1. (7 points) STATE and PROVE the Chinese Remainder Theorem.

The Chinese Remainder Theorem. Suppose $m$ and $n$ are relatively prime non-zero integers. Prove that the groups $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ are isomorphic.

Define $\varphi: \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $\varphi(a) = (a + m\mathbb{Z}, a + n\mathbb{Z})$ for all $a \in \mathbb{Z}$. We show that $\varphi$ is a group homomorphism. Take $a$ and $b$ in $\mathbb{Z}$. We see that $\varphi(a+b) = (a+b+m\mathbb{Z}, a+b+n\mathbb{Z}) = (a+m\mathbb{Z}, a+n\mathbb{Z}) + (b+m\mathbb{Z}, b+n\mathbb{Z}) = \varphi(a) + \varphi(b)$.

To show that $\varphi$ is onto, we use the Lemma from Number Theory which says that the greatest common divisor of any two non-zero integers is equal to a linear combination (with integer coefficients) of the two integers. In particular, there exist integers $r$ and $s$ with $rm + sn = 1$.

Let $(a + m\mathbb{Z}, b + n\mathbb{Z})$ be an arbitrary element of $\mathbb{Z}_m \times \mathbb{Z}_n$. Observe that $\varphi(asn + brom) = (a + m\mathbb{Z}, b + n\mathbb{Z})$. It is clear that $mn\mathbb{Z}$ is contained in the kernel of $\varphi$. We show that $\ker \varphi \subseteq mn\mathbb{Z}$. Take $a \in \ker \varphi$. It is clear that $a \in n\mathbb{Z}$ and $a \in m\mathbb{Z}$. Multiply (*) by $a$ to see that $a \in mn\mathbb{Z}$. The First Isomorphism Theorem says that $\mathbb{Z}_{\ker \varphi}$ is isomorphic to $\text{im} \varphi$. In other words, $\mathbb{Z}_{mn\mathbb{Z}}$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$.

2. (8 points) STATE and PROVE the First Isomorphism Theorem.

The First Isomorphism Theorem. If $\varphi: G \to G'$ is a group homomorphism, then $\varphi: G/\ker \varphi \to \text{im} \varphi$, which is given by $\varphi(g \ker \varphi) = \varphi(g)$, is a group isomorphism.

We first observe that $\varphi$ is a well-defined function. Suppose $g_1$ and $g_2$ are in $G$ and $g_1 \ker \varphi$ and $g_2 \ker \varphi$ are equal cosets. It follows that $g_1 = g_2k$ for some $k \in \ker \varphi$; and therefore, $\varphi(g_1) = \varphi(g_2k) = \varphi(g_2)\varphi(k) = \varphi(g_2)\text{id} = \varphi(g_2)$. We see that $\varphi(g_1 \ker \varphi) = \varphi(g_2 \ker \varphi)$, as we desired.
We observe that \( \varphi \) is a homomorphism. If \( g_1 \) and \( g_2 \) are in \( G \), then
\[
\varphi(g_1 \ker \varphi) \varphi(g_2 \ker \varphi) = \varphi(g_1) \varphi(g_2) = \varphi(g_1 g_2) = \varphi(g_1 g_2 \ker \varphi).
\]

We observe that \( \varphi \) is onto. Take an arbitrary element \( g' \) of the target of \( \varphi \), which is \( \text{im} \varphi \). It follows that \( g' = \varphi(g_1) \) for some \( g_1 \in G_1 \); and therefore, \( g' = \varphi(g_1 \ker \varphi) \).

We observe that \( \varphi \) is one-to-one. Take \( g_1 \) and \( g_2 \) in \( G_1 \) with \( \varphi(g_1 \ker \varphi) = \varphi(g_2 \ker \varphi) \). It follows that \( \varphi(g_1) = \varphi(g_2) \); so, \( \varphi(g_1 g_2^{-1}) = \text{id} \). Thus, \( g_1 g_2^{-1} \in \ker \varphi \) and the cosets \( g_1 \ker \varphi \) and \( g_2 \ker \varphi \) are equal.

3. (7 points) Are the groups \( \mathbb{Z}_6 \times \mathbb{Z}_5 \) and \( \mathbb{Z}_2 \times \mathbb{Z}_15 \) isomorphic? PROVE your answer.

YES. According to the Chinese Remainder Theorem each group is isomorphic to \( \mathbb{Z}_30 \).

4. (7 points) Are the groups \( \mathbb{Z}_4 \times \mathbb{Z}_4 \) and \( \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \) isomorphic? PROVE your answer.

NO. The group on the left has 12 elements of order 4, 3 elements of order 2, and 1 element of order 1. The group on the right has 8 elements of order 4, 7 elements of order 2, and 1 element of order 1. Every group isomorphism induces bijection between the elements of order \( \ell \) in the domain and the elements of order \( \ell \) in the target for all non-negative integers \( \ell \).

5. (7 points) Are the groups \( (\mathbb{R}, +) \) and \( (\mathbb{R}^{\text{pos}}, \times) \) isomorphic? PROVE your answer. (I am using \( \mathbb{R}^{\text{pos}} \) to represent the set of positive real numbers.)

YES. Define \( \phi: \mathbb{R} \to \mathbb{R}^{\text{pos}} \) by \( \phi(a) = 10^a \). Observe that
\[
\phi(a + b) = 10^{a+b} = 10^a 10^b = \phi(a) \phi(b).
\]

The map \( \phi \) is onto because if \( r \in \mathbb{R}^{\text{pos}} \), then \( \log_{10} r \in \mathbb{R} \) and \( \phi(\log_{10} r) = r \).

The map \( \phi \) is one-to-one, because if \( a \) and \( b \) are in \( \mathbb{R} \) with \( \phi(a) = \phi(b) \), then \( 10^a = 10^b \) and we may apply \( \log_{10} \) to both sides to see that \( a = b \).

6. (7 points) Let \( \phi: G_1 \to G_2 \) and \( \theta: G_2 \to G_3 \) be group homomorphisms. Prove that \( \theta \circ \phi \) is a group homomorphism.

Take \( g \) and \( g' \) in \( G_1 \). Observe that
\[
(\theta \circ \phi)(gg') = \theta(\phi(gg')) = \theta(\phi(g)\phi(g')) = \theta(\phi(g))\theta(\phi(g')) = (\theta \circ \phi)(g)(\theta \circ \phi)(g').
\]
7. (7 points) Suppose that $S$ and $T$ are sets and $\phi: S \to T$ and $\theta: T \to S$ are functions with $\theta \circ \phi$ equal to the identity function on $S$.

(a) Does $\phi$ have to be one-to-one? PROVE or give a COUNTEREXAMPLE.

YES. Take $s$ and $s'$ in $S$ with $\phi(s) = \phi(s')$. Apply $\theta$ to each side to get:

$$s = \theta(\phi(s)) = \theta(\phi(s')) = s'.$$

(b) Does $\theta$ have to be onto? PROVE or give a COUNTEREXAMPLE.

YES. Take $s \in S$. The hypothesis tells us that $\phi(s)$ is an element of $T$ and $\theta(\phi(s)) = s$. 