1. (DF4.3.21) Let $\mathcal{K}$ be a conjugacy class in S_n and assume that $\mathcal{K} \subseteq A_n$. Show $\sigma \in \mathcal{K}$ does *not* commute with any odd permutation if and only if the cycle type of σ consists of distinct odd integers. Deduce that $\mathcal{K}$ consists of two conjugacy classes in A_n if and only if the cycle type of an element of $\mathcal{K}$ consists of distinct odd integers.

Proof. (1) Let $\mathcal{K}$ be a conjugacy class in S_n with $\mathcal{K} \subseteq A_n$ as given. Then suppose that $\sigma \in \mathcal{K}$ does not commute with any odd permutation in S_n. Consider the cycle decomposition of σ into a finite product of disjoint cycles $\sigma = \sigma_1\sigma_2\cdots\sigma_s$ (including all of the 1-cycles). Each σ_i for $1 \leq i \leq s$ will commute with σ because each of the cycles in the cycle decomposition are disjoint. Given any σ_i, we may pass it through σ by commuting σ_i with the first $i-1$ cycles, from which we may take the adjacent cycle σ_i and pass it similarly all the way over:

$$\begin{aligned}\sigma_i\sigma &= \sigma_i(\sigma_1\sigma_2\cdots\sigma_i\cdots\sigma_s)\\ &= \sigma_1\sigma_2\cdots\sigma_i\sigma_i\cdots\sigma_s\\ &= (\sigma_1\sigma_2\cdots\sigma_i\cdots\sigma_s)\sigma_i\\ &= \sigma\sigma_i\end{aligned}$$

Now suppose that some σ_k in the cycle decomposition for σ is of even length. Because σ_k is of even length, we may decompose it into an odd number of transpositions, so that σ_k is an odd permutation. But σ does not commute with any odd permutations, which is in contradiction to the assumption that σ commutes with any cycle in its cycle decomposition. It follows that there cannot be a cycle of even length in the cycle decomposition of σ.

Then suppose that two cycles σ_j and σ_k with $j \neq k$ have the same odd length n. Write $\sigma_j = (a_1\, a_2\, \cdots\, a_n)$ and $\sigma_k = (b_1\, b_2\, \cdots\, b_n)$, and note that because these cycles are disjoint we have that $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ are all distinct, and also do not appear in any σ_i where $i \neq j \neq k$.

We can form the product of n disjoint transpositions

$$\tau = \prod_{i=1}^{n}(a_i\, b_i) = (a_1\, b_1)(a_2\, b_2)\cdots(a_n\, b_n)$$

which interchanges corresponding elements in the cycles σ_j and σ_k. Then observe that τ commutes with all σ_i where $i \neq j \neq k$ because none of a_i or b_j show up in those cycles. (So τ fixes all of the elements found in the other cycles σ_i.)

Since n is odd, τ is an odd permutation. Observe that

$$\begin{aligned}
\tau\sigma\tau^{-1} &= \tau(\sigma_1\sigma_2\cdots\sigma_j\cdots\sigma_k\cdots\sigma_s)\tau^{-1} \\
&= \sigma_1\sigma_2\cdots(\tau\sigma_j\tau^{-1})\cdots(\tau\sigma_k\tau^{-1})\cdots\sigma_s \\
&= \sigma_1\sigma_2\cdots(\tau(a_1\,a_2\,\cdots\,a_n)\tau^{-1})\cdots(\tau(b_1\,b_2\,\cdots\,b_n)\tau^{-1})\cdots\sigma_s \\
&= \sigma_1\sigma_2\cdots(\tau(a_1)\,\tau(a_2)\,\cdots\,\tau(a_n))\cdots(\tau(b_1\,\tau(b_2\,\cdots\,\tau(b_n))\cdots\sigma_s \\
&= \sigma_1\sigma_2\cdots(b_1\,b_2\,\cdots\,b_n)\cdots(a_1\,a_2\,\cdots\,a_n)\cdots\sigma_s \\
&= \sigma_1\sigma_2\cdots\sigma_k\cdots\sigma_j\cdots\sigma_s \\
&= \sigma,
\end{aligned}$$

using our very useful formula in the fifth equality and the fact that σ_j and σ_j were disjoint in the last equality. This implies that τ commutes with σ, but this is in contradiction with the assumption that σ did not commute with odd permutations. Therefore the assumption that there could be two cycles in the cycle decomposition of σ with the same odd length cannot hold.

Hence the cycle type of σ consists of only distinct odd integers, and because σ was an arbitrary element of the conjugacy class $\mathcal{K}$, the same can be said for the cycle type of any element of $\mathcal{K}$, as they all have the same cycle type.

Conversely, suppose that the cycle type of $\sigma \in \mathcal{K}$ consists of only distinct odd integers, and again write its cycle decomposition as $\sigma = \sigma_1\sigma_2\cdots\sigma_s$ (including all of the 1-cycles). Observe that every element $\pi \in \langle\sigma_1, \sigma_2, \ldots, \sigma_s\rangle$ commutes with σ because π will be a finite product of σ_i, each of which we can commute with σ, as we saw earlier. It also does not matter which order the cycles in π appear since any two σ_i, σ_j which appear in the decomposition for π are either disjoint or equal to each other (and hence commute with each other), as they are from the cycle decomposition of σ.

We show that σ commutes only with permutations from $\langle\sigma_1, \sigma_2, \ldots, \sigma_s\rangle$. Consider some element τ *not* in $\langle\sigma_1, \sigma_2, \ldots, \sigma_s\rangle$; that is to say, the cycle decomposition of τ contains disjoint cycles (at least one) $\tau_1, \ldots, \tau_j$ which do not take on the form σ_i for every i. It suffices to show that the permutation $\tau_1\cdots\tau_j$ does not commute with σ (as all of the other cycles in τ will by assumption).

It is impossible for $(\tau_1\cdots\tau_i)\sigma(\tau_i^{-1}\cdots\tau_1^{-1}) = \sigma$ to occur, because every cycle in the cycle decomposition for σ has distinct length, and because each of $\tau_1, \ldots, \tau_j$ are disjoint from each other (so there is no way for conjugation by $(\tau_1\cdots\tau_j)$ to act as an identity for some given σ_i). The disjointness of each of the cycles τ_i imply that the only way to satisfy $(\tau_1\cdots\tau_i)\sigma(\tau_i^{-1}\cdots\tau_1^{-1}) = \sigma$ is by interchanging pairs of cycles in the cycle decomposition of σ, which cannot happen since each cycle σ_i has distinct length. So τ does not commute with σ.

Thus σ commutes with only those elements in $\langle\sigma_1, \sigma_2, \ldots, \sigma_s\rangle$. All of these elements are even permutations since each σ_i is a (disjoint) cycle of odd length, and the composition of a finite number of even permutations is still even. Therefore none of the odd permutations in S_n commute with σ, where σ was any element of the conjugacy class $\mathcal{K}$.

Hence $\sigma \in \mathcal{K}$ does *not* commute with any odd permutation if and only if the cycle type of σ consists of distinct odd integers. □

Proof. Then to deduce that $\mathcal{K}$ consists of two conjugacy classes in A_n if and only if the cycle type of an element of $\mathcal{K}$ consists of distinct odd integers, suppose first that any $\sigma \in \mathcal{K}$ is an element whose cycle type consists of distinct odd integers (so the conjugacy class $\mathcal{K}$ consists of all permutations of the same cycle type as σ). Then we saw earlier that σ does not commute with any odd permutation in S_n.

The size of the conjugacy class $\mathcal{K}$ containing σ is

$$|\mathcal{K}| = \frac{|S_n|}{|C_{S_n}(\sigma)|}.$$

But $C_{S_n}(\sigma) \cap A_n = C_{A_n}(\sigma)$ since σ does not commute with any odd permutations in S_n, so

$$|\mathcal{K}| = \frac{|S_n|}{|C_{S_n}(\sigma)|} = \frac{2|A_n|}{|C_{A_n}(\sigma)|},$$

which means that half of the elements of $\mathcal{K}$ are contained in the conjugacy class $\mathcal{K}_\sigma$ of σ in A_n. The other half of the elements of $\mathcal{K}$ we can obtain by taking some element σ' not in $\mathcal{K}_\sigma$ and applying the same argument as above to see that the conjugacy class $\mathcal{K}_{\sigma'}$ containing σ' also has size which is half of the size of $\mathcal{K}$. Conjugacy classes are distinct, so we have found two conjugacy classes of A_n which are contained in $\mathcal{K}$.

Conversely, suppose that $\mathcal{K}$ consists of two conjugacy classes in A_n. Let σ and σ' be representatives of these two conjugacy classes $\mathcal{K}_\sigma$ and $\mathcal{K}_{\sigma'}$ respectively (so $\sigma \neq \sigma'$ as well). There is a permutation that conjugates σ into σ' in S_n which is not found in A_n; that is, only conjugation by an odd permutation maps elements from $\mathcal{K}_\sigma$ to $\mathcal{K}_{\sigma'}$ and vice versa. Therefore, conjugation by any odd permutation will send some element of $\mathcal{K}_\sigma$ to $\mathcal{K}_{\sigma'}$ (and vice versa). Furthermore, the elements of $\mathcal{K}_\sigma$ are conjugate to each other in A_n and the same can be said about the elements in $\mathcal{K}_{\sigma'}$.

Take any odd permutation τ and conjugate $\sigma \in \mathcal{K}_\sigma$ by τ to form $\tau\sigma\tau^{-1} = \sigma'_\tau \in \mathcal{K}_{\sigma'}$ (so $\sigma \neq \sigma'_\tau$). We may find another even permutation α such that for $\sigma' \in \mathcal{K}_{\sigma'}$ (so $\sigma \neq \sigma'$), we have $\sigma' = \alpha\sigma'_\tau\alpha' = \alpha\tau\sigma\tau^{-1}\alpha^{-1} = (\alpha\tau)\sigma(\alpha\tau)^{-1}$. Since the product of an even permutation with an odd permutation is still an odd permutation, it follows that $\alpha\tau$ is an odd permutation which sends σ to σ'. So for any odd permutation π and $\sigma \in \mathcal{K}_\sigma$, $\sigma \neq \pi\sigma\pi^{-1}$. The same is true if $\sigma \in \mathcal{K}_{\sigma'}$.

Therefore the elements in $\mathcal{K}_\sigma$ and $\mathcal{K}_{\sigma'}$ do not commute with odd permutations (if they did then conjugation of an element in one conjugacy class by an odd permutation would not return an element in the other conjugacy class). Hence any element in $\mathcal{K}$ does not commute with any odd permutation, and by the previous result, $\mathcal{K}$ consists of elements whose cycle type is distinct odd integers.

Hence $\mathcal{K}$ consists of two conjugacy classes in A_n if and only if the cycle type of an element of $\mathcal{K}$ consists of distinct odd integers. □

2. (DF4.3.30) If G is a group of odd order, prove for any non-identity element $x \in G$ that x and x^{-1} are not conjugate in G.

Proof. Let G be a group of odd order as given and let $x \in G$ be a non-identity element. Then suppose by way of contradiction that x is conjugate to x^{-1}; that is, there exists $g \in G$ such that $x = gx^{-1}g^{-1}$. We have that $xg = gx^{-1}$.

Then take powers of xg so that for $k \geq 0$

$$\begin{aligned}(xg)^{2k} = (gx^{-1})^{2k} &= \overbrace{(gx^{-1}gx^{-1})(gx^{-1}gx^{-1})\cdots(gx^{-1}gx^{-1})}^{k \text{ times}} \\ &= \overbrace{(gx^{-1}xg)(gx^{-1}xg)\cdots(gx^{-1}xg)}^{k \text{ times}} \\ &= \overbrace{(g^2)(g^2)\cdots(g^2)}^{k \text{ times}} \\ &= g^{2k},\end{aligned}$$

so that $(xg)^{2k+1} = xg(xg)^{2k} = xg(g^{2k}) = xg^{2k+1}$. It follows by induction on n that

$$(xg)^n = \begin{cases} g^n & \text{if } n \text{ is even,} \\ xg^n & \text{if } n \text{ is odd.}\end{cases}$$

(This holds for $n = 0, 1$; take out one power of xg for odd powers of xg and apply the inductive hypothesis to verify the equality for odd powers of xg. For even powers simply strip away two powers of xg and again apply the inductive hypothesis and use the equality $xg = gx^{-1}$ in the same manner as above to verify the equality for even powers of xg.)

Then let $|g| = m$, and note that because $|G|$ is odd, it follows that m is odd as well (since $m = |\langle g \rangle|$ divides $|G|$). Then $(xg)^m = xg^m = x$, so that $xg(xg)^{m-1} = x \iff (xg)^{m-1} = g^{-1} = g^{m-1}$. Then

$$x = (xg)^m = (xg)^{m-1}xg = g^{-1}xg,$$

so that $gx = xg$, and because $xg = gx^{-1}$, we have $gx = gx^{-1}$, which implies $x = x^{-1}$, meaning $x^2 = 1$. But $x \in G$, meaning that $|x|$ must be odd (since $|x| = |\langle x \rangle|$ divides $|G|$). This forces $x = 1$, which is in contradiction to the assumption that x was a non-identity element, so the assumption that x was conjugate to x^{-1} cannot hold.

Hence for any non-identity element $x \in G$, we have that x and x^{-1} are not conjugate in G. □

3. (DF4.3.34) Prove that if p is a prime and P is a subgroup of S_p of order p, then $\left|N_{S_p}(P)\right| = p(p-1)$.

Proof. Let $P \leq S_p$ be of order p, so that P is a cyclic group of order p. This means that $P = \langle \sigma \rangle = \left\{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\right\}$, where σ is some p-cycle in S_p.

For some permutation $\tau \in S_p$, observe that because conjugation preserves the order of elements, $\tau P \tau^{-1} = \langle \tau\sigma\tau^{-1} \rangle = \left\{1, \tau\sigma\tau^{-1}, \ldots, (\tau\sigma\tau^{-1})^{p-1}\right\}$. It follows from our very useful formula that each of the non-identity elements in $\tau\sigma\tau^{-1}$ are each p-cycles, since if $\sigma = (a_1\, a_2\, \cdots\, a_p)$, then $\tau\sigma\tau^{-1} = (\tau(a_1)\, \tau(a_2)\, \cdots\, \tau(a_p))$. There

are $p-1$ non-identity elements (p-cycles) in P, so there are $p-1$ non-identity elements (p-cycles) in $\tau P \tau^{-1}$ for any $\tau \in S_p$. Hence every conjugate of P contains $p-1$ p-cycles.

The number of p-cycles in S_p is given by

$$\frac{p \cdot (p-1) \cdots (p-p+1)}{p} = \frac{p!}{p} = (p-1)!\,,$$

which we can interpret as the number of ways to permute p elements where we divide out the number of ways to cycle them in p slots (as any cyclic permutation of a cycle is the same cycle).

With $P = \langle \sigma \rangle$, if $\sigma \neq \tau \sigma \tau^{-1}$ for $\tau \in S_p$, it follows that $\sigma^k \neq (\tau \sigma \tau^{-1})^k$ for $1 \leq k \leq p-1$ (when $k = p$ both become the identity). Hence P and $\tau P \tau^{-1}$ intersect trivially. So if there are n distinct conjugates of P in S_p, in total there are $n \cdot (p-1)$ p-cycles in S_p. Using the previous computation, it follows that there are $n = (p-2)!$ conjugates of P in S_p.

This number is the index of the stabilizer of P in S_n, under the action of conjugation by S_p. But the stabilizer of P under conjugation is precisely the normalizer of P in S_p, so we have that

$$(p-2)! = \frac{|S_p|}{\left|N_{S_p}(P)\right|} = \frac{p!}{\left|N_{S_p}(P)\right|},$$

which implies that $\left|N_{S_p}(P)\right| = p(p-1)$. □

4. (DF4.4.18) This exercise shows that for $n \neq 6$ every automorphism of S_n is inner. Fix an integer $n \geq 2$ with $n \neq 6$.

   (a) Prove that the automorphism group of a group G permutes the conjugacy classes of G, i.e., for each $\sigma \in \mathrm{Aut}(G)$ and each conjugacy class $\mathcal{K}$ of G the set $\sigma(\mathcal{K})$ is also a conjugacy class of G.

   Proof. Let G be a group. Let $\mathcal{K}$ be any conjugacy class of G, and let x be a representative for $\mathcal{K}$. Then every element $y \in \mathcal{K}$ is equal to gxg^{-1} for some $g \in G$. Then for $\sigma \in \mathrm{Aut}(G)$, let $\sigma(g) = g'$. We have that $\sigma(y) = \sigma(gxg^{-1}) = \sigma(g)\sigma(x)\sigma(g^{-1}) = g'\sigma(x)(g')^{-1}$, which is an element of $\sigma(\mathcal{K})$.
   The conjugacy class of $\sigma(x)$ is the set containing all of the conjugates of $\sigma(x)$ in G. So any element of the conjugacy class of $\sigma(x)$ takes on the form $g'\sigma(x)(g')^{-1}$ for any $g' \in G$, and because σ is an automorphism of G, g' has the preimage $g \in G$ under σ. Then $g'\sigma(x)(g')^{-1} = \sigma(g)\sigma(x)\sigma(g)^{-1} = \sigma(gxg^{-1})$. But $gxg^{-1} \in \mathcal{K}$, and as g' takes on all of the elements of G so will g. Hence every element in the conjugacy class of $\sigma(x)$ is actually an element of $\sigma(\mathcal{K})$; furthermore every element in $\sigma(\mathcal{K})$ is conjugate to each other, since every element in $\mathcal{K}$ is conjugate to each other. We can always find an element of G which conjugates the preimage of $y \in \sigma(\mathcal{K})$ under σ into the preimage of $z \in \sigma(\mathcal{K})$ under σ.
   Hence $\sigma(\mathcal{K})$ is a conjugacy class (we may think of it as the conjugacy class of $\sigma(x)$). □

   (b) Let $\mathcal{K}$ be the conjugacy class of transpositions in S_n and let $\mathcal{K}'$ be the conjugacy class of any element of order 2 in S_n that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$. Deduce that any automorphism of S_n sends transpositions to transpositions.

Proof. Any element of order 2 in S_n which is not a transposition has cycle type $1, 1, \ldots, 1, \underbrace{2, \ldots, 2}_{k \text{ times}}$ where $k > 1$ but k is not so large that $n - 2k$ becomes negative ($k \leq \lfloor n/2 \rfloor$). Transpositions have cycle type $1, 1, \ldots, 1, 2$. Then by using the formula found in Exercise 33 of Section 4.3, we have that the size of the conjugacy class of permutations of order 2 which are not transpositions is

$$|\mathcal{K}'| = \frac{n!}{(n-2k)!k!2^k}$$

while the size of the conjugacy class of a transposition is

$$|\mathcal{K}| = \frac{n!}{(n-2)! \cdot 2}.$$

The two equations are equal if and only if $(n-2k)!k!2^k = (n-2)! \cdot 2$. We show that this equation does not hold for $2 \leq n \neq 6$.

For $n = 2, 3$ there are no elements of order 2 which are not transpositions, for $n = 4, 5$ the equation does not hold for the one choice of k which is available: $k = 2$. What remains is to prove (by induction) that the equation does not hold for $n > 6$; in particular we can show that $(n-2k)!k!2^k < (n-2)! \cdot 2$ for $n > 6$. For $n = 7, 8$ the inequality holds (manually checked for the appropriate ranges of k), and assume the inequality holds for $n = j$ with $1 < k \leq \lfloor n/2 \rfloor$. What remains is to show that for $n = j + 2$ the inequality holds (as we have base cases $n = 7, 8$).

Then for $n = j + 2$ and $1 < k \leq \lfloor j/2 \rfloor$,

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

where in the last equality we used the fact that $k > 1$ to see that $j(j-1) > (j-2k+2)(j-2k+1)$. Then for $k = \lfloor (j+2)/2 \rfloor$, we can try in both cases when j is either odd ($k = (j+1)/2$) or even ($k = (j+2)/2$) to see that the inequality still holds, as $j! \cdot 2 > ((j+1)/2)!2^{(j+1)/2}$ and $j! \cdot 2 > (j/2+1)!2^{j/2+1}$.

Thus for $2 \leq n \neq 6$, $|\mathcal{K}| \neq |\mathcal{K}'|$.

By (a) any automorphism of S_n must induce a mapping from $\mathcal{K}$ onto a conjugacy class whose elements have order 2, but because $|\mathcal{K}| \neq |\mathcal{K}'|$ for $2 \leq n \neq 6$ we have that any automorphism of S_n sends $\mathcal{K}$ to itself; that is, it sends transpositions to transpositions. □

(c) Prove that for each $\sigma \in \mathrm{Aut}(S_n)$

$$\sigma\colon (1\,2) \mapsto (a\,b_2), \quad \sigma\colon (1\,3) \mapsto (a\,b_3), \quad \ldots, \quad \sigma\colon (1\,n) \mapsto (a\,b_n)$$

for some distinct integers $a, b_2, b_3, \ldots, b_n \in \{1, 2, \ldots, n\}$.

Proof. Let $\sigma \in \mathrm{Aut}(S_n)$. Then using the fact that σ sends transpositions to transpositions, suppose that for $k \neq j \neq m$ we have

$$\sigma((m\,k)) = (a\,b_k) \quad \text{and} \quad \sigma((m\,j)) = (x\,b_j).$$

Then consider $\sigma((m\,k)(m\,j)) = \sigma((m\,j\,k)) = (a\,b_k)(x\,b_j)$. If $a = x$ and $b_k = b_j$, it follows that the cycle of order 3 was sent to the identity, which cannot happen since σ preserves the order of the elements it maps. Similarly, if $a \neq x$ and $b_k \neq b_j$, then the cycle of order 3 was sent to the product of two disjoint transpositions, which has order 2. This also cannot happen, so the only case that remains is when $a = x$ and $b_k \neq b_j$ (without loss of generality just one of the corresponding elements has to be equal and the other pair must not be equal, we may cyclically permute the locations of the items in each transposition to match our notation).

We can prove by induction that if two transpositions in S_n move one element in common and under σ the resulting transpositions also move one element in common, then all of the transpositions which move one element in S_n are mapped to transpositions which move exactly one element in common (as in the sequence in the problem statement). Without loss of generality we may take $m = 1$ and if we view the above computation with $k = 1$ and $j = 2$ we have a base case for the inductive argument.

Then suppose that $(1\,2) \mapsto (a\,b_2), (1\,3) \mapsto (a\,b_3), \ldots,$ and $(1\,k) \mapsto (a\,b_k)$ under σ, and suppose that $(1\,(k+1)) \to (x, b_{k+1})$. We have that $\sigma((1\,2)(1\,3)\cdots(1\,k)) = (a\,b_k\,\cdots\,b_2)$, a k-cycle (order k). Then $\sigma((1\,2)(1\,3)\cdots(1\,k)(1\,(k+1))) = (a\,b_k\,\cdots\,b_2)(x, b_{k+1})$; again suppose that $x \neq a$ and $b_{k+1} \neq b_i$ for every $2 \leq i \leq k$ to find that what should have order $k+1$ has instead order $\operatorname{lcm}(k, 2)$ which is either $2k$ or k depending on if k is even or odd. Instead if $x = a$ and $b_{k+1} = b_i$ for some $2 \leq i \leq k$, then the resulting cycle should have order $k+1$, but instead has order $k-1$.

So without loss of generality we have $x = a$ and $b_{k+1} \neq b_i$ for $2 \leq i \leq k$. Hence by induction the sequence of mappings

$$\sigma\colon (1\,2) \mapsto (a\,b_2), \quad \sigma\colon (1\,3) \mapsto (a\,b_3), \quad \ldots, \quad \sigma\colon (1\,n) \mapsto (a\,b_n)$$

for any $\sigma \in \operatorname{Aut}(S_n)$ can be formed for some distinct integers $a, b_2, b_3, \ldots, b_n \in \{1, 2, \ldots, n\}$. □

(d) Show that $(1\,2)$, $(1\,3)$, …, $(1\,n)$ generate S_n and deduce that any automorphism of S_n is uniquely determined by its action on these elements. Use (c) to show that S_n has at most $n!$ automorphisms and conclude that $\operatorname{Aut}(S_n) = \operatorname{Inn}(S_n)$ for $n \neq 6$.

Proof. We may form any transposition $(k\,j) \in S_n$ as the product $(1\,k)(1\,j)(1\,k)^{-1} = (1\,k)(1\,j)(1\,k)$, and any cycle decomposition of a permutation (and hence any permutation) can be formed out of the product of transpositions of this form as a result. Hence $\{(1\,i) \mid 2 \leq i \leq n\}$ generate S_n

We may form any transposition $(b_k\,b_j) \in \sigma(S_n)$ by taking the product $(a\,b_k)(a\,b_j)(a\,b_k)^{-1} = (a\,b_k)(a\,b_j)(a\,b_k)$. Both $(a\,b_k)$ and $(a\,b_j)$ have preimages under σ, so that

$$(b_k\,b_j) = (a\,b_k)(a\,b_j)(a\,b_k) = \sigma((1\,k)(1\,j)(1\,k)) = \sigma((k\,j)).$$

In a similar manner any transposition of $\sigma(S_n)$ may be formed, and as a result any permutation of $\sigma(S_n)$ may be formed. Each permutation in $\sigma(S_n)$ has a preimage in S_n under σ which can be written as the product of finitely many transpositions of the form $(1\,i)$ for $2 \leq i \leq n$. Hence the action of σ on S_n is entirely determined by the action of σ on $\{(1\,i) \mid 2 \leq i \leq n\}$.

In (c), observe that there are n choices for a, $n-1$ choices for b_2, and so on until there is only one choice left for b_n. Hence there are at most $n!$ different ways that the action of σ on $\{(1\,i) \mid 2 \leq i \leq n\}$ could go, so $|\mathrm{Aut}(S_n)| \leq n!$.

But $\mathrm{Inn}(S_n) \leq \mathrm{Aut}(S_n)$ (so $|\mathrm{Inn}(S_n)| \leq |\mathrm{Aut}(S_n)| \leq n!$), with $\mathrm{Inn}(S_n) \cong S_n/Z(S_n)$, and because the center of the symmetric group is trivial, we have $|\mathrm{Inn}(g)| = |S_n|/|Z(S_n)| = n!/1 = n!$. Hence $|\mathrm{Aut}(S_n)| = n!$, so that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ whenever $n \neq 6$ □