Lec 11/6

Tuesday, November 6, 2018 11:31

R : principal ideal domain – integral domain (no zero divisors), every ideal is generated by one element.

hypothesis: R is a domain

Lemma: $(a) = (b)$ iff $a = ub$ for some $u \in R^\times$

Pf $(a) \subset (b)$ means $a \in (b)$ i.e. $a = xb$

$(b) \subset (a)$ . . . . $b = ya$

So $a = xb = xya$ so $(1-xy)a = 0 \Rightarrow xy = 1$ if $a \neq 0$.

Lemma: R : PID, $P \subsetneq R$ prime ideal ($P \neq (0)$). Then P is maximal.

Pf If $P \subsetneq \underbrace{M \subset R}_{\text{ideal}}$ then $M = R$ (to show).

$P = (p)$, $M = (m)$ for some $p \in P$, $m \in M$.

$P \subset M \Rightarrow p = xm$ for some $x \in R$. $P \neq M$ means $m \notin P$,

So $x \in P$ since P is prime. thus $x = yp$.

$p = ypm$ so $(1 - ym) = 0 \Rightarrow ym = 1$ so $m \in R^\times$ meaning $(m) = R$.

A general statement

If R is a commutative ring and

$M \subsetneq R$ is a maximal ideal then $M^n \subsetneq R$ is primary $\forall n \geq 1$.

Reason: in R/M^n every element is a unit or nilpotent.

$x = a_0 + M$. Zero div in R/M^n = nilpotent in R/M^n

i.e. M^n is primary.

In P.I.D's non-zero primary = power of nonzero prime ideal $\rightarrow$ max'l

Prop: R : P.I.D. $Q \subsetneq R$ non-zero primary ideal

$\text{Rad}(Q) = P = (p)$, then $\exists n \geq 1$ s.t. $Q = (p^n)$

Proof: $P = (p)$, $Q = (q)$, $P = \underbrace{\text{Rad}(Q)}^{\{a : a^\ell \in Q \text{ for some } \ell \geq 1\}} \supset Q$

Choose smallest n s.t. $p^n \in Q$ $\left(p^{n-1} \notin Q. \right)$

i.e. $p^n = xq$ and $q = yp \Rightarrow p^n = xyp \Rightarrow p^{n-1}(1-xy)p = 0$

but $p \neq 0$ so $p^{n-1} = xy$. by minimality of n.

$x \notin (p)$. $xy \in \overbrace{(p^{n-1})}^{\text{Primary}}$, $x \notin \text{Rad}((p^{n-1}))$ i.e. $x^k \notin (p^{n-1})$ for any k,

So $y \in (p^{n-1})$. So $q = yp \in (p^n)$.

So $Q \subset (p^n)$, and $(p^n) \subset Q$ by defn of n.

Recall $\text{Rad}(p^n) = P$ for a prime ideal P.

in P.I.D. then $(p)\cdot(q) = (pq)$

Noether's Primary Decomposition Theorem (for P.I.D.'s)

Recall: R : Noetherian & $I \subsetneq R$ ideal $\Longrightarrow I = Q_1 \cap \cdots \cap Q_\ell$

where Q_i are all primary, $\text{Rad}(Q_i) = P_i$ are all distinct

$\text{Min}(I) \subset \{P_i : 1 \leq i \leq \ell\}$ and $\text{Min}(I)$ is uniquely determined by I.

In P.I.D.: $I = (n)$. $Q_i = (p_i^{k_i})$, P_i are all nonzero primes $\Rightarrow$ maximal

So no embedded primes ($\text{Min}(I) = \{P_1, \ldots, P_\ell\}$ is uniquely determined).

$\longrightarrow$ if $P_i \notin \text{Min}(I)$ then $\exists P_j \in \text{Min}(I)$ s.t. $P_j \subset P_i$.

but this contradicts "all primes are maximal".

i.e. (p_i) are uniquely determined.

and Q_i is uniquely determined if P_i is minimal

So all Q_i are uniquely determined.

$$(n) = (p_1^{k_1}) \cap \cdots \cap (p_\ell^{k_\ell})$$

$$= (p_1^{k_1} \cdots p_\ell^{k_\ell})$$

Chinese remainder thm:

$\underset{\text{max'l}}{M_1 \neq M_2} \Rightarrow M_1 + M_2 = R$

I, J coprime $\Rightarrow I^k, J^\ell$ are coprime

If coprime: $I \cap J = I \cdot J$

$I + J = R$

$x + y = 1$

$(x+y)^\ell = 1^\ell = 1$

$\underbrace{x^\ell + \binom{\ell}{1} x^{\ell-1} y + \cdots + \binom{\ell}{1} x y^{\ell-1}}_{\in I} + \underbrace{y^\ell}_{\in J^\ell}$

P.I.D.

$\forall n \in R \setminus \{0\}$

So $n = u\, p_1^{k_1} \cdots p_\ell^{k_\ell}$

where (1) u is a unit

(2) $(p_1), \ldots, (p_\ell)$ are distinct non-zero prime ideals in R

(3) $(p_1), \ldots, (p_\ell)$ are uniquely determined by n
$k_1, \ldots, k_\ell$

Our examples of PID's:

$\mathbb{Z}$ $\qquad N(n) = |n|$

$K[x]$ $\qquad N(f(x)) = \deg(f(x))$

$\mathbb{Z}[\sqrt{-1}]$ $\qquad N(a+bi) = a^2 + b^2$

in each case we had a function

$N : R \longrightarrow \mathbb{Z}_{\geq 0}$ s.t. $\forall a, b \in R,\ b \neq 0,\ \exists q, r \in R$

$\cdot \ \mathbb{Z}_{\geq 0}$ s.t. $\forall\, a, b \in R$, $b \neq 0$, $\exists\, q, r \in R$

so that $a = qb + r$ where either $r = 0$ or $N(r) < N(b)$

<u>Defn</u>: A domain R is called euclidean if this function exists.

<u>Easy Lemma</u>: Every euclidean domain is a P.I.D.

<u>Pf</u>: $\overset{R}{\underset{\cup}{}} I \neq (0)$. choose $b \in I \setminus \{0\}$ of smallest $N(b)$.

Prove $I = (b)$.

Reading for tomorrow:

§7.1 example 229