D-MATH | Algebra I | HS18

Prof. Rahul Pandharipande

Solution 4

Ideals, First Isomorphism Theorem

1. Let R be a commutative ring.

   (a) Show that there exists a unique ring homomorphism

   $$\varphi : R[X_1][X_2] \longrightarrow R[X_2][X_1]$$

   which sends $X_1 \mapsto X_1$, $X_2 \mapsto X_2$ and is the identity on R, and that φ is a ring isomorphism. This means that the order of the variables in the expression $R[X_1, X_2]$ is irrelevant.

   (b) Prove that there exists a ring isomorphism

   $$R[X_1, X_2]/X_1 R[X_1, X_2] \xrightarrow{\sim} R[X_2].$$

Solution:

(a) Recall the universal properties for polynomial rings: for every ring homomorphism $t : A \longrightarrow S$ and element $s \in S$, there exists a unique ring homomorphism $\hat{t} : A[X] \longrightarrow S$ such that $\hat{t} \circ \iota_A = t$, where $\iota_A : A \longrightarrow A[X]$ is the canonical inclusion. This can be expressed by a commutative diagram

$$\begin{tikzcd}
A \arrow[rr, "t"] \arrow[dr, hook] & & S & s \\
& A[X] \arrow[ur, dashed, "\exists!\hat{t}"] & X \arrow[ur, mapsto] &
\end{tikzcd}$$

or by saying that there is a bijection $\mathrm{Hom}(A[X], S) \xrightarrow{\sim} \mathrm{Hom}(A, S) \times S$ sending $f \mapsto (f \circ \iota_A, f(X))$.

Let $\theta_{21} : R \hookrightarrow R[X_2][X_1]$ be the composition of canonical inclusions

$$R \overset{\iota_2}{\hookrightarrow} R[X_2] \overset{\iota_{21}}{\hookrightarrow} R[X_2][X_1]$$

and $\theta_{12} : R \hookrightarrow R[X_1][X_2]$ the composition of canonical inclusions

$$R \overset{\iota_1}{\hookrightarrow} R[X_1] \overset{\iota_{12}}{\hookrightarrow} R[X_1][X_2].$$

Let S be any commutative ring and $u : R \longrightarrow S$ a ring homomorphism. Fix two elements $s_1, s_2 \in S$. By the universal property of the polynomial ring,

$$\exists! u_1 : R[X_1] \longrightarrow S \text{ ring hom.}: \begin{cases} \forall r \in R,\ u_1(\iota_1(r)) = u(r) \\ u_1(X_1) = s_1. \end{cases} \tag{1}$$

A second application of the universal property tells us that

$$\exists! u_{12} : R[X_1][X_2] \longrightarrow S \text{ ring hom.}: \begin{cases} \forall f \in R[X_1],\ u_{12}(\iota_{12}(f)) = u_1(f) \\ u_{12}(X_2) = s_2. \end{cases}$$

By uniqueness in (1), the first of the two conditions on u_{12} above is equivalent to saying that $u_{12}(\iota_{12}(X_1)) = s_1$ and $\varphi(\theta_{12}(r)) = u(r)$, so that we have proven the following result:

Lemma 1 (Universal property for bivariate polynomial rings)**.** *Let R and S be commutative rings, $u : R \longrightarrow S$ a ring homomorphism and $s_1, s_2 \in S$. Let ι_1, ι_{12} and $\theta_{12} = \iota_{12} \circ \iota_1$ be the canonical inclusion as above. Then*

$$\exists! u_{12} : R[X_1][X_2] \longrightarrow S \text{ ring hom.}: \begin{cases} \forall r \in R, \varphi(\theta_{12}(r)) = u(r) \\ u_{12}(\iota_{12}(X_1)) = s_1 \\ u_{12}(X_2) = s_2 \end{cases}$$

that is, such that the following diagram commutes:

$$\begin{tikzcd}
R \arrow[rr, "u"] \arrow[dr, hook, "\theta_{12}"'] & & S & s_1 & s_2 \\
& R[X_1, X_2] \arrow[ur, "\exists! u_{12}"'] & \iota_{12}(X_1) \arrow[ur, mapsto] & X_2 \arrow[ur, mapsto] &
\end{tikzcd}$$

Applying Lemma 1 to $S = R[X_2][X_1]$, $u = \theta_{21} : R \longrightarrow R[X_2][X_1]$, $s_1 = X_1$ and $s_2 = \iota_{21}(X_2)$, we see that there exists a unique ring homomorphism

$$\begin{aligned} \varphi : R[X_1][X_2] &\longrightarrow R[X_2][X_1] \\ \text{s.t. } \forall r \in R, \theta_{12}(r) &\longmapsto \theta_{21}(r), \\ \iota_{12}(X_1) &\longmapsto X_1 \text{ and} \\ X_2 &\longmapsto \iota_{21}(X_2) \end{aligned}$$

as desired. Notice that in the text of the exercise the natural inclusions are omitted for simplicity.

Let us now prove that φ is bijective by finding an inverse. Applying Lemma 1 with switched variable names to $S = R[X_1][X_2]$, $u = \theta_{12}$, $s_1 = \iota_{12}(X_1)$ and $s_2 = X_2$, we find a unique ring homomorphism

$$\begin{aligned} \varphi : R[X_2][X_1] &\longrightarrow R[X_1][X_2] \\ \text{s.t. } \forall r \in R, \theta_{21}(r) &\longmapsto \theta_{12}(r), \\ \iota_{21}(X_2) &\longmapsto X_2 \text{ and} \\ X_1 &\longmapsto \iota_{12}(X_1). \end{aligned}$$

We now prove that $\psi \circ \varphi = \mathrm{id}_{R[X_1][X_2]}$. Looking carefully, we see that

$$\begin{aligned} \psi \circ \varphi : R[X_1][X_2] &\longrightarrow R[X_1][X_2] \\ \text{sends } \forall r \in R, \theta_{12}(r) &\longmapsto \theta_{12}(r), \\ \iota_{12}(X_1) &\longmapsto \iota_{12}(X_1) \text{ and} \\ X_2 &\longmapsto X_2. \end{aligned}$$

Again by Lemma 1, there exists precisely one such a ring homomorphism and since the identity behaves as $\psi \circ \varphi$, we get $\psi \circ \varphi = \mathrm{id}_{R[X_1][X_2]}$. The equality $\varphi \circ \psi = \mathrm{id}_{R[X_2][X_1]}$ can be proven analogously. We can then conclude that φ is a ring isomorphism.

(b) From now on we will not spell out the canonical immersions $\iota : R \hookrightarrow R[X]$. By part (a), there is an isomorphism $\varphi : R[X_1, X_2] \xrightarrow{\sim} R[X_2, X_1] = R[X_2][X_1]$. Moreover, there is a unique ring homomorphism $\mathrm{ev}_0 : R[X_2][X_1] \longrightarrow R[X_2]$ which is the identity on $R[X_2]$ and sends $X_1 \mapsto 0$. Let $f = \mathrm{ev}_0 \circ \varphi : R[X_1, X_2] \longrightarrow R[X_2]$.

The map ev_0 is surjective has it contains the image of the identity on $R[X_2]$ which is all $R[X_2]$. Hence f is surjective. Moreover,

$$\begin{aligned} \ker(\mathrm{ev}_0) &= \left\{ f = \sum_{j=0}^{d} a_j X_1^j : a_j \in R[X_2], a_0 = 0 \right\} \\ &= \left\{ f = X_1 \cdot \sum_{j=1}^{d} a_j X_1^{j-1} : a_j \in R[X_2] \right\} = X_1 R[X_2][X_1]. \end{aligned}$$

Then $\ker(f) = \varphi^{-1}(X_1 R[X_2][X_1]) = X_1 R[X_1, X_2]$ because φ is an isomorphism. By the first isomorphism theorem, f induces an isomorphism

$$R[X_1, X_2]/X_1 R[X_1, X_2] = R[X_1, X_2]/\ker(f) \xrightarrow{\sim} \mathrm{im}(f) = R[X_2].$$

2. Let m be a positive integer. Prove that there exists a ring isomorphism

$$\mathbb{Z}[X]/m\mathbb{Z}[X] \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})[X].$$

Solution: The projection $\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ induces a unique ring homomorphism

$$\pi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}/m\mathbb{Z}[X]$$

sending $a \in \mathbb{Z}$ to the constant polynomial $a + m\mathbb{Z}$ and $X \mapsto X$. For every $f \in \mathbb{Z}[X]$, the polynomial $\overline{f} \in \mathbb{Z}/m\mathbb{Z}[X]$ is obtained by reducing each coefficient modulo m. Let $u = \sum_{i=1}^{d} u_i X^i \in \mathbb{Z}/m\mathbb{Z}[X]$. For each $u_i \in \mathbb{Z}/m\mathbb{Z}$ there exists a (canonical representative) $\hat{u}_i \in \{0, \dots, m-1\}$ such that $u_i = \hat{u}_i + m\mathbb{Z}$. Then for $f = \sum_{i=1}^{d} \hat{u}_i X^i \in \mathbb{Z}[X]$ we have $\pi(f) = u$. This implies that π is a surjective map [*It is* *true in general that if $\psi : R \longrightarrow S$ is a surjective ring homomorphism, the induced ring homomorphism $\overline{\psi} : R[X] \longrightarrow S[X]$ sending $X \mapsto X$ and $R \ni r \mapsto \psi(r)$ is surjective as well, since each coefficient of every polynomial in $S[X]$, as well as $X \in S[X]$ is in the image of ψ in S and hence in the image of $\overline{\psi}$ in $S[X]$].*

Moreover,

$$\begin{aligned}
\ker(\pi) = \{f \in \mathbb{Z}[X] : \pi(f) = 0\} &= \left\{ f = \sum_{j=0}^{d} a_j X^j \in \mathbb{Z}[X] : \sum_{j=0}^{d} (a_j + m\mathbb{Z}) X^j = 0 \right\} \\
&= \left\{ f = \sum_{j=0}^{d} a_j X^j \in \mathbb{Z}[X] : \forall j,\ a_j + m\mathbb{Z} = 0 \right\} \\
&= \left\{ f = \sum_{j=0}^{d} a_j X^j \in \mathbb{Z}[X] : \forall j,\ m | a_j \right\} = \{mf : f \in \mathbb{Z}[X]\} = m\mathbb{Z}[X].
\end{aligned}$$

Then, by the first isomorphism theorem, the map π induces a ring isomorphism

$$\mathbb{Z}[X]/m\mathbb{Z}[X] = \mathbb{Z}[X]/(\ker(\pi)) \xrightarrow{\sim} \mathrm{im}(\pi) = (\mathbb{Z}/m\mathbb{Z})[X].$$

3. Let $\varphi : R \longrightarrow S$ be a surjective ring homomorphism.

   (a) Prove: if $I \subset R$ is an ideal, then $\varphi(I)$ is an ideal.

   (b) Does (a) hold for any (i.e., not necessarily surjective) ring homomorphism?

   Solution:

   (a) Let $j, j' \in \varphi(I)$ and write $j = \varphi(i)$, $j' = \varphi(i')$ for some $i, i' \in I$. Then $i - i' \in I$ because I is an ideal, so that

   $$j - j' = \varphi(i) - \varphi(i') = \varphi(i - i') \in \varphi(I).$$

   This proves that $\varphi(I)$ is an abelian group. Notice that we did not use surjectivity of φ for this part.
   Now let $j = \varphi(i) \in \varphi(I)$ for $i \in I$ and $s \in S$. By surjectivity of φ, we can write $s = \varphi(r)$ for some $r \in R$. Then $ir \in I$ since I is an ideal, so that

   $$js = \varphi(i)\varphi(r) = \varphi(ir) \in \varphi(I).$$

   Altogether, this proves that $\varphi(I)$ is an ideal.

   (b) No, it does not. For instance, consider the immersion $\mathbb{Z} \hookrightarrow \mathbb{Q}$. The ideal $2\mathbb{Z}$ is mapped to $2\mathbb{Z} \subset \mathbb{Q}$, which is not an ideal, since for example $2 \cdot 2^{-1} = 1 \notin 2\mathbb{Z}$.

4. Which of the following ideals are principal? Prove that they are not or find a generator.

(a) $(88, 274)\mathbb{Z} \subseteq \mathbb{Z}$;

(b) $(X, Y)\mathbb{C}[X, Y] \subseteq \mathbb{C}[X, Y]$ (*Hint:* Suppose f is a generator. Look at the degree in X and Y of f);

(c) $(X, 2)\mathbb{Z}[X] \subseteq \mathbb{Z}[X]$;

(d) $(2i, 1 - i)\mathbb{Z}[i] \subseteq \mathbb{Z}[i]$ (*Hint:* Assignment 2, Exercise 5(b));

(*e) $(X, 2)\mathbb{Z}/4\mathbb{Z}[X] \subseteq \mathbb{Z}/4\mathbb{Z}[X]$ (*Hint:* Exercise 3).

Solution:

(a) As seen in class, every ideal in $\mathbb{Z}$ is principal. Moreover, $(88, 274)\mathbb{Z}$ is generated by $\gcd(88, 274)$ which can be obtained with the Euclidean division:

$$\begin{aligned} 274 &= 3 \cdot 88 + 10 \\ 88 &= 8 \cdot 10 + 8 \\ 10 &= 1 \cdot 8 + 2 \\ 8 &= 4 \cdot 2 \end{aligned}$$

Hence $(88, 274)\mathbb{Z} = 2\mathbb{Z}$. Notice that the Bezout identity obtained by the Euclidean division, i.e. $2 = 9 \cdot 274 - 28 \cdot 88$, proves the harder inclusion $(88, 274)\mathbb{Z} \supseteq 2\mathbb{Z}$.

(b) We prove that $(X, Y)\mathbb{C}[X, Y]$ is not a principal ideal in $\mathbb{C}[X, Y]$. Since $\mathbb{C}$ is an integral domain, the total degree of a product of polynomials $f, g \in \mathbb{C}[X, Y]$ is the sum of their total degrees. This can be checked by noticing that the total degree of $f \in \mathbb{C}[X, Y]$ can be defined as the degree of the polynomial $\pi(f) \in \mathbb{C}[X]$, where π is the unique ring homomorphism $\mathbb{C}[X, Y] \longrightarrow \mathbb{C}[X]$ extending $\mathrm{id}_{\mathbb{C}[X]}$ and sending $Y \mapsto X$.

Suppose that $(X, Y)\mathbb{C}[X, Y] = f\mathbb{C}[X, Y]$. Then f divides X, so that $\deg(f) \leqslant 1$. Moreover, $f \in (X, Y)\mathbb{C}[X, Y]$ implies that $f = Xf_1 + Yf_2$ for some $f_1, f_2 \in \mathbb{C}[X, Y]$, so that f has trivial constant term. Since $f \neq 0$ (as $(X, Y)\mathbb{C}[X, Y]$ is non-trivial), the only possibility is that $f = aX + bY$ for some $(a, b) \in \mathbb{C}^2 \smallsetminus \{(0, 0)\}$. Since $X = fg_1$ and $Y = fg_2$ for some $g_1, g_2 \in \mathbb{C}[X, Y]$, by degree reasons both g_1 and g_2 must be constants. The equality $X = fg_1$ implies that $b = 0$, whereas $Y = fg_2$ implies that $a = 0$, giving a contradiction. Hence $(X, Y)\mathbb{C}[X, Y]$ is not a principal ideal.

(c) We prove that $(X, 2)\mathbb{Z}[X]$ is not a principal ideal in $\mathbb{Z}[X, 2]$.

Suppose that $(X, 2)\mathbb{Z}[X] = f\mathbb{Z}[X]$ for some $f \in \mathbb{Z}[X]$. Since $\mathbb{Z}$ is an integral domain, the degree is additive. Then $f|2$ implies that f is constant. The only possibilities are $f = \pm 1$ and $f = \pm 2$. Since $f = 2g_0 + Xg_1$ for some $g_0, g_1 \in \mathbb{Z}[X]$, we see that $f \neq \pm 1$, so that the only possibility is that $f = \pm 2$ and $(X, 2)\mathbb{Z}[X] = 2\mathbb{Z}[X] = -2\mathbb{Z}[X]$. But $2 \nmid X$, because multiples of 2 are polynomials containing even coefficients only, which is a contradiction.

(d) By Assignment 2, Exercise 3, we can perform Euclidean division on $\mathbb{Z}[i]$ and this allows us to find a greatest common divisor.

We first divide $2i$ by $1-i$, as $|2i| = 2 > \sqrt{2} = |1-i|$. Notice that

$$\frac{2i}{1-i} = \frac{2i(1+i)}{1-i^2} = \frac{2i-2}{1-i^2} = i - 1 \in \mathbb{Z}[i],$$

so that $1-i$ is already the greatest common divisor. More simply, $2i \in (1-i)\mathbb{Z}[i]$, so that $(2i, 1-i)\mathbb{Z}[i] = (1-i)\mathbb{Z}[i]$ and it is a principal ideal.

(e) We want to prove that the given ideal is not principal. Since $\mathbb{Z}/4\mathbb{Z}$ is not a domain, we cannot use additivity of the degree on products.

In the notation of Exercise 3, one can prove that if $I = (r_1, \ldots, r_k)$, then $\varphi(I) = (\varphi(r_1), \ldots, \varphi(r_k))S$. Indeed, the elements $\varphi(r_j)$ lay in $\varphi(I)$ by definition and so does the ideal they generate since $\varphi(I)$ is an ideal in S by surjectivity of φ (here we are using that if an ideal contains some elements, then it contains the ideal they generate, which follows immediately from Exercise 7), whereas any element of $\varphi(I)$ can be written as $y = \varphi(\sum_{j=1}^k \lambda_j r_j)$ for some $\lambda_j \in R$, so that $y = \sum_{j=1}^k \varphi(\lambda_j)\varphi(r_j) \in (\varphi(r_1), \ldots, \varphi(r_k))S$.

Consider now the unique ring homomorphism $p : \mathbb{Z}/4\mathbb{Z}[X] \longrightarrow \mathbb{Z}/2\mathbb{Z}[X]$ which sends $X \mapsto X$ and reduces modulo 4 the coefficients. Let $I = (X, 2)\mathbb{Z}/4\mathbb{Z}[X]$. Then $p(I) = (X, 0)\mathbb{Z}/2\mathbb{Z}[X] = X\mathbb{Z}/2\mathbb{Z}[X]$. Suppose by contradiction that $I = f\mathbb{Z}/4\mathbb{Z}[X]$ for some $f \in \mathbb{Z}/4\mathbb{Z}[X]$. Then $p(I) = p(f)\mathbb{Z}/4\mathbb{Z}[X]$. Then $X|p(f)$ and $p(f)|X$ which means that $f = uX$ for some unit $u \in (\mathbb{Z}/2\mathbb{Z}[X])^\times = \{1\}$ since $\mathbb{Z}/2\mathbb{Z}$ is an integral domain (Assignment 3, Exercise 2). Hence $p(f) = X$ so that $f = X + 2g$ for some $g \in \mathbb{Z}/4\mathbb{Z}[X]$, which means that

$$\exists \ell \in \mathbb{Z}/4\mathbb{Z}[X] : \; f = 2 \pm X + X^2\ell.$$

Now suppose that $fg = 2$ for $g = a_0 + a_1X + X^2 \cdot h \in \mathbb{Z}/4\mathbb{Z}[X]$ where $h \in \mathbb{Z}/4\mathbb{Z}[X]$ and $a_0, a_1, a_2 \in \mathbb{Z}/4\mathbb{Z}$. Then

$$2 = fg = 2a_0 + (2a_1 \pm a_0)X + X^2(\pm a_1 + h + \ell)$$

implies that $2a_0 = 2$, which is true for $a_0 = \pm 1$, and $2a_1 \pm a_0 = 0$, hence $2a_1 \pm 1 = 0$ which implies that $1 = -2a_1$, impossible in $\mathbb{Z}/4\mathbb{Z}$. This is a contradiction, so that $(2, X)\mathbb{Z}/4\mathbb{Z}[X]$ is not a principal ideal in $\mathbb{Z}/4\mathbb{Z}[X]$.

5. (a) Give an example of a commutative ring R with nonzero ideals I and J such that $I \cap J = \{0\}$.

(b) Prove: if I and J are nonzero ideals in a domain R, then $I \cap J \neq \{0\}$.

Solution:

(a) As part (b) suggests, we need to look at a ring which is not an integral domain and which is big enough to contain two non-trivial ideals with zero intersection. An easy example is $R = \mathbb{Z}/6\mathbb{Z}$, which contains the ideals $2\mathbb{Z}/6\mathbb{Z}$ and $3\mathbb{Z}/6\mathbb{Z}$.

Another example is $\mathbb{Z} \times \mathbb{Z}$, the operations being defined componentwise: as shown in Exercise 6(b), the subsets $0 \times \mathbb{Z}$ and $\mathbb{Z} \times 0$ are ideals. Clearly, they have trivial intersection.

(b) We prove the statement by contraposition. Suppose I, J are non-trivial ideals in a commutative ring R and that $I \cap J = \{0\}$. Let $i \in I \setminus \{0\}$ and $j \in J \setminus \{0\}$. Since both I and J are ideals, we have $ij \in I \cap J = 0$, so that $ij = 0$ and i, j are non-trivial zero-divisors, so that R is not an integral domain, proving the desired statement.

6. Let R_1, R_2 be two commutative rings.

(a) Prove that the set $R_1 \times R_2$, endowed with componentwise sum and multiplication, is a commutative ring.

(b) Prove that $R_1 \times \{0\}$ is an ideal in $R_1 \times R_2$ and that there is an isomorphism

$$(R_1 \times R_2)/(R_1 \times \{0\}) \xrightarrow{\sim} R_2.$$

(c) Find all ring homomorphisms $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$.

Solution:

(a) Both sum and multiplication on $R_1 \times R_2$ are associative and commutative, since they are defined component-wise and both properties hold in R_1 and R_2.

The element $(0_{R_1}, 0_{R_2})$ (resp., $(1_{R_1}, 1_{R_2})$) is a neutral element for the sum (resp., the multiplication), again because the operations are defined component-wise. Each element $(r_1, r_2) \in R_1 \times R_2$ is seen to have inverse element with respect to the sum $(-r_1, -r_2) \in R$.

As an example for all the above arguments, we conclude with an explicit check of distributivity. Let $r_1, s_1, t_1 \in R_1$ and $r_2, s_2, t_2 \in R_2$. Then

$$\begin{aligned}(r_1, r_2) \cdot (\,(s_1, s_2) + (t_1, t_2)\,) &= (r_1, r_2) \cdot (\,(s_1 + t_1, s_2 + t_2)\,)\\ &= (r_1(s_1 + t_1), r_2(s_2 + t_2)) = (r_1 s_1 + r_1 t_1, r_2 s_2 + r_2 t_2)\\ &= (r_1 s_1, r_2 s_2) + (r_1 t_1, r_2 t_2) = (r_1, r_2) \cdot (s_1, s_2) + (r_1, r_2) \cdot (t_1, t_2).\end{aligned}$$

Hence $R_1 \times R_2$, endowed with component-wise sum and multiplication, is a commutative ring.

(b) Consider the projection map $\pi : R_1 \times R_2 \longrightarrow R_2$ sending $(r_1, r_2) \mapsto r_2$. Since the operations on $R_1 \times R_2$ are defined component-wise, π respects sum and multiplication. Moreover, $\pi(1_{R_1 \times R_2}) = \pi((1,1)) = 1$. This implies that π is a ring homomorphism. Notice that

$$\ker(\pi) = \{(r_1, r_2) \in R_1 \times R_2 : r_2 = 0\} = R_1 \times \{0\}$$

is an ideal. As π is surjective (for each $s \in R_2$, $\pi(0, s) = s$), the first isomorphism theorem gives an isomorphism

$$(R_1 \times R_2)/(R_1 \times \{0\}) = (R_1 \times R_2)/\ker(\pi) \xrightarrow{\sim} \operatorname{im}(\pi) = R_2.$$

(c) Let $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ be a ring homomorphism. Let $e = (1, 0) \in \mathbb{Z} \longrightarrow \mathbb{Z}$. Notice that $1 - e = (1,1) - (1,0) = (0,1)$, so that every element $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ can be decomposed as

$$(a, b) = a \cdot e + b \cdot (1 - e) = b \cdot 1_R + (a - b) \cdot e$$

and this means that

$$f((a, b)) = b + (a - b)f(e). \tag{2}$$

Since e is *idempotent*, that is, $e^2 = e$, we obtain an equality $f(e)^2 = f(e^2) = f(e) \in \mathbb{Z}$, which holds only for $f(e) \in \{0, 1\}$. For $f(e) = 0$, (2) reads $f((a, b)) = b$, whereas for $f(e) = 1$ it reads $f((a, b)) = a$. Those are the two projections on the first and second coordinate, that are proven as in (b) to be ring homomorphisms. Hence there are precisely two ring homomorphisms $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, that is, the two projections.

7. (a) Let $(I_j)_{j \in X}$ be a family of ideals in R. Prove: $\bigcap_{j \in X} I_j$ is an ideal in R.

(b) Let $\{x_1, \ldots, x_h\} \subseteq R$. Prove that

$$(x_1, \ldots, x_h)R = \bigcap_{\substack{I \subseteq R \text{ ideal} \\ \text{s.t. } \forall i : x_i \in I}} I.$$

Solution:

(a) Let $u, v \in \bigcap_{j \in X} I_j$, meaning that $u, v \in I_j$ for each $j \in X$. Then, for each $j \in X$, $u - v \in I_j$ since I_j is an ideal, implying that $u - v \in \bigcap_{j \in X} I_j$.
Now let $r \in R$ and $u \in \bigcap_{j \in X} I_j$. Then, for each $j \in X$, $ru \in I_j$ since I_j is an ideal, so that $ru \in \bigcap_{j \in X} I_j$. We can hence conclude that $\bigcap_{j \in X} I_j$ is an ideal.

(b) We prove the two inclusions.
The elements of $(x_1, \ldots, x_h)R$ have the form $\sum_{j=1}^h r_j x_j$ for $r_j \in R$, so that for $r \in R$ we obtain $r \sum_{j=1}^h r_j x_j = \sum_{j=1}^h (r r_j) x_j \in (x_1, \ldots, x_h)R$. Moreover, if $\sum_{j=1}^h r'_j x_j$ is another element of this set, then

$$\sum_{j=1}^h r_j x_j - \sum_{j=1}^h r'_j x_j = \sum_{j=1}^h (r_j - r'_j) x_j \in (x_1, \ldots, x_h)R.$$

Hence $(x_1, \ldots, x_h)R$ is an ideal. Since for each $k = 1, \ldots, h$

$$x_k = \sum_{j=1}^h \delta_{jk} x_j,$$

the ideal $(x_1, \ldots, x_h)R$ contains all the elements x_k, so that it appears itself in the intersection $\bigcap_{\substack{I \subseteq R \text{ ideal} \\ \text{s.t. } \forall i\colon x_i \in I}} I$. This provers the inclusion "$\supseteq$".
Now let $I \subseteq R$ be an ideal containing all the elements x_i. Then, for each $(r_j)_{j \in X} \subseteq R$, we have $r_i x_i \in I$, so that $\sum_{j \in I} r_j x_j \in I$, because I is an ideal. Hence $(x_1, \ldots, x_h)R \subseteq I$. By arbitrarity of I, $(x_1, \ldots, x_h)R$ is contained in $\bigcap_{\substack{I \subseteq R \text{ ideal} \\ \text{s.t. } \forall i\colon x_i \in I}} I$ and we are done.

8. Let $R \neq 0$ be a commutative ring whose only ideals are $\{0\}$ and R. Prove that R is a field.

Solution: Let $x \in R \smallsetminus \{0\}$. Then $0 \neq x \in xR$, so that $xR \neq 0$ and by hypothesis $xR = R$. This implies that $1 \in xR$, i.e., there exists $r \in R$ such that $xr = rx = 1$, so that $x \in R^\times$. Hence $R^\times = R \smallsetminus \{0\}$ and R is a field.

9. (a) Let $\varphi : R \longrightarrow S$ be a ring homomorphism and $I \subset R$ and $J \subset S$ ideals such that $\varphi(I) \subset J$. Prove that there exists a unique morphism $\overline{\varphi} : R/I \longrightarrow S/J$ such that the following diagram

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "p_R"'] & S \arrow[d, "p_S"'] \\ R/I \arrow[r, "\overline{\varphi}"] & S/J, \end{tikzcd}$$

where p_R and p_S are canonical projections, *commutes*, i.e., $\overline{\varphi} \circ p_R = p_S \circ \varphi$.

(b) What can you say about $\overline{\varphi}$ when $I = \varphi^{-1}(J)$?

Solution:

(a) Let $\psi = p_S \circ \varphi$. Then $\psi(I) = p_S(\varphi(I)) \subseteq p_S(J) = \{0_{S/J}\}$, so that $I \subseteq \ker(\psi)$ and by the statement of the First Isomorphism Theorem given in class we obtain that there exists a unique ring homomorphism $\overline{\varphi} : R/I \longrightarrow S/J$ such that $\overline{\varphi} \circ p_R = \psi = p_S \circ \varphi$.

(b) Since $\varphi^{-1}(J) = \varphi^{-1}(p_S^{-1}(\{0_{S/J}\})) = \psi^{-1}(\{0_{S/J}\}) = \ker(\psi)$, if $I = \varphi^{-1}(J)$, then the first isomorphism theorem tells us that $\overline{\varphi}$ is injective.