Commutative Algebra
Chapter 4: Primary Decomposition

Sichuan University, Fall 2023

Reminder (Prime ideals; see Chapter 1)

- An ideal $\mathfrak{p}$ in a ring A is *prime* if $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.
- Equivalently, $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is an integral domain.
- Every maximal ideal is prime.
- If $\mathfrak{a}$ is an ideal, then we have a one-to-one correspondance between prime (resp., maximal) ideals of $A/\mathfrak{a}$ and prime (resp., maximal) ideals of A containing $\mathfrak{a}$ (Proposition 1.1*; see slides on Chap. 1).

Primary Decomposition

Definition (Primary Ideals)

An ideal $\mathfrak{q}$ in A is *primary* if $\mathfrak{q} \neq A$ and

$$xy \in \mathfrak{q} \Longrightarrow x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n \geq 1.$$

Remarks

1. If $\mathfrak{q} \neq A$, then
$$\mathfrak{q} \text{ primary} \Longleftrightarrow \text{every zero-divisor in } A/\mathfrak{q} \text{ is nilpotent.}$$
2. Every prime ideal is primary.
3. If $f : A \to B$ is a ring homomorphism and $\mathfrak{q}$ is a primary ideal in B, then its contraction $\mathfrak{q}^c = f^{-1}(\mathfrak{q})$ is a primary ideal in A.

Primary Decomposition

Reminder (Radicals of ideals; see Chapter 1)

- If $\mathfrak{a}$ is an ideal in A, then its *radical* is
$$r(\mathfrak{a}) = \{x \in A;\ x^n \in \mathfrak{a} \text{ for some } n \geq 1\}.$$
- $r(\mathfrak{a})$ is the intersection of all the prime ideals that contain $\mathfrak{a}$. In particular, this is an ideal containing $\mathfrak{a}$.
- This is the contraction of the nilradical $\mathfrak{N}(A/\mathfrak{a})$ under the canonical homomorphism $A \rightarrow A/\mathfrak{a}$.
- $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$ (see Exercise 1.13).
- If $\mathfrak{p}$ is a prime ideal, then $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n \geq 1$ (see Exercise 1.13).

Remark

If $\mathfrak{q}$ is an ideal $\neq A$, then $\mathfrak{q}$ is primary if
$$xy \in \mathfrak{q} \Longrightarrow x \in \mathfrak{q} \text{ or } y \in r(\mathfrak{q}).$$

Primary Decomposition

Proposition (Proposition 4.1)

Let $\mathfrak{q}$ be a primary ideal in a ring A. Then $r(\mathfrak{q})$ is a prime ideal, and hence it's the smallest prime ideal containing $\mathfrak{q}$.

Proof.

- It is enough to show that $r(\mathfrak{q})$ is prime.
- If $xy \in r(\mathfrak{q})$, then $x^m y^m \in \mathfrak{q}$.
- As $\mathfrak{q}$ primary, $x^m \in \mathfrak{q}$ or $y^{mn} \in \mathfrak{q}$, and hence x or y is in $r(\mathfrak{q})$.
- Thus, $r(\mathfrak{q})$ is prime.

The result is proved. □

Primary Decomposition

Definition

If $\mathfrak{p}$ is a prime ideal, then any primary ideal $\mathfrak{q}$ such that $r(\mathfrak{q}) = \mathfrak{p}$ is called $\mathfrak{p}$-*primary*.

Remark

Warning! If $\mathfrak{a}$ is an ideal whose radical $r(\mathfrak{a})$ is prime, then $\mathfrak{a}$ need not be primary (see slide 9).

Primary Decomposition

Example

The primary ideals in $\mathbb{Z}$ are (0) and (p^n) with p prime, since:

- They are primary ideals.
- They are the only ideals in $\mathbb{Z}$ with prime radical.

Example

Let $A = k[x,y]$, k field, and $\mathfrak{q} = (x, y^2)$. Then $\mathfrak{q}$ is primary, since:

- $A/\mathfrak{q} \simeq \big(k[x,y]/(x)\big)/\big((x,y^2)/(x)\big) \simeq k[y]/(y^2)$.
- Every zero-divisor in $k[y]/(y^2)$ is a multiple of y, and hence is nilpotent in $k[y]/(y^2)$.

The radical of $\mathfrak{q}$ is $\mathfrak{p} = (x, y)$. We have

$$\mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}.$$

This shows that a primary ideal need not be a prime-power.

Example

Let $A = k[x, y, z]/(xy - z^2)$, and denote by $\overline{x}$, $\overline{y}$, $\overline{z}$ the images of x, y, z in A. Set $\mathfrak{p} = (\overline{x}, \overline{z})$.

- The ideal $\mathfrak{p}$ is prime, since $A/\mathfrak{p} \simeq k[x, y, z]/(x, z) \simeq k[y]$ is an integral domain.
- The ideal $\mathfrak{p}^2$ is not primary, since $\overline{xy} = \overline{z}^2 \in \mathfrak{p}^2$, but $\overline{x} \notin \mathfrak{p}^2$ and $\overline{y} \notin \mathfrak{p} = r(\mathfrak{p}^2)$.

This shows that a prime-power need be a primary ideal. However, we have the following result:

Primary Decomposition

The previous example shows that a prime-power need be a primary ideal. However, we have the following result:

Proposition (Proposition 4.2)

If $\mathfrak{a}$ is an ideal in A whose radical radical $r(\mathfrak{a})$ is maximal, then $\mathfrak{a}$ is primary. In particular, every power of a maximal ideal $\mathfrak{m}$ is $\mathfrak{m}$-primary.

Proof of Proposition 4.2.

- $r(\mathfrak{a})$ is contraction of the nilradical $\mathfrak{N}(A/\mathfrak{a})$ under the canonical homomorphism $A \to A/\mathfrak{a}$.
- As $r(\mathfrak{a})$ is maximal and contains $\mathfrak{a}$, we see that $\mathfrak{N}(A/\mathfrak{a})$ is maximal.
- As $\mathfrak{N}(A/\mathfrak{a})$ is the intersection of all prime ideals of $A/\mathfrak{a}$, it follows that $\mathfrak{N}(A/\mathfrak{a})$ is the unique prime ideal of $A/\mathfrak{a}$.
- If $\overline{y} \in A/\mathfrak{a}$ is not a unit, it is contained in some maximal ideal.
- This maximal ideal must be $\mathfrak{N}(A/\mathfrak{a})$, so $\overline{y} \in \mathfrak{N}(A/\mathfrak{a})$, i.e., $\overline{y}$ is nilpotent. It follows that

$$\bar{x}\bar{y} = 0 \text{ in } A/\mathfrak{a} \Longrightarrow \overline{x} = 0 \text{ or } \overline{y}^n = 0.$$

- Therefore, if $xy \in \mathfrak{a}$, then $xy = 0$ in $A/\mathfrak{a}$, and hence $x \in \mathfrak{a}$ or $y^n \in \mathfrak{a}$ for some n. That is, $\mathfrak{a}$ is primary.

The proof is complete. □

Primary Decomposition

Lemma (Lemma 4.3)

If $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary ideals, then $\mathfrak{q} = \cap_{i=1}^{n} \mathfrak{q}_i$ is $\mathfrak{p}$-primary.

Proof.

- We have $r(\mathfrak{q}) = r(\cap \mathfrak{q}_i) = \cap r(\mathfrak{q}_i) = \mathfrak{p}$.
- If $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, then $\exists i$ such that $x \notin \mathfrak{q}_i$ and $xy \in \mathfrak{q}_i$.
- As $\mathfrak{q}_i$ is primary, $y^n \in \mathfrak{q}_i$, i.e., $y \in r(\mathfrak{q}_i) = \mathfrak{p} = r(\mathfrak{q})$, and hence $y^m \in \mathfrak{q}$ for some m.
- Thus, $\mathfrak{q}$ is primary.

This proves the result. □

Reminder (Ideal quotients; see Chapter 1)

- If $\mathfrak{a}$ is an ideal in A and $x \in A$, then
$$(\mathfrak{a} : x) = \{y \in A;\ xy \in \mathfrak{a}\}.$$
In particular, $(\mathfrak{a} : x)$ is an ideal.
- $(\mathfrak{a} : x) \cap (\mathfrak{b} : x) = (\mathfrak{a} \cap \mathfrak{b} : x)$.

Lemma (Lemma 4.4)

Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal, and let $x \in A$. Then:

(i) *If $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = (1)$.*

(ii) *If $x \notin \mathfrak{q}$, then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary. In particular, $r(\mathfrak{q} : x) = \mathfrak{p}$.*

(iii) *If $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.*

Proof of (i) and (iii).

- By definition $(\mathfrak{q} : x) = \{y \in A;\ xy \in \mathfrak{q}\}$.
- If $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = A = (1)$.
- Suppose that $x \notin \mathfrak{p} = r(\mathfrak{q})$. Then, as $\mathfrak{q}$ is primary,

$$xy \in \mathfrak{q} \Longleftrightarrow y \in \mathfrak{q}.$$

Thus $(\mathfrak{q} : x) = \mathfrak{q}$. □

Proof of (ii).

- Suppose that $x \notin \mathfrak{q}$. As $(\mathfrak{q} : x) \supseteq \mathfrak{q}$, we have $r(\mathfrak{q} : x) \supseteq r(\mathfrak{q}) = \mathfrak{p}$.
- If $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$. As $\mathfrak{q}$ is primary, $y \in r(\mathfrak{q}) = \mathfrak{p}$.
- Thus, $(\mathfrak{q} : x) \subseteq \mathfrak{p}$, and hence $r(\mathfrak{q} : x) \subseteq r(\mathfrak{p}) = \mathfrak{p}$.
- It follows that $r(\mathfrak{q} : x) = \mathfrak{p}$.
- If $yz \in (\mathfrak{q} : x)$ and $y \notin \mathfrak{p}$, then $(xz)y \in \mathfrak{q}$, and hence $xz \in \mathfrak{q}$ since $\mathfrak{q}$ is $\mathfrak{p}$-primary, i.e., $z \in (\mathfrak{q} : x)$.
- This shows that $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.

The proof of Lemma 4.4 is complete. □

Primary Decomposition

Definition (Primary Decomposition)

- A *primary decomposition* of an ideal $\mathfrak{a}$ in A is of the form,

$$\mathfrak{a} = \bigcap_{1 \leq i \leq n} \mathfrak{q}_i, \qquad \mathfrak{q}_i \text{ primary ideal.}$$

- We say that the primary decomposition is *minimal* if
  (i) $r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$ for $i \neq j$.
  (ii) $\mathfrak{q}_i \not\supseteq \cap_{j \neq i} \mathfrak{q}_j$ for $i = 1, \ldots, n$.

Remarks

1. Some ideals don't admit a primary decomposition. An ideal that admits a primary decomposition is called *decomposable*.
2. Any primary decomposition can be reduced to a minimal one:
   - Lemma 4.3 allows us ro to reach (i) by taking the intersections of the $\mathfrak{q}_i$ with same radical.
   - Once we have (i) we achieve (ii) by throwing away the primary ideals $\mathfrak{q}_i$ such that $\mathfrak{q}_i \supseteq \cap_{j \neq i} \mathfrak{q}_j$.

Primary Decomposition

Reminder (Proposition 1.11)

Assume that $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals and $\mathfrak{p}$ is a prime ideal containing $\cap \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. If $\mathfrak{p} = \cap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Theorem (1st Uniqueness Theorem; Theorem 4.5)

Let $\mathfrak{a}$ be a decomposable ideal and $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ a minimal primary decomposition. Set $p_i = r(\mathfrak{q}_i)$, $i = 1, \ldots, n$. Then the $\mathfrak{p}_i$ are exactly the prime ideals of the form $r(\mathfrak{a} : x)$, $x \in A$. In particular, they don't depend on the primary decomposition of $\mathfrak{a}$.

Primary Decomposition

Proof of Theorem 4.5.

- Let $x \in A$. Then $(\mathfrak{a} : x) = (\cap \mathfrak{q}_i : x) = \cap(\mathfrak{q}_i : x)$, and hence
$$r(\mathfrak{a} : x) = r\Big(\bigcap(\mathfrak{q}_i : x)\Big) = \bigcap r(\mathfrak{q}_i : x).$$
- By Lemma 4.4 $r(\mathfrak{q}_i : x) = (1)$ if $x \in \mathfrak{q}_i$ and $r(\mathfrak{q}_i : x) = \mathfrak{p}_i$ otherwise. Thus,
$$r(\mathfrak{a} : x) = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j.$$
- Suppose that $r(\mathfrak{a} : x)$ is prime. Then Proposition 1.11 ensures that $r(\mathfrak{a} : x) = \mathfrak{p}_j$ for some j such that $x \notin \mathfrak{q}_j$.
- Conversely, as the primary decomposition is minimal, for each i there is $x \notin \mathfrak{q}_i$ such that $x \in \cap_{j \neq i} \mathfrak{q}_j$, and hence $x \in \mathfrak{q}_j$ for $j \neq i$.
- Thus, $r(\mathfrak{a} : x) = \cap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j = \mathfrak{p}_i$.

This proves the result. □

Primary Decomposition

Remarks

1. The proof of the uniqueness theorem shows that for each i there is $x_i \in A$ such that $(\mathfrak{a} : x_i)$ is $\mathfrak{p}_i$-primary.
2. The primary components are not independent of the minimal decomposition in general (see next slide).

Primary Decomposition

Example

Let $A = k[x, y]$, k field, and $\mathfrak{a} = (x^2, xy)$.

- Set $\mathfrak{p}_1 = (x)$ and $\mathfrak{p}_2 = (x, y)$. Then

$$\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$$

  This is a (minimal) primary decomposition, since:

  - $\mathfrak{p}_1$ is a prime ideal, and hence is primary.
  - $\mathfrak{p}_2$ is a maximal ideal, since $k[x, y]/(x, y) \simeq k$ is a field.
  - The ideal $\mathfrak{p}_2^2$ then is $\mathfrak{p}_2$-primary by Proposition 4.2.

- We have another minimal primary decomposition,

$$\mathfrak{a} = (x) \cap (x^2, y).$$

  Here (x^2, y) can be shown to be primary in the same way as in the example of slide 7.

- Thus, we may have distinct minimal primary decompositions.

Primary Decomposition

Definition

Let $\mathfrak{a}$ be a decomposable ideal in A and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ the prime ideals associated with any minimal primary decomposition.

- The prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are said to *belong to* $\mathfrak{a}$ or to be *associated with* $\mathfrak{a}$.
- The minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ are called *minimal* or *isolated* prime ideals associated with $\mathfrak{a}$.
- The other prime ideals are called *embedded*.

Remark

The terminology isolated/embedded comes from algebraic geometry (see Atiyah-MacDonald's book).

Example

Let $A = k[x, y]$ and $\mathfrak{a} = (x^2, xy) = (x) \cap (x, y)^2$. The only minimal prime ideal is (x), since $(x) \subseteq (x, y)$.

Reminder (see Propositions 1.11 & 1.11*; slides on Chapter 1)

Let $\mathfrak{a}$ be an ideal of A and $f : A \rightarrow A/\mathfrak{a}$ the canonical homomorphism.

1. We have a one-to-one correspondance $\mathfrak{b} \rightarrow \mathfrak{b}^e$ with inverse $\overline{\mathfrak{b}} \rightarrow \overline{\mathfrak{b}}^c$ between ideals of A containing $\mathfrak{a}$ and ideals of $A/\mathfrak{a}$.
2. In particular:
   - If $\mathfrak{b}$ is an ideal of A containing $\mathfrak{a}$, then $\mathfrak{b}^{ec} = \mathfrak{b}$.
   - If $\overline{\mathfrak{b}}$ is ideal of $A/\mathfrak{a}$, then $\overline{\mathfrak{b}}^{ce} = \overline{\mathfrak{b}}$.
3. This induces a one-to-one correspondance between prime (resp., maximal) ideals of A containing $\mathfrak{a}$ and prime (resp., maximal) ideals of $A/\mathfrak{a}$.

Primary Decomposition

Reminder (see Exercise 1.18)

If $\overline{\mathfrak{b}}$ is an ideal of $A/\mathfrak{a}$, then $r(\overline{\mathfrak{b}}^c) = r(\overline{\mathfrak{b}})^c$.

Fact

If $\mathfrak{b}$ is an ideal of A containing $\mathfrak{a}$, then $r(\mathfrak{b}^e) = r(\mathfrak{b})^e$.

Proof.

For $x \in A$ denote by $\overline{x}$ its image in $A/\mathfrak{a}$.

- As $\mathfrak{b} \supseteq \mathfrak{a}$, we have
$$\overline{x} \in \mathfrak{b}^e \Longleftrightarrow x \in \mathfrak{b} + \mathfrak{a} \Longleftrightarrow x \in \mathfrak{b}.$$
- Thus,
$$\overline{x} \in r(\mathfrak{b}^e) \Leftrightarrow \overline{x}^n \in \mathfrak{b}^e \Leftrightarrow x^n \in \mathfrak{q} \Leftrightarrow x \in r(\mathfrak{b}) \Longleftrightarrow \overline{x} \in r(\mathfrak{b})^e.$$
Hence $r(\mathfrak{b}^e) = r(\mathfrak{b})^e$.

The result is proved. □

Primary Decomposition

Proposition*

Let $\mathfrak{a}$ be an ideal of A and $f : A \to A/\mathfrak{a}$ the canonical homomorphism.

1. *If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal of A containing $\mathfrak{a}$, then $\mathfrak{q}^e$ is a $\mathfrak{p}^e$-primary ideal of $A/\mathfrak{a}$.*
2. *If $\overline{\mathfrak{q}}$ is a $\overline{\mathfrak{p}}$-primary ideal of $A/\mathfrak{a}$, then $\overline{\mathfrak{q}}^c$ is a $\overline{\mathfrak{p}}^c$-primary ideal of A.*
3. *We have a one-to-one correspondance $\mathfrak{q} \to \mathfrak{q}^e$ with inverse $\overline{\mathfrak{q}} \to \overline{\mathfrak{q}}^c$ between primary ideals of A containing $\mathfrak{a}$ and primary ideals of $A/\mathfrak{a}$.*

Proof of Proposition*.

If $x \in A$, we denote by $\overline{x}$ its image in $A/\mathfrak{a}$.

- Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal of A containing $\mathfrak{a}$. Then $\mathfrak{q}^e$ is an ideal of $A/\mathfrak{a}$ and $r(\mathfrak{q}^e) = r(\mathfrak{q})^e = \mathfrak{p}^e$.
- As $\overline{x} \in \mathfrak{q}^e \Leftrightarrow x \in \mathfrak{q}$, we have
$$\begin{aligned} \bar{x}\bar{y} \in \mathfrak{q}^e \Longleftrightarrow xy \in \mathfrak{q} &\Longleftrightarrow x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \\ &\Longleftrightarrow \overline{x} \in \mathfrak{q}^e \text{ or } \overline{y}^n \in \mathfrak{q}^e. \end{aligned}$$
This shows that $\mathfrak{q}^e$ is $\mathfrak{p}^e$-primary.
- Let $\overline{\mathfrak{q}}$ be a $\overline{\mathfrak{p}}$-primary ideal of $A/\mathfrak{a}$. Then $\overline{\mathfrak{q}}^c$ is an ideal of A and $r(\overline{\mathfrak{q}}^c) = r(\overline{\mathfrak{q}})^c = \mathfrak{p}^c$.
- We have
$$\begin{aligned} xy \in \overline{\mathfrak{q}}^c \Longleftrightarrow \overline{xy} \in \overline{\mathfrak{q}} &\Longleftrightarrow \overline{x} \in \overline{\mathfrak{q}} \text{ or } \overline{y}^n \in \overline{\mathfrak{q}} \\ &\Longleftrightarrow x \in \overline{\mathfrak{q}}^c \text{ or } y^n \in \overline{\mathfrak{q}}^c. \end{aligned}$$
It follows that $\overline{\mathfrak{q}}^c$ is $\overline{\mathfrak{p}}^c$-primary.

The proof is complete. □

Primary Decomposition

Reminder (see Chapter 1)

- If $x \in \mathfrak{a}$, then $(0:x)$ is the annihilator of x, i.e.,
$$(0:x) = \{y \in A;\ xy = 0\}.$$
- Let D be the set of all zero-divisors in A. By Lemma 1.15 we have
$$D = \bigcup_{x \neq 0} (0:x) = \bigcup_{x \neq 0} r(0:x).$$

Primary Decomposition

Proposition (Proposition 4.7)

Suppose that $\mathfrak{a}$ *is a decomposable ideal in* A*. Let* $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ *be a minimal primary decomposition, and set* $\mathfrak{p}_i = r(\mathfrak{q}_i)$*. We have*

$$\bigcup_{1 \leq i \leq n} \mathfrak{p}_i = \{x \in A;\ (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

In particular, if the zero ideal is decomposable, then the set D *of zero-divisors is the union of the prime ideals that belong to* 0*.*

Proof of Proposition 4.7; Case $\mathfrak{a} = 0$.

- Suppose that $\mathfrak{a} = 0$, i.e., $0 = \cap \mathfrak{q}_i$ is a minimal primary decomposition of 0.
- By Proposition 1.15, we have $D = \cup_{x \neq 0} r(0 : x)$.
- By the proof of Proposition 4.5, $r(0 : x) = \cap_{x \notin q_j} \mathfrak{p}_j \subseteq \mathfrak{p}_i$ for some i, and hence $D \subseteq \cup \mathfrak{p}_i$.
- By Proposition 4.5 each $\mathfrak{p}_i$ is of the form $r(0 : x)$ for some $x \in A$, and hence $\mathfrak{p}_i \subseteq D$. Thus,

$$D = \bigcup_{1 \leq i \leq n} \mathfrak{p}_i.$$

- Note also that

$$D = \{x \in A;\ \operatorname{Ann}(x) \neq 0\} = \{x \in A;\ (0 : x) \neq 0\}.$$

This proves the result for $\mathfrak{a} = 0$. □

Primary Decomposition

Proof of Proposition 4.7; General Case.

- Suppose that $\mathfrak{a} \neq 0$, and let $f : A \to A/\mathfrak{a}$ be the canonical homomorphism.
- By Proposition* $\mathfrak{q}_i^e$ is $\mathfrak{p}_i^e$-primary.
- As $\mathfrak{q}_i \supseteq \mathfrak{a}$, we have $\cap_{i=1}^n \mathfrak{q}_i^e = \left(\cap_{i=1}^n \mathfrak{q}_i\right)^e \supseteq \mathfrak{a}^e = 0$.
- As the primary decomposition $\cap \mathfrak{q}_i = \mathfrak{a}$ is minimal, $\mathfrak{p}_i \cap \mathfrak{p}_j = \emptyset$, $i \neq j$, and $\mathfrak{q}_i \not\supseteq \cap_{j\neq i} \mathfrak{q}_j$.
- As $\mathfrak{p}_i \supseteq \mathfrak{a}$, we have $\mathfrak{p}_i^e \cap \mathfrak{p}_j^e = (\mathfrak{p}_i \cap \mathfrak{p}_j)^e = \emptyset$, $i \neq j$.
- Here $\mathfrak{q}_i^{ec} = \mathfrak{q}_i$ (see Proposition 1.1). If $\mathfrak{q}_i^e \supseteq \cap_{j\neq i} \mathfrak{q}_j^e$, then

  $$\mathfrak{q}_i = \mathfrak{q}_i^{ec} \supseteq \cap_{j\neq i} \mathfrak{q}_j^{ec} = \cap_{j\neq i} \mathfrak{q}_i \quad \text{(not possible).}$$

  Hence $\mathfrak{q}_i^e \not\supseteq \cap_{j\neq i} \mathfrak{q}_j^e$.
- It follows that $0 = \cap_{i=1}^n \mathfrak{q}_i^c$ is a minimal primary decomposition.

□

Proof of Proposition 4.7; General Case (Continued).

- Let D be the zero-divisor set of $A/\mathfrak{a}$. By the $\mathfrak{a} = 0$ case, we have
$$D = \bigcup_{1 \leq i \leq n} \mathfrak{p}_i^e.$$
- Thus,
$$D^c = \left(\cup_{i=1}^n \mathfrak{p}_i^e \right)^c = \cup_{i=1}^n \mathfrak{p}_i^{ec} = \cup_{i=1}^n \mathfrak{p}_i.$$
- Denote by $\overline{x}$ the class of x in $A/\mathfrak{a}$. We have
$$D^c = \{x \in A; (0 : \overline{x}) \neq 0\} = \{x \in A; (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$
- Thus,
$$\bigcup_{1 \leq i \leq n} \mathfrak{p}_i = \{x \in A; (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

The proof is complete. □

Remark

Suppose that the zero ideal is decomposable. Let $0 = \cap_{i=1}^{n} \mathfrak{q}_i$ be a minimal decomposition, and set $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Let $\mathfrak{N} = r(0)$ be the nilradical of A. Then

$$\mathfrak{N} = r\left(\cap \mathfrak{q}_i\right) = \cap r(\mathfrak{q}_i) = \cap \mathfrak{p}_i.$$

That is, $\mathfrak{N}$ is the intersection of all prime ideals that belong to 0.

Reminder (Rings of fractions; see Chapter 3)

Let S be a multiplicative subset of A.

- The ring of fractions $S^{-1}A$ consists of classes a/s with $a \in A$ and $s \in S$:
$$a/s = b/t \iff \exists u \in S \text{ such that } u(at - bs) = 0.$$
- The map $f : a \to a/1$ is a ring homomorphism from A to $S^{-1}a$.
- The extension of an ideal $\mathfrak{a}$ is equal to $S^{-1}\mathfrak{a}$.

Primary Decomposition

Reminder (see Proposition 3.11)

- Every ideal $\mathfrak{b}$ of $S^{-1}A$ is an extended ideal, and hence $\mathfrak{b}^{ce} = \mathfrak{b}$.
- For any ideal $\mathfrak{a}$ in A we have
$$(S^{-1}\mathfrak{a})^c = \bigcup_{s\in S}(\mathfrak{a} : s).$$
- There is a one-to-one correspondance ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) between prime ideals of $S^{-1}A$ and prime ideals in A that don't meet S.
- $S^{-1}(\mathfrak{a}\cap\mathfrak{b}) = \left(S^{-1}\mathfrak{a}\right)\cap\left(S^{-1}\mathfrak{b}\right)$.
- $r\left(S^{-1}\mathfrak{a}\right) = S^{-1}r(\mathfrak{a})$.

Proposition (Proposition 4.8)

Let S be a multiplicative closed subset of A and $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal of A.

(i) *If $S \cap \mathfrak{p} \neq \emptyset$, then $S^{-1}\mathfrak{q} = S^{-1}A$.*

(ii) *If $S \cap \mathfrak{p} = \emptyset$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary and $(S^{-1}\mathfrak{q})^c = \mathfrak{q}$.*

In particular, we have a one-to-one correspondance ($\mathfrak{q} \leftrightarrow S^{-1}\mathfrak{q}$) between primary ideals of $S^{-1}A$ and primary ideals of A whose radicals do not meet S.

Proof of Proposition 4.8, Part (i).

- Suppose that $s \in S \cap \mathfrak{p} \neq \emptyset$. Thus, $s^n \in S \cap \mathfrak{q}$ for some n.
- If $x = a/t \in S^{-1}A$, then $x = (as^n)/(ts^n) \in S^{-1}\mathfrak{q}$. Thus, $S^{-1}\mathfrak{q} = S^{-1}A$.

This proves (i). □

Proof of Proposition 4.8, Part (ii).

- Suppose that $S \cap \mathfrak{p} = \emptyset$. If $s \in S$ and $x \in (\mathfrak{q} : s)$, then $xs \in \mathfrak{q}$ and $s \notin \mathfrak{p} = r(\mathfrak{q})$. As $\mathfrak{q}$ is primary, $x \in \mathfrak{q}$. Thus $(\mathfrak{q} : s) = \mathfrak{q}$.
- Therefore, by Proposition 3.11 we get
$$\left(S^{-1}\mathfrak{q}\right)^c = \cup_{s \in S}(\mathfrak{q} : s) = \mathfrak{q}.$$
- We also have $r(S^{-1}\mathfrak{q}) = S^{-1}(r(\mathfrak{q})) = S^{-1}\mathfrak{p}$.
- If $x = a/s$ and $y = b/t$ are such that $xy = (ab)/(st) = z/u \in S^{-1}\mathfrak{q}$ with $z \in \mathfrak{q}$, then $\exists v \in S$ such that $(abu - zst)v = 0$, and hence $(ab)(uv) = zstv \in \mathfrak{q}$.
- Here $uv \in S$, and hence $uv \notin \mathfrak{p} = r(\mathfrak{q})$. As $\mathfrak{q}$ is $\mathfrak{p}$-primary, $ab \in \mathfrak{q}$, and hence $a \in \mathfrak{q}$ or $b \in \mathfrak{p}$, and hence $x = a/s \in S^{-1}\mathfrak{q}$ or $y = b/t \in S^{-1}\mathfrak{p} = r(S^{-1}\mathfrak{q})$.
- This shows that $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary.

This proves (ii). □

Primary Decomposition

Proof of Proposition 4.8, Continued.

- By (ii) if $\mathfrak{q}$ is a primary ideal of A such that $r(\mathfrak{q}) \cap S = \emptyset$, then $S^{-1}\mathfrak{q}$ is a primary ideal of $S^{-1}A$ and $(S^{-1}\mathfrak{q})^c = \mathfrak{q}$.
- Conversely, let $\mathfrak{q}$ be a primary ideal of $S^{-1}A$, and set $\mathfrak{p} = r(\mathfrak{q})$.
- Then $\mathfrak{q}^c$ is a primary ideal of A and $r(\mathfrak{q}^c) = r(\mathfrak{q})^c = \mathfrak{p}^c$.
- By Proposition 3.11 $\mathfrak{p}^c$ is a prime ideal that does not meet S, i.e., $r(\mathfrak{q}^c) \cap S = \emptyset$.
- By Proposition 3.11 every ideal of $S^{-1}A$ is an extended ideal, and so $S^{-1}(\mathfrak{q}^c) = \mathfrak{q}^{ce} = \mathfrak{q}$.
- Therefore $\mathfrak{q} \leftrightarrow S^{-1}\mathfrak{q}$ provides a one-to-one correspondance between primary ideals of $S^{-1}A$ and primary ideals of A whose radicals do not meet S.

The proof is complete. □

Primary Decomposition

Notation

If $\mathfrak{a}$ is an ideal in A, we denote by $S(a)$ the contraction of $S^{-1}\mathfrak{a}$, i.e., $S(a) = f^{-1}(S^{-1}a)$.

Proposition (Proposition 4.9)

Let $\mathfrak{a}$ be a decomposable ideal in A and $\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{q}_i$ a minimal primary decomposition. Set $\mathfrak{p}_i = r(q_i)$, and assume the indexation is so that S meets $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$, but not $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Then

$$S^{-1}\mathfrak{a} = \bigcap_{1\leq i\leq m} S^{-1}\mathfrak{q}_i, \qquad S(\mathfrak{a}) = \bigcap_{1\leq i\leq m} \mathfrak{q}_i,$$

and these decompositions are minimal primary decompositions.

Primary Decomposition

Proof of Proposition 4.9.

- By Prop. 3.11 we have $S^{-1}\mathfrak{a} = S^{-1}(\cap_{i=1}^{n}\mathfrak{q}_i) = \cap_{i=1}^{n} S^{-1}(\mathfrak{q}_i)$.
- By Proposition 4.8 $S^{-1}\mathfrak{q}_i = S^{-1}A$ for $i \geq m+1$. Thus,
$$S^{-1}\mathfrak{a} = \cap_{i=1}^{m} S^{-1}(\mathfrak{q}_i).$$
- By Prop. 4.8 $S^{-1}q_i$ is primary and $(S^{-1}\mathfrak{q}_i)^c = \mathfrak{q}_i$ for $i \leq m$.
- As the $\mathfrak{p}_i$ are pairwise disjoint, so are the $S^{-1}\mathfrak{p}_i$, since $(S^{-1}\mathfrak{p}_i) \cap (S^{-1}\mathfrak{p}_j) = S^{-1}(\mathfrak{p}_i \cap \mathfrak{p}_j) = \emptyset$.
- If $S^{-1}\mathfrak{q}_i \supseteq \cap_{j \neq i} S^{-1}\mathfrak{q}_j$ $(i, j \leq m)$, then
$$\mathfrak{q}_i = (S^{-1}\mathfrak{q}_i)^c \supseteq \Bigg(\bigcap_{j \neq i,\ j \leq m} S^{-1}\mathfrak{q}_j\Bigg)^c = \bigcap_{j \neq i,\ j \leq m} (S^{-1}\mathfrak{q}_i)^c \supseteq \bigcap_{j \neq i} \mathfrak{q}_j.$$
This is not possible, so $S^{-1}\mathfrak{q}_i \not\supseteq \cap_{j \neq i} S^{-1}\mathfrak{q}_j$ $(i, j \leq m)$.
- This shows that $S^{-1}\mathfrak{a} = \cap_{i=1}^{m} S^{-1}(\mathfrak{q}_i)$ is a minimal primary decomposition of $S^{-1}\mathfrak{a}$.

□

Proof of Proposition 4.9, Continued.

- As $(S^{-1}\mathfrak{q}_i)^c = \mathfrak{q}_i$ for $i \leq m$, we get

  $$S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^c = \left(\cap_{i=1}^m S^{-1}\mathfrak{q}_i\right)^c = \cap_{i=1}^m \left(S^{-1}\mathfrak{q}_i\right)^c = \cap_{i=1}^m \mathfrak{q}_i.$$

- This gives a primary decomposition of $S(\mathfrak{q})$.
- This is a minimal decomposition, since the primary decomposition $\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$ is minimal.

The proof is complete. □

Primary Decomposition

Definition

Let $\mathfrak{a}$ be a decomposable ideal. A set Σ of prime ideals belonging to $\mathfrak{a}$ is called *isolated* if, for any prime ideal $\mathfrak{p}'$ belonging to $\mathfrak{a}$, we have

$$\mathfrak{p}' \subseteq \mathfrak{p} \text{ for some } \mathfrak{p} \in \Sigma \implies \mathfrak{p}' \in \Sigma.$$

Remark

If $\Sigma = \{\mathfrak{p}\}$, then Σ is isolated if and only if $\mathfrak{p}$ is minimal.

Reminder (see Proposition 1.11)

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals and $\mathfrak{a}$ an ideal in A. Then

$$\mathfrak{a} \subseteq \bigcup \mathfrak{p}_i \implies \exists i \text{ such that } \mathfrak{a} \subseteq \mathfrak{p}_i.$$

Equivalently,

$$\mathfrak{a} \not\subseteq \mathfrak{p}_i \ \forall i \implies \mathfrak{a} \not\subseteq \bigcup \mathfrak{p}_i.$$

Primary Decomposition

Facts

Let $\mathfrak{a}$ be a decomposable ideal and Σ an isolated set of prime ideals belonging to $\mathfrak{a}$. Set

$$S = A \setminus \left(\bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \right) = \bigcap_{\mathfrak{p} \in \Sigma} (A \setminus \mathfrak{p}).$$

- S is a multiplicative closed subset of A, since this is the intersections of such subsets.
- Let $\mathfrak{p}'$ be a prime ideal belonging to $\mathfrak{a}$. If $\mathfrak{p}' \in \Sigma$, then $\mathfrak{p}' \cap S = \emptyset$.
- Moreover, by Proposition 1.11:

$$\mathfrak{p}' \notin \Sigma \implies \mathfrak{p}' \not\subseteq \bigcup_{p \in \Sigma} \mathfrak{p} \implies \mathfrak{p}' \cap S \neq \emptyset.$$

  Thus,

$$S \cap \mathfrak{p}' = \emptyset \iff \mathfrak{p}' \in \Sigma.$$

Primary Decomposition

Theorem (2nd Uniqueness Theorem; Theorem 4.10)

Let $\mathfrak{a}$ be a decomposable ideal in A and $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ a minimal primary decomposition. Set $\mathfrak{p}_i = r(\mathfrak{q}_i)$, and let $\Sigma = \{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ be an isolated set of prime ideals belonging to $\mathfrak{a}$. Then $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$ is independent of the decomposition.

In particular, we have:

Corollary (Corollary 4.11)

The isolated primary components (i.e., the components whose radicals are minimal primary ideals belonging to $\mathfrak{a}$) are uniquely determined by $\mathfrak{a}$.

Proof of 2nd Uniqueness Theorem.

Set $S = A \setminus \left(\cup_{\mathfrak{p}\in\Sigma} \mathfrak{p} \right) = A \setminus \left(\cup_{l=1}^{m} \mathfrak{p}_{i_l} \right)$.

- From slide 22 we know that S is multiplicatively closed and $\mathfrak{p}_i \cap S = \emptyset \Longleftrightarrow \mathfrak{p}_i \in \Sigma$.
- Applying Proposition 4.9 then gives
$$S(\mathfrak{a}) = \bigcap_{\mathfrak{p}_i \cap S = \emptyset} \mathfrak{q}_i = \bigcap_{l=1}^{m} \mathfrak{q}_{i_l}.$$
- Observe that S only depends on the prime ideals p_{i_l}. By the 1st uniqueness theorem these prime ideals only depends on $\mathfrak{a}$. Thus, $S(\mathfrak{a})$ depends only on $\mathfrak{a}$.
- It then follows that $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$ only depends on $\mathfrak{a}$, and hence is independent of the decomposition.

The result is proved. □