Automorphisms of S_n and of A_n

In this note we prove that if $n \neq 6$, then $\mathrm{Aut}(S_n) \cong S_n \cong \mathrm{Aut}(A_n)$. In particular, when $n \neq 6$, every automorphism of S_n is inner and every automorphism of A_n is the restriction of an inner automorphism of S_n. However, $\mathrm{Aut}(S_6)$ is not isomorphic to S_6; while we do not prove it, in fact, $\mathrm{Aut}(S_6) = \mathrm{Aut}(A_6)$ satisfies $[\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)] = 2$. See Chapter 3.2 of [1] for this fact. Recall that S_n and A_n have trivial center (if $n \neq 2$ for S_n and $n \neq 3$ for A_n).

Our arguments will be combinatorial. For that reason, we mention some relevant properties of S_n. First, the conjugacy class of a permutation σ is the set of all permutations with the same cycle structure as σ. Second, S_n is generated by the transpositions $\{(1,i) : i > 1\}$. To see this we note that $(1,r)(1,s)(1,r) = (r,s)$ if $r \neq s$; this proves the claim since S_n is generated by the transpositions.

Lemma 1. *If $1 \leq k \leq n/2$, then the number of products of k disjoint transpositions in S_n is $n!/\big(2^k k!(n-2k)!\big)$.*

Proof. A product of k disjoint transpositions in S_n has the form $(a_1,b_1)\cdots(a_k,b_k)$ with the a_i, b_i distinct integers between 1 and n. Choosing a single transposition (a,b) can be done in $n(n-1)/2$ ways; we note that $(a,b) = (b,a)$. We have $n(n-1)/2$ choices for (a_1,b_1). Similarly, there are $(n-2)(n-3)/2$ choices for (a_2,b_2) once (a_1,b_1) has been chosen. Continuing this argument, and keeping track of order of the (a_i,b_i), there are

$$\frac{n(n-1)}{2} \cdot \frac{(n-2)(n-3)}{2} \cdot \cdots \cdot \frac{(n-2k-2)(n-2k-1)}{2} = \frac{n!}{2^k(n-2k)!}$$

choices for an ordered list of k disjoint transpositions. Since order doesn't matter, we must divide by $k!$ to get the possible products that result. Thus, the formula stated in the lemma is true. ∎

Lemma 2. *Let $\varphi \in \mathrm{Aut}(S_n)$. If φ sends transpositions to transpositions, then φ is inner.*

Proof. Suppose that $\varphi(1,r) = (a_r,b_r)$ for each r. Then $\varphi\left((1,2)(1,r)\right) = (a_2,b_2)(a_r,b_r)$. However, if $r \geq 3$, then $(1,2)(1,r) = (1,r,2)$, an element of order 3. Thus, either $a_r \in \{a_2,b_2\}$ or $b_r \in \{a_2,b_2\}$. By reversing a_r and b_r if necessary, we may suppose that $a_r \in \{a_2,b_2\}$ for all r. We claim that either $a_r = a_2$ for all r or $a_r = b_2$ for all r; suppose instead that there are $r \neq s$ with $a_r = a_2$ and $a_s = b_2$. Note that $(1,r,2)(1,s,2) = (1,s)(2,r)$ has order 2.

However,

$$\begin{aligned}\varphi\left((1,r,2)(1,s,2)\right) &= (a_2,b_2)(a_r,b_r)(a_2,b_2)(a_s,b_s) \\ &= (a_2,b_2)(a_2,b_r)(a_2,b_2)(b_2,b_s) \\ &= (a_2,b_r,b_2)(a_2,b_2,b_s) \\ &= (b_2,b_s,b_r)\end{aligned}$$

has order 3. This is a contradiction. Thus, we must either have $a_2 = a_r$ for all r or $b_2 = b_r$ for all r. We assume that $a_2 = a_r$ for all r; the other case is similar. We then have $\varphi(1,r) = (a_2, b_r)$ for all $r \geq 3$. Note that this forces $b_r \neq b_s$ if $r \neq s$ since φ is 1-1. Let x be a permutation for which $x(1) = a_2$ and $x(r) = b_r$ for all $r \geq 3$. This uniquely determines x; we have defined x on $n-1$ values, which is enough to completely determine a permutation of n elements. From the choice of x we see that $\varphi(1,r) = (a_2,b_r) = x(1,r)x^{-1}$. Therefore, $\varphi = \mathrm{Int}(x)$ is inner. □

Theorem 3. *If $n \neq 6$, then every automorphism of S_n is inner. Thus,* $\mathrm{Aut}(S_n) \cong S_n$.

Proof. Let $\varphi \in \mathrm{Aut}(S_n)$. If σ is a transposition, then $\varphi(\sigma)$ has order 2. Thus, $\varphi(\sigma)$ is the product of $k \geq 1$ disjoint transpositions for some k. Now, φ sends conjugacy classes to conjugacy classes. The conjugacy class of the product of k disjoint transpositions is the set of all products of k disjoint transpositions. Thus, Lemma 1 implies that $n(n-1)/2 = n!/\left(2^k k!(n-2k)!\right)$. We note that this equation is valid if $k=1$ or if $n=6$ and $k=3$. It is easy to check that it is not valid if $n<6$. We rewrite the equation as $(n-2)! = 2^{k-1}k!(n-2k)!$ We first show, by induction on k, that if $n = 2k \geq 8$, then $(n-2)! > 2^{k-1}k!$ This is clear for $k=4$. Suppose that it is true for k. Then

$$\begin{aligned}(2(k+1)-2)! &= (2k)! = 2k(2k-1)(2k-2)! \\ &> 2k(2k-1)2^{k-1}k! = 2^k k(2k-1)k! > 2^k(k+1)!\end{aligned}$$

since $k(2k-1) \geq k+1$. Thus, this claim is true.

Next we show, by induction on n, that if $n \geq 7$, then $(n-2)! > 2^{k-1}k!(n-2k)!$ whenever $n > 2k \geq 2$. It is easy enough to verify this for $n=5$. Suppose that the result is true for n. If $n+1 > 2k$, then either $n = 2k$ or $n > 2k$. If $n = 2k$, then $k \geq 4$, and by the previous paragraph, we have

$$\begin{aligned}(n-1)! &= (n-1)(n-2)! > (n-1)2^k k! \\ &= (n-1)2^k k!(n-2k)! > 2^k k!(n-2k)!\end{aligned}$$

On the other hand, if $n > 2k$, then the induction hypothesis yields

$$\begin{aligned}(n-1)! &= (n-1)(n-2)! > (n-1)2^k k!(n-2k)! \\ &> 2^k k!(n+1-2k)!\end{aligned}$$

This finishes the proof of this second claim. What we have proven is that, if $n \neq 6$, then the conjugacy classes of transpositions and products of k disjoint transpositions are of different sizes. Thus, φ sends transpositions to transpositions. By Lemma 2, this implies that φ is inner. □

We now consider A_n. Recall that A_n is generated by 3-cycles. For an easy proof of this, we note that A_n is generated by products of 2 transpositions. Since

$$\begin{aligned}(a,b)(c,d) &= (a,c,b)(a,c,d), \\ (a,b)(b,c) &= (a,c,b)\end{aligned}$$

whenever a, b, c, d are distinct, the claim is verified. To help with the following proof, we note that there are four possibilities for the product of two 3-cycles:

$$\begin{aligned}(a,b,c)(a,b,d) &= (a,d)(b,c), \\ (a,b,c)(a,d,b) &= (b,c,d), \\ (a,b,c)(a,d,e) &= (a,b,c,d,e), \\ (a,b,c)(d,e,f). &\end{aligned}$$

The only case where we get an element of order 2 is in the first case.

Lemma 4. *The number of products of k disjoint 3-cycles is $n!/\big(3^k k!(n-3k)!\big)$.*

Proof. The argument is similar to that of Lemma 2. If $\sigma = (a_1, b_1, c_1) \cdots (a_k, b_k, c_k)$, then the number of choices for a_1, b_1, c_1 is $n(n-1)(n-2)$, and the same cycle is represented in three ways. Repeating this idea, we see that the number of choices for an ordered list $\tau_1 \cdots \tau_k$ of disjoint 3-cycles is

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

Since order of the product $\tau_1 \cdots \tau_k$ does not change the permutation, we must divide by $k!$ to count the number of these products. This proves the lemma. □

Lemma 5. *Let $\varphi \in \mathrm{Aut}(A_n)$. If φ sends 3-cycles to 3-cycles, then $\varphi = \mathrm{Int}(x)|_{A_n}$ for some $x \in S_n$.*

Proof. Let $u_i = (1, 2, i)$. We claim that there are a_1, a_2 so that for each $i \geq 3$, we have $\varphi(u_i) = (a_1, a_2, a_i)$ for some a_i. Set $v_i = \varphi(u_i)$. Note that $u_i u_j$ has order 2 whenever $i \neq j$ by the calculation before Lemma 4. Thus, $v_i v_j$ also has order 2. Therefore, there are a_1, a_2 with $v_3 = (a_1, a_2, c)$ and $v_4 = (a_1, a_2, d)$. Consider v_i for $i \geq 5$. If v_i fixes a_1, then we must have $v_i = (a_2, c, *)$ and $v_i = (a_2, d, *)$. This is impossible. Therefore, a_1 occurs in the cycle structure of v_i, and this forces $v_i = (a_1, a_2, a_i)$. This proves our claim. Define $x \in S_n$ by $x(i) = a_i$ for all. Then $x u_i x^{-1} = v_i$ by a short calculation. Thus, $\varphi = \mathrm{Int}(x)|_{A_n}$, as desired. □

To prove the following theorem, we relate conjugacy classes in S_n to those in A_n. If $\sigma \in A_n$, then its conjugacy class $\mathrm{Cl}_{S_n}(\sigma)$ has order $[S_n : C_{S_n}(\sigma)]$, where $C_{S_n}(\sigma)$ is the centralizer of σ in S_n. Similarly, $\mathrm{Cl}_{A_n}(\sigma)$ has order $[S_n : C_{A_n}(\sigma)]$. Now, $C_{A_n}(\sigma) = A_n \cap C_{S_n}(\sigma)$. From this and the counting formula

$$|NH| = \frac{|N|\,|H|}{|N \cap H|}$$

if N and H are subgroups of a groups G with N normal, we conclude that $|\mathrm{Cl}_{A_n}(\sigma)| = |\mathrm{Cl}_{S_n}(\sigma)|$ or $|\mathrm{Cl}_{A_n}(\sigma)| = \frac{1}{2}|\mathrm{Cl}_{S_n}(\sigma)|$. The first case occurs when $C_{A_n}(\sigma) \nsubseteq A_n$, and the second case occurs otherwise. If $\sigma = (a, b, c)$ is a 3-cycle and $n \geq 5$, then $(1, 2)$ commutes with σ and lies outside of A_n. Thus, $|\mathrm{Cl}_{A_n}(\sigma)| = |\mathrm{Cl}_{S_n}(\sigma)|$. If $\sigma = \tau_1 \cdots \tau_k$ is a product of $k \geq 2$ disjoint 3-cycles, write $\tau_1 = (a, b, c)$ and $\tau_2 = (d, e, f)$. Then $(a, d)(b, e)(c, f)$ commutes with σ; thus, we have $|\mathrm{Cl}_{A_n}(\sigma)| = |\mathrm{Cl}_{S_n}(\sigma)|$ also in this case.

Theorem 6. *If $n \geq 3$ and $n \neq 6$, then every automorphism of A_n is the restriction of an inner automorphism of S_n. Consequently,* $\mathrm{Aut}(A_n) \cong S_n$.

Proof. Let $\varphi \in \mathrm{Aut}(A_n)$. if σ is a 3-cycle, then $\varphi(\sigma)$ has order 3; thus, it is the product of $k \geq 1$ disjoint 3-cycles. If $n < 6$, then $k = 1$ is the only possibility; the result then follows from Lemma 5. Thus, suppose that $n \geq 6$. Since φ sends conjugacy classes to conjugacy classes, the conjugacy class in A_n of a 3-cycle then has the same size as the conjugacy class of a product of k disjoint 3-cycles. By Lemma 4 and the comments immediately before the statement of the theorem, we then have $n(n-1)(n-2)/3 = n!/\left(3^k k!(n-3k)!\right)$. This can be proven to occur only when $n = 6$ and $k = 2$ by methods similar to the proof of Theorem 3. Therefore, Lemma 5 shows that φ is the restriction of an automorphism of S_n, and the rest then follows from Theorem 3. □

For completness, we prove that $(n-3)! > 3^{k-1}k!(n-3k)!$ whenever $n > 6$; this was the claim used in the proof of Theorem 6. We do this in two cases. First, if $k \geq 3$, we prove that $(3k-3)! > 3^{k-1}k!$ by induction on k. The case $k = 3$ is clear. Suppose the result is true for k. Then

$$\begin{aligned}
(3(k+1)-3)! &= (3k)! = (3k)(3k-1)(3k-2)(3k-3)! \\
&> (3k)(3k-1)(3k-2)3^{k-1}k! = 3^k k(3k-1)(3k-2)k! \\
&> 3^k(k+1)!
\end{aligned}$$

Thus, by induction, this claim is true for all $k \geq 3$. Next, we prove by induction on n, that if $n \geq 7$ and $n \geq 3k$, then $(n-3)! > 3^{k-1}k!(n-3k)!$. The result is easily seen to be true for $n = 7$. Thus, we assume that $n \geq 7$ and that the result holds for n. If $n > 3k \geq 3$, then by the induction hypothesis,

$$\begin{aligned}
(n-2)! &= (n-2)(n-3)! > (n-2)3^{k-1}k!(n-3k)! \\
&\geq 3^{k-1}k!(n+1-3k)
\end{aligned}$$

since $k \geq 1$. On the other hand, if $n = 3k$, then

$$\begin{aligned}(n-2)! &= (n-2)(n-3)! > (n-2)3^{k-1}k! \\ &= (n-2)3^{k-1}k!(n+1-3k)! \\ &> 3^{k-1}k!(n+1-3k)!\end{aligned}$$

by the earlier claim. Thus, the result is true for all $n \geq 7$ and all k with $n \geq 3k$.

References

[1] Michio Suzuki, *Group theory. I*, Springer-Verlag, Berlin, 1982.