1. In this problem, you prove that $\text{Aut}(S_n) = \text{Inn}(S_n)$ if $n \geq 7$.
   (All the automorphisms of $S_n$ are inner.) Suppose $\varphi \in \text{Aut}(S_n)$.

(a) Suppose $n \geq 5$, and $\varphi$ sends transpositions to transpositions; that means $|\text{supp}(\varphi(a \ b))| = 2$ for any $1 \leq a < b \leq n$. Prove that $\varphi$ is an inner automorphism.

**Hint:** Suppose $T_1$ and $T_2$ are two transpositions. Observe:

- $T_1$ and $T_2$ do not commute if and only if $|\text{supp}(T_1) \cap \text{supp}(T_2)| = 1$.
- Any transposition gives us an edge in the complete graph with $n$ vertices; by assumption $\varphi$ induces a bijection on the edges of the complete graph. ① implies two edges with a common vertex are mapped to two edges with a common vertex. Use this to get a permutation on vertices.

(b) Show that for any transposition $T$, $\varphi(T) \varphi^{-1} = T$.

(c) Prove that $\varphi(\sigma_1)$ and $\varphi(\sigma_2)$ are conjugate if and only if $\sigma_1$ and $\sigma_2$ are conjugate.

Let $T_k$ be the set of permutations with cycle type $\frac{2, \ldots, 2}{k}$, $\frac{1}{n-2k}$ for instance $T_1$ consists of transpositions. Show that
\[ |T_k| = n(n-1) \cdots (n-2k+1)/k! \cdot 2^k \geq \frac{n(n-1) \cdots (n-2k+1)}{2} \frac{(2k-2)!}{k! \cdot 2^{k-1}}. \]

1. Prove that \( \varphi(T_i) = T_k \) for some \( 1 \leq k \leq n/2 \). (Use part 1.)

2. Prove that \( \varphi(T_i) = T_i \) and deduce that \( \varphi \in \text{Inn}(S_n) \).

3. In this problem, you prove that \( \text{Aut}(S_6) \neq \text{Inn}(S_6) \).

(In this problem you can use the fact that \( A_n \) is simple if \( n \geq 5 \))

(a) Show that \( S_5 \) has 6 Sylow 5-subgroups. Deduce that \( S_6 \) has a subgroup \( H \) which is isomorphic to \( S_5 \) and acts transitively on \( \{1, 2, \ldots, 6\} \). And so \( \text{Fix}(\sigma \cdot H \cdot \sigma^{-1}) = \emptyset \) for any \( \sigma \in S_6 \).

(b) Consider \( S_6 \acts S_6/H \) by the left translations. Since \( |H| = |S_5| \), we have \( |S_6/H| = 6 \). So the above action gives us a group homomorphism \( \varphi : S_6 \rightarrow S_6 \). Prove that \( \varphi \) is an isomorphism.

(c) Show that \( \text{Fix}(\varphi(H)) \neq \emptyset \), and deduce \( \varphi \) is NOT an inner automorphism of \( S_6 \).
One of the important result in finite group theory is the following result of Burnside:

**Burnside’s normal $p$-complement theorem.**

Suppose $G$ is a finite group, $1 \neq P$ is a Sylow $p$-subgroup, and $P \subseteq Z(N_G(P))$. Then $\exists \ N \triangleleft G$ st. $|N| = |G/P|$. This is an extremely useful theorem; for instance try to use this to give a short of a result we have proved earlier:

a group $G$ of order $p^{e+1}$ has a normal subgroup of order $p$ or $p+1$. (This is not part of the problem). In this problem you will see the powerful combination of this theorem with the Schur-Zassenhaus theorem:

3. Suppose $\gcd(n, \varphi(n)) = 1$, and $G$ is a group of order $n$. Prove that a group of order $n$ is cyclic.

(Hint: Arithmetic observations: $\gcd(n, \varphi(n)) = 1 \Rightarrow n$ is square-free

$\gcd(n, \varphi(n)) = 1 \Rightarrow \gcd(m, \varphi(m)) = \gcd(m, \varphi(m) + \varphi(m)) = \gcd(n, \varphi(n)) = 1$. Use strong induction on $n$; and the mentioned theorems.)
4. Suppose \( G \) is a finite group and for any \( d \in \mathbb{Z}^+ \),
\[
|\{g \in G \mid g^d = e_G \}| \leq d.
\]
Prove that \( G \) is cyclic.

(Hint: Let \( X_d := \{g \in G \mid o(g) = d \} \) and \( \Psi(d) := |X_d| \).

**Step 1.** Show, if \( \Psi(d) \neq 0 \), then \( \Psi(d) = \phi(d) \).

**Step 2.** Notice \( \sum_{d \mid n} \Psi(d) = n \) where \( n = |G| \).

**Step 3.** From arithmetic we know \( \sum_{d \mid n} \phi(d) = n \). (You are allowed to use this without proof.) Use steps 1 and 2 to show \( d \mid n \Rightarrow \Psi(d) = \phi(d) \); and finish proof.

5. For a group \( G \), let \([G,G]\) be the subgroup generated by
\[
[g_1, g_2] := g_1^{-1} g_2^{-1} g_1 g_2 \quad \text{for} \quad g_1, g_2 \in G.
\]

(a) Show that \([G,G]\) is a characteristic subgroup of \( G \).

(b) For \( N \trianglelefteq G \), prove that \( G/N \) is abelian if and only if \([G,G] \subseteq N \).

(c) Prove that \([S_n,S_n] = A_n\) if \( n \geq 3 \).
6. Prove that there is no finite group $G$ such that

\[ [G,G] \cong S_4. \]

(Hint. Suppose to the contrary that there is such a group $G$. Convince yourself that $P := \langle I, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \rangle$ is the unique Sylow 2-subgp of $A_4$; and so $P$ is a characteristic subgroup of $A_4$.

- $G$ acts by conjugation on $[G,G] \cong S_4$; argue why this induces an action on $A_4/P \cong \mathbb{Z}/3\mathbb{Z}$;

- Argue why $[G,G]$ should act trivially on $A_4/P$; and deduce $S_4 \cap A_4/P$ by conjugation should be the trivial action.

- Check that $(1\ 2\ 3)^{(1\ 2)} \neq (1\ 2\ 3)^P$, and get a contradiction.)

7. (a) Prove that $\langle (1\ 2), (1\ 2\ \ldots\ n) \rangle = S_n$.

(b) Suppose $p$ is an odd prime, $\tau \in S_p$ is a transposition and $\sigma \in S_p$ has order $p$. Prove that $\langle \tau, \sigma \rangle = S_p$. 
(Hint. (a) Let $H = \langle (1, 2), (1, 2 \ldots n) \rangle$. Notice $(1, 2)(2, 3 \ldots n) = (1, 2 \ldots n)$ and so $(2, 3 \ldots n) \in H \Rightarrow (1, 2) (2, 3 \ldots n) = (1, 2 \ldots n) \in H$. 

(b) After reordering, we can assume $\sigma = (1, 2 \ldots p)$. Let $H = \langle (a, b), (1, 2 \ldots p) \rangle$; argue why we can further assume $H = \langle (b, a), (1, 2 \ldots p) \rangle$ after another reordering if needed; using $\sigma^{-1}$ and part (a) finish the proof.)