1. Let G be a group and let N and K be normal subgroups of G.

   (a) Show that $N \cap K \lhd K$.

   (b) Prove that $NK = \{nk | n \in N, k \in K\}$ is a normal subgroup of G.

   (c) Prove that $N \lhd NK$.

   (d) Prove that the function $f : K \to NK/N$ given by $f(k) = Nk$ is a surjective homomophism with kernel $K \cap N$.

   (e) Prove that $K/(N \cap K) \cong NK/N$.

(a) Pf. Take arbitrary $g \in K$ and $h \in N \cap K$.

Since $N, K \lhd G$, $gNg^{-1} \subseteq N$ and $gKg^{-1} \subseteq K$

$\Downarrow$ $\Downarrow$

So $ghg^{-1} \in N$ and $ghg^{-1} \in K$

So $ghg^{-1} \in N \cap K$

Therefore $\forall g \in K$, $g N \cap K g^{-1} \subseteq N \cap K$

By Thm 8.11, $N \cap K \lhd K$

(b) Take arbitrary $g \in G$ and $h \in NK$

So $h = nk$ for some $n \in N$ and $k \in K$

$ghg^{-1} = gnkg^{-1} = (gn)(kg^{-1})$

Since K, N are normal, $gN = Ng$ and $g^{-1}K = Kg^{-1}$

So $gn = n'g$ for some $n' \in N$

$kg^{-1} = g^{-1}k'$ for some $k' \in K$

So $ghg^{-1} = (gn)(kg^{-1}) = n'gg^{-1}k' = n'k' \in NK$

Therefore we have proved $\forall g \in G$, $gNKg^{-1} \subseteq NK$

Therefore $NK \trianglelefteq G$

(c) Take arbitrary $n \in N$ and $h \in NK$

So $h = n_2 k$ for some $n_2 \in N$, $k \in K$

Then $hnh^{-1} = n_2 k n (n_2 k)^{-1}$

$= \underline{n_2 k n k^{-1} n_2^{-1}}$

Since $N \trianglelefteq G$, $kN = Nk$

So $kn = n' k$ for some $n' \in N$

and $n_2 n' = n'' n_2$ for some $n'' \in N$

$\Rightarrow hnh^{-1} = n''(n_2 k k^{-1} n_2^{-1}) = n'' \in N$

So $\forall h \in NK$, $hNh^{-1} \subseteq N$

Therefore $N \trianglelefteq NK$

(d) Since $N \trianglelefteq NK$, NK/N is a well-defined quotient ring.

For $f: K \to NK/N$ given by sending
$k \mapsto Nk$

Let h be an arbitrary element of NK/N

So $h = N(nk)$ for some $nk \in NK$ where $n \in N, k \in K$

By definition, $N(nk) = \{n^*(nk) \mid n^* \in N\}$

$$= \{(n^*n)k \mid n^* \in N\}$$

$$= \{n^*k \mid n^* \in N\} = Nk$$

So $f(k) = Nk = N(nk) = h$

Therefore f is surjective.

Since the identity of NK/N is N

Note that $f(k) = Nk = N \iff k \in N \iff k \in N \cap K$ (and $k \in K$ for sure)

So $\ker(f) = N \cap K$

(e) by the first isomorphism theorem,

$K/\ker f \cong NK/N$

so $K/(N \cap K) \cong NK/N$

2. In the following problem, it may help to use the first isomorphism theorem.

(a) Prove that $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^\times$ (HINT: consider the function $e^{2\pi i z}$).

(b) Prove that $\mathbb{R}/\mathbb{Z} \cong S^1$.

(c) Prove that the subset $N = \{e, (12)(34), (13)(24), (14)(23)\} \subset A_4$ is a normal subgroup. What familiar group is the quotient A_4/N isomorphic to?

(a) Pf. Consider the function $f: \mathbb{C} \to \mathbb{C}^\times$ sending $z \mapsto e^{2\pi i z}$

① f is a group homomorphism.

since $\forall z_1, z_2 \in \mathbb{C}$, $f(z_1+z_2) = e^{2\pi i(z_1+z_2)}$
$= e^{2\pi i z_1} \cdot e^{2\pi i z_2} = f(z_1) \cdot f(z_2)$

② f is surjective

since $\forall z' \in \mathbb{C}^\times$, z' is a nonzero complex number so $z' = ke^{2\pi i r}$ for some $r \in \mathbb{R}$ and $k \in \mathbb{R}^+$, by Euler's formula.

And $k \in \mathbb{R}^+ \Rightarrow k = e^{2\pi x}$ for some $x \in \mathbb{R}$

So consider $z = x - ir$, $f(z) = e^{2\pi(x-ir)} = z'$

Therefore f is surjective.

③ Note that $f(z) = e_{\mathbb{C}^\times} = 1 \Leftrightarrow z \in \mathbb{Z}$

So $\ker \varphi = \mathbb{Z}$

So by the first isomorphism theorem, $\mathbb{C}/\ker f \cong \mathbb{C}^\times$

so $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^\times$

(b) Still consider the map $f: \mathbb{R} \to S^1$ sending

$r \mapsto e^{2\pi i r}$

① f is a group homomorphism

$\forall r_1, r_2 \in \mathbb{R}$, $f(r_1+r_2) = e^{2\pi i(r_1+r_2)} = e^{2\pi i r_1} \cdot e^{2\pi i r_2}$

$= f(r_1) \cdot f(r_2)$

② f is surjective

since $\forall s \in S^1$, $s = e^{2\pi i r}$ for some $r \in \mathbb{R}$

③ Note that $f(r) = e_{S^1} = 1 \iff r \in \mathbb{Z}$

Since $\forall r \in \mathbb{Z}$, $s = e^{2\pi i r} = \cos(2\pi r) + i\sin(2\pi r)$

$= \cos(2\pi r) = 1$

So $\ker(f) = \mathbb{Z}$

Therefore by the first isomorphism theorem,

$$\mathbb{R}/\ker f \cong S^1$$

$$\Rightarrow \mathbb{R}/\mathbb{Z} \cong S^1$$

(c) First the subset N is a subgroup of A_4

① $e \in N$

since ② $e^2 = e$ $\quad ((12)(34))^2 = e$

$((13)(24))^2 = e \quad ((14)(23))^2 = e$

A_4 is closed under inverse

Then we show $N \lhd A_4$

Let $\sigma \in A_4$ be an arbitrary permutation

$t \in N$ be an arbitrary element

So $t = (\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$

for a, b, c, d respectively representing a unique number in $\{1,2,3,4\}$

Then $\sigma^{-1} t \sigma = \begin{pmatrix} a & b & c & d \\ \sigma(a) & \sigma(b) & \sigma(c) & \sigma(d) \end{pmatrix}$

$\hookrightarrow \begin{pmatrix} \sigma(b) & \sigma(a) & \sigma(d) & \sigma(c) \end{pmatrix}$

$\hookrightarrow \begin{pmatrix} b & a & d & c \end{pmatrix}$

So $\forall \sigma \in A_n, t \in N$ the σ-conjuate of $t = (\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d)) \in N$ is $(ab)(cd) \in N$

Therefore $\forall \sigma \in A_n$, $\sigma N \sigma^{-1} \leq N$

by Thm, $N \lhd A_n$

By Lagrange's Thm,

$$|A_4/N| = \frac{|A_n|}{|N|} = 3,$$

So $A_4/N \cong \mathbb{Z}_3$ since every finite group of order $3 \cong \mathbb{Z}_3$.

3. Let p be a prime number. The goal of this problem is to prove that any group G of order p^2 is abelian.

(a) Let the group G act on itself by the conjugacy action defined in the previous problem set. Prove that $h \in Z(G)$ if and only if the orbit (AKA the conjugacy class) of h has exactly 1 element.

(b) Use the Class Equation to deduce that p divides $|Z(G)|$. (Thus there are two possibilities $|Z(G)| = p$ or $|G|$, in the latter case G is abelian.)

(c) Suppose that $|Z(G)| = p$ and let $g \in G$ with $g \notin Z(G)$. Define $\langle Z(G), g\rangle$ to be the group generated by g and every element of $Z(G)$. Show that $\langle Z(G), g\rangle$ is abelian.

(d) Suppose that $|Z(G)| = p$ and let $g \in G$ with $g \notin Z(G)$. Define $\langle Z(G), g\rangle$ to be the group generated by g and every element of $Z(G)$. Show that $\langle Z(G), g\rangle = G$.

(e) Deduce (in one line) that G is abelian.

(f) Give an example of a group with p^3 elements that is not abelian.

(g) Use the Class Equation to conclude that any p-group[1] H satisfies p divides $|Z(H)|$.

[1] A p-group H is a group such that $|H| = p^k$ for some $k > 0$ and p a prime number.

(a) Pf. $O(h) = \{g^{-1}hg \mid g \in G\}$

Assume $h \in Z(G)$ $\Rightarrow \forall g \in G,\ gh = hg$

$\Rightarrow O(h) = \{g^{-1}gh \mid g \in G\} = \{h\}$

So $|O(h)| = 1$

Assume $|O(h)| = 1$

So $\forall g \in G,\ g^{-1}hg = h$ since $h \in O(h)$ $\quad \hat{=} e \cdot h$

$\Rightarrow \forall g \in G,\ hg = gh$

$\Rightarrow h \in Z(G)$

Therefore $|O(h)| = 1$ iff $h \in Z(G)$

(b) Let $g_1, \dots, g_n$ be the representatives of the distinct conjugacy classes of G not contained in $Z(G)$.

Class equation:

$$|G| = |Z(G)| + \underbrace{\sum_{i=1}^{n} [G : C_G(g_i)]}$$ $= \sum_{i=1}^{n} |O(g_i)|$ by the conjugation action.

Since p is prime and $|G| = p^2$ ($p \mid |G|$)

every subgroup of $|G|$ can only has size of : $\underbrace{1, p \text{ or } p^2}$

since for each i, $O(g_i)$ is a subgroup of G that has $\underbrace{\text{more than one element}}$

so $|O(g_i)| = \underbrace{p \text{ or } p^2}$

So $\underbrace{p \mid \sum_{i=1}^{n} [G : C_G(g_i)]} \Rightarrow p \Big| \Big(|G| - \sum_{i=1}^{n} [G : C_G(g_i)]\Big)$

$\Rightarrow \underbrace{p \mid |Z(G)|}$ (Therefore either $|Z(G)| = p$ or $|Z(G)| = p^2$)

(c) Let $z_1^{n_1} z_2^{n_2} \cdots g^{n_i} \cdots z_k^{n_k}$,

$q_1^{m_1} q_2^{m_2} \cdots g^{m_i} \cdots q_e^{m_e}$ be two arbitrary ele

$$(z_1^{n_1} z_2^{n_2} \cdots g^{n_j} \cdots z_k^{n_k})(g_1^{m_1} g_2^{m_2} \cdots g^{m_i} \cdots g_e^{m_e})$$

$$= (g_1^{m} z_1^{n_1} z_2^{n_2} \cdots g^{n_j} \cdots z_k^{n_1})(g_2^{m_2} \cdots g^{m_i} \cdots g_e^{m_e})$$

$$= \cdots$$

$$= (g_1^{m_1} g_2^{m_2} \cdots g^{m_i} \cdots g_e^{m_e})(z_1^{n_1} z_2^{n_2} \cdots g^{n_j} \cdots z_k^{n_1})$$

Since every element of $Z(G)$ commute with each other and g.

So $\langle Z(G), g \rangle$ is Abelian

(d) We have known that any subgroup of G can only has order of $1, p$ or p^2

And since $|\langle Z(G), g\rangle| \geq \underbrace{|Z(G)| + 1}_{= p+1}$,

$|\langle Z(G), g\rangle| = p^2 = |G|$

So $\langle Z(G), g\rangle = G$.

(e) Since $\langle Z(G), g\rangle = G$ by (d) and $\langle Z(G), g\rangle$ is Abelian by (c), $\underline{G \text{ is Abelian}}$.

(f) $|D_4| = 8 = 2^3$, but D_4 is not Abelian

(g) Let H be a p-group, so $|H| = p^k$ for some prime p and $k \in \mathbb{Z}^+$.

By class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(g_i)] \quad = \sum_{i=1}^{n} |O(g_i)| \text{ by the conjugation action.}$$

Since p is prime and $|G| = p^k$ ($p \mid |G|$)

every subgroup of $|G|$ can only has size of: $1, p, p^2, \dots, p^k$

since for each i, $O(g_i)$ is a subgroup of G that has more than one element

So $|O(g_i)| = p$ or $p^2 \dots$ or p^k

So $p \mid \sum_{i=1}^{n} [G : C_G(g_i)]$

So $p \mid \left(|G| - \sum_{i=1}^{n} [G : C_G(g_i)]\right)$

So $p \mid |Z(G)|$.

THEOREM 9.7: FUNDAMENTAL STRUCTURE THEOREM FOR FINITE ABELIAN GROUPS: Let G be a finite abelian group. Then G is isomorphic to a group of the form

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \mathbb{Z}_{p_3^{a_3}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$$

where $p_1, p_2, \ldots p_n$ are (not necessarily distinct!) prime numbers. Moreover, the product is unique, up to re-ordering the factors.

4. (a) Suppose that G is abelian and has order 8. Use the Structure Theorem for Finite Abelian Groups to show that up to isomorphism, G must be isomorphic to one of three possible groups, each a product of cyclic groups of prime power order.
   (b) Determine the number of abelian groups of order 18, up to isomorphism.
   (c) For p prime, how many isomorphism types of abelian groups of order p^4?
   (d) If an abelian group of order 100 has no element of order 4, prove that G contains a Klein 4-group.

(a) Since the prime factorization of $8 = 2^3$

And G is Abelian and $|G| = 8$,

by the Structure theorem for finite Abelian

either $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

or $G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2$ $(\mathbb{Z}_4 \times \mathbb{Z}_2)$

or $G \cong \mathbb{Z}_{2^3}$ $(\mathbb{Z}_8)$

(b) $18 = 3^2 \times 2$

So the possible isomorphism is

$\mathbb{Z}_9 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$,

$(3 \times 3) \times 2$ $\quad$ $3 \times 3 \times 2$

There are two possible isomorphism types.

(c) There are 5 isomorphism types.

$p \times p \times p \times p$: $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

$(p \times p) \times p \times p$: $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$

$(p \times p \times p) \times p$: $\mathbb{Z}_{p^3} \times \mathbb{Z}_p$

$(p \times p \times p \times p)$: $\mathbb{Z}_{p^4}$

$(p \times p) \times (p \times p)$: $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$

(d) prime factorization of 100: $100 = 2^2 \times 5^2$

Since G is Abelian and $|G| = 100$,

$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{5^2}$ ①

or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2}$ ②

or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ ③

And note that ① is impossible since $([1]_4, [0]_5)$ is an order 4 element in it

Therefore $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$ ② or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ ③

For ②: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times [0]_{25}$ is a subgroup which is a Klein 4-group.

For ③: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times [0]_5 \times [0]_5$ is a subgroup which is a Klein 4-group.