1. Let \( \phi \) be a ring homomorphism from \( R \) to \( S \). Prove that \( R/\ker(\phi) \) is isomorphic to \( \phi(R) \).

Proof by (Lilith, Lisa, Nathan M, Rob). Let \( \tau : R/\ker \phi \to \phi(R) \) be defined by \( \tau(r + \ker \phi) = \phi(r) \) for \( r \in R \). Let \( (r + \ker \phi), (r' + \ker \phi) \in R/\ker \phi \). Suppose \( r + \ker \phi = r' + \ker \phi \). Then, \( r \in (r + \ker \phi) = (r' + \ker \phi) \). So, \( r = r' + k_0 \) for some \( k_0 \in \ker \phi \), which implies that \( r - r' = k_0 \in \ker \phi \). Thus,

\[
\begin{align*}
\phi(r - r') &= 0_s \\
(\Rightarrow) \quad \phi(r) - \phi(r') &= 0_s & \text{by the definition of kernel} \\
(\Rightarrow) \quad \phi(r) - \phi(r') + \phi(r') &= 0_s + \phi(r') \\
(\Rightarrow) \quad \phi(r) + 0_s &= 0_s + \phi(r') & \text{by the additive inverse} \\
(\Rightarrow) \quad \phi(r) &= \phi(r') & \text{by the additive identity} \\
(\Rightarrow) \quad \tau(r + \ker \phi) &= \tau(r' + \ker \phi)
\end{align*}
\]

Therefore, \( \tau \) is well-defined. Notice,

\[
\begin{align*}
\tau((r + \ker \phi) + (r' + \ker \phi)) &= \tau((r + r') + \ker \phi) \\
&= \phi(r + r') \\
&= \phi(r) + \phi(r') & \text{since } \phi \text{ is a ring homomorphism} \\
&= \tau(r + \ker \phi) + \tau(r' + \ker \phi)
\end{align*}
\]

Also, note that

\[
\begin{align*}
\tau((r + \ker \phi)(r' + \ker \phi)) &= \tau(rr' + \ker \phi) \\
&= \phi(rr') \\
&= \phi(r)\phi(r') & \text{since } \phi \text{ is a ring homomorphism} \\
&= \tau(r + \ker \phi)\tau(r' + \ker \phi)
\end{align*}
\]

Therefore, \( \tau \) is a ring homomorphism. Let \( \tau(r + \ker \phi) = \tau(r' + \ker \phi) \). Then, \( \phi(r) = \phi(r') \). Thus, \( 0_s = \phi(r) - \phi(r') = \phi(r - r') \) since \( \phi \) is a ring homomorphism. So, \( r - r' \in \ker \phi \) which implies that \( r + \ker \phi = r' + \ker \phi \). Therefore, \( \tau \) is one-to-one.

Let \( y = \phi(r) \) for some \( r \in R \). So, \( \tau(r + \ker \phi) = \phi(r) = y \) and \( (r + \ker \phi) \in R/\ker \phi \). Therefore, \( \tau \) is onto. Thus, \( \tau \) is an isomorphism, and \( R/\ker \phi \cong \phi(R) \). \( \square \)

2. Recall a ring element is called idempotent if \( a^2 = a \). Prove that a ring homomorphism carries an idempotent to an idempotent.

Proof by (Anne, Zach, Linda, Jayna). Suppose \( \phi \) is a ring homomorphism from \( R \) to \( S \). Let \( a \in R \) where \( a^2 = a \). We want to show that \( \phi(a) = \phi(a)^2 \in S \).

Consider

\[
\begin{align*}
\phi(a)^2 &= \phi(a) \cdot \phi(a) \\
&= \phi(a \cdot a) & \text{since we have a ring homomorphism} \\
&= \phi(a^2) \\
&= \phi(a) & \text{since we know } a \text{ is an idempotent}.
\end{align*}
\]

Thus, \( \phi(a) = \phi(a)^2 \in S \), and a ring homomorphism carries an idempotent to an idempotent. \( \square \)
3. Suppose that $R$ and $S$ are commutative rings with unities. Let $\phi$ be a ring homomorphism from $R$ onto $S$ and let $A$ be an ideal of $S$.

(a) If $A$ is prime in $S$, show that $\phi^{-1}(A) = \{x \in R \mid \phi(x) \in A\}$ is prime in $R$.

(b) If $A$ is maximal in $S$, show that $\phi^{-1}(A)$ is maximal in $R$.

Proof by (Ron, Caitlyn, Nathan S, Derrek). (a) Let $A$ be prime in $S$. We first note that because $A$ is an ideal, we have from Property 4 of ring homomorphisms, that $\phi^{-1}(A)$ is also an ideal. Now, let $x, y \in R$. If $xy \in \phi^{-1}(A)$, then $\phi(xy) = \phi(x)\phi(y) \in A$. As $A$ is prime, we must have either $\phi(x) \in A$ or $\phi(y) \in A$. That is, either $x \in \phi^{-1}(A)$ or $y \in \phi^{-1}(A)$, and hence, $\phi^{-1}(A)$ is prime.

(b) Let $A$ be maximal in $S$. Now, because $A$ is maximal, we know that $S/A$ is a field. Let $\tau$ be a ring homomorphism from $R$ to $S/A$, where, for $r \in R$, $\tau(r) = \phi(r) + A$. Because $\phi$ is onto, all elements of $S$, $\phi(r)$, have a pre-image in $R$. So, $\tau(R) = S/A$. Now consider the mapping $\omega : R/\ker \tau \rightarrow \tau(R)$. $\ker \tau$ will be all those elements which get mapped to the zero element of $S/A$, namely $A$. Those elements which get mapped to $A$ are $\phi^{-1}(A)$. So the domain of $\omega$ is $R/\phi^{-1}(A)$, and the range, $\tau(R)$, is the same as $S/A$. By the first isomorphism theorem for rings, we have that $R/\phi^{-1}(A) \cong S/A$. Because $S/A$ is a field, it must also be the case then that $R/\phi^{-1}(A)$ is a field. But $R/\phi^{-1}(A)$ is an ideal iff. $\phi^{-1}(A)$ is maximal, and so $\phi^{-1}(A)$ must be maximal in $R$. 

4. Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z} \right\}$, and let $\phi$ be the mapping that takes $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ to $a - b$.

(a) Show that $\phi$ is a homomorphism.

(b) Determine the kernel of $\phi$.

(c) Show that $R/\ker(\phi)$ is isomorphic to $\mathbb{Z}$.

(d) Is $\ker(\phi)$ a prime ideal?

(e) Is $\ker(\phi)$ a maximal ideal?

Proof by (Robert, Sarah, Julia, Matthew). (a) In order to show that $\phi$ is a homomorphism, we must show that it is well-defined, preserves multiplication, and preserves addition.

- Suppose that $\begin{bmatrix} a & b \\ b & a \end{bmatrix} = \begin{bmatrix} a' & b' \\ b' & a' \end{bmatrix}$. Then $\begin{bmatrix} a & b \\ b & a \end{bmatrix} - \begin{bmatrix} a' & b' \\ b' & a' \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Observe $\phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} - \begin{bmatrix} a' & b' \\ b' & a' \end{bmatrix} \right) = \phi \left( \begin{bmatrix} a-a' & b-b' \\ b-b' & a-a' \end{bmatrix} \right) = \phi \left( \begin{bmatrix} a-a' & b-b' \\ b-b' & a-a' \end{bmatrix} \right) = (a-a') - (b-b') = (a-b) - (a'-b')$ and $\phi \left( \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right) = 0 - 0 = 0$. Thus $(a-b) - (a'-b') = 0$ which implies $a-b = a'-b'$. Therefore $\phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) = \phi \left( \begin{bmatrix} a' & b' \\ b' & a' \end{bmatrix} \right)$ and $\phi$ is well-defined.

- Now let $\begin{bmatrix} a & b \\ b & a \end{bmatrix}, \begin{bmatrix} c & d \\ d & c \end{bmatrix} \in R$. Then

  $\phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) \phi \left( \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) = (a-b)(c-d) = ac - bc - ad + bd = (ac + bd) - (ad + bc) = \phi \left( \begin{bmatrix} ac + bd & ad + bc \\ ad + bc & ac + bd \end{bmatrix} \right)$. Therefore $\phi$ preserves multiplication.
• Once again, let \[
\begin{bmatrix}
  a & b \\
  b & a \\
\end{bmatrix},
\begin{bmatrix}
  c & d \\
  d & c \\
\end{bmatrix} \in \mathbb{R}.
\]
Then
\[
\phi\left(\begin{bmatrix}
  a & b \\
  b & a \\
\end{bmatrix}\right) + \phi\left(\begin{bmatrix}
  c & d \\
  d & c \\
\end{bmatrix}\right) = (a - b) + (c - d) = (a + c) - (b + d) = \phi\left(\begin{bmatrix}
  a + c & b + d \\
  b + d & a + c \\
\end{bmatrix}\right).
\]
Therefore \(\phi\) preserves addition and is a homomorphism. 

(b) Recall that \(\ker \phi = \{r \in \mathbb{R} | \phi(r) = 0\}\). Thus we are looking for all elements of \(\mathbb{R}\) that map to \(a - b = 0\). Hence \(a = b\) and \(\ker \phi = \left\{ \begin{bmatrix} a \\ a \end{bmatrix} \big| a \in \mathbb{Z} \right\}\). 

(c) Observe that \(\phi(\mathbb{R}) = \mathbb{Z}\). Thus by the First Isomorphism Theorem for Rings (Problem 1), we have that \(\mathbb{R}/\ker \phi \cong \phi(\mathbb{R})\).

(d) Notice that \[
\begin{bmatrix}
  a & b \\
  b & a \\
\end{bmatrix},
\begin{bmatrix}
  c & d \\
  d & c \\
\end{bmatrix} = \begin{bmatrix}
  ac + bd & ad + bc \\
  ad + bc & ac + bd \\
\end{bmatrix}.\]
If \[
\begin{bmatrix}
  ac + bd & ad + bc \\
  ad + bc & ac + bd \\
\end{bmatrix} \in \ker \phi,
\]
we must have \(ac + bd = ad + bc\). Thus we would have \(ac - ad = bc - bd \Rightarrow a(c - d) = b(c - d)\). Since the integers are an integral domain, this implies that either \(a = b\) or \(c - d = 0 \Rightarrow c = d\). Therefore either \[
\begin{bmatrix}
  a & b \\
  b & a \\
\end{bmatrix} \text{ or } \begin{bmatrix}
  c & d \\
  d & c \\
\end{bmatrix} \in \ker \phi \text{ and } \ker \phi \text{ is a prime ideal}.
\]

(e) Recall the theorem: "Let \(R\) be a commutative ring with unity with an \(A\) and ideal of \(R\). Then \(R/A\) is a field iff \(A\) is maximal." Note that \(R\) is commutative since \[
\begin{bmatrix}
  a & b \\
  b & a \\
\end{bmatrix},
\begin{bmatrix}
  c & d \\
  d & c \\
\end{bmatrix} = \begin{bmatrix}
  ac + bd & ad + bc \\
  ad + bc & ac + bd \\
\end{bmatrix} = \begin{bmatrix}
  bc + ad & bd + ac \\
  bd + ac & bc + ad \\
\end{bmatrix} = \begin{bmatrix}
  a & b \\
  b & a \\
\end{bmatrix}.\]
But by part c we know that \(R/\ker \phi\) is isomorphic to \(\mathbb{Z}\) which is not a field, so \(R/\ker \phi\) is not a field. Thus by the theorem, we have that \(\ker \phi\) is not a maximal ideal.