The Outer Automorphism of S_6

Meena Jagadeesan[1] Karthik Karnik[2]
Mentor: Akhil Mathew

[1]Phillips Exeter Academy

[2]Massachusetts Academy of Math and Science

PRIMES Conference, May 2016

What is a Group?

Definition

A **group** G is a set of elements together with an operation that satisfies the four fundamental properties: closure, associativity, identity, and inverses.

Our Focus: Symmetric group S_n

Set = permutations π of n elements; Operation = $\circ$ (composition)

- Closure: For $\pi_1, \pi_2 \in S_n$, $\pi_1 \circ \pi_2 \in S_n$
- Associativity: For $\pi_1, \pi_2, \pi_3 \in S_n$, $(\pi_1 \circ \pi_2) \circ \pi_3 = \pi_1 \circ (\pi_2 \circ \pi_3)$
- Identity: Take permutation $e = \pi$ such that $\pi(i) = i$ for all $1 \leq i \leq n$.
- Inverses: For inverse of π_1, take π_1^{-1} such that $\pi_1^{-1}(i) = j$ iff $\pi_1(j) = i$.

What is an Automorphism Group?

Definition

Given a group G, the **automorphism group** $Aut(G)$ is the group consisting of all isomorphisms from G to G (bijective mappings that preserve the structure of G.)

Example: $Aut(S_2)$ ($S_2 = \{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$)

- $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ is the identity
- An automorphism f must send $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ to itself
- f must send $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ to itself
- f is the identity e
- This means $Aut(S_2)$ is trivial

What is an Automorphism Group?

Example: $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ ($\mathbb{Z}_2 \times \mathbb{Z}_2$ is group of pairs of elements modulo 2)

- Observe that $\mathbb{Z}_2 \times \mathbb{Z}_2$ consists of the identity and three other elements of order 2
- An automorphism f must send the identity *to itself*
- The other three elements are permuted by f
- This means that $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$

What is an Inner Automorphism?

Definition

An **inner automorphism** is an automorphism of the form $f : x \mapsto a^{-1}xa$ for a fixed $a \in G$.

This gives us an automorphism of G for each element of G.
There might be repeats. (If G is commutative, then f is always trivial)
Trivial inner automorphisms $= Z(G)$ (elements that commute with all other elements)

Theorem

The inner automorphisms $Inn(G)$ form a normal subgroup of $Aut(G)$ and $Inn(G) \cong G/Z(G)$

Complete Groups

Definition

A group G is **complete** if G is centerless (no nontrivial center) and every automorphism of G is an inner automorphism.

G complete $\Rightarrow Aut(G) \cong G$

Theorem

S_n is complete for $n \neq 2, 6$.

The center of S_2 is itself. S_6 is a genuine exception:

Theorem (Hölder)

There exists exactly one outer automorphism of S_6 (up to composition with an inner automorphism), so that $|Aut(S_6)| = 1440$.

Transpositions

Definition

A **transposition** is a permutation $\pi \in S_n$ that fixes exactly $n-2$ elements (and flips the remaining two elements).

Lemma

An automorphism of S_n preserves transpositions if and only if it is an inner automorphism.

Proof Overview: Completeness of S_n for $n \neq 2, 6$

- Let T_k be the conjugacy class in S_n consisting of products of k disjoint transpositions.
- A permutation π is an involution if and only if it lies in some T_k.
  - If $f \in Aut(S_n)$, then $f(T_1) = T_k$ for some k.
- It suffices to show $|T_k| \neq |T_1|$ for $k \neq 1$.
  - This is true for $n \neq 6$.
  - For $n = 6$, it turns out that $|T_1| = |T_3|$ is the only exception.

Transitive Group Actions

Definition

A group G **acts on** a set X if each element g is a permutation π_g of the set X satisfying $\pi_e = e$ and $\pi_{gf} = \pi_g \circ \pi_f$.

Example 1: S_n acts on $\{1, 2, 3, \ldots, n\}$.
Example 2: S_{n-1} acts on $\{1, 2, 3, \ldots, n\}$ by fixing n.
Example 3: G acts on the coset space G/H by multiplication.

Definition

A group action is **transitive** if for each pair $(x, y) \in X^2$ there exists $g \in G$ such that $g(x) = y$.

Examples 1 and 3 are transitive group actions, but Example 2 is not.

Proof Overview (Existence of an Outer Automorphism of S_6)

Key Step: Construct a 120-element subgroup H of S_6 that acts transitively on $\{1, 2, 3, 4, 5, 6\}$.

- This subgroup cannot be S_5 or any of its conjugates (none are transitive subgroups).
- Consider the action of S_6 on the 6-element coset space S_6/H.
- Let f the corresponding mapping from S_6 to S_6.
- Note that $f : H \mapsto S_5$. (H fixes coset consisting of H and permutes all other cosets. H has order 120, the same as S_5.)
- H (the preimage of S_5 in f) is transitive.
  - The preimage of S_5 is not conjugate to S_5.
  - f cannot be inner.

Methods of Construction

1. Simply 3-transitive action of $PGL_2(\mathbb{F}_5)$ on the six-element set $\boldsymbol{P^1(\mathbb{F}_5)}$
2. Transitive action of S_5 on its six 5-Sylow subgroups

Construction 1: Properties of $PGL_2(K)$

Let K be a field.

Definition

$GL_2(K)$ is the set of 2x2 invertible matrices, whose elements are in the field K.
$PGL_2(K)$ is the quotient of the group $GL_2(K)$ by the scalar matrices $K^\times$ (nonzero elements of K).
$\boldsymbol{P}^1(K)$ is the set of one-dimensional vector spaces (lines) in K^2.

- There is a natural action of $GL_2(K)$ on $\boldsymbol{P}^1(K)$
  - Permutation of the lines through the origin in K^2
  - Matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

where $a \in K$, fix lines, so we have an action of $PGL_2(K)$ on $\boldsymbol{P}^1(K)$

Construction 1: Properties of $P^1(K)$

- Now, $\boldsymbol{P^1}(K)$ can be identified as the union of K and a "point at infinity"
- We consider the following points in $\boldsymbol{P^1}(K)$:
  - The point $[0:1]$, represented by the column vector $\begin{bmatrix}0\\1\end{bmatrix}$
  - The point $[1:1]$, represented by the column vector $\begin{bmatrix}1\\1\end{bmatrix}$
  - The point $[1:0]$, corresponding to the "point at infinity"
  - Each column vector spans a line, which is a point of $\boldsymbol{P^1}(K)$

Construction 1: Linear Fractional Transformations

Definition

A **linear fractional transformation** is a transformation of the form $f(x) = \frac{ax+b}{cx+d}$, where $a, b, c, d \in K$ and $ad - bc \neq 0$.

- $PGL_2(K)$ can be identified with the group of linear fractional transformations
- Through linear fractional transformations (for instance, f in the definition above), we can take the point $-\frac{d}{c}$ to the "point at infinity" and the "point at infinity" to the point $\frac{a}{c}$ when $c \neq 0$

Construction 1: $PGL_2(K)$ is simply 3-transitive

Definition

A group action is **simply 3-transitive** if for all pairs of pairwise distinct 3-tuples (s_1, s_2, s_3) and (t_1, t_2, t_3), there exists a unique $g \in G$ that maps s_i to t_i for $i = 1, 2, 3$.

Note: simply 3-transitive actions are quite rare.

Lemma

The action of $PGL_2(K)$ on $\mathbf{P}^1(K)$ is simply 3-transitive.

- Proof overview (of lemma):
  - Consider the function $f(x) = \frac{x-a}{x-c} \cdot \frac{b-c}{b-a}$.
  - f maps $a \mapsto 0$, $b \mapsto 1$, and $c \mapsto \infty$.
  - f maps any three arbitrary points are mapped to $[0 : 1], [1 : 1], [1 : 0]$

Construction 1: Computing the order of $PGL_2(\mathbb{F}_5)$

- Let K be a finite field of n elements.
- $|PGL_2(K)| = \frac{|GL_2(K)|}{n-1}$ since $PGL_2(K)$ is the quotient of $GL_2(K)$ by the scalar matrices $K^\times$.
- A matrix in $GL_2(K)$ is represented by a nonzero row vector $\boldsymbol{v_1} \in K^2$ and a row vector $\boldsymbol{v_2}$ that is not a scalar multiple of $\boldsymbol{v_1}$.
  - Thus,
    $$|GL_2(K)| = (n^2 - 1)(n^2 - n).$$
    and
    $$|PGL_2(K)| = \frac{(n^2 - 1)(n^2 - n)}{n - 1} = n^3 - n.$$
- Observe that when $K = \mathbb{F}_5$, we have a group of order 120 that acts simply 3-transitively on the six-element set $\boldsymbol{P^1(\mathbb{F}_5)}$

Construction 2: Sylow Subgroups

Definition

Consider a group G with order of the form $p^n \cdot a$ for some prime p, positive integer n, and a relatively prime to p. A ***p*-Sylow subgroup** of G is a subgroup of order p^n.

Theorem (Sylow)

For a group G with order divisible by p, there exists a p-Sylow subgroup. Let x be the number of p-Sylow subgroups. Then,

$$x \equiv 1 \pmod{p} \text{ and } x \Big| |G|.$$

All p-Sylow subgroups are conjugate. (For every pair of p-Sylow subgroups H and K, there exists $g \in G$ with $g^{-1}Hg = K$.)

Construction 2: Action of S_5 on 5-Sylow Subgroups

- The 5-Sylow subgroups of S_5 are the exactly the subgroups generated by a 5-cycle. Let X be the set of these subgroups.
- Then, $|X| \equiv 1 \pmod{5}$ and $|X| \big| 120$ so $|X| = 6$.
- Consider the action of S_5 on X by conjugation (g sends X to $g^{-1}Xg$).
  - By Sylow's theorem, this action is transitive.

Construction 2: Injective Homomorphism from S_5 into S_6

- The action gives a homomorphism $f : S_5 \to S_6$, since $|X| = 6$.
- $ker(f)$ (elements that f maps to identity) forms a normal subgroup, so $ker(f) = A_5, S_5, \{e\}$.
- Since the action is transitive, $|ker(f)| \leq |S_5|/6 = 20$.
  - Hence $|ker(f)| = 1$.
- Thus, $im(f)$ is a transitive 120-element subgroup of S_6.

Conclusion

- We presented two methods of constructing a 120-element transitive subgroup of S_6.
  - Action of $PGL_2(\mathbb{F}_5)$ on $\boldsymbol{P^1(\mathbb{F}_5)}$
  - Action of S_5 on its 5-Sylow subgroups
- These transitive subgroups can be used to construct an automorphism of S_6 whose preimage of S_5 is transitive.
  - This automorphism is outer.
- S_6 is the only symmetric group apart from S_2 that is not complete. Recall that a complete group is a centerless group with no outer automorphisms.

Acknowledgments

We would like to thank

- Akhil Mathew (Harvard), our mentor
- MIT-PRIMES Program

Texts used:

- *An Introduction to the Theory of Groups* by J.J. Rotman
- *Algebra* by S. Lang
- *Topics in Algebra* by I.N. Herstein