Solutions for some homework problems

7.2.4: Let $p$ be a prime number and let $C$ be a cyclic subgroup of order $p$ in $S_p$. Compute the order of the normalizer $N(C)$ of $C$.

**Solution:** Let $\sigma$ be a generator of $C$ and write $\sigma$ as a product $\gamma_1 \cdots \gamma_r$ of disjoint cycles. The order of $\sigma$ is the least common multiple of the lengths of these cycles, so they each have length $p$. Since we are the $S_p$, we must have $r = 1$. Write $\sigma = (a_1 \ a_2 \ \cdots \ \ a_p)$. There are $p!$ such expressions, but each cycle can be written $p$ ways as such an expression. This gives us $(p-1)!$ $p$-cycles in $S_p$, and we know they are all conjugate. Each of these cycles generates a group of order $p$, and each such group has $p-1$ generators. Thus there are $(p-2)!$ cyclic subgroups of order $p$ in $S_p$, all conjugate. Hence the normalizer of any one of them has index $(p-2)!$ and hence has order $p(p-1)$.

7.3.8: Let $G$ be a finite $p$-group and let $H$ be a proper subgroup. Show that there is an element $g \in G \setminus H$ such that $gHg^{-1} = H$.

**Solution:** Let us consider the action of $G$ on the set $S := G/H$ of left cosets of $H$. Restrict this to an action of $H$ on $S$: $H \times S \to S$. Note that $H$ is a $p$-group and that $S$ has $[G:H]$ elements; this number is a positive power of $p$. Then Lemma 7.3.7 implies that $|S^H|$ is divisible by $p$. Now $H \in |S^H|$, so $|S^H| \geq 1$, hence in fact $|S^H| \geq p$. Thus there exists some coset, call it $gH$, with $g \notin G$, such that $gH \in S^H$. Then for any $h \in H$, $hgH = gH$, i.e. $g^{-1}hgH = H$, so $g^{-1}hg \in H$.

7.2.18: Compute the conjugacy classes of $A_5$ and use the result to show that $A_5$ is a simple group.

Recall that in class we showed that two elements $\sigma$ and $\sigma'$ of $S_n$ are conjugate if and only if their respective cycle decompositions:

$$\sigma = \gamma_1 \cdots \gamma_r, \sigma' = \gamma'_1 \cdots \gamma'_r$$

have the same “shape”; i.e., $r = r'$ and $\text{length}(\gamma_i) = \text{length}(\gamma'_i)$ for all $i$ (after reordering if necessary). This is not quite true in $A_n$, but it not hard to see what is happening there.

**Lemma.** Let $\alpha$ be an element of $A_n$, let $Z_\alpha := \{\sigma : \alpha = \alpha^\sigma : \sigma \in S_n\}$ be its centralizer, and let $C(\alpha) := \{\alpha^\sigma : \sigma \in S_n\}$ be its $S_n$-conjugacy class. On the other hand, let $C'(\alpha) := \{\alpha^\sigma : \sigma \in A_n\}$ be the $A_n$ conjugacy class of $\alpha$. Evidently $C'(\alpha) \subseteq C(\alpha)$, and we want to know how and when these differ. We have isomorphisms: $C(\alpha) \cong S_n/Z_\alpha$ (of $S_n$-sets) and $C'(\alpha) \cong A_n/(Z_\alpha \cap A_n)$ (of $A_n$-sets). There are two cases:

Case 1: $Z_\alpha \subseteq A_n$. In this case $Z_\alpha \cap A_n = Z_\alpha$, and since $A_n$ has just half as many elements as $S_n$, we have that $C'(\alpha) \cong A_n/Z_\alpha$ has half as many elements as $C(\alpha) \cong S_n/Z_\alpha$.

Case 2: $Z_\alpha \not\subseteq A_n$. In this case it follows that $C'(\alpha) = C(\alpha)$. Indeed, by assumption there is some odd element $\tau$ of $Z_\alpha$. Then if $\sigma$ is any odd element of $S_n$,

$$\alpha^\sigma = (\alpha^\tau)^{\sigma^\tau} = \alpha^{\sigma\tau} \in C'(\alpha)$$

1
Now let us look at the various possibilities:

3-cycles, e.g. \( \alpha = (1 \ 2 \ 3) \). There are 20 of these, all conjugate in \( S_5 \), and (4 5) is an odd element of the centralizer of (1 2 3), so they are also conjugate in \( A_5 \) (Case 1).

5-cycles, e.g. \( \alpha = (1 \ 2 \ 3 \ 4 \ 5) \). There are 24 of these, all conjugate in \( S_5 \). It follows that the index of the centralizer of \( Z_\alpha \) in \( S_5 \) is 5, so \( Z_\alpha = \langle (\alpha) \rangle \) is contained in \( A_5 \) (Case 2). Thus this conjugacy class splits into two pieces, each of size 12. (For example, \( 2(1 \ 3 \ 4 \ 5) \) is not in the \( A_n \)-conjugacy class of \( \alpha \).)

Products of 2 2-cycles, e.g. \( \alpha = (1 \ 2)(3 \ 4) \). There are \( (5 \cdot 4 \cdot 3 \cdot 2)/2 \cdot 2 \cdot 2 = 15 \) of these, all conjugate in \( S_n \). In fact \( (1 \ 2) \) is an odd element of the centralizer of \( \alpha \). so we are in Case 1 and they are all conjugate in \( A_n \).

The identity element. This is fixed by conjugation.

Thus \( A_n \) has the following conjugacy classes:

- \( C(1 \ 2 \ 3) \), with 20 elements.
- \( C(1 \ 2 \ 3 \ 4 \ 5) \), with 12 elements.
- \( C(2 \ 1 \ 3 \ 4 \ 5) \), with 12 elements.
- \( C((1 \ 2)(3 \ 4)) \) with 15 elements.
- \( C(e) \) with 1 element.

Note that 60 = 20 + 12 + 12 + 15 + 1, as it should. Now any normal subgroup is invariant under conjugation, and hence must be a union of conjugacy classes, and must contain \( e \). So the number of elements in such a group is a sum of the some of the above numbers, including 1. Furthermore, this number divides 60. But the only numbers of this form are 1 and 60. Hence \( A_n \) has no proper normal subgroups, and hence it is simple.

**7.3.13ab** Show that \( S_n \) acts transitively on the set \( \{1, \ldots, n\} \), and that \( A_n \) also does if \( n > 2 \). Indeed, for \( S_n \) just have to show that given any \( i, j \), there exists an element \( \sigma(i) = j \). This is trivial if \( i = j \), and if not we can take the transposition \( (i \ j) \). To do this for \( A_n \), we must use the fact that \( n > 2 \), so there is some \( k \) with \( 1 \leq k \leq n \) and \( k \neq i, j \). Then the 3-cycle \( (i \ j \ k) \) is even and takes \( i \) to \( j \).