**Math 412. Ring Homomorphisms**  
Professor Karen E. Smith

**Definition:** A ring homomorphism is a mapping \( R \to S \) between two rings (with identity) which satisfies:

1. \( \phi(x + y) = \phi(x) + \phi(y) \) for all \( x, y \in R \).
2. \( \phi(x \cdot y) = \phi(x) \cdot \phi(y) \) for all \( x, y \in R \).
3. \( \phi(1_R) = 1_S \).

**Definition:** A ring isomorphism is a bijective ring homomorphism. We say that two rings \( R \) and \( S \) are isomorphic if there is an isomorphism \( R \to S \) between them.

You should think of an isomorphism as a renaming: isomorphic rings are “the same ring” with the elements named differently.

**Definition:** The kernel of a ring homomorphism \( R \to S \) is the set of elements in the source that map to the ZERO of the target; that is,

\[ \ker \phi = \{ r \in R \mid \phi(r) = 0_S \}. \]

**Theorem:** A ring homomorphism \( R \to S \) is injective if and only if its kernel is zero.

---

**A. Examples of Homomorphisms:** Which of the following mappings between rings is a homomorphism? Which are isomorphisms?

1. The inclusion mapping \( \mathbb{Z} \to \mathbb{Q} \) sending each integer \( n \) to the rational number \( \frac{n}{1} \).
2. The doubling map \( \mathbb{Z} \to \mathbb{Z} \) sending \( n \mapsto 2n \).
3. The residue map \( \mathbb{Z} \to \mathbb{Z}_n \) sending each integer \( a \) to its congruence class \( [a]_n \).
4. The “evaluation at 0” map \( \mathbb{R}[x] \to \mathbb{R} \) sending \( f(x) \mapsto f(0) \).
5. The differentiation map \( \mathbb{R}[x] \to \mathbb{R}[x] \) sending \( f \mapsto \frac{df}{dx} \).
6. The map \( \mathbb{R} \to M_2(\mathbb{R}) \) sending \( \lambda \mapsto \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \).
7. The map \( \mathbb{R} \to M_2(\mathbb{R}) \) sending \( \lambda \mapsto \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \).
8. The map \( M_2(\mathbb{Z}) \to \mathbb{R} \) sending each \( 2 \times 2 \) matrix to its determinant.

For homomorphism: Yes, No (1 not preserved), yes, yes, no (does not preserve \( \times \)), yes, no (does not preserve 1), no (does not preserve +) NONE of these are isomorphisms.

**B. Basic Proofs:** Let \( \phi : S \to T \) be a homomorphism of rings.

1. Show that \( \phi(0_S) = 0_T \).
2. Show that for all \( x \in S \), \( -\phi(x) = \phi(-x) \). That is: a ring homomorphism “respects additive inverses”.
3. Show that if \( u \in S \) is a unit, then also \( \phi(u) \in T \) is a unit.

- \( \phi(0_S) = \phi(0_S + 0_S) = \phi(0_S) + \phi(0_S) \). Now, add \( -\phi(0_S) \) to both sides: get \( 0_T = \phi(0_S) \).
- \( 0_T = \phi(0_S) = \phi(x - x) = \phi(x) + \phi(-x) \). So the additive inverse of \( \phi(x) \) is \( \phi(-x) \). That is, \(-\phi(x) \) is \( \phi(-x) \).
C. KERNEL OF RING HOMOMORPHISMS: Let \( \phi : R \to S \) be a ring homomorphism

1. Prove that \( \ker \phi \) is non-empty.
2. Compute the kernel of the canonical homomorphism: \( \mathbb{Z} \to \mathbb{Z}_n \) sending \( a \mapsto [a]_n \).
3. Compute the kernel of the homomorphism \( \mathbb{Z} \to \mathbb{Z}_7 \times \mathbb{Z}_{11} \) sending \( n \mapsto ([n]_7, [n]_{11}) \).
4. For arbitrary rings \( R, S \), compute the kernel of the projection homomorphism \( R \times S \to R \) sending \( (r, s) \mapsto r \).

Write your answer in set-builder notation.

D. Prove the THEOREM: A ring homomorphism \( \phi : R \to S \) is injective if and only if its kernel is ZERO.

Assume \( \phi \) is injective. Take arbitrary \( x \in \ker \phi \). Then \( \phi(x) = 0 \). But also \( \phi(0) = 0 \). By injectivity, \( x = 0 \). So \( \ker \phi \subseteq \{0\} \).

Conversely, assume \( \ker \phi = 0 \). Take arbitrary \( x, y \in R \) such that \( \phi(x) = \phi(y) \). Then \( \phi(x) - \phi(y) = \phi(x) + \phi(-y) = \phi(x - y) = 0 \). So \( x - y \in \ker \phi \), which means \( x - y = 0 \). So \( x = y \) and \( \phi \) is injective.

E. ISOMORPHISM. Suppose that \( R \xrightarrow{\phi} S \) is a ring isomorphism. True or False.

1. \( \phi \) induces a bijection between units.
2. \( \phi \) induces a bijection between zero-divisors.
3. \( R \) is a field if and only if \( S \) is a field.
4. \( R \) is an (integral) domain if and only if \( S \) is an (integral) domain.

All true. Isomorphism just changes the name, but since it preserves 0 and 1, it preserves zero divisors and units. The last two statement then follow directly from the definitions (of domain, field, respectively) and (1) and (2) (respectively).

F. ISOMORPHISM. Consider the set \( S = \{a, b, c, d\} \) and the associative binary operations \( \heartsuit \) and \( \spadesuit \) listed below. You showed last time that \( (S, \spadesuit, \heartsuit) \) is a ring.

<table>
<thead>
<tr>
<th>( \heartsuit )</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>c</td>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td>d</td>
<td>a</td>
<td>d</td>
<td>c</td>
<td>b</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( \spadesuit )</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>a</td>
<td>d</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>a</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td>b</td>
<td>a</td>
</tr>
</tbody>
</table>

1. Discuss and recall some of the features of the ring \( (S, \spadesuit, \heartsuit) \). To what more familiar ring is it isomorphic?
2. The operations \( \oplus \) and \( \otimes \) (whose tables are listed below) define a different ring structure on \( S \). What are the zero and one? Is the ring \( (S, \oplus, \otimes) \) isomorphic to \( (S, \spadesuit, \heartsuit) \)? Explain
3. Find an explicit isomorphism \( \mathbb{Z}_2 \times \mathbb{Z}_2 \to (S, \oplus, \otimes) \).
4. Find a different isomorphism \( \mathbb{Z}_2 \times \mathbb{Z}_2 \to (S, \oplus, \otimes) \)?
5. Can there be more than one isomorphism \( \mathbb{Z}_4 \to (S, \spadesuit, \heartsuit) \)?

1. \( \mathbb{Z}_4 \)
2. zero is \( a \) and one is \( b \).
3. \( (0, 0) \to a, \ (0, 1) \to d, \ (1, 0) \to c, \ (1, 1) \to b \).
4. \( (0, 0) \to a, \ (1, 0) \to d, \ (0, 1) \to c, \ (1, 1) \to b \).
G. Practice with well-definedness:

1. Show that $\mathbb{Z}_4 \to \mathbb{Z}_2$ defined by $[a]_4 \mapsto [a]_2$ is a well-defined ring homomorphism. What does well-defined mean here? Remember the element of $\mathbb{Z}_4$ are sets.

2. Explain why the map $\mathbb{Z}_5 \to \mathbb{Z}_2$ defined by $[a]_5 \mapsto [a]_2$ is not well defined.

3. Show that for any $m, n \in \mathbb{Z}$, the map $\mathbb{Z}_n \to \mathbb{Z}_m$ is well-defined if and only if $m|n$.

4. We can define $\phi : \mathbb{Z}_5 \to \mathbb{Z}_2$ by $[r]_5 \mapsto [r]_2$ for $0 \leq r < 5$. Explain why this is well-defined. Explain why it is not a ring homomorphism, nor very "natural".

H. Cautionary Examples: Let $R$ and $S$ be arbitrary rings.

1. Is the map $R \to R \times S$ sending $a \mapsto (a, 0)$ a ring homomorphism? Explain.

2. Is the map $R \to R \times S$ sending $a \mapsto (a, 1)$ a ring homomorphism? Explain.

Neither is. In the first, $1_R \mapsto (1, 0)$ which is not the multiplicative identity of $R \times S$. In the second, $0$ goes to $(0, 1)$ which is not the additive identity.

I. Canonical Ring Homomorphisms: Let $R$ be any ring\(^1\). Prove that there exists a unique ring homomorphism $\mathbb{Z} \to R$.

**Bonus:** Find a necessary and sufficient condition on integers $n, m$ so that $\mathbb{Z}_{mn} \cong \mathbb{Z}_n \times \mathbb{Z}_m$:

---

\(^1\)with identity of course