Lecture 29: PIDs, Primary Decompositions for PIDs

Last Time: Reduced Primary Decompositions for ideals of Noetherian rings (commutative)

Definition: A primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_\ell$ is reduced if

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

& (2) $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ are all distinct

Def: $\boxed{\mathrm{Ass}(\mathfrak{a})} = \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_\ell}\}$ = Associated primes of $\mathfrak{a}$

Key results:
- $\mathrm{Ass}(\mathfrak{a})$ doesn't depend on the choice of reduced primary decomp (we didn't give a proof of this!)
- Any $\mathfrak{p}$ prime containing $\mathfrak{a}$ where $\mathfrak{p}/\mathfrak{a}$ is a minimal prime of $R/\mathfrak{a}$ must feature in $\mathrm{Ass}(\mathfrak{a})$. Call them $\mathrm{Min}(\mathfrak{a})$
- Uniqueness of $\mathfrak{q}_i$ only applies to $\mathfrak{q}_i$'s with $r(\mathfrak{q}_i) \in \mathrm{Min}(\mathfrak{a})$
  ($\mathfrak{q}_i = j_i^{-1}(j_i(\mathfrak{a}))$ $\quad j_i : R \longrightarrow R_{\mathfrak{p}_i}$ $\quad \mathfrak{p}_i = r(\mathfrak{q}_i)$)

§1. Primary Decompositions for PIDs:

Recall A commutative ring R is a principal ideal domain (PID) if it is a domain and every ideal of R is of the form (a) for $a \in R$.

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

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

- ① & ② are Euclidean domains & all Euclidian Domains are PIDs.

Observation: PID $\Rightarrow$ Noetherian (Ideals are finitely generated!)

As a consequence, we have primary decompositions for PIDs.

Q: What do they look like?

Lemma 1: Fix a PID R & a non-zero prime ideal $\wp$ of R. Then, $\wp$ is a maximal ideal of R.

Proof: Write $\wp = (a)$ with $a \neq 0$ (R is a PID & $\wp$ is an ideal)

Assume $\wp = (a) \subsetneq I = (b) \subseteq R$. We need to show $I = R$.

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

If $I \neq \wp$ then $b \notin \wp$. The prime condition gives $c \in \wp$, so $c = ax$.

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

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

Corollary If q is a nonzero primary ideal in a PID, then $r(q)$ is a maximal ideal.

Q: What more can we say about primary components?

Lemma 2 If R is a PID & $q \neq (0)$ is a primary ideal, then $q = m^n$ for some maximal ideal ($m = r(q)$)

Proof: We know $q \subseteq r(q) = m$

Since R is a PID, we have $q = (q)$ & $m = (p)$ with $p^n \in q$ for some $n \geq 1$.

Pick smallest such n, ie $p^n \in q$ but $p^{n-1} \notin q$.

- Since $q \in (p)$, we have $q = px$ for some x
- Since $p^n \in (q)$ we have $p^n = qy$ for some $y \in R \setminus m$ (otherwise, we get $p^{n-1} \in (q)$)

$\Rightarrow p^n = qy = (px)y$ gives $p(p^{n-1} - xy) = 0$

Since R is a domain, $p^{n-1} = xy = yx \in m^{n-1}$

- But m^{n-1} is a primary ideal ($r(m^{n-1}) = m$ is maximal), so $yx \in m^{n-1}$ & $y \notin m = r(m^{n-1})$ forces $x \in m^{n-1}$ (definition of primary ideal)

$\Rightarrow x \in (p^{n-1})$ & we can write $x = p^{n-1} z$ for some $z \in R$.

Conclude: $q = px = p(p^{n-1}z) = p^n z$

$\Rightarrow \mathfrak{q} = (q) \subseteq (p^n) = \mathfrak{m}^n \underset{p^n \in \mathfrak{q}.}{\subseteq} (q)$ giving $\mathfrak{q} = \mathfrak{m}^n$. $\square$

This statement has a crucial consequence:

Theorem 1 (Primary Decompositions for PIDs)

Fix a nonzero proper ideal $\mathfrak{a}$ of a PID R. Then, there exists primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$ of R satisfying:

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

(2) $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ (no redundancies in (1))

(3) $\{\mathfrak{p}_i = r(\mathfrak{q}_i)\}_{1 \leq i \leq \ell}$ are distinct non-zero prime ideals of R

} reduced primary decomp.

Furthermore, $\mathrm{Min}(\mathfrak{a}) = \mathrm{Ass}(\mathfrak{a})$, & $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$ are unique.

$\hookrightarrow$ all nonzero prime ideals are maximal (so $\mathrm{Ass}(\mathfrak{a}) \subseteq \mathrm{Min}(\mathfrak{a})$)

Pf/ Use existence of reduced primary decomp for Noetherian rings, (Lecture 28, Thm 1 & Lemma 1). For the uniqueness, we that $\mathfrak{m}_i := r(\mathfrak{q}_i)$ is maximal by Lemma 1 & $\mathfrak{q}_i = \mathfrak{m}_i^{n_i}$ by Lemma 2. In particular, any 2 reduced primary decompositions will have the form:

$$\mathfrak{a} = \mathfrak{m}_1^{n_1} \cap \cdots \cap \mathfrak{m}_\ell^{n_\ell} = \mathfrak{m}_1^{s_1} \cap \cdots \cap \mathfrak{m}_\ell^{s_\ell}$$

The Associated primes are unique because they are minimal over $\mathfrak{a}$ (Lecture 28, Lemma 2)

- To finish, we have to show $n_i = s_i$ for each s_i.

Claim $n_i \leq \max\{n \geq 1 \quad \mathfrak{a} \subseteq \mathfrak{m}_i^n\}$ (This will be crucial to show that the n_i's are unique)

Pf/ $\mathfrak{a}$ is proper & $\mathfrak{m}_i \in \mathrm{Min}(\mathfrak{a})$ so $\mathfrak{a} \subseteq \mathfrak{m}_i$.

We want to show $\Lambda = \{n \geq 1 : \mathfrak{a} \subseteq \mathfrak{m}_i^n\}$ is finite. If not, this will force $\Lambda = \mathbb{Z}_{\geq 1}$ since $\mathfrak{m}_i^{j+1} \subseteq \mathfrak{m}_i^j$ says "$j+1 \in \Lambda \Rightarrow j \in \Lambda$".

Since R is a PID, write $\mathfrak{a} = (a)$ $a \neq 0$ & $\mathfrak{m}_i = (x)$ $x \neq 0$ & not a unit

• $\mathfrak{a} \subseteq \mathfrak{m}_i^j$ translates to $a = b_j x^j$ for each $j \geq 1$

Since R is a domain $a = b_{j+1} x^{j+1} = b_j x^j$ yields $b_j = b_{j+1} x$, and so we get an ascending chain of ideals in R:

$$(b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \cdots\cdots$$

Since R is Noetherian $\exists m$ with $(b_m) = (b_{m+1}) = \cdots$

Thus, $b_m = b_{m+1} x$ & $b_{m+1} \in (b_m)$ gives $b_{m+1} = c b_m$ for c in R

$\Rightarrow$ $b_m = (c b_m) x = b_m c x$ gives $1 = cx$, which cannot occur because $x \in \mathfrak{m}_i$ mxl ideal.

<u>Conclusion</u>: Λ is bounded say $\Lambda = \{1, \ldots, N_i\}$

By construction, $\mathfrak{a} \subseteq \mathfrak{m}_i^{N_i}$ & $\mathfrak{a} \not\subseteq \mathfrak{m}_i^{N_i+1}$. This forces $n_i \leq N_i$ $\square$

By intersecting $\mathfrak{a}$ with $\mathfrak{m}_i^{N_i}$ we get:

$$\mathfrak{a} = \mathfrak{a} \cap \mathfrak{m}_i^{N_i} = \mathfrak{m}_1^{n_1} \cap \cdots\cdots \cap \underbrace{(\mathfrak{m}_i^{n_i} \cap \mathfrak{m}_i^{N_i})}_{= \mathfrak{m}_i^{N_i}} \cap \cdots \cap \mathfrak{m}_\ell^{n_\ell}$$

<u>Conclusion</u>: $\mathfrak{a} = \mathfrak{m}_1^{N_1} \cap \cdots \cap \mathfrak{m}_\ell^{N_\ell}$ is a reduced primary decomposition. (assoc. primes are $\neq$ & minimal)

Now: $\mathfrak{a} = \mathfrak{m}_1^{n_1} \cap \cdots \cap \mathfrak{m}_\ell^{n_\ell} = \mathfrak{m}_1^{N_1} \cap \cdots \cap \mathfrak{m}^{N_\ell}$ with $n_i \leq N_i$ $\forall i$

• We want to show $n_i = N_i$ $\forall i$

Since $\mathfrak{m}_1, \ldots, \mathfrak{m}_\ell$ are different maximal ideals, they are pairwise coprime and so are $\{\mathfrak{m}_1^{n_1}, \ldots, \mathfrak{m}_\ell^{n_\ell}\}$ & $\{\mathfrak{m}_1^{N_1}, \ldots, \mathfrak{m}_\ell^{N_\ell}\}$ (extend Lemma 1, Lecture 27)

So
$$\mathfrak{m}_1^{n_1} \cap \cdots \cap \mathfrak{m}_\ell^{n_\ell} = \mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_\ell^{n_\ell}$$
$$\mathfrak{m}_1^{N_1} \cap \cdots \cap \mathfrak{m}_\ell^{N_\ell} = \mathfrak{m}_1^{N_1} \cdots \mathfrak{m}_\ell^{N_\ell}$$
by Problem 2 HW7

Write $\mathfrak{m}_i = (x_i)$ for $i = 1, \ldots, \ell$, so
$$\mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_\ell^{n_\ell} = (x_1^{n_1} \cdots x_\ell^{n_\ell})$$
$$\mathfrak{m}_1^{N_1} \cdots \mathfrak{m}_\ell^{N_\ell} = (x_1^{N_1} \cdots x_\ell^{N_\ell})$$

Since $x_1^{n_1} \cdots x_\ell^{n_\ell} \in (x_1^{N_1} \cdots x_\ell^{N_\ell})$ we get $x_1^{n_1} \cdots x_\ell^{n_\ell} = c\, x_1^{N_1} \cdots x_\ell^{N_\ell}$ for some $c \in R$

Since $n_i \leq N_i$ & R is a domain, we get $1 = c\, x_1^{N_1 - n_1} \cdots x_\ell^{N_\ell - n_\ell} \in \mathfrak{m}_i^{N_i - n_i}$.
If $n_i < N_i$ for some i, then we get $1 \in \mathfrak{m}_i^{N_i - n_i} \subseteq \mathfrak{m}_i$, which can't happen.
This ends our proof.

<u>Corollary</u>: Assume R is a PID & fix $x \in R \setminus \{0\}$. Then x can be uniquely written as $x = u\, p_1^{n_1} \cdots p_\ell^{n_\ell}$ where

(1) u is a unit in R

(2) $n_1, \ldots, n_\ell \geq 0$ are integers

(3) $p_1, \ldots p_\ell$ are prime elements in R (meaning (p_i) is a prime ideal) with $(p_i) \neq (p_j)$ if $i \neq j$ & $\{(p_1), \ldots, (p_\ell)\}$ is unique

<u>Definition</u>: A commutative ring R satisfying (1)–(3) is called a <u>unique factorization domain</u> (U.F.D.)

<u>Remark</u>: Our corollary says all PIDs are UFDs.

<u>Proof of Corollary</u>: Combine Theorem 1 & Lemma 3 to write

$(0) \neq (x) = (p_1^{n_1}) \cap \cdots \cap (p_\ell^{n_\ell}) = (p_1)^{n_1} \cap \cdots \cap (p_\ell)^{n_\ell}$

• $(p_1^{n_1}), \ldots, (p_\ell)^{n_\ell}$ are unique $\Rightarrow$ • $n_1, \ldots, n_\ell$ are unique &

• $(p_i) = r\left((p_i)^{n_i}\right)$ are unique

• The proof of Theorem 1 says $n_i = \max\{n : x \in (p_i)^n\}$. so they are unique! $\square$

<u>Example</u>: In $\mathbb{Z}$: $\underset{\pm 1, 0}{\neq} m = \pm p_1^{n_1} \cdots p_\ell^{n_\ell}$ p_i distinct primes (>0)

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

• $(\pm 1) = \mathbb{Z}$ has no primary component other than $\mathbb{Z}$ itself, so $\ell = 0$ for $m = \pm 1$