LECTURE 12

08.03.2024

Ring homomorphisms

A function $f : (R, +, \cdot) \longrightarrow (R', +', \cdot')$ 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) $f(r_1 \cdot r_2) = f(r_1) \cdot' f(r_2)$

Kernel of a ring homomorphism

Let R and R' be two rings, and let $f : R \to R'$ be a ring homomorphism. The kernel of f, denoted $\operatorname{Ker} f$ is defined as follows:

$$\operatorname{Ker} f = \{ r \in R : f(r) = 0_{R'} \}$$

Q. Suppose $a, b \in \operatorname{Ker} f$. Is $a + b \in \operatorname{Ker} f$?

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

So, $a + b \in \operatorname{Ker} f$.

Q. Suppose $a, b \in \text{Ker } f$. Is $a \cdot b \in \text{Ker } f$?

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

Q. Suppose $r \in R$ and $a \in \text{Ker } f$. Do $r + a$ and $r \cdot a \in \text{Ker } f$?

- $f(r + a) = f(r) + f(a) = f(r) + 0_{R'}$
  $= f(r)$ which may or may not be $0_{R'}$.

Hence, $f(r+a)$ may not be $0_{R'}$, that is $r + a$ may not belong to $\text{Ker } f$.

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

So, $r \cdot a$ will always be in $\text{Ker } f$.

So, we can say the following:

- $\text{Ker } f$ forms a subgroup of R under $+$.
- If $r \in R$ and $a \in \text{Ker } f$, then $r \cdot a \in \text{Ker } f$.

This leads to the notion of ideals.

Ideals of a ring R

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

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

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: $(a) = \{r.a : r \in R\}$. Does (a) form an ideal of R? Yes (check!)

(a) is known as a principal ideal of R generated by a.

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

Is the converse true? Given an ideal I of a ring R, can we get a homomorphism f s.t. $\ker f = I$? To answer this question let us introduce the concept of quotient rings.

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 $(r+I).(r'+I) = rr'+I$.

Does this definition make sense?

Note that $r+I$, $r'+I$, $rr'+I$ are all sets of elements from 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:

$$\begin{aligned} a \cdot b &= (r+i).(r'+i') \\ &= rr' + ri' + ir' + ii' \\ &= rr' + i^{\#}, \text{ where } i^{\#} \in I \quad (\text{Why?}) \\ &\in rr' + I \end{aligned}$$

So, we see that the definition does make sense. Check its well-definedness!!

- $\cdot$ is associative in R/I (Check!)
- distributivity laws hold in R/I (Check!)

So, $(R/I, +, \cdot)$ forms a ring.

Now, the ring is commutative as well.

Also, it has the multiplicative identity, given by $1 + I$, where 1 denotes the multiplicative identity of R.

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 $f : R \to R/I$; $r \mapsto r + I$, we have $\ker f = I$.

Units in a ring R.

An element $a \in R$ is said to be a unit in R if there exists $b \in R$ s.t. $a \cdot b = 1$.

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 $(M_n(\mathbb{R}), +, \cdot)$?

(Note that this is a non-commutative ring)

All the elements of $GL_n(\mathbb{R})$.

Field

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 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Q. What are the ideals of a field R?

$\{0_R\}$ is an ideal of R.

Now, let I be an ideal of R, such that $I \neq \{0_R\}$. Take any $a \in I$, s.t. $a \neq 0_R$. Since R is a field, there is a $b \in R$, s.t. $a \cdot b = 1$. So, $1 \in I$, that is $I = R$. R can have only two ideals.

Q. What about the converse?

Let us consider a commutative ring with identity, R, say, such that R has only two ideals. Does R form a field?

To show that R is a field, we need to show that every non-zero element of R is a unit.

Take $a \in R$, s.t. $a \neq 0_R$.

To show that a is a unit.

The information that we have about R is that R has only two ideals. Now, let us consider (a), the principal ideal generated by a. Can the principal ideal generated by a be $\{0_R\}$? No, as $a \neq 0_R$. So, $(a) = R$. Then, $1_R \in (a)$. So, there is $b \in R$ s.t. $b.a = 1_R$. Hence, a is a unit.

Hence, every non-zero element

in R is a unit. Thus, R forms a field. This completes the proof.

Example :

Ideals of $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$ are

$\{[0]\}$, $\mathbb{Z}/4\mathbb{Z} = ([1])$, $([2]) = \{[0], [2]\}$

Number of ideals > 2

H.W. What are the ideals of $(\mathbb{Z}, +, \cdot)$?

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