Problem 1:

Let G be a group, and let $a, b \in G$ with $|a| = m$, $|b| = n$.

Part a:

First, if $m \mid k$, then $m = lk$ for some $l \in \mathbb{Z}$. So $a^k = a^{lm} = (a^m)^l = e^l = e$.

Next, if $m \nmid k$, then $k = lm + j$ for some $l \in \mathbb{Z}$, $j \in \mathbb{N}$ with $0 < j < m$. So $a^k = a^{lm+j} = a^{lm}a^j = a^j \neq e$. ($a^j \neq e$ for any j between 0 and m (exclusive), because otherwise the order of a would be less than m, which is against our assumptions.)

So $m \mid k$ if and only if $a^k = e$.

Part b:

Let $ab = ba$, and $\langle a \rangle \cap \langle b \rangle = \{e\}$.

First, $|ab| \leq \mathrm{lcm}(m, n)$:

Then $(ab)^{\mathrm{lcm}(m,n)} = a^{\mathrm{lcm}(m,n)} b^{\mathrm{lcm}(m,n)} = ee = e$.

So $\mathrm{lcm}(m, n)$ is a positive number with the property $(ab)^{\mathrm{lcm}(m,n)} = e$; $\mathrm{lcm}(m, n)$ is greater than or equal to the order of ab. (So $|ab| \leq \mathrm{lcm}(m, n)$).

Next, $|ab| \geq \mathrm{lcm}(m, n)$:

Let $(ab)^r = e$, with $r \in \mathbb{N}$ and $r \geq 1$.

Then $(ab)^r = a^r b^r = e$. To rewrite this, we know that $a^r = b^{-r}$. Now, because $\langle a \rangle \cap \langle b \rangle = \{e\}$, we know that $a^s = b^t$ for any $s, t \in \mathbb{Z}$ implies that $a^s = b^t = e$. By the earlier problem, this means that $m \mid r$ and $n \mid -r$ (or equivalently, $n \mid r$).

So by theorems of number theory, this means that $\mathrm{lcm}(m, n) \mid r$. So $r \geq \mathrm{lcm}(m, n)$ if $(ab)^r = e$ and $r \geq 1$.

So by the squeeze theorem, $|ab| = \mathrm{lcm}(m, n)$.

Problem 2:

Consider $\delta = (1\ 2 \ldots n)$.

From theorem 4.9a, we know that the number of conjugacy classes of δ is equal to $[G : C(x)]$.

From theorem 5.6, we know that every n-cycle is conjugate to δ. There are $(n-1)!$ n-cycles in S_n:

We know that there are $n!$ elements of S_n. Pick an element of S_n...call it σ. Now, write the cycle $(\sigma(1)\ \sigma(2)\ \sigma(3)\ \ldots \sigma(n))$. This cycle is equivalent to n other cycles, each given by

$$(\sigma(2)\ \sigma(3)\ \sigma(4)\ \ldots \sigma(n)\ \sigma(1))$$
$$(\sigma(3)\ \sigma(4)\ \sigma(5)\ \ldots \sigma(n)\ \sigma(1)\ \sigma(2))$$
$$\ldots$$
$$(\sigma(n)\ \sigma(1)\ \sigma(2)\ \ldots \sigma(n-1)).$$

So there are $n!/n = (n-1)!$ different n-cycles in S_n

So $[G : C(x)] = (n-1)!$. So $|C(x)| = n$.

Now, there are n elements of the form δ^i; we know from class that an n-cycle has order n, so $|\{\delta^i : i \in \mathbb{Z}\}| = |\langle \delta \rangle| = n$.

Each element of the form δ^i commutes with δ trivially.

So the only elements that commute with δ are the elements of the form δ^i; there are n of them, and there can only be n different elements that commute with δ.

Problem 3:

The following proof is constructive; it mimicks a selection sort.

Define $s = (1\ 2)$ and $r = (1\ 2\ 3 \ldots\ n)$. ("swap" and "rotation").

Let $\sigma \in S_n$. Then for each $m \in \{1, 2, \ldots, n\}$:

Define $\alpha_0 = (1)$. Determine $\sigma(1)$. Consider

Thus, we have represented σ as a product of $(1\ 2)$, $(1\ 2\ 3 \ldots n)$, and their inverses; $\sigma \in \langle (1\ 2), (1\ 2\ 3 \ldots n) \rangle$ for all $\sigma \in S_n$, that is $S_n \subset \langle (1\ 2), (1\ 2\ 3 \ldots n) \rangle$, which implies that $S_n = \langle (1\ 2), (1\ 2\ 3 \ldots n) \rangle$ (because subgroups generated by elements are still subgroups.)

Problem 4:

Let p be a prime number and let $H < S_p$ contain a transposition and act transitively on $\{1, \ldots, p\}$.

From the earlier homework, H has an element with no fixed point (it acts transitively on a finite set).

However, any element that acts on $\{1, \ldots, p\}$ with no fixed point must be a p-cycle:

This means that H contains a transposition and a p-cycle; by a quick adaptation of the above problem below, this means that $H = S_p$.

The adaptation is this:

Problem 5:

This is given as an exercise in Hungerford: out of a sense of honesty, I must admit that I ran across this in the book, instead of coming up with it independently.

Consider $H = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

First, $H \leq G$;

We apply the subgroup criterion, and proceed by exhaustion. (In the below, I freely use the facts that 2-cycles are their own inverse and that disjoint cycles commute).

$$\begin{aligned}
(1)(1)^{-1} &= (1) \\
(1)((1\ 2)(3\ 4))^{-1} &= (3\ 4)(1\ 2) = (1\ 2)(3\ 4) \\
(1)((1\ 3)(2\ 4))^{-1} &= (2\ 4)(1\ 3) = (1\ 3)(2\ 4) \\
(1)((1\ 4)(2\ 3))^{-1} &= (2\ 3)(1\ 4) = (1\ 4)(2\ 3) \\
(1\ 2)(3\ 4)(1)^{-1} &= (1\ 2)(3\ 4) \\
(1\ 2)(3\ 4)((1\ 2)(3\ 4))^{-1} &= (1) \\
(1\ 2)(3\ 4)((1\ 3)(2\ 4))^{-1} &= (1\ 2)(3\ 4)(2\ 4)(1\ 3) = (1\ 4)(2\ 3) \\
(1\ 2)(3\ 4)((1\ 4)(2\ 3))^{-1} &= (1\ 2)(3\ 4)(2\ 3)(1\ 4) = (1\ 3)(2\ 4) \\
(1\ 3)(2\ 4)(1)^{-1} &= (1\ 3)(2\ 4) \\
(1\ 3)(2\ 4)((1\ 2)(3\ 4))^{-1} &= (1\ 3)(2\ 4)(3\ 4)(1\ 2) = (1\ 4)(2\ 3) \\
(1\ 3)(2\ 4)((1\ 3)(2\ 4))^{-1} &= (1) \\
(1\ 3)(2\ 4)((1\ 4)(2\ 3))^{-1} &= (1\ 3)(2\ 4)(2\ 3)(1\ 4) = (1\ 2)(3\ 4) \\
(1\ 4)(2\ 3)(1)^{-1} &= (1\ 4)(2\ 3) \\
(1\ 4)(2\ 3)((1\ 2)(3\ 4))^{-1} &= (1\ 4)(2\ 3)(3\ 4)(1\ 2) = (1\ 3)(2\ 4) \\
(1\ 4)(2\ 3)((1\ 3)(2\ 4))^{-1} &= (1\ 4)(2\ 3)(2\ 4)(1\ 3) = (1\ 2)(3\ 4) \\
(1\ 4)(2\ 3)((1\ 4)(2\ 3))^{-1} &= (1)
\end{aligned}$$

Next, $H \trianglelefteq S_4$;

Recall that two elements of S_4 are conjugate if and only if their cycle decomposition has the same cycle type. Note that H contains all of the elements of S_4 composed of a product of two disjoint 2-cycles.

So an element is conjugate to an element of H if and only if it is in H. That is, $ghg^{-1} \in H$ for all $g \in G$, $h \in H$.

Thus, $H \trianglelefteq S_4$. (And so, $H \trianglelefteq A_4$).

Problem 6:

We know from class that for $n \geq 5$, A_n is simple.

Let $H \trianglelefteq S_n$, with $n \geq 5$.

Problem 7:

Define $\phi : \mathrm{Aut}(A_4) \to S_4$ by: