Lecture 26: Primary Decomposition (III)

Last Time: a Primary Decomp $\rightsquigarrow$ a Reduced One: $\boxed{\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_\ell}$

(1) $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ are all distinct.

(2) $\mathfrak{q}_i \not\supseteq \bigcap_{\substack{1 \leq j \leq \ell \\ j \neq i}} \mathfrak{q}_j$ for all $i = 1, \ldots, \ell$. (ie, no $\mathfrak{q}_i$ is redundant)

Example $\mathfrak{a} = (x^2, xy) = (x) \cap (x,y)^2 = (x) \cap (x^2, y)$ reduced, not unique!

$\mathfrak{p}_1 = (x)$, $\mathfrak{p}_2 = (x,y)$

TODAY: 1 Discussed uniqueness features of reduced primary decomp

2 Special case: R is a PID

Theorem 1: The set of prime ideals $\{\mathfrak{p}_1, \ldots \mathfrak{p}_\ell\}$ of a reduced primary decomposition of $\mathfrak{a}$ is uniquely determined by $\mathfrak{a}$. More precisely:

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell\} = \{ r((\mathfrak{a} : x)) : x \in R \ \& \ r((\mathfrak{a}:x)) \text{ is prime}\}$$

this does NOT require a primary decomp.

(so (LHS) is indep of our choice of red. primary decomp)

Lemma: Let $\mathfrak{q} \subsetneq R$ be primary & $\mathfrak{p} := r(\mathfrak{q})$. Given $x \in R$, we have:

(1) $x \in \mathfrak{q} \Rightarrow (\mathfrak{q} : x) = R$

(2) $x \notin \mathfrak{q} \Rightarrow (\mathfrak{q} : x)$ is primary & $r(\mathfrak{q} : x) = \mathfrak{p}$.

(3) $x \notin \mathfrak{p} \Rightarrow (\mathfrak{q} : x) = \mathfrak{q}$.

Recall: $(\mathfrak{a} : \mathfrak{b}) = \{ r \in R : r\mathfrak{b} \subseteq \mathfrak{a} \}$ for $\mathfrak{a}, \mathfrak{b}$ ideals.

Proof: (1) is clear.

For (3): if $y \in (\mathfrak{q} : x)$ & $x \notin \mathfrak{p}$, then $y \in \mathfrak{q}$ (otherwise,

$xy \in \mathfrak{q}$ & $y \notin \mathfrak{q} \Rightarrow x \in r(\mathfrak{q}) = \mathfrak{p}$)

So $\underset{\text{Always}}{\mathfrak{q} \subseteq} (\mathfrak{q} : x) \subseteq \mathfrak{q}$ gives $(\mathfrak{q} : x) = \mathfrak{q}$.

For (2): To show: $x \notin \mathfrak{q} \Rightarrow (\mathfrak{q}:x)$ is primary & $r(\mathfrak{q}:x) = \mathfrak{p}$

- Claim 1: $(\mathfrak{q}:x) \subset \mathfrak{p}$.

Pf/ Let $y \in (\mathfrak{q}:x)$ so $xy \in \mathfrak{q}$. Since $x \notin \mathfrak{q}$, then $y^n \in \mathfrak{q}$ for some $n>0$, ie, $y \in \mathfrak{p}$. So $\mathfrak{q} \subseteq (\mathfrak{q}:x) \subset \mathfrak{p}$.

- Taking radicals gives $\mathfrak{p} = r(\mathfrak{q}) \subseteq r((\mathfrak{q}:x)) \subseteq r(\mathfrak{p}) = \mathfrak{p}$

$\Rightarrow r((\mathfrak{q}:x)) = \mathfrak{p}$.

- Claim 2: $(\mathfrak{q}:x)$ is primary

Pf/ Pick $yz \in (\mathfrak{q}:x)$, ie $yzx \in \mathfrak{q}$. We'll use the contrapositive in the definition of primary ideal.

Assume $y^n \notin (\mathfrak{q}:x)$ $\forall n>0$. Then, $y \notin \mathfrak{p}$ & so $y^n \notin \mathfrak{q}$ $\forall n>0$).

Then, $xz \in \mathfrak{q}$ so $z \in (\mathfrak{q}:x)$. $\square$

Theorem: The set of prime ideals $\{\mathfrak{p}_1, \dots \mathfrak{p}_\ell\}$ in a reduced decomp of $\mathfrak{a}$ is $\{\mathfrak{p}_1, \dots, \mathfrak{p}_\ell\} = \{ r((\mathfrak{a} : x)) : x \in R \ \& \ r((\mathfrak{a}:x)) \text{ is prime}\}$

Proof: ($\subseteq$) We want to show each $\mathfrak{p}_i = r((\mathfrak{a} : x_i))$ for some $x_i \in R$.

Fix $i = 1, \dots, \ell$ & choose $x_i \in \left(\bigcap_{j \neq i} \mathfrak{q}_j\right) \setminus \mathfrak{q}_i$ (ok by reduced and (2))

Then $(\mathfrak{a} : x_i) = \bigcap_{1 \le j \le \ell} (\mathfrak{q}_j : x_i) \underset{\text{Lemma (1)}}{=} (\mathfrak{q}_i : x_i) \cap R = (\mathfrak{q}_i : x_i)$

$\Rightarrow r(\mathfrak{a} : x_i) = r(\mathfrak{q}_i : x_i) = \mathfrak{p}_i$ by Lemma (2).

($\supseteq$) Assume $r(\mathfrak{a} : x)$ is prime. Then:

$$(\mathfrak{a} : x) = \left(\bigcap_{i=1}^{\ell} \mathfrak{q}_i : x\right) = \bigcap_{i=1}^{\ell} (\mathfrak{q}_i : x) \underset{\text{Lemma (1)}}{=} \bigcap_{\substack{1 \le i \le \ell \\ x \notin \mathfrak{q}_i}} (\mathfrak{q}_i : x)$$

$$\Rightarrow r(\mathfrak{a} : x) = r\left(\bigcap_{\substack{1 \le i \le \ell \\ x \notin \mathfrak{q}_i}} (\mathfrak{q}_i : x)\right) = \bigcap_{\substack{1 \le i \le \ell \\ x \notin \mathfrak{q}_i}} \underbrace{r(\mathfrak{q}_i : x)}_{= \mathfrak{p}_i \text{ by Lemma (2)}}$$

So (1) $r(\mathfrak{a} : x) \subseteq \mathfrak{p}_i \ \forall i = 1, \dots, \ell$ with $x \notin \mathfrak{q}_i$ & (2) $\bigcap_{\substack{1 \le i \le \ell \\ x \notin \mathfrak{q}_i}} \mathfrak{p}_i \subseteq r(\mathfrak{a} : x)$ prime

Prime Avoidance $\Rightarrow$ $\boxed{\mathfrak{p}_i \subseteq r(\mathfrak{a} : x)} \overset{(1)}{\subseteq} \mathfrak{p}_i$ for some i. So equality holds.

Notation $\boxed{\mathrm{Assoc}(\mathfrak{a})} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell\}$ is the set of primes associated to $\mathfrak{a}$ (it doesn't depend on a prim decomp, but solely on $\mathfrak{a}$).

Corollary: If $\mathfrak{p} \subsetneq R$ prime ideal minimal among primes containing $\mathfrak{a}$, then $\mathfrak{p} \in \mathrm{Assoc}(\mathfrak{a})$. That is, $\boxed{\mathrm{Min}(\mathfrak{a}) \subseteq \mathrm{Ass}(\mathfrak{a})}$

- We relabel $\mathrm{Assoc}(\mathfrak{a})$ so that $\mathrm{Min}(\mathfrak{a}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ for some $k \leq \ell$
- Assuming $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_\ell$ is reduced primary decomp, where:

Theorem: $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$ are uniquely determined by $\mathfrak{a}$.

More explicitly, $\mathfrak{q}_i = j_i^{-1}(j_i(\mathfrak{a}) R_{\mathfrak{p}_i})$ for $i = 1, \ldots, k$,

where $j_i : R \longrightarrow R_{\mathfrak{p}_i}$.

Proof: Fix i & write $j = j_i : R \longrightarrow R_{\mathfrak{p}_i}$, $S = R \setminus \mathfrak{p}_i$.

Take $\mathfrak{b}$ = ideal in $R_{\mathfrak{p}_i}$ generated by $j(\mathfrak{a}) = \mathfrak{a} R_{\mathfrak{p}_i} = S^{-1}\mathfrak{a}$. **To show**: $\mathfrak{q}_i = j^{-1}(\mathfrak{b})$

Since $\mathfrak{a} = \bigcap_{k=1}^{\ell} q_k$, we get $\boxed{S^{-1}\mathfrak{a} = \bigcap_{1\le k\le \ell} S^{-1}(q_k)}$ (*)

<u>Claim 1</u>: $S^{-1}q_k = S^{-1}R$ if $k \neq i$. $\quad (\Rightarrow S^{-1}\mathfrak{a} = S^{-1}q_i)$

Pf/ It suffices to show $S \cap q_k = \emptyset$. By contradiction, assume $q_k \subseteq R \setminus S = \wp_i$

Then $\wp_k = r(q_k) \subseteq r(\wp_i) = \wp_i$. So $\mathfrak{a} \subseteq q_k \subseteq \wp_k \subseteq \underset{\text{Min}(\wp_i)}{\wp_i} \Rightarrow \wp_k = \wp_i$.

This cannot happen (as prim dec. is reduced!) $\square$

<u>Claim 2</u>: $j^{-1}(S^{-1}q_i) = q_i$ $\quad$ (This implies $j^{-1}(t) = q_i$)

Pf/ Clearly $q_i \subseteq j^{-1}(S^{-1}q_i)$. <u>Note</u>: $q_i \subseteq r(q_i) = \wp_i$ so $q_i \cap S = \emptyset$.

Conversely, if $x \in j^{-1}(S^{-1}q_i)$ then $x = \frac{x}{1} \in S^{-1}q_i$, so $\frac{x}{1} = \frac{a}{s}$ for

some $s \in S$ & $a \in q_i$. Thus, $\exists\, s' \in S$ with $s'(xs - a) = 0$ in R

$\Rightarrow (s's)x = s'a \in q_i$ $\quad$ But q_i is primary so either $x \in q_i$ or

$s's \in r(q_i) = \wp_i$ (Contr. to $S \cap \wp_i = \emptyset$). <u>Conclude</u> $x \in q_i$ $\square$

Primary decomposition for PID's

Def: A commutative ring R is a principal ideal domain (PID) if it is a domain and every ideal of R can be generated by 1 element.

Observation: PID $\Rightarrow$ Noetherian. so we have primary decomp. for PID's

Ex: ① $\mathbb{Z}$, $(I \subseteq \mathbb{Z}$ & $I \neq (0) \Rightarrow I = (\min \mathbb{Z}_{>0} \cap I))$

② $\mathbb{K}[x]$ $(I \subseteq \mathbb{K}[x]$ & $I \neq (0) \Rightarrow I = (f)$, where $0 \neq f \in I$ has minimal degree.)

Q: What do primary decompositions look like for PIDs?

Lemma: Fix R = PID & $\mathfrak{P} \subsetneq R$ nonzero prime ideal. Then, $\mathfrak{P}$ is maximal

Pf/ $\mathfrak{P} = (a)$, $a \neq 0$. Assume $\mathfrak{P} = (a) \subsetneq I = (b) \subseteq R$

- Since $a \in (b)$ we write $a = bc$ for $c \in R$. If $I \neq \mathfrak{P}$ then $b \notin \mathfrak{P}$

$\underset{\mathfrak{P}\text{ prime}}{\Longrightarrow}$ $c \in \mathfrak{P}$ so $c = ax$ for some $x \in R$. Thus $a = bxa$, ie $a(bx-1) = 0$

R domain & $a \neq 0$ $\Rightarrow$ $bx = 1$ so $I = (b) = R$. $\square$

Corollary: (HW9) All nonzero primary ideals in PID have maximal radicals

Theorem (Prim Decomp for PIDs)

Given $(0) \neq \mathfrak{a} \subsetneq R$ ideal in a PID, there exist primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$ s.t.

(1) $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_\ell$

(2) $\{ \mathfrak{p}_i = r(\mathfrak{q}_i) \}_{1 \le i \le \ell}$ are distinct non-zero prime ideals

(3) $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$

Furthermore $\operatorname{Min}(\mathfrak{a}) = \operatorname{Ass}(\mathfrak{a})$, so we get uniqueness of all $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$.

Q: What more can we say about primary ideals?

Lemma: If R is a PID & $(0) \neq \mathfrak{q}$ is primary, then $\mathfrak{q} = \mathfrak{m}^n$ for some $n > 0$ where $\mathfrak{m} = r(\mathfrak{q})$ is a maximal ideal.

Pf/ We know $\mathfrak{m} = r(\mathfrak{q})$ is maximal by the previous lemma.

Write: $\mathfrak{q} = (q)$ & $\mathfrak{m} = (p)$. Pick $n \geq 1$ minimal st $p^n \in \mathfrak{q}$.

$\rightsquigarrow \mathfrak{q} \supseteq (p^n)$. Want to show: $q \in (p^n)$.

Write $q = px$ for $x \in R$. & $p^n = qy$ for $y \in R \setminus \mathfrak{m}$

So $p^n = pxy$ gives $\underset{\neq 0}{p}(p^{n-1} - xy) = 0$, so $xy = p^{n-1}$.

But $\mathfrak{m}^{n-1}$ is primary ideal (radical is maximal!)

$\left.\begin{array}{l} xy \in \mathfrak{m}^{n-1} = (p^{n-1}) \\ y \notin \mathfrak{m} = r(\mathfrak{m}^{n-1}) \end{array}\right\} \Longrightarrow x \in \mathfrak{m}^{n-1} = (p^{n-1})$, say $x = p^{n-1}z$

Thus, $q = px = p^n z$ gives $q \in (p^n) \subseteq q \Rightarrow q = (p^n) = \mathfrak{m}^n$ $\square$

Corollary: $(0) \neq \mathfrak{a} = \mathfrak{p}_1^{n_1} \cap \cdots \cap \mathfrak{p}_\ell^{n_\ell} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_\ell^{n_\ell}$. (because $\mathfrak{p}_i$ max'l)

So if $\mathfrak{a} = (x)$, we can find $p_1, \ldots, p_\ell$ ($\mathfrak{p}_i = (p_i)$) and $u \in R^\times$

with $x = u p_1^{n_1} \cdots p_\ell^{n_\ell}$ ("unique factorization") Here $x \neq 0, \pm 1$.

Corollary 2: PID $\Longrightarrow$ UFD (unique factorization domain)

Example: In $\mathbb{Z}$: $m = \pm p_1^{n_1} \cdots p_\ell^{n_\ell}$, p_i distinct primes $\rightsquigarrow (m) = (p_1)^{n_1} \cap \cdots \cap (p_\ell)^{n_\ell}$ primary decomposition

$m \neq 0, \pm 1$