Group Theory and the Fifteen Puzzle

Sherry Lim and Mirilla Zhu
Mentored by Margalit Glasgow

April 19, 2018
MIT PRIMES Conference

Group Axioms

Definition

A set G is a group under the operation $\star$ if it satisfies the following properties:

Group Axioms

Definition

A set G is a group under the operation $\star$ if it satisfies the following properties:

- Closure: If $a, b \in G$, then $a \star b \in G$.

Group Axioms

Definition

A set G is a group under the operation $\star$ if it satisfies the following properties:

- Closure: If $a, b \in G$, then $a \star b \in G$.
- Identity: There exists $e \in G$ such that for all $a \in G$, $a \star e = e \star a = a$.

Group Axioms

Definition

A set G is a group under the operation $\star$ if it satisfies the following properties:

- Closure: If $a, b \in G$, then $a \star b \in G$.
- Identity: There exists $e \in G$ such that for all $a \in G$, $a \star e = e \star a = a$.
- Inverse: For all $a \in G$, there exists $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.

Group Axioms

Definition

A set G is a group under the operation $\star$ if it satisfies the following properties:

- Closure: If $a, b \in G$, then $a \star b \in G$.
- Identity: There exists $e \in G$ such that for all $a \in G$, $a \star e = e \star a = a$.
- Inverse: For all $a \in G$, there exists $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.
- Associativity: For all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.

The Fifteen Puzzle

The unscrambled Fifteen Puzzle looks like this:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

We move the tiles by sliding the empty slot.

The Fifteen Puzzle

The unscrambled Fifteen Puzzle looks like this:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

We move the tiles by sliding the empty slot.

Question

Which configurations of tiles can we achieve on the Fifteen Puzzle?

The Fifteen Puzzle (cont.)

Proposition

The set of moves that leave cell 16 empty on the Fifteen Puzzle forms a group, with the group operation being the composition of moves.

Let P denote the set.

Proposition

The set of moves that leave cell 16 empty on the Fifteen Puzzle forms a group, with the group operation being the composition of moves.

Let P denote the set.

- Closure: If $a, b \in P$, then $a * b$ is another scrambled state with cell 16 empty.

The Fifteen Puzzle (cont.)

Proposition

The set of moves that leave cell 16 empty on the Fifteen Puzzle forms a group, with the group operation being the composition of moves.

Let P denote the set.

- Closure: If $a, b \in P$, then $a * b$ is another scrambled state with cell 16 empty.
- Identity: The default state is the identity element.

The Fifteen Puzzle (cont.)

Proposition

The set of moves that leave cell 16 empty on the Fifteen Puzzle forms a group, with the group operation being the composition of moves.

Let P denote the set.

- Closure: If $a, b \in P$, then $a * b$ is another scrambled state with cell 16 empty.
- Identity: The default state is the identity element.
- Inverse: Every move is reversible.

Permutations

Definition

A function σ is a *permutation* of a finite set S if it is a reordering of the elements of S.

Permutations

Definition

A function σ is a *permutation* of a finite set S if it is a reordering of the elements of S.

Example

Suppose that σ is represented by the following map:

n	1	2	3	4	5	6
$\sigma(n)$	4	3	2	6	1	5

Permutations

Definition

A function σ is a *permutation* of a finite set S if it is a reordering of the elements of S.

Example

Suppose that σ is represented by the following map:

n	1	2	3	4	5	6
$\sigma(n)$	4	3	2	6	1	5

Then we can represent σ as $(1\ 4\ 6\ 5)(2\ 3)$.

Permutations

Definition

A function σ is a *permutation* of a finite set S if it is a reordering of the elements of S.

Example

Suppose that σ is represented by the following map:

n	1	2	3	4	5	6
$\sigma(n)$	4	3	2	6	1	5

Then we can represent σ as $(1\ 4\ 6\ 5)(2\ 3)$.

Proposition

The set of permutations on n elements forms a group under composition. This group is called the *symmetric group* S_n.

Transpositions

Definition

A *transposition* is a two-cycle of the form (a b).

Transpositions

Definition

A *transposition* is a two-cycle of the form (a b).

Proposition

Any permutation σ can be written as a product of transpositions.

Transpositions

Definition

A *transposition* is a two-cycle of the form (a b).

Proposition

Any permutation σ can be written as a product of transpositions.

Example

$(1\ 5\ 2\ 4) = (1\ 4)(1\ 2)(1\ 5)$

Transpositions (cont.)

Question

Are transposition representations of permutations unique?

Transpositions (cont.)

Question

Are transposition representations of permutations unique?

Example

The permutation $\sigma = (1\ 5\ 2\ 4)$ can be written as $(1\ 4)(1\ 2)(1\ 5)$

Question

Are transposition representations of permutations unique?

Example

The permutation $\sigma = (1\ 5\ 2\ 4)$ can be written as $(1\ 4)(1\ 2)(1\ 5)$

- or $(1\ 5)(5\ 2)(2\ 4)$

Transpositions (cont.)

Question

Are transposition representations of permutations unique?

Example

The permutation $\sigma = (1\ 5\ 2\ 4)$ can be written as $(1\ 4)(1\ 2)(1\ 5)$

- or $(1\ 5)(5\ 2)(2\ 4)$
- or $(1\ 5)(5\ 2)(2\ 4)(1\ 3)(1\ 3)$

Transpositions (cont.)

Question

Are transposition representations of permutations unique?

Example

The permutation $\sigma = (1\ 5\ 2\ 4)$ can be written as $(1\ 4)(1\ 2)(1\ 5)$

- or $(1\ 5)(5\ 2)(2\ 4)$
- or $(1\ 5)(5\ 2)(2\ 4)(1\ 3)(1\ 3)$

Question

Which properties of permutations relating to their transposition representations are well-defined?

Parity of Permutations

Definition

A permutation is *even* if it can be written as the product of an even number of transpositions and *odd* if it can be written as the product of an odd number of transpositions.

Parity of Permutations

Definition

A permutation is *even* if it can be written as the product of an even number of transpositions and *odd* if it can be written as the product of an odd number of transpositions.

Proposition

Every permutation is either even or odd.

Parity of Permutations

Definition

A permutation is *even* if it can be written as the product of an even number of transpositions and *odd* if it can be written as the product of an odd number of transpositions.

Proposition

Every permutation is either even or odd.

The Alternating Group

Proposition

The set of even permutations is a subgroup of S_n. This subgroup is called the *alternating group* A_n.

The Alternating Group

Proposition

The set of even permutations is a subgroup of S_n. This subgroup is called the *alternating group* A_n.

Example

$A_4 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

The Fifteen Puzzle Challenge: (14 15)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

$\xrightarrow{?}$

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Question

Is it possible to go from the default state to a state with 14 and 15 swapped?

$P < S_{15}$

Proposition

The set of all moves on the Fifteen Puzzle that leave cell 16 empty is a subgroup of S_{15}.

$P < S_{15}$

Proposition

The set of all moves on the Fifteen Puzzle that leave cell 16 empty is a subgroup of S_{15}.

Example

This sequence of moves represents the permutation (7 11 8):

7	8
11	12
15	

→

7	8
11	
15	12

→

7	8
	11
15	12

→

	8
7	11
15	12

→

8	
7	11
15	12

→

8	11
7	
15	12

→

8	11
7	12
15	

$P < A_{15}$

Theorem

The set of possible configurations P is a subgroup of A_{15}.

$P < A_{15}$

Theorem

The set of possible configurations P is a subgroup of A_{15}.

- Every move is a product of transpositions involving the empty slot:

$$\sigma = \tau_r \tau_{r-1} \cdots \tau_2 \tau_1.$$

- The number of transpositions r is even because:
  - Same number of 'up' and 'down' transpositions
  - Same number of 'left' and 'right' transpositions

$P < A_{15}$

Theorem

The set of possible configurations P is a subgroup of A_{15}.

- Every move is a product of transpositions involving the empty slot:

$$\sigma = \tau_r \tau_{r-1} \cdots \tau_2 \tau_1.$$

- The number of transpositions r is even because:
  - Same number of 'up' and 'down' transpositions
  - Same number of 'left' and 'right' transpositions

Corollary

It is impossible to go from the default state to a state with 14 and 15 swapped.

Generators of the Alternating Group

Definition

The set $\{g_1, g_2, ..., g_n\}$ *generates* a group G if all $g \in G$ can be written as a combination of the g_i and their inverses.

Generators of the Alternating Group

Definition

The set $\{g_1, g_2, ..., g_n\}$ *generates* a group G if all $g \in G$ can be written as a combination of the g_i and their inverses.

Proposition

For $n \geq 3$, A_n is generated by the three-cycles of S_n.

Definition

The set $\{g_1, g_2, ..., g_n\}$ *generates* a group G if all $g \in G$ can be written as a combination of the g_i and their inverses.

Proposition

For $n \geq 3$, A_n is generated by the three-cycles of S_n.

Examples

$(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$

Generators of the Alternating Group

Definition

The set $\{g_1, g_2, ..., g_n\}$ *generates* a group G if all $g \in G$ can be written as a combination of the g_i and their inverses.

Proposition

For $n \geq 3$, A_n is generated by the three-cycles of S_n.

Examples

$(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$
$(1\ 2)(1\ 3) = (1\ 2\ 3)$

Generators of the Alternating Group

Definition

The set $\{g_1, g_2, ..., g_n\}$ *generates* a group G if all $g \in G$ can be written as a combination of the g_i and their inverses.

Proposition

For $n \geq 3$, A_n is generated by the three-cycles of S_n.

Examples

$(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$
$(1\ 2)(1\ 3) = (1\ 2\ 3)$

Proposition

For $n \geq 3$, A_n is generated by the cycles of the form $(1\ 2\ m)$, where $m \in [3, n]$.

$A_{15} < P$

Theorem

A_{15} is a subgroup of P.

$A_{15} < P$

Theorem

A_{15} is a subgroup of P.

Proposition

A_{15} is generated by the 3-cycles $\{(11\ 12\ 1), \ldots, (11\ 12\ 10), (11\ 12\ 13), (11\ 12\ 14), (11\ 12\ 15)\}$.

$A_{15} < P$

Theorem

A_{15} is a subgroup of P.

Proposition

A_{15} is generated by the 3-cycles $\{(11\ 12\ 1), \ldots, (11\ 12\ 10), (11\ 12\ 13), (11\ 12\ 14), (11\ 12\ 15)\}$.

Proposition

$(11\ 12\ 15) \in P$.

$A_{15} < P$

Theorem

A_{15} is a subgroup of P.

Proposition

A_{15} is generated by the 3-cycles $\{(11\ 12\ 1), \ldots, (11\ 12\ 10), (11\ 12\ 13), (11\ 12\ 14), (11\ 12\ 15)\}$.

Proposition

$(11\ 12\ 15) \in P$.

Proof:

11	12
15	

$\rightarrow$

11	
15	12

$\rightarrow$

	11
15	12

$\rightarrow$

15	11
	12

$\rightarrow$

15	11
12	

;

$A_{15} < P$ (cont.)

Lemma

For any permutation $\rho \in S_{15}$, $\rho^{-1}(i_1\ i_2\ i_3)\rho = (\rho^{-1}(i_1)\ \rho^{-1}(i_2)\ \rho^{-1}(i_3))$.

$A_{15} < P$ (cont.)

Lemma

For any permutation $\rho \in S_{15}$, $\rho^{-1}(i_1\ i_2\ i_3)\rho = (\rho^{-1}(i_1)\ \rho^{-1}(i_2)\ \rho^{-1}(i_3))$.

Proposition

$(11\ 12\ j) \in P$ for $1 \leq j \leq 15, j \neq 11, 12, 15$.

$A_{15} < P$ (cont.)

Lemma

For any permutation $\rho \in S_{15}$, $\rho^{-1}(i_1\ \ i_2\ \ i_3)\rho = (\rho^{-1}(i_1)\ \ \rho^{-1}(i_2)\ \ \rho^{-1}(i_3))$.

Proposition

$(11\ 12\ j) \in P$ for $1 \leq j \leq 15, j \neq 11, 12, 15$.

By the lemma, if we can find $\rho_j \in P$ such that

$$\begin{aligned} \rho_j : j &\mapsto 15 \\ 11 &\mapsto 11 \\ 12 &\mapsto 12 \\ 16 &\mapsto 16 \end{aligned}$$

then

$$\rho_j^{-1}(11\ 12\ 15)\rho_j = (\rho_j^{-1}(11)\ \rho_j^{-1}(12)\ \rho_j^{-1}(15)) = (11\ 12\ j).$$

$A_{15} < P$: Constructing ρ_j

Consider (11 12 16):

1	2	3	4
5	6	7	8
9	10	16	11
13	14	15	12

.

Clearly, by design, (11 12 16) $\notin P$. Here are two paths (bold font) the empty slot, 16, can move on so that a new number, j, would show up at cell 15 while 16 comes back to the same cell:

1	**2**	**3**	4
5	6	**7**	8
9	10	**16**	11
13	**14**	**15**	12

1	**2**	**3**	**4**
5	**6**	**7**	**8**
9	**10**	**16**	11
13	**14**	**15**	12

.

$A_{15} < P$: Constructing ρ_j (cont.)

Call such a move ω_j, which leaves cell 11 empty. As a permutation, ω_j fixes cells 11, 12, 16 and send j to 15. In other words,

$$\begin{aligned} \omega_j : j &\mapsto 15 \\ 11 &\mapsto 11 \\ 12 &\mapsto 12 \\ 16 &\mapsto 16 \end{aligned}$$

$A_{15} < P$: Constructing ρ_j (cont.)

We know the 3-cycle (11 12 16) does not affect j and 15. Thus, if we define ρ_j as

$$\rho_j = (11\ 12\ 16)^{-1}\omega_j(11\ 12\ 16),$$

then we can see

$$\begin{aligned} \rho_j : j &\mapsto 15 \\ 11 &\mapsto 11 \\ 12 &\mapsto 12 \\ 16 &\mapsto 16 \end{aligned}$$

and $\rho_j \in P$ because the empty slot is in cell 16.

$A_{15} < P$: Constructing ρ_j (cont.)

Now we know

$$(11\ 12\ j) = \rho_j^{-1}(11\ 12\ 15)\rho_j \in P$$

Thus we have shown

$$\{(11\ 12\ 1), \ldots, (11\ 12\ 10), (11\ 12\ 13), (11\ 12\ 14), (11\ 12\ 15)\} \in P,$$

proving

Theorem

A_{15} is a subgroup of P.

$P = A_{15}$

Since we have proven P is a subgroup of A_{15} and A_{15} is a subgroup of P, we can conclude:

Theorem

$P = A_{15}$.

Acknowledgments

We would like to thank the following for their support and guidance throughout this project:

- Our mentor, Margalit Glasgow
- Isabel Vogt and the PRIMES Circle program
- The MIT Math Department
- Our parents
- Amtrak and Uber

Questions?