Chapter 10. Ring Homomorphisms, Ideals and Quotient Rings

10.1 Definition: Let R and S be rings. A **ring homomorphism** from R to S is a map $\phi : R \to S$ such that

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and}$$
$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in R$. The **kernel** of ϕ is the set

$$\text{Ker}(\phi) = \phi^{-1}(0) = \left\{ a \in R \middle| \phi(a) = 0 \right\}$$

and the **image** (or **range**) of ϕ is the set

$$\text{Image}(\phi) = \phi(R) = \left\{ \phi(a) \middle| a \in R \right\}.$$

A ring **isomorphism** from R to S is a bijective ring homomorphism from R to S. For two rings R and S, we say that R and S are **isomorphic**, and we write $R \cong S$, when there exists an isomorphism $\phi : R \to S$.

10.2 Theorem: *Let $\phi : R \to S$ be a ring homomorphism. Then*
(1) $\phi(0) = 0$,
(2) for $a \in R$ we have $\phi(ka) = k\phi(a)$ for all $k \in \mathbb{Z}$,
(3) if R has a 1 and ϕ is surjective, then S has a 1 and $\phi(1) = 1$,
(4) for $a \in R$ we have $\phi(a^k) = \phi(a)^k$ for all $k \in \mathbb{Z}^+$, and
(5) if R has a 1, ϕ is surjective, and $a \in R$ is a unit, then $\phi(a^k) = \phi(a)^k$ for all $k \in \mathbb{Z}$.

10.3 Theorem: *Let $\phi : R \to S$ and $\psi : S \to T$ be ring homomorphisms. Then*
(1) the identity map $I : R \to R$ is a ring homomorphism,
(2) the composite $\psi \circ \phi : R \to T$ is a ring homomorphism, and
(3) if ϕ is bijective then the inverse $\phi^{-1} : S \to R$ is a ring homomorphism.

10.4 Corollary: I*somorphism is an equivalence relation on the class of rings.*

10.5 Theorem: *Let $\phi : R \to S$ be a ring homomorphism. Then*
(1) If K is a subring of R then $\phi(K)$ is a subring of S. In particular, Image(ϕ) is a subring of S.
(2) if L is a subring of S then $\phi^{-1}(L)$ is a subring of R. In particular, Ker(ϕ) is a subring of R.

10.6 Theorem: *Let $\phi : R \to S$ be a ring homomorphism. Then*
(1) ϕ is injective if and only if Ker$(\phi) = \{0\}$, and
(2) ϕ is surjective if and only if Image$(\phi) = S$.

10.7 Example: For rings R and S, the **zero function** $0 : R \to S$, given by $0(x) = 0$ for all $x \in R$, is a ring homomorphism. For a ring R, the **identity function** $I : R \to R$, given by $I(x) = x$ for all $x \in R$, is a ring homomorphism.

10.8 Example: Let R be a ring. For $a \in R$, define $\phi_a : \mathbb{Z} \to R$ by $\phi_a(k) = ka$. Show that the ring homomorphisms $\phi : \mathbb{Z} \to R$ are the maps $\phi = \phi_a$ with $a \in R$ such that $a^2 = a$.

Solution: For $a \in R$, let $\phi_a : \mathbb{Z} \to R$ be the map given by $\phi_a(k) = ka$. Note that for any ring homomorphism $\phi : \mathbb{Z} \to R$, if we let $a = \phi(1)$ then for all $k \in \mathbb{Z}$ we have $\phi(k) = \phi(k \cdot 1) = k \cdot \phi(1) = ka = \phi_a(k)$. Thus every ring homomorphism $\phi : \mathbb{Z} \to R$ is of the form $\phi = \phi_a$ for some $a \in R$. Also note that in order for ϕ_a to be a ring homomorphism, we must have $a^2 = \phi(1)^2 = \phi(1^2) = \phi(1) = a$. Finally, note that given $a \in R$ with $a^2 = a$, the map ϕ_a is a ring homomorphism because $\phi_a(k+l) = (k+l)a = ka + la = \phi_a(k) + \phi_l(a)$ and $\phi_a(kl) = (kl)a = (kl)a^2 = (ka)(la) = \phi_a(k)\phi_l(a)$. Thus the ring homomorphisms from $\mathbb{Z}$ to R are precisely the maps ϕ_a where $a \in R$ with $a^2 = a$.

10.9 Example: Let R be a ring. For $a, b \in R$, define the map $\phi_{a,b} : \mathbb{Z} \times \mathbb{Z} \to R$ by $\phi_{a,b}(k, l) = (ka)(lb)$. As an exercise, show that the ring homomorphisms $\phi : \mathbb{Z} \times \mathbb{Z} \to R$ are the maps $\phi = \phi_{a,b}$ with $a, b \in R$ such that $a^2 = a$, $b^2 = b$ and $ab = ba = 0$.

10.10 Definition: An element a in a ring R is called **idempotent** when $a^2 = a$.

10.11 Example: The complex conjugation map $\phi : \mathbb{C} \to \mathbb{C}$ given by $\phi(z) = \overline{z}$ is a ring homomorphism since $\overline{z + w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\,\overline{w}$, but the norm map $\psi(z) = ||z||$ is not a ring homomorphism because, in general, we do not have $||z + w|| = ||z|| + ||w||$.

10.12 Definition: Let R be a ring. For $a \in R$, the map $\phi_a : R[x] \to R$ given by $\phi_a\big(f(x)\big) = f(a)$, that is by

$$\phi_a\Big(\sum_{i=0}^{n} c_i x^i\Big) = \sum_{i=0}^{n} c_i a^i,$$

is called the **evaluation map** at a. If $a \in Z(R)$ then ϕ_a is a homomorphism because for $f = \sum b_i x^i$ and $g = \sum c_i x^i$ we have

$$\phi_a(f + g) = \phi_a\big(\sum_i (b_i + c_i)x^i\big) = \sum_i (b_i + c_i)a^i = \sum_i b_i a^i + \sum_i c_i x^i = \phi_a(f) + \phi_a(g)$$
$$\phi_a(fg) = \phi_a\big(\sum_{i,j} b_i c_j x^{i+j}\big) = \sum_{i,j} b_i c_j a^{i+j} = \sum_{i,j} b_i a^i c_j a^j = \sum_i b_i x^i \sum_j c_j a^j = \phi_a(f)\phi_a(g).$$

The **evaluation map** $\phi : R[x] \to \mathrm{Func}(R, R)$ is then given by $\phi(f)(a) = \phi_a(f) = f(a)$, in other words ϕ sends the polynomial $f(x) = \sum c_i x^i$ to the function $f(x) = \sum c_i x^i$. If R is commutative, then the above calculation shows that this map ϕ is a homomorphism. If R is not commutative, then the multiplication operations in $R[x]$ and in $\mathrm{Func}(R, R)$ are different and the evaluation map is not a homomorphism (in fact we are usually only interested in the polynomial ring $R[x]$ in the case that R is commutative).

10.13 Example: Show that $\mathbb{R} \not\cong \mathbb{C}$ (as rings).

Solution: If $\phi : \mathbb{R} \to \mathbb{C}$ was a ring isomorphism, then the restriction of ϕ to $\mathbb{R}^*$ would be a group isomorphism $\phi : \mathbb{R}^* \to \mathbb{C}^*$. But we know that the groups $\mathbb{R}^*$ and $\mathbb{C}^*$ are not isomorphic.

10.14 Example: Show that $2\mathbb{Z} \not\cong 3\mathbb{Z}$ (as rings).

Solution: In $2\mathbb{Z}$ we have $2 \cdot 2 = 4 = 2 + 2$, but there is no element $0 \neq a \in 3\mathbb{Z}$ with $a \cdot a = a + a$.

10.15 Theorem: (*Ideals and Quotient Rings*) *Let S be a subring of a ring R. Note that S is a subgroup of R under addition. Let R/S be the quotient group $R/S = \{a+S \big| a \in \mathbb{R}\}$ with addition operation given by $(a+S)+(b+S) = (a+b)+S$. We can define a multiplication operation on R/S by*

$$(a+S)(b+S) = ab+S$$

if and only if S has the property that for all $r \in R$ and $s \in S$ we have

$$rs \in S \text{ and } sr \in S.$$

In this case R/S is a ring under the above addition and multiplication operations. If R has identity 1, then R/S has identity $1+S$.

Proof: Suppose the formula $(a+S)(b+S) = ab+S$ gives a well-defined operation on R/S. Then for all $a_1, a_2, b_1, b_2 \in R$, if $a_1+S = a_2+S$ and $b_1+S = b_2+S$ then $a_1b_1+S = a_2b_2+S$. Equivalently, for all $a_1, b_1, a_2, b_2 \in R$, if $a_1 - a_2 \in S$ and $b_1 - b_2 \in S$ then $a_1a_2 - b_1b_2 \in S$. Let $r \in R$ and $s \in S$. Taking $a_1 = a_2 = r$, $b_1 = s$ and $b_2 = 0$, we have $a_1 - a_2 = 0 \in S$ and $b_1 - b_2 = s \in S$ and so $rs = a_1b_1 - a_2b_2 \in S$. Similarly, taking $a_1 = s$, $a_2 = 0$ and $b_1 = b_2 = r$ we see that $sr \in S$.

Conversely, suppose that for all $r \in R$ and $s \in S$ we have $rs \in S$ and $sr \in S$. Let $a_1, a_2, b_1, b_2 \in R$ with $a_1 - a_2 \in S$ and $b_1 - b_2 \in S$. Say $a_1 - a_2 = s \in S$ and $b_1 - b_2 = t \in S$. Then $a_1b_1 - a_2b_2 = a_1b_1 - (a_1 - s)(b_1 - t) = a_1b_1 - (a_1b_1 - a_1t - s\,b_1 + st) = a_1t + s\,b_1 + st \in S$. Thus the formula $(a+S)(b+S) = ab+S$ gives a well-defined operation on R/S.

Now we suppose that S has the required property so that $(a+S)(b+S) = ab+S$ does give a well-defined multiplication operation. This multiplication is associative because

$$\begin{aligned}\big((a+S)(b+S)\big)(c+S) &= (ab+S)(c+S) = (ab)c+S = a(bc)+S \\ &= (ab+S)(c+S) = (a+S)\big((b+S)(c+S)\big)\end{aligned}$$

and it is distributive over the addition operation on R/S because

$$\begin{aligned}(a+S)\big((b+S)+(c+S)\big) &= (a+S)\big((b+c)+S\big) = a(b+c)+S = ab+ac+S \\ &= (ab+S)+(ac+S) = (a+S)(b+S)+(a+S)(c+S)\end{aligned}$$

and similarly $\big((a+S)+(b+S)\big)(c+S) = (a+S)(c+S)+(b+S)(c+S)$. Thus R/S is a ring under these two operations.

10.16 Definition: Let R be a ring. An **ideal** in R is a subring $A \subseteq R$ with the property that for all $r \in R$ and $a \in A$ we have $ra \in A$ and $ar \in A$. When A is an ideal in R, the ring R/A, equipped with the operations of the above theorem, is called the **quotient ring** of R by A. It is easy to check that the zero element in R/A is $0+A$, the additive inverse of $a+A$ in R/A is $-(a+A) = -a+A$, if R has identity 1 then R/A has identity $1+A$, and if $a \in R$ is a unit then $a+A$ is a unit in R/A with $(a+A)^{-1} = a^{-1}+A$.

10.17 Example: In the cyclic group $\mathbb{Z}$, the subgroups are the groups $\langle n \rangle = n\mathbb{Z}$ with $n \geq 0$. Each of these subgroups is also an ideal in the ring $\mathbb{Z}$. For $n \in \mathbb{Z}^+$, the ring $\mathbb{Z}_n$ is the quotient ring $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle = \mathbb{Z}/n\mathbb{Z}$.

10.18 Example: In the group $\mathbb{Z}_n$ the subgroups are the groups $\langle d \rangle$ where $d \big| n$. Each of the subgroups is also an ideal in the ring $\mathbb{Z}_n$.

10.19 Example: In the group $\mathbb{Q}$, we have the subgroup $\langle 2\rangle = \{\cdots, -2, 0, 2, 4, \cdots\} = 2\mathbb{Z}$. This subgroup is also a subring of $\mathbb{Q}$ because it is closed under multiplication. But it is not an ideal in $\mathbb{Q}$ because it is not closed under multiplication by elements in $\mathbb{Q}$, for example $2 \in \langle 2\rangle$ and $\frac{1}{2} \in \mathbb{Q}$, but $1 = 2 \cdot \frac{1}{2} \notin \langle 2\rangle$.

10.20 Definition: Let R be a ring and let $U \subseteq R$. The **ideal in R generated by U**, denoted by $\langle U\rangle$, is the smallest ideal in R which contains U, or equivalently, the intersection of all ideals in R which contain U. The elements in U are called **generators** of $\langle U\rangle$. When U is finite we often omit the set brackets, so for $U = \{u_1, u_2, \cdots, u_n\}$ we write $\langle U\rangle = \langle u_1, u_2, \cdots, u_n\rangle$. An ideal of the form $\langle u_1, u_2, \cdots, u_n\rangle$ for some $u_i \in R$ is said to be **finitely generated**. An ideal of the form $\langle u\rangle$ for some $u \in R$ is called a **principal ideal**.

10.21 Theorem: *Let R be a ring and let U be a non-empty subset of R.*

(1) If R has a 1 then $\langle U\rangle = \left\{ \sum_{i=1}^{n} r_i u_i s_i \,\middle|\, n \in \mathbb{Z}^+, u_i \in U, r_i, s_i \in R \right\}$.

(2) If R is commutative with 1 then $\langle U\rangle = \left\{ \sum_{i=1}^{n} u_i r_i \,\middle|\, n \in \mathbb{Z}^+, u_i \in U, r_i \in R \right\}$. *In particular, for $a \in R$ we have* $\langle a\rangle = \{ar \,|\, r \in R\}$.

10.22 Note: In a field F, the only ideals are $\{0\}$ and F. Indeed let A be an ideal in F with $A \neq \{0\}$. Choose $0 \neq a \in A$. Since $a \in A$ and $a^{-1} \in F$, we must have $1 = a\,a^{-1} \in A$. Given any element $x \in F$, since $1 \in A$ and $x \in F$ we must have $x = x \cdot 1 \in A$. Thus $A = F$.

10.23 Definition: Let A and B be ideals in a ring R. The **intersection**, **sum** and the **product** of A and B are the sets

$$\begin{aligned} A \cap B &= \{a \in R \,|\, a \in A \text{ and } a \in B\}, \\ A + B &= \{a + b \,|\, a \in A, b \in B\} \text{ , and} \\ AB &= \left\{ \sum_{i=1}^{n} a_i b_i \,\middle|\, n \in \mathbb{Z}^+, a_i \in A, b_i \in B \right\}. \end{aligned}$$

As an exercise, show that $A \cap B$, $A + B$ and AB are all ideals in R.

10.24 Example: In $\mathbb{Z}$, for $k, l \in \mathbb{Z}^+$ verify that

$$\begin{aligned} \langle k\rangle \cap \langle l\rangle &= \langle m\rangle \text{ where } m = \text{lcm}(k, l) \\ \langle k\rangle + \langle l\rangle &= \langle d\rangle \text{ where } d = \gcd(k, l), \text{ and} \\ \langle k\rangle\langle l\rangle &= \langle kl\rangle. \end{aligned}$$

10.25 Theorem: (*The First Isomorphism Theorem*) *Let $\phi : R \to S$ be a homomorphism of rings. Let $K = \text{Ker}((\phi)$. Then K is an ideal in R and we have $R/K \cong \phi(R)$. Indeed the map $\Phi : R/K \to \phi(R)$ given by $\Phi(a + K) = \phi(a)$ is a ring isomorphism.*

10.26 Theorem: (*The Second Isomorphism Theorem*) *Let A and B be ideals in a ring R. Then A is an ideal in $A + B$, $A \cap B$ is an ideal in B, and*

$$(A + B)/A \cong B/(A \cap B).$$

10.27 Theorem: (*The Third Isomorphism Theorem*) *Let A and B be ideals in a ring R with $A \subseteq B \subseteq R$. Then B/A is an ideal in R/A and*

$$(R/A)/(B/A) \cong R/B.$$

10.28 Example: Let $d, n \in \mathbb{Z}^+$ with $d \big| n$. Then the map $\phi : \mathbb{Z}_n \to \mathbb{Z}_d$ given by $\phi(k) = k$ is a ring homomorphism with $\mathrm{Ker}(\phi) = \langle d \rangle$. By the First Isomorphism Theorem, we have $\mathbb{Z}_n / \langle d \rangle \cong \mathbb{Z}_d$.

10.29 Example: Define a map $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ by $\phi(f) = f(\sqrt{2})$. Then ϕ is a homomorphism because $\phi(f+g) = (f+g)(\sqrt{2}) = f(\sqrt{2}) + g(\sqrt{2}) = \phi(f) + \phi(g)$ and $\phi(fg) = (fg)(\sqrt{2}) = f(\sqrt{2})g(\sqrt{2}) = \phi(f)\phi(g)$. Also note that ϕ is surjective because $\phi(a+bx) = a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. Finally note that for $f \in \mathbb{Q}[x]$ we have

$$\begin{aligned} f(x) \in \mathrm{Ker}(\phi) &\iff f(\sqrt{2}) = 0 \in \mathbb{R} \iff f(\sqrt{2}) = f(-\sqrt{2}) = 0 \in \mathbb{R} \\ &\iff (x^2 - 2) \big| f(x) \iff f(x) \in \langle x^2 - 2 \rangle, \end{aligned}$$

where we used the fact that for $f(x) = \sum c_i x^i \in \mathbb{Q}[x]$ we have

$$f(\pm\sqrt{2}) = \Big(\sum c_{2k} 2^k \Big) \pm \Big(\sum c_{2k+1} 2^k \Big) \sqrt{2}$$

so that $f(\sqrt{2}) = 0 \iff f(-\sqrt{2}) = 0 \iff \sum c_{2k} 2^k = 0 = \sum c_{2k+1} 2^k$. By the First Isomorphism Theorem, we have $\mathbb{Q}[x]/\langle x^2 - 2 \rangle \cong \mathbb{Q}[\sqrt{2}]$.

10.30 Example: Define $\phi : \mathbb{R}[x] \to \mathbb{C}$ by $\phi(f) = f(i)$. Then ϕ is a homomorphism since $\phi(f+g) = (f+g)(i) = f(i) + g(i) = \phi(f) + \phi(g)$ and $\phi(fg) = (fg)(i) = f(i)g(i) = \phi(f)\phi(g)$. The map ϕ is surjective because $\phi(a+bx) = a + bi$ for $a, b \in \mathbb{R}$. Also, for $f(x) \in \mathbb{R}[x]$,

$$f(x) \in \mathrm{Ker}(\phi) \iff f(i) = 0 \in \mathbb{C} \iff (x^2+1) \big| f(x) \in \mathbb{R}[x] \iff f(x) \in \langle x^2 + 1 \rangle \subseteq \mathbb{R}[x].$$

Thus by the First Isomorphism Theorem, we have $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$.

10.31 Example: Define $\phi : \mathbb{Z}[i] \to \mathbb{Z}_5$ by $\phi(a + bi) = a + 2b$. The map ϕ is a ring homomorphism because

$$\begin{aligned} \phi\big((a+bi) + (c+di)\big) &= \phi\big((a+c) + (b+d)i\big) = (a+c) + 2(b+d) \\ &= (a+2b) + (c+2d) = \phi(a+bi) + \phi(c+di) \text{ , and} \\ \phi\big((a+bi)(c+di)\big) &= \phi\big((ac-bd) + (ad+bc)i\big) = (ac-bd) + 2(ad+bc) \\ &= ac + 2ad + 2bc + 4bd = (a+2b)(c+2d) = \phi(a+bi)\phi(c+di). \end{aligned}$$

Also note that ϕ is surjective because $\phi(a + 0i) = a$. We claim that $\mathrm{Ker}\,\phi = \langle 2 - i \rangle$. Let $a + ib \in \mathrm{Ker}\,\phi$ where $a, b \in \mathbb{Z}$. Then $a + 2b = 0 \in \mathbb{Z}_5$, say $a + 2b = 5t$ where $t \in \mathbb{Z}$. Then we have $a + ib = 5t - 2b + ib = (2-i)\big((2+i)t - b\big) \in \langle 2 - i \rangle$, and hence $\mathrm{Ker}\,\phi \subseteq \big\langle 2 - i \big\rangle$. On the other hand, if $a + ib \in \langle 2 - i \rangle$, say $a + ib = (2-i)(x+iy) = (2x+y) + i(2y-x)$, then we have $\phi(a+ib) = a + 2b = (2x+y) + 2(2y-x) = 5y = 0 \in \mathbb{Z}_5$, and hence $\langle 2 - i \rangle \subseteq \mathrm{Ker}\,\phi$. Thus $\mathrm{Ker}\,\phi = \langle 2 - i \rangle$, as claimed. By the First Isomorphism Theorem, it follows that $\mathbb{Z}[i]/\langle 2 - i \rangle \cong \mathbb{Z}_5$.

10.32 Definition: Let R be a commutative ring. Consider the evaluation homomorphism $\phi : R[x] \to \text{Func}(R,R)$ given by $\phi(f) = f$, that is the map which sends the polynomial $f(x)$ to the function $f(x)$. A polynomial $f \in R[x]$ is equal to zero when all of its coefficients are equal to zero. A function $f \in \text{Func}(R,R)$ is equal to zero when we have $f(a) = 0$ for all $a \in R$. The kernel of the evaluation homomorphism is

$$\text{Ker}(\phi) = \big\{ f \in R[x] \,\big|\, f(a) = 0 \text{ for all } a \in R \big\}.$$

The image $\phi\big(R[x]\big) \subseteq \text{Func}(R,R)$ is called the **ring of polynomial functions** on R. By the First Isomorphism Theorem, it is isomorphic to the quotient ring $R[x]\big/\text{Ker}(\phi)$.

10.33 Example: If R is an infinite field, then $\text{Ker}(\phi) = 0$ since for $f(x) \in R[x]$, if $f(a) = 0$ for all $a \in R$ then $f(x)$ has infinitely many roots, and so $f(x) = 0$ as a polynomial (a non-zero polynomial of degree $n \geq 0$ over a field has at most n roots). In this case, ϕ is injective so the polynomial ring $R[x]$ is isomorphic to the ring of polynomial functions $\phi\big(R[x]\big) \subseteq \text{Func}(R,R)$, and we often identify $R[x]$ with $\phi\big(R[x]\big)$.

If R is a finite field, the situation is quite different. In this case $R[x]$ is infinite but $\text{Func}(R,R)$ is finite, so $R[x]$ is certainly not isomorphic to a subring of $\text{Func}(R,R)$. Let us consider the case that $R = \mathbb{Z}_p$ where p is prime. By Fermat's Little Theorem, we know that $a^p = a$ for all $a \in \mathbb{Z}_p$, and so every $a \in \mathbb{Z}^p$ is a root of the polynomial $p(x) = x^p - x$. Since there are exactly p elements in $\mathbb{Z}_p$, it follows that $p(x)$ factors as

$$p(x) = x^p - x = (x-0)(x-1)(x-2)\cdots(x-(p-1)).$$

For a polynomial $f(x) \in \mathbb{Z}_p[x]$ we have

$$\begin{aligned} f(x) \in \text{Ker}(\phi) &\iff f(a) = 0 \text{ for all } a \in \mathbb{Z}_p \iff (x-a)\big|f(x) \text{ for all } a \in \mathbb{Z}_p \\ &\iff p(x)\big|f(x) \iff f(x) \in \big\langle p(x) \big\rangle = \langle x^p - x \rangle. \end{aligned}$$

Furthermore, we claim that ϕ is surjective. For $a \in \mathbb{Z}_p$, let $g_a(x) \in \mathbb{Z}_p[x]$ be the polynomial

$$g_a(x) = \frac{\displaystyle\prod_{i \in \mathbb{Z}_p, i \neq a} (x-i)}{\displaystyle\prod_{i \in \mathbb{Z}_p, i \neq a} (a-i)}.$$

Notice that for all $k \in \mathbb{Z}_p$ we have

$$g_a(k) = \delta_{a,k} = \begin{cases} 1 \text{ if } k = a, \\ 0 \text{ if } k \neq a. \end{cases}$$

Given any function $f(x) \in \text{Func}(\mathbb{Z}_p, \mathbb{Z}_p)$, for all $k \in \mathbb{Z}_p$ we have

$$\sum_{a \in \mathbb{Z}_p} f(a) g_a(k) = \sum_{a \in \mathbb{Z}_p} f(a) \delta_{a,k} = f(k).$$

It follows that $f(x) = \sum_{a \in \mathbb{Z}_p} f(a) g_a(x) \in \text{Func}(\mathbb{Z}_p, \mathbb{Z}_p)$. Notice that $\sum_{a \in \mathbb{Z}_p} f(a) g_a(x) \in \mathbb{Z}_p[x]$ and we have $f(x) = \phi\Big(\sum_{a \in \mathbb{Z}_p} f(a) g_a(x)\Big)$. Thus ϕ is surjective, as claimed. Thus the ring of polynomial functions $\phi\big(\mathbb{Z}_p[x]\big)$ is equal to the ring of all functions $\text{Func}(\mathbb{Z}_p, \mathbb{Z}_p)$, and by the First Isomorphism Theorem, we have $\mathbb{Z}_p[x]\big/\langle x^p - x \rangle \cong \phi\big(\mathbb{Z}_p[x]\big) = \text{Func}(\mathbb{Z}_p, \mathbb{Z}_p)$.