1. Determine all ring homomorphisms from $\mathbb{Z}_{10}$ to $\mathbb{Z}_{25}$.

Proof. Note that a ring homomorphism is a group homomorphism with multiplicative condition. Thus, for a ring homomorphism from a cyclic group to an arbitrary group, the whole homomorphism is determined by where the generator is mapped to.

Let $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{25}$ be a ring homomorphism. Then it should satisfy the following two conditions; $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for any $a, b \in \mathbb{Z}_{10}$. Thus,

$$ab\phi(1) = \phi(1) + \cdots + \phi(1) = \phi(1 + \cdots + 1) = \phi(ab)$$

$$= \phi(a)\phi(b) = \phi(1 + \cdots + 1)\phi(1 + \cdots + 1) = \left(\phi(1) + \cdots + \phi(1)\right) \left(\phi(1) + \cdots + \phi(1)\right) = ab\phi(1)^2$$

Dividing both sides by $ab$, we may note that the image of 1 must satisfy $\phi(1) = \phi(1)^2$, i.e. 1 must be mapped to an idempotent.

Let $x \in \mathbb{Z}_{25}$ be an idempotent element of $\mathbb{Z}_{25}$; i.e. $x^2 = x$ in $\mathbb{Z}_{25}$. This is equivalent to find all solutions of $x(x - 1) = 0$ in $\mathbb{Z}_{25}$. Since 25 is not a prime, $\mathbb{Z}_{25}$ is not an integral domain; thus, there might be some $x \in \mathbb{Z}_{25}$ other than 0 and 1 yet satisfying the given equation. That is, one needs to find a pair of zero-divisors of $\mathbb{Z}_{25}$ which differ by 1.

Lemma: an element that has a multiplicative inverse (i.e. unit) is not a zero-divisor. Suppose $u$ is a unit of a ring $R$ with $vu = 1$. If $ux = 0$ for some $x \in R$, then $1 \cdot x = vux = v \cdot 0 = 0$. Thus, if $u$ is a unit, $ux = 0 \iff x = 0$, and hence a unit cannot be a zero divisor.

Recall the fact $U(n)$ is a multiplicative subgroup of $\mathbb{Z}_n$ containing the units. Thus, zero-divisors of $\mathbb{Z}_{25}$ must not be included in $U(25) = \{k \in \mathbb{Z}_{25} : \gcd(k, 25) = 1\}$. Note that the elements in $\mathbb{Z}_{25}$ that are not in $U(25)$ are the multiples of 5. In fact, the multiples of five are the only zero-divisors of $\mathbb{Z}_{25}$, and none of pairs differs by 1. Thus, the only idempotents in $\mathbb{Z}_{25}$ are 0 and 1 (even though it is not an integral domain.)

Note that $\phi(1)$ cannot be 1; if so, then $\phi$ fails to be a group homomorphism because $|\phi(1)| = 25 \nmid 10 = |1|$. (Recall the fact if $f : G \to H$ is a group homomorphism between finite groups, $|f(g)| \mid |g|$ for any $g \in G$.) Thus, $\phi(1) = 0$ is the only ring homomorphism from $\mathbb{Z}_{10}$ to $\mathbb{Z}_{25}$. □

2. In $\mathbb{Z}_7[x]$ let $I = \langle x^2 + 3x - 2 \rangle$. Find the multiplicative inverse of $x + 2 + I$ in $\mathbb{Z}_7[x]/I$.

Proof. By the division algorithm, for any $f(x) \in \mathbb{Z}_7[x]$, we can find a representative $g(x)$ of which degree $\leq 1$ such that $f(x) + I = g(x) + I$, since $I$ is generated by a polynomial of degree 2. Thus, we need to find $a, b \in \mathbb{Z}_7$ such that $(x + 2 + I)(ax + b + I) = 1 + I$.

$$((x + 2) + I)((ax + b) + I) = (ax^2 + (2a + b)x + 2b) + I = a(x^2 + 3x - 2) - 3ax + 2a + (2a + b)x + 2b + I$$

$$= (-a + b)x + 2a + 2b + I = 1 + I.$$
Hence \(-a + b \equiv 0 \pmod{7}\) and \(2a + 2b \equiv 1 \pmod{7}\). Solving these equations, we obtain \(a = b = 2\). Thus, \((2x + 2) + I\) is the multiplicative inverse of the given element.

\[
((x + 2) + I)((2x + 2) + I) = (2x^2 + 6x + 4) + I = 2(x^2 + 3x - 2) + 8 + I = 8 + I = 1 + I.
\]

\(\Box\)

3. Let \(R = \mathbb{Z}[x]\) and let \((2, x + x^2)\). Is \(I\) a maximal ideal in \(R\)? Explain your answer.

**Proof.** Let us denote the ideal by \(I\). Claim, \(x + I \neq 0 + I\); this is equivalent to show that \(x \notin I\). Every element in \(I\) is in the form of \(2f(x) + (x + x^2)g(x)\) where \(f(x), g(x) \in R\). After removing the unnecessary terms from \(f(x)\) and \(g(x)\), one may assume that \(g(x)\) is zero. (More specifically, assume \(g(x)\) is non-zero. Derive a contradiction if the leading coefficient is odd, and reduce the degree of \(g(x)\) by removing unnecessary terms if the leading coefficient is even. If you do not understand the procedure behind this, ask to your TA.) Hence, \(x = 2f(x)\). However, \(f(x) \in \mathbb{Z}[x] = R\), and there is no polynomial of integer coefficients satisfying \(2f(x) = x\). Thus, \(x \notin I\), and hence \(x + I \neq 0 + I\). One can show \((x + 1) + I\) by the similar reasoning.

However, note \((x + I)((x + 1) + I) = (x^2 + x) + I = 0 + I\). Thus, \(R/I\) is not an integral domain, nor is a field. (Recall the fact that every field is an integral domain.) By **Theorem 14.4** in the textbook, \(I\) is not a maximal ideal.

\(\Box\)

Another solution;

**Proof.** One can show that there exists an ideal \(J \trianglelefteq R\) such that \(I \subsetneq J \subsetneq R\). Claim: \(J = \langle 2, x \rangle\) is an ideal that is strictly including \(I\) and strictly included in \(R\).

Every element in \(I\) is in the form of \(2p(x) + (x^2 + x)q(x)\) for some \(p(x), q(x) \in \mathbb{Z}[x]\). Note that replacing \((x + 1)q(x) = Q(x)\), we can rephrase the element in the form of \(2p(x) + xQ(x)\), which is in the form of elements in \(J\). Thus, \(I \subset J\). Note that \(x \notin I\) (I proved this in the previous proof, so I will skip here), while \(x \in J\). Thus \(I \subsetneq J\).

\(J\) is an ideal of \(R\), and hence it is clearly included in \(R\). However, in order to demonstrate that \(I\) is not a maximal ideal, we need to prove that \(J \neq R\). I claim that \(1 \notin J\). Suppose \(1 \in J\). Then, \(1 = 2p(x) + xq(x)\) for some \(p(x), q(x) \in \mathbb{Z}[x]\). Evaluating the both sides for \(x = 0\), we obtain \(1 = 2p(0)\); here \(p(x) \in \mathbb{Z}[x]\), and hence \(p(0)\) the constant term of \(p(x)\) must be an element of \(\mathbb{Z}\); yet there is no integer \(k\) with \(2k = 1\). Thus, \(1\) cannot be written in such form, and hence \(1 \notin J\) while \(1 \in R\). Therefore, \(J = \langle 2, x \rangle\) is an ideal such that \(I \subseteq J \subsetneq R\).

Similarly, one can show that \(J' = \langle 2, x + 1 \rangle\) is another ideal satisfying the inclusion relation provided. \(\Box\)

4. Let \(R = \mathbb{Z}_3[x]\) and let \(I = \langle x^2 - x - 1 \rangle\). Is \(I\) a maximal ideal in \(R\)? Explain your answer.
Proof. Take an advantage of Theorem 17.5, i.e. if $F$ is a field, and for $p(x) \in F[x]$, $\langle p(x) \rangle$ is maximal if and only if $p(x)$ is irreducible over $F$. Since $\mathbb{Z}_3$ is a field, the given ideal is maximal if (and only if) the polynomial generating it is irreducible over $\mathbb{Z}_3$. Note that $x^2 - x - 1$ is a degree 2 polynomial, and hence by Theorem 17.1, it suffices to check whether $p(x) = x^2 - x - 1$ has a zero over $\mathbb{Z}_3$. However, $p(x) \neq 0$ for any of $x \in \mathbb{Z}_3$, and hence irreducible. Thus, given ideal is maximal. \qed

5. Let $f(x) = x^3 + 4x^2 - 2x - 5$. Write $f(x)$ as a product of irreducible polynomials over $\mathbb{Z}_{11}$.

Proof. Since $\mathbb{Z}_{11}$ is a field and $f(x)$ has degree 3, again by Theorem 17.1, $f(x)$ is reducible if and only if $f(x)$ has zero over $\mathbb{Z}_{11}$. Note that $f(-1) = (-1)^3 + 4(-1)^2 - 2(-1) - 5 = 0$; i.e. $f(x)$ is divisible by $(x + 1)$.

\[
\begin{array}{c|ccccc}
   & x^2 + 3x - 5 \\
\hline
x + 1 & x^3 + 4x^2 - 2x - 5 \\
      & - x^3 - x^2 \\
      & 3x^2 - 2x \\
      & - 3x^2 - 3x \\
      & - 5x - 5 \\
      & 5x + 5 \\
      & 0 \\
\end{array}
\]

Now, one needs to check whether $g(x) = x^2 + 3x - 5$ is reducible in $\mathbb{Z}_{11}$; however, for any $x \in \mathbb{Z}_{11}$, $g(x) \neq 0$ in $\mathbb{Z}_{11}$. Thus, $f(x) = (x + 1)(x^2 + 3x - 5)$. \qed