Week 9

9.1 Homomorphisms

Definition. Let R and R' be rings. A **ring homomorphism** from R to R' is a map $\phi : R \to R'$ with the following properties:

1. $\phi(1_R) = 1_{R'}$;
2. $\phi(a + b) = \phi(a) + \phi(b)$, for all $a, b \in R$;
3. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, for all $a, b \in R$.

Note that if $\phi : R \to R'$ is a homomorphism, then:

- $$\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0),$$
  which implies that $\phi(0) = 0$.
- For all $a \in R$, $0 = \phi(0) = \phi(-a + a) = \phi(-a) + \phi(a)$, which implies that $\phi(-a) = -\phi(a)$.
- If u is a unit in R, 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 9.1.1. The map $\phi : \mathbb{Z} \to \mathbb{Q}$ defined by $\phi(n) = n$ is a homomorphism, since:

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

Example 9.1.2. 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 $\mathbb{Z}_m = \{0, 1, 2, \ldots, m\}$ is a ring, with $s + t = \overline{s +_{\mathbb{Z}} t}$ and $s \cdot t = \overline{s \cdot_{\mathbb{Z}} t}$, for all $s, t \in \mathbb{Z}_m$.

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. $\phi(s + t) = \overline{s +_{\mathbb{Z}} t} = \overline{\overline{s} +_{\mathbb{Z}} \overline{t}} = \overline{s} + \overline{t} = \phi(s) + \phi(t)$.
3. $\phi(st) = \overline{s \cdot_{\mathbb{Z}} t} = \overline{\overline{s} \cdot_{\mathbb{Z}} \overline{t}} = \overline{s} \cdot \overline{t} = \phi(s)\phi(t)$.

□

Example 9.1.3. 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.** □

Remark. In fact this is the only homomorphism from $\mathbb{Z}$ to R since we need to have $\phi(1) = 1_R$ and this implies that

$$\phi(n) = n \cdot \phi(1) = n \cdot 1_R.$$

Example 9.1.4. Let R be a commutative ring. For each element $r \in R$, we may define a 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. *Shown in class.* □

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

Notation. If R and R' are isomorphic, we write $R \cong R'$.

Proposition 9.1.5. *If $\phi : R \to R'$ is an isomorphism, then $\phi^{-1} : R' \to R$ 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 $\phi(1_R) = 1_{R'}$, we have $\phi^{-1}(1_{R'}) = \phi^{-1}(\phi(1_R)) = 1_R$.

2. For all $b_1, b_2 \in R'$, 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 $b_1, b_2 \in R'$, 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. □

The key point here is that an isomorphism is more than simply a bijective map, for it must preserve algebraic structure. For example, there is a bijective map $f : \mathbb{Z} \to \mathbb{Q}$ since both are countable, but they cannot be isomorphic as rings: Suppose $\phi : \mathbb{Z} \to \mathbb{Q}$ is an isomorphism. Then we must have $\phi(n) = n\phi(1) = n$ for any $n \in \mathbb{Z}$. So ϕ cannot be surjective.

Theorem 9.1.6. *If F is a field, then $\mathrm{Frac}(F) \cong F$.*

Proof. Define a map $\phi : F \to \mathrm{Frac}(F)$ as follows:

$$\phi(s) = [(s, 1)], \quad \forall s \in F.$$

Exercise:

1. Show that ϕ is a homomorphism.

2. Show that ϕ is bijective.

$\square$

Let R be a commutative ring, let $R[x, y]$ denote the ring of polynomials in x, y with coefficients in R:

$$R[x, y] = \left\{ \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j : m, n \in \mathbb{Z}_{\geq 0}, a_{ij} \in R \right\}$$

Proposition 9.1.7. *$R[x, y]$ is isomorphic to $R[x][y]$.*

(Here, $R[x][y]$ is the ring of polynomials in y with coefficients in the ring $R[x]$.)

Proof. We define a map $\phi : R[x, y] \to R[x][y]$ as follows:

$$\phi\left(\sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j \right) = \sum_{j=0}^{n} \left(\sum_{i=0}^{m} a_{ij} x^i \right) y^j$$

Exercise: Show that ϕ is a homomorphism.

It remains to show that ϕ is one-to-one and onto.

For $f = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} x^i y^j \in \ker \phi$, we have:

$$\phi(f) = \sum_{j=0}^{n} \left(\sum_{i=0}^{m} a_{ij} x^i \right) y^j = 0_{R[x][y]} = \sum_{j=0} 0_{R[x]} \cdot y^j,$$

which implies that, for $0 \leq j \leq n$, we have:

$$\sum_{i=0}^{m} a_{ij} x^i = 0_{R[x]}, \quad 0 \leq i \leq m.$$

Hence,

$$a_{ij} = 0_R, \quad \text{for } 0 \leq i \leq m, 0 \leq j \leq n,$$

which implies that $\ker \phi = \{0\}$. Hence, ϕ is one-to-one.

Given $g = \sum_{j=0}^{n} p_j y^j \in R[x][y]$, where $p_j \in R[x]$. We want to find $f \in R[x, y]$ such that $\phi(f) = g$. Let m be the maximum degree of the p_j's. We may write:

$$g = \sum_{j=0}^{n} \left(\sum_{i=0}^{m} a_{ji} x^i \right) y^j,$$

where a_{ji} is the coefficient of x^i in p_j, with $a_{ji} = 0$ if $i > \deg p_j$. It is clear that:

$$\phi\left(\sum_{i=0}^{m} \sum_{j=0}^{n} a_{ji} x^i y^j \right) = g.$$

Hence, ϕ is onto.

$\square$

9.1.1 Subrings

Definition. Let R be a ring. A subset S of R is said to be a **subring** of R if it is a ring under the addition $+_R$ and multiplication $\times_R$ associated with R, and its additive and multiplicative identity elements $0, 1$ are those of R.

To show that a subset S of a ring R is a subring, it suffices to show that:

- S contains the multiplicative identity of R.
- $a - b \in S$ for any $a, b \in S$.
- S is closed under multiplication, i.e. $a \cdot b \in S$ for all $a, b \in S$.

Definition. The **kernel** of a ring homomorphism $\phi : R \to R'$ is the set:

$$\ker \phi := \{a \in R : \phi(a) = 0\}$$

The **image** of ϕ is the set:

$$\operatorname{im} \phi := \{b \in R' : b = \phi(a) \text{ for some } a \in R\}.$$

Proposition 9.1.8. *Let $\phi : R \to R'$ be a ring homomorphism.*

1. *If S is a subring of R, then $\phi(S)$ is a subring of R'.*
2. *If S' is a subring of R', then $\phi^{-1}(S')$ is a subring of R.*

Proof. Let us prove 1. and leave 2. as an exercise. So let S be a subring of R.

- Since $1 \in S$, we have $\phi(1) = 1 \in \phi(S)$.
- $\phi(a) - \phi(b) = \phi(a - b) \in \phi(S)$ for any $a, b \in S$.
- $\phi(a) \cdot \phi(b) = \phi(a \cdot b) \in \phi(S)$ for any $a, b \in S$.

We conclude that $\phi(S)$ is a subring of R'. □

Corollary 9.1.9. *For a ring homomorphism $\phi : R \to R'$, $\operatorname{im} \phi$ is a subring of R'.*

Remark. Note that $\ker \phi$ is not a subring unless R' is the zero ring.

Proposition 9.1.10. *A ring homomorphism $\phi : R \to R'$ is one-to-one if and only if $\ker \phi = \{0\}$.*

Proof. Suppose ϕ is one-to-one. For any $a \in \ker \phi$, we have $\phi(0) = \phi(a) = 0$, which implies that $a = 0$ since ϕ is one-to-one. Hence, $\ker \phi = \{0\}$.

Suppose $\ker \phi = \{0\}$. If $\phi(a) = \phi(a')$, then $0 = \phi(a) - \phi(a') = \phi(a - a')$, which implies that $a - a' \in \ker \phi = \{0\}$. So, $a - a' = 0$, which implies that $a = a'$. Hence, ϕ is one-to-one. □

Proposition 9.1.11. *A subring of a field is an integral domain.*

Proof. Let F be a field and $S \subset F$ be a subring. Suppose we have $a, b \in S$ with $a \neq 0$ such that $ab = 0$. We need to show that $b = 0$. Since F is a field, $a \neq 0$ implies that it is a unit, i.e. it has a multiplicative inverse a^{-1}. So we have $0 = a^{-1}(ab) = b$. $\square$

For example, any subring of $\mathbb{C}$ is an integral domain. This produces a lot of interesting examples which are important in number theory. For instance, the *ring of Gaussian integers*:

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

is an integral domain. More generally, for any $\xi \in \mathbb{C}$, the subset

$$\mathbb{Z}[\xi] = \{f(\xi) : f(x) \in \mathbb{Z}[x]\} \subset \mathbb{C}$$

is an integral domain.