Problem One

1) Show that A_4 has a normal subgroup $H \trianglelefteq A_4$ isomorphic to $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
2) Show that $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ has a unique subgroup of order 3
3) Conclude that $A_4 \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$ where $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$
is the inclusion of the unique subgroup of order 3.

~ Let $H = \langle (12)(34), (13)(24) \rangle$. Computation of the elements is straightforward:
$H = \{1, (12)(34), (13)(24), (14)(23)\}$
$H \trianglelefteq S_4$ since $H < S_4$ and is a union of conjugacy classes ~ the class of permutations of ~~cycles~~ of type $(2,2)$ and identity. But every element of H is an even permutation since every element is either the identity or has cycle type $(2,2)$.
Hence, $H \trianglelefteq A_4$ as $A_4 < S_4$.
There are only two groups of order 4 up to isomorphism: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Z}/4\mathbb{Z}$ contains an element of order 4 (eg: the residue class of 1 mod 4) and all non-identity elements of H have order 2, it follows that $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

~ We have that $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$ (any permutation of the non-identity elements give rise to an automorphism). The unique subgroup of order 3 is the subgroup generated by the automorphism which cyclically permutes the non-identity elements of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ~ the cyclic subgroup that corresponds to $\langle (1\ 2\ 3) \rangle$ in S_3. The uniqueness of this subgroup follows from the Sylow theorems: the number n_3 of Sylow 3-subgroups of a group of order 6 divides 2 and satisfies $n_3 \equiv 1 \pmod 3$ hence $n_3 = 1$.

~ The 3-cycle $(1\ 23)$ is even (cycle of odd length), hence $K \equiv \langle (1\ 2\ 3) \rangle < A_4$
By Lagrange's theorem, $H \cap K = \{1\}$ (every non-identity element of H has order 2, and for K it's 3). Since $H \trianglelefteq A_4$, $HK \leq A_4$, but $|HK| = |H||K| = 4 \times 3 = 12 = |A_4|$. Hence $A_4 = HK$.
Equivalently, $A_4 \cong H \rtimes_\varphi K$, where $\varphi : K \to \mathrm{Aut}(H)$ and $\varphi(k)$ is the conjugation map by k.

Problem 2

~ Finish the proof started in the lecture that A_n is simple for $n \geq 5$ as follows: Suppose $N \triangleleft A_n$ is a non-trivial normal subgroup, in particular it contains a non trivial element $\sigma \in N$.

1) Depending on the cycle decomposition of σ find a 3-cycle $(i\,j\,k)$ such that $\sigma(i\,j\,k)\sigma^{-1}(k\,j\,i)$ is either a 3-cycle or we land in one of four cases.

a) σ containing a ≥ 4-cycle

→ Suppose that the cycle decomposition of σ contains a cycle of length at least 4: $\sigma = \mu(i\,j\,k\,l\,\ldots)$ with μ disjoint

$$\sigma(i\,j\,k)\sigma^{-1}(i\,j\,k)^{-1} = \mu\mu^{-1}(\sigma(i)\,\sigma(j)\,\sigma(k))(k\,j\,i)$$
$$= (j\,k\,l)(k\,j\,i)$$
$$= (i\,l\,j)$$

b) σ containing at least two 3-cycles

→ Suppose that the cycle decomposition of σ contains at least two 3-cycl[es]

$\sigma = \mu(i\,j\,k)(l\,m\,n)$, then

$$\sigma(i\,j\,l)\sigma^{-1}(i\,j\,l)^{-1} = \mu\mu^{-1}(\sigma(i)\,\sigma(j)\,\sigma(l))(l\,j\,i)$$
$$= (j\,k\,m)(l\,j\,i)$$
$$= (i\,l\,k\,m\,j)$$

Hence, $(i\,l\,k\,m\,j) \in N \Rightarrow$ we can reduce to (a) by replacing σ with [a] 5-cycle.

c) σ contains 1 3-cycle and 1 2-cycle

→ Suppose that the cycle decomposition of σ contains a 3-cycle and a 2[-cycle] (μ disjoint and product of disjoint 2-cycles), then

$\sigma = \mu(i\,j\,k)(l\,m)$

$$\Rightarrow \sigma(i\,j\,l)\sigma^{-1}(i\,j\,l)^{-1} = \mu\mu^{-1}(\sigma(i)\,\sigma(j)\,\sigma(l))(l\,j\,i)$$
$$= (j\,k\,m)(l\,j\,i)$$
$$= (i\,l\,k\,m\,j)$$

• Hence, $(i\,l\,k\,m\,j) \in N$ and we are reduced to case (a) as above (b).

d) σ contains only 2-cycles:
$\sigma = \mu(ij)(kl)$. Then

$$\begin{aligned}\sigma(ijk)\sigma^{-1}(ijk)^{-1} &= (\sigma(i)\sigma(j)\sigma(k))(kji) \\ &= (jil)(lji) \\ &= (ijl)\end{aligned}$$

Hence N contains a 3-cycle.

2) Conclude that An is simple
$\Rightarrow$ If case (a) fails, then there is at most one 3-cycle in the cycle decomposition. If case (b) fails, then there is at most one 3-cycle in the cycle decomposition. If the cycle decomposition is a 3-cycle, we are done.
Otherwise, the cycle decomposition contains a 2-cycle and a 3-cycle, which is case (c) or contains only two-cycles, in which case (d). Thus, it follows from (I) that N contains a 3-cycle. But N is normal, hence is a union of conjugacy classes. Hence, N contains the conjugacy class of the 3-cycle it contains. But, all 3-cycles are conjugate in An, $n \geq 5$. Hence An contains all 3-cycles. But, An is generated by all 3-cycles for $n \geq 3$. Hence $N = An$ and it follows that An contains no non-trivial proper normal subgroup for $n \geq 5$ i.e. An is simple for $n \geq 5$.

Problem Three

Let G be a group and $S \subseteq G$ a subset. We define the group generated by S to be

$$\langle S \rangle \equiv \bigcap_{S \subseteq H \leq G} H$$

Show that for any group K a group homomorphism $\phi : \langle S \rangle \to K$ is completely determined by the restriction $\phi|_S : S \to K$. That is, show that if we have group homomorphisms $\phi_1, \phi_2 : \langle S \rangle \to K$ such that

$\phi_1(s) = \phi_2(s) \quad \forall s \in S$, then

$\phi_1 = \phi_2$.

$\Rightarrow$ Let $x \in \langle S \rangle$ and let $\phi_1, \phi_2 : \langle S \rangle \to K$ be group homomorphisms which satisfy $\phi_1(s) = \phi_2(s)$ $\forall s \in S$. We must show that there exists finitely many elements $s_1, s_2, \dots, s_n \in S$ such that

$$x = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$$

as therefore

$$\phi_1(x) = \phi_1(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}) = \phi_1(s_1^{\epsilon_1}) \cdots \phi_1(s_n^{\epsilon_n}) = \phi_2(s_1^{\epsilon_1}) \cdots \phi_2(s_n^{\epsilon_n}) = \phi_2(x)$$

Firstly, define a set $\bar{S}$ to be the subset of G consisting of all finite products of elements of S and their inverses:

$\bar{S} = \{ s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \mid s_i \in S,\ \epsilon_i \in \{\pm 1\} \text{ for each } i \in \{1, \dots, n\} \}$

where $\bar{S} = \{1\}$ if $S = \emptyset$. Thus $\bar{S} \neq \emptyset$ & if $y = t_1^{\delta_1} \cdots t_n^{\delta_n}$ is in $\bar{S}$, then $y^{-1} = t_n^{-\delta_n} \cdots t_1^{-\delta_1}$ is also in $\bar{S}$ $\Rightarrow$ $\bar{S}$ is closed under inversion of elements. If $x = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$ is any other element of $\bar{S}$, then

$$xy^{-1} = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} t_n^{-\delta_n} \cdots t_n^{-\delta_1}$$

which is, again, in $\bar{S}$. Thus, it follows that $\bar{S} \leq G$. But, for $s \in S$ $\Rightarrow s \in \bar{S}$, that is $S \subset \bar{S}$. Hence $\langle S \rangle \leq \bar{S}$

Problem 4

- Let n be a natural number and define the group
$$G = \langle s_1, \ldots, s_n \mid R \rangle$$
where R is the set of relations consisting of
s_i^2, $\forall i = 1, \ldots, n$
$(s_i s_{i+1})^3$, $\forall i = 1, \ldots, n-1$
$(s_i s_j)^2$ $\forall i, j$ such that $|i-j| > 1$
Show that there exists a surjective group homomorphism $\phi : G \to S_{n+1}$

→ Let $S = \{s_1, \ldots, s_n\}$ be the generating set and define a map $\varphi : S \to S_{n+1}$ by $s_i \to (i\ i{+}1)$
Then $\varphi(s_i)^2 = 1$ for all $i \in \{1, \ldots, n\}$ since every transposition has order 2. Next, we have
$$[\varphi(s_i)\varphi(s_{i+1})]^3 = [(i\ i{+}1)(i{+}1\ i{+}2)]^3 = [(i\ i{+}1\ i{+}2)]^3 = 1$$
For all $i \in \{1, \ldots, n-1\}$ since every 3-cycle has order 3. Lastly, we have
$$[\varphi(s_i)\varphi(s_j)]^2 = [(i\ i{+}1)(j\ j{+}1)]^2 = (i\ i{+}1)^2(j\ j{+}1)^2 = 1$$
For all $i, j \in \{1, \ldots, n\}$ such that $|i-j| > 1$, since disjoint cycles commute

Let $(i\ j)$ be any transposition in S_{n+1}. If $|i-j| = 1$, then $\varphi(s) = (i\ j)$ for some $s \in S$. Suppose instead that $|i-j| > 1$ and assume $i < j-1$. Then
$$(i\ j) = (i\ i{+}1) \cdots (j{-}2\ j{-}1)(j{-}1\ j)(j{-}2\ j{-}1) \cdots (i\ i{+}1)$$
Therefore, $\varphi(S)$ generates all transpositions in S_{n+1} and hence generates S_{n+1} (every permutation can be written as a product of transpositions)
→ By Problem (3), we can extend φ to a group homomorphism $\phi : G \to S_{n+1}$ by $\phi|_S = \varphi$, by requiring that ϕ is a group homomorphism. It is clear by definition of the restriction of the homomorphism that it is a surjection