1. Suppose that $G$ is a finite group, with $H$ a subgroup of $G$ and $g$ an element of $G$. Suppose that $k$ is the smallest positive integer so that $g^k \in H$. Prove that $k | o(g)$. Hint: Use the division algorithm to write $o(g) = kq + r$, and show that $r = 0$.

**Answer:** Write $o(g) = kq + r$, with $0 \leq r < k$. We have $g^{o(g)} = e \in H$, and $g^k \in H$. Therefore, $e = (g^k)^q g^r \in H$, so $g^r = (g^k)^{-q} \in H$. But $r < k$, and $k$ is the smallest positive integer so that $g^k \in H$. The conclusion is that $r = 0$ and then $k | o(g)$.

2. Suppose that $G$ is a group, $H$ a subgroup of $G$, and $N \triangleleft G$. Show that $H \cap N \triangleleft H$.

**Answer:** We know that $H \cap N$ is a subgroup from earlier homework, so the only issue is proving normality. Suppose that $h \in H$ and $n \in H \cap N$. We must show that $hnh^{-1} \in H \cap N$. Because $h \in H$ and $n \in H$, we know that $hnh^{-1} \in H$. Our remaining problem is to show that $hnh^{-1} \in N$, but that follows because $N \triangleleft G$ and $h \in G$.

3. Suppose that $\phi : G_1 \to G_2$ is a homomorphism, and $N_2 \triangleleft G_2$. Let

$$N_1 = \{ g_1 \in G_1 : \phi(g_1) \in N_2 \}.$$

(1) Show that $N_1 \triangleleft G_1$.

(2) Show that ker$(\phi) \subseteq N_1$.

**Answer:** (1) We showed on the examination that $N_1$ is a subgroup of $G_1$, so normality is the only remaining problem. Take $g_1 \in G_1$ and $n_1 \in N_1$, so that $\phi(n_1) = n_2 \in N_2$, and we must show that $g_1n_1g_1^{-1} \in N_1$. We have $\phi(g_1n_1g_1^{-1}) = \phi(g_1)\phi(n_1)\phi(g_1)^{-1} = \phi(g_1)n_2\phi(g_1)^{-1} \in N_2$. Therefore, $g_1n_1g_1^{-1} \in N_1$.

(2) If $k \in \ker(\phi)$, then $\phi(k) = e_2 \in N_2$, and therefore $k \in N_1$.

4. Suppose that $G$ is a finite group with subgroups $A$ and $B$. Suppose that $o(A) > o(B) > \sqrt{o(G)}$. Prove that $A \cap B \neq \{e\}$.

**Answer:** Suppose that $A \cap B = \{e\}$. We compute the number of elements in $AB = \{ab \mid a \in A, b \in B\}$. If $a_1b_1 = a_2b_2$, then $a_2^{-1}a_1 = b_2b_1^{-1} \in A \cap B = \{e\}$, implying that $a_1 = a_2$ and $b_1 = b_2$. This shows that $o(AB) = o(A)o(B) > \sqrt{o(G)}\sqrt{o(G)} = G$. But $AB \subseteq G$, so we have a contradiction. The conclusion is that $A \cap B \neq \{e\}$.

5. Suppose that $G_1$ is a group, and $G = G_1 \times G_1$. Let $D = \{ (a,a) \in G : a \in G_1 \}$.

(1) Show that $D$ is a subgroup of $G$.

(2) Suppose that $D \triangleleft G$. Prove that $G_1$ is abelian.

**Answer:** (1) First, $(e,e) \in D$, so $D$ contains the identity element in $G$.

Second, if $(a,a), (b,b) \in D$, then $(a,a)(b,b) = (ab,ab) \in D$.

Third, if $(a,a) \in D$, then $(a,a)^{-1} = (a^{-1},a^{-1}) \in D$.

This shows that $D$ is a subgroup.

(2) Suppose that $D \triangleleft G$. Take two elements $a,b \in G_1$, and we must show that $ab = ba$. The element $(a,a) \in D$, and the element $(e,b) \in G$, and therefore $(e,b)(a,a)(e,b)^{-1} \in D$. We
compute \((e, b)(a, a)(e, b)^{-1} = (a, bab^{-1})\). But if \((a, bab^{-1}) \in D\), then \(a = bab^{-1}\), or \(ab = ba\), which proves that \(G_1\) is abelian.

6. If \(M \triangleleft G\), \(N \triangleleft G\), and \(M \cap N = \{e\}\), show that for \(m \in M\), \(n \in N\), \(mn = nm\). Hint: Show that \(mnm^{-1}n^{-1} \in M \cap N\).
   
   Answer: Note that \(mnm^{-1}n^{-1} = (mnm^{-1})n^{-1}\). Because \(N \triangleleft G\), we have \(mnm^{-1} \in N\), and therefore \((mnm^{-1})n^{-1} \in N\).

   Note as well that \(mnm^{-1}n^{-1} = m(nm^{-1}n^{-1})\). Because \(M \triangleleft G\), we have \(nm^{-1}n^{-1} \in M\) (because \(m^{-1} \in M\)). Therefore, \(m(nm^{-1}n^{-1}) \in M\).

   So \(mnm^{-1}n^{-1} \in M \cap N = \{e\}\), so \(mnm^{-1}n^{-1} = e\), which in turn says that \(mn = nm\).

7. Recall that an automorphism of a group \(G\) is an isomorphism \(\phi : G \to G\). Find all automorphisms of the group \(\mathbb{Z}/8\mathbb{Z}\). To define an automorphism, you can show explicitly where it maps each of the 8 elements of \(\mathbb{Z}/8\mathbb{Z}\). For example, the identity isomorphism is

\[
\begin{align*}
0 &\to 0 \\
1 &\to 1 \\
2 &\to 2 \\
\text{id} &\to 3 \\
4 &\to 4 \\
5 &\to 5 \\
6 &\to 6 \\
7 &\to 7
\end{align*}
\]

Answer: If \(\phi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}\) is a homomorphism, we know that \(\phi(0) = 0\), so we only have to define \(\phi\) for the remaining 7 elements of \(\mathbb{Z}/8\mathbb{Z}\). We also know that if \(\phi\) is an injection and \(x \neq 0\), then \(\phi(x) \neq 0\), because \(\phi(0) = 0\).

Now, if \(\phi(1) = 2\), then \(\phi\) is not an injection, because \(\phi(4) = \phi(1 + 1 + 1 + 1) = \phi(1) + \phi(1) + \phi(1) + \phi(1) = 2 + 2 + 2 + 2 = 0\). Similarly, if \(\phi(1) = 4\), then \(\phi\) is not an injection, because \(\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 4 + 4 = 0\). Finally, if \(\phi(1) = 6\), then \(\phi(4) = \phi(1 + 1 + 1 + 1) = \phi(1) + \phi(1) + \phi(1) + \phi(1) = 6 + 6 + 6 + 6 = 0\).

The remaining possibilities are \(\phi_3(1) = 3\), meaning that \(\phi_3(x) = 3x\); \(\phi_5(1) = 5\), meaning \(\phi_5(x) = 5x\); and \(\phi_7(1) = 7\), meaning \(\phi_7(x) = 7x\). Because \(\phi_c(x + y) = c(x + y) = cx + cy = \phi_c(x) + \phi_c(y)\), we know that these three functions are homomorphisms. Because \(\phi_3 \circ \phi_3 = \phi_5 \circ \phi_5 = \phi_7 \circ \phi_7 = \text{id}\), we know that each of these three functions is invertible—in fact, each is its own inverse—and therefore each must be a bijection.