1) Determine all abelian groups of order 400.

   400 = 2^4 \times 5^2. The possibilities are 1) \( \mathbb{Z}_{16} \times \mathbb{Z}_{25} \), 2) \( \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_{25} \), 3) \( \mathbb{Z}_4 \times \mathbb{Z}_{25} \), 4) \( \mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25} \), 5) \( \mathbb{Z}_2 \times \mathbb{Z}_{125} \), 6) \( \mathbb{Z}_{16} \times \mathbb{Z}_5 \), 7) \( \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \), 8) \( \mathbb{Z}_4^2 \times \mathbb{Z}_2 \), 9) \( \mathbb{Z}_2^2 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \), 10) \( \mathbb{Z}_2^4 \times \mathbb{Z}_5 \).

2) To which of the following groups is \( \mathbb{Z}_{20} \times \mathbb{Z}_{50} \times \mathbb{Z}_2 \) isomorphic to?

\( \mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \), \( \mathbb{Z}_{2000} \), \( \mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25} \times \mathbb{Z}_{25} \), \( \mathbb{Z}_4^2 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \), or \( \mathbb{Z}_4^2 \times \mathbb{Z}_5 \times \mathbb{Z}_{25} \)?

\( \mathbb{Z}_{20} \times \mathbb{Z}_{50} \times \mathbb{Z}_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_2 \cong \mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{25} .

3) Prove that there is no surjective homomorphism \( \phi : \mathbb{Z}_4^2 \rightarrow \mathbb{Z}_8 \).

Find a surjective homomorphism \( \psi : D_4 \rightarrow \mathbb{Z}_2^2 \) (Hint: find a normal subgroup \( N \) of index 4 and show that \( G/N \cong \mathbb{Z}_2^2 \).)

\( \mathbb{Z}_8 \) is cyclic and so the image of \( \mathbb{Z}_2^2 \) is cyclic hence generated by an element say \( \phi(x) \) of order 8. Since every element \( x \in \mathbb{Z}_4^2 \) has order \( \leq 4 \), this is impossible.

Let \( N = Z(G) \), then \( |Z(G)| = 2 \) and in fact \( Z(G) = \{ e, \rho^2 \} \). We must show that \( D_4/Z(G) \cong \mathbb{Z}_2^2 \) i.e. that elements in \( D_4/Z(G) \) have order at most 2. Let \( Z = Z(G) \). We have \( D_4/Z = \{ \rho \rho Z, \sigma \rho Z, \rho \sigma Z \} \). Clearly \( (\rho \rho Z)^2 = \rho^2 Z = Z \), \( (\sigma \rho Z)^2 = \sigma^2 Z = Z \) and \( (\rho \sigma Z)^2 = \rho \sigma \rho \sigma Z = \rho \rho^3 Z = Z \).

4) Write \( (1,7,3)(2,3,4)(5,8,6)(8,9) \) as a product of disjoint cycles and as a product of transpositions. What is its order and sign?

\[
(1,7,3)(2,3,4)(5,8,6)(8,9) = (1,7,3,4,2)(5,8,9,6) = (1,2)(1,4)(1,3)(1,7)(5,6)(5,9)(5,8).
\]

The order is 20 and the sign is odd.

5) Define \( U_m \), prove that it is a group and show that if \( a \) and \( m \) are two positive integers such that \( (a, m) = 1 \) then \( a^{\varphi(m)} = 1 \) modulo \( m \).

We let \( U_m = \{ [x] | 0 < x < m \text{ and } (x, m) = 1 \} \) where \([x] \) denotes the equivalence class of \( x \) modulo \( m \). \( U_m \) is a group with respect to multiplication. It is closed under multiplication since \((x, m) = 1 \) and \((y, m) = 1 \) implies \((xy, m) = 1 \). The identity element is \([1] \), associativity follows from associativity in \( \mathbb{Z} \): \( ([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = ([a \cdot b] \cdot c) = [a \cdot (b \cdot c)] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c]) \). To prove the existence of the inverse of \([x] \in U_m \), note that as \((x, m) = 1 \), we can write \( ax + bm = 1 \) for some integers \( a, b \). But then \((a, m) = 1 \) so that \([a] \in U_m \) and \([x][a] = [xa] = [xa + bm] = [1] \) as required.

Since \(|U_m| = \varphi(m)\), the order of any element \([a] \in U_m \) divides \( \varphi(m) \).

But then \([a^{\varphi(m)}] = [a]^{\varphi(m)} = [1] \) as required.
6) Let $G$ be a group of order $p^n$ where $p$ is prime. Show that $Z(G) \neq \{e\}$.

By the Class Equation we have

$$G = \sum_{a \in G} \text{cl}(a) = \sum_{a \in G} \frac{|G|}{|C(a)|} = |Z(G)| + \sum_{a \in G - Z(G)} \frac{|G|}{|C(a)|}.$$

Note that $p$ divides $G$ and $\frac{|G|}{|C(a)|}$ for any $a \in G - Z(G)$. Therefore $p$ divides $|Z(G)|$. Since $e \in Z(G)$, we have $|Z(G)| \geq p$ so that $Z(G) \neq \{e\}$.

7) Let $p$ be a prime. Prove that any group of order $p^2$ is abelian (you may use ex. 6).

We know that $|Z(G)| \in \{1, p, p^2\}$. By ex. 6) $|Z(G)| \neq 1$. If $|Z(G)| = p$, then $G$ is abelian and so we may assume that $|Z(G)| = p$. Let $x \in G - Z(G)$ and consider the subgroup $C(x)$. We have $Z(G) \subset C(x)$ and $x \in C(x)$ so that $|C(x)| > p$. Since $|C(x)|$ divides $p^2$, we have $|C(x)| = p^2$ and so $C(x) = G$ i.e. $x \in Z(G)$ which is impossible.

8) If $M$ and $N$ are normal subgroups of a group $G$, such that $M \cap N = \{e\}$ and $MN = G$, then show that $mn = nm$ for any $n \in N$ and $m \in M$ and that $M \times N$ is isomorphic to $G$.

Let $n \in N$ and $m \in M$. As $N, M$ are normal subgroups, $mn^{-1}m^{-1} \in N$, and $nmm^{-1} \in M$. But then $nmm^{-1}m^{-1} = n(mn^{-1}m^{-1}) \in N$ and $nmm^{-1}m^{-1} = (nmm^{-1})m^{-1} \in M$ so that $nmm^{-1}m^{-1} \in M \cap N = \{e\}$. Thus $nmm^{-1}m^{-1} = e$ and so $nm = mn$.

Define $\phi : M \times N \to G$ by $\phi(n, m) = n \cdot m$. Then $\phi$ is a homomorphism because

$$\phi((n, m)(n', m')) = \phi(n, m, n', m') = nmnm' = nmm'n' = \phi(n, m)\phi(n', m').$$

$\phi$ is injective because $\phi(n, m) = e$ implies $nm = e$ so that $n = m^{-1} \in N \cap M = \{e\}$. Thus $n = m^{-1} = e$ i.e. $(n, m) = (e, e)$ is the identity.

$\phi$ is surjective because (as $G = NM$) for any $g \in G$ we have $g = nm = \phi(n, m)$.

9) State and prove Lagrange’s Theorem.

Theorem. Let $H$ be a subgroup of a finite group $G$, then the order of $H$ divides the order of $G$.

Proof. Define the equivalence relation $a \sim b$ if $ab^{-1} \in H$. (Symmetric: $a \sim a$ as $aa^{-1} = e \in H$; Reflexive: $a \sim b$ implies $ab^{-1} \in H$ so that $ba^{-1} = (ab^{-1})^{-1} \in H$ and hence $b \sim a$; Transitive: if $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$ so that $ac^{-1} = ab^{-1}bc^{-1} \in H$. Thus $a \sim c$.)
It is easy to see that $|a| = Ha$ and that $|Ha| = |H|$ for any $a \in G$. But then since $G = \bigcup_{a \in G} Ha$, we have that the order of $G$ is the product of $|H|$ times the number of equivalence classes. 

10) State and prove Cayley’s Theorem.

**Theorem.** Let $G$ be any group, then there is a set $S$ such that $G$ is a subgroup of $A(S)$.

**Proof.** Let $S = G$ and define $\phi : G \to S$ by $\phi(g) = \sigma_g$ where $\sigma_g(x) = gx$.

We check that $\phi$ is a homomorphism i.e. that $\phi(gg') = \phi(g) \circ \phi(g')$ for all $g, g' \in G$, i.e. that $\phi(gg')(x) = (\phi(g) \circ \phi(g'))(x)$ for all $x \in S$. In fact $\phi(gg')(x) = \sigma_{gg'}(x) = (gg')x = g(g'x) = \sigma_g(\sigma_{g'}(x)) = \phi(g)(\phi(g')(x)) = (\phi(g) \circ \phi(g'))(x)$.

Finally we check that $\phi$ is injective. Suppose that $\phi(g) = id$, then $\phi(g)(e) = id(e)$ so that $g = ge = e$. 

\[\square\]