2

For $\mathbb{Z}_7$ the solution is 3 and in $\mathbb{Z}_{23}$ it is 16.

10

The characteristic of $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ is $\operatorname{lcm}(6, 15) = 30$

12

Since $\mathcal{R}$ has characteristic 3, $3 \cdot x = 0$ for all $x \in \mathcal{R}$. Therefore

$$\begin{aligned}(a+b)^9 &= \left((a+b)^3\right)^3 \\ &= \left(a^3 + 3a^2b + 3ab^2 + b^3\right)^3 \\ &= \left(a^3 + b^3\right)^3 \\ &= a^9 + 3a^6b^3 + 3a^3b^6 + b^9 \\ &= a^9 + b^9\end{aligned}$$

23

Proof. Let $\mathcal{R}$ be a division ring. Note that $0^2 = 0$ and $1^2 = 1$, hence 0 and 1 are idempotent. Assume towards contradiction there is some $a \in \mathcal{R}$ that is idempotent and $a \neq 0$ and $a \neq 1$. Then $a^2 = a \implies a(a-1) = 0$. Since $\mathcal{R}$ is a division ring and $a \neq 0$, there exists a^{-1} meaning $a - 1 = 0 \implies a = 1$, a contradiction. Hence $\mathcal{R}$ only has 2 idempotents (0 and 1). ■

27

By the previous exercise, the unity of an integral domain is the unique non-zero idempotent element of $\mathcal{D}$. Therefore any subdomain of $\mathcal{D}$ has the same unity as $\mathcal{D}$. Therefore since characteristic is defined as the smallest $n \in \mathbb{Z}_+$ such that $n \cdot 1 = 0$ or 0 if n doesn't exist, then any subdomain will have the same characteristic since it has the same unity.

28

Proof. Let X be a subdomain of an integral domain $\mathcal{D}$. Note X contains the same unity as $\mathcal{D}$. Therefore since X is closed under addition, $n \cdot 1 \in X$ for all $n \in \mathbb{Z}$. Hence the set $R = \{n \cdot 1 : n \in \mathbb{Z}\}$ is a subset of X. R is closed under addition since $(n \cdot 1) + (m \cdot 1) = (m + n) \cdot 1$. Since $(-n \cdot 1) + (n \cdot 1) = 0$ and $0 \cdot 1 = 0$, R also contains 0 and has all additive inverses meaning $\langle R, + \rangle$ is an abelian group. R is closed under multiplication since $(n \cdot 1)(m \cdot 1) = (mn) \cdot 1$. It also follows $1 \cdot 1 = 1$ meaning R must be a commutative ring with unity. Since any product $xy = 0$ in R is also a product in $\mathcal{X}$, R must have no zero divisors. Therefore R is a subdomain of all subdomains $\mathcal{X}$. ■

29

Proof. Assume towards contradiction that an integral domain $\mathcal{D}$ has a characteristic of mn where $m, n > 1$. Then by the distributive laws $(m \cdot 1)(n \cdot 1) = (mn) \cdot 1 = 0$. Since $\mathcal{D}$ is an integral domain, this means that either $m \cdot 1 = 0$ or $n \cdot 1 = 0$. However, $m, n < mn$ meaning if either case was true, the characteristic would be smaller than mn. This is a contradiction since the characteristic is the smallest possible integer k such that $k \cdot 1 = 0$. Therefore $\mathcal{D}$ must have a zero or prime characteristic. ■

30

Part A

Proof. Examine the axioms for S to be a ring.

$\mathcal{R}_1$) Since both $\langle R, +\rangle$ and $\langle Z, +\rangle$ (or $\langle \mathbb{Z}_n, +\rangle$) are abelian groups, their direct product is also an abelian group. Since addition on S is defined in the same manner as the direct product, $\langle S, +\rangle$ is an abelian group.

$\mathcal{R}_2$) Let $(r_1, n_1), (r_2, n_2), (r_3, n_3) \in S$. Then

$$\begin{aligned}(r_1, n_1)[(r_2, n_2)(r_3, n_3)] &= (r_1, n_1)[(r_2r_3 + n_2 \cdot r_3 + n_3 \cdot r_2, n_2n_3)] \\ &= (r_1r_2r_3 + n_2 \cdot r_1r_3 + n_3 \cdot r_1r_2 + \\ &\quad\ n_1 \cdot r_2r_3 + (n_1n_2) \cdot r_3 + (n_1n_3) \cdot r_2 + \\ &\quad (n_2n_3) \cdot r_1, n_1n_2n_3)\end{aligned}$$

which equals

$$(r_1r_2r_3 + (n_2n_3) \cdot r_1 + (n_1n_3) \cdot r_2 + (n_1n_2) \cdot r_3 + n_3 \cdot r_1r_2 + n_1 \cdot r_2r_3 + n_2 \cdot r_1r_3, n_1n_2n_3).$$

Grouping the first two terms gives

$$\begin{aligned}[(r_1, n_1)(r_2, n_2)]\,(r_3, n_3) &= [(r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1n_2)]\,(r_3, n_3) \\ &= (r_1r_2r_3 + n_1 \cdot r_2r_3 + n_2 \cdot r_1r_3 + \\ &\quad\ n_3 \cdot r_1r_2 + (n_1n_3) \cdot r_2 + (n_2n_3) \cdot r_1 + \\ &\quad (n_1n_2) \cdot r_3, n_1n_2n_3).\end{aligned}$$

Since addition is commutative and the distributivity laws hold, it is equal to

$$(r_1r_2r_3 + (n_2n_3) \cdot r_1 + (n_1n_3) \cdot r_2 + (n_1n_2) \cdot r_3 + n_3 \cdot r_1r_2 + n_1 \cdot r_2r_3 + n_2 \cdot r_1r_3, n_1n_2n_3).$$

Therefore multiplication is associative.

$\mathcal{R}_3$) Checking the left distributive law

$$\begin{aligned}(r_1, n_1)[(r_2, n_2) + (r_3, n_3)] &= (r_1, n_1)(r_2 + r_3, n_2 + n_3) \\ &= (r_1(r_2 + r_3) + (n_2 + n_3) \cdot r_1 + n_1 \cdot (r_2 + r_3), n_1(n_2 + n_3)) \\ &= (r_1 r_2 + n_2 \cdot r_1 + n_1 \cdot r_2, n_1 n_2) + (r_1 r_3 + n_3 \cdot r_2 + n_2 \cdot r_3, n_1 n_3) \\ &= (r_1, n_1)(r_2, n_2) + (r_1, n_1)(r_3, n_3)\end{aligned}$$

Therefore the left distributivity law holds. The right law follows from a similar argument. ■

Part B

Proof. Consider $(0, 1) \in S$. Note that

$$(0, 1)(r, n) = (0r + 1 \cdot r + n \cdot 0, 1 \cdot n) = (r, n)$$

and

$$(r, n)(0, 1) = (r0 + n \cdot 0 + 1 \cdot r, n \cdot 1) = (r, n).$$

Therefore $(0, 1) \in S$ is unity. ■

Part C

Proof. By the previous part, $(0, 1)$ is the unity of S. Assume that R has characteristic $n \neq 0$. Note $\mathbb{Z}_n$ is a ring of characteristic n, meaning n is the smallest integer such that $n \cdot 1_{\mathbb{Z}_n} = 0_{\mathbb{Z}_n}$. Since $n \cdot 0_R = 0_R$ for any n, it follows $n \cdot (0, 1) = (0, 0)$. Therefore n is the characteristic of S. Assume that R has characteristic 0. Then $S = R \times \mathbb{Z}$. $\mathbb{Z}$ has characteristic zero meaning there is no $n \in \mathbb{Z}_+$ such that $n \cdot 1 = 0$. Note then that for any $n \in \mathbb{Z}_+$ that $n \cdot (0, 1) = (n \cdot 0, n \cdot 1) \neq (0, 0)$. Hence S has characteristic 0. ■

Part D

Proof. Let $\overline{S} = \{(r, 0) : r \in \mathbb{R}\} \subseteq S$ and $r_1, r_2 \in R$. Note that $(0, 0) \in \overline{S}$, $(r_1, 0) - (r_2, 0) = (r_1 - r_2, 0) \in \overline{S}$, and $(r_1, 0)(r_2, 0) = (r_1 r_2, 0) \in \overline{S}$. Therefore $\overline{S}$ is a subring of S. Consider the requirements for ϕ to be an isomorphism between R and $\overline{S}$.

- Note that $\phi(r_1 + r_2) = (r_1 + r_2, 0) = (r_1, 0) + (r_2, 0) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 r_2) = (r_1 r_2, 0) = (r_1, 0)(r_2, 0) = \phi(r_1)\phi(r_2)$. Therefore ϕ is a homomorphism.
- Assume that $\phi(r_1) = \phi(r_2)$. Then $(r_1, 0) = (r_2, 0)$ meaning $(r_1 - r_2, 0) = (0, 0)$. Therefore $r_1 = r_2$ hence ϕ is injective. Let $(r, 0) \in \overline{S}$. Note that $\phi(r) = (r, 0)$, hence ϕ is onto. Therefore ϕ is a bijection between R and $\overline{S}$

Since ϕ is a one-to-one and onto homomorphism between R and $\overline{S}$, the statement holds. ■