Solutions 09

P9.1. **i.** Express the ring $\mathbb{Z}/\langle 720\rangle$ as a product of three quotient rings.

ii. Exhibit elements e_1, e_2, and e_3 in $\mathbb{Z}/\langle 720\rangle$ such that

$$e_1^2 = e_1\,, \qquad e_2^2 = e_2\,, \qquad e_3^2 = e_3\,, \qquad e_2\,e_3 = 0\,, \qquad e_1\,e_3 = 0\,, \qquad e_1\,e_2 = 0\,,$$

and $[1]_{720} = e_1 + e_2 + e_3$.

Solution. Set $R := \mathbb{Z}/\langle 720\rangle$.

i. Since

$$\begin{aligned} 4(16) - 7(9) = 1 &\equiv 1 \bmod 720\,, \\ 1(16) - 3(5) = 1 &\equiv 1 \bmod 720\,, \quad \text{and} \\ -1(9) + 2(5) = 1 &\equiv 1 \bmod 720\,, \end{aligned}$$

we see that $\langle [16]_{720}\rangle + \langle [9]_{720}\rangle = R$, $\langle [16]_{720}\rangle + \langle [5]_{720}\rangle = R$, and $\langle [9]_{720}\rangle + \langle [5]_{720}\rangle = R$. As $720 = (2^4)(3^2)(5)$, the least common multiple of $2^4 = 16$, $3^2 = 9$, and 5 equals 720, so $\langle [16]_{720}\rangle\, \langle [9]_{720}\rangle\, \langle [5]_{720}\rangle = \langle [16]_{720}\rangle \cap \langle [9]_{720}\rangle \cap \langle [5]_{720}\rangle = \langle [0]_{720}\rangle$. Hence, the Remainder Theorem shows that $\mathbb{Z}/\langle 720\rangle$ is isomorphic to $\mathbb{Z}/\langle 16\rangle \times \mathbb{Z}/\langle 9\rangle \times \mathbb{Z}/\langle 5\rangle$.

ii. Since

$$\begin{aligned} [225]_{720}^2 &= [50625]_{720} = [70(720) + 225]_{720} = [225]_{720} \\ [576]_{720}^2 &= [331776]_{720} = [460(720) + 576]_{720} = [576]_{720} \\ [640]_{720}^2 &= [409600]_{720} = [568(720) + 640]_{720} = [640]_{720} \\ [225]_{720}\,[576]_{720} &= [129600]_{720} = [180(720) + 0]_{720} = [0]_{720} \\ [225]_{720}\,[640]_{720} &= [144000]_{720} = [200(720) + 0]_{720} = [0]_{720} \\ [576]_{720}\,[640]_{720} &= [368640]_{720} = [512(720) + 0]_{720} = [0]_{720} \end{aligned}$$

and $[225]_{720} + [576]_{720} + [640]_{720} = [1441]_{720} = [2(720)+1]_{720} = [1]_{720}$, we see that the elements $e_1 := [225]_{720}$, $e_2 := [576]_{720}$, and $e_3 := [640]_{720}$ in $\mathbb{Z}/\langle 720\rangle$ have the desired properties. □

Remark. Observe that

$$\begin{aligned} \langle [16]_{720}\rangle &= \langle [(31)(16)]_{720}\rangle = \langle [496]_{720}\rangle = \langle [1-225]_{720}\rangle\,, \\ \langle [9]_{720}\rangle &= \langle [(9)(81)]_{720}\rangle = \langle [81]_{720}\rangle = \langle [(9)(9)]_{720}\rangle = \langle [1-640]_{720}\rangle\,, \quad \text{and} \\ \langle [5]_{720}\rangle &= \langle [(29)(5)]_{720}\rangle = \langle [145]_{720}\rangle = \langle [1-576]_{720}\rangle\,. \end{aligned}$$

P9.2. **i.** Let $\varphi\colon R \to S$ be a ring homomorphism between commutative rings. Assume that the subsets D in R and E in S are multiplicative and satisfy $\varphi(D) \subseteq E$. Prove that there exists a unique ring homomorphism $\widehat{\varphi}\colon R[D^{-1}] \to S[E^{-1}]$ such that $\widehat{\varphi}(r/1) = \varphi(r)/1$ for all r in R.

ii. Demonstrate that any automorphism of a domain admits a unique extension to its field of fractions.

Solution.

i. Let $\eta\colon R \to R[D^{-1}]$ and $\theta\colon S \to S[E^{-1}]$ be the canonical ring homomorphisms associated to rings of fractions. By definition, we have $\eta(r) = r/1$ for any r in R

and $\theta(s) = s/1$ for any $s \in S$. Hence, the claim is equivalent to proving that there exists a unique ring homomorphism $\widehat{\varphi}\colon R[D^{-1}] \to S[E^{-1}]$ such that the diagram

$$\begin{array}{ccc} R & \xrightarrow{\quad\varphi\quad} & S \\ {\scriptstyle\eta}\big\downarrow & & \big\downarrow{\scriptstyle\theta} \\ R[D^{-1}] & \xrightarrow{\;\widehat{\varphi}\;} & S[E^{-1}] \end{array}$$

commutes. Since $\varphi(D) \subseteq E$, it follows that, for any element d in D, its image $(\theta\,\varphi)(d) = \eta(\varphi(d)) = \varphi(d)/1$ is a unit in the ring $S[E^{-1}]$. Hence, the universal property of $R[D^{-1}]$, applied to the composite map $\theta\,\varphi\colon R \to S[E^{-1}]$, shows that there is a unique ring homomorphism $\widehat{\varphi}\colon R[D^{-1}] \to S[E^{-1}]$ such that $\theta\,\varphi = \widehat{\varphi}\,\eta$.

ii. Let R be a commutative domain. Setting $D \coloneqq R \setminus \{0_R\}$, the ring $R[D^{-1}]$ is its field of fractions and $\eta\colon R \to R[D^{-1}]$ is the canonical ring homomorphism.

Suppose that $\varphi\colon R \to R$ is an automorphism of R. By definition, there exists a ring homomorphism $\psi\colon R \to R$ such that $\varphi\,\psi = \mathrm{id}_R$ and $\psi\,\varphi = \mathrm{id}_R$. Applying part **i** twice, there exists unique ring homomorphisms $\widehat{\varphi}\colon R[D^{-1}] \to R[D^{-1}]$ and $\widehat{\psi}\colon R[D^{-1}] \to R[D^{-1}]$ such that $\widehat{\varphi}\,\eta = \eta\,\varphi$ and $\widehat{\psi}\,\eta = \eta\,\psi$ or, equivalently, we have the following commutative diagrams:

$$\begin{array}{ccc} R & \xrightarrow{\quad\varphi\quad} & R \\ {\scriptstyle\eta}\big\downarrow & & \big\downarrow{\scriptstyle\eta} \\ R[D^{-1}] & \xrightarrow{\;\widehat{\varphi}\;} & R[D^{-1}] \end{array} \qquad \begin{array}{ccc} R & \xrightarrow{\quad\psi\quad} & R \\ {\scriptstyle\eta}\big\downarrow & & \big\downarrow{\scriptstyle\eta} \\ R[D^{-1}] & \xrightarrow{\;\widehat{\psi}\;} & D[R^{-1}] \end{array} .$$

It follows that

$$\eta = \eta\ \mathrm{id}_R = \eta\,\varphi\,\psi = \widehat{\varphi}\,\eta\,\psi = \widehat{\varphi}\,\widehat{\psi}\,\eta \quad\text{and}\qquad \eta = \eta\ \mathrm{id}_R = \eta\,\psi\,\varphi = \widehat{\psi}\,\eta\,\varphi = \widehat{\psi}\,\widehat{\varphi}\,\eta\,.$$

Using part **i** a third time, the identity map $\mathrm{id}_{R[D^{-1}]}\colon R[D^{-1}] \to R[D^{-1}]$ is the unique ring homomorphism such that $\eta\ \mathrm{id}_{R[D^{-1}]} = \mathrm{id}_R\ \eta = \eta$. Hence, we deduce that $\widehat{\varphi}\,\widehat{\psi} = \mathrm{id}_{R[D^{-1}]}$ and $\widehat{\psi}\,\widehat{\varphi} = \mathrm{id}_{R[D^{-1}]}$. In other words, the automorphism $\varphi\colon R \to R$ has the unique extension $\widehat{\varphi}\colon R[D^{-1}] \to R[D^{-1}]$. □

P9.3. Describe all of the maximal ideals in the product ring $\mathbb{Z}/\langle 343\rangle \times \mathbb{Z}/\langle 343\rangle$.

Solution. Given the inclusion $\langle 343\rangle = \langle 7^3\rangle \subset \langle 7\rangle$ of ideals in the ring $\mathbb{Z}$ of integers, the Induced Map Lemma, applied to the identity map $\mathrm{id}_{\mathbb{Z}}\colon \mathbb{Z} \to \mathbb{Z}$, produces the ring homomorphism $\overline{\mathrm{id}_{\mathbb{Z}}}\colon \mathbb{Z}/\langle 343\rangle \to \mathbb{Z}/\langle 7\rangle$. As $\mathbb{Z}/\langle 7\rangle$ is a field, it has only two ideals: $\langle [0]_7\rangle$ and $\langle [1]_7\rangle$. Hence, the Correspondence Theorem establishes that there are only two ideals in $\mathbb{Z}/\langle 343\rangle$ containing the ideal $\langle [7]_{343}\rangle$, namely $\langle [7]_{343}\rangle$ and $\langle [1]_{343}\rangle$. It follows that $\langle [7]_{343}\rangle$ is a maximal ideal in the ring $\mathbb{Z}/\langle 343\rangle$. On the other hand, any integer m not divisible by 7 is coprime to 343, so the congruence class $[m]_{343}$ is a unit in the ring $\mathbb{Z}/\langle 343\rangle$. We deduce that the only ideal with an element not contained in $\langle [7]_{343}\rangle$ is the ideal $\langle [1]_{343}\rangle = R$. Thus, the unique maximal ideal in the ring $\mathbb{Z}/\langle 343\rangle$ is $\langle [7]_{343}\rangle$.

Since addition and multiplication are defined componentwise on a product of rings, we see that the ideals in the ring $\mathbb{Z}/\langle 343\rangle \times \mathbb{Z}/\langle 343\rangle$ are all of the form $I \times J$ where I and

J are ideals in the quotient ring $\mathbb{Z}/\langle 343\rangle$. Hence, a maximal ideal has one factor that is a maximal ideal in $\mathbb{Z}/\langle 343\rangle$ and another factor that is $\langle [1]_{343}\rangle = \mathbb{Z}/\langle 343\rangle$. In particular, the two maximal ideals in the product ring $\mathbb{Z}/\langle 343\rangle \times \mathbb{Z}/\langle 343\rangle$ are $\langle [7]_{343}\rangle \times \langle [1]_{343}\rangle$ and $\langle [1]_{343}\rangle \times \langle [7]_{343}\rangle$. □

Remark. Basically the same argument shows that, for any positive integer m and any positive prime integer p, the ring $\mathbb{Z}/\langle p^m\rangle$ has $\langle [p]_{p^m}\rangle$ as its unique maximal ideal.

Fix a positive integer e. For any positive integers $m_1, m_2, \dots, m_e$, and any positive prime integers $p_1, p_2, \dots, p_e$, the product ring

$$\prod_{j=1}^{e} \frac{\mathbb{Z}}{\langle p_j^{m_j}\rangle} = \frac{\mathbb{Z}}{\langle p_1^{m_1}\rangle} \times \frac{\mathbb{Z}}{\langle p_2^{m_2}\rangle} \times \cdots \times \frac{\mathbb{Z}}{\langle p_3^{m_e}\rangle}$$

has e distinct maximal ideals: namely, the ideal

$$\left(\prod_{i=1}^{j-1} \frac{\mathbb{Z}}{\langle p_i^{m_i}\rangle}\right) \times \left\langle [p_j]_{p_j^{m_j}} \right\rangle \times \left(\prod_{k=j}^{e} \frac{\mathbb{Z}}{\langle p_k^{m_k}\rangle}\right),$$

for all $1 \leqslant j \leqslant e$.