Math 2070 Week 10

Ideals, Principal Ideal Domains, Quotient Rings

10.1 Ring Homomorphisms - continued

An isomorphism is more than simply a bijective map, for it must preserve algebraic structure.

For example, there is a bijective map $f : \mathbb{Z} \to \mathbb{Q}$, but the two are clearly not isomorphic as rings:

Suppose $\phi : \mathbb{Z} \to \mathbb{Q}$ is an isomorphism. Then, both ϕ and ϕ^{-1} must send units to units.

Consider $2 \in \mathbb{Q}$. Since $\mathbb{Q}$ is a field, the nonzero element 2 is a unit. So $\phi^{-1}(2)$ must be a unit of $\mathbb{Z}$.

But the only units of $\mathbb{Z}$ are ± 1. Since ϕ is an homomorphism, we have $\phi(1) = 1 \neq 2$.

So, we are left with the case $\phi(-1) = 2$. This cannot hold either, since:

$$1 = \phi((-1)(-1)) = \phi(-1)\phi(-1)$$

implies that $\phi(-1)$ could only be $\pm 1 \neq 2$.

So, $\mathbb{Z}$ and $\mathbb{Q}$ cannot be isomorphic.

Theorem 10.1. *The fields* $\mathbb{Q}$ *and* $\mathrm{Frac}(\mathbb{Z})$ *are isomorphic.*

Proof of Theorem 10.1. Define a map $\phi : \mathbb{Q} \to \mathrm{Frac}(\mathbb{Z})$ as follows:

$$\phi(a/b) = [(a, b)], \quad \forall\, a/b \in \mathbb{Q}, a, b \in \mathbb{Z}, b \neq 0.$$

We first need to show that ϕ is well-defined. Namely, suppose $a/b = c/d$ in $\mathbb{Q}$, we need to show that $\phi(a/b) = [(a, b)]$ is equal to $\phi(c/d) = [(c, d)]$.

This is clear, since $a/b = c/d$ implies that $ad = bc$, which by definition of $\mathrm{Frac}(\mathbb{Z})$ implies that $[(a, b)] = [(c, d)]$.

We now show that ϕ is a homomorphism:

1. $\phi(1) = \phi(1/1) = [(1,1)]$, which is indeed the multiplicative identity of $\operatorname{Frac}(\mathbb{Z})$.

2. For $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$, we have:

$$\begin{aligned}\phi(a/b + c/d) = \phi((ad + bc)/(bd)) &= [(ad + bc, bd)] \\ &= [(a,b)] + [(c,d)] = \phi(a/b) + \phi(c/d)\end{aligned}$$

3. For $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$, we have:

$$\begin{aligned}\phi((a/b)(c/d)) = \phi((ac)/(bd)) &= [(ac, bd)] \\ &= [(a,b)] \cdot [(c,d)] = \phi(a/b)\phi(c/d)\end{aligned}$$

Finally, we need to show that ϕ is one-to-one and onto.

Suppose there are $a, b, c, d \in \mathbb{Z}$ such that $\phi(a/b) = \phi(c/d)$. Then, by definition of ϕ we have $[(a,b)] = [(c,d)]$, which implies that $ad = bc$, from which it follows that $a/b = c/d$ as elements of $\mathbb{Q}$. So, ϕ is one-to-one.

Given $[(a,b)] \in \operatorname{Frac}(\mathbb{Z})$, $a, b \in \mathbb{Z}$, $b \neq 0$, it is clear that a/b belongs to $\mathbb{Q}$, and $\phi(a/b) = [(a,b)]$. So ϕ is onto.

Hence, ϕ is a bijective homomorphism. In other words, it is an isomorphism. □

Theorem 10.2. *If F is a field, then* $\operatorname{Frac}(F) \cong F$.

Proof of Theorem 10.2. Define a map $\phi : F \to \operatorname{Frac}(F)$ 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.

□

Definition 10.3. The **kernel** of a ring homomorphism $\phi : A \to B$ is the set:

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

The **image** of ϕ is the set:

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

Claim 10.4. *A ring homomorphism $\phi : A \to B$ is one-to-one if and only if* $\ker \phi = \{0\}$.

Proof of Claim 10.4. 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:

$$0 = \phi(a) + (-\phi(a')) = \phi(a) + (\phi(-a')) = \phi(a + (-a')),$$

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

Definition 10.5. An **ideal** I in a commutative ring R is a subset of R which satisfies the following properties:

1. $0 \in I$;
2. If $a, b \in I$, then $a + b \in I$.
3. For all $a \in I$, we have $ar \in I$ for all $r \in R$.

If an ideal I is a proper subset of R, we say it is a **proper ideal** .

Note. If an ideal I contains 1, then $r = 1 \cdot r \in I$ for all $r \in R$, which implies that $I = R$.

Remark. There is a definition of an **ideal** in the more general case where the ring is not necessarily commutative. It is similar to the definition above, except for one extra condition: ra belongs to I for all $a \in I$, $r \in R$.

Clearly, this general definition coincides with the one above in the special case that the ring is commutative. In this introductory course, unless otherwise noted, we will always discuss ideals in the context of commutative rings.

Example 10.6. For any commutative ring R, the set $\{0\}$ is an ideal, since $0+0 = 0$, and $0 \cdot r = 0$ for all $r \in R$.

Example 10.7. For all $m \in \mathbb{Z}$, the set $I = m\mathbb{Z} := \{mn : n \in \mathbb{Z}\}$ is an ideal:

1. $0 = m \cdot 0 \in I$;
2. $mn_1 + mn_2 = m(n_1 + n_2) \in I$.
3. Given $mn \in I$, for all $l \in \mathbb{Z}$, we have $mn \cdot l = m \cdot nl \in I$.

Example 10.8. Recall the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_m$ defined by $\phi(n) = \overline{n}$. We claim that the kernel of ϕ is:

$$\ker \phi = m\mathbb{Z}.$$

Proof of Example 10.8. If $\phi(n) = \overline{n} = 0$, then $n = mq + 0 = mq$ for some $q \in \mathbb{Z}$. So, $n \in m\mathbb{Z}$. Hence, $\ker \phi \subseteq m\mathbb{Z}$.

Given $mn \in m\mathbb{Z}$, where $n \in \mathbb{Z}$, the remainder $\overline{mn}$ of the division of mn by m is clearly 0, so $\phi(mn) = 0$, which implies that $m\mathbb{Z} \subseteq \ker \phi$.

Hence, $\ker \phi = m\mathbb{Z}$. □

Claim 10.9. *Let A be a commutative ring. If $\phi : A \to B$ is a ring homomorphism, then* $\ker \phi$ *is an ideal of A.*

Proof of Claim 10.9.

1. Since ϕ is a homomorphism, we have $\phi(0) = 0$. Hence, $0 \in \ker \phi$.
2. If $a, b \in \ker \phi$, then $\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$. Hence, $a + b \in \ker \phi$.
3. Given any $a \in \ker \phi$, for all $r \in R$ we have $\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0$. Hence, $ar \in \ker \phi$ for all $r \in R$.

□

Remark.

The claim still holds if we remove the requirement that A be commutative, and "ideal" is defined using the more general definition mentioned earlier.

10.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**

10.2 Principal Ideals

For a fixed finite set of elements $a_1, a_2, \ldots, a_n$ in a commutative ring R, let $(a_1, a_2, \ldots, a_n)$ denote the subset:

$$\{r_1a_1 + r_2a_2 + \cdots + r_na_n : r_i \in R\}.$$

Claim 10.10. *The set $I = (a_1, a_2, \ldots, a_n)$ is an ideal of R.*

Proof of Claim 10.10.

1. $0 = 0 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_n \in I$.
2. For $\sum_i r_ia_i$ and $\sum_i r'_ia_i$ in I, we have $\sum_i r_ia_i + \sum_i r'_ia_i = \sum_i (r_i + r'_i)a_i \in I$.

3. Given any $\sum_i r_i a_i \in I$, for any $r \in R$ we have $r \sum_i r_i a_i = \sum_i (r r_i) a_i \in I$. □

We call $(a_1, a_2, \ldots, a_n)$ the ideal **generated** by $a_1, a_2, \ldots, a_n$. An ideal $(a) = \{ar : r \in R\}$ generated by one element $a \in R$ is called a **principal ideal** .

Note that $R = (1)$ and $\{0\} = (0)$ are both principal ideals.

Claim 10.11. *A nonzero commutative ring R is a field if and only if its only ideals are $\{0\}$ and R.*

Proof of Claim 10.11. Suppose a nonzero commutative ring R is a field. If an ideal I of R is nonzero, it contains at least one nonzero element a of R.

Since R is a field, a has a multiplicative inverse a^{-1} in R. Since I is an ideal, and $a \in I$, we have $1 = a^{-1}a \in I$.

So, I is an ideal which contains 1, hence it must be the whole field R.

Conversely, let R be a nonzero commutative ring whose only ideals are $\{0\}$ and R.

Given any nonzero element $a \in R$, the principal ideal $(a) := \{ar : r \in R\}$ generated by a is nonzero because it contains $a \neq 0$.

Hence, by hypothesis the ideal (a) is necessarily the whole ring R. In particular, the element 1 lies in (a), which means that there is an $r \in R$ such that $ar = 1$. This shows that any nonzero element of R is a unit. Hence, R is a field. □

Claim 10.12. *Let k be a field, and R a nonzero ring. Any ring homomorphism $\phi : k \to R$ is necessarily one-to-one.*

Proof of Claim 10.12. Since R is not a zero ring, it contains $1 \neq 0$. So, $\phi(1) = 1 \neq 0$, which implies that $\ker \phi$ is a proper ideal of k. Since k is a field, we have $\ker \phi = \{0\}$. It now follows from a previous claim that ϕ is one-to-one. □

Example 10.13. For any natural number $m > 1$, there can be no ring homomorphisms from $\mathbb{Q}$ to $\mathbb{Z}_m$.

The reason is as follows:

By the previous claim, any ring homomorphism from the field $\mathbb{Q}$ to $\mathbb{Z}_m$ must be one-to-one, but there can be no one-to-one map from the infinite set $\mathbb{Q}$ to the finite set $\mathbb{Z}_m$.

Claim 10.14. *Given a, b in a commutative ring R. If $b = au$ for some unit $u \in R$, then $(a) = (b)$.*

If R is an integral domain and $(a) = (b)$, then $b = au$ for some unit $u \in R$.

Proof of Claim 10.14. We leave the first part of the claim as an exercise.

We now prove the second part. Suppose $(a) = (b)$. If $b = 0$, then a is necessarily zero. So, $b = 0 = 0 \cdot 1 = a \cdot 1$, and we are done.

Now suppose $b \neq 0$. The condition $(a) = (b)$ implies that there exist $u, v \in R$ such that $b = au$ and $a = bv$.

Putting the two together, we have:

$$b = buv,$$

which implies that $b(1 - uv) = 0$.

Since R is by assumption an integral domain, and $b \neq 0$, we have $1 - uv = 0$, which implies that $uv = 1$. This shows that u is unit. □

Definition 10.15. If R is an integral domain in which every ideal is principal, we say that R is a **Principal Ideal Domain** (*abbrev.* **PID**).

Theorem 10.16. *The ring $\mathbb{Z}$ is a principal ideal domain.*

Proof of Theorem 10.16. Let I be an ideal of $\mathbb{Z}$. We already know that the zero ideal $\{0\} = (0)$ is principal.

So, we may assume that I contains a nonzero element a. Since $-1 \in \mathbb{Z}$ and I is an ideal, we have $-a = (-1) \cdot a \in I$. Hence, if I is nonzero, it contains at least one positive integer.

By the Least Integer Axiom, the ideal I contains a positive integer d which is smaller than all other positive elements of I. We claim that $I = (d)$.

By the division theorem, for every $a \in I$, we have $a = dq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < d$. But this implies that $r = a - dq$ lies in I, since I is an ideal.

Since $0 \leq r < d$ and d is the minimal positive integer in I, r must necessarily be zero. This implies that $a = dq$. Hence, $I \subseteq (d)$.

Conversely, since $d \in I$ and I is an ideal, we have $dr \in I$ for all $r \in \mathbb{Z}$, which implies that $(d) \subseteq I$.

Hence, $I = (d)$. In other words, I is a principal ideal generated by d. □

We claim that for any field k, the ring of polynomials $k[x]$ is also a PID.

To prove this we first establish the following theorem:

Theorem 10.17 (Division Theorem for Polynomials with Unit Leading Coefficients)**.** *Let R be a commutative ring. For all $d, f \in R[x]$, such that the leading coefficient of d is a unit in R, there exist $q, r \in R[x]$ such that:*

$$f = qd + r,$$

with $\deg r < \deg d$.

Proof of Division Theorem for Polynomials with Unit Leading Coefficients. The proof is essentially the same as that of the division theorem for $\mathbb{Q}[x]$. We prove by induction:

The base case corresponds to the case where $\deg f < \deg d$; and the inductive step corresponds to showing that, for any fixed d, the claim holds for f if it holds for all f' with $\deg f' < \deg f$.

Base case: If $\deg f < \deg d$, we take $r = f$. Then, indeed $f = 0 \cdot d + r$, with $\deg r < \deg d$.

Inductive step: Let $d = \sum_{i=0}^{n} a_i x^i \in R[x]$ be fixed, where a_n is a unit in R. For any given $f = \sum_{i=0}^{m} b_i x^i \in R[x]$, $m \geq n$, suppose the claim holds for all f' with $\deg f' < \deg f$.

Let:

$$f' = f - a_n^{-1} b_m x^{m-n} d.$$

Then, $\deg f' < \deg f$, hence by hypothesis there exist $q', r' \in R[x]$, with $\deg r' < \deg d$, such that:

$$f - a_n^{-1} b_m x^{m-n} d = f' = q'd + r',$$

which implies that:

$$f = (q' + a_n^{-1} b_m x^{m-n})d + r'.$$

So, $f = qd + r'$, where $q = q' + a_n^{-1} b_m x^{m-n} \in R[x]$, and $\deg r' < \deg d$. □

Theorem 10.18. *Let k be a field. Then, $k[x]$ is a PID.*

Proof of Theorem 10.18. Since k is a field, the previous claim holds for all $d, f \in k[x]$ such that $d \neq 0$.

Let I be an ideal of $k[x]$.

If $I = \{0\}$ then, it is principal, since $\{0\} = (0)$.

Suppose I is nonzero. Let d be the polynomial in I with the least degree among all nonzero polynomials in I. Since the degree of any nonzero polynomial is a nonnegative integer, such an element d exists by the Least Integer Axiom. It is clear that $(d) \subseteq I$. It remains to show that $I \subseteq (d)$.

For all $f \in I$, by the previous claim we have:

$$f = qd + r,$$

for some $q, r \in k[x]$ such that $\deg r < \deg d$.

Observe that $r = f - qd = f + (-1)qd$ lies in I. Since d is a nonzero element of I with the least degree, the element r must necessarily be zero.

In order words $f = qd$, which implies that $f \in (d)$. Hence, $I \subseteq (d)$, and we may now conclude that $I = (d)$. □

10.3 Quotient Rings

Let R be a commutative ring. Let I be an ideal of R. We define a relation $\sim$ on R as follows:

$$a \sim b, \quad \text{if } a - b \in I.$$

Notation/Terminology: If $a \sim b$, we say that a is **congruent modulo** I to b, and write:

$$a \equiv b \mod I.$$

Claim 10.19. *Congruence modulo I is an* **equivalence relation** .

Proof of Claim 10.19.

- **Reflexivity** $a - a = 0 \in I$, since I is an ideal; hence, $a \equiv a \mod I$.
- **Symmetry** If $a - b \in I$, then $b - a = -1(a - b) \in I$, since I is an ideal and $-1 \in R$. Hence, $a \equiv b \mod I$ implies that $b \equiv a \mod I$.
- **Transitivity** If $a - b \in I$ and $b - c \in I$, then $a - c = a + (-b + b) - c = (a - b) + (b - c) \in I$, since I, being an ideal, is closed under addition. Hence, $a \equiv b, b \equiv c \mod I$ implies that $a \equiv c \mod I$.

□

Let R/I be the set of equivalence classes of R with respect to the relation $\sim$. Each element of R/I has the form:

$$\overline{r} = r + I = \{r + a : a \in I\}, \quad r \in R.$$

Terminology.
We call $\overline{r}$ the **residue** of r in R/I.
Note that if $r \in I$, then $\overline{r} = \bar{0}$, since $r - 0 = r \in I$.
Observe that: for all $r, r' \in R$, and $a, a' \in I$,

$$(r + a) + (r' + a') = (r + r') + (a + a') \in (r + r') + I = \overline{r + r'},$$

$$(r + a) \cdot (r' + a') = rr' + ra' + r'a + aa' \in rr' + I = \overline{rr'}.$$

Hence, we may define binary operations $+, \cdot$ on R/I as follows:

$$\overline{r} + \overline{r'} = \overline{r + r'},$$
$$\overline{r} \cdot \overline{r'} = \overline{rr'},$$

for all $\overline{r}, \overline{r'} \in R/I$.

Claim 10.20. *The set R/I, equipped with the addition $+$ and multiplication $\cdot$ defined above, is a commutative ring.*

Proof of Claim 10.20. We note here only that the additive identity element of R/I is $\overline{0} = 0 + I$, the multiplicative identity element of R/I is $\overline{1} = 1 + I$, and that $-\overline{r} = \overline{-r}$ for all $r \in R$.

We leave the rest of the proof (additive and multiplicative associativity, commutativity, distributativity) as an **Exercise.** □

Claim 10.21. *The map $\pi : R \to R/I$, defined by*

$$\pi(r) = \overline{r}, \quad \forall r \in R.$$

is a surjective ring homomorphism with kernel $\ker \pi = I$.

Proof of Claim 10.21. **Exercise.** □

Let m be a natural number. The set:

$$m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$$

is an ideal of $\mathbb{Z}$.

Claim 10.22. *The quotient ring $\mathbb{Z}/m\mathbb{Z}$ is isomorphic to $\mathbb{Z}_m$.*

Proof of Claim 10.22. For $r \in \mathbb{Z}$, let r_m denote the remainder of the division of r by m.

Exercise: We have $\overline{r} = \overline{r_m}$ in $\mathbb{Z}/m\mathbb{Z}$, where $\bar{r}$ is the residue of r in $\mathbb{Z}/m\mathbb{Z}$.
Define a map $\phi : \mathbb{Z}_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$ as follows:

$$\phi(r) = \bar{r}, \quad \forall\, r \in \mathbb{Z}_m.$$

We claim that ϕ is a homomorphism:

- $\phi(1) = \bar{1} = 1_{\mathbb{Z}/m\mathbb{Z}}$.
-
$$\begin{aligned}\phi(r +_{\mathbb{Z}_m} r') = \overline{r +_{\mathbb{Z}_m} r'} = \overline{(r +_{\mathbb{Z}} r')_m}& \\ = \overline{r +_{\mathbb{Z}} r'} = \overline{r} + \overline{r'} = \phi(r) + \phi(r')&\end{aligned}$$
-
$$\begin{aligned}\phi(r \cdot_{\mathbb{Z}_m} r') = \overline{r \cdot_{\mathbb{Z}_m} r'} = \overline{(r \cdot_{\mathbb{Z}} r')_m}& \\ = \overline{r \cdot_{\mathbb{Z}} r'} = \overline{r} \cdot \overline{r'} = \phi(r) \cdot \phi(r')&\end{aligned}$$

Hence, ϕ is a homomorphism.

Next, we show that ϕ is bijective:

For all $\bar{r} \in \mathbb{Z}/m\mathbb{Z}$, we have $\phi(r_m) = \overline{r_m} = \overline{r}$. Hence, ϕ is onto.

Suppose r is an element in $\mathbb{Z}_m$ such that $\phi(r) = \overline{r} = 0$ in $\mathbb{Z}/m\mathbb{Z}$. By definition, this means that $r \in m\mathbb{Z}$, or equivalently, that $m|r$. Since $0 \leq r < m$, we must have $r = 0$. Hence, $\ker \phi = \{0\}$. It now follows from Claim 10.4 that ϕ is one-to one.

We conclude that $\phi : \mathbb{Z}_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$ is an isomorphism. □

Claim 10.23. *Let $\phi : R \longrightarrow R'$ be a ring homomorphism. Then, the image of ϕ:*

$$\operatorname{im} \phi = \{r' \in R' : r' = \phi(r) \textit{ for some } r \in R\}$$

is a ring under the addition and multiplication operations of R'. (In fact, it is a subring of R'.)

Proof of Claim 10.23. **Exercise.** □

Theorem 10.24 (First Isomorphism Theorem)**.** *Let R be a commutative ring. Let $\phi : R \longrightarrow R'$ be a ring homomorphism. Then:*

$$R/\ker \phi \cong \operatorname{im} \phi,$$

(i.e. $R/\ker \phi$ is isomorphic to $\operatorname{im} \phi$.)

Proof of First Isomorphism Theorem. We define a map $\overline{\phi} : R/\ker \phi \longrightarrow \operatorname{im} \phi$ as follows:

$$\overline{\phi}(\overline{r}) = \phi(r), \quad \forall\, r \in R,$$

where $\overline{r}$ is the residue of r in $R/\ker \phi$.

We first need to check that ϕ is well-defined. Suppose $\overline{r} = \overline{r'}$, then $r' - r \in \ker \phi$. We have:

$$\phi(r') - \phi(r) = \phi(r' - r) = 0.$$

Hence, $\phi(r') = \phi(r)$. So, $\overline{\phi}$ is well-defined.

Next, we show that $\overline{\phi}$ is a homomorphism:

- $\overline{\phi}(\overline{1}) = \phi(1) = 1;$
- $\overline{\phi}(\overline{a} + \overline{b}) = \overline{\phi}(\overline{a + b}) = \phi(a + b) = \phi(a) + \phi(b) = \overline{\phi}(\overline{a}) + \overline{\phi}(\overline{b});$
- $\overline{\phi}(\overline{a} \cdot \overline{b}) = \overline{\phi}(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(\overline{a})\overline{\phi}(\overline{b}).$

Finally, we show that $\overline{\phi}$ is a bijection, i.e. one-to-one and onto.

For any $r' \in \operatorname{im}\phi$, there exists $r \in R$ such that $\phi(r) = r'$. Since $\overline{\phi}(\overline{r}) = \phi(r) = r'$, the map $\overline{\phi}$ is onto.

Let r be an element in R such that $\overline{\phi}(\overline{r}) = \phi(r) = 0$. We have $r \in \ker\phi$, which implies that $\overline{r} = 0$ in $R/\ker\phi$. Hence, $\ker\overline{\phi} = \{0\}$, and it follows from Claim 10.4 that $\overline{\phi}$ is one-to-one. □

Corollary 10.25. *If a ring homomorphism $\phi : R \longrightarrow R'$ is surjective, then:*

$$R' \cong R/\ker\phi$$