There are 3 problems with a total of 9 sections. This is a closed book test. Any student caught cheating will receive a score of zero. In any of the 9 sections, you may assume the results from the other sections.

1. Consider a subgroup $H \leq G$ and two elements $a, b \in G$.
   (a) **Prove** that $aH = bH$ implies $a^{-1}b \in H$. (Hint: Note that $b \in bH$.)

   *Proof.* Suppose that $aH = bH$. Since $b \in bH = aH$, there exists $h \in H$ such that $b = ah$. But then $a^{-1}b = h \in H$. □

   (b) **Prove** that $a^{-1}b \in H$ implies $aH = bH$. (You need $aH \subseteq bH$ and $bH \subseteq aH$.)

   *Proof.* Suppose that $a^{-1}b = h \in H$. In order to show $aH = bH$ we must show $aH \subseteq bH$ and $bH \subseteq aH$. So consider an arbitrary element $ak \in aH$ with $k \in H$. Then we have $ak = (bh)^{-1}k = b(h^{-1}k) \in bH$, hence $aH \subseteq bH$. The proof of $bH \subseteq aH$ is similar. □

2. Let $G = \langle g \rangle$ be a cyclic group with a subgroup $H \leq G$.
   (a) **Prove** that $\varphi(n) := g^n$ defines a surjective homomorphism $\varphi : \mathbb{Z} \to G$.

   *Proof.* By definition, every element of $G = \langle g \rangle$ has the form $g^n$ for some $n \in \mathbb{Z}$, hence the map is surjective. It is a homomorphism because $\varphi(m + n) = g^{m+n} = g^m g^n = \varphi(m) \varphi(n)$ for all $m, n \in \mathbb{Z}$. □

   (b) **Prove** that $\varphi^{-1}(H) := \{n \in \mathbb{Z} : \varphi(n) \in H\}$ is a subgroup of $\mathbb{Z}$. It follows that $\varphi^{-1}(H) = a\mathbb{Z}$ for some $a \in \mathbb{Z}$ (you don’t need to prove this).

   *Proof.* First note that $0 \in \varphi^{-1}(H)$ since $\varphi(0) = g^0 = 1_G \in H$. Next, suppose that $n \in \varphi^{-1}(H)$; i.e. $\varphi(n) \in H$. But then $\varphi(-n) = \varphi(n)^{-1}$ is also in $H$, hence $-n \in \varphi^{-1}(H)$. Finally, let $m, n \in \varphi^{-1}(H)$; i.e. $\varphi(m)$ and $\varphi(n)$ are in $H$. But then $\varphi(m + n) = \varphi(m) \varphi(n)$ is also in $H$, hence $m + n \in \varphi^{-1}(H)$. □

   (c) **Prove** that $H = \langle g^a \rangle$ and hence $H$ is cyclic.

   *Proof.* Since $\varphi^{-1}(H) \leq \mathbb{Z}$, we have $\varphi^{-1}(H) = a\mathbb{Z}$ for some $a \in \mathbb{Z}$. Then by definition we have $\varphi(a\mathbb{Z}) = H$. That is, every element of $H$ has the form $\varphi(ak) = g^{ak} = (g^a)^k$ for some $k \in \mathbb{Z}$. We conclude that $H = \langle g^a \rangle$. (In particular, $H$ is cyclic.) □

3. Consider two finite subgroups $H, K \leq G$ with $K \leq G$ a normal subgroup.
   (a) **Prove** that $HK := \{hk : h \in H, k \in K\}$ is a subgroup of $G$.

   *Proof.* First note that $1_G \in HK$ because $1_G \in H \cap K$, hence $1_G = 1_G \cdot 1_G \in HK$. Next, consider $g \in HK$. Then there exist $h \in H, k \in K$ such that $g = hk$. We wish to show that $g^{-1} = k^{-1}h^{-1} \in HK$. But $k^{-1}h^{-1} \in Kh^{-1} = h^{-1}K$ means there exists $k' \in K$ such that $k^{-1}h^{-1} = h^{-1}k' \in HK$. Finally, consider $h_1k_1$ and $h_2k_2$ in $HK$. We wish to show that $h_1k_1h_2k_2 \in HK$. Indeed, since $k_1h_2 \in Kh_2 = h_2K$, there exists $k'' \in K$ such that $k_1h_2 = h_2k''$. Hence $h_1k_1h_2k_2 = h_1h_2k''k_2 \in HK$. □

   (b) Since $K \leq HK$ we can form the quotient group $(HK)/K$. **Prove** that the map $\varphi(h) := hK$ is a surjective homomorphism $\varphi : H \to (HK)/K$. 
Proof. The map is a homomorphism since \( \varphi(ab) = (ab)K = (aK)(bK) = \varphi(a)\varphi(b) \).

Then note that each coset in \( HK/K \) looks like \((hk)K = hK\) for some \( h \in H \), \( k \in K \). In this case we have \( \varphi(h) = hK = (hk)K \), so the map is surjective. \( \square \)

(c) **Prove** that the kernel of \( \varphi \) is \( H \cap K \).

**Proof.** Note that \( \varphi(h) = hK = K \) if and only if \( h \in K \). Hence \( h \in H \) is in the kernel if and only if \( h \) is also in \( K \). We conclude that \( \ker \varphi = H \cap K \). (In particular, this proves that \( H \cap K \triangleleft H \).) \( \square \)

(d) Use the **First Isomorphism Theorem** and **Lagrange’s Theorem** to prove that

\[
|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.
\]

**Proof.** By the First Isomorphism Theorem we have \( H/\ker \varphi \approx \text{im} \varphi \), which by parts (b) and (c) says that \( H/(H \cap K) \approx (HK)/K \). Applying Lagrange’s Theorem to both sides gives \( |H|/|H \cap K| = |HK|/|K| \). Then multiply both sides by \( |K| \). \( \square \)