Homework #11 Solutions

# 12 in 3.2

(a) Prove that $[a]_n$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $(a, n) = 1$.

If $(a, n) = 1$, then $\exists x, y \in \mathbb{Z}$ such that

$ax + ny = 1$. Therefore $[a][x]_n = [1]_n$ in $\mathbb{Z}/n\mathbb{Z}$. And thus, $[a]_n$ is a unit. If $(a, n) = d > 1$, then $a = ad'$ and $n = nd'$ for some $a', n', d' \in \mathbb{Z}$.

Since $0 < n' < n$, $[n'] 
eq [0]_n$ in $\mathbb{Z}/n\mathbb{Z}$.

$[a][n'] = [a'd'][n'] = [a'n'] = [0]_n$ in $\mathbb{Z}/n\mathbb{Z}$.

Therefore if $[a]_n$ were a unit with inverse $[b]_n$, then $[1]_n = [b][a]_n$. But then

$[1]_n = [1][n'] = [b][n'] = [b][0]_n = [0]_n$.

But we already saw that $[n'] 
eq [0]_n$. This is a contradiction. Hence, $[a]_n$ is not a unit.

(b) Prove that $[a]_n$ is a nonunit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $[a]_n$ is a zero divisor.

Proof: By part (a), $[a]_n$ is a nonunit if and only if $(a, n) 
eq 1$. And in the proof of (a), we saw this is equivalent to the existence of a nonzero element $[n']_n$ such that

$[a][n'] = [0]_n$, i.e. $[a]_n$ is a zero divisor.

# 34 in 3.2

Prove that $(a, b)$ is a unit in $\mathbb{M}(\mathbb{R})$ if and only if $ad - bc 
eq 0$. Verify that the
Inverses in this case is \[
\begin{pmatrix}
d/t & -b/t \\
-c/t & a/t
\end{pmatrix}
\]
when \( t = ad - bc \neq 0 \).

Proof: If \( ad - bc \neq 0 \), a direct computation shows that the matrix is invertible with the designated inverse.

If \( ad - bc = 0 \), then either \( a = 0 \) or \( d = 0 \) and so the matrix is \((0,0)\) or one of \( a \) and \( d \) is zero and then with

\[
\begin{pmatrix}
d/d & -b/c \\
-c/d & a/c
\end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}
\]

shows that \((a/b)\) is a zero divisor.

In a ring \( R \) set, \( R + 1 \), a zero divisor is not a unit (we proved this in class; here is the argument again: Suppose \( a \) is a unit and that \( ab = 0 \).

Then \( \forall b \in R, \ a - 1 \cdot b = 0 \) and \( a - 1 \cdot 0 = 0 \). Thus, if \( a \) is a unit, \( a \) is not a zero divisor; i.e. if \( a \) is a zero divisor, \( a \) cannot be a unit.

Here is a second solution to the problem.

Let \( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \). If \( A \) is a unit, then \( A^{-1} A = I \) \( \Rightarrow (\det A)^{-1} (\det A) = 1 \)

\( \Rightarrow \det A = ad - bc \neq 0 \).

# 8 in 3.3 Proof that \( IR \) is isomorphic to the subring \( S = \{ (a,0) : a \in R \} \) of \( M(2,R) \).

Proof: Define \( f : R \rightarrow S \) via \( f(a) = (a,0) \). Clearly \( f \) is bijective since \( f(a + b) = (a,0) + (b,0) \) and \( f(ab) = (a,0)(b,0) \), \( f \) is a homomorphism.
Which of the following are homomorphisms?

(a) \( f: \mathbb{Z} \rightarrow \mathbb{Z}, \quad f(x) = -x \)

\[ f(1) \cdot f(1) = f(1) \cdot f(-1) = 1 \cdot 1 = 1 \]  \( \text{not equal} \)

(b) \( f: \mathbb{Z} \rightarrow \mathbb{Z}, \quad f(x) = -x \)

Yes. In \( \mathbb{Z}, -a = a \) for every \( a \in \mathbb{Z} \).

So, \( f \) is the identity function. This is always a homomorphism.

(c) \( g: \mathbb{Q} \rightarrow \mathbb{Q}, \quad g(x) = \frac{1}{x^2 + 1} \)

No. \( g(1 + 1) = g(2) = \frac{1}{5} \)

\[ g(1) + g(1) = \frac{1}{2} + \frac{1}{2} = 1 \]

(d) \( h: \mathbb{R}_2 \rightarrow M(2\mathbb{R}), \quad h(a) = \begin{pmatrix} -a & 0 \\ a & 0 \end{pmatrix} \)

No. \( h(1) = \begin{pmatrix} -10 \\ 10 \end{pmatrix} \) \[ h(1) \cdot h(1) = \begin{pmatrix} -10 \\ 10 \end{pmatrix} \begin{pmatrix} -10 \\ 10 \end{pmatrix} = \begin{pmatrix} 100 \\ -100 \end{pmatrix} \neq h(1) \cdot h(1) \]

(e) \( f: \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{14}, \quad f([x]_{12}) = [x]_{14} \)

\( [x]_{14} = \begin{cases} [x]_{12} & \text{if } x \leq 12 \\ [x + 1]_{12} = [x]_{14} & \text{if } x > 12 \end{cases} \)

\[ f([x]_{12}) = [x]_{14} \quad \text{yes} \]

Check it is well-defined: \([x]_{12} = [y]_{12} \Rightarrow \]
\[ x = y + 12k \text{ for some } k \in \mathbb{Z} \]

\[ \Gamma x \Gamma_4 = \Gamma y + 12k \Gamma_4 = \Gamma y \Gamma_4. \]

Thus, if \( \Gamma x \Gamma_4 = \Gamma y \Gamma_4 \), the images \( f(\Gamma x) \) and \( f(\Gamma y) \) are the same.

Check it is a homomorphism:

\[
\begin{align*}
\Gamma f(\Gamma x \Gamma y) &= f(\Gamma x \Gamma y) = \Gamma xy \Gamma_4 = \Gamma x \Gamma_4 \Gamma y \Gamma_4 \\
&= f(\Gamma x) + f(\Gamma y) \\
f(\Gamma x \Gamma y) &= f(\Gamma x + \Gamma y) \\
&= \# \Gamma x + \Gamma y \Gamma_4 = \Gamma x \Gamma_4 + \Gamma y \Gamma_4 = f(\Gamma x) + f(\Gamma y).
\end{align*}
\]

# 17 in 3.3

Show that \( S = \{0, 4, 8, \ldots, 24\} \) is a subgroup of \( \mathbb{Z}_{28} \)

and prove that \( f : \mathbb{Z}_{28} \to S \)

\[ f(x) = 8x \]

is an isomorphism.

\textbf{Proof:} \( S = \{4a | a \in \mathbb{Z}_{28} : 4 \not| a \} \)

Since multiples of 4 and 6 differ by a difference of multiples of 4, \( S \)

is a subgroup of \( \mathbb{Z}_{28} \).

\textbf{Well-defined:} If \( [a] = [b] \) in \( \mathbb{Z}_{28} \)

we need to check that \( [8a] = [8b] \) in \( \mathbb{Z}_{28} \):

\[ 7 | (b-a) \Rightarrow 28 | (8b-8a) \quad \text{true.} \]

\textbf{Homomorphism:} \( f([a] + [b]) = [8a] + [8b] = [8a+b] \)

Since \( 64 \equiv 8 \pmod{28} \)

\[ f(\Gamma a + \Gamma b) = f(\Gamma a) + f(\Gamma b) \]

\[ = 8(\Gamma a + \Gamma b) \quad \checkmark \]

\( f \) is onto (clearly). Since \( |\mathbb{Z}_{28}| = |\mathbb{Z}_{28}| < \infty \),

\( f \) is also 1-1. Hence \( f \) is an isomorphism.
Let \( \mathbb{R} \times \mathbb{R} \) be the field of extension \#37 in 3.1.

When \((a, b) + (c, d) = (a + c, b + d)\)
and \((a, b)(c, d) = (ac - bd, ad + bc)\)

Show that \( \mathbb{R} \times \mathbb{R} \cong \mathbb{C} \).

**Proof.** Define \( f(a, b) = a + bi \).

This is a function from \( \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{C} \)
which is clearly a bijection.

We check it is a homomorphism:

\[
\begin{align*}
  f(a, b) + (c, d) &= f((a + c, b + d)) = (a + c) + (b + d)i \\
                 &= a + b i + c + d i = f((a, b)) + f((c, d)) \\
  f((a, b)(c, d)) &= f((ac - bd, ad + bc)) \\
                    &= ac - bd + (ad + bc)i = (a + bi)(c + di) \\
                    &= f((a, b)) \cdot f((c, d)). 
\end{align*}
\]