Ring Theory

Lecture 23

Let R be a ring. $I \subset R$ is said to be an ideal of R if I is a subgp of $(R,+)$ and I is closed under left & right multiplication i.e $rI \subseteq I$ and $Ir \subseteq I$ $\forall r \in R$.

In any (non zero) ring R there always exists two ideals the zero ideal which is generated by (0). and the whole ring which is gen by (1)

$$(1) = \{ r.1 \mid r \in R \} = R.$$

Let R be any ring and $a \neq 0 \in R$ then $(a) = \{ ar \mid r \in R \}$.

Example In $\mathbb{Z}$ if I consider any nonzero integer say n then

$$(n) = \{nm \mid m \in \mathbb{Z}\} = n\mathbb{Z}.$$

Let $a_1, \ldots, a_n \in R$ then we can consider the ideal generated by $a_1, \ldots, a_n$ which is defined as

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

An ideal I is said to be proper if it is not (0) or (1).

Prop (a) Let F be a field. The only ideals of F are zero and unit ideal.

(b) If a nonzero ring R has exactly two ideals then R is a field.

Pf: (a) Let $0 \neq a \in F$ then $(a) = (1)$

Since a is invertible $\exists\ b \in F$ s.t $ba = 1$. $\therefore 1 = ba \in (a)$.

$\therefore (a) = (1)$.

(b) Let R has exactly two ideals.

Let $0 \neq a \in R$. be any elt.

$(a) = (1)$. i.e $a \in (1)$.

i.e $\exists\ b \in R$ s.t $ba = 1$.

Therefore a has an inverse and hence R is a field.

Propn. Let F be a field and R be any non-zero ring. Then every ring homo $\varphi : F \to R$ is injective.

Pf: $\ker\phi$ is either (0) or (1).

If $\ker\phi = (1)$ then R will be the zero ring which is a contradiction.

$\therefore \ker\phi = (0)$.

Hence ϕ is injective.

If $\ker\phi = (1)$.

$\phi(1) = 0$

$\phi(1) = 1_R$.

i.e $1_R = 0$.

then R is the zero ring.

Integral domain : An integral domain R is a non zero ring having no zero divisor i.e if $ab = 0$ then $a = 0$ or $b = 0$

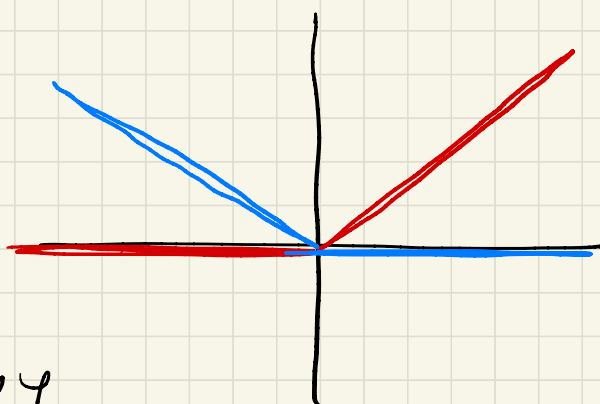
Example (1) Any field is an integral domain

(2) $\mathbb{Z}$, $F[x]$ where F is a field is an integral domain.

(3) $C(\mathbb{R}) = \{ f : \mathbb{R} \to \mathbb{R} \mid f \text{ is cont}^{n}. \}$ is not an integral domain

Define $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} 0 & \forall x < 0 \\ x & \forall x \geq 0 \end{cases}$$



and $g : \mathbb{R} \to \mathbb{R}$ by

$$g(x) = \begin{cases} x & \forall x \leq 0 \\ 0 & \forall x > 0. \end{cases}$$

Then $f \cdot g \equiv 0$ but $f \neq 0$, $g \neq 0$.

Propn: $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is a prime number.

Propn: Let R be an integral domain if $ab = ac$ and $a \neq 0$ then $b = c$.

Pf: $ab = ac \Rightarrow a(b-c) = 0$

Since R is an integral domain

so either $a = 0$ or $(b-c) = 0$.

But $a \neq 0$ therfore $b - c = 0$

$\Rightarrow b = c$.

Propn. Let R be an integral domain then $R[x]$ is also an integral domain.

Propn. A finite integral domain is a field.

Pf: Let R be a finite integral domain.

WTS every $0 \neq x \in R$ has inverse.

Consider the elts $1, x, x^2, x^3, \ldots \in R$.

$\because R$ is finite $\exists\ r > s$ s.t

$$x^r = x^s$$

$$\Rightarrow x^r - x^s = 0$$

$$\Rightarrow x^s (x^{r-s} - 1) = 0$$

$\because R$ is an int domain & $x^n \neq 0$

$$\Rightarrow x^{r-s} = 1$$

$$\Rightarrow x \cdot x^{r-s-1} = 1$$

$\Rightarrow x^{r-s-1}$ is the inverse of x. $\therefore R$ is a field.

Quotient ring :

Let I be any ideal of R. Then we have already seen that the set of all left cosets of I forms a g/p R/I under addition.

Q Does R/I has a ring structure?

Want to define multiplication of two left cosets.

$$(a+I)\cdot(b+I) = ab + I$$

$$(a+u)\cdot(b+v) = ab + \underbrace{av+ub+uv}_{I}$$

$u \in I$, $v \in I$

Well defined:

$a + I = a' + I$

$b + I = b' + I$.

WTS $ab + I = a'b' + I$

$\hookrightarrow a - a' = u \in I$ and $b - b' = v \in I$.

Then $ab = (a'+u)(b'+v)$

$= a'b' + \underbrace{a'v + ub' + uv}_{\in I}$

$\Rightarrow ab - a'b' \in I$.

Thus $ab + I = a'b' + I$. ——(*)

Thus R/I has a ring structure with multiplication defined as in (*) with identity $1 + I$.

1st Isomorphism Thm: Let $f: R \to S$ be a surjective ring homo then $\bar{f}: R/\ker f \to S$ is an isomorphism i.e $R/\ker f \cong S$.

Pf: Define $\bar{f}: R/\ker f = I \to S$ by

$$\bar{f}(a+I) = f(a) \quad [\text{Let } I = \ker f]$$

WTS $\bar{f}$ is a ring homo.

$$\bar{f}(a+I+b+I) = \bar{f}(a+b+I) = f(a+b)$$

$$\bar{f}(a+I) + \bar{f}(b+I) = f(a) + f(b) = f(a) + f(b).$$

$$\bar{f}((a+I)\cdot(b+I)) = \bar{f}(ab+I) = f(ab)$$

$$\bar{f}(a+I)\cdot\bar{f}(b+I) \longrightarrow = f(a)f(b)$$

$\bar{f}(1+I) = f(1) = 1_S$.

$\therefore$ $\bar{f}$ is a ring homo.

Clearly $\bar{f}$ is surjective as f is surjective

$$\ker \bar{f} = \{ a+I \in R/I \mid \bar{f}(a+I) = 0 \}$$

$$= \{ a+I \in R/I \mid f(a) = 0 \}$$

$$= \{ a+I \in R/I \mid a \in I \},$$

$$= I.$$

$\therefore$ $\bar{f}$ is injective.

$\therefore$ $\bar{f}$ is an isomorphism.

Defn. A ring homo $g: R \to S$ is said to be an isomorphism if g is 1-1 and onto.

Example (1) Let $\mathbb{R}[x]$ = poly ring with coeff in $\mathbb{R}$.

Define $\phi : \mathbb{R}[x] \longrightarrow \mathbb{C}$.

$$\phi(f(x)) = f(i^0)$$

ϕ is surjective as $a+bx \longmapsto a+ib$.

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

Note that $(x^2+1) \in \ker\phi$.

Let $f(x) \in \ker\phi$.

Then $f(x) = (x^2+1)\,q(x) + r(x)$

where $\deg r(x) \leq 1$ or $r(x) = 0$.

Since $f(i^0) = 0. \Rightarrow r(i^0) = 0.$

$\Rightarrow r(x) = 0.$

$\therefore f(x) \in (x^2+1).$

Hence $\ker\phi = (x^2+1)$. $\quad \frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{C}$

Ex. Show that $\frac{\mathbb{Z}[x]}{(x^2+1)} \cong \mathbb{Z}[i]$.

where $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$.

$\mathbb{Z}[i]$ is a ring. and this is known as the ring of Gaussian integers.

Propn. Let $f: R \to S$ be a surj ring homo and $J \subseteq S$ be an ideal. Then $f^{-1}(J) := \{a \in R \mid f(a) \in J\}$ is an ideal of R and $R/f^{-1}(J) \cong S/J$.

Pf: It is clear that $f^{-1}(J)$ is a subgp of R. Let $r \in R$ and $a \in f^{-1}(J)$ WTS $ra \in f^{-1}(J)$.

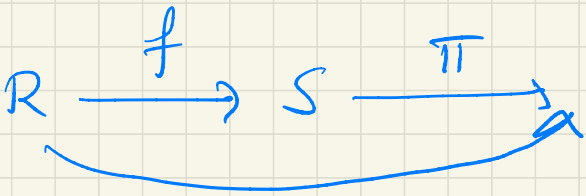
Now $f(ra) = f(r)f(a)$

Since $f(a) \in J$ and J is an ideal

$\therefore f(r)f(a) \in J$.

Thus $ra \in f^{-1}(J)$

Hence $f^{-1}(J)$ is an ideal of R.



$\pi(b) = b + J$.

check π is a surj ring homo.

$\pi \circ f : R \longrightarrow S/J$ is a surjective ring homo.

$$\ker(\pi \circ f) = \{a \in R \mid (\pi \circ f)(a) \in J\}$$
$$= \{a \in R \mid f(a) \in J\} = f^{-1}(J)$$

∴ By 1st isomorphism Thm

$$R/f^{-1}(J) \cong S/J.$$

Cor Let $\pi: R \longrightarrow R/I$ where I is an ideal of R. Let $J \supseteq I$ be an ideal of R. Then $\pi^{-1}(J/I) = J$.

and by previous cor.

$$R/J \cong R/I \Big/ J/I.$$

where $J/I = \{a+I \mid a \in J\}$.

Cor Ideals of R/I have the form $J/I = \{b+I \mid b \in J\}$ where J is an ideal of R containing I

Homomorphism Thm:

Let $f: R \to S$ be a surjective ring homo. Then $\exists$ a bijection between the set $(K = \ker f)$

$$\left\{\begin{array}{l}\text{all ideals of } R \\ \text{containing } K\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{all ideals} \\ \text{of } S\end{array}\right\}.$$

$$J \rightsquigarrow f(J)$$

$$f^{-1}(I) \reflectbox{$\rightsquigarrow$} I$$

Ex 1. Show that $f(J)$ is an ideal of S where J is an ideal of R.

Ex 2. Show that $f^{-1}(I)$ is an ideal of R containing K.