OUTER AUTOMORPHISM OF S6

SAHITI DOKE

1. Abstract

The symmetric group S_6 is the only symmetric group with an outer automorphism. The outer automorphism can also be constructed in many different cute ways. This paper covers the proof of the existence of the outer automorphism of S_6 as well as shows different constructions of it.

2. Introduction

Elements of a symmetric group S_n can be represented in the form of an Amida diagram with n vertical edges.

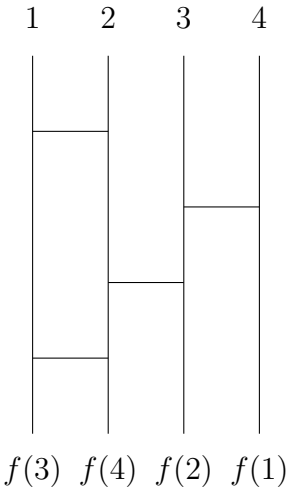

Figure 1. Amida diagram representing the permutation $f \in S_4$ defined by $f(1) = 4$, $f(2) = 3$, $f(3) = 1$, and $f(4) = 2$

In this context, the vertical axes are numbered from 1 to n from left to right. To determine the image $f(i)$ of a number i using a given Amida diagram, we start from the top of the i-th vertical axis and follow the line downward. If we encounter the endpoint of a horizontal edge that joins the current vertical axis with an adjacent one, we move to the opposite vertical axis by crossing the horizontal edge and then continue downward. We determine $f(i) = j$ if we finally reach the bottom of the j-th vertical axis. By definition, distinct numbers map to different numbers, so f is a permutation, $f \in S_n$.

When $f, g \in S_n$ are determined by Amida diagrams as described, we can construct another Amida diagram by concatenating the two diagrams, with the diagram for f attached at the

bottom of the one for g. The resulting Amida diagram defines the product $f \cdot g \in S_n$. Conversely, we can construct another Amida diagram by turning the diagram for f upside down, corresponding to the inverse f^{-1} of f.

Conversely, given an element f of S_n, we can construct an Amida diagram to represent f as follows: First, for the number i that is mapped by f to n, we join the i-th and $(i+1)$-th vertical axes with a horizontal edge, then join the $(i+1)$-th and $(i+2)$-th vertical axes with another horizontal edge, and so on, until we join the $(n-1)$-th and n-th vertical axes with a horizontal edge. These edges guide the number i to the n-th vertical axis correctly. Next, we guide the number mapped by f to $n-1$ to the $(n-1)$-th vertical axis correctly by joining vertical axes, except for the n-th vertical axis, with horizontal edges in a similar way. After these two numbers have correctly moved to the $(n-1)$ and n-th vertical axes, respectively, we iterate this process recursively to obtain the desired Amida diagram corresponding to f.

3. Acknowledgements

I would like to thank Emma Cardwell and Simon Rubinstein-Salzedo for providing guidance to help me write this paper.

4. Body

Definition 1. *A transposition is a permutation which exchanges two elements and keeps all others fixed.*

Proposition 1. *The symmetric group on $\{1, 2, \ldots, n\}$ is generated by the permutations*

$$(1\ 2), (2\ 3), \ldots, (n-1\ n).$$

Proof. We will prove this by induction on n.

For $n = 2$, the statement is trivially true since the group consists only of the identity and a single transposition.

Now, assume that permutations of n elements are generated by transpositions of successive elements. Let ϕ be a permutation of $\{1, 2, \ldots, n+1\}$. If $\phi(n+1) = n+1$, then the restriction of ϕ to $\{1, 2, \ldots, n\}$ is a permutation of n elements, which by the induction hypothesis, can be expressed as a product of adjacent transpositions.

Suppose instead that $\phi(n+1) = m$ with $m \neq n+1$. Consider the following product of transpositions:

$$(n+1\ m)(n\ n+1)\cdots(m+1\ m+2)(m\ m+1).$$

It is evident that this product of transpositions maps m to $n+1$. Therefore, applying the permutation

$$(n+1\ m)(n\ n+1)\cdots(m+1\ m+2)(m\ m+1)\phi$$

to $n+1$ results in $n+1$. Consequently, the restriction of this permutation to $\{1, 2, \ldots, n\}$ is a permutation of n elements, and by the induction hypothesis, it can be expressed as a product of adjacent transpositions. Since a transposition is its own inverse, ϕ can also be expressed as a product of transpositions. □

Lemma 1. *If $\alpha, \beta \in S_n$, then $\alpha\beta\alpha^{-1}$ is the permutation with the same cycle structure as β which is obtained by applying α to the symbols in β.*

Example 1. *If $\beta = (1)(3)(247)$ and $\alpha = (2)(56)(143)$, then*

$$\alpha\beta\alpha^{-1} = (\alpha(1)\alpha(3))(\alpha(2)\alpha(4)\alpha(7)) = (4)(1)(537).$$

Proof. Let γ be the permutation defined in the lemma. If β fixes a symbol i, then γ fixes $\alpha(i)$, for $\alpha(i)$ resides in a 1-cycle; but $\alpha\beta\alpha^{-1}(\alpha(i)) = \alpha\beta(i) = \alpha(i)$, and so $\alpha\beta\alpha^{-1}$ fixes $\alpha(i)$ as well. Assume that β moves i; say, $\beta(i) = j$. Let the complete factorization of β be

$$\beta = \gamma_1\gamma_2 \cdots (\cdots i\, j \cdots) \cdots \gamma_t.$$

If $\alpha(i) = k$ and $\alpha(j) = l$, then $\gamma : k \to l$. But $\alpha\beta\alpha^{-1}$: $k \to l \to \ldots$, and so $\beta\alpha$ maps k to l, and similarly for all symbols in the cycles of β.

□

Theorem 1. *Permutations α, β S, are conjugate if and only if they have the same cycle structure.*

Proof. Since any element can be expressed as the product of permutations, let f, g be denoted as permutations α and β. For contradiction, define $\gamma \in S_n$ as follows: place the complete factorization of α over that of β so that cycles of the same length correspond, and let γ be the function sending the top to the bottom. For example, if

$$\alpha = (a_1a_2 \ldots a_i)(a_{i+1} \ldots a_j) \ldots (a_{k+1} \ldots a_l)$$

$$\beta = (b_1b_2 \ldots b_i)(b_{i+1} \ldots b_j) \ldots (b_{k+1} \ldots b_l),$$

then $\gamma(a_1) = b_1, \gamma(a_2) = b_2, \ldots, \gamma(a_i) = b_i$, etc. Notice that γ is a permutation, for every element i between 1 and n occurs exactly once in a complete factorization. The lemma above gives $\gamma\alpha\gamma^{-1} = \beta$, and so α and β are conjugate.

□

Now let's get to some group definitions.

Definition 2. *A group G is a set of elements together with an operation that satisfies the four fundamental properties: closure, associativity, identity, and inverses*

In this paper we are going to focus on the symmetric group S_n. The set we are going to define is the permutations π of n elements and the operation we are going to use is $\circ$ (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 $\pi_1(j) = i$.

Definition 3. *Let $G, *$ and $H, \triangle$ be groups.A group homomorphism $f : G \to H$ is a function such that for all $x, y \in G$ we have*

$$f(x * y) = f(x) \triangle f(y).$$

Another way to think about homomorphisms is that it is a structure-preserving map that commutes with multiplication, addition, scaling or whatever operations characterize the algebraic group.

Definition 4. *A group isomorphism is a group homomorphism which is a bijection.*

Definition 5. *An automorphism is simply an isomorphism of a group G to G. The set of all automorphisms of G forms a group, called the automorphism group of G, and denoted Aut(G).*

If G is a group, and S a subset of G, we say that S generates G (and that S is a set of generators for G) if every element of G can be expressed as a product of elements of S and their inverses. So another definition of automorphism can be defined as ϕ that sends generators to generators.

Example 2. *There are two automorphisms of Z: the identity, and the mapping $n \to -n$ Thus, Aut(Z) $\cong C_2$*

Definition 6. *An inner automorphism of a group G is an automorphism of the form $\phi(g) = h^{-1}gh$ where h is a fixed element of G; otherwise it is an outer automorphism*

Example 3. *The automorphism of S_3 is an inner automorphism because it maps the permutation (123) to (132) and it is an inner automorphism since (132) = (12)(123)(12)*

Lemma 2. *An automorphism φ of S_n, preserves transpositions ($\varphi(\tau)$ is a transposition whenever τ is) if and only if φ is inner.*

Proof. It is sufficient to show that for some distinct numbers $a_1, a_2, \ldots, a_n \in 1, 2, \ldots, n$, we have $\varphi((i\ i+1)) = (a_i\ a_{i+1})$ for every index i with $1 \leq i \leq n-1$. Here, by choosing the element $f \in S_n$ satisfying $f(j) = a_j$ for each $j \in \{1, 2, \ldots, n\}$ (or fixes a), we have $\varphi(x) = fx_if^{-1}$ for each adjacent transposition $x_i = (i\ i+1)$. We can use the fact proved in Proposition 1 that every $g \in S_n$ can be written as a product of the elements x_i or in other words adjacent transpositions therefore we have $\varphi(g) = fgf^{-1}$.

From now, we verify the above-mentioned property. We consider the case $n \geq 2$, since the case $n = 1$ is trivial. First, by the assumption of this lemma, $\varphi((12))$ is a transposition, which can be written as $\varphi((12)) = (a_1a_2)$. This proves the claim when $n = 2$; we consider the case $n \geq 3$ from now on. Secondly, by the assumption of this lemma, we have $\varphi((23)) = (b_1b_2)$ for some b_1 and b_2. Then $\varphi((12)(23)) = \varphi((12))\varphi((23)) = (a_1a_2)(b_1b_2)$. Now if two sets $\{a_1, a_2\}$ and $\{b_1, b_2\}$ are disjoint, then we have $((a_1a_2)(b_1b_2))^3 \neq id$ (where id is the identity permutation) since $((a_1a_2)(b_1b_2))^3 = (a_1a_2)^3(b_1b_2)^3 = (a_1a_2)(b_1b_2)$ which is obviously not the id , while $((12)(23))^3 = id$ since its the same as (123); this is a contradiction. Therefore, $\{a_1, a_2\}$ and $\{b_1, b_2\}$ have a common element, say (by symmetry) $a_2 = b_1$. We rewrite b_2 as a_3. This proves the claim when $n = 3$; we consider the case $n \geq 4$ from now on. By the

assumption of this lemma, we have $\varphi((34)) = (c_1c_2)$ for some c_1 and c_2. Now, owing to the fact $((23)(34))^3 = id$, a similar argument implies that $\{a_2, a_3\}$ and $\{c_1, c_2\}$ have a common element, while the fact $((12)(34))^2 = id$ implies that $\{a_1, a_2\}$ and $\{c_1, c_2\}$ should be disjoint. Therefore, we have $a_3 \in \{c_1, c_2\}$, and (c_1c_2) can be written as $(c_1c_2) = (a_3a_4)$ for some a_4. By iterating this argument, we finally have the above-mentioned property. This proves that if an automorphism φ of S_n maps every transposition to a transposition, then φ is an inner automorphism.

Now we prove that φ is an inner automorphism if and only if a transposition in S_n is always mapped by φ to a transposition. If φ is inner, then it preserves the cycle structure of every permutation due to Theorem 1.

□

Couple of more definitions before we start to think about the outer automorphism.

Definition 7. *The center of a group G is the set of elements that commute with every element of G. It is denoted $Z(G)$. In formal terms: $Z(G) = \{z \in G \mid \forall g \in G, zg = gz\}$.*

Example 4. *The quartenion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ has $Z(Q_8) = \{\pm 1\}$ which means that $1x = x1$ and $-1x = x(-1)$*

Definition 8. *A group is said to be centerless if $Z(G)$ is trivial; i.e., consists only of the identity element.*

Definition 9. *A group G is complete if it is centerless and every automorphism of G is inner.*

Theorem 2. *If $n \neq 2$ or $n \neq 6$, then S_n is complete.*

Remark 1. *Permutations with the same cycle structure belong to the same conjugacy class.*

Proof. Let T_k denote the conjugacy class of S_n consisting of the product of k disjoint transpositions. A permutation is an involution iff it lies in T_k. This comes from the fact that a permutation is an involution if and only if it can be written as a finite product of disjoint transpositions. A transposition is an involution if for an automorphism Γ of S_n, the square of the image of any transposition by θ is the identity permutation (since the transposition has the same property). In other words, $\alpha \in S_n$, s.t $\alpha^2 = \text{id}$. It follows that $\theta \in Aut(S_n)$ then $\theta(T_1) = T_k$ for some k. We will show that if $n \neq 6$, then $|T_k| \neq |T_1|$ for $k \neq 1$. If we run into such a situation then $\theta(T_1) = T_1$ and the lemma above proves it.

$|T_1| = \frac{n(n-1)}{2}$ or $\binom{n}{2}$. We can count $|T_k|$ by noting that there are

$$\frac{n(n-1)\cdots(n-2k+1)}{2^k}$$

k-tuples of disjoint transpositions. Disjoint transpositions commute and there are $k!$ orderings that can be obtained from any k-tuple, so

$$|T_k| = \frac{n(n-1)\cdots(n-2k+1)}{2^k \cdot k!}.$$

To prove whether $|T_1| = |T_k|$ it is sufficient to show that there is some $k > 1$ such that

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

Since the right side of (1) is positive, we must have $n \geq 2k$. Therefore, for fixed n,

$$\text{left side} \geq (2k-2)(2k-3)\cdots(2k-2k+1) = (2k-2)!.$$

An easy induction shows that if $k \geq 4$, then $(2k-2)! > k!2^{k-1}$, and so (1) can hold only if $k = 2$ or $k = 3$. When $k = 2$, the right side is 4, and it is easy to see that equality never holds; we may assume, therefore, that $k = 3$. Since $n \geq 2k$, we must have $n \geq 6$. If $n > 6$, then the left side of (1) $\geq 5 \times 4 \times 3 \times 2 = 120$, while the right side is 24. We have shown that if $n \neq 6$, then $|T_1| \neq |T_k|$ for all $k > 1$, as desired.

□

We now show that S_6 is an exception to this. Before we do this, some definitions!

Definition 10. *A subgroup G of S_n is called transitive if for each $i, j \in \{1, 2, ..., n\}$, there is a $\tau \in G$ with $\tau(i) = j$*

Lemma 3. *A subgroup N of a group G is called a normal subgroup if it is invariant under conjugation; that is, for each element $n \in N$ and each $g \in G$, the element gng^{-1} is still in N.*

Example 5. *In an abelian group every subgroup H is normal because for all $h \in H$ and $g \in G$ we have $gh = hg$.*

Definition 11. *If p^k is the highest power of a prime p dividing the order(number of elements) of a finite group G, then a subgroup of G of order p^k is called a sylow p-subgroup of G.*

Lemma 4. *Let $H \leq G$ and let X be the family of all the conjugates of H in G. There is a homomorphism ψ: $G \to S_x$*

Proof. If $a \in G$, define $\psi_a : X \to X$ by $\psi_a(gHg^{-1}) = agHg^{-1}a^{-1}$. If $b \in G$, then $\psi_a\psi_b(gHg^{-1}) = \psi_a(bgHg^{-1}b^{-1}) = abgHg^{-1}b^{-1}a^{-1} = \psi_{ab}(gHg^{-1})$. From this, we can conclude that ψ_a has inverse $\psi_{a^{-1}}$, so that $\psi_a \in S_X$ and $\psi : G \to S_X$ is a homomorphism. □

Lemma 5. *Let $H \leq G$. If both H and G/H are p-groups, then G is a p-group.*

Proof. Let $x \in G$; then $(xH)^{p^a} = H$, for some a, becauseG/H is a p-group. This means that $x^{p^a} \in H$, but then $(x^{p^a})p^b = 1$, for some b, because H is a p-group. □

Lemma 6. *Let P be a Sylow p-subgroup of a finite group G.*
(i) *$|N_G(P)/P|$ is relatively prime to p.*
(ii) *If $a \in G$ has an order that is some power of p and $aPa^{-1} = P$, then $a \in P$.*

Proof.

(i) If p divides $|N_G(P)/P|$, then by Cauchy's theorem, which states that if G is a finite group whose order is divisible by a prime p, then G contains an element of order p, $N_G(P)/P$ contains an element Pa of order p. Thus, $S^* = \langle Pa \rangle$ has order p. According to the Correspondence Theorem, there exists a subgroup $S \leq N_G(P) \leq G$ containing P such that $S/P \cong S^*$. Given that both P and S^* are p-groups, we know that S is also a p-group due to Lemma 5 , which contradicts the maximality of P.

(ii) By replacing a with a suitable power of a if necessary, we can assume that a has order p. Since a normalizes P, we have $a \in N_G(P)$. If $a \notin P$, then the coset $Pa \in N_G(P)/P$ has order p, which contradicts (i).

□

Definition 12. *The normalizer of S in the group G is defined as*
$\mathrm{N}_G(S) = \{g \in G \mid gS = Sg\} = \left\{g \in G \mid gSg^{-1} = S\right\}$,

Theorem 3. *(i) If P is a Sylow p-subgroup of a finite group G, then all Sylow p-subgroups of G are conjugate to P.*
(ii) If there are r Sylow p-subgroups, then r is a divisor of $|G|$ and $r \equiv 1$ mod p.

Proof. Let $X = \{P_1, \ldots, P_r\}$ be the family of all the Sylow p-subgroups of G, where we have denoted P by P_1. We know that G acts on X by conjugation by Lemma 4: there is a homomorphism ψ: G $\to S_x$ sending $a \mapsto \psi(a)$ where $\psi_a(P_i) = aP_ia^{-1}$. Let Q be a Sylow p-subgroup of G. Restricting ψ to Q shows that Q acts on X; every orbit of X under this action has size dividing $|Q|$; that is, every orbit has size some power of p. If the orbit has size 1, there would be an i with $\psi_a(P_i) = P_i$ for all $a \in Q$; that is, $aP_ia^{-1} = P_i$ for all $a \in Q$. By Lemma 5(ii), if $a \in Q$, then $a \in P_i$; that is, $Q \leq P_i$; since Q is a Sylow p-subgroup, $Q = P_i$. If $Q = P = P_1$, we conclude that every P-orbit of X has size an "honest" power of p save $\{P_1\}$ which has size 1. Therefore, $|X| = r \equiv 1 \pmod{p}$.

Suppose there were a Sylow p-subgroup Q that is not a conjugate of P; that is, $Q \notin X$. If $\{P_i\}$ is a Q-orbit of size 1, then we have seen that $Q = P_i$, contradicting $Q \notin X$. Thus, every Q-orbit of X has size an honest power of p, and so p divides $|X|$; that is, $r \equiv 0 \pmod{p}$. The previous congruence is contradicted, and so no such subgroup Q exists. Therefore, every Sylow p-subgroup Q is conjugate to P.

Finally, the number r of conjugates of P is the index of its normalizer, and so it is a divisor of $|G|$.

□

Definition 13. *The kernel of a group homomorphism $f : G \to G'$ is the set of all elements of G which are mapped to the identity element of G'. The kernel is a normal subgroup of G, and always contains the identity element of G. It is reduced to the identity element iff f is injective.*

Definition 14. *Let G be a group and H a subgroup of G. Define a left coset of H with representative $g \in G$ to be the set $gH = \{gh : n \in H\}$. Right cosets can be defined similarly by $Hg = \{hg : h \in H\}$*

Theorem 4. *There exists a transitive subgroup $K \leq S_6$ of order 120 which contains no transpositions.*

Proof. If σ is a 5-cycle, then $P = \langle\sigma\rangle$ is a Sylow 5-subgroup of S_5. The Sylow theorem says that if r is the number of conjugates of P, then $r \equiv 1 \mod 5$ and r is a divisor of 120; it follows easily that $r = 6$. The representation of S_5 on X, the set of all left cosets of $N = N_{S_5}(P)$, is a homomorphism $\rho : S_5 \to S_X \cong S_6$. Now X is a transitive S_5-set and so $|\ker\rho| \leq |S_5|/r = |S_5|/6$. Since the only normal subgroups of S_5 are S_5, A_5, and 1, it follows that $\ker\rho = 1$ and ρ is an injection. Therefore, $\operatorname{im}\rho \cong S_5$ is a transitive subgroup of S_X of order 120.

For notational convenience, let us write $K \leq S_6$ instead of $\operatorname{im}\rho \leq S_X$. Now K contains an element α of order 5 which must be a 5-cycle; say, $\alpha = (1\ 2\ 3\ 4\ 5)$. If K contains a transposition $(i\ j)$, then transitivity of K provides $\beta \in K$ with $\beta(j) = 6$, and so $\beta(i\ j)\beta^{-1} = (\beta i\ \beta j) = (l\ 6)$ for some $l \neq 6$ (of course, $l = \beta i$). Conjugating $(l\ 6) \in K$ by the powers of α shows that K contains (1 6), (2 6), (3 6), (4 6), and (5 6). But these transpositions generate S_6 and this contradicts $K(\cong S_5)$ being a proper subgroup of S_6.

The "obvious" copy of S_5 in S_6 consists of all the permutations fixing 6; plainly, it is not transitive, and it does contain transpositions. □

Theorem 5. *(Hölder, 1895) There exists an outer automorphism of S_6.*

Proof. Let K be a transitive subgroup of S_6 of order 120, and let Y be the family of its left cosets: $Y = \{\alpha_1 K, \ldots, \alpha_6 K\}$. If $\theta : S_6 \to S_Y$ is the representation of S_6 on the left cosets of K, then $\ker\theta \leq K$ is a normal subgroup of S_6. But A_6 is the only proper normal subgroup of S_6, so that $\ker\theta = 1$ and θ is an injection. Since S_6 is finite, θ must be a bijection, and so $\theta \in \operatorname{Aut}(S_6)$, for $S_Y \cong S_6$. Were θ inner, then it would preserve the cycle structure of every permutation in S_6. In particular, $\theta(1\ 2)$, defined by $\theta(1\ 2)\alpha_i K \mapsto (1\ 2)\alpha_i K$ for all i, is a transposition, and hence θ fixes $\alpha_i K$ for four different i. But if $\theta(1\ 2)$ fixes even one left coset, say $\alpha_i K = (1\ 2)\alpha_i K$, then $\alpha_i^{-1}(1\ 2)\alpha_i$ is a transposition in K. This contradiction shows that θ is an outer automorphism. □

These are some calculation results regarding the outer automorphism of $F(x) = y$ to $x \mapsto y$ abbreviated as F in the calculations. Calculations from [Nui15]

(12) ↦ (12)(34)56)
(23) ↦ (16)(24)(35)
(34) ↦ (14) (23) (56)
(45) ↦ (16) (25) (34)
(56) ↦ (13) (24) (56)

First, we calculate the images by F of the other transpositions:

(13) = (12) (23)(12) ↦ (12) (34) (56) · (16) (24) (35) · (12)(34) (56) = (13) (25) (46)
(24) = (23) (34) (23) ↦ (16) (24)(35) · (14) (23)(56) · (16) (24) (35) = (13) (26) (45)
(35) = (34)(45) (34)↦ (14)(23)(56) · (16) (25)(34) ·(14)(23) (56) = (12) (36) (45)
(46) = (45) (56) (45) ↦ (16)(25) (34) · (13) (24)(56) · (16) (25) (34) = (12) (35) (46)
(14) = (12)(24)(12) ↦ (12) (34)(56) · (13)(26) (45) · (12) (34) (56) = (15) (24) (36)

$(25) = (23)\ (35)\ (23) \mapsto (16)\ (24)\ (35) \cdot (12)\ (36)(45) \cdot (16)\ (24)\ (35) = (15)\ (23)\ (46)$
$(36) = (34)(46)\ (34) \mapsto (14)\ (23)\ (56) \cdot (12)\ (35)(46) \cdot (14)(23)\ (56) = (15)\ (26)\ (34)$
$(15) = (12)(25)(12) \mapsto (12)(34)(56) \cdot (15)\ (23)(46) \cdot (12)\ (34)\ (56) = (14)\ (26)\ (35)$
$(26) = (23)\ (36)\ (23) \mapsto (16)\ (24)(35) \cdot (15)\ (26)\ (34) \cdot (16)\ (24)\ (35) = (14)\ (25)\ (36)$
$(16) = (12)\ (26)(12) \mapsto (12)(34)\ (56) \cdot (14)\ (25)\ (36) \cdot (12)\ (34)(56) = (16)\ (23)\ (45)$

Secondly, for each possible cycle type of elements of S_6, we calculate the image by F of an element of S_6 having the cycle type:

$(12)\ (34) = (12) \cdot (34) \mapsto (12)\ (34)\ (56) \cdot (14)\ (23)(56) = (13)\ (24)$
$(12)\ (34)(56) = (12)(34) \cdot (56) \mapsto (13)\ (24) \cdot (13)\ (24)\ (56) = (56)$
$(123) = (12) \cdot (23) \mapsto (12)\ (34)(56) \cdot (16)\ (24)\ (35) = (154)\ (236)$
$(123)(45) = (123) \cdot (45) \mapsto (154)\ (236) \cdot (16)\ (25)(34) = (124653)$
$(123)\ (456) = (123)(45) \cdot (56) \mapsto (124653) \cdot (13)\ (24)(56) = (263)$
$(1234) = (123) \cdot (34) \mapsto (154)\ (236) \cdot (14)\ (23)\ (56) = (2645)$
$(1234)\ (56) = (1234) \cdot (56) \mapsto (2645) \cdot (13)(24)(56) = (13)\ (2546)$
$(12345) = (1234) \cdot (45) \mapsto (2645) \cdot (16)\ (25)(34) = (14356)$
$(123456) = (12345) \cdot (56) \mapsto (14356) \cdot (13)\ (24)(56) = (15)\ (234)$

From these calculations and the fact that for an automorphism F of S_n and any possible cycle type of elements of S_n, the cycle type of F(f) for any element $f \in S_n$ of the fixed cycle type is uniquely determined, regardless of the choice of such an element f since if $g \in S_n$ is any element with the same cycle type as f then by Theorem 1, f and g are conjugate, namely $g = hfh^{-1}$ for some $h \in S_n$. So $F(g) = F(hfh^{-1}) = F(h)F(f)F(h)^{-1}$ therefore $F(f)$ and $F(g)$ are conjugate to each other as well and by Theorem 1, this implies that $F(f)$ and $F(g)$ have the same cycle type, the cycle types of elements of S_6 are changed by applying the map F as follows: Types $(1^4 2^1)$ and (2^3) are exchanged; types $(1^3 3^1)$ and (3^3) are exchanged; types $(1^1 2^1 3^1)$ and (6) are exchanged; and any other type is not changed.

This only proves that there is an outer automorphism. However, we can make the sentence stricter by proving that there exists a unique outer automorphism or in other words only one outer automorphism of S_6.

Definition 15. *Syntheme is a product of three disjoint transpositions and a pentad is a family of 5 synthemes with pairwise distinct transpositions (no two transpositions are common)*

S_6 contains 6 pentads as there are 15 synthemes and each lie in at most 2 pentads. Then we must have 6 pentads as there are $2{\cdot}15 = 30 = 6{\cdot}5$

Theorem 6. *$Aut(S_6)/Inn(S_6) \equiv \mathbb{Z}_2$. and so $|Aut(S_6)| = 1440$.*

Proof. Let T_1 be the class of all transpositions in S_6, and let T_3 be the class of all products of 3 disjoint transpositions. If θ and ψ are outer automorphisms of S_6, then both interchange T_1 and T_3 since if n = 6, then in the proof of the theorem, (1) does not hold if $k \neq 3$; when k= 3, both sides of (1) equal 24, and so $\theta^{-1}\psi(T_1) = T_1$. Therefore,$\theta^{-1}\psi(T_1) \in Inn(S6)$, by Lemma 2, and Aut(S)/Inn(S6) has order 2. □

	cycle structure	order	parity	number of such
C_1	(1)	1	even	1
C_2	(12)	2	odd	15
C_3	(123)	3	even	40
C_4	(1234)	4	odd	90
C_5	(12345)	5	even	144
C_6	(123456)	6	odd	120
C_7	(13)(34)	2	even	45
C_8	(12)(345)	6	odd	120
C_9	(12)(3456)	4	even	90
C_{10}	(12)(34)(56)	2	odd	15
C_{11}	(123)(456)	3	even	40
				$720 = 6!$

Figure 2. Janusz 1982
[JR82]

The proof of the essential uniqueness of the outer automorphism can be seen in this table. Recall that two permutations lie in the same conjugacy class if and only if they have the same cycle structure

Theorem 7. *If $\{\sigma_1, ., \sigma_6\}$ is a pentad in some ordering, then there is a unique outer automorphism θ of S_6 with θ: $\rightarrow \sigma_i$ for i = 2,3,4,5,6. Every outer automorphism of S_6 has this form.*

Denote X = $\{(12), (13), (14), (15), (16)\}$. If θ is the outer automorphism of S_6 then by theorem 1.2, we know that if $n \neq 6$ then the theorem does not hold if $k \neq 3$. This shows that each $\theta((1i))$ is a syntheme. We also know that for $i \neq j$, (1 i) and (1 j) do not commute, it follows that $\theta((1i))$ and $\theta((1j))$ do not commute and hence $\theta(X)$ is a pentad. For an outer automorphism X, there are 6 choices of pentads and given a pentad P, there are 120 (5!) bijections that are possible from $X \rightarrow P$. Hence there are at most 720 bijections from $X \rightarrow P$ which could restrict the outer automorphisms. However, we know for sure that there are 720 outer automorphisms since if T_1 is the class of all transpositions in S_6, and T_3 be the class of all products of 3 disjoint transpositions. If θ and ψ are outer automorphisms of S_6, then both interchange T_1 and T_3 since Equation 1 does not hold if $k \neq 3$ and so $\theta^{-1}\psi(T_1) = T_1$. Therefore, $\theta^{-1}\psi \in Inn(S_6)$, by Lemma 2, and Aut($S_6$)/Inn($S_6$) has order 2. $|Aut(S_6)| = 1440$ so Inn(S_6) = 720 and no two of them can restrict to the same bijection because X generates S_6

The above construction of the outer automorphism of S_6 using the Sylow groups is most common. The next few pages will describe the outer automorphism in several other ways like mystic pentagons, labeled triangles and labeled icosahedron. [BHV08]

4.0.1. ***Mystic Pentagons***. There are 12 ways to two-color the edges of a complete graph on 5 vertices, such that the edges of each color form a 5-cycle: the six from $\{a, \ldots, f\}$ and the other six by interchanging the colors. Each element of S_5 induces a permutation of the six mystic pentagon pairs via its action on the vertices giving a map $i : S_5 = S_{1,\ldots,5} \to S_{a,\ldots,f} = S_6$. This is an inclusion, in other words, a fancy way to say that every element in $S_{1,\ldots,5}$ is also an element in $S_{a,\ldots,f}$. Hence there is a homomorphism between $S_{1,\ldots,5}$ and $S_{a,\ldots,f}$ and the kernel is a normal subgroup under a homomorphism (let h ∈ H by applying f to it you get $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = e$) and the normal subgroups of S_5 are $e, A_5, or S_5$ but we visually verify that (123) acts nontrivially. Moreover, it is not a usual inclusion as (12) induces permutation $(ad)(bc)(ef)$ — not a transposition. Hence $S_6 = S_{\{a,\ldots,f\}}$ acts on the six cosets of $i(S_5)$, inducing a map $f : S_{\{a,\ldots,f\}} \to S_{\{1,\ldots,6\}}$. This is the outer automorphism. This can be verified in several ways (e.g., $(ad)(bc)(ef)$ induces the nontrivial permutation $(12) \in S_{\{1,\ldots,6\}}$, so f is injective and hence an isomorphism; and i is not a usual inclusion, so f is not inner). We can also get pentads from these mystic pentagons. Each mystic pentagon determines a bijection between the dashed edges and the dotted edges, where edge AB corresponds with edge CD if AB and CD don't share a vertex. If $E = \{1, \ldots, 5\} - \{A, B, C, D\}$, then to each such pair we obtain the syntheme $AB/CD/E6$, and there are clearly five such synthemes, no two of which share an edge, which hence form a pentad. For example, mystic pentagon a yields the pentad.

$$\{12/35/56, 23/14/56, 34/25/16, 45/13/26, 15/24/36\}.$$

Another common description of the outer automorphism is to find a subgroup $G < S_5$ of size 20; we take the subgroup preserving figure **a** of Figure 1. Then S_5 acts transitively on the six cosets of G, giving a map $i : S_5 \to S_6$. This map is an inclusion as (123) is not in its kernel. Then S_6 acts transitively on the six cosets of $i(S_5)$, yielding a map $\sigma : S_6 \to S_6$. The image (as it is transitive) has size > 2, hence (as S_6 has only 3 normal subgroups) the kernel is e, hence σ is an automorphism. Then it is not inner, as $i(S_5))$ is not one of the six "obvious" S5's in S6.

4.0.2. ***Labeled Triangles***. Consider the set of $\binom{6}{3}$ or 20 triangles formed from six vertices labeled $\{1, 2, 3, 4, 5, 6\}$. We can divide these 20 triangles into two sets of 10 in six different ways, with the following conditions: (i) any two disjoint triangles must have opposite colors, and (ii) every tetrahedron must have two triangles of each color. The bijection between these divisions and the mystic pentagons (labeled a through f) is as follows: The triangle $6AB$ is colored the same as the edge AB, and the triangle CDE (where $6 \neq C, D, E$) is colored opposite to the "complementary" edge AB (where $\{A, B\} = \{1, 2, 3, 4, 5\} - \{C, D, E\}$). The action of S_6 on this set represents the outer automorphism of S_6. The permutation (12) induces a nontrivial permutation $(ad)(bc)(ef)$ of the mystic pentagons, making the induced map $S_6 \to S_{\{a,\ldots,f\}} \cong S_6$ injective and thus an isomorphism. However, since (12) does not induce a transposition on $\{a, \ldots, f\}$, the automorphism is not inner. This isomorphism $S_{\{1,\ldots,6\}} \to S_{\{a,\ldots,f\}}$ is the inverse of the isomorphism shown in 4.0.1.

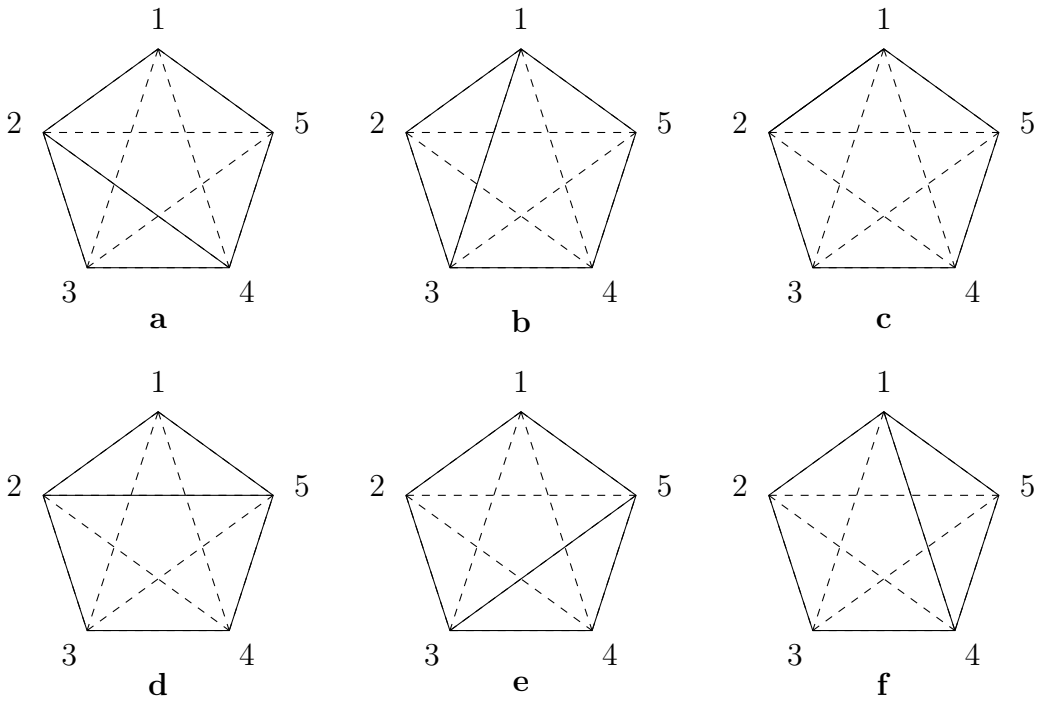

Figure 3. Pentagons with various edges and diagonals

4.0.3. ***Labeled Icosahedron***. There are twelve ways to number the vertices of an icosahedron from 1 through 6, considering rotations and reflections, such that antipodal vertices have the same label. Each icosahedron results in ten triples in $\{1, \ldots, 6\}$, corresponding to the vertices around its faces. These twelve icosahedra form six pairs, where two icosahedra are "opposite" if they have no triples in common. The group S_6 acts on these six pairs, representing the outer automorphism. This can be shown through bijections to the descriptions in 4.0.1 and 4.0.2. Each pair of mystic icosahedra corresponds to the two-coloring of the triangles in $\{1, \ldots, 6\}$ as described in 4.0.2. For the bijection to 4.0.1, the cyclic order of the vertices around vertex 6 forms a mystic pentagon.

Another construction of the outer automorphism of S_6 can be found in the subgroups of Mathieu groups, in particular, M_{12}. The five Mathieu groups M_{11}, M_{12},M_{22}, M_{23}, and M_{24} were the first sporadic groups discovered by Mathieu.

Definition 16. *If X is a set and G is a group, then X is a G-set if there is a function α:$G \times X \to X$ (called an action), denoted by $\alpha : (g, x) \mapsto gx$, such that: (i) $1x = x$ for all $x \in X$; and (ii) $g(hx) = (gh)x$ for all g, $h \in G$ and $x \in X$.*

Definition 17. *A G-set X with action α is faithful if α: $G \to S_x$ injective.*

Definition 18. *Let X be a G-set of degree n and let $k \leq n$ be a positive integer. Then X is k-transitive if, for every pair of k-tuples having distinct entries in X, say, $(x_1 \ldots, x_k)$ and $(y_1, \ldots, y_k,)$ there is $g \in G$ with $gx_i = y_i$ for $i = 1, \ldots, k$.*

Definition 19. *A k-transitive G-set X is sharply k-transitive if only the identity fixes k distinct elements of X.*

Definition 20. *The orbit of an element $x \in X$ is defined as* $Orb(x) := \{y \in X : \exists\ g \in G : y = g * x\}$

Definition 21. *The centralizer of a subset S of group G is defined as* $\mathrm{C}_G(S) = \{g \in G \mid gs = sg \text{ for all } s \in S\} = \left\{g \in G \mid gsg^{-1} = s \text{ for all } s \in S\right\},$

Definition 22. *For each $x \in X$, the stabilizer of x by G is defined as* $Stab(x) = \{g \in G : g * x = x\}$

Theorem 8. *Regard $X = GF(9) \cup \{\infty, \omega, \Omega\}$ as an M_{12}-set. There is a subgroup $\Sigma \leq M_{12}$, isomorphic to S_6, having two orbits of size 6, say, Z and Z', and which acts sharply 6-transitively on Z. Moreover,*

$$\Sigma = \{\mu \in M_{12} : \mu(Z) = Z\}.$$

Proof. Denote the 5-set $\{\infty, \omega, \Omega, 1, -1\}$ by Y. For each permutation τ of Y, sharp 5-transitivity of M_{12} provides a unique $\tau^* \in M_{12}$ with $\tau^*|_Y = \tau$. It is easy to see that the function $S_Y \to M_{12}$, given by $\tau \mapsto \tau^*$, is an injective homomorphism; we denote its image (isomorphic to S_5) by Q.

Let us now compute the Q-orbits of X. One of them, of course, is Y. If τ is the 3-cycle $(\infty\ \omega\ \Omega)$, then $\tau^* \in Q$ has order 3 and fixes 1 and -1. Now τ^* is a product of three disjoint 3-cycles (fewer than three would fix too many points of X), so that the $\langle\tau^*\rangle$-orbits of the 7-set $X - Y$ have sizes (3, 3, 1). Since the Q-orbits of X (and of $X - Y$) are disjoint unions of $\langle\tau^*\rangle$-orbits, the Q-orbits of $X - Y$ have possible sizes (3, 3, 1), (6, 1), (3, 4), or 7. If Q has one orbit of size 7, then Q acts transitively on $X - Y$; this is impossible, for 7 does not divide $|Q| = 120$. Furthermore, Q has no orbits of size t, where $2 < t < 5$. We conclude that $X - Y$ has two Q-orbits of sizes 6 and 1, respectively. There is thus a unique point in $X - Y$, namely, the orbit of size 1, that is fixed by every element of Q. If $\sigma \in S_Y$ is the transposition $(1\ \ -1)$, then its correspondent $\sigma^* \in Q$ fixes ∞, ω, Ω and interchanges 1 and -1. But $\zeta : \mathrm{GF}(9) \to \mathrm{GF}(9)$, defined by $\zeta : \lambda \mapsto -\lambda$, lies in M_{10} (for -1 is a square in GF(9)) and $\zeta|_Y = \sigma$, so that $\zeta = \sigma^*$. Since the only other point fixed by ζ is 0, the one-point Q-orbit of $X - Y$ must be $\{0\}$.

Define $Z = Y \cup \{0\} = \{\infty, \omega, \Omega, 1, -1, 0\}$. $M_{10} \leq M_{12}$ contains $\sigma_1 : \mathbb{P}^1(9) \to \mathbb{P}^1(9)$, where $\sigma_1 : \lambda \mapsto -1/\lambda$ $(0\ \infty)\ (1\ \text{-}1)\ (\pi^3\pi)(\pi^5\pi^7))$. Let us see that the subgroup $\Sigma = \langle Q, \sigma_1\rangle \cong S_6$. The set Z is both a Q-set and a $\langle\sigma_1\rangle$-set, hence it is also a Σ-set. As Σ acts transitively on Z and the stabilizer of 0 is Q (which acts sharply 5-transitively on $Z - \{0\} = Y$), we have Σ acting sharply 6-transitively on the 6-point set Z, and so $\Sigma \cong S_6$. Finally, the 6 points $X - Z$ comprise the other Σ-orbit of X (for we have already seen that $X - Z$ is a Q-orbit). □

Theorem 9. *Let X be a faithful t-transitive G-set, where $t \geq 2$, let H be the stabilizer of t points $x_1, \ldots, x_t$ in X, and let U be a Sylow p-subgroup of H for some prime p.*

(i) *$N_G(U)$ acts t-transitively on $\mathcal{F}(U)$.*

(ii) *If $k = |\mathcal{F}(U)| > t$ and U is a nontrivial normal subgroup of H, then $(X, \mathcal{B})$ is a Steiner system of type $S(t, k, v)$, where $|X| = v$ and*

$$\mathcal{B} = \{g\mathcal{F}(U) : g \in G\} = \{\mathcal{F}(U^g) : g \in G\}.$$

Proof. (i) Note that $\mathcal{F}(U)$ is a $N_G(U)$-set: if $g \in N_G(U)$, then $U = U^g$ and $\mathcal{F}(U) = \mathcal{F}(U^g) = g\mathcal{F}(U)$. Now $\{x_1, \ldots, x_t\} \subset \mathcal{F}(U)$ because $U \leq H$, the stabilizer of $x_1, \ldots, x_t$; hence $k = |\mathcal{F}(U)| \geq t$. If $y_1, \ldots, y_t$ are distinct elements of $\mathcal{F}(U)$, then t-transitivity of G gives $g \in G$ with $gy_i = x_i$ for all i. If $u \in U$, then $gug^{-1}x_i = guy_i = gy_i = x_i$ (because $y_i \in \mathcal{F}(U)$); that is, $U \leq H$. By the Sylow theorem, there exists $h \in H$ with $U^g = U^h$. Therefore $h^{-1}g \in N_G(U)$ and $(h^{-1}g)y_i = h^{-1}x_i = x_i$ for all i.

(ii) The hypothesis gives $1 < t < k \leq v$. If $k = v$, then $\mathcal{F}(U) = X$; but $U \neq 1$, contradicting G acting faithfully on X. It is also clear that $k = |\mathcal{F}(U)| = |g\mathcal{F}(U)|$ for all $g \in G$.

If $y_1, \ldots, y_t$ are distinct elements of X, then there is $g \in G$ with $gx_i = y_i$ for all i, and so $\{y_1, \ldots, y_t\} \subset \mathcal{F}(U)$. It remains to show that $g\mathcal{F}(U)$ is the unique block containing the y_i. If $\{y_1, \ldots, y_t\} \subset h\mathcal{F}(U)$, then there are $z_1, \ldots, z_t \in \mathcal{F}(U)$ with $y_i = hz_i$ for all i. By (i), there is $\sigma \in N_G(U)$ with $z_i = \sigma x_i$ for all i, and so $gx_i = y_i = h\sigma x_i$ for all i. Hence $g^{-1}h\sigma$ fixes all x_i and $g^{-1}h\sigma \in H$. Now $H \leq N_G(U)$, because $U \leq H$, so that $g^{-1}h\sigma \in N_G(U)$ and $g^{-1}h \in N_G(U)$. Therefore, $U^g = U^h$ and $g\mathcal{F}(U) = \mathcal{F}(U^g) = \mathcal{F}(U^h) = h\mathcal{F}(U)$. Thus $g\mathcal{F}(U)$ is the unique block containing the y_i.

□

Theorem 10. *S_6 has an outer automorphism of order 2.*

Proof. Recall from Theorem 8 that if $X = \{\infty, \omega, \Omega\} \cup \mathrm{GF}(9)$ and $\Sigma(\cong S_6)$ is the subgroup of M_{12} in Theorem 8, then X has two Σ-orbits, say, $Z = Y \cup \{0\}$ and $Z' = Y' \cup \{0'\}$, each of which has 6 points. If $\sigma \in \Sigma$ has order 5, then σ is a product of two disjoint 5-cycles (only one 5-cycle fixes too many points), hence it fixes, say, 0 and 0'. It follows that if $U = \langle\sigma\rangle$, then each of Z and Z' consists of two U-orbits, one of size 5 and one of size 1. Now $H = (M_{12})_0 \cong M_{10}$, and U is a Sylow 5-subgroup of H. By Theorem 8, $N = N_{M_{12}}(U)$ acts 2-transitively on $\mathcal{F}(U) = \{0, 0'\}$, so there is $\alpha \in N$ of order 2 which interchanges 0 and 0'.

Since α has order 2, $\alpha = \tau_1 \cdots \tau_m$, where the τ_i are disjoint transpositions and $m \leq 6$. But M_{12} is sharply 5-transitive, so that $4 \leq m$; also, $M_{12} \leq A_{12}$, and $m \leq 6$. But M_{12} is sharply 5-transitive, so that $4 \leq m$; also, $M_{12} \leq A_{12}$, so that $m = 4$ or $m = 6$.

We claim that α interchanges the sets $Z = Y \cup \{0\}$ and $Z' = Y' \cup \{0'\}$. Otherwise, there is $y \in Y$ with $\alpha(y) = z \in Y$. Now $\sigma\alpha = \alpha\sigma$ for some σ because α normalizes $\langle\sigma\rangle$. If $\alpha(y) = u$ and $\alpha(z) = v$, then $u, v \in Y$ because $Y \cup \{0\}$ is a Σ-orbit. But $\alpha = \sigma\alpha(y) = \sigma\alpha(z) = \alpha(v)$, and it is easy to see that y, z, u, v are all distinct. Therefore, the cycle decomposition of α involves $(0\ 0'), (y\ z), (u\ v)$. There is only one point remaining in Y, say a, and there are two cases: either $\alpha(a) = a$ or $\alpha(a) \in Y'$. If α fixes a, then there is $y' \in Y'$ moved by α, say, $\alpha(y') = z' \in Y'$. Repeat the argument above: the cycle decomposition of α involves $(y'\ z')$ and $(v'\ u')$ in Y', with transpositions $(y'\ z')$ and $(v'\ u')$ involved in the cycle decomposition of α. If a' is the remaining point in Y', then the transposition $(a\ a')$ must also occur in the factorization of α because α is not a product of 5 disjoint transpositions. In either case, we have $\alpha \in Y$ and $a' \in Y'$ with $\alpha = (0\ 0')(y\ z)(u\ v)(a\ a')\beta$, where β permutes $Y' - \{a'\}$. But $\alpha\alpha(a) = \sigma(a) = \alpha(a) = \alpha(a)$. On the other hand, if $\alpha(a') = b'$ for all $a' \in Y'$, say,

then $\alpha\alpha(a) = \alpha\alpha(b') = b' = \alpha'\alpha'$, so that $\alpha(b') = b' = a'$, that is, α fixes a'. This is a contradiction, for α fixes only 0 and 0'.

It is easy to see that α normalizes Σ. Recall that $\alpha \in \Sigma$ if and only if $\alpha(Z) = Z$ (and hence $\alpha(Z') = Z'$). Now $\sigma\alpha(Z) = \sigma\alpha(Z') = Z, sothat\alpha \in \Sigma$. Therefore, $\gamma = \gamma_\alpha$ (conjugation by α) is an automorphism of Σ.

Suppose there is $\beta \in \Sigma$ with $\sigma^*\alpha = \beta\sigma^*\beta^{-1}$ for all $\sigma^* \in \Sigma$; that is, $\beta^{-1}\alpha = C = C_{M_{12}}(\Sigma)$. If $C = 1$, then $\alpha = \beta \in \Sigma$, and this contradiction would show that γ is an outer automorphism. If $\sigma^* \in \Sigma$, then $\sigma^* = \sigma'$, where σ permutes Z and fixes Z' and σ' permutes Z' and fixes Z.

$$\sigma^* = (z\ \cdots)(z'\ x'\ \cdots);$$

if $\mu \in M_{12}$, then (as any element of S_{12}),

$$\mu\sigma^*\mu^{-1} = (\mu z\ \mu x'\ \cdots).$$

In particular, if $\mu \in C$ (so that $\mu\sigma^*\mu^{-1} = \sigma^*$), then either $\mu(Z) = Z$ and $\mu(Z') = Z'$ or μ switches Z and Z'. In the first case, $\mu \in \Sigma$, by Lemma 5, and $\mu \in C \cap \Sigma = Z(\Sigma) = 1$. In the second case, $\mu\sigma'\mu^{-1} = \sigma'$ (and $\mu\sigma'\mu^{-1} = \sigma$), so that σ and σ' have the same cycle structure for all $\sigma^* = \sigma' \in \Sigma$; but there is $\sigma^* \in \Sigma$ with σ a transposition. If such μ exists, then σ' would be a product of two disjoint transpositions and hence would fix 8 points, contradicting M_{12} being sharply 5-transitive. □

The last way we are going to see the construction of the outer automorphism of S_6 is through the complex Hadamard matrices. This paper will only give a brief overview; if you want to learn more, check out [Hal62]

Let G be a finite group and $\rho : G \to \mathrm{Aut}(V)$ a representation. Let $\sigma \in \mathrm{Aut}(G)$. We aim to determine when σ can be realized as an element of $\mathrm{Aut}(V)$. Specifically, we seek $S \in \mathrm{Aut}(V)$ such that, for all $g \in G$,

$$\rho(g^\sigma) = S^{-1}\rho(g)S.$$

The Mathieu group M_{12} has two conjugacy classes of subgroups M_{11}. The coset action on either class is 5-transitive on 12 points. The outer automorphism of M_{12} swaps the classes of M_{11}s, and hence the two actions. These actions cannot be linearly equivalent, as the traces are different, e.g.,

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 2 & 3 & 1 & 9 & 10 & 6 & 7 & 4 & 8 & 11 & 12 \end{pmatrix}$$

$$P^\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 1 & 6 & 2 & 7 & 5 & 3 & 9 & 8 & 4 & 12 & 11 \end{pmatrix}$$

Theorem 11. *(M. Hall, 1962) Let H be a Hadamard matrix of order 12. Modulo the centre of $Aut(H)$, the automorphisms of H are the Mathieu group M_{12} of order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040$. Here M_{12} is represented as a quintuply transitive group of monomial permutations on the columns or rows of H. The row and column representations of H are isomorphic, but the correspondence given by $P = HQH^{-1}$ determines an outer automorphism of M_{12} of order 2.*

Let H be a Hadamard matrix of order 12. The automorphism group of H is given by

$$\mathrm{Aut}(H) = \{(P, Q) \mid PHQ^\top = H, \text{ where } P, Q \text{ are } \pm 1\text{-monomial}\}.$$

Consider the representations $\alpha : 2.M_{12} \to P$ and $\beta : 2.M_{12} \to Q$:

$$\alpha(x) = H\beta(x)H^{-1}.$$

By Hall's theorem, $\beta(x) = \alpha(x^\sigma)$ for some outer automorphism σ of M_{12}. So for every $x \in 2.M_{12}$, we have

$$\alpha(x^\sigma) = H^{-1}\alpha(x)H,$$

which gives a linear representation of the outer automorphism of $2.M_{12}$.

While the outer automorphism of M_{12} (acting on 12 points) cannot be realised linearly, it *almost can*. Given an element of M_{12}, we can lift to $2.M_{12}$, conjugate by H and project back onto M_{12}. For example:

$$\pi^{-1}(P) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ -5 & 2 & -3 & -1 & -9 & 10 & 6 & 7 & -4 & 8 & 11 & -12 \end{pmatrix}$$

$$\pi^{-1}(P^\sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 1 & 6 & 2 & 7 & 5 & 3 & 9 & 8 & 4 & 12 & 11 \end{pmatrix} = \pi^{-1}(P)H$$

The outer automorphism of S_6 can be described by:

$$(1,2) \to (1,2)(3,6)(4,5)$$
$$(1,2,3) \to (1,5,6)(2,3,4)$$
$$(1,2,3,4,5,6) \to (1,5)(2,3,6) \text{ etc.}$$

Our goal is to find a matrix H which intertwines or lifts off these representations of S_6. A sporadic example of the complex Hadamard matrices with doubly transitive automorphism groups is:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega & \omega \\ 1 & \omega & 1 & \omega & \omega & \omega \\ 1 & \omega & \omega & 1 & \omega & \omega \\ 1 & \omega & \omega & \omega & 1 & \omega \\ 1 & \omega & \omega & \omega & \omega & 1 \end{pmatrix}$$

which has an automorphism group $3.A_6$. Note that $HH^\dagger = 6I_6$. H intertwines two representations of 3.A6. By restricting to A_6 we get inequivalent representations ofA_6. Hence, every automorphism of H is of the form $\rho(x)H_\rho(x^\sigma)$. Now, rho extends to a representation of $3.S_6$. If we take y to be an odd permutation, then $\rho(y)H_\rho(y^\sigma) = H^\dagger$. But H is not Hermitian(a square matrix that is equal to the transpose of its conjugate matrix). In any case, H could never intertwine representations of $3.S_6$: involutions of shape 1^42 have non-zero trace over $\mathbb{C}$, but are mapped to elements of shape 2^3 (Cf. elements of order 3.)
The split-quaternions, denoted Ξ are a 4-dimensional algebra over $\mathbb{R}$ generated by $\{1, i, \tau, i\tau\}$ where:

$$i^2 = -1, \quad \tau^2 = 1, \quad \tau i \tau = -i$$

They are isomorphic to $M_2(\mathbb{R})$:

$$i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

They are not a division algebra as $(i + \tau i)^2 = 0$. They contain $\mathbb{C} \cong \langle 1, i \rangle$ as a subalgebra. S_6 Take $S = \tau I_6$. Then, for any odd permutation $y \in S_6$, we have:

$$S\rho(y)H\rho(y^\sigma)S = SH^\dagger S = H$$

So odd permutations can be made into Ξ-linear automorphisms of H. Note that τ and τi have trace 0, so all odd permutations lift to elements of equal trace. Even permutations are defined over $\mathbb{C}$, and odd permutations involve τ. We have $3.S_6$ acting on H with the row and column actions differing by an outer automorphism of S_6. To compute the image of $\sigma \in S_6$ under an outer automorphism we can lift σ to $3.S_6$, if odd, we multiply by S, conjugate by H, and restrict to S_6. Hence, we now have a construction of the outer automorphism for S_6.

5. Conclusion

In this paper, we explored the outer automorphism of S_6 and saw various descriptions of it.

References

[BHV08] A. Snowden B. Howard, J. Millson and R. Vakil. . a description of the outer automorphism of s6, and the invariants of six points in projective space. *J. Combin. Theory Ser. A,*, (10):1296—-1303, 2008.

[Hal62] M. Hall. *Note on the Mathieu group* $M_{12}.Springer - Verlag, New York - Heidelberg, 1962.Arch.Math.(Basel),$.

[JR82] Gerald Janusz and Joseph Rotman. Outer automorphisms of s6. *The American Mathematical Monthly*, (10):407–410, 1982.

[Kar11] M. I. Kargapolov. *Fundamentals of the theory of groups*. Springer New York, illustrated edition, 2011.

[Nui15] Koji Nuida. Note: The outer automorphism of s6. *Biglobe*, 2015.