Math 412. Adventure sheet on the First Isomorphism Theorem

NOETHER'S FIRST ISOMORPHISM THEOREM: *Let $R \xrightarrow{\phi} S$ be a surjective homomorphism of rings. Let I be the kernel of ϕ. Then R/I is isomorphic to S.*

A: Fix any real number a. Consider the evaluation map

$$\eta : \mathbb{R}[x] \to \mathbb{R} \qquad f \mapsto f(a)$$

(1) Understand why the evaluation map is a **surjective ring homomorphism.**
(2) Prove[1] that the kernel of η is the ideal $I = (x-a)$ of $\mathbb{R}[x]$ generated by $x - a$.
(3) Use the first isomorphism theorem to prove that $\mathbb{R}[x]/(x-a)$ is isomorphic to $\mathbb{R}$.
(4) Give a direct proof that $\mathbb{R}[x]/(x-a) \cong \mathbb{R}$ by thinking about the congruence classes $f + (x-a)$.[2] Why is there a bijection with $\mathbb{R}$ that preserves the ring structure?

Solution.

(1) For any $\lambda \in \mathbb{R}$, the constant polynomial λ is taken to λ. This is a ring homomorphism because $1 \mapsto 1$, $\eta(f+g) = f(a) + g(a) = \eta(f) + \eta(g)$, and $\eta(fg) = f(a)g(a) = \eta(f)\eta(g)$.
(2) Elements in I are of the form $g(x)(x-a)$, and $\eta(g(x)(x-a)) = g(a) \cdot (a-a) = 0$. On the other hand, suppose $g \in \ker \eta$, and use the division algorithm to write $g(x) = h(x)(x-a) + r(x)$, where $r(x) = 0$ or has degree 0. Then $r(x) = r$ is a constant polynomial, and

$$0 = \eta\left(h(x)(x-a) + r(x)\right) = 0 + \eta(r(x)) = r.$$

Therefore, $g \in (x-a)$.
(3) We have shown that η is a surjective ring homomorphism with kernel I. The statement follows by the First Isomorphism Theorem.

B: Let i be the complex number $\sqrt{-1}$. Consider the ring homomorphism

$$\phi : \mathbb{R}[x] \to \mathbb{C} \qquad f \mapsto f(i)$$

(1) Prove that ϕ is **surjective**.
(2) Prove that $x^2 + 1 \in \ker \phi$.
(3) Prove that the kernel contains no (nonzero) polynomial of degree less than two.
(4) Prove that $x^2 + 1$ generates $\ker \phi$. [Hint: If $f(x)$ is in the kernel, use the division algorithm to divide f by $x^2 + 1$ and see what happens under ϕ.]
(5) Use the First Isomorphism Theorem to explain how to think about the complex numbers as a quotient of the polynomial ring $\mathbb{R}[x]$.

Solution.

(1) For any $\lambda \in \mathbb{C}$, the constant polynomial λ is taken to λ.
(2) $i^2 + 1 = 0$.

[1] Hint for the harder direction: say $g \in \ker \eta$, and use the division algorithm to divide g by $x - a$; apply η.
[2] Hint: For quotient rings of polynomial rings over a field, every congruence class contains a unique [what?]

(3) The kernel contains no nonzero constant polynomial, ϕ is the identity map on constants. Given a polynomial of degree 1, say $f(x) = bx + c$, $\phi(f) = bi + c = 0$ if and only if both imaginary parts are 0, meaning $b = c = 0$.

(4) Consider any $f \in \mathbb{C}[x]$ in the kernel of ϕ. If $r \in \mathbb{C}[x]$ is the remainder of dividing f by $x^2 + 1$, either $r = 0$ or r has degree at most 1. But

$$0 = \phi(f) = \phi(q(x^2 + 1) + r) = \phi(r),$$

so r must be in the kernel of ϕ as well. We have shown there are no nonzero polynomials of degree at most 1 in the kernel of ϕ, so $r = 0$. Therefore, $f \in (x^2+1)$, and since we have shown that $x^2 + 1$ is in the kernel of ϕ, we conclude that $(x^2 + 1)$ is the kernel of ϕ.

(5) We have shown that ϕ is a surjective ring homomorphism with kernel $(x^2 + 1)$, so the First Isomorphism Theorem says that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

C: Proof of the First Isomorphism Theorem. Fix a surjective ring homomorphism $\phi : R \to S$. Let I be its kernel, Define $\overline{\phi} : R/I \to S$ by $\overline{\phi}(r + I) = \phi(r)$.

(1) Show that $\overline{\phi}$ is a well-defined map.
(2) Show that $\overline{\phi}$ is a surjective ring homomorphism.
(3) Show that $\overline{\phi}$ is injective.
(4) Prove the First Isomorphism Theorem.

Solution.

(1) Given $r, s \in R$ such that $r - s \in I$,

$$\phi(r) - \phi(s) = \phi(r - s) = 0,$$

so $\phi(r) = \phi(s)$.

(2) Given any class $s \in S$, pick $r \in R$ such that $\phi(r) = s$. Then $\overline{\phi}(r + I) = \phi(r) = s$. Moreover,

$$\overline{\phi}(1 + I) = \phi(1) = 1,$$

$$\overline{\phi}\left((r + I) + (s + I)\right) = \overline{\phi}\left((r + s) + I\right) = \phi(r + s) = \phi(r) + \phi(s) = \overline{\phi}(r + I) + \overline{\phi}(s + I),$$

and similarly for the multiplication.

(3) If $r + I$ is in the kernel of $\overline{\phi}$, then

$$\phi(r) = \overline{\phi}(r + I) = 0$$

and $r \in I$, so $r + I = 0$.

(4) We have found an explicit isomorphism $\overline{\phi}$ between R/I and S.

D: New proofs for old facts.

(1) Show that whenever n and m are relatively prime integers, $\mathbb{Z}_{mn} \cong \mathbb{Z}_n \times \mathbb{Z}_m$.[3]
(2) Let k be a field, $d \geqslant 1$, and $R = k[x_1, \ldots, x_d]$. Show that $R/(x_1, \ldots, x_d) \cong k$.

Solution.

[3] We have done this in a problem set! But now we can give a new proof using the First Isomorphism Theorem.

(1) Consider the ring homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$ given by $a \mapsto ([a]_n, [a]_m)$. This is a surjective ring homomorphism by the Chinese Remainder Theorem, which we proved in a problem set, and its kernel is (nm). By the First Isomorphism Theorem, $\mathbb{Z}/(nm) \cong \mathbb{Z}_n \times \mathbb{Z}_m$.
(2) Consider the evaluation map $R \longrightarrow k$ given by $f \mapsto f(0)$. This is a surjective ring homomorphism with kernel $(x_1, \ldots, x_d)$, so by the First Isomorphism Theorem, $R/(x_1, \ldots, x_d) \cong k$.

E: PRIME IDEALS. An ideal $P \subsetneq R$ in a commutative ring R is prime if $fg \in P$ implies $f \in P$ or $g \in P$.

(1) Show that an ideal P is a prime ideal if and only if R/P is a domain.
(2) What are the prime ideals in $\mathbb{Z}$?
(3) Show that the ideal (x, y) in $\mathbb{Z}[x, y]$ is prime.

Solution.

(1) Suppose R/P is a domain. Consider $f, g \in R$ such that $fg = 0$. Then $(f + P)(g + P) = 0 + P$, so either $f + P = 0 + P$ or $g + P = 0 + P$. If $f + P = 0 + P$, that means $f \in P$. On the other hand, assume P is prime, and consider two nonzero elements $f + P, g + P \in R/P$. Then $f \notin P$ and $g \notin P$, so $fg \notin P$ and $(f + P)(g + P) = fg + P \neq 0$.
(2) The (principal) ideals generated by prime integers.
(3) Similarly to what we have done before, we can use the first Isomorphism Theorem to show $\mathbb{Z}[x, y]/(x, y) \cong \mathbb{Z}$, which is a domain.