Lecture 46

(46.0) Recall from the last lecture - for a commutative ring R :

- $\boxed{Q \underset{+}{\subsetneq} R}$ ideal is primary, if $ab \in Q$, $a \notin Q \Rightarrow \exists\, n \geq 1$ s.t. $b^n \in Q$

- $\boxed{I \subseteq R}$ ideal $\rightsquigarrow$ $\mathrm{Rad}(I) := \{ x \in R \mid \exists\, n \geq 1$ such that $x^n \in I \}$

$$I \subseteq \mathrm{Rad}(I) \subseteq R$$

(also an ideal)

We proved in last lecture :

(1) (page 2 of Lecture 45): Q : primary $\Rightarrow \mathrm{Rad}(Q)$: prime.

(2) (page 3 of Lecture 45):

$P \underset{+}{\subsetneq} R$ (prime ideal) $\Rightarrow$ ~~$\mathrm{Rad}(P^n)$~~ $\mathrm{Rad}(P^n) = P$ $\forall\, n \geq 1$

(3) $I \subsetneq P \Rightarrow \mathrm{Rad}(I) \subsetneq P$

(where $I \underset{+}{\subsetneq} R$ is an ideal)

(46.1) Now, if R is <u>Noetherian</u> and $M \underset{+}{\subsetneq} R$ is <u>maximal</u> (remember : maximal $\Rightarrow$ prime.) we can prove that M^n is primary for every $n \geq 1$.

Recall that this statement would be false if the hypothesis of being maximal is changed to being prime.
(see Ex. 7 of HW ~~8~~ – optional one).

In fact we can prove the following stronger statement:

Lemma: Let R be a commutative Noetherian ring; $M \subsetneq R$ a maximal ideal; and $I \subsetneq R$ a proper ideal. Then the following assertions are equivalent:

(a) $\exists\ n \geq 1$ s.t. $M^n \subset I$.

(b) I is primary and $\mathrm{Rad}(I) = M$.

(c) $\mathrm{Rad}(I) = M$

Proof: (a) $\Rightarrow$ (b): assume $M^n \subset I$. Then

$\mathrm{Rad}(M^n) \subset \mathrm{Rad}(I)$ (see defn. of radical – this is clear.)

M (equality)

Since M is maximal $M \subset \mathrm{Rad}(I) \subset R \Rightarrow$

$M = \mathrm{Rad}(I)$ or $\mathrm{Rad}(I) = R$;

In this case, $1 \in R = \mathrm{Rad}(I)$

$\Rightarrow 1^\ell \in I$ for some $\ell \geq 1$

$\Rightarrow 1 \in I \Rightarrow I = R$

Contradicts proper containment $I \subsetneq R$.

Thus (a) $\Rightarrow$ (c).

(b) $\Leftrightarrow$ (c) : We need to prove that $\mathrm{Rad}(I) = M$:

a maximal ideal implies I is primary.

So, let $ab \in I$ and assume $a \notin I$.

- If $b \in M$ then $(M = \mathrm{Rad}(I))$ $b^l \in I$ for some $l \geq 1$.
- If $b \notin M$ (we should get a contradiction !)

then $xb + m = 1$ for some $x \in R$, $m \in M$ (since $(M, b) = R$.)

i.e. $abx + am = a$

So in R/I : $am = a - x(ab)$

$\equiv a \pmod{I}$ as $ab \in I$.

i.e. $a(1-m) = 0 \pmod{I}$

$(1-m)$ is a unit in R/I because $m \in M \Rightarrow m^r \in I$ for some $r \geq 1$ i.e. m is a nilpotent mod I.

$\Rightarrow a = 0 \pmod{I}$

i.e. $a \in I$.

contradiction!

(c) $\Rightarrow$ (a) : $M = \mathrm{Rad}(I)$

R : Noetherian, i.e. $M = (a_1, \ldots, a_k)$ for some $a_1, \ldots, a_k \in M$.

$\Rightarrow a_1^{n_1}, \ldots, a_k^{n_k} \in I$ for some $n_1, \ldots, n_k \geq 1$.

Take $N > n_1 + \dots + n_k$. Then for any

$$x = r_1 a_1 + \dots + r_k a_k \in M \quad , \text{ we have :}$$

$x^N \in R$ - linear combination of terms

$$a_1^{j_1} \dots a_k^{j_k} \quad \text{s.t.} \quad j_1 + \dots + j_k = N.$$

$\Rightarrow$ for some j_t, $j_t > n_t$ $\Rightarrow$ this term is in I

$\Rightarrow$ $x^N \in I$. Hence $M^N \subset I$. □

(46.2) Now we specialize to the case when R is a principal ideal domain. (see Lecture 36).

Lemma. R : PID and $P \subsetneq R$ non-zero prime ideal.

Then P is maximal.

Proof. $P = (a)$; $a \neq 0$.

Assume $P \subset I = (b) \underset{\text{(ideal)}}{\subset} R$. We need to show that either $P = I$ or $I = R$.

Since $a \in (b)$ we can write $a = b \cdot c$ for some $c \in R$.

- If $b \in P$, then $I = P$.
- If $b \notin P$, then, as P is prime, $c \in P \Rightarrow c = a \cdot x$ for some $x \in R$

Combining: $a = b \cdot c = b \cdot a \cdot x$

$\Rightarrow a(1-bx) = 0$

$\Rightarrow \quad 1-bx = 0 \quad \Rightarrow \quad b \in R^{\times} \Rightarrow I = (b) = R.$

(R is a domain & $a \neq 0$) $\square$

(46.3) Consequences of Primary Decomposition Theorem

(Thms 45.3 (page 6) and 45.5 (page 10)) and Lemma (46.2).

R = a principal ideal domain. (hence every ideal is finitely generated – i.e. R is Noetherian.).

- Let $I \subsetneq R$ be a proper (non-zero) ideal. From the results of the last lecture –

There exist primary ideals $Q_1, \dots, Q_\ell$ s.t

(1) $I = Q_1 \cap \dots \cap Q_\ell$

(2) $\{P_i = \mathrm{Rad}(Q_i)\}_{1 \le i \le \ell}$ are distinct, non-zero, prime ideals.

(3) $Q_i \not\supseteq \bigcap_{\substack{1 \le j \le \ell \\ j \neq i}} Q_j$ ← true for every $i = 1, \dots, \ell$.

(4) $\mathrm{Min}(I) = \{P_1, \ldots, P_k\}$ - see page 9 of Lecture 45.

and $Q_1, \ldots, Q_k$ are uniquely determined by I.

Now - using Lemma 46.2 - each $P_1, \ldots, P_\ell$ is maximal.

Thus: $k = \ell$. In other words $\boxed{\mathrm{Min}(I) = \mathrm{Assoc}(I)}$.
(see page 10 of Lecture 45).

[Proof: if $P \subsetneq R$ is a prime ideal containing I, then $P_j \subset P$ for some $j \in \{1, \ldots, k\}$ as these are the minimal primes containing I.

P_j is also maximal ideal now, so, $P_j = P$.
(or $P = R$ - but we assumed that such is not the case).]

(46.3) Lemma: R: PID; $Q \subsetneq R$ (non-zero) primary ideal; $M = \mathrm{Rad}(Q) \subsetneq R$ (M maximal by Lemma 46.2). Then $Q = M^n$ for some $n \geq 1$.

Proof: We already know $Q = (q) \subset M = (p)$.

as $p^\ell \in Q$ for some $\ell \geq 1$, we get -

- assuming n is smallest ≥ 1 number so that $p^{n-1} \notin Q$ & $p^n \in Q$ -

$q = x \cdot p$ for some $x \in R$.

$p^n \in Q$ i.e. $p^n = y \cdot q$ for some $y \in R$. & $y \notin (p)$.

(as n is smallest! - check!!)

$\Rightarrow p^n = xyp \Rightarrow p(xy - p^{n-1}) = 0$

$\Rightarrow xy = p^{n-1}$; as $p \neq 0$ & R is a domain.

Thus $\left[\begin{array}{l} M^{n-1} = (p^{n-1}) \text{ is primary} \\ y \notin (p) \end{array}\right]$ $x \in (p^{n-1})$. (say $x = r \cdot p^{n-1}$).

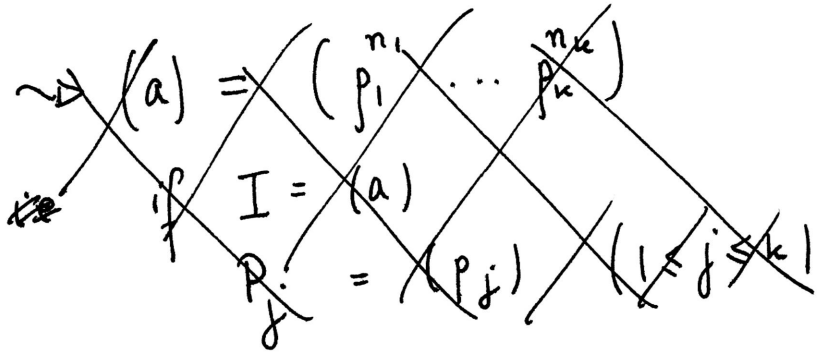
This implies $q = r \cdot p^{n-1} \cdot p \in (p^n)$. □

(46.4) Combining the above lemma with the findings of Section 46.2 above: (same notation as in 46-2).

$$I = P_1^{n_1} \cap \cdots \cap P_k^{n_k}$$

($P_1, \ldots, P_k \subsetneq R$ distinct non-zero (max'l) ← prime ideals)

$n_1, \ldots, n_k \geq 1$ uniquely determined by I.



Distinct Max'l ideals are coprime.

J_1, J_2 coprime $\Rightarrow J_1^{n_1}, J_2^{n_2}$ are coprime.

$J_1 \cap J_2 = J_1 \cdot J_2$ for coprime ideals

$\Rightarrow \quad I = P_1^{n_1} \cdots P_k^{n_k}$ i.e. $(a) = (p_1^{n_1} \cdots p_k^{n_k})$

where $I = (a)$ & $P_j = (p_j) \quad \forall \ 1 \leq j \leq k.$

$\Rightarrow \quad a = u \cdot p_1^{n_1} \cdots p_k^{n_k}$ for some $u \in R^\times$.

(remember : A : integral domain and $(a) = (b)$

$\Rightarrow a = ub$ for some $u \in A^\times$ - invertible elt)

Thus we have proved :

P.I.D. $\Longrightarrow$ unique factorization domain

(defined in next lecture !)