Lecture 12: Ideals, Quotient rings

Lecture: Sujata Ghosh *Scribe: Aranya Kumar Bal, Sandeep Chatterjee*

1 Topics for this lecture

In this lecture, we shall talk about the following

1. Ring Homomorphism
2. Ideals and Principal Ideal
3. Quotient Rings
4. Units in a Ring
5. Introduction to Fields

2 Ring Homomorphism

Definition 2.1 *A function $f : (R, +, \cdot) \to (R', +', \cdot')$ is said to be a ring homomorphism if the following hold for all $r_1, r_2 \in R$:*

1. $f(r_1 + r_2) = f(r_1) +' f(r_2)$
2. $f(r_1 \cdot r_2) = f(r_1) \cdot' f(r_2)$

2.1 Kernel of a ring homomorphism

Let R and R' be two rings, and let $f : R \to R'$ be a ring homomorphism. Then, kernel of f, denoted $\ker f$ is defined as follows:

$$\ker f = \{r \in R \mid f(r) = 0_{R'}\}$$

Question: Suppose $a, b \in \ker f$. Is $a + b \in \ker f$?

$$f(a + b) = f(a) + f(b) = 0 + 0 = 0$$

So, $a + b \in \ker f$.
Question: Suppose $a, b \in \ker f$. Is $a \cdot b \in \ker f$?

$$f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot 0 = 0$$

So, $a \cdot b \in \ker f$.
Question: Suppose $r \in R$ and $a \in \ker f$. Do $r + a$ and $r \cdot a$ belong to $\ker f$?

$$f(r + a) = f(r) + f(a) = f(r) + 0_{R'} = f(r)$$

which may or may not be 0, hence, $r + a$ may not belong to $\ker f$.

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0_{R'} = 0_{R'}$$

So, $r \cdot a$ will always be in $\ker f$.

So, we can say the following now.

Theorem 2.2 *For $f : R \to R'$ a ring homomorphism*

- $\ker f$ *forms a subgroup of R under $+$*
- *If $r \in R$ and $a \in \ker f$, then $r \cdot a \in \ker f$*

This leads to the notion of ideals.

3 Ideals of a ring R

Let R be a commutative ring with identity. I subset of R is said to be an ideal of R if:

- $(I, +)$ is a subgroup of $(R, +)$
- For any $r \in R$, $a \in I$, $r \cdot a \in I$

Examples:

1. $\ker f$, where f is a ring homomorphism
2. $\{0_R\}$
3. R, the entire ring
4. take any $a \in R$, Consider $\langle a \rangle = \{r \cdot a | r \in R\}$ then $\langle a \rangle$ forms an ideal of R. This is called the principal ideal generated by a in R.

Exercise: Prove that $\langle a \rangle$ is an ideal of R

Homework: What are the ideals of $(\mathbb{Z}, +, \cdot)$?

Homework: What are the ideals of $(\mathbb{Z}/p^k\mathbb{Z}, +, \cdot)$, where p is a prime number, $k \geq 1$?

Now, we have that for any homomorphism f, we have an ideal given by $\ker f$.

How about the opposite side? Given an ideal I of a ring R, can we get a homomorphism f such that $\ker f = I$? To answer this question, let us introduce the concept of quotient rings

4 Quotient Ring

Let R be a ring and I be an ideal of R. Since $(I,+)$ is a subgroup of $(R,+)$, we can define the quotient group $(R/I,+)$, where $R/I = \{r + I : r \in R\}$, and

$$(r + I) + (r' + I) = (r + r') + i$$

We have that $(R/I,+)$ forms a commutative group.
Now, define

$$(r + I) \cdot (r' + I) = r \cdot r' + I$$

> **Exercise:** Explain the definition of $(r + I) \cdot (r' + I)$

Note that $r + I$, $r' + I$, $rr' + I$ are all subsets of R.
Take $a \in r + I$ and $b \in r' + I$. Then, $a = r + i$ and $b = r' + i'$ for some $i, i' \in I$. Now , we have

$$a \cdot b = (r + i) \cdot (r' + i') = rr' + ri' + ir' + ii' = rr' + i^{\#}, \text{ where } i^{\#} \in I$$

> **Exercise:** Prove that $i^{\#} \in I$

So, we see that the definition does make sense.

> **Exercise:** Show the following :
>
> 1. $\cdot$ is associative in R/I
> 2. Distributive laws hold in R/I .

So, $(R/I,+,\cdot)$ does form a ring. Now, since R is commutative with identity, so is R/I with $(1 + I)$ serving as the identity. So, $(R/I,+,\cdot)$ is a commutative ring with identity.

Coming back to our original question regarding a ring R and its ideal I, consider $f : R \to R/I : r \to r + I$. we have $\ker f = I$

5 Units in a ring R

An element $a \in R$ is said to be a unit in an unital ring R if there exists $b \in R$ such that $a \cdot b = 1$.
Examples:

1. What are the units in $(\mathbb{Z},+,\cdot)$?
   $\{1,-1\}$
2. What are the units in $(\mathbb{Z}/4\mathbb{Z},+,\cdot)$?
   $\{[1],[3]\}$

3. What are the units in $(\mathbb{Z}/5\mathbb{Z}, +, \cdot)$?
   All the non-zero elements of $\mathbb{Z}/5\mathbb{Z}$
4. What are the units in $(M_n(\mathbb{R}), +, \cdot)$?
   All the elements of $GL_n(\mathbb{R})$. [Note that this is a non-commutative ring]

6 Field

Definition 6.1 *A field is a commutative ring with identity such that every non-zero element is a unit.*

From the examples above, $(\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ forms a field. Other examples are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Complete Definition of a Field

A field is a nonempty set F with at least two elements and binary operations $+$ and $\cdot$, denoted $(F, +, \cdot)$, and satisfying the following field axioms:

- Associativity of addition: Given any $a, b, c \in F$, $(a + b) + c = a + (b + c)$.
- Commutativity of addition: Given any $a, b \in F$, $a + b = b + a$.
- Additive identity: There exists an element $0_F \in F$ such that for all $a \in F$, $a + 0_F = 0_F + a = a$.
- Additive inverse: Given any $a \in F$, there exists a $b \in F$ such that $a + b = b + a = 0_F$.
- Associativity of multiplication: Given any $a, b, c \in F$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- Commutativity of multiplication: Given any $a, b \in F$, $a \cdot b = b \cdot a$.
- Multiplicative identity: There exists an element $1_F \in F$ such that for all $a \in F$, $1_F \cdot a = a \cdot 1_F = a$.
- Multiplicative inverse: For all $a \in F$, $a \neq 0_F$, there exists a $b \in F$ such that $a \cdot b = b \cdot a = 1_F$.
- Left distributivity: For all $a, b, c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$.
- Right distributivity: For all $a, b, c \in F$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

If you had read the pervious lecture scribe, you would quickly realise that this just saying that a field is nothing but $(F, +, \cdot)$ such that $+$ and $\cdot$ both form groups and $+$ distributes over $\cdot$.

7 Ideals of a field R

Question: What are the ideals of a field R?

Since a field is also a ring, clearly $\{0_R\}$ and R are ideals of R.

A fun theorem now says

Theorem 7.1 *A field has no other ideals.*

Proof. If I is any other ideal, then say $a \in I$, $a \neq 0$. Then there is some $b \in R$ such that $ab = 1$. Since I is an ideal, $1 = ab \in I$ and thus $I = R$ a contradiction. □

The next fun theorem states that things are even funnier.

Theorem 7.2 *Any non-trivial commutative ring R with identity with only 2 ideals is a field.*

Proof. All we have to show is that every element has inverses. Since R is non-trivial, there is some element $a \in R$ with $a \neq 0$. Then clearly the principal ideal (a) is not $\{0\}$ as $a \in (a)$. Then $(a) = R$. Then $1 \in (a)$. Thus $1 = ab$ for some $b \in R$ and thus b is the inverse of a and we are done. □

We can summarise the fun theorems as follows.

Theorem 7.3 *Let R be a commutative ring with identity. Then the following are equivalent.*

1. *R is a field.*
2. *The only ideals of R are $\{0\}$ and R*

Example: Ideals of $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ are $\{[0]\}$, $\{[0], [2]\}$, $\mathbb{Z}/4\mathbb{Z}$. Since the number of ideals more than 2, this is not a field.

Ideals of a general unital ring

Let R be a ring with identity. Then the definition of ideals we made directly does not make sense since $ar \in I$ does not mean $ra \in I$. So we separate them out into three parts.

A subset $I \subset R$ is called a *left ideal* of R if $a, b \in I \Rightarrow a + b \in I$ and $a \in I \Rightarrow ra \in I$ for all $a \in R$.

A subset $I \subset R$ is called a *right ideal* of R if $a, b \in I \Rightarrow a + b \in I$ and $a \in I \Rightarrow ar \in I$ for all $r \in R$.

A subset is called a *both sided ideal* if it is both a left and right ideal. Note that for a commutative ring, all the three notions are the same.

Exercise*: Let R be a ring with identity. Show that the following are equivalent.

1. R is a division ring.
2. The only left ideals of R are $\{0\}$ and R.