1. $G$ is a cyclic group of order $n$ and $m|n$. Prove that there is a unique subgroup of order $m$ in $G$.

   **Solution**:

   Let $G =< a >$ be a cyclic group of order $n$. The cyclic subgroup $< a^{\frac{n}{m}} >$ is of order $m$, since
   $$< a^{\frac{n}{m}} >= \{1, a^{\frac{n}{m}}, a^{\frac{2n}{m}}, ..., a^{\frac{(m-1)n}{m}}\}$$
   Now for any subgroup $H$ of $G$ with $|H| = m$, $H =< a^k >$ for some $1 \leq k \leq n$. If we can show $a^k \in < a^{\frac{n}{m}} >$, then $< a^k > \subseteq < a^{\frac{n}{m}} >$, and together with $| < a^k > | = | < a^{\frac{n}{m}} > | = m$, we can conclude $H =< a^k >=< a^{\frac{n}{m}} >$.

   Now we will show $a^k \in < a^{\frac{n}{m}} >$: $|a^k| = m$, so $(a^k)^m = 1$, i.e., $a^{km} = 1$. This means $n|km$, there exists $b \in \mathbb{Z}$ such that $km = bn$. We have $k = \frac{n}{m} \times b$, so $a^k = (a^{\frac{n}{m}})^b$, $a^k \in < a^{\frac{n}{m}} >$.

2. $G$ is a group of order $p^2$, where $p$ is a prime. Prove that if $G$ has a unique subgroup of order $p$, then $G$ is cyclic.

   **Solution**:

   If the only cyclic subgroup of order $p$ is $< x >$, let $y \in G$ and $y \notin < x >$. $|y|$ divides $|G| = p^2$, $|y| \neq 1$ since it is not the identity, $|y| \neq p$ otherwise there will be another cyclic subgroup of order $p$, so $|y| = p^2$, $G =< y >$ is cyclic.

3. If $G$ is a finite group with $|G| > 1$, and the only subgroups of $G$ are $\{1\}$ and $G$, prove $G$ is a cyclic group with prime order.

   **Solution**: We first prove $G$ is a cyclic group. Take any $x \in G$ such that $x \neq 1$, the cyclic subgroup generated by $x$ is $< x >\neq \{1\}$, and the only subgroups of $G$ are $\{1\}$ and $G$, so $< x >= G$, we get $G$ is a cyclic group.

   Suppose $|G| = | < x > | = |x| = n$ is not prime, then there exists $k \in \mathbb{N}$ such that $1 < k < n$ and $k$ divides $n$. $(x^k)^{\frac{n}{k}} = x^n = 1$, so $| < x^k > | \leq \frac{n}{k} < n = |G|$, which means $< x^k >\neq G$. $1 < k < n = |x|$ implies $x^k \neq 1$, so $< x^k >\neq \{1\}$, so we get a subgroup $< x^k >$ which is not 1 or $G$, contradiction. We conclude $|G|$ is prime.

4. $f : G \longrightarrow G'$ is a homomorphism, $H'$ is a subgroup of $G'$, and $H = f^{-1}(H') = \{g \in G|f(g) \in H'\}$.

(i). Prove $\ker f \subseteq H$.

(ii). Prove $H$ is a subgroup of $G$.

(iii). If $H'$ is a normal subgroup of $G'$, is $H$ a normal subgroup of $G$? If yes, prove it; if no, provide a counter example.

**Solution**:

(i). For any $x \in \ker f$, $f(x) = 1' \in H'$ since $H'$ is a subgroup of $G'$, so $x \in H$, $\ker f \subseteq H$.

(ii). For any $a, b \in H$, $f(a) \in H'$ and $f(b) \in H'$, then $f(a^{-1}b) = f(a)^{-1}f(b) \in H'$, so $a^{-1}b \in H$, $H$ is a subgroup of $G$.

(iii). $H$ is a normal subgroup of $G$:

$H'$ is a normal subgroup of $G'$, so for any $h \in H$ and $g \in G$, $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H'$, which means $ghg^{-1} \in H$, $H$ is a normal subgroup of $G$.

5. $G$ is a group. $f : G \longrightarrow G$ is defined by $f(g) = g^2$. Prove that $f$ is a homomorphism if and only if $G$ is abelian.

   **Solution**: If $G$ is abelian, then for any $a, b \in G$:

$$f(ab) = (ab)^2 = abab = a^2b^2 = f(a)f(b)$$

   $f$ is a homomorphism.

   Conversely, if $f$ is a homomorphism, then for any $a, b \in G$,

$$a(ab)b = a^2b^2 = f(a)f(b) = f(ab) = (ab)^2 = a(ba)b$$

   by Cancellation Law, $ab = ba$. We conclude $G$ is abelian.

6. $\mathbb{Z}$ is the group of integers with addition as composition, and $G = \{\pm 1\}$ is the group of $\pm 1$ with multiplication.

   (i). For $a \in \mathbb{Z}$, let $f_a : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the function $f_a(x) = ax$ for any $x \in \mathbb{Z}$. Prove $Aut(\mathbb{Z}) = \{f_1, f_{-1}\}$.

   (ii). Let $G = \{\pm 1\}$ be the group with multiplication. Prove $F : Aut(\mathbb{Z}) \longrightarrow G$ defined by $F(f) = f(1)$ is an isomorphism.

   **Solution**:

   (i). First, it is easy to see $f_1 \in Aut(\mathbb{Z})$ and $f_{-1} \in Aut(\mathbb{Z})$. We need to show these are the only elements in $Aut(\mathbb{Z})$.

For any $f \in Aut(\mathbb{Z})$, $f$ is a homomorphism, then for any positive integer $k$, $f(k) = \phi(\underbrace{1 + ... + 1}_{k\text{-copies}}) = \underbrace{f(1) + ... + f(1)}_{k\text{-copies}} = kf(1)$, and $f(-k) = f(\underbrace{(-1) + ... + (-1)}_{k\text{-copies}}) = \underbrace{f(-1) + ... + f(-1)}_{k\text{-copies}} = kf(-1) = -kf(1)$. Thus we see $f(x) = f(1)x$ for any integer $x$, so $f = f_a$ with $a = f(1)$.

Also $f = f_a$ is bijective, by Homework 1, $a = \pm 1$. So $f = f_1$ or $f = f_{-1}$, we conclude $Aut(\mathbb{Z}) = \{f_1, f_{-1}\}$.

(ii). $F(f_1) = f_1(1) = 1$ and $F(f_{-1}) = f_{-1}(1) = -1$, so $F$ is bijective.

$F$ is a homomorphism since It is a homomorphism since for $f, f' \in Aut(\mathbb{Z})$, $F(f \circ f') = f \circ f'(1) = f(f'(1)) = f(1)f'(1) = F(f)F(f')$.

We conclude that $\Phi$ is an isomorphism.