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

Definition: A primary decomposition \( \mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_l \) is reduced if

1. \( \mathfrak{q}_i \neq \bigcap_{j \neq i} \mathfrak{q}_j \) for \( j = 1, \ldots, l \) (i.e. no \( \mathfrak{q}_i \) is redundant)

2. \( \mathfrak{q}_i = \sqrt{\mathfrak{q}_i} \) are all distinct

**Def.** \( \text{Ass} (\mathfrak{a}) = \{ \sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_l} \} = \text{Associated primes of } \mathfrak{a} \)

Key results:
- \( \text{Ass}(\mathfrak{a}) \) doesn't depend on the choice of reduced primary decompos.
- Any \( \mathfrak{p} \) prime containing \( \mathfrak{a} \) where \( \mathfrak{p}/\mathfrak{a} \) is a minimal prime of \( \mathfrak{p}/\mathfrak{a} \) must feature in \( \text{Ass}(\mathfrak{a}) \). Call them \( \text{Min}(\mathfrak{a}) \)
- Uniqueness only applies to \( \mathfrak{q}_i \)'s with \( (\mathfrak{q}_i) \in \text{Min}(\mathfrak{a}) \)

(\( \mathfrak{q}_i = j_i^{-1}(j_i(\mathfrak{a})) \) \( j_i : R \to R_{\mathfrak{p}_i} \) \( \mathfrak{p}_i = \sqrt{(\mathfrak{q}_i)} \))

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 \( I = (\text{min}(I \cap \mathbb{Z}_{>0})) \))
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 Euclidean 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 $R$ and a nonzero prime ideal $\mathfrak{p}$ of $R$. Then $\mathfrak{p}$ is a maximal ideal of $R$.

**Proof:** Write $\mathfrak{p} = (a)$ with $a \neq 0$ (it is a PID and $\mathfrak{p}$ is an ideal) Assume $\mathfrak{p} = (a) \subseteq I = (b) \subseteq R$. We need to show $I = R$.

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

If $I \neq \mathfrak{p}$ then $b \notin \mathfrak{p}$. The prime condition gives $c \notin \mathfrak{p}$, so $c = ax$. Then $a = bc = bax$, i.e. $a(bx - 1) = 0$.

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

Corollary 1: If $\mathfrak{q}$ is a nonzero primary ideal in a PID, then $\mathfrak{q}(\mathfrak{q})$ is a maximal ideal.

Q: What more can we say about primary components?

Lemma 2: If $R$ is a PID and $\mathfrak{q} \neq (0)$ is a primary ideal, then $\mathfrak{q} = \mathfrak{m}^n$ for some maximal ideal $(\mathfrak{m} = \mathfrak{q}(\mathfrak{q}))$.

**Proof:** We know $\mathfrak{q} \subseteq \mathfrak{q}(\mathfrak{q}) = \mathfrak{m}$.

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

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

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

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

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

But $\mathfrak{m}^{n-1}$ is a primary ideal ($\mathfrak{q}(\mathfrak{m}^{n-1}) = \mathfrak{m}$ is maximal), so $yx \in \mathfrak{m}^{n-1}$ and $y \notin \mathfrak{m} = \mathfrak{q}(\mathfrak{m}^{n-1})$ forces $x \in \mathfrak{m}^{n-1}$ (definition of primary ideal).
\[ x \in \left(p^{n-1}\right) \Rightarrow \text{we can write } x = p^{n-1} z \text{ for some } z \in R. \]

**Conclude:**
\[ \mathfrak{q} = p\mathfrak{x} = p(\mathfrak{p}^{n-1} z) = \mathfrak{p}^{n} z \]
\[ \Rightarrow \mathfrak{q} = (\mathfrak{p}^{n}) = M^n \subseteq (\mathfrak{q}) \text{ giving } \mathfrak{q} = M^n. \]

\[ \mathfrak{p}^{n} \in \mathfrak{q}. \]

This statement has a crucial consequence:

**Theorem (Primary Decompositions for PIDs)**

Fix a nonzero proper ideal \( \mathfrak{a} \) of a PID \( R \). Then, there exists a primary decomposition of \( \mathfrak{a} \) by the following:

1. \( \mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_l \) ("Primary Decomposition of \( \mathfrak{a} \))
2. \( \mathfrak{q}_i \neq \bigcap_{j \neq i} \mathfrak{q}_j \) (no redundancies in (1))
3. \( \{ \mathfrak{q}_i \}_{1 \leq i \leq l} \) are distinct non-zero prime ideals of \( R \)

Furthermore, \( \text{Min} (\mathfrak{a}) = \text{Ass} (\mathfrak{a}) \), \( \mathfrak{q}_1, \ldots, \mathfrak{q}_l \) are unique.

For any two primary ideals \( \mathfrak{m}_1, \mathfrak{m}_2 \) of \( R \), the ideal \( \mathfrak{m}_1 \cap \mathfrak{m}_2 \) is also a primary ideal.

**Proof:** Use existence of reduced primary decomps for Noetherian rings.

(See Lecture 28, Thm 1 & Lemma 3). For the uniqueness, we find that \( M_i = M_i^{n_i} \) is maximal by Lemma 1 & \( M_i = M_i^{n_i} \) by Lemma 2. In particular, any 2 reduced primary decompositions will have the form:

\[ \mathfrak{a} = M_i^n \cap \cdots \cap M_l^n \subseteq M_i^s \cap \cdots \cap M_l^s. \]

The associated primes are unique because they are minimal (Lecture 28, Lemma 1). In particular, any 2 reduced primary decompositions will have the form:

\[ \mathfrak{a} = M_i^{n_i} \cap \cdots \cap M_l^{n_l} = M_i^{s_i} \cap \cdots \cap M_l^{s_l} \]

To finish, we have to show \( n_i = s_i \) for each \( s_i \).

**Claim** \( n_i \leq \max \{ n \geq 1 : \alpha \subseteq M_i^n \} \) (This will be crucial to show that the \( n_i \)'s are unique).

**Proof:** \( \alpha \) is proper & \( M_i \in \text{Min} (\mathfrak{a}) \), so \( \alpha \subseteq M_i \).

We want to show \( \lambda = \sum_{j \geq 1} \alpha \subseteq M_i^{n_j} \) is finite. If not, this will force \( \lambda = \mathbb{Z}_{\geq 1} \) since \( M_i^{n_j} \subseteq M_i^{j} \) says \( j+1 \in \lambda \Rightarrow j \in \lambda \).

Since \( R \) is a PID, write \( \mathfrak{a} = (a) \), \( a \neq 0 \) & \( \mathfrak{m} = (x) \), \( x \neq 0 \) but not unit.
\( \alpha \in M_i \) translates to \( a = b_j x^j \) in each \( j \geq 1 \).

Since \( R \) is a domain \( a = b_j x^{j+i} = b_j x^i \) yields \( b_j = b_{j+1} x \), and so we get an ascending chain of ideals in \( R \):
\[
(b_1) \subseteq (b_2) \subseteq (b_3) \subseteq \ldots
\]

Since \( R \) is Noetherian \( \exists m \) with \( (b_m) = (b_{m+1}) = \ldots \). Theorem : \( b_m = b_{m+1} x \) \& \( b_{m+1} \subseteq (b_m) \) gives \( b_{m+1} = cb_m \) \& \( c \in R \)

\[ \Rightarrow b_m = (cb_m) x = b_m cx \] yields \( 1 = cx \), which cannot occur because \( x \in M_i \) and ideal.

**Conclusion :** \( \mathcal{A} \) is bounded say \( \mathcal{A} = \{1, \ldots, N_i \} \)

By construction, \( \mathcal{A} \subseteq M_i \) \& \( \mathcal{A} \not\subseteq M_i \). This frees \( n_i \leq N_i \).

By intersecting \( \mathcal{A} \) with \( M_i \) we get:
\[
\mathcal{A} = \mathcal{A} \cap M_i = M_i \cap \ldots \cap (M_i^{n_i} \cap M_i^{N_i}) \cap \ldots \cap M_i^{n_e} = M_i^{n_i}
\]

**Conclusion :** \( \mathcal{A} = M_i^{n_1} \cap \ldots \cap M_i^{n_e} \) is a reduced primary decomposition. (These are \( \mathcal{A} \) are \( \mathcal{A} \) are coprime)

Now: \( \mathcal{A} = M_i^{n_1} \cap \ldots \cap M_i^{n_e} = M_i^{n_1} \cap \ldots \cap M_i^{n_e} \) with \( n_i \leq N_i \).

We want to show \( n_i = N_i \) \& \( \forall i \)

Since \( M_i, \ldots, M_e \) are different maximal ideals, they are pairwise coprime and so are \( \{M_i^{n_1}, \ldots, M_i^{n_e}\} \) and \( \{M_i^{n_1}, \ldots, M_i^{n_e}\} \) (extend Lemma 1, Lecture 27)

So \( M_i^{n_1} \cap \ldots \cap M_i^{n_e} = M_i^{n_1} \cap \ldots \cap M_i^{n_e} \) by Problem 2, HW 7

Write \( M_i = (x_i) \) \& \( i = 1, \ldots, e \), so \( M_i^{n_1} \cap \ldots \cap M_i^{n_e} = (x_1^{n_1}, \ldots, x_e^{n_e}) \) \& \( M_i^{n_1} \cap \ldots \cap M_i^{n_e} = (x_1^{n_1}, \ldots, x_e^{n_e}) \)

\[ \text{Since } x_1^{n_1}, \ldots, x_e^{n_e} \in (x_1^{n_1}, \ldots, x_e^{n_e}) \text{ we get } x_1^{n_1}, \ldots, x_e^{n_e} = c x_1^{n_1}, \ldots, x_e^{n_e} \text{ for some } c \in \mathbb{R} \]

Since \( n_i \leq N_i \) \& \( R \) is a domain, we get \( 1 = c x_1^{n_1} \ldots x_e^{n_e} \) \( \in M_i^{n_i} \).

If \( n_i < N_i \) for some \( i \), then we get \( 1 \in M_i^{n_i} \subseteq M_i \), which can't happen.

This ends our proof.
Corollary: Assume \( R \) is a PIDs \( \{x \in R: x \neq 0\} \). Then \( x \) can be uniquely written as \( x = u p_1^{n_1} \cdots p_e^{n_e} \) where

1. \( u \) is a unit in \( R \)
2. \( n_1, \ldots, n_e > 0 \) are integers
3. \( p_1, \ldots, p_e \) are prime elements in \( R \) (meaning \( (p_i) \) is a prime ideal) with \( (p_i) \neq (p_j) \) if \( i \neq j \) and \( \{p_1, \ldots, p_e\} \) is unique

Definition: A commutative ring \( R \) satisfying (1)–(3) is called a unique factorization domain (UFD).

Remark: Our corollary says all PIDs are UFDs.

Proof of Corollary: Combine Theorem 1 and Lemma 3 to write

\[
\not\exists (x) \neq (p_1^{n_1}) \cap \cdots \cap (p_e^{n_e}) = (p_1)^{n_1} \cap \cdots \cap (p_e)^{n_e}
\]

\( (p_1^{n_1}), \ldots, (p_e^{n_e}) \) are unique \( \implies \) \( n_1, \ldots, n_e \) are unique \&

\( (p_i) = \not\exists \{p_i \} \) are unique

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

Example: In \( \mathbb{Z} \), \( m = \pm p_1^{n_1} \cdots p_e^{n_e} \) \( p_i \) distinct primes \( (> 0) \)

corresponds to \( (m) = (p_1)^{n_1} \cap \cdots \cap (p_e)^{n_e} \).

\( \pm 1 = \mathbb{Z} \) have no primary component other than \( \mathbb{Z} \) itself, so \( k = 0 \) for \( m = \pm 1 \)