals!

(2) In a group G, for $g \in G$ and $a \in \mathbb{Z}$, we can define exponentiation such that $g^a = \underbrace{g \circ g \circ \cdots \circ g}_{a \text{ times}}$. The order of an element $g \in G$ is the smallest $n \in \mathbb{Z}_{\geq 0}$ such that $g^n = e$, the identity.

Short Facts about Groups

(1) *Abelian* groups are groups where the operation is commutative.

Fun Fact 1.

These groups are named after the mathematician Niels Henrik Abel. He did a lot of neat things. Of particular note is his proof that no polynomials of degree greater than 4 have a solution in terms of radicals!

(2) In a group G, for $g \in G$ and $a \in \mathbb{Z}$, we can define exponentiation such that $g^a = \underbrace{g \circ g \circ \cdots \circ g}_{a \text{ times}}$. The order of an element $g \in G$ is the smallest $n \in \mathbb{Z}_{\geq 0}$ such that $g^n = e$, the identity.

(3) The identity element of a group is unique. Suppose $e, f \in G$ were both identity elements. Then, $e = ef = f$.

Short Facts about Groups

(1) *Abelian* groups are groups where the operation is commutative.

Fun Fact 1.

These groups are named after the mathematician Niels Henrik Abel. He did a lot of neat things. Of particular note is his proof that no polynomials of degree greater than 4 have a solution in terms of radicals!

(2) In a group G, for $g \in G$ and $a \in \mathbb{Z}$, we can define exponentiation such that $g^a = \underbrace{g \circ g \circ \cdots \circ g}_{a \text{ times}}$. The order of an element $g \in G$ is the smallest $n \in \mathbb{Z}_{\geq 0}$ such that $g^n = e$, the identity.

(3) The identity element of a group is unique. Suppose $e, f \in G$ were both identity elements. Then, $e = ef = f$.

(4) Inverses in a group are unique. Suppose h, h' in G were inverses of g. Then, by associativity, $h = hgh' = h'$.

Part 2

Introduction to Group Actions & Burnside's Lemma

Burnside's Lemma

Theorem 5.

Let a finite group G act on a finite set X. Write X/G for the set of orbits in X, and X^g for the set of elements of X fixed by $g \in G$, i.e. $X^g = \{x \in X \mid g \cdot x = x\}$. Then,

$$|G| \times |X/G| = \sum_{g \in G} X^g.$$

Burnside's Lemma

Theorem 5.

Let a finite group G act on a finite set X. Write X/G for the set of orbits in X, and X^g for the set of elements of X fixed by $g \in G$, i.e. $X^g = \{x \in X \mid g \cdot x = x\}$. Then,

$$|G| \times |X/G| = \sum_{g \in G} X^g.$$

What does this mean!? That's what our goal with this section is.

Burnside's Lemma

Theorem 5.

Let a finite group G act on a finite set X. Write X/G for the set of orbits in X, and X^g for the set of elements of X fixed by $g \in G$, i.e. $X^g = \{x \in X \mid g \cdot x = x\}$. Then,

$$|G| \times |X/G| = \sum_{g \in G} X^g.$$

What does this mean!? That's what our goal with this section is.

Fun Fact 2.

Burnside's Lemma was not found by Burnside. It was originally a theorem of Cauchy that was misattributed to Burnside. That's why you'll find that this result is often jokingly referred to as 'not Burnside's Lemma' or 'the theorem that is not Burnside's'

Subgroups

The most natural way to define 'subgroup' is a subset who is a group with the same operation. This yields the following definition.

Subgroups

The most natural way to define 'subgroup' is a subset who is a group with the same operation. This yields the following definition.

Definition 6.

A subgroup group of a group G is a subset $H \subseteq G$ such that

(1) for $h_1, h_2 \in H$, $h_1 h_2 \in H$

(2) and, for $h \in H$, $h^{-1} \in H$.

Subgroups

The most natural way to define 'subgroup' is a subset who is a group with the same operation. This yields the following definition.

Definition 6.

A subgroup group of a group G is a subset $H \subseteq G$ such that

(1) for $h_1, h_2 \in H$, $h_1 h_2 \in H$

(2) and, for $h \in H$, $h^{-1} \in H$.

Example 7.

(1) For any group G, the subset $\{e\}$ is a subgroup. It's called the *trivial group*. Similarly, the entire group G is also technically a subgroup.

(2) For any group G and element $g \in G$, $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$ is a subgroup of G. $\langle g \rangle$ is called the cyclic group generated by g.

We say $H \leq G$ when H is a subgroup of G.

Group Actions

Definition 8.

Let X be a set and G a group. An action of G on X is a function $\phi : G \times X \to X$ such that

(1) $\phi(e, x) = x$ for all $x \in X$

(2) and $\phi(g_1 g_2, x) = \phi(g_1, \phi(g_2, x))$.

Group Actions

Definition 8.

Let X be a set and G a group. An action of G on X is a function $\phi : G \times X \to X$ such that

(1) $\phi(e, x) = x$ for all $x \in X$

(2) and $\phi(g_1 g_2, x) = \phi(g_1, \phi(g_2, x))$.

For the sake of simplifying notation, we often drop the "phi". So, instead of $\phi(g, x)$, we usually just write gx.

Group Actions

Definition 8.

Let X be a set and G a group. An action of G on X is a function $\phi : G \times X \to X$ such that

(1) $\phi(e, x) = x$ for all $x \in X$

(2) and $\phi(g_1 g_2, x) = \phi(g_1, \phi(g_2, x))$.

For the sake of simplifying notation, we often drop the "phi". So, instead of $\phi(g, x)$, we usually just write gx. We've actually seen some group actions already!

Example 9 (Prototypical).

Remember the symmetric group S_n? Well, consider the obvious group action on the set $X = \{1, 2, \ldots, n\}$. Since $f \in S_n$ is a permutation of X by definition, we can define our action on X such that, for $x \in X$, $fx = f(x)$.

More Examples

This should make our fairly abstract definition clearer.

Example 10.

More Examples

This should make our fairly abstract definition clearer.

Example 10.

(1) The group D_n acts on the set of vertices of a regular n-gon in the expected way. Recall that the symmetries of an n-gon correspond to specific permutations of the vertices.

More Examples

This should make our fairly abstract definition clearer.

Example 10.

(1) The group D_n acts on the set of vertices of a regular n-gon in the expected way. Recall that the symmetries of an n-gon correspond to specific permutations of the vertices.

(2) $\mathbb{Z}/4\mathbb{Z}$ acts on the $\mathbb{R}^2$ as follows: $0 \cdot (x, y) := (x, y)$, $1 \cdot (x, y) := (y, x)$, $2 \cdot (x, y) := (-x, -y)$, and $3 \cdot (x, y) := (y, -x)$. I.e. $\mathbb{Z}/4\mathbb{Z}$ rotates the plane in $\pi/2$ increments. We can make a similar action with $\mathbb{Z}/n\mathbb{Z}$ and rotations of $2\pi/n$.

More Examples

This should make our fairly abstract definition clearer.

Example 10.

(1) The group D_n acts on the set of vertices of a regular n-gon in the expected way. Recall that the symmetries of an n-gon correspond to specific permutations of the vertices.

(2) $\mathbb{Z}/4\mathbb{Z}$ acts on the $\mathbb{R}^2$ as follows: $0 \cdot (x, y) := (x, y)$, $1 \cdot (x, y) := (y, x)$, $2 \cdot (x, y) := (-x, -y)$, and $3 \cdot (x, y) := (y, -x)$. I.e. $\mathbb{Z}/4\mathbb{Z}$ rotates the plane in $\pi/2$ increments. We can make a similar action with $\mathbb{Z}/n\mathbb{Z}$ and rotations of $2\pi/n$.

(3) Let G be an arbitrary group with group operation $*$. We can make G act on its underlying set (i.e. itself) by left multiplication. That is, for $g \in G$ and $x \in X = G$, $gx := g * x$.

Preliminary Definitions

Let G act on X.

Preliminary Definitions

Let G act on X.

Definition 11 (Orbit).

For $x \in X$, the orbit of x is $\mathcal{O}(x) := \{y \in X \mid \exists g \in G \text{ such that } gx = y\}$.

Think of this as the universe of x or, rather, where x can be sent under G.

Preliminary Definitions

Let G act on X.

Definition 11 (Orbit).

For $x \in X$, the orbit of x is $\mathcal{O}(x) := \{y \in X \mid \exists g \in G \text{ such that } gx = y\}$.

Think of this as the universe of x or, rather, where x can be sent under G.

Definition 12 (Stabilizer).

For $x \in X$, the stabilizer of x is $G_x = \{g \in G \mid gx = x\}$.

In words, the stabilizer of x contains the elements of G that fix or stabilize x.

Preliminary Definitions

Let G act on X.

Definition 11 (Orbit).

For $x \in X$, the orbit of x is $\mathcal{O}(x) := \{y \in X \mid \exists g \in G \text{ such that } gx = y\}$.

Think of this as the universe of x or, rather, where x can be sent under G.

Definition 12 (Stabilizer).

For $x \in X$, the stabilizer of x is $G_x = \{g \in G \mid gx = x\}$.

In words, the stabilizer of x contains the elements of G that fix or stabilize x.

Definition 13 (Coset).

A coset of a subgroup $H \leq G$ is a set of the form $gH := \{gh \mid h \in H\}$, where $g \in G$.

Useful Results

In our proof of Burnside's Lemma, we require two important facts about groups and group actions.

Useful Results

In our proof of Burnside's Lemma, we require two important facts about groups and group actions.

Theorem 14 (Lagrange's Theorem).

Let G be a group and $H \leq G$. Let n be the number of cosets of H. When $|G|$ is finite, $|G| = n|H|$.

Useful Results

In our proof of Burnside's Lemma, we require two important facts about groups and group actions.

Theorem 14 (Lagrange's Theorem).

Let G be a group and $H \leq G$. Let n be the number of cosets of H. When $|G|$ is finite, $|G| = n|H|$.

Theorem 15 (Orbit-Stabilizer Theorem).

Let the finite group G act on the finite set X. For $x \in X$, $|\mathcal{O}(x)| \times |G_x| = |G|$.

Useful Results

In our proof of Burnside's Lemma, we require two important facts about groups and group actions.

Theorem 14 (Lagrange's Theorem).

Let G be a group and $H \leq G$. Let n be the number of cosets of H. When $|G|$ is finite, $|G| = n|H|$.

Theorem 15 (Orbit-Stabilizer Theorem).

Let the finite group G act on the finite set X. For $x \in X$, $|\mathcal{O}(x)| \times |G_x| = |G|$.

We'll omit the proofs from this presentation. We do this not because they are beyond the viewer but because they lead to group theoretical rabbit holes. For the sake of time and clarity, we'll assume their validity. However, do make sure to see their proofs in the write-up 'Group Theory Proofs' on your own time.

Guess Who's Back, Back Again.

We'll prove Burnside's Lemma now. To recap, we're trying to show $|G| \times |X/G| = \sum_{g \in G} X^g$, where X/G are the set of orbits of X under the action of G and $X^g = \{x \in X \mid g \cdot x = x\}$.

Guess Who's Back, Back Again.

We'll prove Burnside's Lemma now. To recap, we're trying to show $|G| \times |X/G| = \sum_{g \in G} X^g$, where X/G are the set of orbits of X under the action of G and $X^g = \{x \in X \mid g \cdot x = x\}$.

Proof.

By the orbit-stabilizer Theorem,

$$\begin{aligned}
\sum_{g \in G} |X^g| &= \sum_{g \in G} |\{x \in X : \; gx = x\}| = |\{(x, g) \in X \times G : \; gx = x\}| \\
&= \sum_{x \in X} |g \in G : \; gx = x| = \sum_{x \in X} |G_x| = |G| \sum_{x \in X} \frac{1}{|\mathcal{O}(x)|} \\
&= |G| \sum_{k \in |X/G|} 1 \\
&= |G| \times |X/G|
\end{aligned}$$

$\blacksquare$

Part 3
Using Burnside's Lemma

The Rotations of a Cube

We'll finally answer Big Question 1. Recall that I asked you to try to categorize the rotations of a cube. The categories I was looking for were

The Rotations of a Cube

We'll finally answer Big Question 1. Recall that I asked you to try to categorize the rotations of a cube. The categories I was looking for were

(1) rotations about an axis passing through the centres of opposite faces,

The Rotations of a Cube

We'll finally answer Big Question 1. Recall that I asked you to try to categorize the rotations of a cube. The categories I was looking for were

(1) rotations about an axis passing through the centres of opposite faces,

(2) rotations about an axis passing through two vertices, and

The Rotations of a Cube

We'll finally answer Big Question 1. Recall that I asked you to try to categorize the rotations of a cube. The categories I was looking for were

(1) rotations about an axis passing through the centres of opposite faces,

(2) rotations about an axis passing through two vertices, and

(3) rotations about an axis passing through the mid-points of edges.

Pull your Rubik's cube out (if you have one) to try and convince yourself of this!

The Rotations of a Cube

We'll finally answer Big Question 1. Recall that I asked you to try to categorize the rotations of a cube. The categories I was looking for were

(1) rotations about an axis passing through the centres of opposite faces,

(2) rotations about an axis passing through two vertices, and

(3) rotations about an axis passing through the mid-points of edges.

Pull your Rubik's cube out (if you have one) to try and convince yourself of this!

Now, let G be the group of rotations of the cube and X the total number of colored cubes (we can use n colors), where two cubes are considered distinct even if they can be rotated onto one another. Clearly, $|X| = n^6$. We'll let G act on X in the standard way: a rotation in $\rho \in G$ sends a given cube to the cube obtained when it's rotated by ρ. Perhaps you can see that answering our question now boils down to determining $|X/G|$ in our group action. This is where Burnside's Lemma comes into play.

Big Question 1

Proposition 16.

$|G| = 24.$

Proposition 17.

$\sum_{g \in G} |X^g| = n^6 + 3n^4 + 12n^3 + 8n^2.$

Big Question 1

Proposition 16.

$|G| = 24$.

Proof.

From inspection, there are $3 \times 3 = 9$ rotations of about an axis passing through the centres of opposite faces, $4 \times 2 = 8$ rotations about an axis passing through two vertices, $6 \times 1 = 6$ rotations about an axis passing through the mid-points of edges, and 1 identity rotation. Use a Rubik's cube (or any other (preferably colored) cube) or your imagination to verify this. Then, we note $9 + 8 + 6 + 1 = 24$. ∎

Proposition 17.

$\sum_{g \in G} |X^g| = n^6 + 3n^4 + 12n^3 + 8n^2$.

Big Question 1

Proposition 16.

$|G| = 24$.

Proof.

From inspection, there are $3 \times 3 = 9$ rotations of about an axis passing through the centres of opposite faces, $4 \times 2 = 8$ rotations about an axis passing through two vertices, $6 \times 1 = 6$ rotations about an axis passing through the mid-points of edges, and 1 identity rotation. Use a Rubik's cube (or any other (preferably colored) cube) or your imagination to verify this. Then, we note $9 + 8 + 6 + 1 = 24$. ■

Proposition 17.

$\sum_{g \in G} |X^g| = n^6 + 3n^4 + 12n^3 + 8n^2$.

We'll leave this for the PSET :) Using these results, we conclude, by Burnside's Lemma, that there are $\frac{n^6+3n^4+12n^3+8n^2}{24}$ distinct cubes.