Exceptional Automorphism of S_6

John Doe
Unknown Department, Unknown University

November 21, 2016

Theorem 1. *S_n can be generated by* $(1\ 2)$, $(1\ 3)$, $\dots$, $(1\ n)$.

Theorem 2. *Every permutation $\sigma \in S_n$ is either a cycle or a product of disjoint cycles.*

Definition 1. A complete factorization of a permutation σ is a factorization of σ as a product of disjoint cycles which contains one 1-cycle (i) for every i fixed by σ.

Theorem 3. *Let $\sigma \in S_n$ and let $\sigma = \sigma_1 \dots \sigma_t$ be a complete factorization into disjoint cycles. This factorization is unique except for the order in which the factors occur.*

Lemma 1. *Let $\sigma \in S_n$. If $\sigma^2 = e$, then either $\sigma = e$, σ is a transposition, or σ is a product of disjoint transpositions.*

Proof. Let $\sigma = \sigma_1 \dots \sigma_t$ be a complete factorization into disjoint cycles. Then $e = \sigma^2 = \sigma_1^2 \dots \sigma_t^2$, and $|\sigma_i| = 1$ or $|\sigma_i| = 2$ for all i, $1 \leq i \leq t$, by Theorem 3. Hence either $\sigma = e$, σ is a transposition, or σ is a product of disjoint transpositions. □

Definition 2. An automorphism of a group G is an isomorphism with itself.

We will denote the set of all automorphisms of G by $\mathrm{Aut}(G)$.

Theorem 4. $\mathrm{Aut}(G)$ *is a subgroup of S_G, the group of permutations of G.*

Definition 3. Let G be a group and $g \in G$. Conjugation by g is a map $i_g : G \to G$ by $i_g(x) = gxg^{-1}$ (or $i_g(x) = g^{-1}xg$; usage varies).

Theorem 5. *i_g defines an automorphism of G.*

Definition 4. Such an automorphism is called an inner automorphism. The set of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

Theorem 6. *Let G be a group. Define a map $\varphi : G \to \mathrm{Aut}(G)$ by $\varphi(g) = i_g$ for any $g \in G$. Then φ is a homomorphism $G \to \mathrm{Aut}(G)$. Then image of φ is the group $\mathrm{im}(\varphi) = \mathrm{Inn}(G)$ of inner automorphisms and whose kernel is the center of G: $\ker(\varphi) = Z(G)$.*

Corollary 1. $G/Z(G) \cong \mathrm{Inn}(G)$.

Corollary 2. *Thus, if G has trivial center it can be embedded into its own automorphism group $\mathrm{Aut}(G)$.*

Theorem 7. $\mathrm{Inn}(G)$ *is a normal subgroup of* $\mathrm{Aut}(G)$.

Definition 5. A group G is complete if the map $g \mapsto i_g : G \to \mathrm{Aut}(G)$ is an isomorphism.

Theorem 8. *A group G is complete if and only if (a) G is centerless, i.e., the centre $Z(G)$ of G is trivial, and (b) every automorphism of G is inner.*

Definition 6. Two permutations $\sigma, \tau \in S_n$ have the same cycle structure if their complete factorizations into disjoint cycles have the same number of r-cycles for each r.

Lemma 2. *If $\sigma, \tau \in S_n$, then $\sigma\tau\sigma^{-1}$ is the permutation with the same cycle structure as τ which is obtained by applying σ to the symbols in τ.*

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

$$\tau = \tau_1\tau_2 \dots (\dots i\ j \dots) \dots \tau_t.$$

If $\sigma(i) = k$ and $\sigma(j) = l$, then $\pi : k \mapsto l$. But $\sigma\tau\sigma^{-1} : k \mapsto i \mapsto j \mapsto l$, and so $\sigma\tau\sigma^{-1}(k) = \pi(k)$. Therefore, π and $\sigma\tau\sigma^{-1}$ agree on all symbols of the form $k = \sigma(i)$; since σ is a surjection, it follows that $\pi = \sigma\tau\sigma^{-1}$. $\square$

Theorem 9. *Permutations $\sigma, \tau \in S_n$ are conjugate if and only if they have the same cycle structure.*

Proof. $\Rightarrow$: Lemma 2.
$\Leftarrow$: Define $\pi \in S_n$ as follows: place the complete factorization of σ over that of τ so that cycles of the same length correspond, and let π be the function sending the top to the bottom: if

$$\sigma = \sigma_1\sigma_2 \dots (\dots i\ j \dots) \dots \sigma_t$$
$$\tau = \tau_1\tau_2 \dots (\dots k\ l \dots) \dots \tau_t$$

then $\pi(i) = k$, $\pi(j) = l$, etc. Notice that π is a permutation, for every i between 1 and n occurs exactly once in a complete factorization. The lemma 2 gives $\pi\sigma\pi^{-1} = \tau$, and so σ and τ are conjugate. $\square$

Corollary 3. *A subgroup H of S_n is a normal subgroup if and only if, whenever $\sigma \in H$, then every τ having the same cycle structure as σ also lies in H.*

Proof. $H \trianglelefteq S_n$ if and only if H contains every conjugate of its elements. $\square$

Theorem 10. *If $H \leq G$ and $[G : H] = n$, then there is a homomorphism $\varphi : G \to S_n$ with $\ker(\varphi) \leq H$.*

Proof. If $a \in G$ and X is the family of all the left cosets of H in G, define a function $\varphi_a : X \to X$ by $gH \mapsto agH$ for all $g \in G$. It is easy to check that each φ_a is a permutation of X (its inverse is $\varphi_{a^{-1}}$) and that $a \mapsto \varphi_a$ is a homomorphism $\varphi : G \to S_X \cong S_n$. If $a \in \ker\varphi$, then $agH = gH$ for all $g \in G$; in particular, $aH = H$, and so $a \in H$; therefore, $\ker(\varphi) \leq H$. $\square$

Corollary 4. *A simple group G which contains a subgroup H of index n can be embedded in S_n.*

Proof. There is a homomorphism $\varphi : G \to S_n$ with $\ker\varphi \leq H < G$. Since G is simple, $\ker\varphi = \{1\}$, and so φ is an injection. $\square$

Lemma 3. *An automorphism φ of S_n preserves transpositions ($\varphi(\tau)$ is a transposition whenever τ is) if and only if φ is inner.*

Proof. If φ is inner, then it preserves the cycle structure of every permutation, by Theorem 9.

We prove, by induction on $t \geq 2$, that there exist conjugations $i_2, \dots, i_t$ such that $i_t^{-1} \dots i_2^{-1}\varphi$ fixes $(1\ 2), \dots, (1\ t)$. If $\pi \in S_n$, we will denote $\varphi(\pi)$ by π^φ. By hypothesis, $(1\ 2)^\varphi = (i\ j)$ for some i, j; define i_2 to be conjugation by $(1\ i)(2\ j)$ (if $i = 1$ or $j = 2$, then interpret $(1\ i) = (1\ 1)$ or $(2\ j) = (2\ 2)$ as the identity). By Lemma 2, the quick way of computing conjugates in S_n we see that $(1\ 2)^\varphi = (1\ 2)^{i_2}$, and so $i_2^{-1}\varphi$ fixes $(1\ 2)$.

Let $i_2, \dots, i_t$ be given by the inductive hypothesis, so that $\psi = i_t^{-1} \dots i_2^{-1}\varphi$ fixes $(1\ 2), \dots, (1\ t)$. Since ψ preserves transpositions, $(1\ t+1)^\psi = (l\ k)$. Now $(1\ 2)$ and $(l\ k)$ cannot be disjoint, lest $[(1\ 2)(1\ t+1)]^\psi = (1\ 2)^\psi(1\ t+1)^\psi = (1\ 2)(l\ k)$ have order 2, while $(1\ 2)(1\ t+1)$ has order 3.

Thus, $(1\ t+1)^{\psi} = (1\ k)$ or $(1\ t+1)^{\psi} = (2\ k)$. If $k \leq t$, then $(1\ t+1)\psi \in \langle (1\ 2), \dots, (1\ t)\rangle$, and hence it is fixed by ψ; this contradicts ψ being injective, for either $(1\ t+1)^{\psi} = (1\ k) = (1\ k)^{\psi}$ or $(1\ t+1)^{\psi} = (2\ k) = (2\ k)^{\psi}$. Hence, $k \geq t+1$. Define i_{t+1} to be conjugation by $(k\ t+1)$. Now i_{t+1} fixes $(1\ 2), \dots, (1\ t)$ and $(1\ t+1)^{i_{t+1}} = (1\ t+1)^{\psi}$, so that $i_{t+1}^{-1} \dots i_2^{-1}\varphi$ fixes $(1\ 2), \dots, (1\ t+1)$ and the induction is complete. It follows that $i_n^{-1} \dots i_2^{-1}\varphi$ fixes $(1\ 2), \dots, (1\ n)$. But these transpositions generate S_n, and so $i_n^{-1} \dots i_2^{-1}\varphi$ is the identity. Therefore, $\varphi = i_2 \dots i_n \in \mathrm{Inn}(S_n)$. □

Theorem 11. $\mathrm{Aut}(S_1)$ *is trivial.*

Proof. $S_1 = \{e\}$, where $e = (1)$. Let $\varphi \in \mathrm{Aut}(S_1)$. Then $\varphi(e) = e$, so $\varphi = \mathrm{id}$, and we obtain that $\mathrm{Aut}(S_1) = \{\mathrm{id}\}$ is trivial. □

Remark. Obviously $\mathrm{Aut}(S_1) \cong S_1$.

Theorem 12. $\mathrm{Aut}(S_2)$ *is trivial.*

Proof.

$$S_2 = \{e, \sigma\},$$

where

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2).$$

Let $\varphi \in \mathrm{Aut}(S_2)$. Then $\varphi(e) = e$, $\varphi(\sigma) = \sigma$, so $\varphi = \mathrm{id}$. Hence $\mathrm{Aut}(S_2) = \{\mathrm{id}\}$ is trivial. □

Lemma 4. *Let $k \in \mathbb{N}$. If $k \geq 4$, then $(2k-2)! > k!2^{k-1}$.*

Proof. We prove this Lemma by induction on $k \geq 4$. Let $k = 4$, then $(2k-2)! = 6! = 720 > 192 = 4! \cdot 2^3 = k!2^{k-1}$. By hypothesis, $(2k-2)! > k!2^{k-1}$, hence $(2(k+1)-2)! = (2k)! = (2k-2)!(2k-1)2k > k!2^{k-1}(2k-1)2k = k!(2k-1)k2^k > (k+1)!2^k$, since $k > 1$, $2k-1 > k+1$. □

Theorem 13. *For $n \neq 2, 6$, S_n is complete.*

Proof. Let T_k denote the conjugacy class in S_n consisting of all products of k disjoint transpositions. By Lemma 1, a permutation in S_n is an involution if and only if it lies in some T_k. It follows that if $\theta \in \mathrm{Aut}(S_n)$, then $\theta(T_1) = T_k$ for some k. We shall show that if $n \neq 6$, then $|T_k| \neq |T_1|$ for $k \neq 1$. Assuming this, then $\theta(T_1) = T_1$, and Lemma 3 completes the proof.

Now $|T_1| = n(n-1)/2$. To count T_k, observe first that there are

$$\frac{1}{2}n(n-1) \times \frac{1}{2}(n-2)(n-3) \times \dots \times \frac{1}{2}(n-2k+2)(n-2k+1)$$

k-tuples of disjoint transpositions. Since disjoint transpositions commute and there are $k!$ orderings obtained from any k-tuple, we have

$$|T_k| = n(n-1)(n-2)\dots(n-2k+1)/k!2^k.$$

The question whether $|T_1| = |T_k|$ leads to the question whether there is some $k > 1$ such that

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

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

$$(n-2)(n-3)\dots(n-2k+1) \geq (2k-2)(2k-3)\dots(2k-2k+1) = (2k-2)!.$$

Since if $k \geq 4$, then $(2k-2)! > k!2^{k-1}$ by Lemma 4, and so equation 1 can hold only if $k = 2$ or $k = 3$. When $k = 2$, we obtain

$$(n-2)(n-3) = 4,$$

and obviously this equality never holds for any $n \in \mathbb{N}$; we may assume, therefore, that $k = 3$. Since $n \geq 2k$, we must have $n \geq 6$. If $n > 6$, then we have for the left side of equation 1: $(n-2)(n-3)\ldots(n-2k+1) \geq 5 \times 4 \times 3 \times 2 = 120$, while the right side is $3!2^2 = 24$. We have shown that if $n \neq 6$, then $|T_1| \neq |T_k|$ for all $k > 1$, as desired. □

Corollary 5. *If θ is an outer automorphism of S_6, and if $\tau \in S_6$ is a transposition, then $0(\tau)$ is a product of three disjoint transpositions.*

Proof. If $n = 6$, then we saw in the proof of the theorem that equation 1 does not hold il $k \neq 3$. (When $k = 3$, both sides of equation 1 equal 24.) □

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

Proof. If G is complete, then $Aut(G) \cong G$. □

We now show that S_6 is a genuine exception.

Definition 7. A subgroup $K \leq S_X$ is transitive if, for every pair $x, y \in X$, there exists $\sigma \in K$ with $\sigma(x) = y$.

In Theorem 10, we saw that if $H \leq G$, then the family X of all left cosets of H is a G-set (where $\varphi_a : gH \mapsto agH$ for each $a \in G$); indeed, X is a transitive G-set: given gH and $g'H$, then $\varphi_a(gH) = g'H$, where $a = g'g^{-1}$.

Lemma 5. *Let $P \leq G$ be a Sylow subgroup. If $N_G(P) \leq H \leq G$, then H is equal to its own normalizer; that is $H = N_G(H)$.*

Lemma 6. *Let X be a G-set with action $\varphi : G \times X \to X$, and let $\psi : G \to S_X$ send $g \in G$ into the permutation $x \mapsto gx$. If X is a transitive G-set, then $|\ker(\psi)| \leq |G|/|X|$.*

Lemma 7. *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 $\varphi : S_5 \to S_X \cong S_6$. Now X is a transitive S_5-set, by Lemma 5, and so $|\ker\varphi| \leq |S_5|/r = |S_5|/6$, by Lemma 6. Since the only normal subgroups of S_5 are trivial, A_5, and S_5, it follows that $\ker\varphi = \{1\}$ and φ is an injection. Therefore, $\mathrm{im}(\varphi) \cong S_5$ is a transitive subgroup of S_X of order 120.

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

Theorem 14 (Hölder). *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: $Y = \{\sigma_1 K, \ldots, \sigma_6 K\}$. 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 $\theta \in \mathrm{Aut}(S_6)$, 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 $\theta_{(1\ 2)} : \sigma_i K \mapsto (1\ 2)\sigma_i K$ for all i, is a transposition, and hence θ fixes $\sigma_i K$ for four different i. But if $\theta_{(1\ 2)}$ fixes even one left coset, say $\sigma_i K = (1\ 2)\sigma_i K$, then $\sigma_i^{-1}(1\ 2)\sigma_i$ is a transposition in K. This contradiction shows that θ is an outer automorphism. □

Theorem 15. $\mathrm{Aut}(S_6)/\mathrm{Inn}(S6) \cong \mathbb{Z}_2$, *and so* $|\mathrm{Aut}(S_6)| = 1440$.

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, by Corollary 5, and so $\theta^{-1}\psi(T_1) = T_1$. Therefore, $\theta^{-1}\psi \in \mathrm{Inn}(S_6)$, by Lemma 3, and $\mathrm{Aut}(S_6)/\mathrm{Inn}(S_6)$ has order 2. □

This theorem shows that there is essentially only one outer automorphism θ of S_6; given an outer automorphism θ, then every other such has the form $\varphi\theta$ for some inner automorphism φ. It follows that S_6 has exactly 720 outer automorphisms, for they comprise the other coset of $\mathrm{Inn}(S_6)$ in $\mathrm{Aut}(S_6)$.

The following table contains the above results.

n	$\mathrm{Aut}(S_n)$	$\mathrm{Out}(S_n)$
$n \neq 2, 6$	S_n	1
$n = 2$	1	1
$n = 6$	$S_6 \rtimes C_2$	C_2

References

[1] Ben Howard, John Millson, Andrew Snowden, and Ravi Vakil. A description of the outer automorphism of S_6, and the invariants of six points in projective space. Journal of Combinatorial Theory, Series A, Volume 115, Issue 7, October 2008, pp. 1296–1303.

[2] Robert T. Curtis. 2007. Symmetric Generation of Groups. With Applications to Many of the Sporadic Finite Simple Groups. Cambridge University Press.

[3] Janusz, G. and Rotman, J. Outer automorphisms of S_6. The American Mathematical Monthly, Vol. 89, No. 6 (Jun. — Jul., 1982), pp. 407–410.

[4] Miller, D. W. On a theorem of Hölder. The American Mathematical Monthly, Vol. 65, No. 4 (Apr., 1958), pp. 252–254.

[5] Rotman, J. J. 1995. An introduction to the theory of groups, volume 148 of Graduate Texts in Mathematics. Springer-Verlag, New York, fourth edition.