MATH 320 S26, Exam 4 Solutions

1. Consider the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ given by $f((m, n)) = (n, m)$. Prove or disprove that f is a homomorphism.

   The statement is true. Let $a = (m_1, n_1)$ and $b = (m_2, n_2)$ be arbitrary elements of $\mathbb{Z} \times \mathbb{Z}$.
   We calculate $f(a + b) = f((m_1 + m_2, n_1 + n_2)) = (n_1 + n_2, m_1 + m_2) = (n_1, m_1) + (n_2, m_2) = f((m_1, n_1)) + f((n_2, m_2)) = f(a) + f(b)$, and
   $f(ab) = f((m_1m_2, n_1n_2)) = (n_1n_2, m_1m_2) = (n_1, m_1)(n_2, m_2) = f((m_1, n_1))f((n_2, m_2)) = f(a)f(b)$.

   NOTE: Both parts of the proof offer a chain of equalities, leading from one side of the desired equality to the other – it would be incorrect to start with the desired equality, plug in, and end up with the useless $1 = 1$.

2. Consider the function $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $g((m, n)) = m + n$. Prove or disprove that g is a homomorphism.

   The statement is false – although this function respects addition it does not respect multiplication. To disprove requires an explicit, specific counterexample. Many are possible, such as: Let $a = (2, 1), b = (1, -1)$. Here $g(ab) = g((2, -1)) = 1$, but $g(a)g(b) = 3 \cdot 0 = 0$, so $g(ab) \neq g(a)g(b)$.

3. Recall that $M_2(\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{R} \right\}$. Consider the function $h : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ given by $h\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$. Prove or disprove that h is a homomorphism.

   The statement is false – this function also respects addition but does not respect multiplication. Again we need a specific counterexample. Many are possible, such as: Let $u = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right), v = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Here $h(uv) = h\left(\left(\begin{smallmatrix} 2 & 1 \\ 4 & 3 \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} 2 & 4 \\ 1 & 3 \end{smallmatrix}\right)$, but $h(u)h(v) = \left(\begin{smallmatrix} 1 & 3 \\ 2 & 4 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 3 & 1 \\ 4 & 2 \end{smallmatrix}\right)$, so $h(uv) \neq h(u)h(v)$.

   NOTE: The function h takes the matrix transpose. You might recall that the transpose satisfies $(AB)^T = B^TA^T$; for this to be a homomorphism we would instead need $(AB)^T = A^TB^T$ (which is true for certain matrices A, B, but not in general).

4. Prove that $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$ are not isomorphic.

   We argue by contradiction. Suppose $f : \mathbb{Z}_9 \to \mathbb{Z}_3 \times \mathbb{Z}_3$ were an isomomorphism. Then $f([1]) = ([a], [b])$ for some $[a], [b] \in \mathbb{Z}_3$. Because f is a homomorphism, $f([3]) = f([1]+[1]+[1]) = f([1])+f([1])+f([1]) = ([a], [b]) + ([a], [b]) + ([a], [b]) = ([3a], [3b]) = ([0], [0]) = 0_{\mathbb{Z}_3 \times \mathbb{Z}_3}$ (since $3n \equiv 0 \pmod 3$ for any integer n). However, by the Basic Homomorphism Properties Theorem, $f([0]) = ([0], [0]) = 0_{\mathbb{Z}_3 \times \mathbb{Z}_3}$ as well. We have found $f([0]) = f([3])$ but $[0] \neq [3]$, so f is not injective. This is a contradiction.

5. Prove the Ring Image Theorem.

   Let $f : R \to S$ be a homomorphism. To prove that $Im(f) = \{f(r) : r \in R\}$ is a subring of S we need to prove four properties.
   Let $a, b \in Im(f)$. Then there are $r_1, r_2 \in R$ (not necessarily distinct) with $f(r_1) = a, f(r_2) = b$. First, we see that $a + b = f(r_1) + f(r_2) = f(r_1 + r_2)$ (since f is a homomorphism). Since $r_1 + r_2 \in R$, $a + b \in Im(f)$. Second, we see that $ab = f(r_1)f(r_2) = f(r_1r_2)$ (since f is a homomorphism). Since $r_1r_2 \in R$, $ab \in Im(f)$. Third, the Basic Homomorphism Properties Theorem (i) tells us that $f(0_R) = 0_S$, so $0_S \in Im(f)$. Lastly, the Basic Homomorphism Properties Theorem (ii) tells us that $-a = -f(r_1) = f(-r_1)$, so $-a \in Im(f)$.

6. Let R be a commutative ring with identity, and let $c \in R$. Prove that the principal ideal $(c) = \{rc : r \in R\}$ is indeed an ideal.

   SOLUTION 1: There are five properties to prove. Let $r_1c, r_2c \in (c)$ be arbitrary (not necessarily distinct). First, we have $r_1c + r_2c = (r_1 + r_2)c$, and $r_1 + r_2 \in R$, so $r_1c + r_2c \in (c)$. Second, we have $(r_1c)(r_2c) = (r_1cr_2)c$, and $r_1cr_2 \in R$, so $(r_1c)(r_2c) \in (c)$. Third, $0_Rc = 0_R$ by exercise 2.9, so $0_R \in (c)$. Fourth, $r_1c + (-r_1)c = (r_1 - r_1)c = 0_Rc = 0_R$, so $(-r_1)c = -(r_1c)$ is in (c). We have proved that (c) is a subring of R. Now, let $r \in R$ be arbitrary. We have $r(r_1c) = (rr_1)c$, and $rr_1 \in R$, so $r(r_1c) \in (c)$.

SOLUTION 2: Using exercise 4.9, we have three properties to prove. First, $0_R c \in (c)$, so (c) is nonempty. Second, let $r_1 c, r_2 c \in (c)$ be arbitrary (not necessarily distinct). We have $r_1 c - r_2 c = (r_1 - r_2)c$, and $r_1 - r_2 \in R$, so $r_1 c - r_2 c \in (c)$. Second, let $r \in R$ be arbitrary. We have $r(r_1 c) = (r r_1)c$, and $r r_1 \in R$, so $r(r_1 c) \in (c)$.

7. Let R be a commutative ring, and let I be an ideal. Prove that equivalence modulo I is transitive.

Let $a, b, c \in R$ with $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$. Hence, $a - b \in I$ and $b - c \in I$. Because I is a subring, it is closed under addition. Hence, $(a - b) + (b - c) = a - c \in I$. Hence $a \equiv c \pmod{I}$.

8. Consider the ring $\mathbb{Z}[x]$. Prove or disprove that $(2) \cap (x^2) = (2x^2)$.

The statement is true, and a proof requires two directions. First, let $f(x) \in (2x^2)$. Then $f(x) = 2x^2 g(x)$, for some $g(x) \in \mathbb{Z}[x]$. We have $f(x) = 2(x^2 g(x))$, so $f(x) \in (2)$. We also have $f(x) = x^2(2g(x))$, so $f(x) \in (x^2)$. Hence, $f(x) \in (2) \cap (x^2)$. This proves that $(2) \cap (x^2) \supseteq (2x^2)$.

Now, let $f(x) \in (2) \cap (x^2)$. Since $f(x) \in (2)$, there is some $g(x) \in \mathbb{Z}[x]$ with $f(x) = 2g(x)$. Writing $g(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, we have $f(x) = 2a_0 + 2a_1 x + 2a_2 x^2 + \cdots + 2a_n x^n$. Now, since $f(x) \in (x^2)$, there is some $h(x) \in \mathbb{Z}[x]$ with $f(x) = x^2 h(x)$. Writing $h(x) = b_0 + \cdots + b_m x^m$, we have $f(x) = b_0 x^2 + \cdots + b_m x^{2+m}$. In particular, note that $a_0 = a_1 = 0_R$, because the lowest power of x that can appear in a term of $f(x)$ is x^2. Going back to $f(x) = 2a_0 + 2a_1 x + 2a_2 x^2 + \cdots + 2a_n x^n = 2a_2 x^2 + \cdots + 2a_n x^n = 2x^2(a_2 + \cdots + a_n x^{n-2})$. Since $a_2 + \cdots + a_n x^{n-2} \in \mathbb{Z}[x]$, we see that $f(x) \in (2x^2)$. This proves that $(2) \cap (x^2) \subseteq (2x^2)$.

9. Consider the ring $\mathbb{Z}[x]$, and its ideal $I = (2) + (x^2) = \{a + b : a \in (2), b \in (x^2)\}$. Prove or disprove that I is principal.

The statement is false. We argue by contradiction; suppose that $I = (f(x))$ were principal. Because $2 = 2 + 0x^2 \in I$, there is some $g(x) \in \mathbb{Z}[x]$ with $2 = f(x)g(x)$. By the Degree Sum Theorem ($\mathbb{Z}$ is an integral domain), $0 = \deg(2) = \deg(f(x)) + \deg(g(x))$. Hence $0 = \deg(f(x)) = \deg(g(x))$, i.e., $f(x) = c \in \mathbb{Z}$ and $g(x) = d \in \mathbb{Z}$. So $cd = 2$, as integers. Hence $f(x) = \pm 1$ or $f(x) = \pm 2$.

If $f(x) = \pm 1$, then there are some $a \in (2), b \in (x^2)$ with $a + b = \pm 1$ (because $f(x) \in (f(x)) = I$). We have $a = 2a_0 + 2a_1 x + 2a_2 x^2 + \cdots$ and $b = b_0 x^2 + b_1 x^3 + \cdots$, so $a + b = 2a_0 + 2a_1 x + (2a_2 + b_0)x^2 + \cdots$. However, the constant term of $a + b$ is $2a_0$, which is even and thus not ± 1. This case is impossible.

Lastly, if $f(x) = \pm 2$, then $x^2 = 0 \cdot 2 + 1 \cdot x^2 \in I = (f(x))$, so there is some polynomial $g(x) \in \mathbb{Z}[x]$ with $x^2 = (\pm 2)g(x)$. If $g(x) = g_0 + g_1 x + g_2 x^2 + (\cdots)$, then $(\pm 2)g(x) = (\pm 2)g_0 + (\pm 2)g_1 x + (\pm 2)g_2 x^2 + (\cdots)$. Equating coefficients, we see that $1 = (\pm 2)g_2$, so (± 2) divides 1. This case is also impossible.

10. Consider the ring $\mathbb{Z}[x]$, and its ideal $I = (2) + (x^2) = \{a + b : a \in (2), b \in (x^2)\}$. Find R/I, i.e., find all of the cosets of I. How many are there?

For convenience and intuition (not part of the proof), we first compute the elements of I explicitly: Let $a \in (2), b \in (x^2)$. We have $a = 2a_0 + 2a_1 x + 2a_2 x^2 + 2a_3 x^3 \cdots$ and $b = b_0 x^2 + b_1 x^3 + \cdots$, so $a + b = 2a_0 + 2a_1 x + (2a_2 + b_0)x^2 + (2a_3 + b_1)x^3 + \cdots$. It looks like I contains those polynomials whose constant and first-degree terms are both even (with no restrictions on the other term).

Now, we claim that $R/I = \{0 + I, 1 + I, x + I, 1 + x + I\}$, four cosets. Take some arbitrary $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n \in \mathbb{Z}[x]$. Write $f_0 = r_0 + 2a$, $f_1 = r_1 + 2b$, where $a, b \in \mathbb{Z}$ and $r_0, r_1 \in \{0, 1\}$. These (a, b, r_0, r_1) must always exist, and are unique, by the $\mathbb{Z}$ division algorithm (dividing each of f_0, f_1 by 2). We now write $f(x) = r_0 + r_1 x + 2(a + bx) + x^2(f_2 + \cdots + f_n x^{n-2})$. Note that $a + bx, f_2 + \cdots + f_n x^{n-2} \in \mathbb{Z}[x]$, so $2(a + bx) + x^2(f_2 + \cdots + f_n x^{n-2}) \in I$. Meanwhile, $r_0 + r_1 x$ is among $\{0, 1, x, 1 + x\}$. This proves that every element of $\mathbb{Z}[x]$ is in exactly one of these four cosets.