Solutions to Homework 4

1. (a) Let $\phi: R \to S$ be an isomorphism. Prove that $r \in R$ is a zero-divisor if and only if $\phi(r)$ is a zero-divisor in $S$.

Solution: If $r$ is a zero-divisor in $R$, then $r \neq 0$ and there is some $r' \in R$ with $r' \neq 0$ and $rr' = 0$. Because $\phi$ is a homomorphism,

$$\phi(r)\phi(r') = \phi(rr') = \phi(0) = 0.$$ 

Because $\phi$ is injective, $\phi(r) \neq \phi(0)$ and $\phi(r') \neq \phi(0)$. Thus $\phi(r)$ is a zero-divisor in $S$.

For the reverse implication, we know from problem 3(b) last week that $\phi^{-1}: S \to R$ is also an isomorphism, so if $\phi(r)$ is a zero-divisor in $S$ then $r = \phi^{-1}(\phi(r))$ is a zero-divisor in $R$.

(b) Give an example to show that the conclusion of part (a) may fail if $\phi$ is only a homomorphism. Indicate where your proof from part (a) breaks down if $\phi$ is not a bijection.

Solution: Let $\phi: \mathbb{Z}_4 \to \mathbb{Z}_2$ be the map given by $\phi(\bar{a}) = \bar{a}$, where (unfortunately) the two bars mean different things. In $\mathbb{Z}_4$ we have $2 \cdot 2 = 0$, so 2 is a zero-divisor. But $\phi(2) = 2 = 0$ in $\mathbb{Z}_2$, so $\phi(2)$ is not a zero-divisor.

The places in part (a) where I used the fact that $\phi$ is a bijection are indicated in blue.

(c) Let $\phi: R \to S$ be an isomorphism. Prove that $r \in R$ is a unit if and only if $\phi(r)$ is a unit in $S$.

Solution: If $r$ is a unit in $R$, then there is some $r' \in R$ with $rr' = 1$. Because $\phi$ is a homomorphism,

$$\phi(r)\phi(r') = \phi(rr') = \phi(1) = 1.$$ 

Thus $\phi(r)$ is a unit in $S$.

For the reverse implication, $\phi^{-1}$ is also an isomorphism, so if $\phi(r)$ is a unit in $S$ then $r = \phi^{-1}(\phi(r))$ is a unit in $R$. 
(d) Give an example to show that the conclusion of part (c) may fail if \( \phi \) is only a homomorphism. Indicate where your proof from part (c) breaks down if \( \phi \) is not a bijection.

**Solution:** Let \( \phi : \mathbb{Z} \to \mathbb{Q} \) be the inclusion map. Then 2 is not a unit in \( \mathbb{Z} \), but \( \phi(2) = 2 \) is a unit in \( \mathbb{Q} \).

Or for an example that is surjective rather than injective, let \( \phi : \mathbb{Q}[x] \to \mathbb{Q} \) be the map \( \phi(f) = f(1) \). Then \( x \) is not a unit in \( \mathbb{Q}[x] \), but \( \phi(x) = 1 \) is a unit in \( \mathbb{Q} \).

The place in part (a) where I used the fact that \( \phi \) is a bijection is indicated in blue.

2. (a) Prove that \( \mathbb{Z}_4 \) is not isomorphic to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

**Solution:** First we observe that \( \mathbb{Z}_4 \) has two units, namely 1 and 3, and one zero-divisor, namely 2. On the other hand, \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) has one unit, namely \((1, 1)\), and two zero-divisors, namely \((1, 0)\) and \((0, 1)\), because \((1, 0) \cdot (0, 1) = (0, 0)\).

Suppose that \( \phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \) were an isomorphism. Then \( \phi(3) \) would be a unit different in \( \mathbb{Z}_2 \times \mathbb{Z}_2 \), and it would be different from \( \phi(1) = (1, 1) \); but that is the only unit in \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

Or here’s another proof. Suppose that \( \phi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \) is a homomorphism. Then

\[
\begin{align*}
\phi(0) &= (0, 0) \\
\phi(1) &= (1, 1) \\
\phi(2) &= \phi(1) + \phi(1) = (1, 1) + (1, 1) = (0, 0).
\end{align*}
\]

Thus we see that \( \phi(0) = \phi(2) \), so \( \phi \) is not injective.

(b) Prove that \( \mathbb{Z}_2[x]/\langle x^2 \rangle \) is not isomorphic to \( \mathbb{Z}_4 \) or \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).

**Solution:** The ring \( \mathbb{Z}_2[x]/\langle x^2 \rangle \) has four elements, the equivalence classes of

\[
\begin{align*}
0 &\quad 1 \\
x &\quad x + 1
\end{align*}
\]

modulo \( \langle x^2 \rangle \). Of these, 1 and \( x + 1 \) are units, because

\[
(x + 1)^2 = x^2 + 2x + 1 = 0 + 0 + 1 = 1,
\]

and \( x \) is a zero-divisor, because \( x^2 = 0 \).

Now if \( \phi : \mathbb{Z}_2[x]/\langle x^2 \rangle \to \mathbb{Z}_2 \times \mathbb{Z}_2 \) were an isomorphism, then \( \phi(x + 1) \) would be a unit in \( \mathbb{Z}_2 \times \mathbb{Z}_2 \), and it would be different from \( \phi(1) = (1, 1) \), but again that’s the only unit in \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).
If $\phi: \mathbb{Z}_4 \to \mathbb{Z}_2[x]/\langle x^2 \rangle$ is a homomorphism then as in part (b) we find that $\phi(2) = \phi(0)$, so $\phi$ is not injective.

(c) Prove that $\mathbb{Z}_2[y]/\langle y^2 + y + 1 \rangle$ is not isomorphic to any of the three rings above.

**Solution:** We observe $\mathbb{Z}_2[y]/\langle y^2 + y + 1 \rangle$ contains three units and no zero-divisors, because

$$y(y + 1) = y^2 + y = 1.$$ 

Or we could say that $y^2 + y + 1$ is irreducible in $\mathbb{Z}_2[y]$, so the quotient ring is a field. But if $\mathbb{Z}_2[y]/\langle y^2 + y + 1 \rangle$ were isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_2[x]/\langle x^2 \rangle$ then it would have zero-divisors.

(d) Prove that $\mathbb{Z}_2[z]/\langle z^2 + z \rangle$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

**Hint:** Cook up a suitable homomorphism $\phi: \mathbb{Z}_2[z] \to \mathbb{Z}_2 \times \mathbb{Z}_2$, and apply the first isomorphism theorem. You can reuse some ideas from problem 1(c) on last week’s homework.

**Solution:** Let $\phi: \mathbb{Z}_2[z] \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be defined by

$$\phi(f) = (f(0), f(1)).$$

Just as on problem 1(c) last week, this is a homomorphism. A polynomial $f \in \mathbb{Z}_2[z]$ is in the kernel of $\phi$ if and only if $f(0) = 0$ and $f(1) = 0$. By the root-factor theorem, this holds if and only if $z \mid f$ and $z + 1 \mid f$. Because $\gcd(z, z + 1) = 1$, this holds if and only if $z(z + 1) \mid f$, that is, if and only if $f \in \langle z^2 + z \rangle$.

Or you could just write down a bijection

$$0 \leftrightarrow (0, 0)$$
$$1 \leftrightarrow (1, 1)$$
$$z \leftrightarrow (1, 0)$$
$$z + 1 \leftrightarrow (0, 1),$$

and check (somewhat tediously) that it respects addition and multiplication.
(e) Optional: Prove that \( \mathbb{Z}_2[w]/\langle w^2 + 1 \rangle \) is isomorphic to \( \mathbb{Z}_2[x]/\langle x^2 \rangle \).

**Solution:** Let \( \phi: \mathbb{Z}_2[w] \to \mathbb{Z}_2[x]/\langle x^2 \rangle \) be the map \( \phi(f) = f(x+1) \), which is a homomorphism.

It is surjective, because for any \( \bar{g} \in \mathbb{Z}_2[x]/\langle x^2 \rangle \) we can take \( f(w) = g(w+1) \), and then \( \phi(f) = g(x+2) = g(x) \).

So we want to prove that \( \ker \phi = \langle w^2 + 1 \rangle \), and then the first isomorphism theorem will give the claim. In one direction, \( \phi(w^2 + 1) = (x+1)^2 + 1 = x^2 = 0 \), so \( \langle w^2 + 1 \rangle \subseteq \ker \phi \). In the other direction, if \( g(x+1) = 0 \) then \( g(x+1) = x^2 h(x) \) for some \( h \in \mathbb{Z}_2[x] \); substituting \( x = w + 1 \), we get \( g(w) = (w+1)^2 h(w+1) \), so \( g \in \langle (w+1)^2 \rangle = \langle w^2 + 1 \rangle \).

Or you could just write down a bijection,

\[
0 \leftrightarrow 0 \\
1 \leftrightarrow 1 \\
z \leftrightarrow w + 1 \\
z + 1 \leftrightarrow w
\]

and check that it respects addition and multiplication.

3. Let \( R \) be the set of \( 2 \times 2 \) matrices of the form \( \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \).

(a) Show that \( R \) is a subring of \( M_2(\mathbb{R}) \), and that it is commutative.

**Solution:** We see that \( R \) contains the identity matrix \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \), and it is closed under taking sums, differences, and products:

\[
\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} a + c & b + d \\ 0 & a + c \end{pmatrix} \\
\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} - \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} a - c & b - d \\ 0 & a - c \end{pmatrix} \\
\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad + bc \\ 0 & ac \end{pmatrix}.
\]

To see that \( R \) is commutative, we calculate

\[
\begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} ca & cb + da \\ 0 & ca \end{pmatrix}
\]

and see that it is the same as \( \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \).
(b) Prove that $R \cong \mathbb{R}[x]/\langle x^2 \rangle$.

Hint: Show that the map $\phi: \mathbb{R}[x] \to R$ given by
\[
\phi(a + bx + cx^2 + \cdots) = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}
\]
is a homomorphism, determine its kernel, and quote the first isomorphism theorem.

Solution: We have $\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Given two polynomials
\[
f = a + bx + \cdots \\
g = c + dx + \cdots
\]
we find that
\[
f + g = (a + c) + (b + d)x + \cdots \\
f \cdot g = ac + (ad + bc)x + \cdots.
\]
Thus $\phi(f + g) = \phi(f) = \phi(g)$, and $\phi(fg) = \phi(f)\phi(g)$.

We have $\phi(f) = 0$ if and only if $a = b = 0$, which is true if and only if $x^2 \mid f$. Thus $\ker \phi = \langle x^2 \rangle$.

We also see that $\phi$ is surjective, so by the first isomorphism theorem we conclude that $\mathbb{R}[x]/\langle x^2 \rangle \cong R$. 