1. Let $\mathbb{Z}_n$ and $\mathbb{Z}_m$ be two cyclic groups of order n and m respectively. State and prove a necessary and sufficient condition involving n and m for $\mathbb{Z}_n \times \mathbb{Z}_m$ to be cyclic.

   Solution: $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic if and only if $\gcd(m,n) = 1$.
   ($\Rightarrow$)Let $\mathbb{Z}_n \times \mathbb{Z}_m$ be cyclic. On the contrary, assume that m and n are not co-prime, that is, $\gcd(m,n) = d$ and $d > 1$.
   Let $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_m$. Note that m divides $\frac{mn}{d}$ and n divides $\frac{mn}{d}$. Therefore,

$$(\frac{mn}{d}a \mod n, \frac{mn}{d}b \mod m) = (0,0)$$

$$\implies |(a,b)| = \frac{mn}{d} < mn \text{ as } d > 1.$$

   Therefore, $\mathbb{Z}_n \times \mathbb{Z}_m$ can not be generated by any of its elements. Hence, $\mathbb{Z}_n \times \mathbb{Z}_m$ is not cyclic. Therefore, $\gcd(m,n) = 1$.
   ($\Leftarrow$) Let $\gcd(m,n) = 1$. Let $k \in \mathbb{N}$ such that $k(1,1) = (k \mod n, k \mod m) = (0,0)$. It is possible only when $k = mn$ as n and m are relatively prime. Therefore group generated by $(1,1)$ has order $mn = |\mathbb{Z}_n \times \mathbb{Z}_m|$.
   Therefore $(1,1)$ generates $\mathbb{Z}_n \times \mathbb{Z}_m$. Hence $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic.

2. Prove that if a finite group G is cyclic of order n, then for every positive integer dividing n, there exists a unique subgroup of order d in G.

   Solution: Given that G is a cyclic group of order n. Let a be its generator and $|a| = n$. Since d divides n, the element $(a)^{\frac{n}{d}}$ has order d. If not, then there exists a positive integer $d' < d$ such that $(a^{\frac{n}{d}})^{d'} = e$, where e is the identity of G. Since d divides n, let $\frac{d}{n} = m$. Therefore $a^{md'} = e$ and $md' < md = n$. Therefore $|a| < n$. This is a contradiction to the fact that $|a| = n$. Hence $|a^{\frac{n}{d}}| = d$ and the subgroup $\langle a^{\frac{n}{d}} \rangle$ has order d.

3. (a) If a finite group G acts on a finite set S, show that each orbit has cardinality a divisor of the order of G.

   Solution: Let O_x denotes the orbit of $x \in X$, that is, $O_x = \{g.x | g \in G\}$. Since, $O_x \cong G/G_x$, where G_x is the stabilizer subgroup in G of x. Therefore, cardinality of O_x is same as the cardinality of G/G_x. Hence, cardinality of O_x divides $|G|$.

   (b) Let G be a group of order p^n for some prime p acting on a finite set S whose cardinality is not a multiple of p. Show that there exists $x_0 \in S$ such that $g.x_0 = x_0$ for all $g \in G$.

   Solution: Please go through the proof of Sylow's second theorem.

4. (a) Find the distinct conjugacy class of A_4.

   Solution: There are four conjugacy classes in A_4, namely
   $\{(1)\}, \{(12)(34), (13)(24), (14)(23)\}, \{(123), (243), (134), (142)\}, \{(132), (234), (143), (124)\}$

(b) Determine the class equation for A_4.

Solution: The class equation is: $12 = 1 + 4 + 4 + 3$.

5. Let G be a finite group and p be a prime dividing the order of G. Prove that there exists an element of order p in G. (You may treat the abelian and non-abelian case separately).

Solution: If G is abelian then this is cauchy's theorem. Please refer to Theorem 11 of Abstract Algebra by Dummit and Foote.
If G is non-abelian: On the contrary, assume that no element of G is of order p. Therefore, no proper subgroup of G has order divisible by p. For each proper subgroup H of G, we have

$$|G| = |H|[G : H]$$

Since $|H|$ is not divisible by p and p divides $|G|$, therefore p divides $[G : H]$ for every proper subgroup H of G.
Since G is non-abelian. it has some conjugacy classes of order greater than 1. Let these classes be represented by $g_1, g_2, ..., g_k$. Conjugacy classes of size 1 are the elements of the centralizer of G. Since conjugacy classes in G form a partition of G, we have

$$|G| = |Z(G)| + \sum_{i=1}^{k} (\text{size of conjugacy classes of } g_i) = |Z(G)| + \sum_{i=1}^{k} [G : Z(g_i)] \tag{1}$$

where $Z(g_i)$ is the centralizer of g_i. Since conjugacy classes of each g_i has size greater than 1, we have $[G : Z(g_i)] > 1$. So $Z(g_i) \neq G$ for every i. Therefore p divides $[G : Z(g_i)]$. The left hand side of Equation (1) is divisible by p and $[G : Z(g_i)]$ is also divisible by p. Therefore p divides $|Z(G)|$. Since no proper subgroup of G has order divisible by p. it is possible only when $Z(G) = G$, which is a contradiction to the fact that G is abelian.

6. Give examples of the following and justify your answers.

(a) Two elements $g, h \in G$ such that g and h are of finite order, but gh is of infinite order.
Solution Take $G = GL(n, \mathbb{C})$, the group of all n by n complex invertible matrices and the group operation is matrix multiplication. Take

$$g = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} \text{ and } h = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Clearly, g and h are of order 2. A simple computation yields that

$$(gh)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

Therefore, gh is of infinite order.

(b) An infinite group G, all of whose elements have finite order.
Solution Take $G = \mathbb{Z}_2 \times \mathbb{Z}_2 ... \times \mathbb{Z}_2$ Clearly, $|G|$ is infinite, but every element is of order atmost 2.
or Take $G = \mathbb{Q}/\mathbb{Z}$, clearly G is an infinite group. Let $a \in G$, then $a = m/n + \mathbb{Z}$ for some $m, n \in \mathbb{Z}$. it can be easily seen that the order of a is atmost n.

(c) A group G and subgroups H and K such that $H \trianglelefteq K$, $K \trianglelefteq G$ but $H \ntrianglelefteq G$
Solution Take $G = S_4$, $H = \langle (12)(34) \rangle$ and $K = \{(12)(34), (13)(42), (23)(41), e\}$. It can be easily seen that $H \trianglelefteq K$, $K \trianglelefteq G$. but $H \ntrianglelefteq G$, Since $gHg^{-1} \nsubseteq H$ for $g = (13) \in G$.

(d) A group G with normal subgroups H and K such that $H \cong K$ but $G/H \ncong G/K$.
Solution Take $G = \mathbb{Z}_2 \times \mathbb{Z}_4, H = \{(0,0),(0,2)\}$ and $K = \{(0,0),(1,0)\}$. Here $H \cong K$ but $G/H \ncong G/K$. Since every non-idnetity element of G/H is order 2 but there exists a non identity element $(1,1) \in G/K$ which is not of order 2. Hence G/H and G/K can not be isomorohic.

(e) A group G and a non-trivial subgroup N such that $G/N \cong G$.
Solution Take $G = \mathbb{Z} \times \mathbb{Z}$ and $N = \mathbb{Z} \times \{0\}$. Here, G/N is isomorphic to G.