1. $x$ is an element of order $n$ in a group $G$. $k$ is an integer such that the greatest common divisor of $k$ and $n$ is $d$. Prove $<x^k> = <x>$ if and only if $d = 1$

Solution:

If $d > 1$, then we see $(x^k)^\frac{n}{d} = x^{k\frac{n}{d}} = (x^n)^\frac{k}{n} = 1$, so by the definition of $|x^k|$, $| <x^k>| = |x^k| \leq \frac{n}{d} < n = | <x> |$, $<x^k> \neq <x>$.

If $d = 1$, it suffices to prove $x \in <x^k>$, which implies $<x> \subseteq <x^k>$, and $<x^k> \subseteq <x>$ is trivial, then we can conclude $<x> = <x^k>$. $d = 1$ implies there exists integers $p, q$ such that $np + kq = 1$. Thus $x = x^{np+kq} = x^{np}x^{kq} = x^{kq} = (x^k)^q$, we see $x \in <x^k>$.

2. $\phi : G \rightarrow G'$ and $\phi' : G' \rightarrow G''$ are homomorphisms. Prove $\phi' \circ \phi : G \rightarrow G''$ is also a homomorphism.

Solution:

For any $a, b \in G$, since $\phi, \phi'$ are homomorphisms:

$\phi' \circ \phi(ab) = \phi'(\phi(ab)) = \phi'(\phi(a)\phi(b)) = \phi'\phi(a)\phi'\phi(b) = (\phi' \circ \phi(a))(\phi' \circ \phi(b))$

So $\phi' \circ \phi$ is a homomorphism

3. Prove that $f : GL_n(\mathbb{R}) \rightarrow GL_n(\mathbb{R})$ defined by $f(A) = (A^T)^{-1}$ is an automorphism.

Solution:

$f$ is a homomorphism since for any $A, B \in GL_n(\mathbb{R})$, $f(AB) = ((AB)^T)^{-1} = (B^T A^T)^{-1} = (A^T)^{-1} (B^T)^{-1} = f(A)f(B)$.

$f$ is bijective since $f$ is the inverse function of itself: $f \circ f(A) = f((A^T)^{-1}) = (((A^T)^{-1})^T)^{-1} = ((A^T)^{-1}) = (A^T)^T = A$. So $f \circ f$ is the identity function on $GL_n(\mathbb{R})$

4. $H$ is a subgroup of $G$ and $N$ is a normal subgroup of $G$. Prove $H \cap N$ is a normal subgroup of $H$.

Solution:

First we see $H \cap N$ is a subgroup of $H$, using the same method of argument as that in Question 6, Homework II.

For any $x \in H \cap N$ and any $h \in H$, since $N$ is normal in $G$, $h x h^{-1} \in N$. $x \in H \cap N \subseteq H$ and $h \in H$ implies $h x h^{-1} \in H$. Thus $h x h^{-1} \in H \cap N$, $H \cap N$ is a normal subgroup of $H$. 

1
5. The group $SO_2$ is the set \( \{ A \in O_2(\mathbb{R}) | \det(A) = 1 \} \) with the law of composition to be matrix multiplication.

(i). Show that each element in $SO_2$ can be written as

\[
\begin{bmatrix}
\cos x & -\sin x \\
\sin x & \cos x
\end{bmatrix}
\]

for some $x \in \mathbb{R}$.

(ii). Show that the following map $f$ is a group homomorphism, and find its kernel and image

\[
f : \mathbb{R} \longrightarrow SO_2 \\
x \mapsto \begin{bmatrix}
\cos x & -\sin x \\
\sin x & \cos x
\end{bmatrix}
\]

Solution:

(i). Assume \( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SO_2 \), then \( \det \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = ad - bc = 1 \), so

\[
\begin{bmatrix}
d & -b \\
-c & a
\end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix}
\]

So $a = d$ and $b = -c$, the matrix becomes \( \begin{bmatrix} a & -c \\ c & a \end{bmatrix} \), with $a^2 + c^2 = 1$. We know for a pair of real numbers $a, c$ satisfying $a^2 + c^2 = 1$, the angle $x$ whose terminal edge passing through $(a, c)$ has $\cos x = a$ and $\sin x = c$, hence the matrix can be written as

\[
\begin{bmatrix}
\cos x & -\sin x \\
\sin x & \cos x
\end{bmatrix}
\]

(ii). $f$ is a homomorphism since:

\[
f(x)f(y) = \begin{bmatrix}
\cos x & -\sin x \\
\sin x & \cos x
\end{bmatrix} \begin{bmatrix}
\cos y & -\sin y \\
\sin y & \cos y
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\cos x \cos y - \sin x \sin y & -\cos x \sin y - \sin x \cos y \\
\sin x \cos y + \cos x \sin y & -\sin x \sin y + \cos x \cos y
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\cos(x + y) & -\sin(x + y) \\
\sin(x + y) & \cos(x + y)
\end{bmatrix}
\]

\[= f(x + y)\]
\[ \ker(f) = \{ x \in \mathbb{R} \mid \begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \} = \{ x \in \mathbb{R} \mid \cos x = 1, \sin x = 0 \} = 2\pi \mathbb{Z} \]

\[ \text{Im}(f) = SO_2 \] since by (i), every matrix in \(SO_2\) can be written as \[
\begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix}
\] for some \(x \in \mathbb{R}\).

6. Let \( G = \{1, -1\} \), the group of two elements with law of composition to be multiplication. \( \mathbb{Z} \) is the group of integers with law of composition to be addition.

(i). If \( \phi : \mathbb{Z} \rightarrow \mathbb{Z} \) is a homomorphism, prove the map \( \phi \) is determined by the value \( \phi(1) \).

(ii). If \( \phi : \mathbb{Z} \rightarrow \mathbb{Z} \) is an automorphism, prove \( \phi(1) = 1 \) or \( \phi(1) = -1 \).

(iii). Prove \( \Phi : \text{Aut}(\mathbb{Z}) \rightarrow G = \{1, -1\} \) defined by \( \Phi(\phi) = \phi(1) \) is an isomorphism.

**Solution:**

(i). If \( \phi : \mathbb{Z} \rightarrow \mathbb{Z} \) is a homomorphism, then for any positive integer \( k \), \( \phi(k) = \phi(1 + \ldots + 1) = \phi(1) + \ldots + \phi(1) = k\phi(1) \), and \( \phi(-k) = \phi((-1) + \ldots + (-1)) = \phi(-1) + \ldots + \phi(-1) = k\phi(-1) = -k\phi(1) \). Thus we see \( \phi(n) = n\phi(1) \) for any integer \( n \), i.e. the function \( \phi \) is determined by \( \phi(1) \).

(ii). By (i) we know \( \phi(n) = n\phi(1) \), and it is obvious from this expression that \( \phi \) is bijective only when \( \phi(1) = 1 \) or \( \phi(1) = -1 \).

(iii). By (i), (ii), we see \( \text{Aut}(\mathbb{Z}) \) consists of two automorphisms, \( \phi_1(n) = n \) and \( \phi_{-1}(n) = -n \). So \( \Phi(\phi) = \phi(1) \) is a bijection. It is a homomorphism since for \( \phi, \phi' \in \text{Aut}(\mathbb{Z}) \), \( \Phi(\phi \circ \phi') = \phi \circ \phi'(1) = \phi(\phi'(1)) = \phi(1)\phi'(1) = \Phi(\phi)\Phi(\phi') \). We conclude that \( \Phi \) is an isomorphism.

7. \( G \) is a group and \( H \) is a subgroup of \( G \).

(i). Prove that for any \( g \in G \), \( gHg^{-1} = \{ghg^{-1} \in G \mid h \in H \} \) is a subgroup of \( G \).
(ii). $k$ is a positive integer. Prove that if $H$ is the only subgroup of $G$ that has order $k$, then $H$ is normal in $G$.

Solution:

(i). For any $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$, $(gh_1g^{-1})^{-1}(gh_2g^{-1}) = (gh_1^{-1}g^{-1})(gh_2g^{-1}) = g(h_1^{-1}h_2)g^{-1} \in gHg^{-1}$, so $gHg^{-1}$ is a subgroup of $G$.

(ii). for any $g \in G$, there is a bijection: $\phi_g : H \longrightarrow gHg^{-1}$ defined by $\phi_g(h) = ghg^{-1}$. So the groups $H$ and $gHg^{-1}$ have the same order. Then by the assumption, $H$ is the only subgroup with order $k$, so $|H| = |gHg^{-1}|$ implies $H = gHg^{-1}$. We conclude $H$ is normal.