Solutions 06

P6.1. Let $\mathbb{F}_4$ denote the subset of all (2×2)-matrices having the form

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

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

i. Show that $\mathbb{F}_4$ is a subring of the ring $\mathrm{Mat}(2, \mathbb{Z}/\langle 2\rangle)$ consisting of all (2×2)-matrices with entries in the quotient $\mathbb{Z}/\langle 2\rangle$.

ii. Verify that $\mathbb{F}_4$ is a commutative ring.

iii. Demonstrate that any nonzero element in $\mathbb{F}_4$ has a multiplicative inverse.

Solution.

i. To prove $\mathbb{F}_4$ is a subring, it suffices to show the following.

(*differences*) For any matrices $\mathbf{M}$ and $\mathbf{N}$ in $\mathbb{F}_4$, the difference $\mathbf{M}-\mathbf{N}$ is also in $\mathbb{F}_4$.

(*products*) For any matrices $\mathbf{M}$ and $\mathbf{N}$ in $\mathbb{F}_4$, the product $\mathbf{M}\mathbf{N}$ is also in $\mathbb{F}_4$.

(*identity*) The multiplicative identity $\mathbf{I}$ is also in $\mathbb{F}_4$.

For any ring elements a, b, c, d in the quotient $\mathbb{Z}/\langle 2\rangle$, we have

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

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

$$\begin{bmatrix} 1 & 0 \\ 0 & 1+0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{F}_4$$

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

ii. For any elements a, b, c, and d in $\mathbb{Z}/\langle 2\rangle$, matrix multiplication and part (i) give

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

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

iii. 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 $\mathbf{I}^2 = \mathbf{I}$ and

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

it follows that every nonzero ring element in $\mathbb{F}_4$ has a multiplicative inverse. □

Remark. This algebraic structure is "the" field with 4 elements.

P6.2. **i.** Let $R := \mathbb{Z}/\langle 6\rangle$. For the polynomials

$$f = x^5 + 5\,x^4 + 4\,x^3 + 3\,x^2 + 1 \qquad \text{and} \qquad g = 3\,x^2 + x + 2$$

in $R[x]$, find a quotient and remainder for division of $3^4 f$ by g.

ii. Let K be a field. Consider polynomials $f, g \in K[x]$ such that $\deg(g) > 0$. Confirm that there exist unique polynomials $h_0, h_1, \dots, h_d \in K[x]$ such that

$$f = h_0 + h_1\, g + h_2\, g^2 + h_3\, g^3 + \cdots + h_d\, g^d$$

where $\deg(h_j) < \deg(g)$ or $h_j = 0$ for all $0 \leqslant j \leqslant d$.

Solution.

i. Since $\deg(f) - \deg(g) + 1 = 4$, we divide $3^4 f$ by g. Long division gives

$$\begin{array}{r|r}
 & 3\,x^3{+}0\,x^2{+}0\,x{+}3 \\
3\,x^2 + 1\,x + 2 & 3\,x^5{+}3\,x^4{+}0\,x^3{+}3\,x^2{+}0\,x{+}3 \\
 & 3\,x^5{+}3\,x^4{+}0\,x^3\phantom{{+}3\,x^2{+}0\,x{+}3} \\
\hline
 & 3\,x^2{+}0\,x{+}3 \\
 & 3\,x^2{+}3\,x{+}0 \\
\hline
 & 3\,x{+}3
\end{array}$$

so the quotient is $(3^4 f) \mathbin{/\!/} g = 3\,x^3 + 3$ and the remainder $(3^4 f) \,\%\, g = 3\,x + 3$.

Remark. Since 3 is a zero divisor in $R = \mathbb{Z}/\langle 6\rangle$, neither the quotient nor the remainder are unique: $3^4 f = (3\,x^3 + 1)\,g + (5\,x + 1) = (3\,x^3 + 5)\,g + (x + 5)$.

ii. Let $m := \deg(f)$ and $n := \deg(g)$. Since K is a field, the leading coefficient of any polynomial is invertible and thereby not a zero divisor. Division with remainder implies that there exists unique polynomials $q_0, h_0 \in K[x]$ such that $f = q_0\, g + h_0$ and $\deg(h_0) < \deg(g)$ or $h_0 = 0$. Iterating this division, we see that, for all $j > 0$, there are unique $q_j, h_j \in K[x]$ such that $q_{j-1} = q_j\, g + h_j$ and $\deg(h_j) < \deg(g)$ or $h_j = 0$. Set $d := m \mathbin{/\!/} n = \lfloor m/n \rfloor \in \mathbb{Z}$. Because $\deg(q_{j-1}) = \deg(q_j) + \deg(g)$ and $\deg(f) = \deg(q_0) + \deg(g)$, we observe that $\deg(q_j) = m - (j+1)\,n$ for all $0 \leqslant j < d$. Hence, this iterative process stabilizes after d steps: we have $q_{d-1} = h_d$, $q_d = 0$, and $0 = h_{d+1} = h_{d+2} = h_{d+3} = \cdots$. It follows that

$$\begin{aligned}
f &= h_0 + q_0\, g \\
&= h_0 + (h_1 + q_1\, g)\, g = h_0 + h_1\, g + q_1\, g^2 \\
&= h_0 + h_1\, g + (h_2 + q_2\, g)\, g^2 = h_0 + h_1\, g + h_2\, g^2 + q_2\, g^3 \\
&\ \ \vdots \\
&= h_0 + h_1\, g + h_2\, g^2 + \cdots + q_{d-1}\, g^d = h_0 + h_1\, g + h_2\, g^2 + \cdots + h_d\, g^d\,.
\end{aligned}$$

□

P6.3. Let R be a commutative ring. The *derivative operator* $D\colon R[x] \to R[x]$ is defined, for every polynomial $f := a_m\, x^m + a_{m-1}\, x^{m-1} + \cdots + a_1\, x + a_0 \in R[x]$, by

$$D(f) := (m\, a_m)\, x^{m-1} + \big((m-1)\, a_{m-1}\big)\, x^{m-2} + \cdots + a_1\,.$$

i. Prove that the operator D is R-linear: for all $r, s \in R$ and all $f, g \in R[x]$, we have

$$D(r\, f + s\, g) = r\, D(f) + s\, D(g)\,.$$

CC BY NC ND

ii. Prove that the operator D satisfies the product rule: for all $f, g \in R[x]$, we have

$$D(f\,g) = D(f)\,g + f\,D(g)\,.$$

iii. Consider $f \in R[x]$ and let $b \in R$ be root of f having multiplicity k with $k \geqslant 1$. Prove that b is also a root of the derivative $D(f)$ having multiplicity at least $k-1$. Moreover, when the product $k\,1_R$ is invertible in R, show that b is a root of the derivative $D(f)$ having multiplicity $k-1$.

Solution.

i. For all ring elements $r, s \in R$ and all polynomials

$$f = a_m\,x^m + a_{m-1}\,x^{m-1} + \cdots + a_1\,x + a_0 \in R[x] \qquad \text{and}$$
$$g = b_m\,x^m + b_{n-1}\,x^{m-1} + \cdots + b_1\,x + b_0 \in R[x]\,,$$

we have

$$\begin{aligned}
&D(r\,f + s\,g)\\
&= D\big((r\,a_m + s\,b_m)x^m + (r\,a_{m-1} + s\,b_{m-1})\,x^{m-1} + \cdots + (r\,a_1 + s\,b_1)\,x + (r\,a_0 + s\,b_0)\big)\\
&= m\,(r\,a_m + s\,b_m)x^{m-1} + (m-1)\,(r\,a_{m-1} + s\,b_{m-1})\,x^{m-2} + \cdots + (r\,a_1 + s\,b_1)\\
&= r\Big((m\,a_m)\,x^{m-1} + \big((m-1)\,a_{m-1}\big)\,x^{m-2} + \cdots + a_1\Big)\\
&\qquad + s\Big((m\,b_m)\,x^{m-1} + \big((m-1)\,b_{n-1}\big)\,x^{m-1} + \cdots + b_1\Big)\\
&= s\,D(f) + r\,D(g)\,,
\end{aligned}$$

which proves that D is an R-linear map.

ii. Since part **i** shows that D is R-linear, it suffices to prove that the product rule holds for every monomial x^{m+n} where m and n are positive integers. By definition, we have $D(x^{m+n}) = (m+n)x^{m+n-1}$. We also have

$$\begin{aligned}
D(x^m)\,x^n + x^m\,D(x^n) &= m\,x^{m-1}\,x^n + x^m(n\,x^{n-1})\\
&= m\,x^{m+n-1} + n\,x^{m+n-1} = (m+n)\,x^{m+n-1}\,,
\end{aligned}$$

so the product rule holds.

iii. For any root $b \in R$ of the polynomial $f \in R[x]$ having multiplicity k, there exists a polynomial g in $R[x]$ such that $f = (x-b)^k\,g$ and $\mathrm{ev}_b(g) = g(b) \neq 0$. The product rule implies that

$$D(f) = k(x-b)^{k-1}\,g + (x-b)^k\,D(g) = (x-b)^{k-1}\,\big(k\,g + (x-b)\,D(g)\big)$$

It follows that b is a root of the derivative $D(f)$ having multiplicity at least $k-1$. When the product $k\,1_R$ is invertible in R, we also have

$$\mathrm{ev}_b\big(k\,g + (x-b)\,D(g)\big) = k\ \mathrm{ev}_b(g) + 0\ \mathrm{ev}_b\big(D(g)\big) = k\ \mathrm{ev}_b(g) \neq 0\,.$$

In this case, b is a root of the derivative $D(f)$ having multiplicity $k-1$. □

CC BY NC ND