Sec 4.4, Ex 18  (a) Suppose $K$ is the conjugacy class of some element $h \in G$. Then

$$\sigma(K) = \{\sigma(k) : k \in K\}$$

$$= \{\sigma(ghg^{-1}) : g \in G\}$$

$$= \{g'\sigma(h)(g')^{-1} : g' \in G\}$$

since $G$ is an automorphism

is the conjugacy class of $\sigma(h)$. Therefore, a group automorphism takes a conjugacy class to another conjugacy class.

(b) Let $x$ be an element in $K'$. Since $x$ has order 2 but is not a transposition, it is a product of at least two disjoint 2-cycles. Say $x$ is a product of $k$ disjoint 2-cycles. Then, by Exercise 33 in Section 3,

$$|K'| = \frac{n!}{k!2^k}$$

where $k \geq 2$. Since $|K|$ is the number is 2-cycles in $S_n$, i.e. \( \binom{n}{2} = \frac{n(n-1)}{2} \), if $|K| = |K'|$ then

$$\frac{n!}{k!2^k} = \frac{n(n-1)}{2},$$

i.e. $(n-2)! = k!2^{k-1}$, which only holds when $n = 6$ and $k = 3$. However, we are assuming $n \neq 6$, so $|K| \neq |K'|$.

Any automorphism $\sigma$ of $S_n$ takes an element $p$ of order 2 to an element of order 2. By part (a), the conjugacy classes of $p$ and $\sigma(p)$ have the same order. By the previous paragraph, if $p$ is a transposition, then $\sigma(p)$ must also be a transposition. Therefore, an automorphism of $S_n$ takes transpositions to transpositions.

(c) By part (b), $\sigma(12)$ and $\sigma(13)$ are both transpositions; say

$$\sigma(12) = (ab) \quad \text{and} \quad \sigma(13) = (cd).$$

Note that $(13)(12)(13)^{-1} = (23) \neq (12)$. Hence $\sigma(13) \cdot \sigma(12)(\sigma(13))^{-1} \neq \sigma(12)$, i.e. $\sigma(12)$ and $\sigma(13)$ are not disjoint. On the other hand, $\sigma(12)$ and $\sigma(13)$ cannot be the same transposition, since $\sigma$ is injective. Let $a$ be the symbol that is common to both $\sigma(12)$ and $\sigma(13)$. Then $\sigma(12) = (a \ b_2)$ and $\sigma(13) = (a \ b_3)$ for some distinct integers $1 \leq a, b_2, b_3 \leq n$. The same argument applied to other transpositions of the form $1 \ n$ show that $\sigma(1 \ n) = (a \ b_n)$ for distinct integers $1 \leq a, b_2, \cdots, b_n \leq n$.

(d) Take any transposition $(c \ d)$ in $S_n$. Then $(c \ d) = (1 \ d)(1 \ c)(1 \ d)$. Hence any transposition is a product of transpositions of the form $(1 \ k)$, and so $(1 \ 2), \cdots, (1 \ n)$ generate $S_n$. Since $S_n$ itself is in turn generated by transpositions, any automorphism of $S_n$ is determined by its action on the elements $(1 \ 2), \cdots, (1 \ n)$.

By part (c), there are $n!$ possibilities for an automorphism of $S_n$ that takes $(1 \ 2), \cdots, (1 \ n)$ to transpositions. Hence $|\text{Aut}(S_n)| \leq n!$. On the other hand, distinct elements of $S_n$ induce distinct inner automorphisms of $S_n$. Therefore, $n! = |S_n| \leq |\text{Inn}(S_n)| \leq |\text{Aut}(S_n)| \leq n!$, so we must have equality throughout. Hence $\text{Inn}(S_n)$ and $\text{Aut}(S_n)$ have the same order, and so are in fact the same group.
Sec 4.4, Ex 19 From part (b) of Exercise 18, we know:

- when $n = 6$, $|K| = |K'|$;
- if $x$ is an element of $K'$, then $x$ is a product of three disjoint 2-cycles.

Let $H$ be the subgroup of $\text{Aut}(S_6)$ consisting of automorphisms that takes transpositions to transpositions. Note that $H$ is nonempty, since it contains the identity element.

Take any $\sigma \in \text{Aut}(S_6) \setminus H$. Then $\sigma$ takes some transposition $(a \, b)$ to a product of three disjoint 2-cycles, say $\sigma(a \, b) = (c \, d)(e \, f)(g \, h)$. Because $(c \, d), (e \, f), (g \, h)$ commute, the permutations $\sigma(c \, d), \sigma(e \, f), \sigma(g \, h)$ also commute. This means that, if one of the three permutations $\sigma(c \, d), \sigma(e \, f), \sigma(g \, h)$ is not a 2-cycle, then both of the other two must be 2-cycles, and they must be among $[(p \, q), (r \, s), (u \, v)]$. But this means that $\sigma^2(a \, b) = \sigma(c \, d)\sigma(e \, f)\sigma(g \, h)$ is a 2-cycle. We have shown that, given any automorphism $\sigma$ of $S_6$, the automorphism $\sigma^2$ takes transpositions to transpositions. That is, $\sigma^2 \in H$. This means $H$ has index at most 2 in $\text{Aut}(S_6)$.

(b) It suffices to show that $H \subseteq \text{Inn}(S_6)$. Take any $\sigma \in H$. Since $\sigma$ takes transpositions to transpositions, the argument in part (c) of Exercise 18 shows that

$$\sigma(1 \, 2) = (a \, b_2), \ldots, \sigma(1 \, n) = (a \, b_n)$$

for distinct integers $1 \leq a, b_2, \ldots, b_n \leq n$. However, if we let $\tau$ be the permutation

$$1 \mapsto a, i \mapsto b_i \text{ for } 2 \leq i \leq n,$$

then $\tau(1 \, i)\tau^{-1} = (a \, b_i)$ for $2 \leq i \leq n$. That is, $\sigma$ is the inner automorphism induced by conjugation by $\tau$. Hence $H \subset \text{Inn}(S_6)$, and we can conclude $|\text{Aut}(S_6) : \text{Inn}(S_6)| \leq |\text{Aut}(S_6) : H| \leq 2$.

Sec 4.5, Ex 16 Suppose $G$ has no normal Sylow subgroups for any of the primes $p, q, r$. By Corollary 20, this means $n_p, n_q, n_r$ are all $> 1$. By Sylow’s theorem, we have

$$n_p = 1 + k_p p$$
$$n_q = 1 + k_q q$$
$$n_r = 1 + k_r r$$

for some nonnegative integers $k_p, k_q, k_r$. Because $n_r > 1$, $k_r$ must be $> 0$, and so $n_r \geq 1 + r > p, q$. Since $n_r | pq$ by part (3) of Sylow’s theorem, we have

$$n_r = pq.$$

Similarly, since $n_q > 1$, we have $k_q > 0$, and so $n_q \geq 1 + q > p$; since $n_q | pr$, we conclude

$$n_q = r \text{ or } pr.$$

And also, since $n_p > 1$ and $n_p | qr$, we have

$$n_p \geq q.$$
Now, observe that if $s$ is a prime and Sylow $s$-subgroups of $G$ have prime order $s$, then the intersection of any two distinct Sylow subgroups is exactly $\{1_G\}$. This is because all Sylow $s$-subgroups are cyclic of prime order, so if the intersection of two of them is non-trivial, then the intersection would contain at least $s$ elements, i.e. these two Sylow $s$-subgroups would be the same.

The above observation says that there are $n_r(r-1)$ distinct non-identity elements that lie in Sylow $r$-subgroups, $n_q(q-1)$ distinct non-identity elements that lie in Sylow $q$-subgroups, and $n_p(p-1)$ distinct non-identity elements that lie in Sylow $p$-subgroups.

Using the inequalities we obtained above, we get

$$|G| \geq n_r(r-1) + n_q(q-1) + n_p(p-1)$$

$$\geq pq(r-1) + r(q-1) + q(p-1)$$

$$= pqr + rq - r - q + 1$$

$$= pqr + (r-1)(q-1)$$

$$> pqr \text{ since } r, q > p > 1$$

$$= |G|,$$

giving us a contradiction. Hence one of $n_r, n_q, n_p$ must be equal to one, i.e. $G$ has a normal Sylow subgroups for one of $p, q, r$.

**Sec 4.5, Ex 30** Let $G$ be a simple group of order 168. Note that $168 = 2^3 \cdot 3 \cdot 7$, so any 7-subgroup of $G$ has order exactly 7. By the observation we made in the solution to Exercise 16, we know that in order to count the number of elements of order 7 in $G$, it suffices to find $n_7$, the number of Sylow 7-subgroups of $G$. By Sylow’s theorem, $n_7 = 1 + 7k$ for some integer $k \geq 0$, and also $n_7|2^3 \cdot 3 = 24$. These two conditions imply $n_7 = 1$ or 8, corresponding to $k = 0$ and $k = 1$, respectively. However, that $G$ is simple means it does not have any non-trivial normal subgroup; so $n_7 > 1$ by Corollary 20, and so $n_7 = 8$. Hence the number of elements of order 7 in $G$ is $n_7(7-1) = 8 \cdot 6 = 48$. 