Lecture 26: Primary Decomposition III

Last Time: Analyzed uniqueness features of reduced prim decomp.

Primary decomp $\rightsquigarrow$ Reduced Primary Decomposition

$$\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_r$$

(1) $\mathfrak{p}_i = r(\mathfrak{q}_i)$ are all distinct

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

§1 Uniqueness properties of reduced primary decompositions

Fix $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_\ell$ reduced prim decomp & $\mathfrak{p}_i = r(\mathfrak{q}_i)$ $\forall i$.

Theorem. The set of prime ideals $\{\mathfrak{p}_1, \dots, \mathfrak{p}_\ell\}$ of a reduced prim decomp of $\mathfrak{a}$ is uniquely determined by $\mathfrak{a}$. More precisely:

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

this does NOT require a primary decomp.
(so (LHS) is indep of our choice of red. primary decomp)

To prove this statement, we need one technical lemma (Lecture 25)

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

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

$(\mathfrak{a} : x) = (\mathfrak{a} : (x))$.

Proof of Theorem: ($\subseteq$) We want to show each $\mathfrak{p}_i$ is of the form $r((\mathfrak{a}:x_i))$ for some $x_i \in R$. Fix $i=1,\dots,\ell$ & choose $x_i \in (\bigcap_{j\neq i} \mathfrak{q}_j) \setminus \mathfrak{q}_i$ (this exists by def of reduced prim dec)

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 $\cdot\ r(\mathfrak{a}:x) \subseteq \mathfrak{p}_i \ \forall i=1,\dots,\ell$ with $x\notin \mathfrak{q}_i$

$\cdot \bigcap_{\substack{1\le i\le \ell \\ x\notin \mathfrak{q}_i}} \mathfrak{p}_i \subseteq \underset{\text{prime}}{r(\mathfrak{a}:x)}$. So by prime avoidance

Thm 2 (Lecture 17) $\exists\ i=1,\dots,\ell$ with $x\notin \mathfrak{q}_i$ st $\mathfrak{p}_i \subseteq r(\mathfrak{a}:x)$

Conclude: $r(\mathfrak{a}:x) = \mathfrak{p}_i$. $\square$

Notation $\boxed{\mathrm{Assoc}(\mathfrak{a})} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_\ell\}$ 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, $\mathrm{Min}(\mathfrak{a}) \subseteq \mathrm{Ass}(\mathfrak{a})$

We relabel $\mathrm{Ass}(\mathfrak{a})$ so that $\mathrm{Min}(\mathfrak{a}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ for some $k \leq l$.

Assuming $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_l$ is reduced primary decomp, where

<u>Theorem</u>: $\{\mathfrak{q}_1, \dots, \mathfrak{q}_k\}$ are uniquely determined by $\mathfrak{a}$.

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

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

<u>Proof</u>: We keep $i \in \{1, \dots, k\}$ fixed & write $j = j_i : R \longrightarrow R_{\mathfrak{p}_i} = S^{-1}R$ where $S = R \setminus \mathfrak{p}_i$)

Take $\mathfrak{b}$ = ideal in $R_{\mathfrak{p}_i}$ generated by $j(\mathfrak{a})$

$= S^{-1}\mathfrak{a} = j(\mathfrak{a}) S^{-1}R$.

• <u>To show</u>: $j^{-1}(\mathfrak{b}) = \mathfrak{q}_i$.

Since $\mathfrak{a} = \bigcap_{k=1}^{l} \mathfrak{q}_k$, we get $\boxed{S^{-1}\mathfrak{a} = \bigcap_{k=1}^{l} S^{-1}(\mathfrak{q}_k)}$ (*)

<u>Claim 1</u>: $S^{-1}\mathfrak{q}_k = S^{-1}R$ if $k \neq i$.

Pf/ It suffices to show $S \cap \mathfrak{q}_k \neq \emptyset$. Assume this is not the case, ie $\mathfrak{q}_k \subseteq R \setminus S = \mathfrak{p}_i$. Then $\underbrace{r(\mathfrak{q}_k)}_{= \mathfrak{p}_k} \subseteq r(\mathfrak{p}_i) = \mathfrak{p}_i$

so $\mathfrak{a} \subseteq \mathfrak{q}_k \subseteq \mathfrak{p}_k \subseteq \mathfrak{p}_i$ & $\mathfrak{p}_i \in \mathrm{Min}(\mathfrak{a})$, so $\mathfrak{p}_k = \mathfrak{p}_i$.
Contradicting the reducedness assumption on the prim dec. □

Combining (*) with Claim 1 yields $S^{-1}\mathfrak{a} = S^{-1}\mathfrak{q}_i$.

<u>Claim 2</u>: $j^{-1}(S^{-1}\mathfrak{q}_i) = \mathfrak{q}_i$ (This implies $j^{-1}(\mathfrak{b}) = \mathfrak{q}_i$)

Pf/ Clearly $q_i \subseteq j^{-1}(S^{-1}q_i)$

Note $q_i \subseteq r(q_i) = \wp_i$ 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 $a \in q_i$, $s \in S$ ie $\exists\, s' \in S$ with

$s'(xs - a) = 0$ in R

$(s's)x = s'a \in q_i$

Since q_i is primary, either $x \in q_i$ or $(s's) \in r(q_i) = \wp_i$

But $S \cap \wp_i = \emptyset$ & $s, s' \in S$ so $ss' \in S$.

We conclude $x \in q_i$. $\square$

§2 Primary Decomposition for PIDs:

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)

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 & $\wp \subsetneq R$ nonzero prime ideal. Then $\wp$ is maximal.

Pf/ $\wp = (a)$ $a \neq 0$

Assume $\mathfrak{p} = (a) \subsetneq I = (b) \subseteq R$. We need to show either $I = \mathfrak{p}$ or $I = R$.

- Since $a \in (b)$ we can write $a = bc$ for $c \in R$. If $I \neq \mathfrak{p}$ then $b \notin \mathfrak{p}$. So the prime condition gives $c \in \mathfrak{p}$. so $c = ax$.

  Then $a = bxa$, ie $a(bx-1) = 0$

  Since $a \neq 0$ & R is a domain, we conclude $bx - 1 = 0$, so $I = R$ $\square$

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 $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ s.t.

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

(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 $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$.

Q: What more can we say about primary ideals?

Lemma: If R is a PID & $\mathfrak{q} \neq (0)$ 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: $\mathfrak{q} = (q)$ & $\mathfrak{m} = (p)$ with $p^n \in \mathfrak{q}$ for some ≥ 1.

Pick smallest n with this property, so $p^n \in \mathfrak{q}$ & $p^{n-1} \notin \mathfrak{q}$.

Write $q = px$ for $x \in R$.

$p^n = qy$ for $y \in R \setminus \mathfrak{m}$

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

But $\mathfrak{m}^{n-1}$ is primary ideal

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

say $x = p^{n-1} z$

Thus, $q = px = p^n xz$ gives $q \in (p^n)$

So $\mathfrak{q} \subseteq (p^n) \subseteq \mathfrak{q}$ gives $\mathfrak{q} = (p^n) = \mathfrak{m}^n$. $\square$

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

$\uparrow$ $\mathfrak{p}_1, \dots \mathfrak{p}_\ell$ max

So if $\mathfrak{a} = (x) \neq (0)$, we can find $p_1, \dots, p_\ell$ ($\mathfrak{p}_i = (p_i)$)

and $u \in R^\times$ with $x = u p_1^{n_1} \cdots p_\ell^{n_\ell}$ ("unique factorization")

(Recall in an integral domain $(a) = (b) \Longleftrightarrow a = ub$ $u \in R^\times$)

Example: In $\mathbb{Z}$: $m = \pm p_1^{n_1} \cdots p_\ell^{n_\ell}$ p_i distinct primes $m \neq 0, \pm 1$

$(m) = (p_1)^{n_1} \cap \cdots \cap (p_\ell)^{n_\ell}$ primary decomposition.

Consequence: PID $\Longrightarrow$ UFD (unique factorization domain)