SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Outer automorphisms of S_6

av

Ottilia Andersson

2025 - No K21

Outer automorphisms of S_6

Ottilia Andersson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Wushi Goldring

2025

To my mother.

Abstract

In this thesis, we study inner and outer automorphisms of groups, with a particular focus on the symmetric group. We show that if an automorphism of S_n stabilizes the conjugacy class of transpositions, then it is inner. Using this result, we further show that every automorphism of S_n is inner if $n \neq 6$. Finally, a proof of the existence of an outer automorphism of S_6 is outlined.

Sammanfattning

I den här uppsatsen studerar vi inre och yttre automorfismer av grupper, med särskilt fokus på den symmetriska gruppen. Vi visar att om en automorfism av S_n stabiliserar konjugationsklassen som innehåller transpositioner, så är det en inre automorfism. Därefter visar vi att varje automorfism av S_n är inre om $n \neq 6$. Slutligen skisserar vi ett bevis för existensen av en yttre automorfism i S_6.

Acknowledgement

I want to express my sincere gratitude to my supervisor, Wushi Goldring, for sharing his enthusiasm and providing guidance throughout this project. Thank you for your inspiration, patience, and support.

Contents

1 Introduction

The aim of this thesis is to explain, and outline a proof of, the existence of an outer automorphism of the symmetric group S_6. To do this, we discuss properties of S_n in general, and of S_6 in particular. We also study automorphism groups; specifically, inner and outer automorphism groups. In general, every automorphism of S_n is inner, but $n = 6$ is an exception. Why? This thesis attempts to help answering that question.

The proof of the existence of an outer automorphism of S_6 was first carried out by Hölder in 1895 [Höl95]. Since then, several authors have given explicit constructions of an outer automorphism of S_6, e.g., [Ben24] and [Mil58]. We will follow Janusz and Rotman [JR82] in their outline toward this result. Along the way, we will have to learn about the symmetric group on the one hand and about automorphisms on the other.

Automorphisms are bijective homomorphisms of algebraic structure to itself. The collection of automorphisms can be thought of as all the symmetries of an algebraic object. Thus, as structure-preserving maps, automorphisms are crucial in the study of symmetry. While automorphisms are interesting in themselves, they also play a key role in, for example, the study of group extensions [Rot12, p. 154 ff].

The outline of this paper is as follows. Section 2 covers group actions. In Section 3, we discuss properties of the symmetric group. We become familiar with basic concepts in S_n, such as generating sets and conjugation. Special focus is given to S_6. In Section 4, automorphism groups are introduced. We define inner and outer automorphisms, and provide examples for different types of groups, such as the dihedral group, cyclical groups of prime order and the special linear group. In Section 5, selected results from Section 4 are applied to S_n. We prove that if an automorphism of S_n stabilizes the conjugacy class of transpositions, then it is inner. Using this result, we further prove that every automorphism of S_n is inner if $n \neq 6$. Ultimately, we outline a proof of the existence of an outer automorphism of S_6.

The main sources in writing this thesis have been [DF04] and [Rot12].

2 Group actions and G-sets

Definition 2.1. Let G be a group and A a non-empty set. A *group action* is a map

$$\begin{aligned} G \times A &\to A \\ g \cdot a &\mapsto ga \end{aligned}$$

satisfying

(1) $1 \cdot a = a$ for all $a \in A$

(2) $g \cdot (h \cdot a) = (gh) \cdot a$ for all $g, h \in G, a \in A$.

We say that G acts on A and we call the set A a *G-set*.

Remark 2.2. The notion of a group action is closely related to that of a homomorphism. Let A be a G-set. Each $g \in G$ admits an action

$$\begin{aligned} \sigma_g : A &\to A \\ a &\mapsto g \cdot a. \end{aligned}$$

This is a permutation of A. The action σ_g is associated with a homomorphism

$$\varphi : G \to S_A$$

defined by $\varphi(g) = \sigma_g$, for all $g \in G$. The homomorphism φ is called the *permutation representation* of the action σ_g.

Definition 2.3. Let A be a G-set and let $a \in A$. The set $\{g \cdot a \,|\, g \in G\} \subset A$ is called the *orbit* of G containing a and is denoted $\mathsf{Orb}(a)$. If there is only one orbit of the action, we say that the action is *transitive*; that is, for any two $a, b \in A$, there exists a $g \in G$ such that $a = g \cdot b$. The set $\{g \in G \,|\, g \cdot a = a\} \subset G$ of group elements that fix, or *stabilize*, the element a under the action is called the *stabilizer* of a in G and is denoted $\mathsf{Stab}(a)$.

2.1 The Orbit-Stabilizer Theorem

Theorem 2.4. *Let A be a G-set and let $a \in A$. Then the number of elements in the orbit of a equals the number of left cosets of $\mathsf{Stab}(a)$ in G:*

$$|\mathsf{Orb}(a)| = [G : \mathsf{Stab}(a)].$$

Proof. Finding a bijection between the two sides of the equality is enough to show the theorem. Define a function

$$\begin{aligned} f : \mathsf{Orb}(a) &\to G/\mathsf{Stab}(a) \\ g \cdot a &\mapsto g\,\mathsf{Stab}(a). \end{aligned}$$

Let $g \in G$ and suppose that $ga = ha$ for some $h \in G$. Then $h^{-1}ga = h^{-1}ha = a$, so $h^{-1}g \in \mathsf{Stab}(a)$. But then $g\,\mathsf{Stab}(a) = h\,\mathsf{Stab}(a)$, so f is well-defined. Now suppose that $g\,\mathsf{Stab}(a) = h\,\mathsf{Stab}(a)$. Then $h^{-1}g \in \mathsf{Stab}(a)$, so $h^{-1}ga = a$. Multiplying both sides on the left by h gives that $ga = ha$. Hence, f is injective. For any $g \in G$, $g\,\mathsf{Stab}(a) = f(g \cdot a)$, where indeed $g \cdot a \in \mathsf{Orb}(a)$. Hence, f is surjective. □

Not only can a group act on a set, but a group can also act on itself. Two fundamental examples of groups acting on themselves are left multiplication and conjugation, examined in Section 2.2 and Section 2.3 respectively.

2.2 Groups acting on themselves by left multiplication

If G is a group acting on itself by left multiplication, we define the action

$$g \cdot a = ga \quad \text{for all } g, a \in G,$$

where the product in ga is the group operation. The axioms for a group action, stated in Definition 2.1, are satisfied and easily checked.

Example 2.5. Let the additive group of integers modulo 6, denoted by

$$\mathbb{Z}/6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\},$$

act on itself on the left. Then

$$\overline{a} \cdot \overline{b} = \overline{a} + \overline{b} \quad \text{for all } \overline{a}, \overline{b} \in \mathbb{Z}/6.$$

When the operation is addition, this type of action is often called left *translation*.

Remark 2.6. Left multiplication of group elements can be regarded as a special case of a more general situation. Let H be a subgroup of the group G and define

$$A = \{gH \mid g \in G\}$$

to be the set of all left cosets of H in G. Then G acts on A by

$$g \cdot aH = gaH \quad \text{for all } g \in G,\ aH \in A.$$

When $H = \{1\}$, then $aH = a\{1\} = \{a\}$ for all $a \in G$, so the action of G on A is the same as the action of G on itself.

Example 2.7. Let D_8 denote the dihedral group of order 8 and let $\langle s \rangle = \{1, s\} \leq D_8$ be the subgroup generated by reflections. By Lagrange's theorem (e.g., [DF04, p. 89], Theorem 8 in Section 3.2), the number of left cosets of $\langle s \rangle$ in D_8 is given by

$$\frac{|D_8|}{|\langle s \rangle|} = \frac{8}{2} = 4.$$

The four left cosets of $\langle s \rangle$ in D_8 are

$$\begin{aligned} 1\langle s \rangle &= s\langle s \rangle = \{1, s\} && (1) \\ r\langle s \rangle &= sr^3\langle s \rangle = \{r, sr^3\} && (2) \\ r^2\langle s \rangle &= sr^2\langle s \rangle = \{r^2, sr^2\} && (3) \\ r^3\langle s \rangle &= sr\langle s \rangle = \{r^3, sr\} && (4) \end{aligned} \tag{1}$$

and labelled (1)-(4). The cosets can be verified using the relations in the following presentation of D_8:

$$D_8 = \langle r, s \mid r^4 = s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

The group D_8 acts by left multiplication on the cosets of $\langle s \rangle$. For example, if σ_r denotes acting by r, then

$$\begin{aligned} \sigma_r(1) &= r \cdot 1\langle s \rangle = r\langle s \rangle = (2) \\ \sigma_r(2) &= r \cdot r\langle s \rangle = r^2\langle s \rangle = (3) \\ \sigma_r(3) &= r \cdot r^2\langle s \rangle = r^3\langle s \rangle = (4) \\ \sigma_r(4) &= r \cdot r^3\langle s \rangle = 1\langle s \rangle = (1). \end{aligned}$$

Thus, $\sigma_r = (1234)$, where the numbers correspond to the cosets in Eq. (1). If σ_s denotes acting on the left by s, the same procedure gives that $\sigma_s = (24)$. Since r and s are generators of D_8, every action of D_8 on the set of cosets of $\langle s \rangle$ is known.

For example, the result of acting on the left by sr^3 is given by

$$\sigma_{sr^3} = \sigma_s \sigma_r^3 = (24)(1234)^3 = (12)(34).$$

2.3 Groups acting on themselves by conjugation

If G is a group acting on itself by conjugation, then the action is defined as

$$g \cdot a = gag^{-1} \quad \text{for all } g, a \in G.$$

The axioms for a group action, stated in Definition 2.1, are satisfied and easily checked. When G acts by conjugation, the orbits are called *conjugacy classes*.

Example 2.8. If G is a commutative group, then the conjugation action is the trivial action, since $gag^{-1} = a \iff ga = ag$ for all $g, a \in G$ when G is commutative.

3 Symmetric groups

A *permutation* is a bijective map $\alpha : X \to X$, where X is a non-empty set. We denote by S_X the group of all permutations of X. In particular, when $X = \{1, 2, \ldots, n\}$, we write S_n for the group of all permutations on n letters. We will refer to S_n as *the symmetric group*.

3.1 Cycles

Definition 3.1. Let $\sigma \in S_n$ and let $i_1, i_2, \ldots, i_r \in \{1, 2, \ldots, n\}$ be distinct integers. If

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1,$$

and $\sigma(i_j) = i_j$ for the remaining $n - r$ integers, then $\sigma = (i_1\, i_2\, i_3 \ldots\, i_r)$ is an *r-cycle*. We also say that σ is a *cycle of length r*.

Definition 3.2. A *transposition* is a permutation that consists of a single cycle of length 2.

Definition 3.3. If G is a group, then $g \in G$ is an *involution* if $g^2 = 1$. In particular, transpositions are involutions.

Example 3.4. Elements in S_n that are products of k disjoint transpositions are involutions. Reflections in the dihedral group are involutions.

In Theorem 3.11, Theorem 3.15 and Theorem 3.16, we will see that the symmetric group is in fact generated by transpositions. But first we need a few lemmas, allowing us to rewrite permutations in certain ways.

Lemma 3.5. *Every permutation $\sigma \in S_n$ is a product of disjoint cycles.*

Proof. S_n acts on $\{1, 2, \ldots, n\}$. Let $\sigma \in S_n$ be a permutation and consider the action of the cyclic subgroup $\langle\sigma\rangle \leq S_n$ on $\{1, 2, \ldots, n\}$. The action partitions $\{1, 2, \ldots, n\}$ into a disjoint union of r orbits:

$$\{1, 2, \ldots, n\} = \bigsqcup_{i=1}^{r} \mathsf{Orb}(i).$$

Note that orbits are disjoint or identically the same. Let $j_i \in \mathsf{Orb}(i)$. Then

$$\mathsf{Orb}(i) = \left\{j_i, \sigma(j_i), \ldots, \sigma^{|\mathsf{Orb}(i)|-1}(j_i)\right\}.$$

Every orbit corresponds to a cycle. Define the cycle

$$c_i = \begin{pmatrix} j_i & \sigma(j_i) & \cdots & \sigma^{|\mathsf{Orb}(i)|-1} \end{pmatrix}$$

to be the one corresponding to the set $\mathsf{Orb}(i)$. Since orbits are disjoint, their corresponding cycles are disjoint. Therefore $\sigma = c_1 c_2 \cdots c_r$, with c_i distinct. Hence, every permutation is a product of disjoint cycles.

For an inductive proof of this lemma, see the proof of Theorem 1.1 in [Rot12, p. 6]. □

Lemma 3.6. *Every m-cycle is a product of $m-1$ non-disjoint transpositions. The cycle decomposition is not unique.*

Proof. Note that a general m-cycle $(a_1\, a_2 \ldots a_m)$ can be written as

$$(a_1\ a_2 \ldots a_m) = (a_1\, a_m)(a_1\, a_{m-1}) \ldots (a_1\, a_3)(a_1\, a_2),$$

as well as

$$(a_1\ a_2 \ldots a_m) = (a_1\, a_2)(a_2\, a_3) \ldots (a_{m-2}\, a_{m-1})(a_{m-1}\, a_m).$$

□

Question 3.7. If any permutation is a product of transpositions, should we not regard transpositions as building blocks of S_n? Indeed, we can. This idea is formalized in Section 3.2, in discussing generating sets of S_n.

Now we know that every permutation is a product of disjoint cycles, which in turn can be factored into (non-disjoint) transpositions. This gives a way to characterize permutations in terms of transpositions, captured in Definition 3.8.

Definition 3.8. A permutation $\sigma \in S_n$ is *even* if it is a product of an even number of transpositions.

Example 3.9. Consider $(123) = (12)(23) = (13)(12) \in S_3$. This is an even permutation since it is a product of an even number of transpositions. Note that the transpositions are neither disjoint, nor written in a unique way.

Remark 3.10. Conversely, if a permutation is not a product of an even number of transpositions, we call it an *odd* permutation. Whether a permutation is even or odd is captured in the notion of its *parity*.

3.2 Generating sets

Theorem 3.11. *For $n \geq 2$, the symmetric group S_n is generated by transpositions.*

Proof. We prove this by induction on n. The base case $n = 2$ holds, since S_2 only consists of (12) and the identity element. Let $n \geq 3$ and assume that S_{n-1} is generated by transpositions. Pick $\sigma \in S_n$. If $\sigma(n) = n$, then σ fixes n and can thus be regarded as a permutation in S_{n-1}. By assumption, σ is a product of transpositions. If, on the other hand, $\sigma(n) \neq n$, let $\sigma(n) = m$ for some $m \in \{1, 2, \ldots, n-1\}$. Let $\tau = (m\, n)$ be the transposition interchanging m and n. Then

$$(\tau\sigma)(n) = \tau\Big(\sigma(n)\Big) = \tau(m) = n.$$

So $\tau\sigma$ fixes n and can thus be regarded as a permutation in S_{n-1}. By assumption, $\tau\sigma$ is a product of transpositions. It follows that $\tau\tau\sigma = \sigma$ is a product of transpositions in S_n. By the inductive hypothesis, S_n is generated by transpositions for $n \geq 2$. □

Remark 3.12. All transpositions in S_n form a generating set of S_n of size $n(n-1)/2$. In Theorem 3.15 and Theorem 3.16, we will see that S_n can be generated by a smaller set of transpositions, of size $n - 1$. Before proving that, we will consider a lemma showing that the result of interchanging any two integers can be obtained by sequentially interchanging adjacent integers.

Lemma 3.13. *Every transposition in S_n is a product of the elementary transpositions*

$$s_1 = (12), s_2 = (23), \ldots, s_{n-1} = (n-1\, n).$$

Proof. Let $(a\, b) \in S_n$ be a transposition. Since $(a\, b) = (b\, a)$, we can assume that $a < b$. The proof is carried out by strong induction on the difference $b - a$. If $b - a = 1$, then $(a\, b) = (a\, a+1)$, which is an elementary transposition. Suppose that $b - a = k > 1$, and suppose that the theorem holds for all $b - a < k$. Note that

$$(a\, b) = (a\, a+1)(a+1\, b)(a\, a+1).$$

As noted, $(a\, a+1)$ is an elementary transposition. For the middle transposition, the difference $b-(a+1) = k-1$. But we assumed that all transpositions with difference less than k are products of elementary transpositions. Hence, $(a+1\, b)$ is a product of elementary transpositions. By the inductive hypothesis, all transpositions $(a\, b)$ are products of elementary transpositions. □

Example 3.14. Let $\sigma = (25)$ be a transposition in S_5. Then

$$\sigma = (23)(34)(45)(34)(23),$$

with $\sigma(1) = 1, \sigma(2) = 5, \sigma(3) = 3, \sigma(4) = 4$, and $\sigma(5) = 2$.

Theorem 3.15. *For $n \geq 2$, S_n is generated by the elementary transpositions*

$$s_1 = (12), s_2 = (23), \ldots, s_{n-1} = (n-1\, n).$$

Proof. By Theorem 3.11, S_n is generated by transpositions. By Lemma 3.13, every transposition is a product of elementary transpositions. This concludes the proof. □

Theorem 3.16. *For $n \geq 2$, S_n is generated by the transpositions containing a 1:*

$$(12), (13), \ldots, (1\, n).$$

Proof. Let $n \geq 2$. By Theorem 3.11, it suffices to show that every transposition $(a\, b) \in S_n$ is a product of transpositions containing a 1.

Let $\sigma = (1\, a)$, $\tau = (1\, b)$. Then

$$\sigma\tau\sigma^{-1} = (1\, a)(1\, b)(1\, a) = (a\, b) \quad \text{for all } (a\, b) \in S_n.$$

□

3.3 Conjugation in the symmetric group

Proposition 3.17. *Let $\sigma, \tau \in S_n$ and suppose that*

$$\sigma = (a_1, a_2, \ldots, a_{k_1})(b_1, b_2, \ldots, b_{k_2}) \cdots .$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$\tau\sigma\tau^{-1} = \Big(\tau(a_1), \tau(a_2), \ldots, \tau(a_{k_1})\Big)\Big(\tau(b_1), \tau(b_2), \ldots, \tau(b_{k_2})\Big) \cdots .$$

Proof. Let $\sigma, \tau \in S_n$ and let $\sigma(i) = j$, for some $i, j \in \{1, 2, \ldots, n\}$. Then

$$\tau\sigma\tau^{-1}\Big(\tau(i)\Big) = \tau\Big(\sigma(i)\Big) = \tau(j).$$

Hence, whenever i and j appear consecutively in σ, $\tau(i)$ and $\tau(j)$ appear consecutively in $\tau\sigma\tau^{-1}$. □

Proposition 3.18. *Two elements in S_n are conjugate if and only if they have the same cycle structure.*

Proof. By Proposition 3.17, conjugate elements in S_n have the same cycle structure. Conversely, suppose that σ_1 and σ_2 have the same cycle structure. Define τ to be the map that sends the i^{th} integer in σ_1 to the i^{th} integer in σ_2. This is a permutation. Proposition 3.17 ensures that $\tau\sigma_1\tau^{-1} = \sigma_2$, which concludes the proof. □

Remark 3.19. Note that there could be many different τ conjugating σ_1 into σ_2.

Remark 3.20. Conjugate elements belong to the same conjugacy class.

Proposition 3.21. *The number of conjugacy classes of S_n equals the number of partitions of n.*

Proof. Observe that each cycle type in S_n is a partition of n. Observe also that there is a bijection between the conjugacy classes of S_n and its cycle types. □

3.4 Conjugacy classes in S_6

The symmetric group S_6 has $6! = 720$ elements. There are 11 partitions of the integer 6. Hence, by Proposition 3.21, there are 11 conjugacy classes of S_6. By Proposition 3.18, each conjugacy class consists of elements of the same cycle structure, or cycle *type*. These correspond to one of the partitions of 6, as seen in the first two columns of Table 1. The last column of Table 1 lists the number of elements in each conjugacy class of S_6. To decide how many elements there are in a conjugacy class of S_6, one could follow a combinatorial argument. We show two examples of such an argument and then conclude with a general formula.

To count the total number of elements in the conjugacy class represented by $(12)(345)$, start with the 2-cycle. There are 6 choices for the first number and 5 choices for the second number. That makes $6 \cdot 5$ possibilities. However, since $(ij) = (ji)$, we need to divide by 2. This gives $(6 \cdot 5)/2$ possibilities for the 2-cycle. Similarly, for the 3-cycle, there are 4 choices for the first number (since two numbers are already occupied by the 2-cycle), 3 choices for the second number and 2 choices for the third number. Again, since $(ijk) = (jki) = (kij)$, we need to divide by 3. This gives $(4 \cdot 3 \cdot 2)/3$ possibilities for the 3-cycle. Since the 2-cycle and the 3-cycle

Table 1: A description of the conjugacy classes of the symmetric group S_6.

Partition	Cycle structure	Order	Parity	Number of such
1,1,1,1,1,1	e	1	even	1
1,1,1,1,2	(12)	2	odd	15
1,1,1,3	(123)	3	even	40
1,1,4	(1234)	4	odd	90
1,5	(12345)	5	even	144
6	(123456)	6	odd	120
1,1,2,2	(12)(34)	2	even	45
1,2,3	(12)(345)	6	odd	120
2,4	(12)(3456)	4	even	90
2,2,2	(12)(34)(56)	2	odd	15
3,3	(123)(456)	3	even	40
				720

are disjoint, they commute. However, this does not cause any counting problems, since $(12)(345) \neq (34)(512)$. Thus, the total number of elements in the conjugacy class represented by (12)(345) is

$$\frac{6 \cdot 5}{2} \cdot \frac{4 \cdot 3 \cdot 2}{3} = 120.$$

To compute the number of elements in the conjugacy class represented by (12)(34), the process is similar. For the first 2-cycle, there are $(6 \cdot 5)/2$ possibilities. For the second 2-cycle, there are $(4 \cdot 3)/2$ possibilities. Here, the fact that the two disjoint cycles commute matters. Note that $(12)(34) = (34)(12)$, which implies that we need to divide by 2. This over-counting occurs because both cycles are of the same length, and therefore, no choice is made of which exact cycle a number belongs to. (Compare with the previous example, where the two cycles were of different length.) It follows that the total number of elements in the conjugacy class represented by (12)(34) is

$$\frac{6 \cdot 5}{2} \cdot \frac{4 \cdot 3}{2} \Big/ 2 = 45.$$

This process could of course be generalized, as follows. Let $\sigma \in S_n$ be a permutation in factorized form (all cycles are disjoint). Let $r_i \in \{r_1, r_2, \ldots, r_l\}$ denote the length of each cycle type present in σ. Let m_i denote the number of each cycle type r_i. Then $\Sigma_i m_i r_i = n$. The number of ways to arrange n letters is given by $n!$. For each r-cycle, divide by r to compensate for the cyclical permutations of each r-cycle. In particular, divide by r^m if there are m cycles of length r. Whenever there is more

than one r-cycle of the same length, divide by $m_i!$ for each r_i, to compensate for the number of possible arrangements of the cycles of the same length. In sum, the number of conjugates of σ is given by

$$\frac{n!}{\Pi_i r_i^{m_i} m_i!}. \tag{2}$$

3.5 Centralizers in S_6

Understanding conjugacy classes is closely related to understanding centralizers. When the action of a G-set is conjugation, the stabilizer

$$\mathsf{Stab}(\mathsf{a}) = \{g \in G \mid g \cdot a = gag^{-1} = a\}$$

of an element $a \in G$ is equal to the centralizer

$$\mathsf{Cent}_G(a) = \{g \in G \mid ga = ag\} = \{g \in G \mid gag^{-1} = a\}.$$

Thus, the Orbit-Stabilizer Theorem (Theorem 2.4) relates the size of a conjugacy class with the size of the centralizer, by equating the size of the conjugacy class of an element $\sigma \in S_6$ with the number of left cosets of $\mathsf{Cent}_{S_6}(\sigma)$ in S_6. Note that centralizers of conjugate elements are of the same order, so the order of the centralizer of an element is an invariant of the conjugacy class. Since S_6 is a finite group of relatively small size, the elements of the centralizers can be worked out by hand. In Table 2, the third column lists the size of each centralizer and the fourth column lists all elements in each centralizer. The search for understanding the structure behind this leads to a question.

Question 3.22. What kind of elements belong to the centralizers in S_6, and how are they structured?

For every $\sigma \in S_6$, the centralizer $\mathsf{Cent}_{S_6}(\sigma)$ contains powers of σ, since

$$\sigma^m \sigma^n = \sigma^{m+n} = \sigma^n \sigma^m,$$

for integers m, n. Any $\tau \in S_6$ disjoint from σ also belongs to $\mathsf{Cent}_{S_6}(\sigma)$, since disjoint cycles commute. Compositions of elements of these two types naturally also belong to $\mathsf{Cent}_{S_6}(\sigma)$. We will refer to these types of elements as the *fundamental* elements of the centralizer. If $\sigma \in S_6$ consists of at most one r-cycle, then for every $1 < r \leq 6$,

Table 2: The elements in the centralizers of conjugacy classes of S_6. Note that while the size of the centralizer is an invariant of the conjugacy class, the exact elements may differ. The elements listed in the fourth column are the ones in the centralizers of the elements listed in the first column.

Representative $\sigma \in S_6$	Size of conj. class	Size of centralizer	Elements in the centralizer of σ
id	1	720	All of S_6
(12)	15	48	$id, (12), (34), (35), (36), (45), (46), (56), (345), (346),$ $(354), (356), (364), (365), (456), (465), (3456), (3465),$ $(3546), (3564), (3645), (3654), (34)(56), (35)(46), (36)(45)$ $(12)(34), (12)(35), (12)(36), (12)(45), (12)(46), (12)(56),$ $(12)(34)(56), (12)(35)(46), (12)(36)(45),$ $(12)(345), (12)(346), (12)(354), (12)(356),$ $(12)(364), (12)(365), (12)(456), (12)(465), (12)(3456),$ $(12)(3465), (12)(3546), (12)(3564), (12)(3645), (12)(3654)$
(123)	40	18	$id, (123), (132), (45), (46), (56), (456), (465)$ $(123)(45), (123)(46), (123)(56), (123)(456), (123)(465),$ $(132)(45), (132)(46), (132)(56), (132)(456), (132)(465)$
(1234)	90	8	$id, (1234), (13)(24), (1432)$ $(56), (1234)(56), (13)(24)(56), (1432)(56)$
(12345)	144	5	$id, (12345), (13524), (14253), (15432)$
(123456)	120	6	$id, (123456), (135)(246), (14)(25)(36), (153)(264), (165432)$
(12)(34)	45	16	$id, (12)(34), (12), (34), (56), (12)(34)(56), (12)(56),$ $(34)(56), (13)(24), (14)(23), (13)(24)(56), (14)(23)(56)$ $(1324), (1423), (1324)(56), (1423)(56)$
(12)(345)	120	6	$id, (12), (345), (12)(345),$ $(345)^2 = (354), (12)(345)^2 = (12)(354)$
(12)(3456)	90	8	$id, (12), (3456), (12)(3456),$ $(3456)^2 = (35)(46), (12)(3456)^2 = (12)(35)(46),$ $(3456)^3 = (3654), (12)(3456)^3 = (12)(3654)$
(12)(34)(56)	15	48	$id, (12), (34), (56), (12)(34), (12)(56), (34)(56), (12)(34)(56)$ $(12)(35)(46), (12)(36)(45), (13)(24)(56), (14)(23)(56),$ $(15)(26)(34), (16)(25)(34), (35)(46), (36)(45), (13)(24),$ $(14)(23), (15)(26), (16)(25), (1324), (1324)(56), (1432),$ $(1432)(56), (3546), (3546)(12), (3645), (3645)(12),$ $(1526), (1526)(34), (1625), (1625)(34), (135246), (153264),$ $(146235), (164253), (136245), (145236), (154263), (163254)$ $(154)(326), (136)(524), (163)(425), (145)(623),$ $(164)(325), (153)(426), (146)(523), (135)(624)$
(123)(456)	40	18	$id, (123), (456), (132), (465), (123)(456), (123)(465),$ $(132)(456), (132)(465), (14)(25)(36), (16)(24)(35), (15)(26)(34),$ $(142536), (143625), (152634), (153426), (162435), (163524)$

there are only fundamental elements in $\mathsf{Cent}_{S_6}(\sigma)$. If for some $1 < r \leq 6$, σ consists of more than one r-cycle, $\mathsf{Cent}_{S_6}(\sigma)$ contains not only fundamental elements, but also other kinds of elements. This applies to the conjugacy classes of type $(2,2)$, type $(2,2,2)$ and type $(3,3)$.

Of the centralizers that consist only of fundamental elements, the three cyclic ones are perhaps the simplest:

$$\begin{aligned}
\sigma = (12345) &: \mathsf{Cent}_{S_6}(\sigma) = \langle \sigma \rangle \cong \mathbb{Z}/5 \\
\sigma = (123456) &: \mathsf{Cent}_{S_6}(\sigma) = \langle \sigma \rangle \cong \mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3 \\
\sigma = (12)(345) &: \mathsf{Cent}_{S_6}(\sigma) = \langle \sigma \rangle \cong \mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3.
\end{aligned}$$

Almost as simple, but non-cyclic, are

$$\begin{aligned}
\sigma = (1234), \tau = (56) &: \mathsf{Cent}_{S_6}(\sigma) = \langle \sigma, \tau \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/4 \\
\sigma = (12), \tau = (3456) &: \mathsf{Cent}_{S_6}(\sigma\tau) = \langle \sigma, \tau \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/4.
\end{aligned}$$

The remaining two centralizers that consist of only fundamental elements, $\mathsf{Cent}_{S_6}\Big((12)\Big)$ and $\mathsf{Cent}_{S_6}\Big((123)\Big)$, do not admit as easy a presentation. But note that

$$\mathsf{Cent}_{S_6}\Big((123)\Big) \cong \mathsf{Cent}_{S_6}\Big((123)(456)\Big),$$

where if $\sigma = (123), \tau = (142563)$, and $\pi = (162435)$, then

$$\mathsf{Cent}_{S_6}\Big((123)(456)\Big) = \langle \sigma, \tau \,|\, \sigma^3 = \tau^6 = 1, \sigma\tau\sigma^{-1} = \pi \rangle \cong \mathbb{Z}/3 \times \mathbb{Z}/6.$$

The 9 non-fundamental elements in $\mathsf{Cent}_{S_6}\Big((123)(456)\Big)$ are 6-cycles and elements of type $(2,2,2)$. It remains to describe the centralizers of $(12)(34)$ and $(12)(34)(56)$.

In $\mathsf{Cent}_{S_6}\Big((12)(34)\Big)$, the non-fundamental elements are 4-cycles and elements of type $(2,2)$ that move $1,2,3$ and 4, while fixing 5 and 6. In $\mathsf{Cent}_{S_6}\Big((12)(34)(56)\Big)$, the non-fundamental elements are 6-cycles, 4-cycles and elements of type $(3,3)$, type $(4,2)$, type $(2,2)$ and type $(2,2,2)$.

4 Automorphisms

An isomorphism from a group G to itself is called an *automorphism*. The set of all automorphisms is denoted $\mathsf{Aut}(G)$ and is a group under function composition. Note that $\mathsf{Aut}(G)$ consists of permutations of G and thus is a subgroup of S_G.

Proof. Let $\varphi, \psi \in \mathsf{Aut}(G)$. The composition $\psi \circ \varphi$ is a homomorphism, since

$$\begin{aligned}(\psi \circ \varphi)(gh) &= \psi\Big(\varphi(gh)\Big) \\ &= \psi\Big(\varphi(g)\varphi(h)\Big) && \varphi \text{ homomorphism} \\ &= \psi\Big(\varphi(g)\Big)\psi\Big(\varphi(h)\Big) && \psi \text{ homomorphism} \\ &= (\psi \circ \varphi)(g)(\psi \circ \varphi)(h).\end{aligned} \tag{3}$$

Since ψ and φ share domain and range, $\psi \circ \varphi$ is a well-defined bijection. Now, the identity map is the identity element. Since every $\varphi \in \mathsf{Aut}(G)$ is bijective, there exists $\varphi^{-1} \in \mathsf{Aut}(G)$. Composition of functions is associative, hence $\mathsf{Aut}(G)$ is a group.

By closure and existence of inverses, $\varphi\,\psi^{-1} \in \mathsf{Aut}(G)$. By the subgroup criterion (e.g., [DF04, p. 47], Proposition 1 in Section 2.1), $\mathsf{Aut}(G) \leq S_G$. □

Example 4.1. Any permutation that does not fix the identity element cannot be an automorphism. Thus, in case G is finite, $\mathsf{Aut}(G)$ is always a proper subgroup of S_G.

To better understand automorphism groups and what they could look like, we continue this section by providing examples of automorphism groups for different groups, before moving on to defining inner (Section 4.1) and outer (Section 4.2) automorphism groups.

Example 4.2. Infinite groups can have finite automorphism groups. If $\mathbb{Z}$ is the additive group of integers, then $\mathsf{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2$. To see this, let $G = \langle x \rangle$ be an infinitely cyclic group. There are two generators of this group: x and x^{-1}. Let $\varphi \in \mathsf{Aut}(G)$ be an automorphism of G. Then $\varphi(x)$ has to be a generator, since φ in particular is an isomorphism and must send generators to generators. But G has only two generators, so either $\varphi(x) = x$ or $\varphi(x) = x^{-1}$. Thus, there are two possible automorphisms of G only and therefore $\mathsf{Aut}(G) \cong \mathbb{Z}/2$. But $G \cong \mathbb{Z} = \langle 1 \rangle$, which is also infinitely cyclic. Therefore, $\mathsf{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2$. Geometrically, the two automorphisms of $\mathbb{Z}$ (represented as a number line) can be thought of as either fixing the number line or flipping it around 0.

Example 4.3. Let $V = \{a, b \mid a^2 = b^2 = (ab)^2 = 1\}$ denote the Klein 4-group. An automorphism of V must fix 1. The remaining three elements are all of order 2, and any two of them generate the whole group. Thus, the automorphisms of V are the permutations of these three elements. The automorphism group of V,

$$\mathsf{Aut}(V) \cong S_3$$

is isomorphic to the symmetric group of order 6. As such, this is an example of an automorphism group whose order is greater than the order of the group in question.

Lemma 4.4. *An automorphism $\varphi \in \mathsf{Aut}(G)$ of a finitely generated group G is determined by its action on the generators $g_1, \ldots, g_n$ of G.*

Proof. Let G be a group generated by $g_1, \ldots, g_n$. For any element $g \in G$,

$$g = g_1^{m_1} \cdot g_2^{m_2} \cdot \ldots \cdot g_n^{m_n}$$

with $0 \leq m_i$. Let $\varphi \in \mathsf{Aut}(G)$. Since φ is a homomorphism,

$$\varphi(g_1^{m_1} \cdot \ldots \cdot g_n^{m_n}) = \varphi(g_1^{m_1}) \cdot \ldots \cdot \varphi(g_n^{m_n}) = \varphi(g_1)^{m_1} \cdot \ldots \cdot \varphi(g_n)^{m_n}.$$

□

Example 4.5. Let $\mathbb{Z}/p$ be a cyclic group of prime order p. Then

$$(\mathbb{Z}/p)^\times \cong \mathsf{Aut}(\mathbb{Z}/p), \tag{4}$$

where $(\mathbb{Z}/p)^\times$ is the group of units of $\mathbb{Z}/p$.

Let $\varphi \in \mathsf{Aut}(\mathbb{Z}/p)$. Since the additive group $\mathbb{Z}/p$ is cyclic of prime order p, any non-zero element is a generator. In particular, $\mathbb{Z}/p = \langle \bar{1} \rangle$. By Lemma 4.4, φ is determined by where it sends $\bar{1}$. Assume that $\varphi(\bar{1}) = \overline{a} \in \mathbb{Z}/p$. Then $\overline{a}$ is a generator. For any $x \in \mathbb{Z}/p$,

$$\varphi(x) = \varphi(x \cdot \bar{1}) = \varphi(\underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{x \text{ times}}) = x \cdot \varphi(\bar{1}) = x \cdot \overline{a}.$$

Therefore, any automorphism of $\mathbb{Z}/p$ is multiplication by some $\overline{a} \in \mathbb{Z}/p$. Since φ is a bijection, there exists $\varphi^{-1} \in \mathsf{Aut}(\mathbb{Z}/p)$. Hence, $\overline{a}$ needs to be a unit element. We

denote this multiplication map by

$$\begin{aligned} m_{\overline{a}} : \mathbb{Z}/p &\to \mathbb{Z}/p \\ x &\mapsto x \cdot \overline{a}, \end{aligned}$$

which is an automorphism whenever $\overline{a} \in (\mathbb{Z}/p)\backslash\{\bar{0}\} = (\mathbb{Z}/p)^\times$. An explicit isomorphism to motivate Eq. (4) is then given by

$$\begin{aligned} \psi : (\mathbb{Z}/p)^\times &\to \mathsf{Aut}(\mathbb{Z}/p) \\ \overline{a} &\mapsto m_{\overline{a}}. \end{aligned}$$

Lemma 4.6. *Let $\varphi \in \mathsf{Aut}(G)$ be an automorphism of a group G. Then φ preserves conjugacy classes: if $g, h \in G$ are conjugate, then so are $\varphi(g)$ and $\varphi(h)$.*

Proof. If g and h are conjugate, then there exists $r \in G$ such that $g = rhr^{-1}$. But then

$$\varphi(g) = \varphi(rhr^{-1}) = \varphi(r)\varphi(h)\varphi(r^{-1}) = \varphi(r)\varphi(h)\varphi(r)^{-1},$$

which shows that $\varphi(g)$ and $\varphi(h)$ are conjugate. □

Lemma 4.7. *Automorphisms preserve the order of group elements:*

$$|\varphi(g)| = |g| \quad \textit{for all } \varphi \in \mathsf{Aut}(G),\ g \in G.$$

The order of $\varphi(g)$ is infinite if and only if the order of g is infinite.

Proof. Let G be a group, let $\varphi \in \mathsf{Aut}(G)$ and let $g \in G$ be an element of order m. Then

$$1 = \varphi(1) = \varphi(g^m) = \varphi(g)^m.$$

Hence the order of $\varphi(g)$ divides m.

Since φ is a bijection, it has an inverse. Let $\varphi(g) = h$ be an element of order n. Then

$$1 = \varphi^{-1}(1) = \varphi^{-1}(h^n) = \varphi^{-1}(h)^n = g^n.$$

Hence the order of g divides n. But then $n \mid m$ and $m \mid n$, so $m = n$.

Suppose that the order of g is infinite. Then the order of $\varphi(g)$ cannot be finite, because if it is finite, then $\varphi(g)^n = 1$ for some n. But then

$$1 = \varphi^{-1}(1) = \varphi^{-1}(\varphi(g)^n) = g^n,$$

which contradicts the order of g being infinite. The other direction is analogous. $\square$

Remark 4.8. If φ is a homomorphism, not necessarily a bijection, then the order of $\varphi(g)$ divides the order of g.

Example 4.9. The projection

$$\begin{aligned} \varphi : \mathbb{Z}/2 \times \mathbb{Z}/3 &\to \mathbb{Z}/2 \\ (a, b) &\mapsto a \end{aligned}$$

is a non-bijective homomorphism. In particular, $|\varphi(1,1)| = |1| = 2$ is a divisor of $|(1,1)| = 6$.

Definition 4.10. If H is a subgroup of a group G, and $\varphi(H) = H$ for every automorphism $\varphi \in \mathsf{Aut}(G)$, we say that H is *characteristic* in G. We denote H char G.

Proposition 4.11. *Let G be a group. Then its center $Z(G)$ is characteristic in G.*

Proof. Let $\varphi \in \mathsf{Aut}(G)$, let $z \in Z(G)$ and let $g \in G$. Since φ is surjective, there exists a $h \in G$ such that $g = \varphi(h)$. Then

$$g\,\varphi(z) = \varphi(h)\varphi(z) = \varphi(hz) = \varphi(zh) = \varphi(z)\varphi(h) = \varphi(z)\,g.$$

Thus, $\varphi(z)$ commutes with every $g \in G$, so $\varphi(z) \in Z(G)$. Hence, $\varphi\Big(Z(G)\Big) \subset Z(G)$.

Since φ is bijective, $\varphi^{-1} \in \mathsf{Aut}(G)$. Applying the same argument gives that $\varphi^{-1}\Big(Z(G)\Big) \subset Z(G)$. But then $Z(G) = \varphi\Big(\varphi^{-1}\Big(Z(G)\Big)\Big) \subset \varphi\Big(Z(G)\Big)$. Hence, $\varphi(Z(G)) = Z(G)$, so $Z(G)$ char G. $\square$

Example 4.12. The dihedral group of order 8 is isomorphic to its automorphism group:

$$\mathsf{Aut}(D_8) \cong D_8.$$

We will show this using the fact that D_8 is a normal subgroup of the dihedral group of order 16,

$$D_{16} = \langle R, s \mid R^8 = s^2 = 1, sRs = R^{-1} \rangle.$$

If D_{16} acts by conjugation, then for any $a \in D_{16}$, the map

$$\begin{aligned} \mathsf{int}_a : D_{16} &\to D_{16} \\ b &\mapsto aba^{-1} \end{aligned}$$

sends D_8 to one of its conjugates. But $aD_8a^{-1} \subset D_8$ for any $a \in D_{16}$, by normality. Thus, $\mathsf{int}_a \in \mathsf{Aut}(D_8)$, for any $a \in D_{16}$. The associated homomorphism of this action is therefore the map

$$\varphi : D_{16} \to \mathsf{Aut}(D_8)$$

with kernel

$$\ker \varphi = \{a \in D_{16} \,|\, aba^{-1} = b, \text{ for all } b \in D_8\} = \mathsf{Cent}_{D_{16}}(D_8),$$

which is exactly the definition of the centralizer of D_8 in D_{16}. Consider

$$\mathsf{Cent}_{D_{16}}(D_8) = \{1, R^4\} = \langle R^4 \rangle.$$

By the kernel-image isomorphism theorem (e.g., [Rot12, p. 35], Theorem 2.24),

$$D_{16}/\langle R^4 \rangle \cong \text{im } \varphi.$$

The order of im φ is then given by

$$|\text{im } \varphi| = \frac{|D_{16}|}{|\langle R^4 \rangle|} = \frac{16}{2} = 8.$$

Since im $\varphi \leq \mathsf{Aut}(D_8)$, there are at least 8 automorphisms of D_8. In fact, D_8 also has at *most* 8 automorphisms. We will use a counting argument to show this. Note that

$$D_8 = \langle r, s \,|\, r^4 = s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

By Lemma 4.4, it is enough to examine the possibilities for $\varphi(r)$ and $\varphi(s)$, to determine the order of $\mathsf{Aut}(D_8)$. As seen in Table 3, the generator r has order 4. By

Table 3: Elements of D_8, sorted by conjugacy classes.

Elements	Order
1	1
r^2	2
r, r^3	4
s, sr^2	2
sr, sr^3	2

Lemma 4.7, an automorphism preserves the order of an element, therefore $\varphi(r)$ is

mapped to either r or $r^3 = r^{-1}$. This gives at most 2 choices for r. Similarly, the generator s has order 2, therefore its image $\varphi(s)$ must have order 2. There are 5 elements of D_8 of order 2, as seen in Table 3. However, there are at most 4 choices for $\varphi(s)$. Why? Consider the center of D_8,

$$Z(D_8) = \{1, r^2\} = \langle r^2 \rangle.$$

By Proposition 4.11, the center is a characteristic subgroup, so φ maps $Z(D_8)$ to itself. Hence, r^2 is not a possible target for s, since s is not in the center. The remaining options for $\varphi(s)$ are s, sr, sr^2 and sr^3. In sum, there are at most 8 automorphisms of D_8, so $|\mathsf{Aut}(D_8)| = 8$.

The natural projection

$$\pi : D_{16} \to D_{16}/\langle R^4 \rangle \cong \text{im } \varphi$$

is a surjective map. Since im $\varphi \leq \mathsf{Aut}(D_8)$, the map

$$\psi : D_{16}/\langle R^4 \rangle \to \mathsf{Aut}(D_8)$$

is injective. But $|\text{im } \varphi| = |\mathsf{Aut}(D_8)| = 8$, so ψ is also surjective, hence, an isomorphism. Indeed, there is an isomorphism

$$D_8 \xrightarrow{\sim} D_{16}/\langle R^4 \rangle$$

defined by sending r to $R\langle R^4 \rangle$ and s to $s\langle R^4 \rangle$. It follows that

$$\mathsf{Aut}(D_8) \cong D_8.$$

4.1 Inner automorphisms

An important example of an automorphism is conjugation.

Definition 4.13. Let G be a group and let $g \in G$. Then for all $h \in G$, the conjugation map

$$\begin{aligned} \mathsf{int}_g : G &\to G \\ h &\mapsto ghg^{-1} \end{aligned}$$

is called an *inner* automorphism. Denote by $\mathsf{Int}(G)$[1] the set of all inner automorphisms of G. This is a group under function composition.

Example 4.14. Let $G = \mathrm{SL}_2(F)$ be the special linear group of degree 2 over a field F. The inverse transpose map

$$\begin{aligned} \varphi : \mathrm{SL}_2(F) &\to \mathrm{SL}_2(F) \\ A &\mapsto {}^{T}A^{-1} \end{aligned}$$

is an inner automorphism. To see this, we first show that φ is an automorphism, then that φ is inner.

Let $A, B \in \mathrm{SL}_2(F)$. Then

$$\varphi(AB) = {}^{T}\Big(AB\Big)^{-1} = {}^{T}(B^{-1}A^{-1}) = \Big({}^{T}A^{-1}\Big)\Big({}^{T}B^{-1}\Big) = \varphi(A)\varphi(B),$$

so φ is a homomorphism. Now let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, \tag{5}$$

with entries in F, such that $A \neq B$. Then

$$\varphi(A) = {}^{T}A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

and

$$\varphi(B) = {}^{T}B^{-1} = \frac{1}{\det(B)} \begin{pmatrix} h & -g \\ -f & e \end{pmatrix} = \begin{pmatrix} h & -g \\ -f & e \end{pmatrix}.$$

Note that $\det(A) = \det(B) = 1$ in $\mathrm{SL}_2(F)$ by definition. Since $A \neq B$, there is at least one index (i, j) where $a_{ij} \neq b_{ij}$. But φ has the same effect on each entry of any matrix in $\mathrm{SL}_2(F)$. Therefore, $\varphi(A) \neq \varphi(B)$, which shows φ is injective. To see that the inverse transpose map is surjective, let $B \in \mathrm{SL}_2(F)$. Indeed, there exist $A \in \mathrm{SL}_2(F)$ with ${}^{T}A^{-1} = B$, since if $A := {}^{T}B^{-1}$, then

$${}^{T}A^{-1} = {}^{T}\Big({}^{T}B^{-1}\Big)^{-1} = B.$$

Thus, the inverse transpose map is an automorphism.

[1]The abbreviation Int comes from the word *interieur*, French for *interior*.

Let A and B be as in (5). Consider

$$BAB^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} h & -f \\ -g & e \end{pmatrix}$$

and let $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(F)$. Then

$$BAB^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = {}^{T}A^{-1} = \varphi(A),$$

for all $A \in \mathrm{SL}_2(F)$. Hence, φ is an inner automorphism.

Proposition 4.15. *There is a homomorphism*

$$\begin{aligned} \varphi : G &\to \mathsf{Aut}(G) \\ g &\mapsto \mathsf{int}_g \end{aligned}$$

where int_g *is the conjugation map, for which* $\ker\varphi = Z(G)$ *and im* $\varphi = \mathsf{Int}(G)$.

Proof. Let $g, h \in G$. Then for all $a \in G$,

$$\begin{aligned} \varphi(gh)(a) &= \mathsf{int}_{(gh)}(a) && \text{by def. of } \varphi \\ &= (gh)a(gh)^{-1} && \text{by def. of } \mathsf{int} \\ &= g(hah^{-1})g^{-1} \\ &= \mathsf{int}_g\Big(\mathsf{int}_h(a)\Big) && \text{by def. of } \mathsf{int} \\ &= (\mathsf{int}_g \circ \mathsf{int}_h)(a) \\ &= \mathsf{int}_g(a) \circ \mathsf{int}_h(a) \\ &= \varphi(g)(a) \circ \varphi(h)(a) && \text{by def. of } \varphi. \end{aligned}$$

Hence, φ is a homomorphism. By definition

$$\begin{aligned} \ker\varphi &= \{g \in G \mid \mathsf{int}_g(a) = a \quad \text{for all } a \in G\} \\ &= \{g \in G \mid gag^{-1} = a \quad \text{for all } a \in G\}. \end{aligned} \tag{6}$$

But this is exactly the center of G,

$$Z(G) = \{g \in G \mid ga = ag \quad \text{for all } a \in G\}. \tag{7}$$

Since (6) and (7) are equal, $\ker \varphi = Z(G)$. Lastly, $\operatorname{im} \varphi = \mathsf{Int}(G)$ follows directly from the definition:

$$\operatorname{im} \varphi = \{\varphi(g) \mid g \in G\} = \{\mathsf{int}_g \mid g \in G\} = \mathsf{Int}(G).$$

□

Remark 4.16. It follows that the map

$$\begin{aligned} \varphi : G &\twoheadrightarrow \mathsf{Int}(G) \\ g &\mapsto \mathsf{int}_g \end{aligned}$$

is a surjective homomorphism, considering that $\mathsf{Int}(G)$ is defined to be the image under int_g.

Corollary 4.17. *There is an isomorphism* $G/Z(G) \cong \mathsf{Int}(G)$.

Proof. The corollary follows from Proposition 4.15 and the kernel-image isomorphism theorem (e.g., [Rot12, p. 35], Theorem 2.24). □

Definition 4.18. Let G be a group. If $Z(G) = \{1\}$ we say that G is *centerless*.

Example 4.19. If G is commutative, then $Z(G) = G$. It follows that $\mathsf{Int}(G)$ is trivial.

Example 4.20. If G is centerless, then $Z(G) = \{1\}$. It follows that $\mathsf{Int}(G) \cong G$.

Remark 4.21. Note that in terms of commutativity, a centerless group is "as far as possible" from being abelian. Thus, the center of a group can be regarded as a measure of how commutative the group is. However, note that since

$$gag^{-1} = a \iff ga = ag,$$

conjugation is also a measure of how far a group is from being commutative. Thus, $\mathsf{Int}(G)$ measures "how commutative" a group is. We formalize this in the following proposition.

Proposition 4.22. *The group of inner automorphisms* $\mathsf{Int}(G)$ *of a group* G *is trivial if and only if* G *is commutative.*

Proof. Suppose that $\mathsf{Int}(G)$ is trivial. Then $\mathsf{int}_g(a) = gag^{-1} = a$ for all $g, a \in G$. But this is equivalent to $ga = ag$ for all $g, a \in G$. Thus, G is commutative.

Now suppose that G is commutative. Then $ga = ag$ for all $g, a \in G$. But then $gag^{-1} = a$ for every $g \in G$, so every inner automorphism is trivial. □

Proposition 4.23. *Let G be a group and let $\mathsf{Int}(G)$ be the group of inner automorphisms of G. Then*

$$G \cong \mathsf{Int}(G)$$

if and only if G is centerless.

Proof. This follows from Corollary 4.17. □

Proposition 4.24. *Let G be a centerless group and $\mathsf{Aut}(G)$ the group of automorphisms of G. Then*

$$G \cong \mathsf{Aut}(G)$$

if and only if every automorphism of G is inner.

Proof. This follows from Proposition 4.15 together with the kernel-image isomorphism theorem (e.g., [Rot12, p. 35], Theorem 2.24). □

Remark 4.25. In Corollary 5.7, we will see that Proposition 4.24 applies to almost every symmetric group.

Question 4.26. What about the relation between $\mathsf{Int}(G)$ and $\mathsf{Aut}(G)$? We explore this in Section 4.2.

4.2 Outer automorphisms

Lemma 4.27. *The subgroup $\mathsf{Int}(G)$ is normal in $\mathsf{Aut}(G)$.*

Proof. Let $\varphi \in \mathsf{Aut}(G)$ and let $\mathsf{int}_a \in \mathsf{Int}(G)$. Then for all $g \in G$,

$$\begin{aligned}
(\varphi\, \mathsf{int}_a\, \varphi^{-1})(g) &= \varphi\left(\mathsf{int}_a\big(\varphi^{-1}(g)\big)\right) \\
&= \varphi\big(a\, \varphi^{-1}(g)\, a^{-1}\big) && \text{by def. of } \mathsf{int}_a \\
&= \varphi(a) \cdot \varphi\big(\varphi^{-1}(g)\big) \cdot \varphi(a^{-1}) \\
&= \varphi(a) \cdot g \cdot \varphi(a)^{-1} \\
&= \mathsf{int}_{\varphi(a)}(g) \in \mathsf{Int}(G) && \text{by def. of } \mathsf{int}_{\varphi(a)}.
\end{aligned}$$

Hence, $\mathsf{Int}(G) \lhd \mathsf{Aut}(G)$. □

Knowing that $\mathsf{Inn}(G)$ is a normal subgroup of $\mathsf{Aut}(G)$, we can define what an outer automorphism is.

Definition 4.28. The group

$$\mathsf{Out}(G) := \mathsf{Aut}(G)/\mathsf{Inn}(G) = \{\varphi\,\mathsf{Inn}(G) \mid \varphi \in \mathsf{Aut}(G)\}$$

is called the outer automorphism group of G.

Remark 4.29. A less rigorous definition of an outer automorphism is that $\varphi \in \mathsf{Aut}(G)$ is outer if it is not inner.

Example 4.30. If G is a commutative group, then $\mathsf{Inn}(G)$ is trivial. It follows that all non-trivial automorphisms of a commutative group are outer.

Example 4.31. If $\mathsf{Aut}(G) = \mathsf{Inn}(G)$ for a group G, then the outer automorphism group is trivial.

Example 4.32. We revisit Example 4.12, where we showed that $\mathsf{Aut}(D_8) \cong D_8$.[2] Here, we examine $\mathsf{Aut}(D_8)$ in more detail.

Since $|Z(D_8)| = 2$, then by Corollary 4.17,

$$|\mathsf{Inn}(D_8)| = |D_8|/|Z(D_8)| = 4.$$

Recall that, by Lemma 4.4, an automorphism is determined by its action on the generators of the group. Little computation is needed to see that the four inner automorphisms of D_8 are the ones shown in Table 4.

Table 4: Inner automorphisms φ_i of D_8, determined by $\varphi(r)$ and $\varphi(s)$. The fourth column lists the conjugating elements for each $\varphi_i \in \mathsf{Aut}(D_8)$.

φ_i	$\varphi(r)$	$\varphi(s)$	Conj. by
φ_1	r	s	$1, r^2$
φ_2	r	sr^2	r, r^3
φ_3	r^3	s	s, sr^2
φ_4	r^3	sr^2	sr, sr^3

But what about the remaining four automorphisms of D_8? The group of outer automorphisms of D_8 is non-trivial, since

$$|\mathsf{Out}(D_8)| = |\mathsf{Aut}(D_8)|/|\mathsf{Inn}(D_8)| = 2.$$

[2] We also inherit the established notation, with r being a generator for D_8 and R being a generator for D_{16}.

Recall that $\mathsf{Out}(D_8) \cong \mathbb{Z}/2$ means there are two *cosets* of inner automorphisms in $\mathsf{Aut}(D_8)$. Considering the order of the elements in D_8, one can conclude that the outer automorphisms of D_8 are the ones listed in Table 5. Note that there is by definition no element in D_8 with which one could form a conjugation map, hence the absence of such a column in Table 5.

Table 5: Outer automorphisms φ_i of D_8, determined by $\varphi(r)$ and $\varphi(s)$.

φ_i	$\varphi(r)$	$\varphi(s)$
φ_5	r	sr
φ_6	r	sr^3
φ_7	r^3	sr
φ_8	r^3	sr^3

Recall that $D_8 \lhd D_{16}$ and note that $\mathsf{Aut}(D_8) \subset \mathsf{Aut}(D_{16})$. Interestingly, for every $\varphi \in \mathsf{Aut}(D_8)$ (both inner and outer), $\varphi \in \mathsf{Int}(D_{16})$. As a subgroup of D_{16}, D_8 can be presented as

$$D_8 \cong H = \langle R^2, s \mid R^8 = s^2 = 1, sRs^1 = R^{-1} \rangle \lhd D_{16}.$$

A revisit of the automorphisms of D_8, this time expressed as inner automorphisms of D_{16}, is done accordingly in Table 6.

Table 6: Automorphisms of D_8 expressed in terms of automorphisms of D_{16}. "Inner" means conjugation by an element in D_8. "Outer" means conjugation by an element in $D_{16} \backslash D_8$.

Automorphisms of D_8 within D_{16}							
"Inner"				"Outer"			
φ_i	$\varphi(R^2)$	$\varphi(s)$	Conj. by	φ_i	$\varphi(R^2)$	$\varphi(s)$	Conj. by
φ_1	R^2	s	$1, R^4$	φ_5	R^2	sR^2	R^3, R^7
φ_2	R^2	sR^4	R^2, R^6	φ_6	R^2	sR^6	R, R^5
φ_3	R^6	s	s, sR^4	φ_7	R^6	sR^2	sR, sR^5
φ_4	R^6	sR^4	sR^2, sR^6	φ_8	R^6	sR^6	sR^3, sR^7

Remark 4.33. In fact, this result generalizes to dihedral groups of order $4n$:

$$D_{4n} = \langle r, s \mid r^{2n} = s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

5 Automorphisms of the symmetric group

In this section, we consider automorphisms of S_n, illustrating the theory presented in Section 4. We begin with a proposition showing that S_n is centerless for $n \geq 3$. Note that $S_2 \cong \mathbb{Z}/2$ and thus, has a non-trivial center.

Proposition 5.1. *If $n \geq 3$, then the center $Z(S_n) = \{1\}$.*

Proof. Let $\sigma \in S_n$ be a non-identity element. Then there exists $i, j \in \{1, 2, \ldots, n\}$ such that $\sigma(i) = j \neq i$. Since $n \geq 3$, there exists $k \in \{1, 2, \ldots, n\}$ such that $k \neq i$ and $k \neq j$. Let $\tau = (j\, k) \in S_n$. Then τ fixes i, so that $\sigma\tau(i) = \sigma(i) = j$. But $\tau\sigma(i) = \tau(j) = k$. Since $k \neq j$, clearly $\tau\sigma \neq \sigma\tau$. Thus, we have found an element that does not commute with σ. It follows that if $n \geq 3$, then for any non-identity element $\sigma \in S_n$, it is always possible to find an element $\tau \in S_n$ with which σ does not commute. Hence, $Z(S_n) = \{1\}$. □

Corollary 5.2. *If $n \geq 3$, then $S_n \cong \mathsf{Int}(S_n)$.*

Proof. This follows by Corollary 4.17 and Proposition 5.1. □

Later, in Corollary 5.7, we will see that S_n in fact admits an isomorphism $S_n \cong \mathsf{Aut}(S_n)$, for $n \neq 2, n \neq 6$. Recall that S_2 fails to admit this isomorphism due to its commutativity and, hence, non-trivial center. We will see that S_6 fails to induce this isomorphism because not every automorphism is inner.

Lemma 5.3. *An automorphism φ of S_n is inner if and only if it stabilizes the conjugacy class of transpositions.*

Proof. Let φ be an automorphism of S_n. By Proposition 3.17, conjugation preserves cycle type. Hence, if φ is inner, then it stabilizes the conjugacy class of transpositions.

Conversely, suppose that φ stabilizes the conjugacy class of transpositions. By Lemma 4.4, it is enough to show that there exists $\tau \in S_n$ such that $\varphi(\sigma) = \tau\sigma\tau^{-1}$ for all σ in a generating set of S_n. By Theorem 3.15, the elementary transpositions generate S_n.

Since φ is a homomorphism,

$$\varphi(\sigma_i\sigma_j) = \varphi(\sigma_i)\varphi(\sigma_j)$$

for all permutations σ_i, $\sigma_j \in S_n$. We assumed that φ stabilizes the conjugacy class of transpositions. Therefore, if σ_i and σ_j are transpositions, then so are $\varphi(\sigma_i)$ and $\varphi(\sigma_j)$. Label the image under φ accordingly, as

$$\begin{aligned}(12) &\mapsto (j_1\, k_1)\\ (23) &\mapsto (j_2\, k_2)\\ (34) &\mapsto (j_3\, k_3)\\ &\vdots\\ (n-2\, n-1) &\mapsto (j_{n-2}\, k_{n-2})\\ (n-1\, n) &\mapsto (j_{n-1}\, k_{n-1}),\end{aligned}$$

for $j_i, k_i \in \{1, 2, \ldots, n\}$. Now, two transpositions commute if and only if they are disjoint. Since (12) and (23) do not commute, $(j_1\, k_1)$ and $(j_2\, k_2)$ need to share an element. Note that $(j_i\, k_i) = (k_i\, j_i)$. We may assume that 1 is sent to j_1 and 2 is sent to k_1, and choose an ordering so that the second of $(j_1\, k_1)$ is the first of $(j_2\, k_2)$. Then $k_1 = j_2$. By the same argument, $(j_3\, k_3)$ needs to share an element with $(j_2\, k_2) = (k_1\, k_2)$. Since (12) and (34) commute, $(j_1\, k_1)$ and $(j_3\, k_3)$ need to be disjoint. Thus, $j_3 = k_2$. Exhausting this argument, and shifting the labelling one step results in the following image under φ:

$$\begin{aligned}(12) &\mapsto (k_1\, k_2)\\ (23) &\mapsto (k_2\, k_3)\\ (34) &\mapsto (k_3\, k_4)\\ &\vdots\\ (n-2\, n-1) &\mapsto (k_{n-2}\, k_{n-1})\\ (n-1\, n) &\mapsto (k_{n-1}\, k_n),\end{aligned}$$

with $k_1, k_2, \ldots, k_n \in \{1, 2, \ldots, n\}$ distinct. It follows that φ is defined by

$$\varphi\Big((i\, i+1)\Big) = (k_i\, k_{i+1}),$$

for $1 \leq i < n$. Define τ as follows:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ k_1 & k_2 & k_3 & \ldots & k_n \end{pmatrix}.$$

By Proposition 3.17,

$$\tau(i\,i+1)\tau^{-1} = \Big(\tau(i)\,\tau(i\,i+1)\Big) = (k_i\,k_{i+1}) = \varphi\Big((i\,i+1)\Big).$$

By construction, $\varphi(\sigma) = \tau\sigma\tau^{-1}$ for every elementary transposition σ. □

Lemma 5.4. *If $n \neq 6$, then every automorphism of S_n is inner.*

Proof. Let $n \geq 2$, $n \neq 6$. Let $\varphi \in \mathsf{Aut}(S_n)$. By Lemma 5.3, it suffices to show that φ stabilizes the conjugacy class of transpositions.

Denote by T_1 the conjugacy class of transpositions in S_n. By Lemma 4.6, $\varphi(T_1)$ is also a conjugacy class. By Lemma 4.7, $\varphi(T_1)$ consists of involutions. An involution in S_n is a product of k disjoint transpositions. Let T_k denote the conjugacy class of k disjoint transpositions. If $k = 1$, then $T_k = T_1$ and we are done. Suppose that $k > 1$. Since φ is a bijection, $|T_1| = |T_k|$, where

$$|T_1| = \frac{n(n-1)}{2}. \tag{8}$$

By formula (2) in Section 3.4,

$$|T_k| = \frac{n!}{2^k k!(n-2k)!}. \tag{9}$$

We will show that if $n \neq 6$, then there is no $k > 1$ such that $|T_1| = |T_k|$.

Equating (8) and (9) gives

$$\frac{n(n-1)}{2} \stackrel{?}{=} \frac{n!}{2^k k!(n-2k)!}.$$

Multiplying both sides by $2^k k!$ and dividing both sides by $n(n-1)$ gives

$$2^{k-1}k! \stackrel{?}{=} \frac{(n-2)!}{(n-2k)!}, \tag{10}$$

which after simplifying the factorials becomes

$$2^{k-1}k! \stackrel{?}{=} (n-2)(n-3)\cdots(n-2k+1). \tag{11}$$

Since $k > 1$, $2^{k-1}k! > 0$. Therefore, the right hand side in Eq. (11) must also be

positive, which implies $n \geq 2k$. Then

$$(n-2)(n-3)\cdots(n-2k+1) \geq (2k-2)(2k-3)\cdots 2\cdot 1 = (2k-2)!. \tag{12}$$

We show that Eq. (10) never holds for $k > 1$. For $k \geq 4$, we prove by induction that

$$(2k-2)! > 2^{k-1}k!, \tag{13}$$

and then treat separately the cases $k = 2$ and $k = 3$.

The base case $k = 4$ satisfies Eq. (13), since

$$(2\cdot 4-2)! = 6! = 720 > 192 = 2^{4-1}4!.$$

Assume that the inequality holds for some $k \geq 4$ and observe that

$$(2k)! = (2k)(2k-1)(2k-2)!.$$

If $k > 1$, then $2k \geq 2$ and $2k-1 \geq k+1$. Therefore,

$$(2k)! \geq 2(k+1)(2k-2)!.$$

By hypothesis,

$$(2k-2)! > 2^{k-1}k!.$$

Therefore,

$$(2k)! > 2^k(k+1)!,$$

so the inequality holds for $k+1$. By the inductive hypothesis, Eq. (13) holds for all $k \geq 4$.

Let $k = 2$. Then Eq. (10) becomes

$$4 \stackrel{?}{=} \frac{(n-2)!}{(n-4)!}.$$

If $n = 2k = 4$, then $RHS = 2$, which is less than 4. If $n = 2k+1 = 5$, then $RHS = 6$, which is greater than 4. For $n > 5$, RHS increases, while LHS remains constant, so the equality never holds.

Let $k = 3$. Then Eq. (10) becomes

$$24 \stackrel{?}{=} \frac{(n-2)!}{(n-6)!}.$$

We assumed that $n \neq 6 = 2k$. Therefore, consider the case when $n = 2k + 1 = 7$. Then $RHS = 5! = 120$, which is greater than 24. For $n > 7$, RHS increases, while LHS remains constant, so the equality never holds.

Since no integers $k > 1, n \neq 6$ satisfy Eq. (10), $k = 1$, which shows that φ stabilizes the conjugacy class of transpositions. By Lemma 5.3, φ is inner. □

Remark 5.5. In the proof of Lemma 5.4, in the case when $k = 3$, Eq. (10) holds for $n = 6$. We will consider this special case in Section 5.1, when discussing outer automorphisms of S_6.

Theorem 5.6. *If $n \neq 2, n \neq 6$, then S_n is centerless and every automorphism is inner.*

Proof. Proposition 5.1 and Lemma 5.4 together prove the theorem. □

Corollary 5.7. *If $n \neq 2, n \neq 6$, then $S_n \cong \mathsf{Aut}(S_n)$.*

Proof. This follows from Proposition 4.24 and Theorem 5.6. □

5.1 Outer automorphisms of S_6

In this section, we aim to show that there exists an outer automorphism of S_6.

Definition 5.8. A subgroup K of S_n is called *transitive* if it acts transitively on the set $\{1, 2, \ldots n\}$.

Lemma 5.9. *There exists a transitive subgroup K of S_6 of order 120 and index 6, isomorphic to S_5.*

Proof. This is a sketch of the proof. For a full proof, see the beginning of the proof of Theorem 3 in [JR82] or the proof of Lemma 7.8 in [Rot12].

By Sylow's theorems (e.g., [DF04], Theorem 18 in Section 4.5), S_5 has 6 Sylow 5-subgroups. The Sylow 5-subgroups are conjugate, so when S_5 acts by conjugation on the set of Sylow 5-subgroups in S_5, $\mathsf{Syl}_5(S_5)$, it acts transitively. The action gives a permutation representation:

$$\rho : S_5 \to S_6.$$

One then shows that ρ is injective, to be able to conclude that $K = \text{im } \rho \leq S_6$ is the desired subgroup. □

Lemma 5.10. *If $K \leq S_6$ is a transitive subgroup of order 120, then K does not contain a transposition.*

Proof. See the proof of Lemma 7.8 in [Rot12] or the proof of Lemma 2 in [JR82]. □

Theorem 5.11. *There exists an outer automorphism of S_6.*

Proof. This is a sketch of the proof. For a full proof, see the proof of Theorem 3 in [JR82] or the proof of Theorem 7.9 in [Rot12].

By Lemma 5.9, there exists a transitive subgroup K of S_6 of order 120. Then S_6 acts on S_6/K by left multiplication, giving the representation:

$$\theta : S_6 \to S_6.$$

Using the fact (or showing) that A_6 is the only proper normal subgroup of S_6, one then shows that θ is injective, and, further, concludes that θ is an automorphism of S_6. The strategy is then to assume that θ is inner and show that this leads to a contradiction with Lemma 5.10. □

Proposition 5.12. $|\mathsf{Out}(S_6)| = 2$

Proof. See the proof of Theorem 7.10 in [Rot12, p. 160] or the proof of Theorem 4 in [JR82]. □

6 Conclusion

In this paper, we learned about inner and outer automorphisms. We provided examples for different groups, such as cyclic groups of prime order, the dihedral group and the special linear group. We specifically learned about the symmetric group. We showed that if an automorphism of S_n stabilizes the conjugacy class of transpositions, then it is inner. Using this result, we also showed that if $n \neq 6$, then every automorphism of S_n is inner. Finally, a proof of the existence of an outer automorphism of S_6 was outlined.

Although this thesis offers an introduction to the topic of automorphisms and symmetric groups, the thesis is nowhere exhaustive on the subject. Additional examples throughout the text could be helpful to some readers, especially those with limited prior knowledge in algebra. Moreover, the author is aware of the selective nature of the presentation. Specifically, the thesis would have benefitted from a clearer implication of the discussion of conjugacy classes and centralizers in S_6. Ideally, one would want to use this knowledge and follow up and understand the consequences of Eq. (10) in the proof of Lemma 5.4 being satisfied when $n = 6$, as this is fundamental in understanding the outer automorphisms of S_6.

For future studies, a natural direction is to properly give a proof of the existence of an outer automorphism of S_6 and, further, show that $\mathsf{Out}(S_6) \cong \mathbb{Z}/2$. In line with [JR82], the next step is to explicitly construct an outer automorphism of S_6. For historical perspectives, a comparison with the proofs by [Ben24] and [Mil58] could be instructive. More interestingly, one could study semidirect products and understand how this relates $\mathsf{Aut}(S_6)$ and $\mathsf{Int}(S_6)$. Finally, further research could extend the study of inner and outer automorphism groups to groups beyond the symmetric group.

References

[Ben24] HA Bender. A new method for the determination of the group of isomorphisms of the symmetric group of degree n. *The American Mathematical Monthly*, 31(6):287–289, 1924.

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra, Third edition*. John Wiley Sons, Inc., 2004.

[Höl95] Otto Hölder. Bildung zusammengesetzter gruppen. *Mathematische Annalen*, 46(3):321–422, 1895.

[JR82] Gerald Janusz and Joseph Rotman. Outer automorphisms of s6. *The American Mathematical Monthly*, 89(6):407–410, 1982.

[Mil58] Donald W Miller. On a theorem of hölder. *The American Mathematical Monthly*, 65(4):252–254, 1958.

[Rot12] Joseph Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012.