M202 Project Report

Automorphism group of Symmetric Groups

Submitted by

Ashlin V Thomas

2^{nd} year Int. MSc Student

School of Physical Sciences
National Institute of Science Education and Research,
Tehsildar Office, Khurda
Pipli, Near, Jatni, Odisha 752050

Submitted to

Tushar Kanta Naik

Assistant Professor

School of Mathematical Sciences
National Institute of Science Education and Research,
Tehsildar Office, Khurda
Pipli, Near, Jatni, Odisha 752050

Acknowledgements

I wish to express my profound gratitude to our course instructor Dr. Tushar Kanta Naik and the School of Mathematical Sciences for providing me with an opportunity to undertake this project. Support and guidance provided by Tushar sir during the coursework and project was critical towards the successful completion of this project. Also, I would like to extend gratitude to my fellow classmates for the support they offered in the process of carrying out this project.

Abstract

In the domain of group theory, one finds symmetric groups or permutation groups to be significant when it comes to understanding the symmetries and structure of mathematical objects, extending its applications to topology, combinatorics and cryptography. In this report, we will discuss about the group of automorphisms - structure-preserving maps - on symmetric groups and list a few important theorems.

1 Objective

In this project, we prove the following theorem related to automorphism group of the symmetric group(S_n) -
Theorem 1.1: Let $n \in \mathbb{N}$ and S_n be the corresponding symmetric group, then -

$$Aut(S_n) \cong \begin{cases} S_n & \text{if } n \geq 2 \text{ , } n \neq 6 \\ S_6 \rtimes \frac{\mathbb{Z}}{2\mathbb{Z}} & \text{if } n = 6 \end{cases}$$

Also, $Inn(S_n) \cong S_n$, for $n \geq 3$.

2 Introduction

Before setting out to prove the theorem 1.1, let us look at some preliminary definitions and theorems[1] -

2.1 Definitions

- **Symmetric group** : Let X be a non-empty set. The set of all bijective maps on X forms a group under composition of maps, called permuation group or symmetric group of X and each element is called a permutation. It is denoted by $Sym(X)$ or S_n, where $n = |X|$.
- **Cycles** : Let $i \in [n]$ and $\sigma \in S_n$. Since σ is bijective with a finite codomain, $\exists t \in [n]$ such that $\sigma^t(i) = i$ and choose t to be minimal in this regard. Now, $(i, \sigma(i), \sigma^2(i), ..., \sigma^{t-1}(i))$ is called a cycle of length t or a t-cycle.
- **Transposition** : A cycle of length two is called a transposition.
- **Automorphism group** : Let G be a group. The set of all bijective homomorphisms on G forms a group under composition of maps, called automorphism group of G and each element is called a automorphism. The group is denoted by $Aut(G)$.
- **Inner automorphism** : Let G be a group and $g \in G$. Inner automorphism of G induced by g is defined as $\phi_g \in Aut(G)$, where $\phi_g(x) = g^{-1}xg$. The collection of all such inner automorphisms forms a subgroup of $Aut(G)$ and is denoted by $Inn(G)$.
- **Semi-direct product** : Let H and K be two groups and $\phi : K \to Aut(H)$ be a homomorphism. Semi-direct product of H and K with respect to homomorphism ϕ, denoted by $H \rtimes_\phi K$, is defined as the group of cartesian product of H and K with the following group operation -

$$(h_1, k_1) \star (h_2, k_2) = (h_1\phi(k_1)(h_2), k_1k_2)$$

2.2 Theorems

We state the following theorems without proofs -

- ***Theorem 2.2.1*** : Let G be a group. Then,

$$Inn(G) \cong \frac{G}{Z(G)}$$

- ***Theorem 2.2.2*** : Let $\sigma_1, \sigma_2 \in S_n$. σ_1 and σ_2 commute if and only if

$$\{i \in [n] \mid \sigma_1(i) \neq i\} \cap \{j \in [n] \mid \sigma_2(j) \neq j\} = \emptyset$$

- ***Theorem 2.2.3*** : Every permutation can be written as a cycle or a product of disjoint cycles. Let $\sigma = \alpha_1\alpha_2...\alpha_k$ be the disjoint cycle representation, where length of α_i is t_i. By theorem 2.2.2, disjoint cycles commute and hence we arrange α_is in such a way $t_{i+1} > t_i \ \forall i \in [k-1]$. Then σ is said to have the **cycle type** $(t_1, t_2, ..., t_k)$.
- ***Theorem 2.2.4*** : Every permutation can be written as a product of transpositions.

- ***Theorem 2.2.5*** : Let $\alpha, \beta \in S_n$. α and β are conjugate in S_n (i.e., $\exists \sigma \in S_n$ such that $\alpha = \sigma^{-1}\beta\sigma$) if and only if α and β are of same cycle type.
- ***Theorem 2.2.6*** : Let $\tau_i = (i, i+1) \in S_n$. Then, S_n is generated by $\{\tau_i \mid i \in [n-1]\}$.
- ***Theorem 2.2.7*** : Let $n \geq 3$, then, $Z(S_n) = 1$.
- ***Theorem 2.2.8*** : Let λ be a conjugacy class of S_n containing elements of cycle type $1^{i_1}, 2^{i_2}, ..., n^{i_n}$. Then,
$$|\lambda| = \frac{n!}{(1^{i_1}.2^{i_2}.....n^{i_n}).(i_1!.i_2!....i_n!)}$$
- ***Theorem 2.2.9*** : Let $\phi : G_1 \to G_2$ be a homomorphism. Then,
  - $\phi(G_1) \leq G_2$
  - $Ker(\phi) \trianglelefteq G_1$
  - If $Ker(\phi)$ is trivial, then ϕ is injective.
- ***Theorem 2.2.10*** : For $n \geq 5$, the only normal subgroups of S_n are $\{1\}, A_n, S_n$.
- ***Theorem 2.2.11*** : Let G be a group. Then,
$$Inn(G) \trianglelefteq Aut(G)$$

3 Inn(S$_n$)

Theorem 3.1 : $Inn(S_n) \cong S_n$, for $n \geq 3$.

Proof : From theorem 2.2.1,
$$Inn(S_n) \cong \frac{S_n}{Z(S_n)}$$
We know from theorem 2.2.7 that $Z(S_n) = 1$ for $n \geq 3$. Hence,
$$Inn(S_n) \cong \frac{S_n}{Z(S_n)} = \frac{S_n}{1} = S_n$$
$$\implies Inn(S_n) \cong S_n \ , n \geq 3 \qquad \blacksquare$$

4 Inn(S$_n$) and Aut(S$_n$)

Lemma 4.1 : Let $\phi \in Aut(S_n)$. $\phi \in Inn(S_n)$ if and only if ϕ takes each transposition to a transposition.

Proof : If ϕ is an inner automorphism, it conjugates each element of S_n with a fixed $\sigma \in S_n$. Hence, ϕ conjugates any transposition $\alpha \in S_n$ with σ and by theorem 2.2.5, $\phi(\alpha) = \sigma^{-1}\alpha\sigma$ is also a transposition. Hence, ϕ takes every transposition to another transposition.

Let $\psi \in S_n$ such that ψ takes every transposition to another transposition. Let $\psi((1,2)) = (a_1, a_2)$ and $\psi((2,3)) = (b_1, b_2)$. If (a_1, a_2) and (b_1, b_2) are disjoint, they commute and $\psi((1,2)(2,3)) = \psi((2,3)(1,2))$, which implies $\psi((2,3,1)) = \psi((2,1,3))$. This is a contradiction to the injectivity of ψ. Hence they are not disjoint. For the same reason, they can't be equal. Hence, their supports share a common element.

Inductively, we can assume $\psi((i, i+1)) = (a_i, a_{i+1})$, $i \in [n-1]$. Let $\sigma \in S_n$ defined by $\sigma(i) = a_i$, $\forall i \in [n]$. Now,

$$\phi_\sigma((i, i+1)) = \sigma^{-1}(i, i+1)\sigma = (\sigma(i), \sigma(i+1))$$
$$\implies \phi_\sigma(\tau_i) = (a_i, a_{i+1}) = \psi(\tau_i) \ , \forall i \in [n-1]$$

By theorem 2.2.6, τ_is generate S_n. Since, ϕ_σ and ψ have the same images for the elements of generator, the automorphisms are equal. Hence, $\psi = \phi_\sigma$ is an inner automorphism. $\blacksquare$

Definition : Let $k \in \mathbb{N}$ such that $2 \leq 2k \leq n$. Define $T_k \subset S_n$ as -

$$T_k = \{\sigma \in S_n \mid \sigma \text{ is of cycle type } 2^k\}$$

Lemma 4.2 : Let $\phi \in Aut(S_n)$ and $m \geq 1$ such that $2 \leq 2m \leq n$. Then, $\exists k \geq 1$ such that $\phi(T_m) \subseteq T_k$.

Proof : Let $\sigma_1 \in T_m$. By definition, σ_1 is of cycle type 2^m and hence the order of σ_1 is 2 (l.c.m of orders of disjoint cycles, which are all 2-cycles). Since ϕ is an automorphism, $\phi(\sigma_1)$ should be of order 2. Hence, its cycle type should be 2^k for some $k \in \mathbb{N}$ (Any cycle of length greater than 2 will change the lcm of lengths and hence increase the order from 2). Therefore, $\sigma_1 \in T_k$.

Let $\alpha \in T_m$ be an arbitrarily chosen element. Since both α and σ_1 have cycle type 2^m, they are conjugate to each other by theorem 2.2.5. Hence, $\exists\beta$ such that -

$$\begin{aligned} &\alpha = \beta^{-1}\sigma_1\beta \\ \implies &\phi(\alpha) = \phi(\beta^{-1})\phi(\sigma_1)\phi(\beta) \\ \implies &\phi(\alpha) = \phi(\beta)^{-1}\phi(\sigma_1)\phi(\beta) \end{aligned}$$

Hence, $\phi(\alpha)$ and $\phi(\sigma_1)$ are conjugate to each other. Therefore, by theorem 2.2.5, they have the same cycle type, i.e., $\phi(\alpha) \in T_k$. By arbitrary choice, $\forall\alpha \in T_m$, $\phi(\alpha) \in T_k$. Hence, $\phi(T_m) \subseteq T_k$. ■

Lemma 4.3 : Let $\phi \in Aut(S_n)$. Then, $\exists k \geq 1$ such that $\phi(T_1) = T_k$.

Proof : By lemma 4.2, $\exists k \geq 1$ such that $\phi(T_1) \subseteq T_k$. Since ϕ is an automorphism, $\phi^{-1} \in Aut(S_n)$. Since $\phi(T_1) \subseteq T_k$, $\exists\alpha \in T_k$ such that $\phi^{-1}(\alpha) \in T_1$. Therefore, by lemma 4.2, $\phi^{-1}(T_k) \subseteq T_1 \implies T_k \subseteq \phi(T_1)$. Hence, $\phi(T_1) = T_k$. ■

Lemma 4.4 : Let $n, k \in \mathbb{N}$, $n \geq 2$, $n \neq 6$ and $2 \leq 2k \leq n$. Then, the only solution to the following equation is k=1.

$$2^{k-1}k!(n-2k)! = (n-2)! \tag{1}$$

Proof : By substitution, we find that $k = 1$ is a solution for every $n \geq 2$. Now, we have to show that $k = 1$ is the only solution if $n \neq 6$.

For n=2 and 3, k can only take value 1 and hence is the only solution.

For n=4, k can also take the value 2. Substituting in eq(1), we get $4 = 2!$. Hence, $k = 2$ is not a solution.

Similar to the previous case, for n=5, k can take values 1 and 2 and substituting k=2 in eq(1) gives $4 = 3!$. Hence, $k = 2$ is not a solution.

Now, for $n \geq 7$, we will have two cases -

Case 1: $2k \neq n$

In this case, we can write eq(1) as -

$$\begin{aligned} 2^{k-1}(n-2k)! &= \frac{(n-2)!}{k!} \\ \implies (2.2.....2)(2.3.....(n-2k)) &= (k+1)....(n-2) \end{aligned}$$

Note that LHS and RHS of the above equation has $(n-k-2)$ terms each. If $k \geq 2$, we compare each factor of LHS and RHS in the order written above - $2 < k+1$, $2 < k+2$, ..., $2 < 2k-1$, $2 < 2k$, $3 < 2k+1$, ..., $n-2k < n-2$. Since each factor of LHS is less than the corresponding factor in RHS, the equality doesn't hold. Hence the equation doesn't have any solution in the range $k \geq 2$.

Case 2: $2k = n$

For $n = 2k$, eq(1) takes the form -

$$(2k-2)! = 2^{k-1}k! \tag{2}$$

Since $2k = n \geq 7$, $k \geq 4$.

We claim that

$$(2k-2)! > 2^{k-1}k! \; \forall k \geq 4$$

For k=4, $6! > 8.4!$ and our claim remains true.

Assume that the claim is true for $k = m \geq 4$,i.e., $(2m-2)! > 2^{m-1}m!$.

Now, for k=m+1 -

$$\begin{aligned}(2(m+1)-2)! = (2m)! = 2m(2m-1)(2m-2)!\\ \implies (2(m+1)-2)! > 2m(2m-1)2^{m-1}m!\\ \text{(Induction hypothesis)}\\ \implies (2(m+1)-2)! > m(2m-1)2^m m!\end{aligned}$$

Since $m \geq 4$, $2m-1 \geq 7$. Hence, $m(2m-1) \geq 7m > m+1$. Therefore,

$$\begin{aligned}(2(m+1)-2)! > (m+1)2^m m!\\ \implies (2(m+1)-2)! > 2^m(m+1)!\end{aligned}$$

Hence, the claim is true for $k = m+1$, whenever it is true for $k = m$. Hence, by induction principle, the claim is true for all $k \geq 4$.
By the previous claim, eq(2) has no solution for $k \geq 4$, i.e., for $n \geq 7$.

Hence, $k = 1$ is the only solution of eq(1) for $n \neq 6$. ■

Theorem 4.1 : Let $n \in \mathbb{N}$ and $n \geq 2$. $Aut(S_n) \cong S_n$, if $n \neq 6$.

Proof : Let $\phi \in Aut(S_n)$. By lemma 4.3, $\exists k \geq 1$ such that $\phi(T_1) = T_k$. Since ϕ is bijective, $|T_1| = |T_k|$. Note that T_1 and T_k are conjugacy classes (all elements are of same cycle type and any element of the same cycle type is contained in the set), hence we can compute their sizes using theorem 2.2.8 as -

$$\begin{aligned}|T_1| = |T_k| \implies \frac{n(n-1)}{2} = \frac{n!}{2^k k!(n-2k)!}\\ \implies 2^{k-1}k!(n-2k)! = (n-2)!\end{aligned}$$

By lemma 4.4, the only solution to the above equation is $k = 1$ since $n \neq 6$. Therefore, $\phi(T_1) = T_1$, i.e., ϕ takes every transposition to another transposition and by lemma 4.1, $\phi \in Inn(S_n)$. Since $\phi \in Aut(S_n)$ is chosen arbitrarily, $\forall \phi \in Aut(S_n)$, $\phi \in Inn(S_n)$. Hence, $Aut(S_n) \subseteq Inn(S_n)$. Also, we know that $Inn(S_n) \subseteq Aut(S_n)$. Therefore, $Aut(S_n) = Inn(S_n)$, $\forall\ 3 \leq n \in \mathbb{N}$ and $n \neq 6$.
Hence, we can conclude using theorem 3.1 that -

$$Aut(S_n) = Inn(S_n) \cong S_n$$

for all $n \geq 3$ and $n \neq 6$. ■

5 The Exceptional Case : $\mathbf{Aut(S_6)}$

We find that $n = 6$ and $k = 3$ satisfies eqn(1). This motivates us to doubt whether there could be an outer automorphism θ of S_6 such that $\theta(T_1) = T_3$. We will resolve this doubt through the following lemma.

Lemma 5.1 : $\exists\ \theta \in Aut(S_6)$ such that θ is an outer automorphism.

Proof : Define $\theta\ :\ S_6 \to S_6$ as -

$$\begin{aligned}\theta((1,2)) = (1,2)(3,4)(5,6)\\ \theta((2,3)) = (1,4)(2,5)(3,6)\\ \theta((3,4)) = (1,2)(3,5)(4,6)\\ \theta((4,5)) = (1,3)(2,4)(5,6)\\ \theta((5,6)) = (1,2)(3,6)(4,5)\end{aligned}$$

Here, we have defined θ on the generators of S_6 and we find the image of an arbitrary element of S_6 under θ by writing it as a product of generating elements and then θ acts on the product in such a way that θ remains as a homomorphism.

Claim 5.1.1 : $\theta^2 = Id$
Proof of claim : Let $\tau_i = (i, i+1)$ $1 \leq i \leq 5$. Note that -

$$\theta^2(\tau_1) = \theta(\theta(\tau_1)) = \theta((1,2)(3,4)(5,6))$$
$$\implies \theta^2(\tau_1) = (1,2)(3,4)(5,6)(1,2)(3,5)(4,6)(1,2)(3,6)(4,5) = (1,2) = \tau_1$$

Now, its only a matter of computations to verify that $\theta^2(\tau_i) = \tau_i \ \forall \ i \in [5]$, at each step using the property of θ being a homomorphism.
Let $\alpha \in S_6$. Since τ_is generate S_6,

$$\alpha = \tau_{k_1}.\tau_{k_2}....\tau_{k_m}$$
$$\implies \theta^2(\alpha) = \theta(\theta(\tau_{k_1}).\theta(\tau_{k_2})....\theta(\tau_{k_m})) = \theta^2(\tau_{k_1}).\theta^2(\tau_{k_2})....\theta^2(\tau_{k_m}) = \tau_{k_1}.\tau_{k_2}....\tau_{k_m} = \alpha$$
$$\implies \theta^2(\alpha) = Id(\alpha)$$

Since, $\alpha \in S_6$ is chosen arbitrarily, we can conclude that $\theta^2 = Id$. Hence, the claim.

Let $i \in [5]$ and $\theta(\tau_i) = \alpha_i \implies \theta^2(\tau_i) = \theta(\alpha_i) \implies \theta(\alpha_i) = \tau_i$. Hence, $\forall \ i \in [5]$, $\tau_i \in \theta(S_6)$. Since, θ is a homomorphism, $\theta(S_6) \leq S_6$ using theorem 2.2.9 . Also, $\theta(S_6)$ contains all generating elements of S_6. Hence, $\theta(S_6) = S_6$,i.e., θ is surjective.

According to theorem 2.2.10, the only normal subgroups of S_6 are $\{1\}, A_6, S_6$. Since $Ker(\theta)$ is a normal subgroup of S_6 according to theorem 2.2.9, kernel can be either trivial, S_6 or A_6. $Ker(\theta)$ can't be S_6, as θ takes elements of S_6 to non-identity elements. Also, $Ker(\theta)$ can not be A_6, because it takes even permutations to non-identity elements, for example, $\theta((1,2)(3,4)) = (3,6)(4,5) \neq 1$. Hence, $Ker(\theta)$ is trivial and therefore by theorem 2.2.9, θ is injective.

Since θ is injective and surjective, $\theta \in Aut(S_6)$. Also, by definition, θ takes transpositions to elements which are not transpositions. So, $\theta \notin Inn(S_6)$. Hence, θ is an outer automorphism. ■

Lemma 5.2 : $Aut(S_6) = Inn(S_6).<\theta>$, where, θ has the same definition as in the above lemma.
Proof : Clearly, $Inn(S_6).<\theta> \subseteq Aut(S_6)$.
Let $\phi \in Aut(S_6)$. If ϕ is an inner automorphism, $\phi \in Inn(S_6).<\theta>$.
If ϕ is an outer automorphism, ϕ takes every transposition to a product of 3 transpositions, i.e., $\phi(T_1) = T_3$. Since θ is an outer automorphism, $\theta(T_1) = T_3 \implies \theta^{-1}(T_3) = T_1$ and θ^{-1} is a well-defined function since θ is bijective. Consider the map $\theta^{-1}\phi$.

$$\theta^{-1}\phi(T_1) = \theta^{-1}(T_3) = T_1$$

Hence, $\theta^{-1}\phi$ takes every transposition to some other transposition and by lemma 4.1, $\theta^{-1}\phi = \psi \in Inn(S_6)$. Therefore, $\phi = \theta\psi \in Inn(S_6).<\theta>$. So, $\forall \ \phi \in Aut(S_6)$, $\phi \in Inn(S_6).<\theta>$.
Hence, $Aut(S_6) = Inn(S_6).<\theta>$. ■

Theorem 5.1 : $Aut(S_6) \cong S_6 \rtimes \frac{\mathbb{Z}}{2\mathbb{Z}}$
Proof : By lemma 5.2, $Aut(S_6) = Inn(S_6).<\theta>$. From claim 5.1.1 $<\theta>= \{1, \theta\}$. Since, θ is an outer automorphism, $1 = Inn(S_6) \cap <\theta>$. Also, by theorem 2.2.11, $Inn(S_6) \trianglelefteq Aut(S_6)$. Based on the above three observations, we can conclude that $Aut(S_6) = Inn(S_6) \rtimes <\theta>$.
Since $<\theta>= \{1, \theta\}$, $<\theta>\cong \frac{\mathbb{Z}}{2\mathbb{Z}}$ and by theorem 3.1, $Inn(S_6) \cong S_6$. Therefore, we can conclude that $Aut(S_6) = Inn(S_6) \rtimes <\theta>\cong S_6 \rtimes \frac{\mathbb{Z}}{2\mathbb{Z}}$. ■

6 Conclusion

In this project report, we studied the automorphism groups of symmetric groups and our analysis led us to the conclusion which is stated as theorem 1.1. In the journey of studying the group structure of $Aut(S_n)$, we encountered certain critical lemmas and theorems which enlighted us about the behaviour of automorphisms of S_n. It was quite surprising to note that how S_6 stands out from the rest by having an "exceptional" outer automorphism. Finally, we studied the outer automorphisms of S_6, revealing the total group structure of $Aut(S_6)$.

References

[1] Joseph A. Gallian. *Contemporary Abstract Algebra*. Brooks/Cole, Cengage Learning.