# WORKSHEET ON PRIMARY DECOMPOSITION, MATH 506, SPRING 2016

DUE FRIDAY, MAY 27

All rings are commutative with 1. Please supply proofs/justifications (and one statement) for all theorems/lemmas/propositions and examples. Remarks are given just for your information, but do pay attention to them too.

## 1. Primary ideals

**Definition 1.1.** An ideal $\mathfrak{a} \in R$ is called *primary* if for any $ab \in \mathfrak{a}$, we have either $a \in \mathfrak{a}$ or $b^n \in \mathfrak{a}$ for some $n > 0$.

**Lemma 1.2.** *An ideal $\mathfrak{a}$ is primary if and only if $R/\mathfrak{a} \neq 0$ and any zero divisor in $R/\mathfrak{a}$ is nilpotent.*

Let $I$ be an ideal in $R$, and let $\phi : R \to R/I$ be the canonical projection. Formulate and prove an addition to the "Correspondence theorem" concerning primary ideals.

**Theorem 1.3.** *(Extension of the Correspondence theorem for ideals)*

**Lemma 1.4.** *Let $\mathfrak{a}$ be a primary ideal. Then* $\operatorname{rad}(\mathfrak{a})$ *is prime.*

**Remark 1.5.** The converse is not true. See Example 1.9.

**Definition 1.6.** If $\mathfrak{a}$ is a primary ideal such that $\operatorname{rad}(\mathfrak{a}) = \mathfrak{p}$ then $\mathfrak{a}$ is called $\mathfrak{p}$-primary.

**Proposition 1.7.** *If* $\operatorname{rad}(\mathfrak{a}) = \mathfrak{m}$ *is a maximal ideal then $\mathfrak{a}$ is $\mathfrak{m}$-primary.*

**Corollary 1.8.** *If $\mathfrak{m}$ is maximal then $\mathfrak{m}^n$ is $m$-primary.*

**Example 1.9.** From Worksheet 1 we know that $\operatorname{rad}(\mathfrak{p}^n) = \mathfrak{p}$ for any prime ideal $\mathfrak{p}$. And yet, the above Corollary does not hold for arbitrary prime ideals. Give an example of a prime ideal $\mathfrak{p}$ such that $\mathfrak{p}^n$ is NOT a primary ideal.

**Lemma 1.10.** *A finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

**Motivational example.** Let $R = \mathbb{Z}$. An ideal $(a)$ if $(p)$-primary if and only if $a = p^n$. Hence, the unique factorization in $\mathbb{Z}$ can be restated as follows: any ideal can be decomposed uniquely as a product (=intersection) of primary ideals. This turns out to be the correct formulation to generalize to arbitrary Noetherian rings.

## 2. Primary decomposition

2.1. **Existence.** From now on assume that $R$ is Noetherian. We'll show that any ideal has a *primary decomposition*, that is, can be expressed as an intersection of primary ideals.

**Definition 2.1.** An ideal $\mathfrak{a}$ is called *irreducible* if $\mathfrak{a} = I \cap J$ for two ideals $I$, $J$, implies that $\mathfrak{a} = I$ or $\mathfrak{a} = J$.

**Lemma 2.2.** *Any ideal in a Noetherian ring is a finite intersection of irreducible ideals.*

**Definition 2.3.** Let $\mathfrak{a}$ be an ideal in $R$. We say that $\mathfrak{a}$ has a primary decomposition if $\mathfrak{a}$ is a finite intersection of primary ideals.

**Theorem 2.4.** *(Existence). Any ideal in a Noetherian ring has a primary decomposition.*

2.2. **Uniqueness (sort of).** Let $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_\ell$ be a primary decomposition. By Lemma 1.10 we can replace the ideals with the same radical with their intersection and still have a primary decomposition. We can also make the decomposition efficient by getting rid of irrelevant ideals - namely, the ones that contain the intersection of the rest of them. We say that a primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_\ell$ is *minimal* if

(1) $\operatorname{rad} \mathfrak{q}_i$ are pair-wise distinct,
(2) $\bigcap\limits_{j \neq i} \mathfrak{q}_i \not\subset \mathfrak{q}_j$ for any $j, 1 \leq j \leq \ell$.

**Definition 2.5.** If $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_\ell$ is a minimal primary decomposition, then the prime ideals $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$ are called the associated primes for $\mathfrak{a}$. The set of all primes associated with $\mathfrak{a}$ is denoted $\operatorname{Ass}(\mathfrak{a})$.

Recall that the quotient ideal $(\mathfrak{a} : \mathfrak{b})$ is defined as $\{y \in R \,|\, y\mathfrak{b} \subset \mathfrak{a}\}$. For $x \in R$, we use a streamlined notation $(\mathfrak{a} : x)$ for $(\mathfrak{a} : (x))$.

**Lemma 2.6.** (1) *"Quotients commute with intersections":* $(\bigcap\limits_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap\limits_i (\mathfrak{a}_i : \mathfrak{b})$
(2) *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal in $R$, and let $x \in \mathfrak{q}$. Then* $(\mathfrak{q} : x) = 1$
(3) *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal in $R$, and let $x \notin \mathfrak{q}$. Then* $\operatorname{rad}(\mathfrak{q} : x) = \mathfrak{p}$.

The associated primes can be equivalently defined as follows:

**Proposition 2.7.** *A prime ideal $\mathfrak{p}$ is an associated prime for $\mathfrak{a}$ if and only if there exists $a \in R/\mathfrak{a}$ such that $\mathfrak{p} = \operatorname{rad}(\operatorname{Ann}_R(a))$.*

*Proof.* Hint: express $\operatorname{rad}(\operatorname{Ann}_R(a))$ as a quotient ideal and use Lemma 2.6. □

**Theorem 2.8.** *(Uniqueness) The set of associated primes does not depend on the primary decomposition.*

**Example 2.9.** The primary decomposition itself is not unique. Let $R = k[x, y]$, and let $\mathfrak{a} = (x^2, xy)$. Show that $\mathfrak{a}$ has two minimal primary decompositions:

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

Determine the set of associated primes of $\mathfrak{a}$.

## 3. Geometric interpretation

Let $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_\ell$ be a primary decomposition, and let $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$. Then $V(\mathfrak{a}) = V(\mathfrak{p}_1) \cup \ldots \cup V(\mathfrak{p}_\ell)$.

**Proposition 3.1.** *There exists a subset $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_N}\} \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell\}$ such that*

$$V(\mathfrak{a}) = V(\mathfrak{p}_{i_1}) \cup \ldots \cup V(\mathfrak{p}_{i_N})$$

*and $V(\mathfrak{p}_{i_1}), \ldots, V(\mathfrak{p}_{i_N})$ are precisely the irreducible components of $V(\mathfrak{a})$.*

**Definition 3.2.** The primes described in the proposition are called the **minimal associated primes** of $\mathfrak{a}$. The other primes appearing as radicals of the ideals in a primary decomposition are called the **embedded associated primes**.

Minimal associated primes are simply the primes which are minimal among all primes containing $\mathfrak{a}$. There is one-to-one correspondence:

$$\boxed{\text{Minimal associated primes of } \mathfrak{a}} \leftrightarrow \boxed{\text{Irreducible components of } V(\mathfrak{a})}$$

**Example 3.3.** *Example of an embedded prime.* Consider the ideal $\mathfrak{a}$ from Example 2.9.

(1) Compute $V(\mathfrak{a})$.
(2) Which associated primes are minimal and which are embedded?
(3) Note that for the embedded prime $\mathfrak{p}$, you have $V(\mathfrak{p})$ a proper subset of an irreducible component of $V(\mathfrak{a})$ (here, the entire $V(\mathfrak{a})$). Hence, the name "embedded" - the corresponding algebraic set embeds into a bigger irreducible subset.

From the geometric prospective, we do not "see" the embedded primes, only the minimal ones. The minimal associated primes are also called *isolated* associated primes.

**Remark 3.4.** The primary decomposition can be done more generally for $R$-modules. What we did here was a special case of modules of the form $R/\mathfrak{a}$.