Lagrange's Theorem

Sasha Patotski

Cornell University

ap744@cornell.edu

December 8, 2015

Group action definition

Definition

Let G be a group and X be a set. An **action** of G on X is a homomorphism $G \to Bij(X)$.

- Equivalently, **action** of G on X is a map $G \times X \to X$, $(g, x) \mapsto g.x$ such that $g.(h.x) = (gh).x$ and $e.x = x$.

Definition

Let G be a group acting on a set X. The **orbit** of $x \in X$ is the set $Gx \subseteq X$, i.e. $Gx = \{g.x \mid g \in G\}$.
For a point $x \in X$, its **stabilizer** G_x is the set $G_x = \{g \in G \mid g.x = x\}$.

Abstract groups are not that abstract

Definition

Let G be a group and X be a set. An **action** of G on X is a homomorphism $G \to Bij(X)$.

Any abstract group G is actually a transformation group.

Indeed, take $X = G$ with $G \times X \to X$ being the multiplication map.

In other words, to a $g \in G$ we associate a function $L_g \colon X \to X$, mapping $h \in X = G$ to $L_g(h) := gh$.

This defines **injective** homomorphism $\varphi \colon G \to Bij(X)$, $g \mapsto L_g$.

Corollary: any finite group is a subgroup of S_n for some n.

Cosets

- **Recall:** there is an action of G on itself by $g.h = L_g(h) = gh$ called **left multiplication**.

Cosets

- **Recall:** there is an action of G on itself by $g.h = L_g(h) = gh$ called **left multiplication**.
- There is a similar action called **right multiplication** given by $g.h = hg^{-1}$. Check that this is an action.

Cosets

- **Recall:** there is an action of G on itself by $g.h = L_g(h) = gh$ called **left multiplication**.
- There is a similar action called **right multiplication** given by $g.h = hg^{-1}$. Check that this is an action.
- What goes wrong if we put $g.h = hg$?

Cosets

- **Recall:** there is an action of G on itself by $g.h = L_g(h) = gh$ called **left multiplication**.
- There is a similar action called **right multiplication** given by $g.h = hg^{-1}$. Check that this is an action.
- What goes wrong if we put $g.h = hg$?
- **Recall:** if a group G acts on a set X, then any subgroup $H \subset G$ also acts on X.

Cosets

- **Recall:** there is an action of G on itself by $g.h = L_g(h) = gh$ called **left multiplication**.
- There is a similar action called **right multiplication** given by $g.h = hg^{-1}$. Check that this is an action.
- What goes wrong if we put $g.h = hg$?
- **Recall:** if a group G acts on a set X, then any subgroup $H \subset G$ also acts on X.

Definition

Let G be a group, and $H \subset G$ be a subgroup. Left (resp. right) **cosets** are the orbits of the right (resp. left) multiplication action of H on G.

Cosets

- **Recall:** there is an action of G on itself by $g.h = L_g(h) = gh$ called **left multiplication**.
- There is a similar action called **right multiplication** given by $g.h = hg^{-1}$. Check that this is an action.
- What goes wrong if we put $g.h = hg$?
- **Recall:** if a group G acts on a set X, then any subgroup $H \subset G$ also acts on X.

Definition

Let G be a group, and $H \subset G$ be a subgroup. Left (resp. right) **cosets** are the orbits of the right (resp. left) multiplication action of H on G.

- In other words, a **left** coset of H in G is gH where $g \in G$ (H is on the **right**).

  A **right** coset of H in G is Hg where $g \in G$ (H is on the **left**).

Cosets

- Note: $H \to gH$ sending $h \mapsto gh$ and $H \to Hg$ sending $h \mapsto hg$ are bijections.

Cosets

- Note: $H \to gH$ sending $h \mapsto gh$ and $H \to Hg$ sending $h \mapsto hg$ are bijections.
- For any $h \in H$, $hH = Hh = H$.

Cosets

- Note: $H \to gH$ sending $h \mapsto gh$ and $H \to Hg$ sending $h \mapsto hg$ are bijections.
- For any $h \in H$, $hH = Hh = H$.
- Let $G = \mathbb{R}^2$, $H = \mathbb{R} \subset G$ be the horizontal axis. Then the (left and right) cosets are horizontal lines.

Cosets

- Note: $H \to gH$ sending $h \mapsto gh$ and $H \to Hg$ sending $h \mapsto hg$ are bijections.
- For any $h \in H$, $hH = Hh = H$.
- Let $G = \mathbb{R}^2$, $H = \mathbb{R} \subset G$ be the horizontal axis. Then the (left and right) cosets are horizontal lines.
- Let $G = \mathbb{Z}$ and $H = \{\ldots, -3, 0, 3, 6, \ldots\}$. What are the cosets?

Cosets

- Note: $H \to gH$ sending $h \mapsto gh$ and $H \to Hg$ sending $h \mapsto hg$ are bijections.
- For any $h \in H$, $hH = Hh = H$.
- Let $G = \mathbb{R}^2$, $H = \mathbb{R} \subset G$ be the horizontal axis. Then the (left and right) cosets are horizontal lines.
- Let $G = \mathbb{Z}$ and $H = \{\ldots, -3, 0, 3, 6, \ldots\}$. What are the cosets?
- Let $G = S_3$ and $H = \{1, (12)\}$. What are the cosets?

Theorem

If two left cosets of H in G intersect, then they coincide, and similarly for right cosets. Thus, G is a disjoint union of left cosets of H and also a disjoint union of right cosets of H.

Theorem

If two left cosets of H in G intersect, then they coincide, and similarly for right cosets. Thus, G is a disjoint union of left cosets of H and also a disjoint union of right cosets of H.

Corollary(Lagrange's theorem) If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. In particular, the order of every element of G divides the order of G.

Theorem

If two left cosets of H in G intersect, then they coincide, and similarly for right cosets. Thus, G is a disjoint union of left cosets of H and also a disjoint union of right cosets of H.

Corollary(Lagrange's theorem) If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. In particular, the order of every element of G divides the order of G.

Proof: $|G|/|H|$ is the number of left (or right) cosets, and so is an integer.

Applications of Lagrange's Theorem

Theorem

For any integers $n \geq 0$ and $0 \leq m \leq n$, the number $\frac{n!}{m!(n-m)!}$ is an integer.

Applications of Lagrange's Theorem

Theorem

For any integers $n \geq 0$ and $0 \leq m \leq n$, the number $\frac{n!}{m!(n-m)!}$ is an integer.

Proof. The group $S_m \times S_{n-m}$ is a subgroup of S_n consisting of the permutations which permute $\{1, 2, \ldots, m\}$ and $\{m+1, \ldots, n\}$.

Applications of Lagrange's Theorem

Theorem

For any integers $n \geq 0$ and $0 \leq m \leq n$, the number $\frac{n!}{m!(n-m)!}$ is an integer.

Proof. The group $S_m \times S_{n-m}$ is a subgroup of S_n consisting of the permutations which permute $\{1, 2, \ldots, m\}$ and $\{m+1, \ldots, n\}$.

This subgroup has $m!(n-m)!$ elements, and Lagrange's theorem gives the result.

Applications of Lagrange's Theorem

Theorem

For any positive integers a, b the ratios $\frac{(ab)!}{(a!)^b}$ and $\frac{(ab)!}{(a!)^b b!}$ are integers.

Applications of Lagrange's Theorem

Theorem

For any positive integers a, b the ratios $\frac{(ab)!}{(a!)^b}$ and $\frac{(ab)!}{(a!)^b b!}$ are integers.

Write the integers from 1 to ab as b groups as follows:

$$1, 2, \ldots, a \mid a+1, \ldots, 2a \mid \ldots \mid (b-1)a+1 \ldots, ba$$

Applications of Lagrange's Theorem

Theorem

For any positive integers a, b the ratios $\frac{(ab)!}{(a!)^b}$ and $\frac{(ab)!}{(a!)^b b!}$ are integers.

Write the integers from 1 to ab as b groups as follows:

$$1, 2, \ldots, a \mid a+1, \ldots, 2a \mid \ldots \mid (b-1)a+1 \ldots, ba$$

There is a subgroup of S_{ab} isomorphic to $\underbrace{S_a \times \cdots \times S_a}_{b \text{ times}}$ consisting of permutations only permuting the numbers within their group. Lagrange's Theorem implies the first result.

Applications of Lagrange's Theorem

Theorem

For any positive integers a, b the ratios $\frac{(ab)!}{(a!)^b}$ and $\frac{(ab)!}{(a!)^b b!}$ are integers.

Write the integers from 1 to ab as b groups as follows:

$$1, 2, \ldots, a \mid a+1, \ldots, 2a \mid \ldots \mid (b-1)a+1 \ldots, ba$$

There is a subgroup of S_{ab} isomorphic to $\underbrace{S_a \times \cdots \times S_a}_{b \text{ times}}$ consisting of permutations only permuting the numbers within their group.
Lagrange's Theorem implies the first result.
There is a subgroup of S_{ab} of permutations allowed to permute the above groups of numbers, and after that only to permute numbers within each group. Note that it's **not!** just $S_b \times S_a^b$.

Applications of Lagrange's Theorem

Theorem

For any positive integers a, b the ratios $\frac{(ab)!}{(a!)^b}$ and $\frac{(ab)!}{(a!)^b b!}$ are integers.

Write the integers from 1 to ab as b groups as follows:

$$1, 2, \ldots, a \mid a+1, \ldots, 2a \mid \ \ldots \ \mid (b-1)a+1 \ldots, ba$$

There is a subgroup of S_{ab} isomorphic to $\underbrace{S_a \times \cdots \times S_a}_{b \text{ times}}$ consisting of permutations only permuting the numbers within their group.
Lagrange's Theorem implies the first result.
There is a subgroup of S_{ab} of permutations allowed to permute the above groups of numbers, and after that only to permute numbers within each group. Note that it's **not!** just $S_b \times S_a^b$.
It has $b!(a!)^b$ elements, and Lagrange Theorem gives the proof of the second statement.

Applications of Lagrange's Theorem

Theorem

For an integer $m > 1$ let $\varphi(m)$ be the number of invertible numbers modulo m. For $m \geq 3$ the number $\varphi(m)$ is even.

Applications of Lagrange's Theorem

Theorem

For an integer $m > 1$ let $\varphi(m)$ be the number of invertible numbers modulo m. For $m \geq 3$ the number $\varphi(m)$ is even.

Invertible numbers modulo m for a group, denoted $(\mathbb{Z}/m)^{\times}$, with group operation given by multiplication.

Applications of Lagrange's Theorem

Theorem

For an integer $m > 1$ let $\varphi(m)$ be the number of invertible numbers modulo m. For $m \geq 3$ the number $\varphi(m)$ is even.

Invertible numbers modulo m for a group, denoted $(\mathbb{Z}/m)^\times$, with group operation given by multiplication.

For $m \geq 3$, $\{\pm 1\}$ is a subgroup of the group $(\mathbb{Z}/m)^\times$.

Applications of Lagrange's Theorem

Theorem

For an integer $m > 1$ let $\varphi(m)$ be the number of invertible numbers modulo m. For $m \geq 3$ the number $\varphi(m)$ is even.

Invertible numbers modulo m for a group, denoted $(\mathbb{Z}/m)^\times$, with group operation given by multiplication.

For $m \geq 3$, $\{\pm 1\}$ is a subgroup of the group $(\mathbb{Z}/m)^\times$.

This subgroup has size 2, so by Lagrange's theorem the number of elements in $(\mathbb{Z}/m)^\times$ is even.

Polya's Enumeration Theorem

Theorem

Suppose that a finite group G acts on a finite set X. Then the number of colorings of X in n colors inequivalent under the action of G is

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

where $c(g)$ is the number of cycles of g as a permutation of X.

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

- What is the number of necklaces with 4 beads of two colors?

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

- What is the number of necklaces with 4 beads of two colors?
- First compute it directly.

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

- What is the number of necklaces with 4 beads of two colors?
- First compute it directly.
- The symmetry group of a square has 8 elements: 4 rotations and 4 reflections.

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

- What is the number of necklaces with 4 beads of two colors?
- First compute it directly.
- The symmetry group of a square has 8 elements: 4 rotations and 4 reflections.
- The identity element has 4 cycles, so it contributes $1 \cdot 2^4 = 16$.

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

- What is the number of necklaces with 4 beads of two colors?
- First compute it directly.
- The symmetry group of a square has 8 elements: 4 rotations and 4 reflections.
- The identity element has 4 cycles, so it contributes $1 \cdot 2^4 = 16$.
- The rotations by $\pi/2$ and $3\pi/2$ have only one cycle, so they contribute $2 \cdot 2^1 = 4$.

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

- What is the number of necklaces with 4 beads of two colors?
- First compute it directly.
- The symmetry group of a square has 8 elements: 4 rotations and 4 reflections.
- The identity element has 4 cycles, so it contributes $1 \cdot 2^4 = 16$.
- The rotations by $\pi/2$ and $3\pi/2$ have only one cycle, so they contribute $2 \cdot 2^1 = 4$.
- The rotation by π has two cycles, so it contributes $1 \cdot 2^2 = 4$.

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

- What is the number of necklaces with 4 beads of two colors?
- First compute it directly.
- The symmetry group of a square has 8 elements: 4 rotations and 4 reflections.
- The identity element has 4 cycles, so it contributes $1 \cdot 2^4 = 16$.
- The rotations by $\pi/2$ and $3\pi/2$ have only one cycle, so they contribute $2 \cdot 2^1 = 4$.
- The rotation by π has two cycles, so it contributes $1 \cdot 2^2 = 4$.
- There are 2 reflections with 2 cycles, and 2 reflections with 3 cycles, with contribute $2 \cdot 2^2 + 2 \cdot 2^3 = 24$.

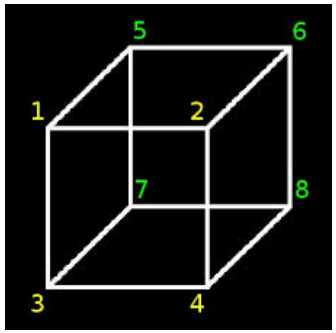
$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

- What is the number of necklaces with 4 beads of two colors?
- First compute it directly.
- The symmetry group of a square has 8 elements: 4 rotations and 4 reflections.
- The identity element has 4 cycles, so it contributes $1 \cdot 2^4 = 16$.
- The rotations by $\pi/2$ and $3\pi/2$ have only one cycle, so they contribute $2 \cdot 2^1 = 4$.
- The rotation by π has two cycles, so it contributes $1 \cdot 2^2 = 4$.
- There are 2 reflections with 2 cycles, and 2 reflections with 3 cycles, with contribute $2 \cdot 2^2 + 2 \cdot 2^3 = 24$.
- Summing up, $N(2) = \frac{1}{8}(16 + 4 + 4 + 24) = 6$.

$$N(n) = \frac{1}{|G|} \sum_{g \in G} n^{c(g)}$$

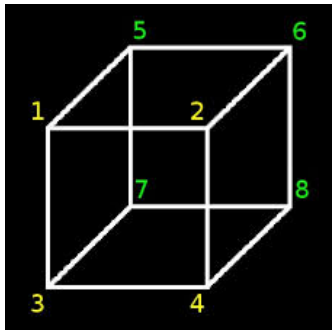
- What is the number of necklaces with 4 beads of two colors?
- First compute it directly.
- The symmetry group of a square has 8 elements: 4 rotations and 4 reflections.
- The identity element has 4 cycles, so it contributes $1 \cdot 2^4 = 16$.
- The rotations by $\pi/2$ and $3\pi/2$ have only one cycle, so they contribute $2 \cdot 2^1 = 4$.
- The rotation by π has two cycles, so it contributes $1 \cdot 2^2 = 4$.
- There are 2 reflections with 2 cycles, and 2 reflections with 3 cycles, with contribute $2 \cdot 2^2 + 2 \cdot 2^3 = 24$.
- Summing up, $N(2) = \frac{1}{8}(16 + 4 + 4 + 24) = 6$.
- For n colors, $N(n) = \frac{n^4+2n^3+3n^2+2n}{8}$. For example, $N(4) = 55$.

One more example



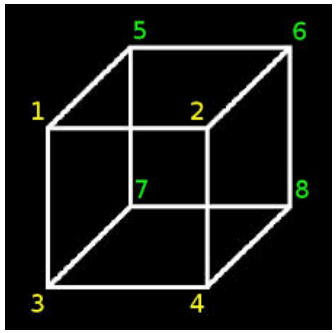
- How many ways are there to color faces of a cube into n colors?

One more example



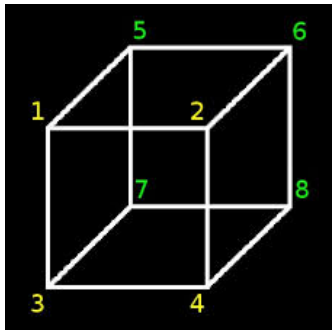
- How many ways are there to color faces of a cube into n colors?
- The element $1 \in S_4$ has 6 cycles, so contributes n^6.

One more example



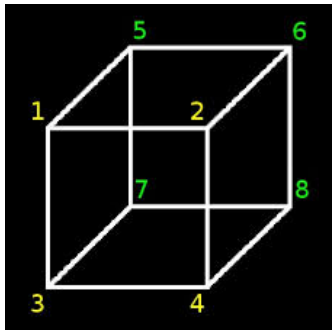
- How many ways are there to color faces of a cube into n colors?
- The element $1 \in S_4$ has 6 cycles, so contributes n^6.
- Rotations by $\pi/2$ and $3\pi/2$ around axes through opposite faces ($2 \cdot 3 = 6$ of them) have 3 cycles, so contribute $6 \cdot n^3$.

One more example



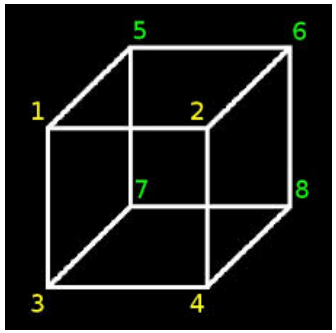
- How many ways are there to color faces of a cube into n colors?
- The element $1 \in S_4$ has 6 cycles, so contributes n^6.
- Rotations by $\pi/2$ and $3\pi/2$ around axes through opposite faces ($2 \cdot 3 = 6$ of them) have 3 cycles, so contribute $6 \cdot n^3$.
- Rotations by π (3 of them) have 4 cycles, so contribute $3 \cdot n^4$.

One more example



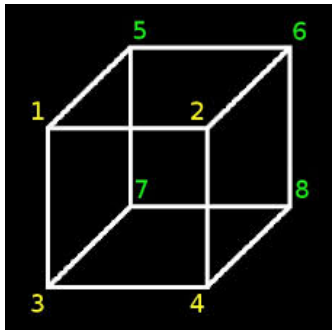
- How many ways are there to color faces of a cube into n colors?
- The element $1 \in S_4$ has 6 cycles, so contributes n^6.
- Rotations by $\pi/2$ and $3\pi/2$ around axes through opposite faces ($2 \cdot 3 = 6$ of them) have 3 cycles, so contribute $6 \cdot n^3$.
- Rotations by π (3 of them) have 4 cycles, so contribute $3 \cdot n^4$.
- Rotations around axes through midpoints of opposite edges (6 of them) have 3 cycles, hence contribute $6 \cdot n^3$.

One more example



- How many ways are there to color faces of a cube into n colors?
- The element $1 \in S_4$ has 6 cycles, so contributes n^6.
- Rotations by $\pi/2$ and $3\pi/2$ around axes through opposite faces ($2 \cdot 3 = 6$ of them) have 3 cycles, so contribute $6 \cdot n^3$.
- Rotations by π (3 of them) have 4 cycles, so contribute $3 \cdot n^4$.
- Rotations around axes through midpoints of opposite edges (6 of them) have 3 cycles, hence contribute $6 \cdot n^3$.
- Rotations around the main diagonals ($4 \cdot 2 = 8$ of them) have 2 cycles, so contribute $8 \cdot n^2$.

One more example



- How many ways are there to color faces of a cube into n colors?
- The element $1 \in S_4$ has 6 cycles, so contributes n^6.
- Rotations by $\pi/2$ and $3\pi/2$ around axes through opposite faces ($2 \cdot 3 = 6$ of them) have 3 cycles, so contribute $6 \cdot n^3$.
- Rotations by π (3 of them) have 4 cycles, so contribute $3 \cdot n^4$.
- Rotations around axes through midpoints of opposite edges (6 of them) have 3 cycles, hence contribute $6 \cdot n^3$.
- Rotations around the main diagonals ($4 \cdot 2 = 8$ of them) have 2 cycles, so contribute $8 \cdot n^2$.
- Summing up, $N(n) = \frac{n^6+3n^4+12n^3+8n^2}{24}$.