Solutions 06

P6.1. **i.** Let $\mathbb{F}_3 := \mathbb{Z}/\langle 3\rangle$ be the field with 3 elements. Consider the commutative ring
$$\mathbb{F}_3[\mathrm{i}] := \{a + b\,\mathrm{i} \mid a, b \in \mathbb{F}_3 \text{ and } \mathrm{i}^2 \equiv -1 \equiv 2 \mod 3\}.$$
Verify that $\mathbb{F}_3[\mathrm{i}]$ is a field.

ii. Let $\mathbb{F}_5 := \mathbb{Z}/\langle 5\rangle$ be the field with 5 elements. Consider the commutative ring
$$\mathbb{F}_5[\mathrm{i}] := \{a + b\,\mathrm{i} \mid a, b \in \mathbb{F}_5 \text{ and } \mathrm{i}^2 \equiv -1 \equiv 4 \mod 5\}.$$
Confirm that $\mathbb{F}_5[\mathrm{i}]$ is not a domain.

Solution.

i. The 9 elements in $\mathbb{F}_3[\mathrm{i}]$ are 0, i, $2\,\mathrm{i}$, 1, $1+\mathrm{i}$, $1+2\mathrm{i}$, 2, $2+\mathrm{i}$, $2+2\,\mathrm{i}$. Since
$$\begin{aligned}
(\mathrm{i})(2\,\mathrm{i}) &= 2(\mathrm{i}^2) = 2(2) = 4 = 1 & 1(1) &= 1\\
(1+\mathrm{i})(2+\mathrm{i}) &= (2+2) + (2+1)\,\mathrm{i} = 1 & 2(2) &= 4 = 1\\
(1+2\,\mathrm{i})(2+2\,\mathrm{i}) &= \big(2+4(2)\big) + (4+2)\,\mathrm{i} = 1\,,
\end{aligned}$$
we see that every nonzero ring element has a multiplicative inverse. Hence, the commutative ring $\mathbb{F}_3[\mathrm{i}]$ is a field.

ii. Among the 25 elements in $\mathbb{F}_5[\mathrm{i}]$, we observe that
$$\begin{aligned}
(1+2\,\mathrm{i})(1+3\,\mathrm{i}) &= \big(1+6(4)\big)+(2+3)\,\mathrm{i} = 0 & (1+2\,\mathrm{i})(2+\mathrm{i}) &= \big(2+2(4)\big)+(4+1)\,\mathrm{i} = 0\\
(1+2\,\mathrm{i})(3+4\,\mathrm{i}) &= \big(3+8(4)\big)+(6+4)\,\mathrm{i} = 0 & (1+2\,\mathrm{i})(4+2\,\mathrm{i}) &= \big(4+4(4)\big)+(8+2)\,\mathrm{i} = 0\\
(2+\mathrm{i})(3+\mathrm{i}) &= \big(6+(4)\big)+(3+2)\,\mathrm{i} = 0 & (2+\mathrm{i})(2+4\,\mathrm{i}) &= \big(4+4(4)\big)+(2+8)\,\mathrm{i} = 0\\
(2+\mathrm{i})(4+3\,\mathrm{i}) &= \big(8+3(4)\big)+(4+6)\,\mathrm{i} = 0 & (1+3\,\mathrm{i})(2+4\,\mathrm{i}) &= \big(2+12(4)\big)+(6+4)\,\mathrm{i} = 0\\
(1+3\,\mathrm{i})(3+\mathrm{i}) &= \big(3+3(4)\big)+(9+1)\,\mathrm{i} = 0 & (1+3\,\mathrm{i})(4+3\,\mathrm{i}) &= \big(4+9(4)\big)+(12+3)\,\mathrm{i} = 0\\
(4+2\,\mathrm{i})(4+3\,\mathrm{i}) &= \big(16+6(4)\big)+(8+12)\,\mathrm{i} = 0 & (2+4\,\mathrm{i})(3+4\,\mathrm{i}) &= \big(6+16(4)\big)+(12+8)\,\mathrm{i} = 0\\
(2+4\,\mathrm{i})(4+2\,\mathrm{i}) &= \big(8+8(4)\big)+(16+4)\,\mathrm{i} = 0 & (3+\mathrm{i})(3+4\,\mathrm{i}) &= \big(9+4(4)\big)+(3+12)\,\mathrm{i} = 0\\
(3+\mathrm{i})(4+2\,\mathrm{i}) &= \big(12+2(4)\big)+(4+6)\,\mathrm{i} = 0 & (3+4\,\mathrm{i})(4+3\,\mathrm{i}) &= \big(12+12(4)\big)+(16+9)\,\mathrm{i} = 0\,.
\end{aligned}$$
Since the commutative ring $\mathbb{F}_5[\mathrm{i}]$ contains zero divisors, it is not a domain. □

P6.2. **i.** Let $R := \mathbb{Z}/\langle 6\rangle$. For the polynomials
$$g = x^5 + 3\,x^3 + 5\,x^2 + 2\,x + 1 \qquad \text{and} \qquad f = 2\,x^2 + 4\,x + 1$$
in $R[x]$, find a quotient and remainder for division of $2^4\,g$ by f.

ii. Let K be a field. Consider elements f and g in the polynomial ring $K[x]$ such that $\deg(g) > 0$. Confirm that there exist unique polynomials $h_0, h_1, \dots, h_d$ in the ring $K[x]$ 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 $\deg(g) - \deg(f) + 1 = 4$, we divide $2^4 g = 4x^5 + 2x^2 + 2x + 4$ by f. Long division gives

$$
\begin{array}{r|l}
 & \qquad\qquad\quad 2x^3+2x^2+\;\;x+1 \\ \hline
2x^2+4x+1 & 4x^5+0x^4+0x^3+2x^2+2x+4 \\
 & 4x^5+2x^4+2x^3 \\ \hline
 & \qquad 4x^2+4x^3+2x^2 \\
 & \qquad 4x^4+2x^3+2x^2 \\ \hline
 & \qquad\qquad 2x^3+0x^2+2x \\
 & \qquad\qquad 2x^2+4x^2+1x \\ \hline
 & \qquad\qquad\qquad 2x^2+1x+4 \\
 & \qquad\qquad\qquad 2x^2+4x+1 \\ \hline
 & \qquad\qquad\qquad\qquad 3x+3
\end{array}
$$

so $(2^4 g) \mathbin{/\!/} f = 2x^3 + 2x^2 + x + 1$ and $(2^4 g) \mathbin{\%} f = 3x + 3$.

Remark. Since 2 is a zero divisor in $R = \mathbb{Z}/\langle 6\rangle$, neither the quotient nor the remainder are unique:

$$
\begin{aligned}
2^4 g &= (2x^3 + 2x^2 + 4x + 4)\, f + 0 \\
&= (2x^3 + 2x^2 + 4x + 1)\, f + 3 \\
&= (2x^3 + 2x^2 + x + 4)\, f + 3x\,.
\end{aligned}
$$

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 and h_0 in the ring $K[x]$ such that $f = q_0\, g + h_0$ and $\deg(h_0) < \deg(g)$ or $h_0 = 0$. Iterating the division with remainder, we see that, for all $j > 0$, there are unique polynomials q_j and 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 $d := m \mathbin{/\!/} n$. 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 any 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 an R-linear map: for any elements r and s in the coefficient ring R and any polynomials f and g in the ring $R[x]$, we have $D(r\,f + s\,g) = r\,D(f) + s\,D(g)$.

ii. Prove that the operator D satisfies the Leibniz product rule: for any polynomials f and g in the ring $R[x]$, we have $D(f\,g) = D(f)\,g + f\,D(g)$.

iii. Let f be a polynomial 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, prove that b is a root of the derivative $D(f)$ having multiplicity $k-1$.

Solution.

i. For any elements r and s in R and any polynomials

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

in $R[x]$, we have

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

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 Leibniz product rule holds for any monomial x^{m+n} where m and n are positive integers. By definition, we have $D(x^{m+n}) = (m+n)x^{m+n-1}$. Since we also have

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

we see that the Leibniz product rule holds.

iii. Since b is a root of f 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 Leibniz 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 $k-1$. □