WORKSHEET ON PRIMARY DECOMPOSITION, MATH 506, SPRING 2012

DUE WEDNESDAY, MAY 16

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 \( a \in R \) is called primary if for any \( ab \in a \), we have either \( a \in a \) or \( b^n \in a \) for some \( n > 0 \).

Lemma 1.2. An ideal \( a \) is primary if and only if \( R/a \neq 0 \) and any zero divisor in \( R/a \) 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 \( a \) be a primary ideal. Then \( \text{rad}(a) \) is prime.

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

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

Proposition 1.7. If \( \text{rad}(a) = m \) is a maximal ideal then \( a \) is \( m \)-primary.

Corollary 1.8. If \( m \) is maximal then \( m^n \) is \( m \)-primary.

Example 1.9. From Worksheet 1 we know that \( \text{rad}(p^n) = p \) for any prime ideal \( p \). And yet, the above Corollary does not hold for arbitrary prime ideals. Give an example of a prime ideal \( p \) such that \( p^n \) is NOT a primary ideal. Since \( \text{rad}(p^n) = p \), this shows that the converse to Lemma 1.4 is not true.

Lemma 1.10. A finite intersection of \( p \)-primary ideals is \( p \)-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 \( a \) is called irreducible if \( a = I \cap J \) for two ideals \( I, J \), implies that \( a = I \) or \( a = J \).

Lemma 2.2. Any ideal in a Noetherian ring is a finite intersection of irreducible ideals.
Definition 2.3. Let $a$ be an ideal in $R$. We say that $a$ has a primary decomposition if $a$ 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 $a = q_1 \cap \ldots \cap q_\ell$ 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 $a = q_1 \cap \ldots \cap q_\ell$ is **minimal** if

1. $\text{rad}(q_i)$ are pair-wise distinct,
2. $\bigcap_{j \neq i} q_j \not\subset q_i$ for any $j, 1 \leq j \leq \ell$.

Definition 2.5. If $a = q_1 \cap \ldots \cap q_\ell$ is a minimal primary decomposition, then the prime ideals $p_i = \text{rad}(q_i)$ are called the associated primes for $a$. The set of all primes associated with $a$ is denoted $\text{Ass}(a)$.

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

Lemma 2.6. (1) “Quotients commute with intersections”: $(\bigcap_i a_i : b) = \bigcap_i (a_i : b)$

(2) Let $q$ be a $p$-primary ideal in $R$, and let $x \in q$. Then $(q : x) = 1$

(3) Let $q$ be a $p$-primary ideal in $R$, and let $x \not\in q$. Then $\text{rad}(q : x) = p$.

The associated primes can be equivalently defined as follows:

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

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

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 $R = \mathbb{k}[x,y]$, and let $a = (x^2, xy)$. Show that $a$ has two minimal primary decompositions:

\[ a = (x) \cap (x^2, xy, y^2) = (x) \cap (x^2, y) \]

Determine the set of associated primes of $a$.

3. **Geometric interpretation**

Let $a = q_1 \cap \ldots \cap q_\ell$ be a primary decomposition, and let $\text{rad}(q_i) = p_i$. Then $V(a) = V(p_1) \cup \ldots \cup V(p_\ell)$.

Proposition 3.1. There exists a subset $\{p_{i_1}, \ldots, p_{i_N}\} \subset \{p_1, \ldots, p_\ell\}$ such that

\[ V(a) = V(p_{i_1}) \cup \ldots \cup V(p_{i_N}) \]

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

Definition 3.2. The primes described in the proposition are called the **minimal associated primes** of $a$. 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 \( a \). There is one-to-one correspondence:

| Minimal associated primes of \( a \) | Irreducible components of \( V(a) \) |

**Example 3.3.** *Example of an embedded prime.* Consider the ideal \( a \) from Example 2.9.

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

From the geometric prospectve, 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 \( R/a \).