Ring Theory

Lecture 22

<u>Defn.</u> Let R be a ring. A non-zero elt $a \in R$ is called a zero divisor if $\exists$ a non zero elt $b \in R$ s.t $a \cdot b = 0$ or $ba = 0$.

<u>Example</u> $\mathbb{Z}/6\mathbb{Z}$ $\quad \bar{2} \cdot \bar{3} = \bar{0}$.

In $\mathbb{Z}/6\mathbb{Z}$, $\bar{2}$ and $\bar{3}$ are zero divisors.

In $\mathbb{Z}/n\mathbb{Z}$, $\bar{m}$ will be a zero divisor if $\gcd(m, n) \neq 1$.

In $M_n(\mathbb{R})$ we can find zero divisor as well.

Remark: Observe that a zero divisor can never be a unit. Suppose a is a zero divisor and also a unit.

$\exists$ some nonzero $b \in R$ s.t

$$ab = 0.$$

Since a is a unit $\exists$ $v \in R$ s.t

$$va = 1.$$

Then $ab = 0$

$$(va)b = v.0 = 0$$

$$\Rightarrow 1.b = 0 \Rightarrow b = 0.$$

which is a contradiction.

Thus a zero divisor can never be an unit.

Defn: A subring of a ring R is a subgp of R under addition which is closed under multiplication and contains 1.

Example. (1) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, are subrings.

Ring Homomorphisms:

Let R an S be two rings. Then a map $\phi : R \longrightarrow S$ is called a ring homomorphism if

(1) $\phi(a+b) = \phi(a) + \phi(b)$

(2) $\phi(ab) = \phi(a)\phi(b)$ $\quad \forall a, b \in R$.

(3) $\phi(1_R) = 1_S$.

$\hookrightarrow$ This condn. is not mandatary in other books like Dummit & Foote. But for this course (3) is compulsory.

<u>Example</u> (1) $f : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

$$f(m) = \overline{m} = m + n\mathbb{Z}.$$

$$f(m_1 + m_2) = \overline{m_1 + m_2} = \overline{m_1} + \overline{m_2}$$
$$= f(m_1) + f(m_2).$$

$$f(m_1 m_2) = \overline{m_1 m_2} = \overline{m_1}\,\overline{m_2} = f(m_1) f(m_2).$$

$$f(1) = \overline{1}.$$

Thus f is a ring homo.

(2) $f : \mathbb{R}[x] \longrightarrow \mathbb{R}$ defined by

$$f\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i \alpha^i$$

where $\alpha \in \mathbb{R}$ is fixed.

f is a ring homomorphism.

<u>Defn</u>. Let $\phi: R \to S$ be a ring homo.

Then $\ker\phi = \{a \in R \mid \phi(a) = 0\}$.

<u>Q</u> Is $\ker\phi$ a subring of R?

Is $\ker\varphi$ closed under multiplication?

Yes. ✓

$\ker\varphi$ is a subgp of R ✓

Suppose $1_R \in \ker\varphi$.

$$\varphi(1_R) = 0_S$$

Since φ is a ring homo $\varphi(1_R) = 1_S$.

i.e $1_S = 0_S$ in S.

$$S = 0.$$

Propn: Let $\varphi : R \longrightarrow S$ be a ring homo.

(1) The image of φ is a subring of S.

(2) The kernel φ is not a subring of R unless it is the whole ring R.

($\ker \varphi = R$)

Furthermore, if $\alpha \in \ker \varphi$ then $r\alpha$ and $\alpha r \in \ker \varphi$ $\forall r \in R$.

Pf: For any $r \in R$,

$$\varphi(r\alpha) = \varphi(r)\,\varphi(\alpha) = \varphi(r) \cdot 0 = 0$$

$\Rightarrow r\alpha \in \ker \varphi.$

Defn. Let R be a ring and I be a subset of R. Then I is said to be a left ideal if I is a subgp of $(R,+)$ and I is closed under left multiplication i.e $rI \subseteq I$.

and I is said to be a right ideal if I is a subgp of $(R,+)$ and I is closed under right multiplication i.e $Ir \subseteq I$.

A subset I is which is both a left ideal and a right ideal is called an ideal of R.

Example Define $\phi : \mathbb{Q}[x] \to \mathbb{R}$.

$$\phi(f(x)) = f(\sqrt{2})$$

$$\ker\phi = \{ f(x) \in \mathbb{Q}[x] \mid \phi(f(x)) = 0 \}$$

$$= \{ f(x) \in \mathbb{Q}[x] \mid f(\sqrt{2}) = 0 \}.$$

Note that $\ker\phi$ doesn't contain any linear or non-zero constant poly.

Note $(x^2 - 2) \in \ker\phi$.

Claim $\ker\phi \underset{\supseteq}{=} \{ (x^2-2)\, q(x) \mid q(x) \in \mathbb{Q}[x] \}$

Let $g(x) \in \ker\phi \Rightarrow g(\sqrt{2}) = 0$.

Applying division algo we get

$$g(x) = (x^2-2)\,p(x) + r(x).$$

where either $r(x) = 0$ or $\deg r(x) < 2$.

$\because\ g(\sqrt{2}) = 0$ $\qquad p(x), r(x) \in \mathbb{Q}[x]$.

$\Rightarrow\ r(\sqrt{2}) = 0.$

$\Rightarrow\ r(x) = 0.$

$\therefore\ \ker\phi = \{ (x^2-2)\,q(x) \mid q(x) \in \mathbb{Q}[x] \}$.

$= (x^2-2)$

In any ring R, the set of multiples of a particular elt forms an ideal, called the principal ideal gen by a and denoted by
$$(a) = \{ ar \mid r \in R \}.$$

We may consider the ideal I gen by a set of elts $a_1, a_2, \dots, a_n$ of R which is defined to be the smallest ideal containing these elts and it is denoted by

$$(a_1, a_2, \dots, a_n) = \{ r_1 a_1 + \dots + r_n a_n \mid r_i \in R \}.$$

In any ring R we have two ideals one is the zero ideal ideal (0). and the other one the whole ring which is gen by $(1) = R$, (0) is called the zero ideal & (1) is called the unit ideal.

Q Identify all the ideals of a field.

Q Identify all the ideals of $\mathbb{Z}$.