MATH 100B: Homework #2

Due on January 25, 2024 at 12:00pm

Professor McKernan

Section A02 6:00PM - 6:50PM
Section Leader: Castellano-Macías

Source Consulted: Textbook, Lecture, Discussion, Office Hour

Ray Tsai
A16848188

Problem 1

If $\varphi : R \to R'$ is a homomorphism of R *onto* R' and R has a unit element, 1, show that $\varphi(1)$ is the unit element of R'.

Proof. Let $r' \in R'$. Since φ is onto, there exists $r \in R$, such that $\varphi(r) = r'$. However,

$$r'\varphi(1) = \varphi(r)\varphi(1) = \varphi(r) = \varphi(1)\varphi(r) = \varphi(1)r',$$

so $\varphi(1)$ is the unit element of R'. $\square$

Problem 2

If I, J are ideals of R, define $I + J$ by $I + J = \{i + j \mid i \in I, j \in J\}$. Prove that $I + J$ is an ideal of R.

Proof. We first show $I + J$ is a subgroup of R. Let $a, b \in I + J$. We know $a = i + j$, $b = i' + j'$, for some $i, i' \in I$ and $j, j' \in J$. Then, $a + b = i + i' + j + j'$. However, $i + i' \in I$ and $j + j' \in J$, so $a + b \in I + J$. Since $a^{-1} = -(i + j) = (-i) + (-j) \in I + J$, $I + J$ is closed under taking inverse. Hence, $I + J$ is a subgrou of R. Let $r \in R$. Since $ri \in I$ and $rj \in J$, we know $r(i + j) = ri + rj \in I + J$. Similarly, since $ir \in I$ and $jr \in J$, we know $(i + j)r = ir + jr \in I + J$. Therefore, $I + J$ is an ideal of R. $\square$

Problem 3

If I is an ideal of R and A is a subring of R, show that $I \cap A$ is an ideal of A.

Proof. We already know the intersection of two groups is a group, and thus $I \cap A$ is a group under addition. Let $i \in I \cap A$ and $a \in A$. Since I is an ideal, $ia, ai \in I$. However, A is closed under multiplication, so $ia, ai \in A$. Thus, $ai, ia \in I \cap A$, so $I \cap A$ is an ideal of A. $\square$

Problem 4

If I, J are ideals of R, show that $I \cap J$ is an ideal of R.

Proof. We already know the intersection of two groups is a group, and thus $I \cap J$ is a group under addition. Let $k \in I \cap J$ and $r \in R$. Since I, J are both ideal, $kr, rk \in I$ and $kr, rk \in J$. Hence, $kr, rk \in I \cap J$, so $I \cap J$ is an ideal of R. $\square$

Problem 5

Let $\varphi : R \to R'$ be a homomorphism of R onto R' with kernel K. If A' is a subring of R', let $A = \{a \in R \mid \varphi(a) \in A'\}$. Show that:

(a) A is a subring of R, $A \supset K$.

Proof. Let $a, b \in A$. Since A' contains the unit, $1 \in A$. Since $\varphi(a+b) = \varphi(a) + \varphi(b) \in A'$ and $\varphi(-a) = -\varphi(a) \in A'$, A is a subgroup under addition. Since $\varphi(ab) = \varphi(a)\varphi(b) \in A'$, A is closed under multiplication, and thus A is a subring of R. Let $k \in K$ and let $0'$ be the zero in A'. Since $\varphi(k) = 0' \in A'$, we know $k \in A$, and so $A \supset K$. $\square$

(b) $A/K \simeq A'$.

Proof. Define $\phi : A \to A'$ as $\phi(a) \mapsto \varphi(a)$. ϕ is well-defined as φ is well-defined. Since φ is surjective, there exists $m \in R$ such that $\varphi(m) = a'$, for all $a' \in A'$. However, $\varphi(m) = a'$ implies that $m \in A$, so ϕ is surjective. Since $A \supset K$, ϕ shares the same kernel K with φ. The result now follows by the Isomorphism Theorem of rings. $\square$

(c) If A' is a left ideal of R', then A is a left ideal of R.

Proof. Let $r \in R$, and $a \in A$. We know $\varphi(a) = a'$, for some $a' \in A'$. Since A' is a left ideal of R', we get $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)a' \in A'$, which makes $ra \in A$. Hence, A is a left ideal of R. $\square$

Problem 6

In Example 4, show that $R/I \simeq \mathbb{Z}_p$.

Proof. Let $a = \frac{m}{n} \in R$, where $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$. Since n is not divisible by p, there exists $[n]^{-1} \in \mathbb{Z}_p$. Thus, we may define $\phi : R \to \mathbb{Z}_p$ as $\phi(a) = [m][n]^{-1}$. Let $b = \frac{p}{q} \in R$, where $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$. Suppose that $a = b$. Then, a, b must have the same reduced form, so $m = p$ and $n = q$. Then, $\phi(a) = [m][n]^{-1} = [p][q]^{-1} = \phi(b)$, so ϕ is well-defined. Since

$$
\begin{aligned}
\phi(a+b) &= \phi\left(\frac{mq+np}{nq}\right) \\
&= [mq+np][nq]^{-1} \\
&= [mq][nq]^{-1} + [np][nq]^{-1} \\
&= [m][q][q]^{-1}[n]^{-1} + [n][p][q]^{-1}[n]^{-1} \\
&= [m][n]^{-1} + [p][q]^{-1} \\
&= \phi(a) + \phi(b),
\end{aligned}
$$

$$
\begin{aligned}
\phi(ab) &= \phi\left(\frac{mp}{nq}\right) \\
&= [mp][nq]^{-1} \\
&= [m][q][q]^{-1}[n]^{-1} \\
&= ([m][n]^{-1})([p][q]^{-1}) \\
&= \phi(a)\phi(b),
\end{aligned}
$$

and $\phi(1) = [1][1]^{-1} = 1$, ϕ is a homomorphism. For $[\alpha] \in \mathbb{Z}_p$, there exists $\alpha \in R$ such that $\phi(\alpha) = [\alpha]$, so ϕ is surjective. Suppose that $a \in \text{Ker } \phi$. $\phi(k) = 0$ if and only if $[m][n]^{-1} = 0$. Since n is not divisible by p, $[m][n]^{-1} = 0$ if and only if $[m] = 0$ if and only if m is divisible by p if and only if $a \in I$. Therefore, Ker $\phi = I$. The result now follows by the Isomorphism Theorem of rings. □

Problem 7

In Example 8, verify that the mapping ψ given is an isomorphism of R onto $\mathbb{C}$.

Proof. Define $\phi : \mathbb{C} \to R$ as $\phi(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. ψ and ϕ are both obviously well-defined. Let $m+ni \in \mathbb{C}$. Since $\psi(\phi(m+ni)) = \psi\left(\begin{bmatrix} m & n \\ -n & m \end{bmatrix}\right) = m+ni$ and $\phi(\psi\left(\begin{bmatrix} m & n \\ -n & m \end{bmatrix}\right)) = \phi(m+ni) = \begin{bmatrix} m & n \\ -n & m \end{bmatrix}$, ϕ is the inverse of ψ, and thus ψ is bijective. Let $\begin{bmatrix} p & q \\ -q & p \end{bmatrix} \in R$. Since

$$\begin{aligned}
\psi\left(\begin{bmatrix} m & n \\ -n & m \end{bmatrix} + \begin{bmatrix} p & q \\ -q & p \end{bmatrix}\right) &= \psi\left(\begin{bmatrix} m+p & n+q \\ -(n+q) & m+p \end{bmatrix}\right) \\
&= (m+p) + (n+q)i \\
&= m + ni + p + qi \\
&= \psi\left(\begin{bmatrix} m & n \\ -n & m \end{bmatrix}\right) + \psi\left(\begin{bmatrix} p & q \\ -q & p \end{bmatrix}\right),
\end{aligned}$$

and

$$\begin{aligned}
\psi\left(\begin{bmatrix} m & n \\ -n & m \end{bmatrix} \begin{bmatrix} p & q \\ -q & p \end{bmatrix}\right) &= \psi\left(\begin{bmatrix} mp-nq & mq+np \\ -(mq+np) & mp-nq \end{bmatrix}\right) \\
&= (mp-nq) + (mq+np)i \\
&= (m+ni)(p+qi) \\
&= \psi\left(\begin{bmatrix} m & n \\ -n & m \end{bmatrix}\right) \psi\left(\begin{bmatrix} p & q \\ -q & p \end{bmatrix}\right),
\end{aligned}$$

ψ is an isomorphism, and thus $R \simeq \mathbb{C}$. $\square$

Problem 8

If I, J are ideals of R, let IJ be the set of all sums of elements of the form ij, where $i \in I, j \in J$. Prove that IJ is an ideal of R.

Proof. Let $m, n \in IJ$. m, n are of the form $i_{m_1}j_{m_1} + i_{m_2}j_{m_2} + \dots$ and $i_{n_1}j_{n_1} + i_{n_2}j_{n_2} + \dots$, respectively. Since $m + n$ and m^{-1} are both sums of elements of the form ij, IJ is closed under addition and taking additive inverses, and thus IJ is a subgroup under addition. Let $r \in R$. Since I, J are ideals, for $i \in I$ and $j \in J$, we know $rij = (ri)j = i'j$, for some $i' \in I$. Similarly, $ijr = i(jr) = ij'$, for some $j' \in J$. Therefore,

$$rm = r(i_{m_1}j_{m_1} + i_{m_2}j_{m_2} + \dots) = ri_{m_1}j_{m_1} + ri_{m_2}j_{m_2} + \dots = i'_{m_1}j_{m_1} + i'_{m_2}j_{m_2} + \dots \in IJ$$

and

$$mr = (i_{m_1}j_{m_1} + i_{m_2}j_{m_2} + \dots)r = i_{m_1}j_{m_1}r + i_{m_2}j_{m_2}r + \dots = i_{m_1}j'_{m_1} + i_{m_2}j'_{m_2} + \dots \in IJ$$

for some $i'_{m_k} \in I, j'_{m_k} \in J$, so IJ is an ideal in of R. $\square$

Problem 9

Prove Theorem 4.3.5 (Second Homomorphism Theorem):

Let A be a subring of a ring R and I an ideal of R. Then $A + I = \{a + i \mid a \in A, i \in I\}$ is a subring of R, I is an ideal of $A + I$, and $(A + I)/I \simeq A/(A \cap I)$.

Proof. We show that $A+I$ is closed under addition, taking additive inverse, multiplication, and contains the unit 1. Let $a+i, a'+i' \in A+I$, where $a, a' \in A$ and $i, i' \in I$. Then, $a+i+a'+i' = (a+a')+(i+i') \in A+I$ and $-(a+i) = (-a)+(-i) \in A+I$, so $A+I$ is a group under addition. For multiplication, $(a+i)(a'+i') = aa' + ai' + ia' + ii'$. Since I is an ideal, $ai' + ia' + ii' \in I$, and thus $A + I$ is closed under multiplication. Since A is a subring, we know $1 \in A$. However, I is an ideal, so $0 \in I$. This gives us $1 + 0 = 1 \in A + I$. Thus, $A + I$ is a subring of R.

Let $m \in I$ and let $a+i \in A+I$. We already know I is a subgroup under addition. Since $m(a+i) = ma+mi \in I$ and $(a + i)m = am + im \in I$, I is an ideal of $A + I$.

Let $A \to A + I$ be the natural inclusion. Since I is an ideal of $A + I$, we may compose the inclusion with the natural projection map to get a homomorphism

$$A \to (A + I)/I.$$

The map sends a to $a + I$.

Suppose that $x \in (A + I)/I$. Then, $x = (a + i) + I = a + I$, for some $a \in A$. Thus the homorphism above is clearly surjective. Suppose that $a \in A$ belongs to the kernel. Then, $a + I = I$, so $a \in I$. Hence, $a \in A \cap I$, and the result follows by the First Isomorphism Theorem of ring applied to the map above. $\square$

Problem 10

Show that $R \oplus S$ is a ring and that the subrings $\{(r,0) \mid r \in R\}$ and $\{(0,s) \mid s \in S\}$ are ideals of $R \oplus S$ isomorphic to R and S, respectively.

Proof. Let $(r,s),(r',s'),(r'',s'') \in R \oplus S$. Since $(r,s)+(r',s') = (r+r', s+s') \in R \oplus S$ and $(r,s)(r',s') = (rr', ss') \in R \oplus S$, $R \oplus S$ is closed under addition and multiplication. Since

$$\begin{aligned}((r,s)+(r',s'))+(r'',s'') &= (r+r',s+s')+(r'',s'')\\ &= (r+r'+r'',s+s'+s'')\\ &= (r,s)+(r'+r'',s'+s'')\\ &= (r,s)+((r',s')+(r'',s''))\end{aligned}$$

and

$$\begin{aligned}((r,s)(r',s'))(r'',s'') &= (rr',ss')(r'',s'')\\ &= (rr'r'',ss's'')\\ &= (r,s)(r'r'',s's'')\\ &= (r,s)((r',s')(r'',s'')),\end{aligned}$$

$R \oplus S$ is associative under both addition and multiplication. Since $(0,0) \in R \oplus S$ such that $(0,0)+(r,s) = (r,s)+(0,0) = (r,s)$, $R \oplus S$ contains the zero. Similarly, there exists unit $(1,1) \in R \oplus S$ such that $(1,1)(r,s) = (r,s)(1,1) = (r,s)$. Since $-(r,s) = (-r,-s) \in R \oplus S$, $R \oplus S$ is closed under taking inverse, and thus $R \oplus S$ is a ring.

Let $r,r' \in R$, $s,s' \in S$. Since $(1,0) \in \{(r,0) \mid r \in R\}$ and $(0,1) \in \{(0,s) \mid s \in S\}$ such that $(1,0)(r,0) = (r,0)(1,0) = (r,0)$ and $(0,1)(0,s) = (0,s)(0,1) = (0,s)$, both sets contain a unit. Since $(r,0)+(r',0) = (r+r',0) \in \{(r,0) \mid r \in R\}$, $(0,s)+(0,s') = (0,s+s') \in \{(0,s) \mid s \in S\}$, $-(r,0) = (-r,0) \in \{(r,0) \mid r \in R\}$, and $-(0,s) = (0,-s) \in \{(0,s) \mid s \in S\}$, we know $\{(r,0) \mid r \in R\}$ and $\{(0,s) \mid s \in S\}$ are subgroups under addition. Since $(r,0)(r',0) = (rr',0) \in \{(r,0) \mid r \in R\}$ and $(0,s)(0,s') = (0,ss') \in \{(0,s) \mid s \in S\}$, $\{(r,0) \mid r \in R\}, \{(0,s) \mid s \in S\}$ are closed under multiplication, adn thus they are both subrings. Lastly, since

$$(r,s)((r',s')+(r'',s'')) = (r,s)(r'+r'',s'+s'') = (rr'+rr'',ss'+ss'') = (r,s)(r',s')+(r,s)(r'',s''),$$

$$((r',s')+(r'',s''))(r,s) = (r'+r'',s'+s'')(r,s) = (r'r+r''r,s's+s''s) = (r',s')(r,s)+(r'',s'')(r,s),$$

$R \oplus S$ is distributive.

We know $\{(r,0) \mid r \in R\}$ and $\{(0,s) \mid s \in S\}$ are both subgroups under addition. Let $(m,n) \in R \oplus S$. Since $(r,0)(m,n) = (rm,0) \in \{(r,0) \mid r \in R\}, (m,n)(r,0) = (mr,0) \in \{(r,0) \mid r \in R\}$, $\{(r,0) \mid r \in R\}$ is an ideal of $R \oplus S$. Similarly, Since $(0,s)(m,n) = (0,sn) \in \{(0,s) \mid s \in S\}, (m,n)(0,s) = (0,ns) \in \{(0,s) \mid s \in S\}$, $\{(0,s) \mid s \in S\}$ is an ideal of $R \oplus S$.

Define $\phi : R \to \{(r,0) \mid r \in R\}$ as $\phi(r) = (r,0)$, and define $\psi : \{(r,0) \mid r \in R\} \to R$ as $\psi((r,0)) = r$. Both functions are obviously well-defined. Since $\phi(\psi(r,0)) = \phi(r) = (r,0)$ and $\psi(\phi(r)) = \psi(r,0) = r$, ϕ is a bijection. We may define a bijective mapping $\tau : S \to \{(0,s) \mid s \in S\}$ in a similar manner. Since

$$\phi(r)+\phi(r') = (r,0)+(r',0) = (r+r',0) = \phi(r+r'),$$

$$\phi(r)\phi(r') = (r,0)(r',0) = (rr',0) = \phi(rr'),$$

$$\tau(s)+\tau(s') = (0,s)+(0,s') = (0,s+s') = \tau(s+s'),$$

$$\tau(s)\tau(s') = (0,s)(0,s') = (0,ss') = \tau(ss'),$$

ϕ and τ are both isomorphisms, and thus $R \simeq \{(r,0) \mid r \in R\}$ and $S \simeq \{(0,s) \mid s \in S\}$. ☐

Problem 11

If $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \text{ real} \right\}$ and $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| b \text{ real} \right\}$, show that:

(a) R is a ring.

Proof. We already know matricies are associative under addition and multiplication, commutes under addition, and distributive. Since R contains the zero matrix and the identity matrix, R contains zero and unit. Let $k = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $m = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$. Since $k + m = \begin{pmatrix} a+x & b+y \\ 0 & c+z \end{pmatrix}$ and $km = \begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix}$, R is closed under addition and multiplication. Since $-k = \begin{pmatrix} -a & -b \\ 0 & -c \end{pmatrix} \in R$, R is closed under taking additive inverse. Therefore, R is a ring. □

(b) I is an ideal of R.

Proof. $k = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$, $m = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}$. Since $k + m = \begin{pmatrix} 0 & a+x \\ 0 & 0 \end{pmatrix} \in I$ and $-k = \begin{pmatrix} 0 & -a \\ 0 & 0 \end{pmatrix} \in I$, I is an additive subgroup of R. Let $r = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \in R$. Since $kr = \begin{pmatrix} 0 & ar \\ 0 & 0 \end{pmatrix}$ and $rk = \begin{pmatrix} 0 & pa \\ 0 & 0 \end{pmatrix}$, I is an ideals of R. □

(c) $R/I \simeq F \oplus F$, where F is the field of real numbers.

Proof. Consider the map $\phi : R \to F \oplus F$ that sends $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ to (a, c). Suppose that $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$. Then $a = a'$ and $c = c'$, and so $\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = (a, c) = (a', c') = \phi\left(\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right)$, so ϕ is well-defined. ϕ is also surjective, as for all $(a, c) \in F \oplus F$, there exists $k = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R$ such that $\phi(k) = (a, c)$. Let $m = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in R$. Since

$$\phi(k) + \phi(m) = (a, c) + (a', c') = (a + a', c + c') = \phi(k + m),$$

and

$$\phi(k)\phi(m) = (a, c)(a', c') = (aa', cc') = \phi(km),$$

ϕ is a homomorphism. The result now follows by the Isomorphism Theorem of rings. □

Problem 12

If I, J are ideals of R, let $R_1 = R/I$ and $R_2 = R/J$. Show that $\varphi : R \to R_1 \oplus R_2$ defined by $\varphi(r) = (r+I, r+J)$ is a homomorphism of R into $R_1 \oplus R_2$ such that Ker $\varphi = I \cap J$.

Proof. Let $m, n \in R$. Note that since I is an ideal of R, for $i \in I$, $(m+i)(n+i) = mn+in+mi+i^2 = mn+i' \in mn+I$, for some $i' = in+mi+i^2 \in I$. By symmetry, we also know $(m+j)(n+j) = mn+j' \in mn+J$, for some $j, j' \in J$. Thus, $(m+I)(n+I) = mn+I$ and $(m+J)(n+J) = mn+J$. Since

$$\begin{aligned}\varphi(m)+\varphi(n) &= (m+I, m+J)+(n+I, n+J)\\ &= ((m+n)+I, (m+n)+J)\\ &= \varphi(m+n)\end{aligned}$$

and

$$\begin{aligned}\varphi(m)\varphi(n) &= (m+I, m+J)(n+I, n+J)\\ &= ((mn)+I, (mn)+J)\\ &= \varphi(mn),\end{aligned}$$

φ is a homomorphism. Let $k \in$ Ker φ. Then, $\varphi(k) = (k+I, k+J) = (I, J)$, so $k \in I$ and $k \in J$, which makes Ker $\varphi = I \cap J$. $\square$

Problem 13

Let $\mathbb{Z}$ be the ring of integers and m, n two relatively prime integers, I_m the multiples of m in $\mathbb{Z}$, and I_n the multiples of n in $\mathbb{Z}$.

(a) What is $I_m \cap I_n$?

Proof. Since m, n are relatively prime, $I_m \cap I_n$ is the multiples of mn, namely I_{mn}. □

(b) Use the result of Problem 12 to show that there is a one-to-one homomorphism from $\mathbb{Z}/I_{mn}$ to $\mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$.

Proof. We first show that I_m and I_n are ideals of $\mathbb{Z}$. We already know I_m and I_n are additive subgroups of $\mathbb{Z}$. Let $x \in \mathbb{Z}$, $p \in I_m$, and $q \in I_n$. Since $xp = px$ is a multiple of m and $xq = qx$ is a multiple of n, I_m and I_n are indeed ideals of $\mathbb{Z}$. It follows by the results of Problem 12 that there exists a homomorphism $\mathbb{Z} \to \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$ that maps x to $(x + I_m, x + I_n)$ and has $I_m \cap I_n = I_{mn}$ as its kernel. By the Isomorphism Theorem of rings, there exists a injective homomorphism $\phi : \mathbb{Z}/I_{mn} \to \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$ that maps $x + I_{mn}$ to $(x + I_m, x + I_n)$. □

Problem 14

If m, n are relatively prime, prove that $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Proof. Since $\mathbb{Z}_{mn} = \mathbb{Z}/I_{mn}$, $\mathbb{Z}_m = \mathbb{Z}/I_m$, and $\mathbb{Z}_n = \mathbb{Z}/I_n$, we may continue using our homomorphism ϕ defined in the previous problem. Note that $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m||\mathbb{Z}_n| = |\mathbb{Z}_m \oplus \mathbb{Z}_n|$. Since ϕ is injective and $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \oplus \mathbb{Z}_n|$ are finite, ϕ is an isomorphism, and thus $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$. $\square$

Problem 15

Use the result of Problem 14 to prove the *Chinese Remainder Theorem*, which asserts that if m and n are relatively prime integers and a, b any integers, we can find an integer x such that $x \equiv a \mod m$ and $x \equiv b \mod n$ simultaneously.

Proof. Define ϕ as we did in Problem 13. Since $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ is an isomorphism, we may find $[x]_{mn} \in \mathbb{Z}_{mn}$ such that $\phi([x]_{mn}) = ([a]_m, [b]_n)$, for any $a, b \in \mathbb{Z}$, and the result now follows. $\square$