Math 2070 Week 9

Ring Homomorphisms

9.1 Homomorphisms

Definition 9.1. *Let* $(A, +_A, \cdot_A)$, $(B, +_B, \cdot_B)$ *be rings. A* **ring homomorphism** *from* A *to* B *is a map* $\phi : A \to B$ *with the following properties:*

1. $\phi(1_A) = 1_B$.
2. $\phi(a_1 +_A a_2) = \phi(a_1) +_B \phi(a_2)$, *for all* $a_1, a_2 \in A$.
3. $\phi(a_1 \cdot_A a_2) = \phi(a_1) \cdot_B \phi(a_2)$, *for all* $a_1, a_2 \in A$.

Note that if $\phi : A \to B$ is a homomorphism, then:

1. $$1 = \phi(1) = \phi(1 + 0) = \phi(1) + \phi(0) = 1 + \phi(0),$$
   which implies that $\phi(0) = 0$.
2. For all $a \in A$, $0 = \phi(0) = \phi(-a + a) = \phi(-a) + \phi(a)$, which implies that $\phi(-a) = -\phi(a)$.
3. If u is a unit in A, then $1 = \phi(u \cdot u^{-1}) = \phi(u)\phi(u^{-1})$, and $1 = \phi(u^{-1} \cdot u) = \phi(u^{-1})\phi(u)$; which implies that $\phi(u)$ is a unit, with $\phi(u)^{-1} = \phi(u^{-1})$.

Example 9.2. *The map* $\phi : \mathbb{Z} \to \mathbb{Q}$ *defined by:*

$$\phi(n) = \frac{n}{1}, \quad n \in \mathbb{Z},$$

is a homomorphism, since:

1. $\phi(1) = \frac{1}{1} = 1_{\mathbb{Q}}$,

2. $\phi(n +_{\mathbb{Z}} m) = \frac{m+n}{1} = \frac{n}{1} +_{\mathbb{Q}} \frac{m}{1} = \phi(n) +_{\mathbb{Q}} \phi(m)$.

3. $\phi(n \cdot_{\mathbb{Z}} m) = \frac{mn}{1} = \frac{n}{1} \cdot_{\mathbb{Q}} \frac{m}{1} = \phi(n) \cdot_{\mathbb{Q}} \phi(m)$.

Example 9.3. *Fix an integer m which is larger than 1. For $n \in \mathbb{Z}$, let $\overline{n}$ denote the remainder of the division of n by m. That is:*

$$n = mq + \bar{n}, \quad 0 \leq \bar{n} < m$$

Recall that $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ is a ring, with the addition law defined by:

$$s +_m t = \overline{s+t},$$

and the multiplication law defined by:

$$s \times_m t = \overline{s \cdot t},$$

for all $s, t \in \mathbb{Z}_m$. Here, $+$ and $\cdot$ are the usual addition and multiplication for integers.

Define a map $\phi : \mathbb{Z} \to \mathbb{Z}_m$ as follows:

$$\phi(n) = \overline{n}, \quad \forall n \in \mathbb{Z}.$$

Then, ϕ is a homomorphism.

Proof. 1. $\phi(1) = \overline{1} = 1$,

2. $\phi(s+t) = \overline{s+t} = \overline{\overline{s} + \overline{t}} = \overline{s} +_m \overline{t} = \phi(s) +_m \phi(t)$.

3. $\phi(s \cdot t) = \overline{s \cdot t} = \overline{\overline{s} \cdot \overline{t}} = \overline{s} \times_m \overline{t} = \phi(s) \times_m \phi(t)$.

□

Example 9.4. *For any ring R, define a map $\phi : \mathbb{Z} \to R$ as follows:*

$$\phi(0) = 0;$$

For $n \in \mathbb{N}$,

$$\phi(n) = n \cdot 1_R := \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}};$$

$$\phi(-n) = -n \cdot 1_R := n \cdot (-1_R) = \underbrace{(-1_R) + (-1_R) + \cdots + (-1_R)}_{n \text{ times}}.$$

The map ϕ is a homomorphism.

Proof. **Exercise.** □

Example 9.5. *Let R be a commutative ring. For each element $r \in R$, we may define the* **evaluation map** $\phi_r : R[x] \to R$ *as follows:*

$$\phi_r \left(\sum_{k=0}^{n} a_k x^k \right) = \sum_{k=0}^{n} a_k r^k$$

The map ϕ_r is a ring homomorphism.

Proof. Discussed in class. □

Definition 9.6. *If a ring homomorphism $\phi : A \to B$ is a bijective map, we say that ϕ is an* **isomorphism***, and that A and B are* **isomorphic** *as rings.*

Notation If A and B are isomorphic, we write $A \cong B$.

Claim 9.7. *If $\phi : A \to B$ is an isomorphism, then $\phi^{-1} : B \to A$ is an isomorphism.*

Proof. Since ϕ is bijective, ϕ^{-1} is clearly bijective. It remains to show that ϕ^{-1} is a homomorphism:

1. Since $\phi(1_A) = 1_B$, we have $\phi^{-1}(1_B) = \phi^{-1}(\phi(1_A)) = 1_A$.
2. For all $b_1, b_2 \in B$, we have

$$\begin{aligned}\phi^{-1}(b_1 + b_2) &= \phi^{-1}(\phi(\phi^{-1}(b_1)) + \phi(\phi^{-1}(b_2))) \\ &= \phi^{-1}(\phi(\phi^{-1}(b_1) + \phi^{-1}(b_2))) = \phi^{-1}(b_1) + \phi^{-1}(b_2)\end{aligned}$$

3. For all $b_1, b_2 \in B$, we have

$$\begin{aligned}\phi^{-1}(b_1 \cdot b_2) &= \phi^{-1}(\phi(\phi^{-1}(b_1)) \cdot \phi(\phi^{-1}(b_2))) \\ &= \phi^{-1}(\phi(\phi^{-1}(b_1) \cdot \phi^{-1}(b_2))) = \phi^{-1}(b_1) \cdot \phi^{-1}(b_2)\end{aligned}$$

This shows that ϕ^{-1} is a bijective homomorphism. □