Ring Theory

Lecture 25

Thm Let R be an integral domain. There exists an inj homo $R \longrightarrow F$ where F is a field.

Pf: Consider the set

$$\mathcal{F} = \{(a,b) \mid a, b \in R \text{ and } b \neq 0\}.$$

Define a relation on $\mathcal{F}$ as follows.

$(a,b) \sim (c,d)$ if $ad - bc = 0$.

WTS $\sim$ is transitive.

If $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$

WTS $(a_1, b_1) \sim (a_3, b_3)$

(1) — $a_1 b_2 - b_1 a_2 = 0$ and $a_2 b_3 - b_2 a_3 = 0$ — (2)

WTS $a_1 b_3 - b_1 a_3 = 0$.

$(1) \times b_3 + (2) \times b_1$ gives me.

$$a_1 b_2 b_3 - a_3 b_2 b_1 = 0.$$

$$\Rightarrow \quad b_2 (a_1 b_3 - a_3 b_1) = 0.$$

Since $b_2 \neq 0$ and R is an integral domain therefore $a_1 b_3 - a_3 b_1 = 0$.

Therefore $\sim$ is an equivalence relation.

$F :=$ Set of all equivalence classes.

Equivalence class of $(a,b) \in \mathcal{F}$ is denoted by a/b.

NTS F is a field.

Define '$+$' and '$\cdot$' in F by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

and $$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Check these are well defined.

F has additive identity $\frac{0}{1}$ and multiplicative identity $\frac{1}{1}$.

WTS Every non-zero elt in F has a multiplicative inverse.

Let $\frac{a}{b} \neq \frac{0}{1}$ i.e $a \neq 0$.

then $\frac{b}{a} \in F$. which is the inverse of $\frac{a}{b}$.

$\therefore$ F is a field.

Define $\phi : R \longrightarrow F \qquad \phi(r) = \frac{r}{1}$.

$$\ker \phi = \left\{ r \in R \mid \phi(r) = \frac{0}{1} \right\}.$$

$$= (0).$$

$\therefore$ ϕ is an inj ring homo.

Defn. F is called the quotient field of R and is denoted by $Q(R)$.

Example. (1) $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$.

(2) The quotient field of poly ring $k[x]$ over k (is a field),

$$k(x) := \left\{ \frac{f(x)}{g(x)} \mid g(x) \neq 0 \right\}.$$

Propn. Let R be an integral domain with quotient field F and let $\varphi : R \to K$ be any injective ring homo from R to a field K. Then there is a unique $\varphi^* : F \to K$ homo which is extension of φ.

Pf: Define $\varphi^* : F \longrightarrow K$

using $\varphi : R \longrightarrow K$.

$$\varphi^*\left(\frac{a}{b}\right) = \varphi(a)\,\varphi(b)^{-1}$$

[$\because \varphi$ is inj° for $b \neq 0$, $\varphi(b) \neq 0$ hence invertible in K].

WTS φ^* is well defined.

Let $\frac{a}{b} = \frac{c}{d}$

WTS $\varphi^*\left(\frac{a}{b}\right) = \varphi^*\left(\frac{c}{d}\right)$

$\hookrightarrow ad - bc = 0$

$\Rightarrow \varphi(ad - bc) = 0$

$\Rightarrow \varphi(a)\varphi(d) - \varphi(b)\varphi(c) = 0$

$\Rightarrow \varphi(a)\varphi(d) = \varphi(b)\varphi(c)$.

$\Rightarrow \varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$

$\Rightarrow \varphi^*(a/b) = \varphi^*(c/d)$.

$\varphi^*\left(\frac{a}{1}\right) = \varphi(a)\varphi(1)^{-1} = \varphi(a)$

$\varphi^*|_R = \varphi$.

(Uniqueness)

Let $g : F \longrightarrow K$ be a homo extending φ.

Then $g\left(\frac{a}{b}\right) = g(a \cdot b^{-1}) = g(a)\, g(b)^{-1}$

$= \varphi(a)\, \varphi(b)^{-1}$

$= \varphi^*\left(\frac{a}{b}\right)$.

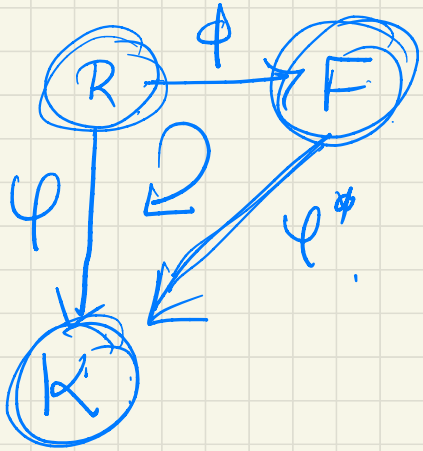
$\frac{a}{1} \cdot \frac{1}{b} = a \cdot b^{-1}$

$\therefore g = \varphi^*$.

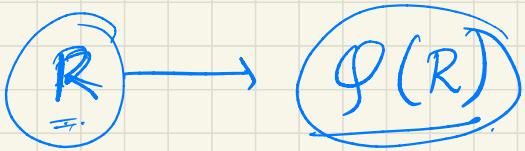
Since g is an extension of φ

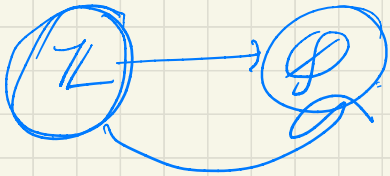
i.e $g|_R = \varphi$

i.e $g(a) = \varphi(a) \quad \forall a \in R$.



$\varphi(n) = \frac{n}{1}$





Q If R is not integral domain then can we still construct some field s.t non-zero elts of R can be inverted?

Yes we can invert and it is called ring of fraction

[we will study in Commutative alg]

Question. Let R be any ring and I be an ideal of R. When R/I is an integral domain?

R/I will be an integral domain if $\bar{a}, \bar{b} \neq \bar{0}$ in R/I s.t $\bar{a}\bar{b} \neq \bar{0}$ i.e $a \notin I, b \notin I$ then $ab \notin I$. (notation $\bar{a} = a + I$).

Equivalently if $ab \in I$ then either $a \in I$ or $b \in I$.

Defn An ideal $I \subsetneq R$ is called a prime ideal if $ab \in I$ then either $a \in I$ or $b \in I$.

Propn Let R be a ring. Then the ideal P is a prime ideal of R iff R/P is an integral domain.

Example (1) Consider the ring $\mathbb{Z}$.

(p) is a prime ideal if p is a prime no.

Let $ab \in (p) \Rightarrow ab = pk$ for some $k \in \mathbb{Z}$. $\Rightarrow p \mid ab$.

Since p is a prime no. this either $p \mid a$ or $p \mid b$

$\Rightarrow a \in (p)$ or $b \in (p)$.

$\therefore (p)$ is a prime ideal when p is a prime number.

In $\mathbb{Z}$, (6) is not a prime ideal as $\mathbb{Z}/6\mathbb{Z}$ is not an int domain.

$2.3 \in (6)$ but $2 \notin (6)$, $3 \notin (6)$.

(2) Consider the (2) in $\mathbb{Z}[i]$.

Is (2) a prime ideal in $\mathbb{Z}[i]$

$$2 = (1+i)(1-i) \in (2).$$

But $(1+i) \notin (2)$ and $(1-i) \notin (2)$.

Suppose $(1+i) \in (2)$.

$$\Rightarrow (1+i) = 2 \cdot (a+ib) = 2a + i2b$$

$$\Rightarrow 2a = 1 \Rightarrow a = 1/2 \quad *$$

Thus $(1+i) \notin (2)$.

(3). Consider the poly ring $k[x]$ where k is a field.

Q When $(f(x))$ is a prime ideal in $k[x]$ where $f(x) \in k[x]$.

$f(x) = (x^2 - 1)$.

Is $(f(x))$ a prime ideal?

$(x^2-1) = (x+1)(x-1) \in ((x^2-1))$

But $(x-1) \notin ((x^2-1))$. & $(x-1) \notin ((x^2-1))$

Thus $((x^2-1))$ is not a prime ideal.

Defn. A poly $f(x) \in k[x]$ is said to be irreducible over k if it is non-constant and can not be factored into the product of two or more non-constant polys with coeffs in k.

$(f(x))$ is a prime ideal in $k[x]$ iff $f(x)$ is an irreducible poly.

Pf: $gh \in (f(x))$.

$\Rightarrow gh = f \cdot k$.

$\Rightarrow f \mid gh$.

If f is irreducible then either

$f \mid g$ or $f \mid h$.

$\Rightarrow$ either $g \in (f(x))$ or $h \in (f(x))$

Thus $(f(x))$ is a prime ideal.

Converse is Ex :)

Remark: A ring R is an int domain iff (0) is a prime ideal.

We observed that if I be a prime ideal then R/I is an int domain.

Q When R/I will be a field?

Defn. An ideal M of a ring R is called a maximal ideal if whenever $M \subset I \subset R$ then either $I = M$ or $I = R$ i.e M is not contained in any ideal other than M

In $\mathbb{Z}$,

$(6) \subseteq (2)$ ✓

$(6) \subseteq (3)$ ✓

(6) is not a maximal ideal.

(p) is a maximal ideal when p is prime no.

Ex 1 Show that every ideal of $\mathbb{Z}$ is of the form (n) where $n \in \mathbb{Z}$.

Prop. Maximal ideal exists in a non-zero ring.

Zorn's lemma: Let S be a partially ordered set. If every totally ordered subset of S has an upper bound then S contains a maximal elt.

Pf: Consider the set $S = \{I \mid I \text{ is a proper ideal of } R\}$. $I \neq R$.

Under inclusion S is a partially ordered set. Let T be a totally ordered subset of S.

Let $U = \bigcup \{ I \mid I \in T \}$.

Then U is an ideal of R.

and U is proper ideal. ie U is an upper bound of T.

By Zorn's lemma S has a maximal elt. ie maximal ideal exists in R.