Math 412. Ring Homomorphisms

DEFINITION: A **ring homomorphism** is a mapping $R \xrightarrow{\phi} S$ between two rings (with identity) that 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) $\phi(1_R) = 1_S$.

Once again, requirement (3) is not present in the book, but we always require this.

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 $R \xrightarrow{\phi} S$ 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 $\{0_R\}$.

A. EXAMPLES OF HOMOMORPHISMS: Which of the following mappings between rings is a **homomorphism**? Which are **isomorphisms**?

(1) The inclusion mapping $\mathbb{Z} \hookrightarrow \mathbb{Q}$ 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 $M_2(\mathbb{Z}) \to \mathbb{R}$ sending each 2×2 matrix to its determinant.

Solution.

(1) homomorphism, but not isomorphism.
(2) not homomorphism, 1 is not mapped to 1.
(3) homomorphism, but not isomorphisms.
(4) homomorphism, but not isomorphisms.
(5) not homomorphism, 1 is not mapped to 0.
(6) homomorphism but not isomorphism.
(7) is NOT a homomorphism because the addition is not preserved: $\det(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}) \neq \det \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \det \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

B. INTRODUCTORY 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.

Solution.

(1) Note that $0_S + 0_S = 0_S$. Apply ϕ: $\phi(0_S + 0_S) = \phi(0_S)$ and use the fact that ϕ respects addition to write $\phi(0_S) + \phi(0_S) = \phi(0_S)$. This is a statement in T. Now, add $-\phi(0_S)$ to both sides as in Warm-up Problem A(1) to conclude: $\phi(0_S) = 0_T$.
(2) Given $x \in S$, we know that $x + -x = 0_S$. Apply ϕ to get a statement in T: $\phi(x + -x) = \phi(0_S) = 0_T$. Because ϕ preserves addition: $\phi(x) + \phi(-x) = 0_T$. This (together with the fact that $+$ is commutative in any ring) exactly says that $\phi(-x)$ is the additive inverse of $\phi(x)$. So $-\phi(x) = \phi(-x)$.
(3) Since u is unit, there exists an element u^{-1} in S such that $uu^{-1} = u^{-1}u = 1$. Then $\phi(uu^{-1}) = \phi(u)\phi(u^{-1}) = \phi(1) = 1$ and $\phi(u^{-1}u) = \phi(u^{-1})\phi(u) = \phi(1) = 1$. Hence $\phi(u)^{-1} = \phi(u^{-1})$.

C. KERNEL OF RING HOMOMORPHISMS: Let $\phi : R \to S$ be a ring homomorphism

(1) Prove that $\ker \phi$ is nonempty.
(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.

Solution.

(1) This follows since $\phi(0) = 0$, so 0 is in the kernel.
(2) The kernel here is $\{nb \,|\, b \in \mathbb{Z}\}$.
(3) $\{77b \,|\, b \in \mathbb{Z}\}$. Note that 77 is the least common multiple of 7 and 11.
(4) $\{(0, s) \,|\, s \in S\}$

D. Prove the THEOREM: *A ring homomorphism $\phi : R \to S$ is injective if and only if* $\ker \phi = \{0_R\}$.

Solution.

Suppose ϕ is injective. Take any $x \in \ker \phi$. Then $\phi(x) = \phi(0) = 0$. By injectivity, we have $x = 0$. So the kernel is $\{0_R\}$. Conversely, assume that $\ker \phi = \{0_R\}$. Suppose that $\phi(x) = \phi(y)$ for $x, y \in R$. Then $\phi(x) + -\phi(y) = 0_S$. Using C(2), we have $\phi(x) + \phi(-y) = 0_S$, and since ϕ respects addition, $\phi(x + (-y)) = 0_S$. So $x + -y$ is in the kernel. By assumption, $x + -y = 0$, so $x = y$.

In this course, you may use the following result. You can also try proving it after class, for extra practice.

THEOREM: Let $\phi : R \to S$ be a ring isomorphism. Then, $\phi^{-1} : S \to R$ is also a ring isomorphism.

Note that, since ϕ is bijective, we know that its inverse function ϕ^{-1} exists and is unique (and bijective!), but it is not obvious that it is a ring homomorphism.

E. ISOMORPHISM. Suppose that $R \xrightarrow{\phi} S$ is a ring isomorphism. True or False. (If True, prove it. If False, come up with an **EXPLICIT** counterexample.)

(1) ϕ induces a bijection between units.
(2) ϕ induces a bijection between zero-divisors.
(3) R is a field* if and only if S is a field. (*What's a field again?)
(4) R is an integral domain if and only if S is an integral domain.

Solution.

(1) True. Let U_S and U_R be set of units in S and R respectively. Then ϕ is a bijective map from U_R to U_S. It is injective because it in injective on R. To see surjectivity, suppose u is a unit in U_s. Since ϕ^{-1} is a ring isomorphism, we have that $\phi^{-1}(u)$ is a unit in R, and $\phi(\phi^{-1}(u)) = u$.
(2) True. If $x \neq 0$ is a zero divisor in R, then there exists a nonzero element $y \in R$ such that $xy = 0$. So, $\phi(x)\phi(y) = 0$. Since ϕ is injective and y is nonzero, $\phi(y)$ is nonzero. Therefore. Hence $\phi(x) \neq 0$ is a zerodivisor in S. ϕ is injective on the set of zerodivisors since it is injective on R. To see that it is surjective, let $m \neq 0$ be a zero divisor in S. Then $mn = 0$ for some $n \in S$. Then $\phi^{-1}(mn) = \phi^{-1}(m)\phi^{-1}(n) = 0$ where $\phi^{-1}(m)$ and $\phi^{-1}(n)$ are nonzero. Hence, $\phi^{-1}(m)$ is a zero divisor in R whose image is m.

(3) and (4) are also true. We think about an isomorphism as relabeling of the elements of the ring. This relabeling changes the look of the ring, but leaves the structure, and how elements interact with each other, intact.

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

$\heartsuit$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	a	c
d	a	d	c	b

$\spadesuit$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$\oplus$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\otimes$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	c	a
d	a	d	a	d

(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 above) 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) Can you find a *different* isomorphism $\mathbb{Z}_2 \times \mathbb{Z}_2 \to (S, \oplus, \otimes)$?
(5) Can there be more than one isomorphism $\mathbb{Z}_4 \to (S, \spadesuit, \heartsuit)$?

Solution.

(1) We can take $\spadesuit$ to be the addition and $\heartsuit$ to be the multiplication. By inspection, we see that both are commutative, and that a is the identity for $\spadesuit$ (hence our "zero") and b is the identity for $\heartsuit$ (hence our "1"). We see that every element has an additive identity (we can scan each row of the addition chart, looking for the zero element...we then can find what element is the additive inverse. So the additive inverse of a is a, the additive inverse of b is d (hence of d is b, and c is its own additive inverse). The distributive property is a beast to check by hand.

$\cdot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The explicit isomorphism is $S \to \mathbb{Z}_4$ sending $a \mapsto [0]$, $b \mapsto [1]$, $c \mapsto [2]$ and $[d] \mapsto [3]$.

(2) Zero is a and one is b. $(S, \oplus, \otimes)$ is not isomorphic to $(S, \spadesuit, \heartsuit)$. There are many ways to see this here is one: If ϕ is an isomorphism from $(S, \spadesuit, \heartsuit)$ to $(S, \oplus, \otimes)$, then one is mapped to one and zero is mapped to zero (we proved the latter.) So $\phi(a) = a$ and $\phi(b) = b$. Now, we should have $\phi(b \spadesuit b) = \phi(b) \oplus \phi(b)$ But $\phi(b \spadesuit b) = \phi(c)$ and $\phi(b) \oplus \phi(b) = b \oplus b = a$. And because ϕ is injective it implies that $c = a$. The contradiction tells us there is **no isomorphism** between the two rings.

(3) $\mathbb{Z}_2 \times \mathbb{Z}_2$ has four elements $(0,0), (1,0), (0,1)$ and $(1,1)$. The zero is $(0,0)$ and the 1 is $(1,1)$.

(4)

$+$	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(0, 0)	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(1, 1)	(1, 1)	(0, 0)	(0, 1)	(1, 0)
(1, 0)	(1, 0)	(0, 1)	(0, 0)	(1, 1)
(0, 1)	(0, 1)	(1, 0)	(1, 1)	(0, 0)

$\cdot$	(0, 0)	(1, 1)	(0, 1)	(1, 0)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1, 1)	(0, 0)	(1, 1)	(0, 1)	(1, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 1)	(0, 0)
(1, 0)	(0, 0)	(1, 0)	(0, 0)	(1, 0)

(4) and (4) The map is $S \to \mathbb{Z}_2 \times \mathbb{Z}_2$ sending $a \mapsto (0,0)$, $b \mapsto (1,1)$, $c \mapsto (0,1)$ and $d \mapsto (1,0)$ is easily checked to be an isomorphism. It is not the only one! The isomorphism must match up the identities, so a must correspond to $(0,0)$ and b must correspond to $(1,1)$. But c and d can go interchangeably to either $(1,0)$ or $(0,1)$.

(5) Any isomorphism sends $[1]$ to b, and preserves addition, hence $[2] = [1] + [1]$ goes to $b \spadesuit b = c$ and $[3] = [1] + [1] + [1]$ goes to $c \spadesuit b = d$ and finally $[0]$ has to go to a. So there is only one isomorphism $\mathbb{Z}_4 \to (S, \spadesuit, \heartsuit)$

G. CAUTIONARY EXAMPLES: Let R and S be arbitrary rings.

(1) Is the map $R \to R \times S$ sending $a \mapsto (a, 1)$ a ring homomorphism? Explain.
(2) Is the map $R \to R \times S$ sending $a \mapsto (a, 0)$ a ring homomorphism? Explain.
(3) Find a natural homomorphism $R \to R \times R$. Can it be an isomorphism?

Solution.

(1) No! The problem is that ring homomorphisms preserve the additive structure, but given $a, b \in R$,

$$a + b \mapsto (a + b, 1) \text{ while also } a + b \mapsto (a, 1) + (b, 1).$$

This would only make sense if $1 + 1 = 1$ in S, but that means $1 = 0$ and S is the ring with one element.

(2) No! A ring homomorphism send 1 to 1, but $1 \mapsto (1, 0)$, while the one in $R \times S$ is $(1, 1)$.
(3) $r \mapsto (r, r)$. This is not an isomorphism, since it cannot be surjective.

H. CANONICAL RING HOMOMORPHISMS: Let R be any ring[1]. Prove that there exists a **unique** ring homomorphism $\mathbb{Z} \to R$.

[1] with identity of course

Solution. Let $f : \mathbb{Z} \to R$ be a ring homomorphism. Then by definition, $f(1) = 1_R$, and by problem B part (1), $f(0) = 0_R$. Now this determines the image of every integer: if $n \geq 1$, then

$$f(n) = \underbrace{f(1) + \cdots + f(1)}_{n \text{ times}} = \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}$$

and $f(-n) = -f(n)$. Hence, we have shown that if there exists a ring homomorphism ϕ from $\mathbb{Z}$ to R, it must be unique, and has to be given by the formula $\phi(n) = n \cdot 1_R$ for each $n \in \mathbb{Z}$, where $n \cdot 1_R$ is defined as

$$n \cdot 1_R = \begin{cases} \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} & \text{if } n \geq 1 \\ 0_R & \text{if } n = 0 \\ \underbrace{-(1_R + \cdots + 1_R)}_{-n \text{ times}} & \text{if } n \leq -1 \end{cases}$$

Note that it was important to define what $n \cdot 1_R$ is, because, although this is useful and intuitive notation, we can't multiply elements of two different rings ($\mathbb{Z}$ and R).

We still have to show that ϕ is a ring homomorphism. $\phi(1) = 1_R$, by definition. Let $m, n \in \mathbb{Z}$. We also have that $\phi(n + m) = (n + m) \cdot 1_R = n \cdot 1_R + m \cdot 1_R = \phi(n) + \phi(m)$, and $\phi(nm) = (nm) \cdot 1_R = (n \cdot 1_R) \times (m \cdot 1_R) = \phi(n) \times \phi(m)$ (where $\times$ is the multiplication on R), so ϕ is indeed a ring homomorphism.