5.4. **Primary decomposition.** In a Noetherian ring, the radical of any ideal \( a \) is the intersection of a finite number of prime ideals

\[
\text{rad} \ a = \bigcap p_i
\]

where \( p_i \) are the primes associated with the module \( R/a \). When \( R = K[X_1, \cdots, X_n] \) this corresponds, by the Nullstellensatz, to the decomposition of the corresponding algebraic set \( A = \mathcal{Z}_a(L) \subset L^n \) as a finite union of irreducible sets:

\[
A = \bigcup V_i
\]

The ideal itself is the intersection of corresponding “primary” ideals \( q_i \):

\[
a = \bigcap q_i
\]

The correspondence is that \( \text{rad} q_i = p_i \). Thus every term in the expression (5.1) is the radical of the corresponding term in (5.3). It is interesting that only the minimal primes are needed in (5.1) but all of the primary ideals in (5.3) are needed.

The zero sets for the ideals in (5.3) corresponding to the nonminimal “embedded” associated primes are contained in the union of the others.

5.4.1. **primary submodule.**

**Definition 5.24.** A submodule \( Q \) of an \( R \)-module \( M \) is called **primary** if any zero divisor of \( M/Q \) is also nilpotent on \( M/Q \).

1. \( a \in R \) is a zero divisor of \( M/Q \) iff there is some \( x \in M, x \notin Q \) so that \( ax \in Q \).

2. \( a \in R \) is nilpotent on \( M/Q \) iff some power of \( a \) annihilates \( M/Q \), i.e., \( a^n M \subseteq Q \) for some \( n \geq 1 \). In other words, \( a \in \text{rad} (\text{ann}(M/Q)) \).

Since the set of zero divisors of \( M/Q \) is the union of the associated ideals and \( \text{rad} \text{ann}(M/Q) \) is the intersection of the associated ideals, we have:

\[
\bigcap_{p \in \text{ass}(M/Q)} p = \bigcap_{p \in \text{ass}(M/Q)} p = \text{rad}(\text{ann}(M/Q))
\]

So,

**Proposition 5.25.** \( Q \subseteq M \) is primary if and only if \( M/Q \) has a unique associated prime \( p = \text{rad}(\text{ann}(M/Q)) \).

We call \( p \) the prime belonging to \( Q \) and we say that \( Q \) is \( p \)-primary. In the special case when \( M = R, Q = q \) is an ideal in \( R \) and \( \text{ann}(R/q) = q \). So, \( p = \text{rad} q \). The definition of a primary module translates to the following.
Definition 5.26. An ideal \( q \subset R \) is called primary if wherever \( a, b \in R \), \( ab \in q, b \notin q \Rightarrow a \in \text{rad} \ q \).

Proposition 5.27. The intersection of finitely many \( p \)-primary submodules of \( M \) is \( p \)-primary.

Proof. Suppose that \( Q_1, \cdots, Q_n \) are \( p \)-primary submodules of \( M \). Then \( \text{ass}(M/Q_i) = \{ p \} \). This implies that

\[
\text{ass} \left( \bigoplus M/Q_i \right) = \bigcup \text{ass}(M/Q_i) = \{ p \}
\]

Since \( M/\cap Q_i \) embeds in \( \bigoplus M/Q_i \) it also has \( p \) as its unique associated prime. So, \( \bigcap Q_i \) is \( p \)-primary. \( \square \)

5.4.2. existence of primary decomposition. Suppose that \( N \subseteq M \). Then a primary decomposition of \( N \) is defined to be a minimal expression of the form

\[
N = Q_1 \cap Q_2 \cap \cdots \cap Q_n
\]

where \( Q_i \) are primary submodules of \( M \). By the proposition, the prime ideals \( p_i \) belonging to the \( Q_i \) will be distinct.

Theorem 5.28. Every submodule \( N \subseteq M \) admits a primary decomposition.

Proof. If not, there exists a maximal \( N \) with no primary decomposition. The plan of the proof is to express \( N \) as the intersection of two larger submodules \( N = K \cap I \). By maximality of \( N \), both \( K \) and \( I \) are intersections of primary submodules. This makes \( N \) an intersection of primary submodules and we will be done.

Since \( N \) is a counterexample, it is in particular not primary. So there is an \( a \in R \) which is a zero divisor for \( M/N \) but is not nilpotent on \( M/N \). This gives a sequence of submodules of \( L = M/N \):

\[
\ker a_L \subseteq \ker a_L^2 \subseteq \ker a_L^3 \subseteq \cdots
\]

By the ACC, this sequence stops. So, \( \ker a_L^m = \ker a_L^{m+1} = \cdots \). Let \( K = \ker a_L^m \subseteq M/N \). Since \( a \) is a zero divisor, \( K \neq 0 \). Let \( I = \text{im} a_L^M \).

Since \( a \) is not nilpotent on \( L \), \( I \neq 0 \). But \( K \cap I = 0 \) since any element of the intersection has the form \( a^m x \) and satisfies \( a^m(a^m x) = 0 \) which implies that \( x \in \ker a_L^{2m} = \ker a_L^m \). So, \( a^m x = 0 \).

But \( K = K/N \) and \( I = I/N \) for some \( K, I \subseteq M \). And \( K \cap I = 0 \Rightarrow K \cap I = N \). So we are done. \( \square \)
5.4.3. partial uniqueness of primary decomposition.

**Lemma 5.29.** There is a primary decomposition \( N = Q_1 \cap \cdots \cap Q_n \) which is reduced in the sense that

1. the primes \( p_i \) belonging to \( Q_i \) are all distinct and
2. each of the \( Q_i \) is necessary, i.e., \( N \neq Q_1 \cap \cdots \cap \tilde{Q}_i \cap \cdots \cap Q_n \) for all \( i \).

In the following theorem I used \( N = 0 \) in class. But that seemed to be confusing so I put an arbitrary \( N \). This also explains where “\( L \)” came from.

**Theorem 5.30.** Suppose \( N = Q_1 \cap \cdots \cap Q_n \) is a (reduced) primary decomposition of \( N \subseteq M \). Let \( p_i \) be the prime belonging to \( Q_i \). Then

\[
\text{ass}(M/N) = \{p_1, \ldots, p_n\}
\]

**Proof.** (\( \subseteq \)) Since \( N = Q_1 \cap \cdots \cap Q_n \), we have a monomorphism

\[
M/N \hookrightarrow \bigoplus M/Q_i
\]

So,

\[
\text{ass}(M/N) \subseteq \text{ass} \left( \bigoplus M/Q_i \right) = \bigcup \text{ass}(M/Q_i) = \{p_1, \ldots, p_n\}
\]

(\( \supseteq \)) We want to show that \( p_1 \in \text{ass}(M/N) \). Let

\[
L = Q_2 \cap \cdots \cap Q_n
\]

Then, \( L \cap Q_1 = N \). So, we have a monomorphism \( L/N \hookrightarrow M/Q_1 \). So,

\[
\text{ass}(L/N) \subseteq \text{ass}(M/Q_1) = \{p_1\}
\]

Since \( L \neq N \), \( L/N \) has at least one associated prime (a maximal \( \text{ann}(x) \) where \( x \neq 0 \in L/N \)). Therefore, \( \text{ass}(L/N) = \{p_1\} \). Since \( L/N \subseteq M/N \) this implies that \( p_1 \in \text{ann}(M/N) \).

**Theorem 5.31.** Suppose that \( \text{ann}(M/N) = \{p_1, \ldots, p_n\} \) and \( N = Q_1 \cap \cdots \cap Q_n \), \( N = Q'_1 \cap \cdots \cap Q'_n \) are two primary decompositions of \( N \subseteq M \) where \( Q_i, Q'_i \) are \( p_i \)-primary. Then for every minimal (=isolated) \( p_i \), \( Q_i = Q'_i \).

**Proof.** Suppose that \( p_i \) is minimal. This means that it does not contain any of the other associated primes. So, for \( i \geq 2 \), there exists \( a_i \in p_i \) so that \( a_i \notin p_1 \). This implies that \( a = a_2a_3 \cdots a_n \in p_i \) for \( i \geq 2 \) but \( a \notin p_1 \).

**Claim:** \( Q_1 = \{x \in M \mid a^m x \in N \text{ for some } m > 0\} \). This will prove that \( Q_1 = Q'_1 \) since the expression on the right is independent of the primary decomposition.
Pf: \((\subseteq)\) Let \(x \in Q_1\). Then we want to show that \(a^m x\) lies in each \(Q_i\) for sufficiently large \(m\). This will show that \(a^m x \in \bigcap Q_i = N\). \(x \in Q_1 \Rightarrow a^m x \in Q_1\). For \(i \geq 2\), \(a \in p_i = \text{rad}\ \text{ann}(M/Q_i) \Rightarrow a^m x \in Q_i\).

\((\supseteq)\) Suppose that \(a^m x \in N\). Then \(x \in Q_1\). Otherwise, \(a\) is a zero divisor for \(M/Q_1\) which implies that \(a \in p_1\) which is a contradiction. This proves the claim and the theorem follows.

5.4.4. example. (from Atiyah-Macdonald) In this example, \(p\) is a prime whose square \(p^2\) is not primary. However, \(\text{rad} p^2 = p\).

Let \(R = K[X,Y,Z]/(XY-Z^2)\) and let \(x, y, z\) denote the image of \(X, Y, Z\) in \(R\). Let \(p = (x, z)\). This is a prime ideal in \(R\) since

\[
R/p \cong K[X,Y,Z]/(X,Z) \cong K[Z]
\]

But \(p^2 = (x^2, xz, z^2)\) is not primary since \(xy = z^2 \in p^2\) but \(x \notin p^2\) and no power of \(y\) lies in \(p^2\). Finally, it is clear that \(\text{rad} p^2 = p\). (For any \(w \in p, w^2 \in p^2\). Conversely, \(p^2 \subseteq p \Rightarrow \text{rad} p^2 \subseteq p\.)

The ideal \(p^2\) has two associated primes: \(p\) and the maximal ideal \(m = (x, y, z)\) which contains \(p\). It is easy to verify that these are associated primes since \(p\) is the annihilator of \(z\) module \(p^2\) and \(m\) is the annihilator of \(x\) module \(p^2\). There are no other associated primes because the primary decomposition of \(p^2\) has only two terms:

\[
p^2 = q_1 \cap q_2
\]

where

\[
q_1 = (x) = (x, z^2)
\]

This is \(p\)-primary since \(p/q_1\) is generated by \(z\) with annihilator \(p\). So there is a short exact sequence

\[
0 \rightarrow R/p \rightarrow R/q_1 \rightarrow R/p \rightarrow 0
\]

which implies that \(p\) is the only prime associated to \(R/q_1\) and, therefore, \(q_1\) is \(p\)-primary. The other primary ideal is

\[
q_2 = m^2 = (x^2, xz, z^2, y^2, yz)
\]

This is \(m\)-primary since \(\text{rad} m^2 = m = \cap \{p_2 \in \text{ass}(M/m^2)\}\). Since \(m\) is maximal, \(p_2 = m\) is the only associated prime.

There is a modified version of the powers of a prime ideal \(p\) called the *symbolic power* of \(p\) which always gives a \(p\)-primary ideal. As a special case of HW6, problem 2, this is given by

\[
p^{(2)} = p^2 R_p|R
\]
5.5. \( \text{Spec}(R) \). For any ideal \( I \subset R \) let \( C(I) (= \mathcal{Z}_I) \) be the set of all prime ideals \( p \) of \( R \) which contain \( I \).

**Definition 5.32.** If \( R \) is a Noetherian ring then \( \text{Spec}(R) \) is the set of all prime ideals in \( R \) with the topology given by taking \( C(I) \) (for all ideals \( I \)), the empty set \( \emptyset \) and the whole space \( \text{Spec}(R) \) to be the closed subsets.

Since \( R \) is Noetherian, \( \text{Spec}(R) \) satisfies the DCC for closed subsets. In particular, any collection of closed subsets has a minimal element. To verify that this is a topology we need to show that any intersection or finite union of closed sets is closed. The DCC implies that any intersection is a finite intersection.

The first problem on HW6 was to show that, given any ideal \( I \), the set \( C(I) \) contains a finite number of minimal elements. The fancy proof of this is the following. First, define a closed subset of \( \text{Spec}(R) \) to be *indecomposable* if it is not the union of two proper subsets.

**Lemma 5.33.** \( C(I) = C(\text{rad}(I)) \).

**Lemma 5.34.** \( C(I) \) is indecomposable iff \( \text{rad}(I) \) is prime.

**Lemma 5.35.** In any topological space satisfying the DCC for closed subsets, every closed subset is a finite union of indecomposable closed subsets.

**Theorem 5.36.** For every ideal \( I \), there are finitely many primes \( p_1, \ldots, p_n \) containing \( I \) so that any other prime which contains \( I \) will contain one of the \( p_i \).

**Proof.** Let \( C(I) = C_1 \cup \cdots \cup C_n \) be a decomposition of \( C(I) \) into indecomposables. Then \( C_i = C(p_i) \) for some prime \( p_i \) containing \( I \) and, for any other primes \( P \) containing \( I \) we have that \( C(P) \subseteq C(I) \) and therefore,

\[
C(P) = (C(P) \cap C_1) \cup \cdots \cup (C(P) \cap C_n)
\]

Since \( C(P) \) is indecomposable, this implies that \( C(P) \subseteq C_i = C(p_i) \) and this implies that \( P \) contains \( p_i \). \( \square \)