Math 333 Problem Set 7

Solutions

1. Prove that $\mathbb{R}$ is isomorphic to the ring $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in \mathrm{Mat}_2(\mathbb{R}) \right\}$.

   Proof. Define $\varphi : \mathbb{R} \to S$ by $\varphi(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$. Let $a, b \in \mathbb{R}$. We have

   $$\begin{aligned} \varphi(a+b) &= \begin{bmatrix} a+b & 0 \\ 0 & a+b \end{bmatrix} \\ &= \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \\ &= \varphi(a) + \varphi(b) \end{aligned}$$

   and

   $$\begin{aligned} \varphi(ab) &= \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix} \\ &= \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \\ &= \varphi(a)\varphi(b). \end{aligned}$$

   Thus, φ is a homomorphism. We show it is injective by showing $\ker(\varphi) = \{0\}$. Let $a \in \ker(\varphi)$, i.e., $\varphi(a) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Clearly this gives $a = 0$ as desired. Finally, let $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in S$. Then $\varphi(a) = A$, so φ is surjective. Since we have shown φ is bijective and a homomorphism, we have $\mathbb{R}$ and S are isomorphic as claimed. $\square$

2. Let $\varphi : R \to S$ be a homomorphism of rings. If r is a zero divisor in R, is $\varphi(r)$ a zero divisor in S? If so, prove it. If not, give a counterexample.

   Let $\varphi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be the map given by $\varphi([x]_4) = [x]_2$. This was shown to be a homomorphism in class. Observe that $[2]_4$ is a zero divisor, but $\varphi([2]_4) = [2]_2 = [0]_2$, so is not a zero divisor.

3. (a) Show that $S = \{0, 4, 8, 12, 16, 20, 24\}$ is a subring of $\mathbb{Z}/28\mathbb{Z}$.

Proof. Observe that S is the collection of multiples of 4 in $\mathbb{Z}/28\mathbb{Z}$. We prove a more general result. Let R be a commutative ring and $r \in R$. We claim the set of multiples of r, denoted $\langle r\rangle$, is a subring of R. Since $0_R = r0_R \in \langle r\rangle$. Let $ra, rb \in \langle r\rangle$. Then $ra + rb = r(a + b) \in \langle r\rangle$ and $(ra)(rb) = r(arb) \in \langle r\rangle$. Finally, since $a \in R$ we have an additive inverse x in R. Observe that $ra + rx = r(a + x) = r0_R = 0_R$ and $rx \in \langle r\rangle$. Thus, $\langle r\rangle$ is a subring of R. In this particular case, we have $\langle [4]_{28}\rangle$ is a subring of $\mathbb{Z}/28\mathbb{Z}$. □

(b) Prove that the map $\varphi : \mathbb{Z}/7\mathbb{Z} \to S$ given by $\varphi([x]_7) = [8x]_{28}$ is an isomorphism.

Proof. First we must show the map is well-defined. Let $[x]_7, [y]_7 \in \mathbb{Z}/7\mathbb{Z}$. If $[x]_7 = [y]_7$, then $x = y + 7t$ for some $t \in \mathbb{Z}$. Then $\varphi([x]_7) = [8x]_{28} = [8(y + 7t)]_{28} = [8y]_{28} + [56t]_{28} = [8y]_{28} = \varphi([y]_7)$. Thus, φ does not depend on the choice of representative of $[x]_7$. One also needs to show that the image of φ is actually in S. For this, observe that $\varphi([0]_7) = [0]_{28}$, $\varphi([1]_7) = [8]_{28}$, $\varphi([2]_7) = [16]_{28}$, $\varphi([3]_7) = [24]_{28}$, $\varphi([4]_7) = [4]_{28}$, $\varphi([5]_7) = [12]_{28}$, and $\varphi([6]_7) = [14]_{28}$. Thus, the image of φ really does land in S. Moreover, this shows φ is surjective. Observe that for any $[x]_7, [y]_7 \in \mathbb{Z}/7\mathbb{Z}$ we have

$$\begin{aligned}
\varphi([x]_7 + [y]_7) &= \varphi([x + y]_7) \\
&= [8(x + y)]_{28} \\
&= [8x + 8y]_{28} \\
&= [8x]_{28} + [8y]_{28} \\
&= \varphi([x]_7) + \varphi([y]_7)
\end{aligned}$$

and

$$\begin{aligned}\varphi([x]_7[y]_7) &= \varphi([xy]_7)\\ &= [8(xy)]_{28}\\ &= [64xy]_{28} \quad \text{since } 64 \equiv 8 \pmod{28}\\ &= [(8x)(8y)]_{28}\\ &= [8x]_{28}[8y]_{28}\\ &= \varphi([x]_7)\varphi([y]_7).\end{aligned}$$

Thus, φ is a homomorphism. We show φ is injective by showing $\ker(\varphi) = \{[0]_7\}$. However, to see this just observe that when we determined the image of φ above the only element that mapped to $[0]_{28}$ is $[0]_7$, thus we have $\ker(\varphi) = \{[0]_7\}$ and so φ is injective. Hence, φ is a bijective homomorphism and so an isomorphism. □

4. Let $\varphi : R \to S$ and $\psi : S \to T$ be homomorphisms. Show that $\psi \circ \varphi : R \to T$ is a homomorphism.

Proof. Let $a, b \in R$. We have

$$\begin{aligned}(\psi \circ \varphi)(a+b) &= \psi(\varphi(a+b))\\ &= \psi(\varphi(a)+\varphi(b)) \quad \text{because } \varphi \text{ is a homomorphism}\\ &= \psi(\varphi(a))+\psi(\varphi(b)) \quad \text{because } \psi \text{ is a homomorphism}\\ &= (\psi \circ \varphi)(a) + (\psi \circ \varphi)(b)\end{aligned}$$

and

$$\begin{aligned}(\psi \circ \varphi)(ab) &= \psi(\varphi(ab))\\ &= \psi(\varphi(a)\varphi(b)) \quad \text{because } \varphi \text{ is a homomorphism}\\ &= \psi(\varphi(a))\psi(\varphi(b)) \quad \text{because } \psi \text{ is a homomorphism}\\ &= (\psi \circ \varphi)(a)(\psi \circ \varphi)(b).\end{aligned}$$

Thus, $\psi \circ \varphi$ is a homomorphism. □

5. Let $\varphi : R \to S$ be an isomorphism of rings. Which of the following properties are preserved by this isomorphism? (Be sure to justify your answers!)

(a) $a \in R$ is a zero divisor.

Let $a \in R$ be a zero divisor, i.e., $a \neq 0_R$ and there exists a nonzero $b \in R$ so that $ab = 0_R$. Since φ is an isomorphism, it is injective and a homomorphism so $\ker(\varphi) = \{0_R\}$. Thus, $\varphi(a) \neq 0_R$ and $\varphi(b) \neq 0_R$. Thus, $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(0_R) = 0_S$ and so $\varphi(a)$ is a zero divisor in S.

(b) $a \in R$ is an idempotent.

Let $a \in R$ be an idempotent, i.e., $a^2 = a$. Then we have $\varphi(a)^2 = \varphi(a)\varphi(a) = \varphi(a^2) = \varphi(a)$ and so $\varphi(a)$ is an idempotent.

(c) if R is an integral domain then S is an integral domain.

We showed in class that if R is a ring with identity and $\varphi : R \to S$ is surjective, then $\varphi(1_R)$ is the identity element of S. Thus, S has an identity. Let $s, t \in S$. Then there exists $a, b \in R$ so that $\varphi(a) = s, \varphi(b) = t$. We have $st = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = ts$. Thus, S is commutative. Finally, suppose there exists $s, t \in S$ so that $st = 0_S$. Let $a, b \in R$ so that $\varphi(a) = s, \varphi(b) = t$. Then $\varphi(ab) = \varphi(a)\varphi(b) = st = 0_S$ and so $ab \in \ker(\varphi) = \{0_R\}$ since φ is an injective homomorphism. Thus, $ab = 0_R$ and since R is an integral domain we must have $a = 0_R$ or $b = 0_R$. This gives $s = 0_S$ or $t = 0_S$ so S is an integral domain.

6. Let $f = 2x^4 + x^2 - x + 1$ and $g = 2x - 1$ be polynomials in $(\mathbb{Z}/5\mathbb{Z})[x]$. Find polynomials $q, r \in (\mathbb{Z}/5\mathbb{Z})[x]$ so that $f = gq + r$ with $r = [0]_5$ or $\deg r < \deg g$.

Use polynomial long division keeping in mind that your coefficients are elements of $\mathbb{Z}/5\mathbb{Z}$ to obtain

$$f = g(x^3 + 3x^2 + 2x + 3) + 3.$$

7. Let F be a field. Is $F[x]$ a field? Justify your answer.

Consider the element $x \in F[x]$. Suppose x is a unit, i.e., there exists a nonzero $f \in F[x]$ so that $xf = 1_F$. Then we have

$$\begin{aligned} 0 &= \deg(1_F) \\ &= \deg(xf) \\ &= \deg(x) + \deg(f) \\ &\geq \deg(x) \\ &= 1. \end{aligned}$$

This is clearly a contradiction as 0 is not greater than 1. Thus, x is a nonzero element of $F[x]$ without an inverse so $F[x]$ cannot be a field.

8. Is the collection of all polynomials in $R[x]$ with constant term 0_R a subring of $R[x]$? Justify your answer.

Proof. Let S denote the collection of polynomials in $R[x]$ with constant term 0_R. Observe that we have

$$S = \langle x \rangle = \{f \in R[x] : x \mid f\}.$$

This is now a special case of the general proof given in 3(a) with $r = x$ and $R = R[x]$. □