Solutions 06

1. Let $\mathbb{F}_4$ denote the set of all (2×2)-matrices of the form

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$$

where a and b are elements in the commutative ring $\mathbb{Z}/\langle 2 \rangle$.

i. Establish that $\mathbb{F}_4$ is a commutative ring under the usual matrix operations.

ii. Demonstrate that $\mathbb{F}_4$ is a field with exactly four elements.

Solution.

i. Matrices over a commutative ring form a noncommutative ring—as addition of matrices is defined entrywise, matrices over a commutative ring clearly form an additive abelian group. Similarly, matrix multiplication is both associative and distributive, and the identity matrix is the multiplicative identity.

Since the identity matrix belongs to $\mathbb{F}_4$, it suffices to show $\mathbb{F}_4$ is commutative and closed under both addition and multiplication. For any elements a, b, c, d in the commutative ring $\mathbb{Z}/\langle 2 \rangle$, we have

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix} + \begin{bmatrix} c & d \\ d & c+d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ b+d & (a+c)+(b+d) \end{bmatrix} \in \mathbb{F}_4$$

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix} \begin{bmatrix} c & d \\ d & c+d \end{bmatrix} = \begin{bmatrix} ac+bd & ad+bc+bd \\ ad+bc+bd & (ac+bd)+(ad+bc+bd) \end{bmatrix} \in \mathbb{F}_4$$

$$\begin{bmatrix} c & d \\ d & c+d \end{bmatrix} \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} = \begin{bmatrix} ac+bd & ad+bc+bd \\ ad+bc+bd & (ac+bd)+(ad+bc+bd) \end{bmatrix}$$

which shows that $\mathbb{F}_4$ is a commutative ring.

ii. Since $|\mathbb{Z}/\langle 2 \rangle| = 2$, there are four elements in $\mathbb{F}_4$, namely

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \qquad \text{and} \qquad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Because we have

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

it follows that every nonzero element is a unit, so $\mathbb{F}_4$ is a field. □

2. Let R be a commutative ring. An element r in R is ***nilpotent*** if $r^n = 0$ for some positive integer n.

i. For any nilpotent element r in R, prove that $1 - r$ is a unit in R.

ii. Prove the set of all nilpotent elements in R is an ideal.

Solution.

i. As the ring element r is nilpotent, there exists a positive integer n such that $r^n = 0$. It follows that

$$\begin{aligned} (1-r)(1+r+r^2+\cdots+r^{n-1}) &= (1+r+r^2+\cdots+r^{n-1}) - (r+r^2+r^3+\cdots+r^n) \\ &= 1 + r^n = 1, \end{aligned}$$

so the element $1 - r$ is a unit.

ii. For a nilpotent element f in R, there is a positive integer n such that $f^n = 0$. For any a in R, we have $(a\,f)^n = a^n\,f^n = a^n\,0 = 0$, so af is also nilpotent. Suppose that g in R is also nilpotent. Hence, there exists a positive integer m such that $g^m = 0$. The binomial formula implies that

$$(f+g)^{n+m-1} = \sum_{k=0}^{n+m-1} \binom{n+m-1}{k} f^k\, g^{n+m-1-k}\,.$$

Since we cannot have both $k < n$ and $n + m - 1 - k < m$, each term in this sum vanishes, so we deduce that $(f+g)^{n+m-1} = 0$. We conclude that the set of nilpotent elements in R forms an ideal. □

3. *i.* Let R be a commutative ring and consider elements f and g in R. Show that the canonical image of the product fg in the quotient ring $R/\langle f - f^2 g\rangle$ is an idempotent. Give an example where this idempotent is distinct from 0 and 1.

ii. Let R and S be commutative rings and let $\varphi\colon R \to S$ and $\psi\colon R \to S$ be ring homomorphisms. Is the set of all elements f in R such that $\varphi(f) = \psi(f)$ a subring of R?

Solution.

i. Set $I := \langle f - f^2 g\rangle$. Since $fg - f^2g^2 = g(f - f^2g) \in I$, the canonical image of the product fg equals the canonical image of $f^2g^2 = (fg)^2$ in R/I. In particular, the element fg is an idempotent.

Consider $R = \mathbb{Z}$, $f = 2$, and $g = 3$. It follows that

$$\frac{R}{\langle f - f^2 g\rangle} \cong \frac{\mathbb{Z}}{\langle 10\rangle}$$

and $fg = 6$ is an idempotent distinct from 0 and 1. Similarly, consider $R = \mathbb{C}[x]$ and $f = x = g$. It follows that

$$\begin{aligned}\frac{R}{\langle f - f^2 g\rangle} \cong \frac{\mathbb{C}[x]}{\langle x - x^3\rangle} &\cong \frac{\mathbb{C}[x]}{\big\langle x(x-1)(x+1)\big\rangle} \\ &\cong \frac{\mathbb{C}[x]}{\langle x\rangle} \times \frac{\mathbb{C}[x]}{\langle x-1\rangle} \times \frac{\mathbb{C}[x]}{\langle x+1\rangle} \cong \mathbb{C}\times\mathbb{C}\times\mathbb{C}\end{aligned}$$

and x^2 is an idempotent distinct from 0 and 1.

ii. Set $T := \big\{ f \in R \mid \varphi(f) = \psi(f) \big\}$. Since $\varphi(1_R) = 1_S = \psi(1_R)$, we see that $1_R \in T$. For any f and g in T, we have

$$\begin{aligned}\varphi(f+g) = \varphi(f) + \varphi(g) = \psi(f) + \psi(g) = \psi(f+g)\\ \varphi(fg) = \varphi(f)\,\varphi(g) = \psi(f)\,\psi(g) = \psi(fg)\end{aligned}$$

so subset T is closed under multiplication and addition. Therefore, the set T is a subring of R. □