**Homework 5**

**(3)** The goal of this exercise is to prove that $A_5$ is simple. Remember, this means that $A_5$ doesn't have any normal subgroups except for 1 and all of $A_5$. Note that $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$.

**(a)** Show that $n_3 = 10$ and $n_5 = 6$. (**Hint:** you should be able to exhibit explicitly all 10 Sylow 3-subgroups and all 6 Sylow 5-subgroups. Then use Sylow's theorems to argue that you have found all of them.)

Any Sylow 3-subgroup has order 3, hence is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Thus, to find a Sylow 3-subgroup, we just need to find an element of order 3 in $A_5$. The elements of order 3 in $A_5$ are exactly the 3-cycles. For example, the 3-cycle $(123)$ generates the cyclic subgroup $\langle (123) \rangle = \{1, (123), (132)\}$. From this, we see that a Sylow 3-subgroup is determined by choosing 3 elements from the set $\{1, 2, 3, 4, 5\}$. Thus, there are $\binom{5}{3} = 10$ Sylow 3-subgroups. Alternatively, we could count the 3-cycles in $A_5$ (there are 20 of them) and observe that each Sylow 3-subgroup contains exactly two 3-cycles, and any two Sylow 3-subgroups intersect just in the identity. So, there are 10 of them.

To count the Sylow 5-subgroups, we reason in a similar way. There are $120/5 = 24$ 5-cycles in $A_5$ (there are 120 different orders to write down the numbers 1-5, and two such orders give the same 5-cycle if they differ by a cyclic shift, which is an action of $\mathbb{Z}/5\mathbb{Z}$). Each Sylow 5-subgroup contains four 5-cycles, and any two Sylow 5-subgroups intersect only in the identity. So, there are 24/4=6 Sylow 5-subgroups.

**(b)** Write down two Sylow 2-subgroups of $A_5$ which have trivial intersection. Deduce in particular that $n_2 \geq 2$. (**Hint:** look at the order 4 subgroup of $A_4$ which I wrote down in the lectures.)

We recall the subgroup

$$P = \{1, (12)(34), (13)(24), (14)(23)\}$$

from lecture. In the lecture, this was presented as a subgroup of $A_4$, but we can just as easily think of it as a subgroup of $A_5$. It has order 4, so it is a Sylow 2-subgroup of $A_5$. Shifting all the numbers up by 1, we get another subgroup

$$Q = \{1, (23)(45), (24)(35), (25)(34)\}$$

This is also a Sylow 2-subgroup, and $P \cap Q = 1$.

**(c)** Suppose that $N \trianglelefteq A_5$ is a normal subgroup. Suppose that 3 divides $|N|$. Prove that every Sylow 3-subgroup of $A_5$ is contained in $N$. Similarly, show that if 5 divides $|N|$, then every Sylow 5-subgroup of $A_5$ is contained in $N$.

Suppose that 3 divides $|N|$. By Sylow's theorems, $N$ has a Sylow 3-subgroup, say $P$. We have $P \leq N \leq A_5$. It follows that $P$ has order 3, and so is also a Sylow 3-subgroup of $A_5$. By Sylow's theorems, any two Sylow 3-subgroups of $A_5$ are conjugate by an element of $A_5$. Thus, if $Q$ is a Sylow 3-subgroup of $A_5$ (!), there exists an element $g \in A_5$ such that $gPg^{-1} = Q$. But $N$ is normal in $A_5$, and $P \leq N$, so $Q = gPg^{-1} \leq gNg^{-1} = N$. Thus, $Q \leq N$.

The same reasoning applies with 3 replaced by 5 to prove the second claim.

**(d)** Suppose that either 3 or 5 divides $|N|$. Using part (c) and Lagrange's theorem, deduce that in fact both 3 and 5 divide $|N|$. Conclude that $N = A_5$. (**Hint:** note that any two subgroups of $N$ each of which have order 3 or 5 must have trivial intersection.)

Suppose that 3 divides $|N|$. By part (c), every Sylow 3-subgroup of $A_5$ is contained in $N$. By part (a), there are 10 Sylow 3-subgroups of $A_5$, any two of which intersect trivially. So, there are $10 \cdot (3-1) = 20$ distinct elements of order 3 in the Sylow 3-subgroups of $A_5$. All of these elements are also in $N$. As $N$ also contains the identity, there are at least 21 elements in $N$. By Lagrange's theorem, we know $|N|$ divides 60. Thus, the only possibilities for $|N|$ are 30 or 60. In either case, we see that 5 must divide $|N|$ too. So, by part (c), every Sylow 5-subgroup of $A_5$ is contained in $N$. by part (a), there are 6 Sylow 5-subgroups of $A_5$, any two of which intersect trivially. This gives $6 \cdot (5-1) = 24$ distinct elements of order 5 in the Sylow 5-subgroups of $A_5$. All of these elements must be contained in $N$. So, $N$ contains the identity, (at least) 20 elements of order 3, and (at least) 24 elements of order 5. This is a total of 45 elements. So, the only possibility is that in fact $|N| = 60$, and hence $N = A_5$.

Next, suppose that 5 divides $|N|$. We apply the above reasoning in the opposite order. Looking at the Sylow 5-subgroups first, we find 24 elements of order 5 in $N$. By Lagrange, we get $|H| = 30$ or 60. So, 3 also divides $|H|$. We then count the order 3 elements and conclude $N = A_5$.

**(e)** Using Sylow's theorems and part (b), show that $A_5$ does not have a normal subgroup of order 4.

By part (b), we have $n_2 \geq 2$. By Sylow's theorems, any two Sylow 2-subgroups are conjugate. Thus, no Sylow 2-subgroup of $A_5$ can be normal. So, $A_5$ does not have a normal subgroup of order 4.

**(f)** Show that if $N$ is a normal subgroup of $A_5$ of order 2, then $N$ is contained in every Sylow 2-subgroup of $A_5$. Using part (b), deduce that $A_5$ does not have a normal subgroup of order 2.

Suppose that $N$ is a normal subgroup of $A_5$ of order 2. By Sylow's theorems, $N$ is contained in a Sylow 2-subgroup of $A_5$. That is, $N \leq H$ for some subgroup $H \leq A_5$ of order 4. By Sylow's theorems, any two Sylow 2-subgroups are conjugate, so $H$ is conjugate to both the subgroup $P$ and the subgroup $Q$ written down in part (b). But $N$ is normal, so it is preserved by conjugation. Hence, we have $N \leq P$ and $N \leq Q$. But $P$ and $Q$ intersect only in the identity. We conclude that $N$ does not have a normal subgroup of order 2.

**(g)** Using Lagrange's theorem, deduce that $A_5$ is simple.

Suppose $N$ is a normal subgroup of $A_5$. By Lagrange's theorem, the order of $N$ must divide $60 = 2^2 \cdot 3 \cdot 5$. Above, we ruled out $|N| = 2$ or 4, and we also showed that if 3 or 5 divides $|N|$, then $|N| = 60$. Thus, the only possibilities are $|N| = 1$ and $|N| = 60$. So, either $N = 1$ or $N = A_5$. We conclude that $A_5$ is simple.