1. (a) **Claim:** $I[x]$ is aee proper ideal of $R[x]$.

We note that $0 \in I$ and since $I \subseteq I[x]$, we get that $0 \in I[x]$.

Meanwhile, for $a_n x^n + \cdots + a_0, b_m x^m + \cdots + b_0 \in I[x]$. Assuming $n \geq m$, for each $k > m$, $a_k \in I$. For each $k \leq m$ that $a_k + b_k \in I$. Hence, we get that $a_n x^n + \cdots + a_{m+1} x^{m+1} + (a_m + b_m) x^m + \cdots + (a_0 + b_0) \in I[x]$. We note that $I[x]$ is closed under addition.

Lastly, for $a_n x^n + \cdots + a_0 \in I[x]$ and $b_m x^m + \cdots + b_0 \in R[x]$, we note that $(a_n x^n + \cdots + a_0)(b_m x^m + \cdots + b_0)$ can be expressed as:

$$\sum_{k=0}^{n} a_k x^k (b_m x^m + \cdots + b_0)$$

For $0 \leq i \leq m$, $a_k b_i \in I$, so $a_k b_i x^{i+k} \in I[x]$. This implies that $a_k b_m x^{m+k} + \cdots a_k b_0 x^k \in I[x]$ as each term is in $I[x]$ and $I[x]$ is closed under addition. Since each item in the sum is in $I[x]$, it further implies that the sum is in $I[x]$.

We proved that $I[x]$ is an ideal of $R[x]$, so we now prove properness. Clearly, $I[x] \subseteq R[x]$. Since I is a proper ideal, $1 \notin I$, so $1 \cdot x = x \notin I[x]$. However, $x \in R[x]$, so we get that $I[x] \neq R[x]$, so it is a proper ideal. □

Claim: $R[x]/I[x] \cong (R/I)[x]$

Our goal is to use the First Isomorphism Theorem to achieve this result.

By Proposition 9.5, a homomorphism $\psi : R[x] \to (R/I)[x]$ is the same as defining a homomorphism $\varphi : R \to (R/I)[x]$ along with an element $\alpha \in (R/I)[x]$. We define φ to be the natural projection map of $r \mapsto [r]_I \in R/I$ for $r \in R$, which exists in $(R/I)[x]$ due to the inclusion of constants. Meanwhile, we choose $\alpha = x \in (R/I)[x]$, so $\psi(x) = \alpha$.

We now prove that $im(\psi)$ is surjective. Let $a_n x^n + \cdots + a_0 \in (R/I)[x]$. For each $0 \leq k \leq n$, $a_k = [r_k]_I$ for some $r_k \in R$. In other words, $\psi(r_k) = a_k$. Hence, considering that $x = \psi(x)$, we note that:

$$\begin{aligned} a_n x^n + \cdots + a_0 &= \psi(r_n) x^n + \cdots + \psi(r_0) \\ &= \psi(r_n)\psi(x^n) + \cdots + \psi(r_0) \\ &= \psi(r_n x^n + \cdots + r_0) \end{aligned}$$

Since $r_n x^n + \cdots + r_0 \in R[x]$, we proved that $im(\psi)$ is surjective.

We now prove that $ker(\psi) = I[x]$. Let $b_n x^n + \cdots b_0 \in I[x]$. We note that $\psi(b_n x^n + \cdots b_0) = [b_n]_I x^n + \cdots + [b_0]_I$. For $0 \leq k \leq n$, we note that $b_k \in I$, so $[b_k]_I = 0$. Hence, $\psi(b_n x^n + \cdots b_0) = 0x^n + \cdots + 0 = 0$. This shows that $I[x] \subset ker(\psi)$. Meanwhile, let $b_n x^n + \cdots b_0 \in ker(\psi)$. Clearly, $\psi(b_n x^n + \cdots + b_0) = 0$. This implies that for each $0 \leq k \leq n$, we get that $\psi(b_k) = 0$, which further implies $[b_k]_I = 0$ and $b_k \in I$. Since each of its coefficients are in I, $b_n x^n + \cdots + b_0 \in I[x]$. Thus, we showed that $I[x] \supset ker(\psi)$. We can now conclude $I[x] = ker(\psi)$.

We satisfied all the conditions for the First Isomorphism Theorem, so $R[x]/I[x] \cong (R/I)[x]$. □

(b) Since the polynomial $f(x)$ is a unit, there exists a $g(x) \in R[x]^\times$ where $f(x)g(x) = 1$. Since a prime ideal is also defined to be a proper ideal, we can apply the homomorphism $\psi : R[x] \to (R/I)[x]$ from (a). We note that $\psi(f(x))$ is a unit in $(R/I)[x]$ because $\psi(f(x)) \cdot \psi(g(x)) = \psi(f(x)g(x)) = \psi(1) = 1$. We then note that from HW6 3(c), since I is a prime ideal, R/I is an integral domain. From Lemma 9.3, this implies $\psi(f(x))$ is a constant. Since $\psi(f(x)) = [a_n]_I x^n + \cdots + [a_0]_I$ and its degree is 0 from being a constant, this implies that for $i \geq 1$ that $[a_i]_I = 0$. In other words, it implies $a_i \in I$ as desired. $\square$

(c) We note that for $0 \leq r \leq 2024$, $[r]$ represents each element in $\mathbb{Z}/2025\mathbb{Z}$ bijectively.

Claim: $[r]$ is nilpotent iff $15 \mid r$.

Let r be arbitrary and assume that for some positive integer n that $[r]^n = [r^n] = 0$. This implies that $2025 \mid r^n$. Since $3 \mid 2025$ and $5 \mid 2025$, we get that $3 \mid r^n$ and $5 \mid r^n$. By Euclid's Lemma, since 3 is prime, either $3 \mid r$ or $3 \mid r^{n-1}$. If $3 \mid r$, we are done. If not, then $3 \mid r^{n-1}$, so we can repeat the process with $3 \mid r$ or $3 \mid r^{n-2}$. Since $3 \nmid r$, it must be that $3 \mid r^{n-2}$. We can repeat this process until we reach $3 \mid r$ or $3 \mid r^0 = 1$. Since $3 \nmid 1$, we reach a contradiction, so it must be that $3 \mid r$. Since 5 is also a prime, we can apply the same process to get $5 \mid r$. We note that $\gcd(3, 5) = 1$, so $3 \cdot 5 \mid r$ as desired.

For the converse, assume $15 \mid r$, so there exists some integer q such that $r = 15q$. If we set $n = 4$, we notice that $[(15q)^4] = [3^4 \cdot 5^4 \cdot q^4] = [25 \cdot 2025 \cdot q^4] = 0$. Thus, $[r]$ is a nilpotent element. $\square$

The claim implies that we only need to look for multiples of 15 within the range of r to search for all nilpotent elements. Hence, there exist $\lfloor 2025/15 \rfloor = 134$ nonzero r's that are multiples of 15. Since $15 \mid 0$, we include it to get that there exist $134 + 1 = 135$ nilpotent elements in $\mathbb{Z}/2025\mathbb{Z}$. $\square$

(d) Let I be a prime ideal of R and r be a nilpotent element in R where $r^n = 0$ for some positive integer n. Since I is an ideal, $r^n \in I$. Since I is a prime ideal, either $r \in I$ or $r^{n-1} \in I$. If $r \in I$, we are done. If not, then $r^{n-1} \in I$, so we can repeat the process with $r \in I$ or $r^{n-2} \in I$. Since $r \notin I$, it must be that $r^{n-2} \in I$. We can repeat this process until we would reach $r^1 = r \in I$, a contradiction. Hence, it must be that $r \in I$. This implies that all nilpotent elements in R belong to every prime ideal of R. $\square$

(e) Let r be a nilpotent elemnt in R where $r^n = 0$ for some positive integer n. We note that $n \geq 2$ because r is a non-zero element.

Claim: $-rx + 1$ is unit in $R[x]$.

$$
\begin{aligned}
(-rx+1)(r^{n-1}x^{n-1} + \cdots + rx + 1) &= -(rx-1)(r^{n-1}x^{n-1} + \cdots + rx + 1) \\
&= -(r^n x^n - 1) \\
&= -(-1) \\
&= 1
\end{aligned}
$$

Hence, there exist a polynomial $f(x) \in R[x]$ where $(-rx + 1)f(x) = 1$. This proves $-rx + 1$ is a unit in $R[x]$. $\square$

Since $-rx + 1$ is a non-constant unit, we proved the existence of an $f(x) \in R[x]^\times$ that is not a constant. $\square$

2. (a) We begin by noting that:

$$\begin{aligned}\alpha^m - 1 &= \prod_{d|m} \Phi_d(\alpha) \\ &= \prod_{\substack{d|m \\ d\neq m}} \Phi_d(\alpha) \cdot \Phi_m(\alpha) \\ &= \prod_{\substack{d|m \\ d\neq m}} \Phi_d(\alpha) \cdot 0 \\ &= 0\end{aligned}$$

Thus, we get that $\alpha^m = 1$. This implies the existence of $o(\alpha)$ and that $o(\alpha) \mid m$. This also implies that $o(\alpha) \leq m$. Let us denote $b = o(\alpha)$ and assume that $b < m$. Since $b \mid m$, any divisor of b is also a divisor of m, which allows us to obtain this expression:

$$\begin{aligned}x^m - 1 &= \Phi_m(x) \cdot \prod_{d|b} \Phi_d(x) \cdot \prod_{\substack{d|m \\ d\nmid b \\ d\neq m}} \Phi_d(x) \\ &= \Phi_m(x) \cdot (x^b - 1) \cdot \prod_{\substack{d|m \\ d\nmid b \\ d\neq m}} \Phi_d(x)\end{aligned}$$

By its definition, $\alpha^b = 1$, so $\alpha^b - 1 = 0$. This implies that α is a root for both $\Phi_m(x)$ and $(x^b - 1)$. By Corollary 9.7, since F is an integral domain from being a field, there exist polynomials $h(x), g(x) \in F[x]$ where $\Phi_m(x) = (x - \alpha)h(x)$ and $(x^b - 1) = (x - \alpha)g(x)$. This allows us to obtain the expression that:

$$x^m - 1 = (x - \alpha)(x - \alpha)h(x)g(x) \prod_{\substack{d|m \\ d\nmid b \\ d\neq m}} \Phi_d(x)$$

This implies that α is a repeated root of $x^m - 1$. However, we note that $(\alpha^m - 1)' = m\alpha^{m-1}$. Notice that $m\alpha^{m-1} = m\alpha^m\alpha^{-1}$. We note that $m\alpha^m = m(1)$ and since $p \nmid m$, $m(1)$ must be non-zero. Since α^{-1} is also a non-zero from being a unit and that F is an integral domain from being a field, this implies that $m\alpha^{m-1}$ is a non-zero element. By Proposition 9.12, this implies that α is not a repeated root for $x^m - 1$, which is a contradiction. Thus, it must be that $b = m$, so we get that $o(\alpha) = m$ as desired. □

(b) **Claim:** $\Phi_m(\alpha) = 0$

We note that:

$$\begin{aligned}\alpha^m - 1 &= \prod_{d|m} \Phi_d(\alpha) \\ &= \prod_{\substack{d|m \\ d\neq m}} \Phi_d(\alpha) \cdot \Phi_m(\alpha)\end{aligned}$$

We then note that for every divisor of m that is not equal to m, we get that $d < m$, so $\alpha^d - 1 \neq 0$ because of $o(\alpha)$'s minimality. Since $\Phi_d(x)$ is a factor of $x^d - 1$, we get that $\Phi_d(\alpha)$ must be non-zero. Since F is an integral domain from being a field we note that:

$$\prod_{\substack{d|m \\ d\neq m}} \Phi_d(\alpha) \neq 0$$

Thus, since $\alpha^m - 1 = 0$, with all other factors being non-zero, this implies that $\Phi_m(\alpha) = 0$. $\square$

Claim: $\Phi'_m(\alpha) \neq 0$

By contradiction, $\Phi'_m(\alpha) = 0$. By Proposition 9.12, this implies that α is a repeated root for $\Phi_m(x)$ as $\Phi_m(\alpha) = 0$. Since $\Phi_m(x)$ is a factor of $x^m - 1$, α is also a repeated root of $x^m - 1$. By Proposition 9.12 again, this implies that $(\alpha^m - 1)' = 0$. However, since $\alpha^m = 1$, we can apply the same reasoning from (a) to deduce that $m\alpha^{m-1} \neq 0$, which is a contradiction. Hence, it must be that $\Phi'_m(\alpha) \neq 0$. $\square$