Algebra 2. The symmetric groups $S_n$.

Roma, December 15, 2009

In this note we determine the automorphism groups of the symmetric groups $S_n$. For $n = 2$ this is very easy: we have $S_2 \cong \mathbb{Z}_2$ and hence $\text{Aut}(S_2)$ is trivial. Therefore we suppose from now on that $n > 2$. The main result is Theorem 8.

For the convenience of the reader we first recall some basic properties of the groups $S_n$ and the subgroups $A_n$ of even permutations.

**Lemma 1.** Let $n > 2$.
(a) The center of $S_n$ is trivial;
(b) For $n > 3$ the center of $A_n$ is trivial.

**Proof.** (a) Let $\sigma \in Z(S_n)$. If $\sigma \neq \text{id}$, then there exist two distinct $a, b \in \{1, 2, \ldots, n\}$ with $\sigma(a) = b$. Choose $c \in \{1, 2, \ldots, n\}$ with $c \neq a$ and $c \neq b$. Then $(b c) \sigma \neq \sigma(b c)$ because $(b c) \sigma$ maps $a$ to $c$, while $\sigma(b c)$ maps $a$ to $b$. This shows that $\sigma = \text{id}$ and $Z(S_n)$ must be trivial, as required.
(b) Similarly, suppose that $\sigma \in Z(A_n)$ is non-trivial. Pick two distinct $a, b \in \{1, 2, \ldots, n\}$ with $\sigma(a) = b$ and choose two elements $c, d \in \{1, 2, \ldots, n\}$ different from $a$ and $b$. Then $(b c d) \sigma \neq \sigma(b c d)$ because the two permutations map $a$ to different elements.

**Lemma 2.** Two elements of $S_n$ are conjugate if and only if they have the same cycle type.

**Proof.** For any $\sigma \in S_n$ and any $d \leq n$ we have

$$\sigma(1 2 \ldots d) \sigma^{-1} = (\sigma(1) \sigma(2) \ldots \sigma(d)).$$

This shows that any conjugate of a $d$-cycle is again a $d$-cycle. Since every permutation is a product of disjoint cycles, it follows that the cycle types of conjugate permutations are the same. In the other direction, let $\tau = (a_1 \ldots a_r)(a_{r+1} \ldots a_s)(a_{l} \ldots a_m)$ and $\tau' = (a_1' \ldots a_r')(a_{r+1}' \ldots a_s')(a_{l}' \ldots a_m')$ be two permutations having the same cycle type. Define $\sigma \in S_n$ by $\sigma(a_i) = a_i'$ for $i = 1, 2, \ldots, m$. Then

$$\sigma \tau \sigma^{-1} = \sigma(a_1 \ldots a_r) \sigma^{-1} \sigma(a_{r+1} \ldots a_s) \sigma^{-1} \ldots \sigma(a_l \ldots a_m) \sigma^{-1},$$

$$= (a_1' \ldots a_r')(a_{r+1}' \ldots a_s')(a_{l}' \ldots a_m'),$$

$$= \tau'.$$

This shows that $\tau$ and $\tau'$ are conjugate, as required.

**Lemma 3.** Let $n > 2$.
(a) The group $A_n$ is generated by 3-cycles.
(b) Any normal subgroup of $A_n$ that contains a 3-cycle, is equal to $A_n$ itself.

**Proof.** (a) The product $(1 2)(2 3)$ is equal to the 3-cycle $(1 2 3)$. The product of two disjoint 2-cycles $(a b)$ and $(c d)$ is equal to $(a b)(b c)(b c)(c d)$ and is hence a product of two 3-cycles. Since any element of $A_n$ is a product of an even number of transpositions, it is therefore a product of 3-cycles.
(b) Let $N \subset A_n$ be a normal subgroup and suppose that $(1 2 3) \in N$. Let $\sigma' \in A_n$ be an arbitrary 3-cycle. Then $\sigma' = \tau(1 2 3) \tau^{-1}$ for some $\tau \in S_n$. If $\tau \in A_n$, then $\sigma' \in N$ and we are done. If not, then $\tau' = \tau(1 2)$ is in $A_n$ and $\sigma' = \tau'(1 3 2) \tau'^{-1}$ is once again in $N$. 

1
Lemma 4. The commutator subgroup of $S_n$ is equal to $A_n$. For $n \geq 5$ the commutator subgroup of $A_n$ is equal to $A_n$ itself.

Proof. Since $S_n/A_n$ is commutative, the commutator subgroup $S'_n$ is contained in $A_n$. Conversely, we have $(12)(13)(12)^{-1}(13)^{-1} = (123)$, showing that every 3-cycle is in $S'_n$. By Lemma 3 (a) the group $A_n$ is generated by 3-cycles, so that $S'_n = A_n$ as required.

The identity

$$(123)(345)(123)^{-1}(345)^{-1} = (143),$$

shows that for $n \geq 5$ every 3-cycle is a commutator of $A_n$. This implies the second statement.

We remark that the group $A_3$ is abelian, so that its commutator subgroup is trivial. The group $A_4$ is not abelian. Its commutator subgroup is

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}.$$ 

Indeed, $V_4$ is normal and the quotient $A_4/V_4$ has order 3 and is hence abelian. It follows that $A'_4 \subset V_4$. Equality follows from the identity $(123)(124)(123)^{-1}(124)^{-1} = (12)(34)$.

Proposition 5. Let $n \geq 5$. Then the group $A_n$ is simple, i.e. does not contain any proper normal subgroups. The only proper normal subgroup of $S_n$ is $A_n$.

Proof. Let $N \subset A_n$ be a non-trivial normal subgroup. We will show that $N$ contains a 3-cycle. Then Lemma 3 (b) implies the required result.

Step 1. Suppose that $N$ contains a permutation $\sigma$ which is a product of disjoint cycles at least one of which has length $d \geq 4$. Then, up to renumbering, we have $\sigma = (12\ldots d)\tau$ where $\tau$ leaves $\{1,2,\ldots,d\}$ invariant. The permutation $\sigma^{-1}(123)\sigma(123)^{-1}$ is contained in $N$. One easily checks that it is equal to the 3-cycle $(13d)$.

Step 2. This leaves us with the possibility that all permutations in $N$ are products of disjoint cycles of length $\leq 3$. Suppose that $N$ contains a permutation $\sigma$ admitting a 3-cycle. If it admits only one 3-cycle, then its square is a 3-cycle and we are done. If it contains at least two 3-cycles, we may assume that $\sigma = (123)(456)\tau$ where $\tau$ leaves $\{1,2,\ldots,6\}$ invariant. Then $\sigma^{-1}(124)\sigma(124)^{-1}$ is contained in $N$. One easily checks that it is equal to $(14236)$ and we are done by Step 1.

Step 3. This leaves us with the possibility that all permutations in $N$ are products of disjoint transpositions. Let $\sigma \in N$ be a non-trivial element. Since $\sigma$ is even, it is a product of at least two transpositions and we may assume that $\sigma = (12)(34)\tau$, where $\tau$ leaves $\{1,2,3,4\}$ invariant. Then $\sigma(123)\sigma(123)^{-1} = (13)(24)$ is in $N$. Since $n \geq 5$ the permutation $(13)(24)(135)(13)(24)(135)^{-1}$ is in $N$. It is equal to the 3-cycle $(135)$ and we are done.

To prove the second statement of the Proposition, let $N$ be a proper normal subgroup of $S_n$. Then $N \cap A_n$ is a normal subgroup of $A_n$. So either $N \subset A_n$ in which case $N = \{1\}$ or $N = A_n$ or we have $N \cap A_n = \{1\}$. In the latter case $\#N \leq 2$ and hence $N \subset Z(S_n)$. Lemma 1 implies then that $N = \{1\}$. This proves the proposition.

We remark that the possibility that arises in Step 3 of the proof of Lemma 5, actually occurs for $n = 4$. In that case the group $V_4$ mentioned above is a normal subgroup of $A_4$. Its elements are products of disjoint transpositions.
Corollary 6. For $n \geq 5$, the proper subgroups of $A_n$ have index at least $n$.

Proof. Let $H \subset A_n$ be a subgroup of index $m$. Translation of the left cosets of $H$ gives rise to a non-trivial homomorphism $A_n \rightarrow S_m$. By Lemma 4 the group $A_n$ admits no proper normal subgroups, so that the map is injective. This implies $\frac{1}{2}n! \leq m!$, which can only happen when $n \leq m$ as required.

Lemma 7. Let $n > 2$ and let $F : S_n \rightarrow S_n$ be an automorphism mapping transpositions to transpositions. Then $F$ is an inner automorphism.

Proof. The product of two distinct transpositions has order 2 when the transpositions are disjoint, while it is a 3-cycle and thus has order 3 when they are not. Therefore any automorphism of $S_n$ maps pairs of disjoint transpositions to pairs of disjoint transpositions.

Let $F(12) = (ab)$. Let $x \in \{1, 2, \ldots, n\}$ be different from 1 or 2. Since $(1 2)(1 x)$ is a 3-cycle, so is $F(12)F(1 x) = (ab)F(1 x)$. It follows that the 2-cycle $F(1 x)$ moves either $a$ or $b$. Switching $a$ and $b$ if necessary, we may assume that it moves $a$, so that $F(1 x) = (ac)$ for some $c$ different from $a$ and $b$.

Claim. For every $y \neq 1$ we have $F(1 y) = (ad)$ for some $d \in \{1, 2, \ldots, n\}$ different from $a$.

Proof of the claim. This is clear when $y = 2$ or $y = x$, so we may assume $y \neq 2, x$. Since both permutations $(1 y)(1 2)$ and $(1 y)(1 x)$ are 3-cycles, so are their images under $F$. We have $F(1 2) = (ab)$ and $F(1 x) = (ac)$. Therefore, if $F(1 y)$ is not moving $a$, then it must move both $b$ and $c$. Since $F(1 y)$ is a transposition, this means that $F(1 y) = (bc)$. Applying $F^{-1}$ to the relation

$$(ab)(ac)(bc) = (ac),$$

we find

$$(1 2)(1 x)(1 y) = (1 x).$$

Since $y \notin \{1, 2, x\}$, the permutation on the left maps 1 to $y$. Since $x \neq y$, this is absurd and we conclude that $F(1 y)$ actually moves $a$ so that $F(1 y) = (ad)$ for some $d$ as required.

Define the permutation $\sigma \in S_n$ by putting $\sigma(1) = a$ and for every $y \neq 1$ put $\sigma(y) = d$, where $d$ is the unique element for which $F(1 y) = (ad)$. Its existence is guaranteed by the claim. Let $s : S_n \rightarrow S_n$ denote the conjugation by $\sigma$ map. For every $y$ we have

$$s^{-1}F(1 y) = s^{-1}(ad) = \sigma^{-1}(ad)\sigma = (1 y).$$

In other words, $s^{-1}F$ fixes all transpositions of the form $(1 y)$. Since $(yz)(1 y)(1 z)$, the group $S_n$ is generated by these transpositions. Therefore $s^{-1}F$ fixes every element of $S_n$, so that $F = s$. This proves the lemma.

Consider the homomorphism

$$S_n \rightarrow \text{Aut}(S_n)$$

that maps $\sigma \in S_n$ to the automorphism given by conjugation by $\sigma$. Its image is the subgroup of inner automorphisms of $\text{Aut}(S_n)$. The kernel is precisely the center of $S_n$. Lemma 1 implies therefore that it is trivial. Therefore we can identify $S_n$ with its image in $\text{Aut}(S_n)$. The main result of this note if the following
Theorem 8. Let \( n > 2 \). We have \( \text{Aut}(S_n) = S_n \) except when \( n = 6 \). In the exceptional case we have \([\text{Aut}(S_6) : S_6] = 2\).

Proof. The involutions (i.e. elements of order 2) of \( S_n \) are precisely the products of disjoint transpositions. For each \( k \) with \( 1 \leq k \leq n/2 \), the set of products of \( k \) disjoint transpositions make up a conjugacy class \( C_k \) of \( S_n \). Any automorphism of \( S_n \) maps involutions to involutions. Moreover, any automorphism \( F \) of \( S_n \) has the property that when \( \sigma, \tau \in S_n \) are conjugate, so are \( F(\sigma) \) and \( F(\tau) \). Therefore an automorphism of \( S_n \) necessarily permutes the conjugacy classes \( C_k \). We have

\[
#C_k = \frac{1}{k!} \binom{n}{2} \binom{n - 2}{2} \cdots \binom{n - 2(k - 1)}{2}.
\]

Let \( n \neq 6 \). Then an application of Lemma 9 below shows that \( #C_1 \neq #C_k \) for any \( k \neq 1 \). It follows that an automorphism \( F : S_n \to S_n \) necessarily maps \( C_1 \) to itself. In other words, \( F \) maps transpositions to transpositions. Lemma 7 implies then that \( F \) is an inner automorphism, as required.

When \( n = 6 \), of number of transpositions is 15. This is the same as the number \( \frac{1}{3!} \binom{6}{2} \binom{6}{4} \) of involutions of cycle type \( (1 2)(3 4)(5 6) \). On the other hand, there are 45 involutions of cycle type \( (1 2)(3 4) \). In other words, we have \( #C_1 = #C_3 = 15 \), while \( #C_2 = 45 \). See Table 12 below. Therefore, any automorphism \( F : S_6 \to S_6 \) either preserves the transpositions and is by Lemma 2 an inner automorphism or it switches the conjugacy classes \( C_1 \) and \( C_3 \) and is not an inner automorphism. It follows that the composition of any two non-inner automorphisms preserves \( C_1 \) and is interior. This shows that \([\text{Aut}(S_6) : S_6] \leq 2\). Below we actually construct a non-inner automorphism of \( S_6 \), showing that the index is 2, as required.

Lemma 9. The only solution \( k, m \in \mathbb{Z} \) of the equation

\[
\left( \frac{m}{2} \right) \binom{m - 2}{2} \cdots \binom{m - 2(k - 1)}{2} = (k + 1)!
\]

with \( m \geq 3 \) and \( 1 \leq k \leq m/2 \), is given by \( m = 4 \) and \( k = 2 \).

Proof. The left hand side of the equation is equal to

\[
\frac{m(m - 1) \cdots (m + 2 - 2k)(m + 1 - 2k)}{2^k} = \frac{m!}{(m - 2k)! 2^k}.
\]

Therefore the equation can be rewritten as

\[
\binom{m}{2k} = \frac{(k + 1)! 2^k}{(2k)!}.
\]

For \( k = 1 \) this becomes \( m(m - 1) = 4 \), which has no solutions in \( \mathbb{Z} \). For \( k = 2 \) we find \( m(m - 1)(m - 2)(m - 3) = 24 \) whose only solutions in \( \mathbb{Z} \) are \( m = 4 \) and \( m = -1 \). For \( k \geq 3 \)
the right hand side of the equation is less than 1. On the other hand, since $1 \leq k \leq m/2$, the binomial coefficient $\binom{m}{k}$ is a positive integer. This shows that there are no further solutions, as required.

**Construction of an outer automorphism of $S_6$.** Consider the symmetric group $S_5$. It contains 24 5-cycles and hence has six cyclic subgroups of cardinality 5. Since $S_5$ acts by conjugation transitively on the 5-cycles, it also acts transitively on the set of six groups of cardinality 5. Therefore we obtain a homomorphism $j : S_5 \rightarrow S_6$ whose image has cardinality at least 6. By Lemma 4 the group $S_5$ has no non-trivial normal subgroups except $A_5$. Therefore $j$ is injective.

**Remark.** The homomorphism $j : S_5 \rightarrow S_6$ preserves parity.

**Proof.** The morphism $j$ maps commutators to commutators. So Lemma 4 implies $j(A_5) \subset A_6$. By Corollary 6 the group $A_6$ does not admit any subgroups of index 3. Therefore the image of $j$ is not contained in $A_6$. This explains the remark.

Let $H$ denote the image of $j$. It is isomorphic to $S_5$ and has index 6 inside $S_6$. Let $X$ denote the set of left cosets of $H$. The group $S_6$ acts on $X$ by left translation. This gives rise to a homomorphism

$$F : S_6 \rightarrow S(X) \cong S_6,$$

which is injective, because $S_6$ contains no proper normal subgroups except $A_6$.

The homomorphism $F$ is an outer automorphism of $S_6$. Indeed, suppose that $F(12)$ is a transposition. Then it has fixed points. This means that $(12)xH = xH$ for some coset $xH$. It follows that $H$ contains the transposition $x^{-1}(12)x$. Since the homomorphism $S_5 \rightarrow S_6$ preserves parity, the permutation $\sigma \in S_5$ that is mapped to this transposition is odd. It follows that $\sigma$ is a transposition that normalizes an order 5 subgroup $P$ of $S_5$.

We may assume that $P$ is generated by $(12345)$ and that $\sigma$ fixes 1. Then

$$\sigma(12345)\sigma^{-1} = (1\sigma(2)\sigma(3), \sigma(4)\sigma(5))$$

is equal to $(12345)$ or its inverse. This implies that $\sigma = \text{id}$ or $\sigma = (25)(34)$ respectively, contradicting the fact that $\sigma$ is odd. We conclude that $F(12)$ is not a transposition. Lemma 7 implies now that $F$ is not an inner automorphism. This proves Theorem 2.

Indeed, as was explained above, the automorphism $F$ constructed above necessarily switches the transpositions and the involution with cycle type $(12)(34)(56)$. In order to describe certain properties of the outer automorphisms of $S_6$, we consider the normalizer of an order 5 subgroup $P$ of $S_5$.

**Lemma 10.** The normalizer $N(P)$ of an order 5 subgroup $P$ of $S_5$ has 20 elements.

**Proof.** Suppose that $P$ is generated by $(12345)$. Then the 4-cycle $(2354)$ normalizes $P$. The group generated by $(12345)$ and $(2354)$ is contained in $N(P)$. It has order 20 and is not contained in $A_5$. If $N(P)$ were strictly larger, then its intersection with $A_5$ would be a subgroup of $A_5$ of index 2 or 3. This is impossible by Corollary 6. The proves the Lemma.
Corollary 11. Any outer automorphism $F$ of $S_6$ switches the 3-cycles and permutations of type $(123)(456)$ and it switches the 6-cycles and the permutations of type $(123)(45)$.

Proof. If $F$ were to map $(123)$ to a 3-cycle, the subgroup $H$ that appears in the construction of the non-inner automorphism $F$ above, contains a 3-cycle. It is the image of a 3-cycle in $S_5$. Since a 3-cycle has fixed points, the normalizer of an order 5 subgroup of $S_5$ contains a permutation of order 3. This contradicts Lemma 10. Similarly, if $F$ maps the conjugacy class of permutations of type $(123)(45)$ to itself, then $H$ contains a permutation of type $(123)(45)$. Since such a permutation has a fixed point, this means that the normalizer of an order 5 subgroup of $S_5$ contains an element of order 6, contradicting Lemma 5.

The conjugacy classes of the 4-cycles and of the permutations of type $(1234)(56)$ both contain 90 elements. However, the automorphism $F$ does not switch these conjugacy classes, because it preserves the characteristic subgroup $A_6$ of $S_6$. Therefore the signs of the permutations $\sigma$ and $F(\sigma)$ are equal for all $\sigma$.

In conclusion, in the table below, any outer automorphism of $S_6$ switches the conjugacy classes (i) and (ii), it switches (vi) and (vii) and it switches (viii) and (ix). It preserves the other ones.

Table 12. Conjugacy classes of $S_6$.

<table>
<thead>
<tr>
<th>conjugacy class</th>
<th>cycle type</th>
<th>order</th>
<th>sign</th>
<th>#</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i)</td>
<td>(123456)</td>
<td>6</td>
<td>–</td>
<td>5!</td>
<td>120</td>
</tr>
<tr>
<td>(ii)</td>
<td>(123)(45)</td>
<td>6</td>
<td>–</td>
<td>$6 \cdot 2 \cdot \frac{5}{2}$</td>
<td>120</td>
</tr>
<tr>
<td>(iii)</td>
<td>(12345)</td>
<td>5</td>
<td>+</td>
<td>$\frac{1}{3} \cdot 5!$</td>
<td>144</td>
</tr>
<tr>
<td>(iv)</td>
<td>(1234)</td>
<td>4</td>
<td>–</td>
<td>$\binom{6}{2} \cdot 3!$</td>
<td>90</td>
</tr>
<tr>
<td>(v)</td>
<td>(1234)(56)</td>
<td>4</td>
<td>+</td>
<td>$\binom{6}{2} \cdot 3!$</td>
<td>90</td>
</tr>
<tr>
<td>(vi)</td>
<td>(123)</td>
<td>3</td>
<td>+</td>
<td>$\frac{1}{3} \cdot 4 \cdot \binom{6}{3}$</td>
<td>40</td>
</tr>
<tr>
<td>(vii)</td>
<td>(123)(456)</td>
<td>3</td>
<td>+</td>
<td>$\frac{1}{3} \cdot 4 \cdot \binom{6}{3}$</td>
<td>40</td>
</tr>
<tr>
<td>(viii)</td>
<td>(12)</td>
<td>2</td>
<td>–</td>
<td>$\binom{6}{2}$</td>
<td>15</td>
</tr>
<tr>
<td>(ix)</td>
<td>(12)(34)(56)</td>
<td>2</td>
<td>–</td>
<td>$\frac{1}{3} \cdot \binom{6}{2} \cdot \binom{6}{4}$</td>
<td>15</td>
</tr>
<tr>
<td>(x)</td>
<td>(12)(34)</td>
<td>2</td>
<td>+</td>
<td>$\frac{1}{2} \cdot \binom{6}{2} \cdot \binom{6}{4}$</td>
<td>45</td>
</tr>
<tr>
<td>(xi)</td>
<td>(1)</td>
<td>1</td>
<td>+</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>