1 Homework 5.

1. Suppose n is a positive integer. Prove that every group of order n is cyclic if and only if $\gcd(n, \phi(n)) = 1$.

   (**Hint.** One of the fundamental results in finite group theory is the following result of Burnside.

   Theorem 1 (Burnside's normal p-complement)**.** *Suppose G is a finite group, P is a Sylow p-subgroup, and $P \subseteq Z(N_G(P))$. Then there exists a normal subgroup N of G such that $|N| = |G/P|$.*

   In this problem, you are allowed to use this theorem without proof. Use strong induction on n to show that every group of order n is cyclic if $\gcd(n, \phi(n)) = 1$. Observe that $\gcd(n, \phi(n)) = 1$ implies that n is square-free. Notice that if $m|n$, then $\gcd(m, \phi(m)) = 1$. By the strong induction hypothesis, deduce that every proper subgroup of G is cyclic. Deduce that if a Sylow p-subgroup is not normal, then $N_G(P)$ is cyclic. Use Burnside's normal complement.)

2. In this problem, you prove that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ if $n \geq 7$.

   (a) Suppose ϕ is an automorphism of S_n which sends transpositions to transpositions; that means $\phi(a\, b)$ is a 2-cycle for every $1 \leq 1 < b \leq n$. Prove that ϕ is an inner automorphism. (For this part it is enough to assume that $n \geq 5$.)

   (b) Suppose ϕ is an automorphism. Prove that for all $\sigma_1, \sigma_2 \in S_n$, $\phi(\sigma_1)$ and $\phi(\sigma_2)$ are conjugate if and only if σ_1 and σ_2 are conjugate. (This is true for an automorphism of an arbitrary group.)

   (c) Let T_k be the set of permutations with cycle type

   $$(\underbrace{2, \ldots, 2}_{k}, \underbrace{1, \ldots, 1}_{n-2k}).$$

   For instance T_1 is the set of 2-cycles. Prove that

   $$|T_k| = \frac{n(n-1)\cdots(n-2k+1)}{k!2^k} \geq \frac{n(n-1)}{2} \cdot \frac{(2k-2)!}{k!2^{k-1}},$$

   for a positive integer $k \leq n/2$.

(d) Prove that for every $\phi \in \mathrm{Aut}(S_n)$, there exists an integer k such that $\phi(T_1) = T_k$.

(e) Prove that for every $\phi \in \mathrm{Aut}(S_n)$, $\phi(T_1) = T_1$. Deduce that

$$\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n).$$

(**Hint.** Consider the complete graph with n vertices. Notice that there exists a bijection between 2-cycles and edges of this graph. If an automorphism ϕ sends 2-cycles to 2-cycles, then it induces a bijection on the edges of this graph. Observe that two 2-cycles τ_1 and τ_2 do not commute if and only if the corresponding edges of τ_1 and τ_2 have a vertex in common. Use this property to show the induced map on the edges gives us an automorphism of the graph and so a permutation σ on the set of vertices. Prove that ϕ is conjugation by σ.)

3. For every group G, the group of outer automorphisms is

$$\mathrm{Out}(G) := \frac{\mathrm{Aut}(G)}{\mathrm{Inn}(G)}.$$

Let $\mathrm{Cl}(G)$ be the set of conjugacy classes of G.

(a) Prove that

$$(\theta\,\mathrm{Inn}(G)) \cdot [a] := [\theta(a)]$$

is a well-defined action of $\mathrm{Out}(G)$ on $\mathrm{Cl}(G)$, where $[g]$ is the conjugacy class of g in G.

(b) Argue why $f : \mathrm{Cl}(G) \to \mathbb{Z} \times \mathbb{Z}, f([g]) := (o(g), |[g]|)$ is fixed along an $\mathrm{Out}(G)$-orbit.

(c) Prove that $\mathrm{Aut}(S_n) \simeq \mathrm{Inn}(S_n)$ if $n \neq 6$.

(d) Prove that $\mathrm{Aut}(S_n) \simeq S_n$ if $n \neq 2, 6$.

(**Hint.** Use an argument similar to part (a) of problem 2.)

4. Suppose n is an integer at least 2.

(a) Prove that $S_n = \langle (1\,2), (1\,2\,\cdots\,n) \rangle$ (this means the smallest subgroup of S_n which contains $(1\,2)$ and $(1\,\cdots\,n)$ is S_n).

(b) Suppose p is prime, $\tau \in S_p$ is a 2-cycle and $\sigma \in S_p$ is an element of order p. Prove that $S_p = \langle \tau, \sigma \rangle$.

(**Hint.** Let $\gamma := (1\,2)(1 \cdots n) = (2 \cdots n)$. Consider $\gamma^i (1\,2) \gamma^{-i}$, and use this to show all 2-cycles are in the group generated by these elements.

For the second part, it is better to use think about permutations of

$$\mathbb{Z}/p\mathbb{Z} = \{0, \dots, p-1\}.$$

Notice that an element of order p is a p-cycle. After relabelling we can and will assume that

$$\sigma : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \quad \sigma(x) := x + 1.$$

Argue why after another relabelling we can and will assume that $\tau = (0\ a)$ for some $a \neq 0$. Consider $\sigma^i \tau \sigma^{-i} = (i\ a+i)$. Use this to obtain that $(ka\ (k+1)a)$ is in this group for every $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. Inductively, show that $(0\ ka)$ is in this group for every $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. Deduce that $(0\,1)$ is in this group. Use the first part.)

5. (15-puzzle) In a 15-puzzle, a player can rearrange the numbers 1 to 15 by sliding the numbers to the empty spot. Starting with the position

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

can we get to the following position?

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

(**Hint.** Think about every position in the 15-puzzle as a permutation in S_{16}. Every sliding is a 2-cycle. Argue why we need even number of sliding moves to go from the initial position to the second given position.)

6. Suppose G is a finite group of order $2^k m$ where k is a positive integer and m is an odd number. Suppose G has a cyclic Sylow 2-subgroup. Prove that G has a characteristic subgroup of order m.

   (You are not allowed to use Burnside's p-complement theorem for this problem.)

   (**Hint.** Suppose $\phi : G \to S_G$ is the embedding given by the action of G on itself by left-translations. Prove that $\epsilon \circ \phi : G \to \{\pm 1\}$ is not trivial. Show that $\ker \epsilon \circ \phi$ is a characteristic subgroup of index 2. By induction prove that for every integer $1 \leq i \leq k$, G has a characteristic subgroup of index 2^i.)