Irena Swanson

Primary decompositions

The aim of these lectures is to show that primary ideals, and also primary modules, are an important tool for solving problems, proving theorems, understanding the structure of rings, modules, and ideals, and that there are enough of them to be able to apply the theory.

Table of contents

1. Primary ideals

This section contains the basic definitions. Throughout all rings are commutative with identity, and most of them are Noetherian.

Definition 1.1. An ideal I in a ring R is *primary* if $I \neq R$ and every zerodivisor in R/I is nilpotent.

Examples 1.2. Here are some examples of primary ideals:

1. Any prime ideal is primary.
2. For any prime integer p and any positive integer n, $p^n\mathbb{Z}$ is a primary ideal in $\mathbb{Z}$.
3. More generally, let $\mathfrak{m}$ be a maximal ideal in a Noetherian ring R. Let I be any ideal in R such that $\sqrt{I} = \mathfrak{m}$. Then I is a primary ideal. Namely, if $r \in R$ is a zerodivisor modulo I, then as R/I is Artinian with only one maximal ideal, necessarily the image of r is in this maximal ideal. But then a power of r lies in I.

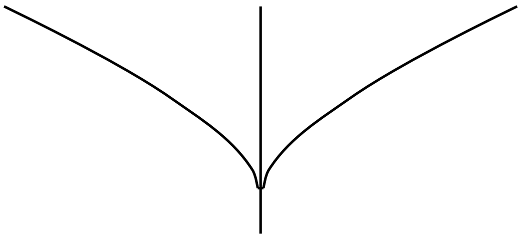
Lemma 1.3. Let I be a primary ideal in a ring R. Then $\sqrt{I}$ is a prime ideal.

Proof: Let $r, s \in R$ such that $rs \in \sqrt{I}$. Then there exists a positive integer n such that $r^n s^n = (rs)^n \in I$. If $s^n \in I$, then $s \in \sqrt{I}$, and we are done. So suppose that $s^n \notin I$. As $r^n s^n \in I$ and as I is primary, r^n is nilpotent on R/I. Thus $r \in \sqrt{I}$. □

Definition 1.4. Let I be a primary ideal in R and $P = \sqrt{I}$. Then I is also called *P-primary.*

The condition that $\sqrt{I}$ be a prime ideal P does not guarantee that I is P-primary, or primary at all. For example, let $R = k[X, Y]$ be a polynomial ring in variables X and Y over a field k. Let I be the ideal (X^2, XY). Then $\sqrt{I} = (X)$ is a prime ideal in R. However, I is not primary as Y is a zerodivisor on R/I, but it is not nilpotent.

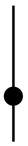
In algebraic geometry an algebraic set (a variety) can be decomposed as a union of irreducible algebraic sets. In the standard correspondence between algebraic sets and ideals, algebraic sets correspond to radical ideals and irreducible algebraic sets correspond to prime ideals. Thus the decomposition of algebraic sets into irreducible ones corresponds to writing a radical ideal as an intersection of prime ideals. For example, the zero set of $X^3 - XY^3$ in $\mathbb{R}^2$ can be drawn as



Clearly this algebraic set is the union of the vertical line $X = 0$ and the curve $X^2 - Y^3 = 0$, which correspond to prime ideals (X) and $(X^2 - Y^3)$. Thus $(X^3 - XY^3) = (X) \cap (X^2 - Y^3)$ reflects the primary (even prime) decomposition.

Now here are two ways to draw the zero set of the polynomials in the ideal (X^2, XY):

and



In the picture on the right we are emphasizing that the functions X^2, XY vanish at the origin $(0, 0)$ to order 2. Clearly $(X^2, XY) = (X) \cap (X^2, XY, Y^2)$. The vanishing along the line $X = 0$ to order 1 is encoded in the intersectand (X), and the vanishing to second order at the origin is expressed by the intersectand $(X, Y)^2 = (X^2, XY, Y^2)$. Indeed, $(X^2, XY) = (X) \cap (X^2, XY, Y^2)$ is a primary decomposition.

Thus primary decompositions can contain also the information on the vanishing along the components, even the embedded ones. More generally there is the famous Zariski-Nagata theorem:

Theorem 1.5. (Zariski, Nagata) *Let k be an algebraically closed field of characteristic zero and R a polynomial ring over k. Let P be a prime ideal in R. For all positive integers n, let P_n be the set of all elements of R which vanish along* *the zero set of P to order at least n. Then P_n equals the smallest P-primary ideal containing P^n.*

Remark 1.6. The smallest P-primary ideal containing P^n is called the *nth symbolic power of* P, and it exists in every Noetherian ring. We will prove this existence in Section 3 as a consequence of the existence of primary decompositions.

2. Primary modules

One can, more generally, develop the analogous theory for modules. We proceed to do so not just for the sake of generality, but because we will need the results for modules to establish the desired results for ideals. See for example proof of Proposition : the result for ideals uses the theory of primary decompositions for modules.

Definition 2.1. Let R be a Noetherian ring and M a finitely generated R-module. A submodule N of M is said to be *primary* if $N \neq M$ and whenever $r \in R$, $m \in M \setminus N$, and $rm \in N$, then there exists a positive integer n such that $r^n M \subseteq N$.

In other words, N is primary in M if and only if for any $r \in R$, whenever multiplication by r on M/N is not injective, then it is nilpotent as a function.

Observe that N is primary in M if and only if 0 is primary in M/N.

Here are some examples of primary modules:

1. If I is a primary ideal in a ring R, then I is also a primary submodule of R, when the ring is thought of as a module over itself.
2. If P is a prime ideal in a ring R, then for any positive integer n, $P \oplus \cdots \oplus P$ (n copies) is a primary submodule of R^n.

Lemma 2.2. Let $N \subseteq M$ be a primary submodule. Then $\sqrt{N :_R M}$ is a prime ideal.

Proof: Let $r, s \in R$ such that $rs \in \sqrt{N :_R M}$. Then there exists a positive integer n such that $(rs)^n \in N :_R M$. Thus $r^n s^n M \subseteq N$. If $s^n M \subseteq N$, then $s \in \sqrt{N :_R M}$, and we are done. So suppose that $s^n M \not\subseteq N$. Choose $m \in M$ such that $s^n m \notin N$. Then $r^n(s^n m) \in N$, so that as N is primary in M, multiplication by r^n on M/N is nilpotent. Thus $r \in \sqrt{N :_R M}$. □

Definition 2.3. Let $N \subseteq M$ be a primary submodule. Then N is also called *P-primary*, where P is the prime ideal $P = \sqrt{N :_R M}$.

Primary modules generalize the notion of primary ideals, and here is another connection:

Lemma 2.4. Let R be a ring, P a prime ideal in R, M an R-module, and N a P-primary submodule of M. Then $N :_R M$ is a P-primary ideal.

Proof: Set $I = N :_R M$. Then by definition, $\sqrt{I} = P$. Let $r, s \in R$ such that $rs \in I$ and $s \notin P$. As P is a prime ideal, then $r \in P$. Hence for some positive integer n, $r^n \in I$. Choose n to be smallest possible. Then $r^{n-1}M \not\subseteq N$. Choose $m \in M$ such that $r^{n-1}m \notin N$. If $n > 1$, as $sr^{n-1}m \in N$, it follows that $s^l M \subseteq N$ for some positive integer l, whence $s^l \in I \subseteq P$, which is a contradiction. So necessarily $n = 1$, so $r \in I$. □

The converse fails in general:

Example 2.5. Let R be a Noetherian ring, $P \subsetneq Q$ prime ideals, $M = R \oplus R$, $N = P \oplus Q$. Then $N :_R M = P$, but N is not P-primary. Namely, choose $r \in Q \setminus P$, and set $m = (0, 1) \in M \setminus N$. Then $rm \in N$, yet $r^n(1, 0)$ is not in N for any n, so that $r^n M$ is not a submodule of N for any n.

Lemma 2.6. The intersection of any two P-primary submodules of M is P-primary.

Proof: Let N, N' be P-primary submodules. Let $r \in R$. Let $m \in M \setminus N \cap N'$ such that $rm \in N \cap N'$. By assumption $m \notin N$ or $m \notin N'$. But both N and N' are primary. If $m \notin N$, then $r^n M \subseteq N$ for all large n, and if $m \notin N'$, then $r^n M \subseteq N'$ for all large n. In any case, a power of r is in P, thus $r \in P$. It follows that $r \in \sqrt{(N : M)} \cap \sqrt{N' : M} = \sqrt{(N : M) \cap (N' : M)} = \sqrt{(N \cap N') : M}$, so that $r^n M \subseteq N \cap N'$ for all large n. Thus $N \cap N'$ is primary to P. □

Lemma 2.7. Let R be a ring, P a prime ideal, M an R-module, and N a P-primary submodule of M. Then for any $r \in R$,

$$N :_M r = \begin{cases} N, & \text{if } r \notin P \\ M, & \text{if } r \in N :_R M \\ \text{a } P\text{-primary submodule of } M \text{ strictly containing } N, & \text{if } r \in P \setminus (N :_R M) \end{cases}$$

Proof: First assume that r is not in P. Let $m \in (N :_M r) \setminus N$. Then $rm \in N$, and by definition of primary modules, $r^n \in N :_R M \subseteq P$ for some positive integer n. Thus $r \in P$, contradiction. Thus $N :_M r = N$ whenever $r \notin P$.

If $r \in N :_R M$, clearly $N :_M r = M$.

Now assume that $r \in P \setminus (N :_R M)$. Let $x \in R$ and $m \in M \setminus (N :_M r)$ such that $xm \in N :_M r$. Then $rm \notin N$ and $xrm \in N$. As N is P-primary, $x^n M \subseteq N$ for some positive integer n. This means that $x \in P$ and that $x^n M \subseteq N :_M r$, so that $N :_M r$ is P-primary. Furthermore, $r \notin N :_R M$, and by definition of P-primary, $r^n \in N :_R M$ for some n. Let n be minimal such integer. Then $n > 1$, and there exists $m \in M$ such that $r^{n-1}m \notin N$. Thus $N :_M r$ contains N and $r^{n-1}m$, so that it contains N properly. □

Lemma 2.8. Let R be a ring, P a prime ideal, and M an R-module. Assume that N is a P-primary submodule of M. Then for any $m \in M$,

$$N :_R m = \begin{cases} R, & \text{if } m \in N; \\ \text{a } P\text{-primary ideal containing } N :_R M, & \text{if } m \notin N. \end{cases}$$

Moreover, if P is finitely generated, there exists $m \in M$ such that $N : m = P$.

Proof: Certainly $N :_R m = R$ if $m \in N$. Now assume that $m \in M \setminus N$. Let $x, y \in R$ such that $xy \in N :_R m$. Assume that $y \notin N :_R m$. Then $ym \notin N$ and $xym \in N$, so that by the definition of primary modules, $x^n M \subseteq N$ for some n. Thus $x^n \in N :_R M \subseteq P$, which proves that $N :_R m$ is a P-primary ideal.

Now assume that P is finitely generated. As N is P-primary in M, by the previous part, $N :_R m$ is P-primary. As P is finitely generated, there exists a positive integer n such that $P^n \subseteq N :_R m$. Choose n to be smallest integer with this property. Then $n \geq 1$, and there exists $r \in P^{n-1}$ such that $r \notin N :_R m$. Then $N :_R rm = (N :_R m) :_R r$ is P-primary by Lemma 0.7, and as it contains P, it equals P. □

Lemma 2.9. Let R be a ring, U a multiplicatively closed subset of R, and $N \subseteq M$ R-modules.

(1) If N is primary in M and $(N :_R M) \cap U \neq \emptyset$, then $U^{-1}N = U^{-1}M$.
(2) If N is primary in M and $(N :_R M) \cap U = \emptyset$, then $U^{-1}N$ is primary in $U^{-1}M$.
(3) There is a one-to-one correspondence between primary submodules N of M such that $(N :_R M)$ is disjoint from U and primary submodules of $U^{-1}M$. The correspondence is given by $N \mapsto U^{-1}N$ for N a submodule in M, and $K \mapsto K \cap M$ for K a submodule of $U^{-1}M$.

Proof: Let N be a primary submodule in M. Part (1) follows trivially. Assume hypotheses of (2). Let $x \in R$, $m \in M$, $u, v \in U$, such that $(x/u)(m/v) \in U^{-1}N$. Assume that $m/v \notin U^{-1}N$. Then $m \notin N$, and there exists $w \in U$ such that $wxm \in N$. Thus $(wx)^n M \subseteq N$ for some integer n, and $wx \in \sqrt{N :_R M}$, which is a prime ideal. But by the assumption on U then $x \in \sqrt{N :_R M}$. Hence x/u is in the radical of $U^{-1}N :_{U^{-1}R} U^{-1}M$, which proves that $U^{-1}N$ is primary to $U^{-1}P$.

Now let K be primary in $U^{-1}M$, and set $N = K \cap M$. Then $N \neq M$. Let $m \in M \setminus N$ and $r \in R$ such that $rm \in N$. Then $m \notin K$ and $rm \in U^{-1}N \subseteq K$. Thus for some positive integer n, $r^n U^{-1}M \subseteq K$. Thus $r^n M \subseteq K \cap M = N$, which proves that N is primary.

Furthermore, it is always true that $N \subseteq U^{-1}N \cap M$ and $U^{-1}(K \cap M) = K$. If $m \in U^{-1}N \cap M$, then $wm \in N$ for some $w \in U$. If $m \notin N$, then $w \in N :_M m$, which is in $\sqrt{N :_R M}$ by Lemma 0.8. But this contradicts the assumption that N is primary to a prime ideal disjoint from U. This establishes the one-to-one correspondence. □

Thus the primary property is preserved under many localizations. It is also preserved under passage to a polynomial extension:

Proposition 2.10. Let R be a ring, X a variable over R, M an R-module and N a primary submodule. Then $NR[X]$ is a primary $R[X]$-submodule of $MR[X]$. Furthermore, if N is a P-primary submodule of M, then $NR[X]$ is $PR[X]$-primary submodule of $MR[X]$.

Proof: It is easy to see that $NR[X] \neq MR[X]$. Let $m \in MR[X] \setminus NR[X]$, $r \in R[X]$ such that $rm \in NR[X]$. Write $r = \sum_{i=j_0}^{j_1} r_i X^i$, $m = \sum_{i=k_0}^{k_1} s_i X^i$, for some $r_i \in R$, $s_i \in M$, with $r_{j_1} \neq 0$, $s_{k_1} \notin N$. We proceed by induction on $j_1 - j_0$. As $rm \in NR[X]$, then $r_{j_1} s_{k_1} \in N$. As N is primary in M, there exists a positive integer n such that $r_{j_1}^n \in N :_R M$. In particular, $r_{j_1}^n m \in NR[X]$. Let a be the smallest integer such that $r_{j_1}^a m \in NR[X]$. Then $a \geq 1$ and $r_{j_1}^{a-1} m \notin NR[X]$. Set $m' = r_{j_1}^{a-1} m$. Then $rm' \in NR[X]$, and $r_{j_1} X^{j_1} m' \in NR[X]$. It follows that $(r - r_{j_1} X^{j_1}) m' \in NR[X]$. But $r - r_{j_1} X^{j_1}$ has strictly fewer terms than r, so by induction, $r - r_{j_1} X^{j_1} \in \sqrt{NR[X] :_{R[X]} MR[X]}$. Thus $r \in \sqrt{NR[X] :_{R[X]} MR[X]}$. The last part follows easily. □

It is not true that the passage to a faithfully flat extension preserves the primary property. For example, let R be the ring $\mathbb{R}[X]/(X^2+1)$. Let S be $\mathbb{C}[X]/(X^2+1)$. Then S is a faithfully flat extension of R. In R, the zero ideal is a prime ideal, hence primary. However, the zero ideal in S is not primary, as X^2+1 factors over $\mathbb{C}$ into two distinct irreducible factors.

3. Primary decompositions

Definition 3.1. Let R be a ring, M an R-module and N a submodule. A *primary decomposition* of N is an expression of N as a finite intersection of primary submodules of M. In other words, a primary decomposition of N is $N = N_1 \cap \cdots \cap N_s$, where each N_i is primary in M.

Note that N has a primary decomposition $N = N_1 \cap \cdots \cap N_s$ if and only if 0 in M/N has a primary decomposition $0 = N_1/N \cap \cdots \cap N_s/N$.

Primary decompositions exist for Noetherian modules, as we prove below.

Most of the time we will work with ideals, so for emphasis we state explicitly the definition of primary decompositions for ideals:

Definition 3.2. Let I be an ideal in a ring R. A decomposition $I = \bigcap_{i=1}^{s} q_i$ is a *primary decomposition* of I if the $q_1, \ldots, q_s$ are primary ideals.

One of course wants a constructive method to obtain primary decompositions. The following lemma is a step in that direction:

Lemma 3.3. Let R be a ring, M a Noetherian R-module, N a submodule of M, and $r \in R$. Then there exists a positive integer n such that $N :_M r^n = N :_M r^{n+1}$, and then for all $m \geq n$, $N :_M r^m = N :_M r^n$ and $N = (N :_M r^m) \cap (N + r^m M)$.

Proof: For any elements $r, s \in R$, $N :_M r \subseteq N :_M rs$. In particular, $N \subseteq N :_M r \subseteq N :_M r^2 \subseteq \cdots$ is an ascending chain of submodules in M. As M is Noetherian, there exists n such that $N :_M r^n = N :_M r^{n+1}$. Assume that $m > n + 1$. If $s \in N :_M r^m$, then $r^{m-1} rs \in N$, so by induction on m, $r^n rs \in N$, whence $r^n s \in N$. This proves that $N :_M r^n = N :_M r^m$ for all $m \geq n$.

Certainly $N \subseteq (N : r^m) \cap (N + r^m M)$. Let $s \in (N : r^m) \cap (N + r^m M)$. Write $s = a + r^m b$ for some $a \in N$ and $b \in M$. Then $sr^m = ar^m + r^{2m} b \in N$, so that $r^{2m} b \in N$. By the first part then $r^m b \in N$, so that $s = a + r^m b \in N$. Thus $N = (N : r^m) \cap (N + r^m M)$. □

In general, an ascending chain of submodules in a Noetherian module need not stabilize as soon as two consecutive submodules are equal, but the proof above shows that this is the case for the chain $N \subseteq N :_M r \subseteq N :_M r^2 \subseteq N :_M r^3 \subseteq N :_M r^4 \subseteq \cdots$. This makes the computation of its stable value feasible.

The stable value of the chain $N \subseteq N :_M r \subseteq N :_M r^2 \subseteq N :_M r^3 \subseteq \cdots$ is typically denoted as $N :_M r^\infty$, but no meaning is attached to the notation r^∞. If I is an ideal, the stable value of $I \subseteq I : r \subseteq I : r^2 \subseteq I : r^3 \subseteq \cdots$ is similarly denoted as $I : r^\infty$.

Theorem 3.4. *Let R be a ring, and M a Noetherian R-module. Then any proper submodule N of M has a primary decomposition.*

In particular, every proper ideal I in a Noetherian ring R has a primary decomposition.

Proof: If N is primary, we are done. So assume that N is not primary. Let $r \in R$, $m \in M \setminus N$ such that $rm \in N$ and $r^n M \not\subseteq N$ for any positive integer n. As M is Noetherian, the chain $N \subseteq N :_M r \subseteq N :_M r^2 \subseteq \cdots$ terminates. Choose n such that $N :_M r^n = N :_M r^{n+1} = \cdots$. Let $N' = N :_M r^n$, $N'' = (N + r^n M)$. Then both N' and N'' properly contain N. By Lemma 0.3, $N = N' \cap N''$, so it suffices to find primary decompositions of N' and N''. But this we can do by Noetherian induction. □

We summarize the procedure from the proof above formally for the case of ideals:
Procedure 3.5. Let I be an ideal in a Noetherian ring R, and $r, s \in R$ such that $r \notin \sqrt{I}$, $s \notin I$, $rs \in I$.

1. Find n such that $I : r^\infty = I : r^n$.
2. Set $I' = I + (r^n)$, $I'' = I : r^n$. Then $I = I' \cap I''$.
3. To find a primary decomposition of I, it suffices to find primary decompositions of strictly larger ideals I' and I''.

Note that Procedure 0.5 does not say how one can find the appropriate zero divisors r, s modulo an ideal in order to compute its primary decomposition. Furthermore, the procedure gives no indication on how to determine whether an ideal is primary.

Nevertheless, the procedure can be used successfully to compute some examples:
Example 3.6. Let I be the ideal $I = (X^2, XY)$ in the polynomial ring $k[X, Y]$. Observe that $X \notin I$, $Y \notin \sqrt{I} = (X)$, but that $XY \in I$. So by Procedure 0.5, we need to find $I : Y^\infty$. Clearly $I : Y = (X) = I : Y^\infty$, so, as in the proof, $I = (I : Y^\infty) \cap (I + (Y)) = (X) \cap (X^2, Y)$. But (X) is prime, hence primary, and (X^2, Y) is primary by Example 0.2 (3), as its radical is a maximal ideal. Thus $(X) \cap (X^2, Y) = I$ is a primary decomposition of I.

If we repeat the same procedure with elements X and Y^n in place of X and Y, then we obtain the decomposition $I = (X) \cap (X^2, XY, Y^n)$, which is a primary decomposition by the same reasoning as the one above.

This example shows that primary decompositions are not unique. See Lemma for a formalization of this.

If, furthermore, we repeat the procedure above with elements X and $Y(Y-1)$ in place of X and Y, then we obtain the decomposition $I = (X) \cap (X^2, XY, Y(Y-1))$. The component (X) is primary, but the component $J = (X^2, XY, Y(Y-1))$ is not: $Y(Y-1) \in J$, $Y \notin J$ and $Y - 1 \notin \sqrt{J} = (X, Y(Y-1))$. Then $J : (Y-1)^\infty = (X^2, Y) = J : (Y-1)$ is primary, and $J + (Y-1) = (X, Y-1)$ is also primary as it is a prime ideal. Thus by Lemma 0.3 or by Procedure 0.5, $J = (X^2, Y) \cap (X, Y-1)$, whence $I = (X) \cap (X^2, Y) \cap (X, Y-1)$ is also a primary decomposition.

However, observe that the component $(X, Y-1)$ in the last decomposition is redundant as it contains the component (X). We next formalize the notion of irredundancy or minimality:

Definition 3.7. A primary decomposition $N = N_1 \cap \cdots \cap N_s$ of a submodule N of M is *irredundant* or *minimal* if

(1) the prime ideals $\sqrt{N_1 :_R M}, \ldots, \sqrt{N_s :_R M}$ are distinct, and
(2) for all $j = 1, \ldots, s$, $N \neq \displaystyle\bigcap_{i \neq j} N_i$.

Explicitly for ideals, a primary decomposition $I = q_1 \cap \cdots \cap q_s$ of ideal I is an *irredundant* or *minimal* decomposition if $\sqrt{q_1}, \ldots, \sqrt{q_s}$ are all distinct, and for any $i \in \{1, \ldots, s\}$, $\cap_{j \neq i} q_j \neq I$.

Irredundant decompositions exist whenever primary decompositions exist:

Proposition 3.8. Let R be a ring, M an R-module and N a submodule of M. If N has a primary decomposition, then N has an irredundant primary decomposition.

Proof: Write $N = N_1 \cap \cdots \cap N_s$, with each N_i primary. By Lemma 0.6, we may combine any two N_i with the same radical to obtain another primary module. Thus once a primary decomposition is given, a primary decomposition satisfying (1) is easy to obtain. If for some j, the condition (2) is not satisfied, then we remove the jth component from the decomposition. By repeating this step, in finitely many steps we obtain a primary decomposition satisfying (1) and (2). □

Proposition 3.9. Let $N \subseteq M$ be modules over a ring R. Assume that N has an irredundant primary decomposition $N = N_1 \cap \cdots \cap N_s$. Then

$$\{\sqrt{N_i :_R M} \mid i = 1, \ldots, s\} = \{P \in \operatorname{Spec} R \mid P \text{ is minimal over } N :_R m \text{ for some } m \in M\}.$$

This set is independent of the irredundant primary decomposition and contains all prime ideals in R which are minimal over $N :_R M$.

If R is Noetherian, then

$$\{\sqrt{N_i :_R M} \mid i = 1, \ldots, s\} = \{P \in \operatorname{Spec} R \mid P = N :_R m \text{ for some } m \in M\}.$$

Proof: For $j = 1, \ldots, s$, let $P_j = \sqrt{N_j :_R M}$. By Lemma 0.2, P_j is a prime ideal.

For each $j \in \{1, \ldots, s\}$, choose $m_j \in \cap_{i \neq j} N_i \setminus N_j$. Then $N :_R m_j = \bigcap_i (N_i : m_j) = N_j : m_j$, which is primary to P_j by Lemma 0.8. Thus by the same lemma, if R is Noetherian, there exists $m \in M$ such that $N :_R m = P$. This proves that each P_j is in the set $\{P \in \operatorname{Spec} R \mid P \text{ is minimal over } N : m \text{ for some } m \in M\}$, or in case of Noetherian ring, in the set $\{P \in \operatorname{Spec} R \mid P = N : m \text{ for some } m \in M\}$.

Now let P be a prime ideal minimal over $N : m$ for some $m \in M$. Then P is minimal over $N : m = \bigcap_{i=i}^{s} (N_i : m)$, so necessarily there exists $j \in \{1, \ldots, s\}$ such that P is minimal over $N_j : m$. But then by Lemma 0.8, necessarily $P = P_j$. This proves the displayed equality, and hence that the set is independent of the irredundant primary decomposition.

Now assume that P is minimal over $N :_R M$. As $N :_R M = \bigcap_i (N_i :_R M)$, it follows that P is minimal over some $N_j :_R M$. But then by Lemma 0.2, $P = P_j$. □

The unique set in the theorem above has a name:

Definition 3.10. Let $N \subseteq M$ be modules over a ring R. The set

$$\{P \in \operatorname{Spec} R \mid P \text{ is minimal over } N :_R m \text{ for some } m \in M\}$$

is called *the set of weakly associated primes of* M/N, and is denoted $\widetilde{\operatorname{Ass}}(M/N)$.

If I is an ideal, *the weakly associated primes of the ideal* I are the weakly associated primes of the module R/I.

Note that $\widetilde{\operatorname{Ass}}(M/N)$ does not depend on N and M, but only on the module M/N. Thus to simplify notation, from now on we will usually talk about (weakly) associated primes and primary decompositions of the zero submodule in a module. Sometimes, for clarity, if M is a module over two rings, we will write $\widetilde{\operatorname{Ass}}_R(M)$ to denote the set of weakly associated primes of M as an R-module.

It is possible that the zero submodule of M does not have a primary decomposition, yet one can define associated primes of M.

Remark 3.11. There are several variant definitions of *associated primes* in the literature. The following are from Iroz-Rush and Divaani-Aazar-Tousi :

(1) If P is minimal over $0 :_R m$ for some $m \in M$, then P is, as above, called a *weakly associated prime* of M. Sometimes P is also called a *weak Bourbaki prime* of M.
(2) If P equals $0 :_R m$ for some $m \in M$, then P is called an *associated prime* of M, or a *Bourbaki prime* of M.
(3) If P is a Bourbaki prime of $M/0_P \cap M$, then P is called a *Noether prime* of M.
(4) If $0 :_R m$ is P-primary for some $m \in M$, then P is called a *Zariski-Samuel prime* of M.
(5) If for every $x \in P$ there exists $m \in M$ such that $x \in 0 :_R m \subseteq P$, then P is called a *Krull prime* of M.
(6) If for every finitely generated ideal $I \subseteq P$ there exists $m \in M$ such that $I \subseteq 0 :_R m \subseteq P$, then P is called a *strong Krull prime* of M.
(7) If there exists a multiplicatively closed subset U of R such that $U^{-1}P$ is a maximal ideal in the set of zerodivisors in $U^{-1}R$ on $U^{-1}M$, then P is called a *Nagata prime* of M.
(8) If there exists a submodule N of M such that $P = 0 :_R N$, then P is called a *Divaani-Aazar-Tousi prime* of M.

By convention, the zero module has no associated primes of any type.

All the primes above are the same if R is Noetherian and M is finitely generated, see Exercise 3.12. But these notions need not agree in general. For example, let k be a field and $t, x_1, x_2, \ldots, y_1, y_2, \ldots$ variables over k. Let

$$R = k[t, x_1, y_1, x_2, y_2, \ldots]/(tx_iy_i \mid i)(y_i^i \mid i),$$

$P = (x_i \mid i)R$, and $Q = (y_i \mid i)R$. Then P is minimal over $0 :_R ty_1$, but P is not the radical of $0 :_R m$ for any $m \in M$. Also, Q is the radical of $0 : tx_1y_1$ but Q is not $0 : N$ for any $N \subseteq M$.

For Noetherian rings and modules at least, the following definition of associated primes is more standard:

Definition 3.12. Let $N \subseteq M$ be modules over a ring R. The set

$$\{P \in \operatorname{Spec} R \mid P = N :_R m \text{ for some } m \in M\}$$

is called *the set of associated primes of* M/N, and is denoted $\operatorname{Ass}(M/N)$ or $\operatorname{Ass}_R(M/N)$ to make the underlying ring clear. If I is an ideal, *the associated primes of the ideal* I are the associated primes of the module R/I.

Associated primes and primary decompositions localize in a natural way:

Corollary 3.13. Let M be an R-module, and U any multiplicatively closed subset of R. Then

$$\widetilde{\operatorname{Ass}}(U^{-1}(M)) = \{U^{-1}P \mid P \in \widetilde{\operatorname{Ass}}(M), P \cap U = \emptyset\},$$

and if R is Noetherian,

$$\operatorname{Ass}(U^{-1}(M)) = \{U^{-1}P \mid P \in \operatorname{Ass}(M), P \cap U = \emptyset\}.$$

If 0 has an irredundant primary decomposition $0 = \bigcap_i N_i$, then

$$U^{-1}0 = \bigcap_{U \cap (N_i :_R M) = \emptyset} U^{-1}N_i$$

is an irredundant primary decomposition if $U^{-1}0 \neq U^{-1}M$.

Proof: Let $P \in \widetilde{\operatorname{Ass}} M$ (resp. in $\operatorname{Ass} M$). Then there exists $m \in M$ such that P is minimal over $0 :_R m$ (resp. $P = 0 :_R m$). If $U \cap P = \emptyset$, then $U^{-1}P$ is minimal over $U^{-1}0 :_{U^{-1}R} m$ (resp. $U^{-1}P = U^{-1}0 :_{U^{-1}R} m$). Thus $U^{-1}P \in \widetilde{\operatorname{Ass}} U^{-1}M$, (resp. $U^{-1}P \in \operatorname{Ass} U^{-1}M$).

Now let $U^{-1}P \in \widetilde{\operatorname{Ass}} U^{-1}M$ (resp. in $\operatorname{Ass} U^{-1}M$). Then $P \cap U = \emptyset$ and there exists $m \in M$ such that $U^{-1}P$ is minimal over $U^{-1}0 :_{U^{-1}R} m$ (resp. $U^{-1}P = U^{-1}0 :_{U^{-1}R} m$). But then P is minimal over $0 :_R m$, and in particular $P \in \widetilde{\operatorname{Ass}} M$. If R is Noetherian, then by Proposition 0.9, $P \in \operatorname{Ass}(0 :_R m)$, hence in $\operatorname{Ass} M$.

This proves that the (weakly) associated primes localize as stated.

Now let $0 = \bigcap_i N_i$ be an irredundant primary decomposition. Let $P_i = \sqrt{N_i :_R M}$. By Proposition 0.9, $P_1, \ldots, P_s$ are the weakly associated primes of M. After reindexing, assume that $P_i \cap U = \emptyset$ for $i = 1, \ldots, r$, and that $P_i \cap U \neq \emptyset$ for $i = r+1, \ldots, s$. By Lemma 0.9, $U^{-1}N_i$ is primary to $U^{-1}P_i$ for $i = 1, \ldots, r$, and $U^{-1}N_i$ is $U^{-1}M$ for $i > r$.

Localize the primary decomposition at U: as $U^{-1}0 \neq U^{-1}M$, $r \geq 1$, and so $U^{-1}0 = \bigcap_{i=0}^{r} U^{-1}N_i$ is a primary decomposition. It is an irredundant primary decomposition because we have proved that the localizations of $P_1, \ldots, P_r$ are (weakly) associated. □

We proved in Proposition 0.9 that $\widetilde{\operatorname{Ass}}(M)$ contains the prime ideals which are minimal over $0 :_R M$. These are special, and form a special subset of $\widetilde{\operatorname{Ass}}(M)$. In general, for any type of associated prime ideals we partition the associated primes as follows:

Definition 3.14. Let R be a ring and M an R-module. Among the associated primes of a module (associated of any type as in Remark 0.11), the ones minimal with respect to inclusion are called the *minimal* prime ideals, the others *embedded* prime ideals.

If $0 = N_1 \cap \cdots \cap N_s$ is an irredundant primary decomposition, then N_i is called an *embedded component* of M if $\sqrt{N_i : M}$ is embedded, and is called a *minimal component* of M if $\sqrt{N_i : M}$ is minimal.

Lemma 3.15. Let R be a ring and M an R-module in which the zero ideal has a primary decomposition. Each minimal component of M is uniquely determined.

Explicitly, if P is a minimal prime in $\operatorname{Ass}(M)$, then the P-primary component of M equals the kernel of the map $M \to M_P$.

If R is Noetherian and M finitely generated, embedded components are never uniquely determined.

Proof: Let $0 = N_1 \cap \cdots \cap N_s$ be an irredundant primary decomposition. Let $P = \sqrt{N_j :_R M}$. If P is minimal, then $0_P = \bigcap_i (N_i)_P = (N_j)_P$, so that $0_P \cap M = (N_j)_P \cap M = N_j$ by Lemma 0.9, whence the P-primary component is uniquely determined.

Now let P be an embedded prime ideal. Let N_j be a P-primary component. As $\sqrt{N_j :_R M} = P$ and R is Noetherian, there exists a positive integer n such that

$P^nM \subseteq N_j$. For any $m \geq n$, set $K_m = P^mM_P \cap M$. By Lemma 0.9, K_m is P-primary. Furthermore, $(K_m)_P = P^mM_P$ is contained in $(N_j)_P$, so that $K_m \subseteq N_j$. It follows that $\bigcap\limits_{i \neq j} N_i \cap K_m \subseteq \bigcap\limits_{i} N_i = 0$, so that $0 = \bigcap\limits_{i \neq j} N_i \cap K_m$. Thus any K_m can be taken to be a P-primary component.

It remains to show that $K_m \neq K_{m'}$ whenever $m' \neq m$. By Lemma 0.9, $K_m \neq K_{m'}$ if and only if $P^mM_P \neq P^{m'}M_P$. By Nakayama's lemma, $P^mM_P = P^{m'}M_P$ if and only if $P^{\min\{m,m'\}}M_P = 0_P$. But P is not minimal over $0 :_R M$, so PR_P is not minimal over $0_P :_{R_P} M$, so $P^mM_P = 0_P$ is impossible. Thus $K_m \neq K_{m'}$ whenever $m' \neq m$. ∎

In particular, if P is a prime ideal in a Noetherian ring R, then for every positive integer n, there is a unique P-primary component of P^n. This component is called the nth *symbolic power* of P, and is usually denoted $P^{(n)}$.

Even though the embedded components are highly non-unique, the P-primary component from one decomposition can be used as the P-primary component in any other decomposition:

Theorem 3.16. ("Mix-and-match", Yao) *Let R be a Noetherian ring and M a finitely generated R-module. Let $\{P_1, \ldots, P_s\} = \operatorname{Ass} M$. Assume that for all $i, j = 1, \ldots, s$, N_{ji} is a P_i-primary component of 0 in M, and that we have s primary decompositions of 0 in M:*

$$0 = \bigcap_{i=1}^{s} N_{ji}, \qquad j = 1, \ldots, s.$$

Then $0 = \bigcap_{i=1}^{s} N_{ii}$ is also a primary decomposition.

4. More ways to get associated primes

The only method for computing the associated primes of a module described so far involves the computation of a primary decomposition. This is not an easy task, as we will show in Section 9. Fortunately, there are indirect and efficient methods for computing the associated primes without computing the primary decompositions. We describe some of those methods in this section. Another method can be found in the proof of Theorem .

For example, the knowledge of zero divisors gives information on associated primes, and vice versa:

Proposition 4.1. Let R be a ring and M an R-module. Then the set of zero divisors on M is contained in the set $\bigcup\limits_{P \in \widetilde{\operatorname{Ass}}(M)} P$. If the latter set is finite (for example, if the zero submodule of M has a primary decomposition), then the set of zero divisors in M equals $\bigcup\limits_{P \in \widetilde{\operatorname{Ass}}(M)} P$.

Proof: Let m be a non-zero element of M and $x \in R$ such that $xm = 0$. Then $x \in 0 :_R m$. Thus by the definition of associated primes, the zerodivisor x on M is contained in some weakly associated prime of M.

Now let x be a non-zero element in some weakly associated prime P of M. Then there exists an element $m \in M$ such that P is minimal over $0 :_R m$. By assumption, there are only finitely many prime ideals minimal over $0 :_R m$. Thus there exists

$r \in R$ contained in all the prime ideals minimal over $0 :_R m$ but not in P. Then rx is contained in all the prime ideals minimal over $0 :_R m$, so that for some integers n, n', $r^{n'} x^n m = 0$. Choose n, n' such that n is smallest possible. By the choice of r, $n \geq 1$. Then the non-zero element $r^{n'} x^{n-1} m$ is annihilated by x. Thus x is a zerodivisor on M. □

This gives another way to decide whether a given prime ideal P is associated to a module:

Lemma 4.2. Let R be a ring, P a prime ideal, and M an R-module. If $0_P :_{M_P} P \neq 0_P$, then $PR_P \in \text{Ass}(M_P)$.

If $PR_P \in \widetilde{\text{Ass}}(M_P)$ is finitely generated (after localization at P), then $0_P :_{M_P} P \neq 0_P$.

Proof: Without loss of generality we may assume that R is a ring whose only maximal ideal is P.

Assume that $0 :_M P \neq 0$. Let m be non-zero in $0 :_M P$. Then $P \subseteq 0 :_R m$. As m is non-zero, $0 :_R m$ is a proper ideal, so that $P = 0 :_R m$, whence $P \in \text{Ass}(M)$ by Proposition 0.9.

Now assume that $P \in \widetilde{\text{Ass}}(M)$. Then P is minimal over $0 : m$ for some $m \in M$. As P is the maximal ideal and finitely generated, there exists an integer n such that $P^n \subseteq 0 :_R m$. Choose n minimal. Then $n \geq 1$ and $P^{n-1} m$ is a non-zero submodule of $0 :_M P$. □

Associated primes and even primary decompositions can be obtained via contraction:

Lemma 4.3. Let R be a ring, S an R-algebra, $N \subseteq M$ S-modules, and K an R-submodule of M. Then $\widetilde{\text{Ass}}_R(K/N \cap K) \subseteq \{P \cap R \mid P \in \widetilde{\text{Ass}}_S(M/N)$.

Furthermore, if N has a primary decomposition $N = N_1 \cap \cdots \cap N_s$ in M, then $N \cap K = (N_1 \cap K) \cap \cdots \cap (N_s \cap K)$, after removing intersectands equal to K, is a primary decomposition of the R-module $N \cap K$ in K.

Proof: Let $P \in \widetilde{\text{Ass}}_R(K/N \cap K)$. By localization we may assume that P is the only maximal ideal in R. There exists $m \in K \setminus N$ such that P is minimal over $N \cap K :_R m$. Then $N :_S m$ is a proper ideal in S which contains P. Any prime ideal Q in S minimal over $N :_S m$ contracts to P and is weakly associated to M/N. This proves the first statement.

Now let N_i be a P-primary submodule of the S-module M. Assume that $N_i \cap K$ is a proper submodule of K. Let $m \in K \setminus N_i$ and $r \in R$ such that $rm \in N_i \cap K$. Then $m \in M \setminus N_i$, and as N_i is primary, there exists a positive integer n such that $r^n M \subseteq N_i$. Thus $r_i^N K \subseteq N_i \cap K$. This proves that $N_i \cap K$ is primary in K. Furthermore, the proof above shows that $\sqrt{N_i \cap K :_R K} \subseteq \sqrt{N_i :_S M} \cap R$, and the other inclusion is trivial. This proves that if N_i is P-primary in M and $K \not\subseteq N_i$, then $N_i \cap K$ is primary in K to the prime ideal $P \cap R$.

Hence $N \cap K = (N_1 \cap K) \cap \cdots \cap (N_s \cap K)$, after removing intersectands K, is a primary decomposition of the R-module $N \cap K$ in K.

One can then also read off the associated primes of the contraction from this:

$$\begin{aligned}\widetilde{\operatorname{Ass}}_R(K/N\cap K) &\subseteq \{\sqrt{N_i\cap K :_R K} \mid i=1,\ldots,s\}\\ &\subseteq \{\sqrt{N_i :_S M}\cap R \mid i=1,\ldots,s\}\\ &\subseteq \{P\cap R \mid P\in \widetilde{\operatorname{Ass}}_S(M/N)\}. \qquad\square\end{aligned}$$

Associated primes can also be read off from short exact sequences:
Proposition 4.4. Let R be a ring and

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

a short exact sequences of R-modules. Then

(1) $\widetilde{\operatorname{Ass}}\, M' \subseteq \widetilde{\operatorname{Ass}}\, M$.
(2) $\widetilde{\operatorname{Ass}}\, M \subseteq \widetilde{\operatorname{Ass}}\, M' \cup \widetilde{\operatorname{Ass}}\, M''$.
(3) If $P\in \widetilde{\operatorname{Ass}}\, M''$ is finitely generated, then $P\in \widetilde{\operatorname{Ass}}\, M \cup \widetilde{\operatorname{Ass}}\, H^1_P(M')$.

Proof: (1) follows from Lemma 0.3.

Let $P\in\widetilde{\operatorname{Ass}}\, M$. By localization, without loss of generality P is the unique maximal ideal of R. There exists $m\in M$ such that P is minimal over $0:_R m$. Let m'' be the image of m in M''. If m'' is non-zero, then P is minimal over $0:_R m''$ so that $P\in\widetilde{\operatorname{Ass}}\, M''$. Now assume that $m''=0$. Then $m\in M'$, and P is minimal over $(0_{M'}):_R m$, so that $P\in\widetilde{\operatorname{Ass}}\, M'$. This proves (2).

Now let $P\in\widetilde{\operatorname{Ass}}\, M''$ be finitely generated. Again without loss of generality by localization P is the only maximal ideal in R. By Lemma 0.8 there exists $m''\in M''$ such that $P=0:_R m''$. Thus m'' is a non-zero element of $H^0_P(M'')$ and $P\in\widetilde{\operatorname{Ass}}\, H^0_P(M'')$. The following is a part of the long exact sequence on local cohomology:

$$H^0_P(M)\longrightarrow H^0_P(M'')\longrightarrow H^1_P(M').$$

If $P\notin\widetilde{\operatorname{Ass}}\, M$, then $H^0_P(M)$ is zero. Thus by (1), $P\in\widetilde{\operatorname{Ass}}\, H^1_P(M')$. $\square$

Associated primes can also be constructed from direct limits:

Proposition 4.5. Let R be a ring, and $\{M_i\}_{i\in I}$ a direct system of R-modules. Let $P\in\operatorname{Ass}(\varinjlim M_i)$ and assume that PR_P is finitely generated. Then $P\in\bigcup\limits_{i\in I}\widetilde{\operatorname{Ass}}\, M_i$.

Proof: By localization we may assume that P is the only maximal ideal of R. By Lemma 0.8, there exists $m\in\varinjlim M_i$ such that $P=0:_R m$. As P is finitely generated, there exists $i\in I$ such that $m\in M_i$ and $Pm=0$ in M_i. Hence $P\subseteq(0_{M_i}):_R m$. But m is non-zero, so that $(0_{M_i}):_R m$ is a proper ideal, whence it equals P. Thus $P\in\widetilde{\operatorname{Ass}}\, M_i$. $\square$

In special cases, a module has a natural corresponding ideal such that the associated primes of the two are equal:

Proposition 4.6. Let R be a ring R, M a square matrix with entries in R, and C the cokernel of M. Then the minimal primes over $(\det M)R$ are precisely the minimal primes over $0:_R C$.

Proof: If M is an $n \times n$ matrix, then $R^n \xrightarrow{M} R^n \to C \to 0$ is exact. For a prime ideal P, $C_P = 0$ if and only if $R^n_P \xrightarrow{M} R^n_P$ is surjective, or equivalently, is an isomorphism. This occurs if and only if $\det M$ is a unit in R_P.

This proves that a prime ideal P contains $\det M$ if and only if $C_P \neq 0$. But C is finitely generated, so then $C_P \neq 0$ if and only if $0 :_R C \subseteq P$. □

5. Witnesses

By definition, every associated prime of an R-module M is minimal over $0 :_R m$ for some $m \in M$. Such m is called a *witness* of P. Witnesses are not unique, but not surprisingly, they carry some structure of the modules.

For example, for an ideal containing a non-zerodivisor, every associated prime has a witness which is a non-zerodivisor:

Proposition 5.1. Let I be an ideal in a ring R which contains a non-zerodivisor. Assume that 0 and I have primary decompositions. Let P be weakly associated to I. Then there exists a non-zerodivisor $r \in R$ such that P is minimal over $I : r$. If R is Noetherian, there exists a non-zerodivisor $r \in R$ such that $P = I : r$.

Proof: Let $P_1, \dots, P_s$ be the associated primes of 0. Let $I = q \cap J$, where q is primary to P and J is the intersection of the irredundant components of I not primary to P. As I contains a non-zerodivisor, so does J. Thus by Proposition 0.1, $J \not\subseteq P_i$ for all i. As $J \not\subseteq q$, by Prime Avoidance (see Exercise 0.7), there exists $r \in J \setminus (q \cup P_1 \cup \cdots \cup P_s)$. Thus r is a non-zerodivisor, and by Lemma 0.8, $I : r = q : r$ is primary to P. If R is Noetherian, there exists a positive integer n such that $P^n \subseteq I : r$. Choose n minimal with this property. Thus $P^{n-1} \not\subseteq I : r$. Then again by Prime Avoidance, there exists $x \in P^{n-1} \setminus ((I : r) \cup P_1 \cup \cdots \cup P_s)$. Then x is a non-zerodivisor, so rx is a non-zerodivisor, $P \subseteq I : rx$, and $I : rx$ is P-primary. Thus $P = I : rx$. □

The following corollary is used in the exercises to prove that for a finite set of ideals in a Noetherian ring, the set of associated primes of products of their powers is finite, see Exercise 7.38.

Corollary 5.2. Let R be a Noetherian ring, $x \in R$ a non-zerodivisor and $P \in \operatorname{Ass}(R/(x))$. Let $y \in P$ be a non-zerodivisor. Then $P \in \operatorname{Ass}(R/(y))$.

Proof: By Proposition 0.1 there exists a non-zerodivisor r such that $P = (x) : r$. Then $ry \in (x)$, so there exists $s \in R$ such that $ry = sx$. Set $Q = (y) : s$. If $z \in P$, then $zr = ax$ for some $a \in R$. Thus $srz = asx = ary$. As r is a non-zerodivisor, $sz = ay$. Hence $z \in (y) : s = Q$.

Conversely, let $z \in (y) : s$. Write $zs = ay$ for some $a \in R$. Then $zsr = ayr = asx$. But s is also a non-zerodivisor, as $sx = ry$ is a product of non-zerodivisors. Thus $rz = ax$, so that $z \in (x) : r$. This proves that $Q = P$, so that P is associated to (y). □

See Exercise 5.33 for a version of this lemma for non-Noetherian rings.

Naturally, associated primes preserve some structure of the ideals:

Proposition 5.3. Let G be a totally ordered abelian monoid (e.g., $G = \mathbb{N}^n$ or $G = \mathbb{Z}^n$). Let R be a G-graded ring, and M be an R-submodule of a G-graded R-module. Then every associated prime P of M is homogeneous. Furthermore, if M is G-graded, there exists a homogeneous element $m \in M$ such that $P = 0 : m$.

Proof: Write $P = 0 : m$ for some $m \in M$. Write $m = \sum_g m_g$, where g varies over a finite subset of G, and each m_g is a homogeneous element of degree g. Let $h = \max\{g \mid m_g \neq 0\}$. Let $p \in P$. Write $p = \sum_g p_g$ (finite sum), with each p_g a homogeneous element of degree g. Let $k = \max\{g \mid p_g \neq 0\}$. Then $p_k m_h$ is the component of $pm = 0$ of degree $k + h$, so that $p_k m_h = 0$.

We claim that there exists a positive integer i such that $p_k^i m = 0$. Suppose that for all $g' > g$, we have proved that $p_k^i m_{g'} = 0$. The term of degree $k + g$ in pm is of the form $\sum_{g' \geq g} p_{k+g-g'} m_{g'}$, so that $p_k^{i+1} m_g = 0$. It follows that for some positive integer i, $p_k^i \in 0 : m = P$, and as P is a prime ideal, then $p_k \in P$. By repeating, we get that every component of p is in P, so that every associated prime of M is homogeneous.

In particular, if M is also G-graded, $P = 0 : m = \cap_g (0 : m_g)$, so that for some g, $P = 0 : m_g$. □

In particular, the only maximal ideal in the polynomial ring $k[X_1, \ldots, X_n]$ which may be associated to homogeneous ideals is $(X_1, \ldots, X_n)$. By Lemma 0.2 one can test whether that maximal ideal is associated.

Another consequence of the proposition above is that all the associated primes of a monomial ideal are monomial, and furthermore one can compute all the associated primes of a monomial ideal: for each of the finitely many primes generated by a subset of the variables, by Lemma 0.2 one can test whether that prime ideal is associated to the monomial ideal.

Example 5.4. Let I be the monomial ideal (X^2, XY) in the polynomial ring $k[X, Y]$. The only prime ideals generated by variables are $0, (X), (Y), (X, Y)$. Clearly 0 and (Y) are not associated to I as they do not contain it. But by using Lemma 0.2, (X) is associated as $I : (X) = (X, Y)$, so that $(I : (X))_{(X)} \neq I_{(X)}$, and (X, Y) is associated as $(I : (X, Y))_{(X,Y)} = (X)_{(X,Y)} \neq (X^2, XY)_{(X,Y)}$. In fact, in Example 0.6 we saw that I has an irredunant primary decomposition $(X^2, XY) = (X) \cap (X^2, Y)$.

As in the case of this example, the primary components of homogeneous modules have graded structure:

Corollary 5.5. Let R be a Noetherian ring graded by a totally ordered abelian monoid G and let M be a Noetherian G-graded R-module. (M is not necessarily graded.) Then the submodule 0 in M has a primary decomposition in which each primary component is homogeneous.

Proof: By Theorem 0.4, every submodule of M has a primary decomposition. Let $0 = N_1 \cap \cdots \cap N_s$ be an irredundant primary decomposition. For each $i = 1, \ldots, s$, let N_i^* be the submodule of N_i generated by all the homogeneous elements of N_i. Then $0 = N_1^* \cap \cdots \cap N_s^*$, and it suffices to prove that each N_i^* is primary to $P_i = \sqrt{N_i : M}$. By Proposition 0.3, P_i is homogeneous.

We change notation, let N be a P-primary submodule of M, where P is a homogeneous prime ideal, and let N^* be the submodule of N generated by the homogeneous elements. By the primary assumption, there exists k such that $P^k M \subseteq N$. But P and M are G-graded, hence $P^k M \subseteq N^*$. Let $r \in R$ and $m \in M \subseteq N^*$ such that $rm \in N^*$. By possibly multiplying m by a power of P, without loss of generality we may assume that $Pm \subseteq N^*$, and that furthermore no homogeneous component of m is in $\subseteq N^*$. Under the total grading of G, let r' be the homogeneous component of r of highest degree, and let m' be the homogeneous component of m of highest degree. Then $r'm' \in N^* \subseteq N$. As m' is not in N^*, it is not in N, so that as N is P-primary, $r' \in P$. But then $r'm \in N^*$. By repeating this for $(r - r')m$, we get that $r \in P$, which proves that N^* is P-primary. □

Now we can describe monomial primary ideals and primary decompositions of monomial ideals:

Proposition 5.6. Let $R = k[X_1, \ldots, X_n]$ be a polynomial ring over a field k and let I be an ideal in R generated by monomials in the X_i. Then

(1) I has a unique minimal generating set S consisting of monomials.

(2) The radical of I equals

$$\{X_{i_1} \cdots X_{i_r} \mid \text{ for some positive integers } a_1, \ldots, a_r, X_{i_1}^{a_1} \cdots X_{i_r}^{a_r} \in S\}.$$

(3) For any $i = 1, \ldots, n$, $I : X_i = \sum_{m \in S} (m) : X_i$, where

$$(X_1^{a_1} \cdots X_n^{a_n}) : X_i = \begin{cases} (X_1^{a_1} \cdots X_n^{a_n}), & \text{if } a_i = 0; \\ ((X_1^{a_1} \cdots X_n^{a_n})/X_i), & \text{if } a_i > 0. \end{cases}$$

(4) I is primary if and only if for every variable X_i, whenever X_i divides one of the monomial generators of I, then $X_i \in \sqrt{I}$.

(5) To find a primary decomposition of I, if I is not primary, find $m \in S$ and a variable X_i such that X_i divides m but $X_i \notin \sqrt{I}$. Let a be any integer greater than or equal to $\max\{e \mid X_i^e \text{ divides some } m \in S\}$. Then $I = (I + (X_i^a)) \cap (I : X_i^a)$ is a decomposition of I into two strictly larger monomial ideals, and so the primary decomposition of I is obtained from Noetherian induction.

Proof: The first three parts are elementary. If I is primary then by the definition for every variable X_i, if X_i divides one of the monomial generators of I, then $X_i \in \sqrt{I}$. Now assume that for every variable X_i, if X_i divides one of the monomial generators of I, then $X_i \in \sqrt{I}$. We know that $\sqrt{I}$ is a monomial ideal. If $X_{i_1} \cdots X_{i_r}$ is one of the minimal monomial generators of $\sqrt{I}$ then for some positive integers $a_1, \ldots, a_r$, $X_{i_1}^{a_1} \cdots X_{i_r}^{a_r} \in S$. By assumption then $X_{i_1} \in \sqrt{I}$, so that $r = 1$. This proves that $\sqrt{I}$ is a prime ideal. By Proposition 0.3, all the associated prime ideals of I are monomial prime ideals, and as $\sqrt{I}$ is a prime ideal, each of the associated primes other than $\sqrt{I}$ contains a variable not in $\sqrt{I}$. Let X_i be one of those variables. Then X_i divides some $m \in S$, so by assumption, $X_i \in \sqrt{I}$, contradicting the choice of X_i. Thus necessarily $\sqrt{I}$ is the only associated prime of I, so that I is primary.

The last part follows from Procedure 0.5 and from part (4). □

Homogeneity can be used in yet another way to compute associated primes:

Proposition 5.7. Let G be a submonoid of $\mathbb{N}^n$. Let R be a G-graded ring and M a G-graded R-module. Let $P \in \widetilde{\operatorname{Ass}}_{R_0} M_g$. Then there exists $Q \in \widetilde{\operatorname{Ass}}_R M$ such that $Q \cap R_0 = P$.

Furthermore, if P is minimal over $0 :_{R_0} m$, then Q is minimal over $0 :_R m$.

In particular, if $\widetilde{\operatorname{Ass}}_R(M)$ is a finite set, then $\displaystyle\bigcup_{g \in G} \widetilde{\operatorname{Ass}}_{R_0} M_g$ is a finite set.

Proof: Let $m \in M_g$ such that P is minimal over $0 :_{R_0} m$. By definition m is homogeneous. Set $I = 0 :_R m$. Let $R_+ = \oplus_{g>0} R_g$. Then by the assumption on G, R_+ is a proper ideal in R, and even $I + R_+ \subseteq P + R_+$ are proper ideals in R.

Clearly $R/(P+R_+) \cong R_0/P$, so that $P+R_+$ is a prime ideal in R. Let Q be a prime ideal in R minimal over PR and contained in $P+R_+$. Then $Q \cap R_0 = P$. Suppose that Q is not minimal over I. Let Q' be a prime ideal containing I and properly contained in Q. Then by the definition of Q, P is not contained in Q'. But then $I \cap R_0 \subseteq Q' \cap R_0 \subsetneq Q \cap R_0 = P$, contradicting the minimality of P over $I \cap R_0$. Thus Q is minimal over I, so that $Q \subseteq \widetilde{\operatorname{Ass}} M$. $\square$

With the set-up as in the previous proposition, under the assumption that M is Noetherian, there are some stabilization properties of the sets $\operatorname{Ass}_{R_0} M_g$:

Proposition 5.8. Let R be a Noetherian $\mathbb{N}$-graded ring generated over R_0 by elements of degree 1. Let M be a finitely generated $\mathbb{N}$-graded R-module. Then there exists an integer m such that for all $n \geq m$, $\operatorname{Ass}_{R_0} M_n = \operatorname{Ass}_{R_0} M_m$.

Proof: As M is Noetherian, by Theorem 0.4, the set $\operatorname{Ass}_R M$ is finite. Thus by the previous proposition, $\bigcup\limits_n \operatorname{Ass}_{R_0} M_n$ is a finite set. It suffices to prove that for each $P \in \operatorname{Spec} R_0$ there exists N such that for all $n \geq N$, $P \in \operatorname{Ass}_{R_0} M_n$ if and only if $P \in \operatorname{Ass}_{R_0} M_N$.

Let $P \in \operatorname{Spec} R_0$. Without loss of generality R_0 is local with maximal ideal P.

Suppose that for some $i \geq 0$, $(0 :_M P) \subseteq (0 :_M R_1^i)$. Let N' be the maximal degree of an element in a minimal homogeneous generating set of $0 :_M P$, and let $N = N' + i$. If $n \geq N$ and $P \in \operatorname{Ass}_{R_0} M_n$, write $P = (0 :_{R_0} b)$ for some $b \in M_n$. Then $b \in 0 :_{M_n} P$, so that as $N - n \geq i$ and by degree count, $b \in R_{N-n}(0 :_M P) = 0$, which is a contradiction, i.e., $P \notin \operatorname{Ass}_{R_0} M_n$ for all $n \geq N$.

Now suppose that for all $i \geq 0$, $(0 :_M P) \not\subseteq (0 :_M R_1^i)$. Fix i such that for all n, $(0 :_M R_1^n) \subseteq (0 :_M R_1^i)$. Let $m \in M$ be a homogeneous element such that $Pm = 0$ and $R_1^i m \neq 0$. Then for all n, $R_1^n m \neq 0$. Let $N = \deg m$. Now for any $n \geq N$, $P = (0 :_{R_0} R_1^{n - \deg m} m)$, so that $P \in \operatorname{Ass}_{R_0} M_n$. $\square$

6. Canonical primary decomposition

We saw in Proposition 0.6 that monomial ideals have primary decompositions in which all primary components are monomial ideals. It is straightforward to show that there is a natural notion of the "largest" possible monomial components:

Proposition 6.1. Let I be a monomial ideal in a polynomial ring over a field. Let P be associated to I. Then there exists a unique largest monomial P-primary ideal q which appears as a P-primary component in some minimal monomial primary decomposition of I. Furthermore, in any primary decomposition of I, the P-primary component of I may be replaced by q.

Proof: For $i = 1, 2$, let q_i be a monomial P-primary ideal in a monomial primary decomposition of I, and let I_i be the intersection of the other primary components of I. By Theorem 0.16, $I_1 \cap q_2 = I$. By Proposition 0.6, $q_1 + q_2$ is a P-primary monomial ideal. The intersection of monomial ideals is generated by the least common multiples of monomials taken one from one ideal and another from the second ideal. Thus $I_1 \cap (q_1 + q_2) = I_1 \cap q_1 + I_1 \cap q_2 = I + I = I$. Thus clearly there exists an ideal q as in the statement of the proposition. The last statement follows from Theorem 0.16. $\square$

We have seen that embedded components need not be unique, but there is a notion of canonical primary decomposition, which is unique:

Theorem 6.2. *(Ortiz) Every ideal I in a commutative Noetherian ring admits a unique irredundant primary decomposition*

$$I = q_1 \cap \cdots \cap q_r$$

with the following property: whenever $I = q'_1 \cap \cdots \cap q'_r$ is another irredundant primary decomposition of I, with $\sqrt{q_i} = \sqrt{q'_i}$ for $i = 1, \ldots, r$, then for all i,

(1) *nilpotency degree $\operatorname{nil}(q_i)$ is less than or equal to $\operatorname{nil}(q'_i)$,*
(2) *if $\operatorname{nil}(q_i) = \operatorname{nil}(q'_i)$, then $q_i \subseteq q'_i$.*

Proof: By Theorem 0.16, it suffices to prove that for each $P \in \operatorname{Ass}(R)$, there exists a P-primary ideal q such that q appears as the P-primary component of I in some primary decomposition of I, the nilpotency degree of q is smallest possible, and if $\operatorname{nil}(q) = \operatorname{nil}(q')$ for some P-primary component q' of I, then $q \subseteq q'$. Let S be the set of all Q-primary components of I with the smallest possible nilpotency degree. Let this nilpotency degree be n. Then S is closed under intersections:

$$Q^n \subseteq \bigcap_{q \in S} q \subseteq Q,$$

and furthermore $\bigcap_{q \in S} q$ is Q-primary. Thus S has a minimal element under inclusion. This element, q_r, satisfies the two conditions of the theorem. □

The construction immediately shows the following:

Corollary 6.3. If q is a canonical component of I, then q equals the q-primary component of $I + (\sqrt{q})^{\operatorname{nil}(q)}$.

7. Associated primes of powers of an ideal

We prove in this section that there are classes of ideals which share the same associated primes. In particular, we prove that for any ideal I in a Noetherian ring R, $\operatorname{Ass}(R/I^n)$ is the same for all large n. It is not true in general that $\operatorname{Ass}(R/I^n) = \operatorname{Ass}(R/I)$ for all n, even for prime ideals:

Example 7.1. Let $R = k[X, Y, Z]$, P the kernel of the map $R \to k[t]$ taking X to t^3, Y to t^4, and Z to t^5. Then $P = (X^3 - YZ, Y^2 - XZ, Z^2 - X^2Y)$ and P is of course a prime ideal. However, P^2 has an embedded component:

$$\begin{aligned}(X^3 - YZ)^2 + (X^2Y - Z^2)(Y^2 - XZ) &= X^6 - 3X^3YZ + X^2Y^3 + XZ^3 \\ &= X(X^5 - 3X^2YZ + XY^3 + Z^3),\end{aligned}$$

so that as X is not in P, $X^5 - 3X^2YZ + XY^3 + Z^3$ is in $P^{(2)}$. Note that under the grading $\deg X = 3$, $\deg Y = 4$, $\deg Z = 5$, P is a homogeneous ideal. By degree count, $X^5 - 3X^2YZ + XY^3 + Z^3$ is not in P^2. Thus P^2 must have at least one embedded associated prime ideal. By homogeneity, that embedded prime ideal is necessarily equal to (X, Y, Z), and P^2 has exactly one embedded prime ideal.

This shows that $\operatorname{Ass}(R/I^n)$ is not a constant function as n varies. The function is also not monotone increasing or decreasing. Here is an easily verifiable example:

Example 7.2. Let $R = k[X, Y, U, V]$, $I = (X^4, X^3Y, X^2Y^2U, XY^3, Y^4) \cap (V, X^2)$. Then it is easy to verify that $\operatorname{Ass}(R/I) = \{(X, Y), (X, Y, U), (V, X)\}$, and that $\operatorname{Ass}(R/I^2) = \{(X, Y), (V, X), (X, Y, U, V)\}$.

We prove below that $\operatorname{Ass}(R/I^n)$ is eventually constant. We will make use of the extended Rees algebras, a ubiquitous construction in the study of properties of powers of an ideal:

Definition 7.3. Let R be a ring, and I an ideal in R. The *Rees algebra* of I is the subalgebra of $R[t]$, where t is a variable over R, generated over R by all elements of the form at, as a varies over the elements of I. This algebra is denoted $R[It]$.

The *extended Rees algebra* of I is the subalgebra of $R[t, t^{-1}]$ generated over R by t^{-1} and all elements of the form at, as a varies over the elements of I. The extended Rees algebra is denoted $R[It, t^{-1}]$.

It is easy to verify that for all $n \in \mathbb{N}$,

$$R[It] = \oplus_{n \geq 0} I^n$$

and that

$$I^n R[It, t^{-1}] \cap R = t^{-n} R[It, t^{-1}] \cap R = I^n, \quad I^n R[It] \cap R = I^n.$$

Also, if I is generated by $a_1, \ldots, a_s$, then the two kinds of Rees algebras are finitely generated over R:

$$R[It] = R[a_1 t, \ldots, a_s t], \quad R[It, t^{-1}] = R[a_1 t, \ldots, a_s t, t^{-1}].$$

In particular, if R is Noetherian, both Rees algebras are Noetherian, and primary decompositions exist in R, $R[It]$, $R[It, t^{-1}]$.

Similarly, if M is an R-module, then $MR[It]$ and $MR[It, t^{-1}]$ are modules over the Rees algebras $R[It]$ and $R[It, t^{-1}]$, respectively. If M is finitely generated, so are these extended modules. In any case,

$$I^n MR[It, t^{-1}] \cap M = t^{-n} MR[It, t^{-1}] \cap M = I^n M, \quad I^n MR[It] \cap M = I^n M.$$

Thus under the Noetherian assumptions, primary decompositions exist in M, $MR[It]$, $MR[It, t^{-1}]$, and by Lemma 0.3, a primary decomposition of $I^n M$ is a contraction of a primary decomposition of $t^{-n} MR[It, t^{-1}]$.

Proposition 7.4. Let R be a Noetherian ring, I an ideal and M a finitely generated R-module. Then $\bigcup\limits_n \operatorname{Ass}(I^n M / I^{n+1} M)$ is a finite set and there exists an integer m such that for all $n \geq m$, $\operatorname{Ass}(I^n M / I^{n+1} M) = \operatorname{Ass}(I^m M / I^{m+1} M)$.

Proof: Let S be the Rees algebra $R[It]$ and N the $\mathbb{N}$-graded S-module $\oplus_n I^n M / I^{n+1} M$. For each non-negative integer m, $N_m = I^m M / I^{m+1} M$. Proposition 0.8 applied to the $\mathbb{N}$-graded ring S finishes the proof. □

A similar proof also shows that $\bigcup\limits_n \operatorname{Ass}(I^n M)$ is a finite set and that there exists an integer m such that for all $n \geq m$, $\operatorname{Ass}(I^n M) = \operatorname{Ass}(I^m M)$. A similar result also holds for the modules $M/I^n M$:

Proposition 7.5. Let R be a Noetherian ring, I an ideal, and M a finitely generated R-module. Then there exists $m \in \mathbb{N}$ such that for all $n \geq m$, $\operatorname{Ass}(M/I^m M) = \operatorname{Ass}(M/I^n M)$.

Proof: For each positive integer n,

$$0 \to \frac{I^n M}{I^{n+1M}} \to \frac{M}{I^{n+1} M} \to \frac{M}{I^n M} \to 0$$

is a short exact sequence. By Proposition 0.4, $\operatorname{Ass}(I^nM/I^{n+1}M) \subseteq \operatorname{Ass}(M/I^{n+1}M) \subseteq \operatorname{Ass}(M/I^nM) \cup \operatorname{Ass}(I^nM/I^{n+1}M)$. By Proposition 0.4, there exists an integer k such that for all $n \geq k$, $\operatorname{Ass}(I^nM/I^{n+1}M) = \operatorname{Ass}(I^kM/I^{k+1}M)$. Thus for $n \geq k$,

$$\operatorname{Ass}(I^nM/I^{n+1}M) \subseteq \operatorname{Ass}(M/I^{n+1}M) \subseteq \operatorname{Ass}(M/I^nM) \cup \operatorname{Ass}(I^n/I^{n+1}M).$$

It immediately follows that $\bigcup\limits_n \operatorname{Ass}(M/I^nM)$ is finite. Also, for each $P \in \bigcup\limits_n \operatorname{Ass}(M/I^nM)$, if P is associated to infinitely many M/I^nM, then it is associated to M/I^nM for all $n \geq k$, and if P is associated to only finitely many M/I^nM, let k_P be the largest integer such that P is associated to $M/I^{k_P}M$. Set $m = \max\{k, k_P \mid P\}$. Then by the set-up, for all $n \geq m$, $\operatorname{Ass}(M/I^mM) = \operatorname{Ass}(M/I^nM)$. □

8. Primary decompositions of powers of an ideal

In this section we prove that one can choose primary components of powers of an ideal in such a way that they "do not grow small too fast". This is one of the many results on the linear properties of primary decompositions. The proof presented here depends on a version of the Artin-Rees lemma for Artinian modules, due to Kirby . We present Kirby's results here for completeness.

Proposition 8.1. (Kirby) Let R be a ring, $X_1, \ldots, X_s$ variables over R, and $M = \sum_{i=-\infty}^{\infty} M_i$ a graded $R[X_1, \ldots, X_s]$-module. (So $X_jM_i \subseteq M_{i+1}$, $RM_i \subseteq M_i$.) Then M is an Artinian $R[X_1, \ldots, X_s]$-module if and only if there exist integers k, l such that

(1) $M_i = 0$ for $i > l$,
(2) $0 :_{M_i} (X_1, \ldots, X_s) = 0$ for $i < k$,
(3) M_i is an Artinian R-module for $i \in \{k, k+1, \ldots, l\}$.

Proof: First assume that M is Artinian. Certainly then conditions (1) and (3) hold. Also, the submodule $0 :_M (X_1, \ldots, X_s)$ of M is Artinian, so that the descending chain $D_n = \oplus_{i=-\infty}^{-n}(0 :_{M_i} (X_1, \ldots, X_s))$ has to stabilize. As $\bigcap\limits_n D_n = 0$, for all sufficiently large n, $D_n = 0$. This proves (2).

Now assume that M satisfies conditions (1), (2) and (3). If $s = 0$, M is trivially an Artinian R-module. So we may assume that $s > 1$. Set $N_n = \frac{0:_M X_s^{n+1}}{0:_M X_s^n}$. Then N_n is a graded $R[X_1, \ldots, X_s]$-module which is annihilated by X_s, so that N_n is a module over $R[X_1, \ldots, X_{s-1}]$. Clearly N_n satisfies conditions (1), (2) and (3), so that by induction on s, N is Artinian over $R[X_1, \ldots, X_{s-1}]$.

For each positive integer n, define $\varphi_n : N_n \to N_0$ by sending $a + 0 :_M X_s^n$ to $X_s^n a$. Then clearly φ_n is injective and $M \supseteq N_0 \supseteq \varphi_1(N_1) \supseteq \varphi_2(N_2) \supseteq \cdots$.

Now let $A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$ be a descending chain of $R[X_1, \ldots, X_s]$ submodules of M. For each i, n, define A_{in} to be the submodule of N_n generated by $A_i \cap (0 :_M X_s^{n+1})$. Then $N_n \supseteq A_{1n} \supseteq A_{2n} \supseteq \cdots$ is a descending chain of $R[X_1, \ldots, X_{s-1}]$-submodules of N_n. But N_n is Artinian, so there exist an Artinian module L_n over $R[X_1, \ldots, X_{s-1}]$ and a positive integer m_n such that for all $k \geq m_n$, $L_n = A_{kn}$. For any $k \geq m_n, m_{n+1}$,

$$\varphi_n(L_n) = \varphi_n(A_{kn}) \supseteq \varphi_{n+1}(A_{k,n+1}) = \varphi_{n+1}(L_{n+1}).$$

It follows that $N_0 \supseteq \varphi_1(L_1) \supseteq \varphi_2(L_2) \supseteq \cdots$ is a descending chain of $R[X_1, \ldots, X_{s-1}]$-submodules of N_0. But N_0 is Artinian, so there exist an Artinian module L and a positive integer t such that for all $k \geq t$, $L = \varphi_k(L_k)$.

Now let $T = \max\{m_0, \ldots, m_t\}$. Then by the choices of the m_i, for all $k \geq T$ and $0 \leq n \leq t$, $A_{kn} = A_{k+1,n} = \cdots = L_n$. Now let $k \geq T$ and $n > t$. Then

$$\varphi_n(L_n) \subseteq \varphi_n(A_{kn}) \subseteq \varphi_t(A_{kt}) = \varphi_t(L_t) = \varphi_n(L_n).$$

Thus equality holds throughout, and since φ_n is injective, $L_n = A_{kn}$. This proves that for all $n \geq 0$ and $k \geq T$, $A_{kn} = A_{k+1,n}$.

Finally we prove that this implies that $A_k = A_{k+1}$. Let $\alpha \in A_k$. By condition (1) there exists n such that $X_s^{n+1}\alpha = 0$. Thus α has an image in N_n, hence in A_{kn}. Thus there exists $\beta \in A_{k+1}$ such that $\alpha - \beta \in 0 :_M X_s^n$. If $n = 0$, then $\alpha = \beta \in A_k$. Otherwise assume that $n > 0$. Then $\alpha - \beta \in (0 :_M X_s^n) \cap A_k$, so $\alpha - \beta$ has an image in $A_{k,n-1}$. But then by induction on n, $\alpha - \beta \in A_{k+1}$, whence $\alpha \in A_{k+1}$. This proves that $A_k = A_{k+1}$ for all $k \geq T$. Thus M is Artinian. □

A consequence is the following version of the Artin-Rees lemma for Artinian modules:

Theorem 8.2. (Kirby) *Let R be a ring, I an ideal, M an Artinian R-module, and N a submodule of M. Then there exists an integer k such that for all $n \geq k$,*

$$N + 0 :_M I^n = \big(N + 0 :_M I^k)\big) :_M I^{n-k}.$$

Proof: Let S be the set of all finitely generated ideals contained in I. Then as M is Artinian, there exists $J \in S$ such that $0 :_M J \subseteq 0 :_M K$ for all $K \in S$. If $m \notin 0 :_M I$, there exists $a \in I$ such that $am \neq 0$. Then $m \notin 0 :_M (J + (a))$, so that by the choice of J, $m \notin 0 :_M J$. It follows that $0 :_M J = 0 :_M I$. Hence by induction on $n \geq 1$, $0 :_M J^n = 0 :_M I^n$.

Let $J = (a_1, \ldots, a_s)$. Define

$$\overline{N}_n = \begin{cases} \frac{M}{0 :_M J^{-n}} & \text{if } n \leq 0; \\ 0 & \text{if } n > 0. \end{cases}$$

Set $\overline{N} = \oplus_{n=-\infty}^{\infty} \overline{N}_n$. Then $\overline{N}$ is a module over $R[X_1, \ldots, X_s]$, if X_i acts by multiplication by a_i. Then $\overline{N}$ satisfies conditions (1), (2) and (3) of Proposition 0.1, so that $\overline{N}$ is an Artinian module over $R[X_1, \ldots, X_s]$. For $n \geq 0$, set

$$K_n = \sum_{i=-\infty}^{-n} \frac{(N + 0 :_M J^n) :_M J^{-n-i}}{0 :_M J^{-i}}.$$

Then K_n is a submodule of $\overline{N}$, and $K_1 \supseteq K_2 \supseteq K_3 \supseteq \cdots$. Thus there exists an integer k such that for all $n \geq k$, $K_k = K_n$. In particular, the graded components of $K_k = K_n$ of degree $i = -n$ yield that $\big(N + 0 :_M J^k\big) :_M J^{n-k} = N + 0 :_M J^n$. Finally,

$$\begin{aligned} N + 0 :_M I^n &\subseteq \big(N + 0 :_M I^k\big) :_M I^{n-k} \\ &\subseteq \big(N + 0 :_M J^k\big) :_M J^{n-k} \\ &= N + 0 :_M J^n \\ &= N + 0 :_M I^n, \end{aligned}$$

so that equality holds throughout. □

Corollary 8.3. Let R be a Noetherian ring, M a finitely generated R-module, E an injective Artinian R-module, I an ideal, and $u \in R$ a non-zerodivisor on M. Then there exists a positive integer k such that for all $n \geq 1$, any R-homomorphism $g : M/u^nM = uM/u^{n+1}M \to E$ with the property $I^ng = 0$ can be extended to an R-homomorphism $\tilde{g} : M/u^{n+1}M \to E$ so that $I^{n+k}\tilde{g} = 0$.

Proof: Let $f : M \to uM/u^{n+1}M \to E$ be the composition. Let $H = \operatorname{Hom}_R(M, E)$. As $\operatorname{Hom}_R(\_, E)$ is exact, H is Artinian and $H = uH$. In particular, there exists $\tilde{f} \in H$ such that $f = u\tilde{f}$.

By Theorem 0.2, there exists an integer k such that for all $n \geq k$, $0 :_H u + 0 :_H I^n = \left(0 :_H u + 0 :_H I^k\right) :_H I^{n-k}$. The assumption $I^ng = 0$ implies that

$$\tilde{f} \in (0 :_H u) :_H I^n \subseteq \left(0 :_H u + 0 :_H I^k\right) :_H I^n \subseteq 0 :_H u + 0 :_H I^{n+k}.$$

Let $f' \in 0 :_H u$ and $f'' \in 0 :_H I^{k+n}$ such that $\tilde{f} = f' + f''$. Then $f = u\tilde{f} = uf''$.

As $u^{n+1}f'' = u^nf(M) = 0$, then f'' defines a map $\tilde{g} : M/u^{n+1}M \to E$ which extends g. Furthermore, $I^{k+n}\tilde{g} = 0$. □

Finally we can prove that primary components of powers of an ideal contain linearly growing powers of their corresponding associated primes:

Theorem 8.4. *Let R be a Noetherian ring, I an ideal and M a finitely generated R-module. Then there exists a positive integer k such that for all positive integers n there exists a primary decomposition*

$$I^nM = N_1 \cap N_2 \cap \cdots \cap N_l$$

such that if $P = \sqrt{I^nM :_R N_i}$, then $P^{kn}M \subseteq N_i$.

This result was first proved for $M = R$ in , and the generalization to arbitrary M was proved by Sharp in . The proof in used prime filtrations of quotients of a ring by powers of an ideal. The proof below, due to Sharp, shows another useful method of finding primary decompositions.

Proof of Theorem 0.4: Let $S = R[It, t^{-1}]$, $K = MR[It, t^{-1}]$. Suppose that theorem holds for primary decompositions of $(t^{-1})^nK = t^{-n}K$, i.e., that there exists a positive integer k such that for all positive integers n there exists a primary decomposition

$$t^{-n}K = N_1 \cap N_2 \cap \cdots \cap N_l$$

such that if $P_i = \sqrt{t^{-n}K :_S N_i}$, then $P_i^{kn}K \subseteq N_i$. By discussion above Proposition 0.4 and by Lemma 0.3, $I^nM = t^{-n}K \cap M = (N_1 \cap M) \cap (N_2 \cap M) \cap \cdots \cap (N_l \cap M)$ is a primary decomposition of I^nM and the associated primes of I^nM are in the set $\{P_i \cap R \mid i\}$. Then $(P_i \cap R)^{kn}M \subseteq P_i^{kn}N \cap M \subseteq N_i \cap M$, so that the theorem also holds for I and M. Thus without loss of generality is suffices to prove the theorem for the case when I is a principal ideal generated by a non-zerodivisor u on M.

For every injective module E, write it as $E = \oplus_P E_P$, where P varies over distinct prime ideals and E_P is the direct sum of injective envelopes of R/P. Let π_P be the natural projection $E \to E_P$.

Now let E_1 be the injective envelope of M/uM and $i_1 : M/uM \to E_1$ the natural inclusion. Then $E_1 = \oplus_P (E_1)_P$, where P varies over a finite set S of prime ideals in R. As N is finitely generated and every element of $(E_1)_P$ is annihilated by a power of P, there exists an integer k such that $P^k\pi_P \circ i_1 = 0$. We may choose k to work for all $P \in S$.

Apply Corollary 0.3 to module M, element u, $I = P$ in S, and $E = (E_1)_P$. By possibly increasing k, we may assume that k works for $(E_1)_P$ as in the Corollary. As S is a finite set, there exists a positive integer k as in the Corollary which works for all $(E_1)_P$ as P varies over elements of S. But then this same k works for all finite direct sums $(E_1)_P^n$, as P varies over elements of S.

We claim that for all $n \geq 1$ there exist an injective module $E_n = (E_1)^n$ and an inclusion $i_n : M/u^nM \to E_n$ such that for all $P \in S$, $P^{kn}\pi_P \circ i_n = 0$. This already holds for $n = 1$. Suppose that it holds for some positive n. Consider the commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & M/u^nM \arrow[r, "u"] \arrow[d, "i_n"] & M/u^{n+1} \arrow[r, "p"] & {} \arrow[r] \arrow[d, "i_1"] & 0 \\
0 \arrow[r] & E_n \arrow[r] & E_n \oplus E_1 \arrow[r] & E_1 \arrow[r] & 0
\end{tikzcd}$$

in which the rows are exact. By assumption, for all $P \in S$ and every summand $E_R(R/P)$ of E_n, $P^{kn}\pi_P \circ i_n = 0$. By Corollary 0.3, there exists $j_P : M/u^{n+1}M \to E_P$ extending $\pi_P \circ i_n$ such that $P^{kn+k}j_P = 0$. Set $j : M/u^{n+1} \to E_n$ be the direct sum of all the j_P. Define $i_{n+1} : M/u^{n+1}M \to E_n \oplus E_1 = (E_1)^{n+1} = E_{n+1}$ by $i_{n+1}(m + u^{n+1}M) = j(m) + i_1 \circ p(m)$. By construction, $P^{kn+k}\pi_P \circ i_{n+1} = 0$ for all $P \in S$. This i_{n+1} makes the diagram commute, and as i_1 and i_n are injective, so is i_{n+1}.

Finally, we prove the primary decomposition result. For each $n \geq 1$ and $P \in S$, set $N_{nP} = \ker(\pi_P \circ i_n)$. As i_n is an inclusion and $E_n = \oplus_{P \in S}(E_n)_P$, it follows that $\bigcap\limits_P N_{nP} = 0$ in M/u^nM. Also, by construction, $P^{kn}M \subseteq \ker(\pi_P \circ i_n) = N_{nP}$. □

Note the that proof does not indicate how k depends on I. A constructive k was achieved for monomial ideals by Hoa and Trung in .

There is a related result that the primary components of I^nM "do not grow too small too slowly", see , whose proof relies on a deep result of Izumi and Rees:

Theorem 8.5. (Swanson) *Let R be a Noetherian ring, I and J ideals in R. Assume that for each n there exists k_n such that $I^n : J^\infty \subseteq I^{k_n}$ and that the k_n may be chosen so that $\lim_n k_n = \infty$. (In other words, assume that the I-adic topology (topology defined by powers of I) is equivalent to the topology defined by $\{I^n : J^\infty\}_n$.) Then there exists an integer k such that for all n, $I^{kn} : J^\infty \subseteq I^n$.*

In particular, the intersection of those primary components of I^{kn} which do not contain any power of J is contained in I^n. In particular, if I is a prime ideal P, this says that whenever the P-adic topology is equivalent to the symbolic topology, then there exists an integer k such that for all n, $P^{(kn)} \subseteq P^n$. The proof in this generality gives no indication on how k depends on I. But here is a special case, first proved by Ein, Lazarsfeld and Smith in in equicharacteristic 0, and later by Hochster and Huneke in in characteristic p. Below is a basic version of their result (but see the two papers for more general statements):

Theorem 8.6. (Ein, Lazarsfeld, Smith ; Hochster, Huneke) *Let R be a regular ring containing a field, and P a prime ideal in R. Then for all n,*

$$P^{(n \cdot \operatorname{ht} P)} \subseteq P^n.$$

9. An algorithm for computing primary decompositions

Given an ideal in a computable ring, can one algorithmically determine its primary decomposition? This answer was already treated to some extent by Grete Hermann in : she proved that there exists a function in n, k, d such that if I is a not necessarily homogeneous ideal in a polynomial ring in n variables over a field, if I is generated by k elements of degree at most d, then there exists a primary decomposition of I such that the generators of its primary components are bounded above by that function. Hermann's function was doubly exponential in n. It is still not known if a doubly exponential bound is indeed necessary.

Since then, several algorithms have been written for primary decompositions and associated primes: Gianni, Trager and Zacharias , Eisenbud, Huneke, Vasconcelos , Wang , Shimoyama, Yokoyama . The best source of information on the algorithms is Decker-Greuel-Pfister's paper . Singular and Macaulay2 have an implementation of the computation of primary decompositions of ideals in polynomial rings.

Below is an outline of the algorithm due to Gianni, Trager and Zacharias . This algorithm is based on the theory of Gröbner bases in polynomial rings $R = A[X_1, \ldots, X_n]$, where A is a principal ideal domain such as $\mathbb{Z}$ or $k[X_0]$ for some field k and variable X_0. The first case of the computation of primary decompositions is of course when $n = 0$. Then the problem reduces to the problem of factorization of integers and polynomials. This is a non-trivial problem. There exist several fairly efficient algorithms for such factorization, due to Berlekamp, Lenstra, Lenstra, Lovasz, Davenport, Trager, etc.

Here is a simplistic approach to the factorization problem in a few special cases. To factor an integer n, one can by brute force check whether any integer between 2 and $\sqrt{n}$ divides n and in this manner obtain a factorization. To factor a polynomial in $k[X]$ if k is a finite field one can again use brute force: there are only finitely many polynomials in $k[X]$ of bounded degree. However, these factorization methods are not efficient.

For more details on factorization, see the excellent book *Modern Computer Algebra* by von zur Gathen and Gerhard. There is a nice tutorial on Berlekamp's algorithm on page 38 in . In these notes we ignore the difficulty of factorization and instead assume:

Assumption 9.1. Let A be either $\mathbb{Z}$ or a polynomial ring in one variable over a finitely generated field extension over a finite field or over $\mathbb{Q}$. Thus A is a special type of principal ideal domain. We assume that in all such principal ideal domains, every element is algorithmically factorable into a product of primes.

One can show that for any principal ideal domain A as above, if K is a finitely generated field extension of the field of fractions of A and X is a variable over K, then also every element in $K[X]$ is algorithmically factorable into a product of primes. For notational purposes we call any principal ideal domain A with this property *computable.*

The primary decomposition algorithm relies on induction on the number of variables. In particular, the following lemma will be useful:

Lemma 9.2. Let B be a Noetherian ring in which primary decompositions and associated primes of ideals are computable. Let $X_1, \ldots, X_n$ be variables over B, $C = B[X_1, \ldots, X_n]$, and I an ideal in C. Then there exist ideals $I_1, \ldots, I_s$ in C such that $I = I_1 \cap \cdots \cap I_s$ and each $I_j \cap B$ is primary in B. Furthermore, these ideals I_j are computable.

Proof: Let $K = I \cap B$. Then K is an ideal in B, so it has a primary decomposition $K = K_1 \cap \cdots \cap K_s$. We proceed by induction on s. If $s = 1$, there is nothing to do. So assume $s > 1$. By assumption the radicals $\sqrt{K_j}$ can be computed. By reindexing we may assume that $\sqrt{K_1}$ is minimal over K. By prime avoidance there exists $r \in K_2 \cap \cdots \cap K_s \setminus \sqrt{K_1}$, and one can actually compute such an element in B. Now we switch to ideals in C. By Lemma 0.3, there exists m such that $I :_C r^\infty = I :_C r^m$ and $I = (I :_C r^m) \cap (I + (r^m))$. Set $I' = I :_C r^m$, $I'' = I + (r^m)$. Then

$$I' \cap B = (I :_C r^m) \cap B = I \cap B :_B r^m = K_1,$$

which is primary in B. Also, $I'' \cap B = (I + (r^m)) \cap B$ is strictly larger than K, so by Noetherian induction one can decompose I'' as in the statement of the lemma, whence one can decompose I. □

We next review what is computable via *Gröbner bases* in the following context: let B be a Noetherian unique factorization domain, $X_1, \ldots, X_n$ variables over B and $C = B[X_1, \ldots, X_n]$.

(1) For each $f \in C$, write $f = \sum_\nu f_\nu X^\nu$, a finite sum, with each $f_\nu \in B$.

(2) Impose an order on the monomials in the X_i satisfying

(i) for all $\nu \neq 0$, $X^\nu > 1$,

(ii) if $X^\nu > X^\mu$ then for any ρ, $X^{\nu+\rho} > X^{\mu+\rho}$.

As every ideal in C is finitely generated, necessarily every set of monomials in C has a least element.

One could take for example the *lexicographic ordering*:

$$X^\nu > X^\mu, \text{ if the first non-zero entry in } \nu - \mu \text{ is positive,}$$

the *degree lexicographic ordering*:

$$X^\nu > X^\mu, \begin{cases} \text{if } |\nu| > |\mu|; \\ \text{or if } |\nu| = |\mu| \text{ and the first non-zero entry in } \nu - \mu \text{ is positive.} \end{cases}$$

or the *reverse lexicographic ordering*:

$$X^\nu > X^\mu, \begin{cases} \text{if } |\nu| > |\mu|; \\ \text{or if } |\nu| = |\mu| \text{ and the last non-zero entry in } \nu - \mu \text{ is negative.} \end{cases}$$

(3) Under the given monomial ordering, let the *initial term* of f, $\operatorname{in} f$, be $f_\nu X^\nu$ such that X^ν is maximal among all monomials appearing in f with a non-zero coefficient. If $\operatorname{in} f = f_\nu X^\nu$, set

$$\operatorname{lm} f = X^\nu, \operatorname{lc} f = f_\nu.$$

These are called *leading monomial* and *leading coefficient* of f. The initial term, the leading monomial and the leading coefficient of f are computable.

(4) For any ideal I in C, define the *initial ideal* $\operatorname{in}(I)$ of I to be $\{\operatorname{in} f \mid f \in I\}$. Similarly, for any set G in C, define the *initial ideal* $\operatorname{in}(G)$ of G to be $\{\operatorname{in} f \mid f \in G\}$.
WARNING: if $I = (f_1, \ldots, f_s)$, $\operatorname{in}(I)$ is in general strictly larger than $(\operatorname{in} f_1, \ldots, \operatorname{in} f_s)$. See Exercise 9.41.

(5) A set $\{g_1, \ldots, g_s\}$ is said to be a *Gröbner basis* of an ideal I if $g_1, \ldots, g_s \in I$ and $\operatorname{in}(I) = (\operatorname{in} g_1, \ldots, \operatorname{in} g_s)$.

(6) For any $f, g \in C$, the *S-polynomial* of f and g is

$$S(f,g) = \frac{\operatorname{lcm}(\operatorname{in} f, \operatorname{in} g)}{\operatorname{in} f} f - \frac{\operatorname{lcm}(\operatorname{in} f, \operatorname{in} g)}{\operatorname{in} g} g.$$

The S-polynomial is computable.

(7) Let $G = \{f_1, \ldots, f_s\}$ be a subset of C and $f \in C$. If $\operatorname{in} f$ is a multiple of some $\operatorname{in} f_j$, say $\operatorname{in} f = m \operatorname{in} f_j$, set $f' = f - m f_j$. Then $\operatorname{in} f' < \operatorname{in} f$. This step is called a *reduction step* of f with respect to G and f' is said to be obtained from f by reduction. Repeat the reduction step on f', then on the polynomial obtained from f' by reduction, etc. The reduction step needs to be repeated only finitely many times before the zero polynomial is obtained in the process, as under the ordering, every set of monomials has a least element. Thus there exists $\tilde{f} \in C$ such that $\tilde{f}$ is obtained from f by applying reduction finitely many times, and either $\tilde{f} = 0$ or $\operatorname{in} \tilde{f}$ is not a multiple of any $\operatorname{in} f_j$. Then $\tilde{f}$ is called a *reduction* of f with respect to G. A reduction of f with respect to G is computable.
WARNING: $\tilde{f}$ is not uniquely determined. See Exercise 9.41.

(8) For any ideal $I = (f_1, \ldots, f_s)$ in C, a Gröbner basis of I is computable. In particular, $\operatorname{in} I$ is computable. Namely, the algorithm goes as follows:
(i) Start with $G = \{f_1, \ldots, f_s\}$.
(ii) For each pair $f, g \in G$, compute $S(f, g)$ and reduce it with respect to G. If the reduction is not zero, add the element to G.
(iii) Repeat the previous step until all S-polynomials reduce to 0 with respect to G.
The indicated algorithm does terminate as at each step the ideal $\operatorname{in}(G)$ becomes strictly larger, and in a Noetherian ring, we cannot increase this ideal indefinitely. Thus the algorithm terminates in finitely many steps. This proves that a Gröbner basis and the initial ideal of I are both computable.

(9) For any variables $Y_1, \ldots, Y_m$ over C, impose on $C[Y_1, \ldots, Y_m]$ a monomial order such that for any $f \in C[Y_1, \ldots, Y_m] \setminus C$, $\operatorname{in} f \notin C$. (Many such orders exist, for example, the lexicographic ordering $Y_1 > Y_2 > \cdots > Y_m > X_1 > \cdots > X_n$.) Let G be a Gröbner basis of an ideal I in $C[Y_1, \ldots, Y_m]$. For any $f \in I \cap C$, as $f \in I$, f can be written as $f = \sum_{g \in G} h_g g$ for some $h_g \in C[Y_1, \ldots, Y_m]$ such that for all $g, \in (h_g h) \leq \in (f)$. But then by the choice of the order, if $h_g \neq 0$, then $h_g, g \in C$, so that $f \in (G \cap C)$. As $G \cap C \subseteq I \cap C$, this proves that $G \cap C$ is a Gröbner basis of $I \cap C$. Thus in particular for any ideal $I \subseteq C[Y_1, \ldots, Y_m]$, $I \cap C$ is computable.

(10) If I and J are ideals in C, then $I \cap J$ is computable. Namely, if Y is a variable over C, then $I \cap J = (IYC[Y] + J(Y-1)C[Y]) \cap C$, so that by the previous case $I \cap J$ is computable.

(11) If I and J are ideals in C, then $I :_C J$ is computable. Namely, if $J = (f_1, \ldots, f_s)$, then $I :_C J = \cap (I :_C f_j)$. By the previous case it suffices to prove that $I :_C f$ is computable for each $f \in C$. We already know that $I \cap (f)$ is computable. But then by using that $I \cap (f) = f(I : f)$, $I : f$ is computable as division of elements is computable.

(12) For any ideal I and element f in C, $I_f \cap C$ is computable. There are several ways to see this:

(i) $I_f \cap C = I : f^\infty$. By Lemma 0.3, it suffices to find an integer m such that $I : f^m = I : f^{m+1}$. This integer exists as C is Noetherian.

(ii) Let Y be a variable over C. Then $I_f \cap C = (IYC[Y] + (fY-1)C[Y]) \cap C$, which is computable.

(13) For any principal prime ideal (p) in B and any ideal I in C, $I_{B\setminus(p)} \cap C$ is computable. Namely, let G be a Gröbner basis of I. For each $g \in G$, write $\operatorname{lc} g = b_g p^{n_g}$ for some non-negative integer n_g and some $b_g \in B \setminus (p)$. Set $b = \prod_g b_g$. Then $I_b \cap C$ is computable and $I_b \cap C \subseteq I_{B\setminus(p)} \cap C$. We want to prove equality in this inclusion. Let $f \in I_{B\setminus(p)} \cap C$. To prove that $f \in I_b \cap C$, it suffices to assume that among all elements in $I_{B\setminus(p)} \cap C$ but not in $f \in I_b \cap C$, f has the least leading monomial. There exists $c \in B\setminus(p)$ such that $cf \in I$. Then $c \operatorname{in} f = \operatorname{in}(cf)$ is a multiple of $\operatorname{in} g = b_g p^{n_g} X^\nu$ for some $g \in G$. As B is a unique factorization domain, $b_g \operatorname{in} f$ is a multiple of $\operatorname{in} g = b_g p^{n_g} X^\nu$. Say $b_g \operatorname{in} f = m \operatorname{in} g$. Then $\operatorname{lm} f = \operatorname{lm}(b_g f) > \operatorname{lm}(b_g f - mg)$. As $b_g f - mg \in I_{B\setminus(p)} \cap C$, by the choice of f, $b_g f - mg \in I_b \cap C$. Hence $b_g f \in I_b \cap C$, whence $f \in I_b \cap C$. Thus $I_{B\setminus(p)} \cap C$ is computable, and equals $I_b \cap C$ as above.

With this background in Gröbner bases, the *Gianni-Trager-Zacharias* algorithm goes as follows. Let A be a computable principal ideal domain. Let $R = A[X_1, \ldots, X_n]$, and I an ideal in R. We want to find a primary decomposition of I and its associated primes.

Case $\mathbf{n = 0}$: The primary decompositions and associated primes are computable by the assumption.

Case $\mathbf{n > 0, I \cap A = 0}$: By item (13) above, $I_{A\setminus\{0\}} \cap R$ is computable and equals $I_a \cap R$ for some computable $a \in A$. By Lemma 0.3 there exists a computable m such that $I : a^\infty = I : a^m$ and $I = (I : a^m) \cap (I + (a^m))$. Then $I : a^m = IR_{A\setminus\{0\}} \cap R$. The ring $R_{A\setminus\{0\}}$ has dimension strictly smaller than R, so a primary decomposition and associated primes of $I : a^m = IR_{A\setminus\{0\}} \cap R$ are computable by induction. But then by Lemma 0.3, a primary decomposition and associated primes of $IR_{A\setminus\{0\}} \cap R$ are computable. Thus it suffices to find a primary decomposition and associated primes of $I + (a^m)$. But the contraction of this ideal to A falls into the next case.

Case $\mathbf{n > 0, I \cap A \neq 0}$: By Lemma 0.2 we may assume that $I \cap A$ is primary. As A is a principal ideal domain, $I \cap A$ is primary to a maximal ideal M. As A is a principal ideal domain, there exists $p \in A$ such that $M = pA$. This breaks into two cases, see below.

Case $\mathbf{n > 0, I \cap A}$ primary to a maximal ideal $\mathbf{(p)}$, $\mathbf{\dim(R/I) > 0}$: Let G be a Gröbner basis G for I. For each $j = 1, \ldots, n$, set

$$G_j = \{g \in G \mid \operatorname{in} g = c_j X_j^m \text{ for some } m \in \mathbb{N}_0,\ c_j \in A\}.$$

Then G_j is computable. Clearly $X_j \in \sqrt{\operatorname{in}(I)}$ if and only if $X_j \in \sqrt{\operatorname{in}(G_j)}$. These equivalent conditions are computable. If $X_1, \ldots, X_n \in \sqrt{\operatorname{in} I}$, then R/I is module-finite over $A/I \cap A$ (generated by finitely many monomials in the X_j), thus integral. But then $\dim(R/I) = \dim(A/I \cap A) = 0$, contradicting the assumption. Thus under the assumption one can compute an integer j such that $X_j \notin \sqrt{\operatorname{in} I}$. Set $A' = A[X_j]$. Then $I \cap A'$ is not zero-dimensional. By item (13) one can compute $b \in A' \setminus pA'$ and an integer m such that $I_{pA'} \cap R = I_b \cap R = I : b^m$. As $I_{pA'}$ is an ideal in the polynomial ring $A'_{pA'}[X_1, \ldots, \widehat{X_j}, \ldots, X_n]$ over a principal ideal domain $A'_{pA'}$, by induction on dimension a primary decomposition and associated primes of $I_{A'\setminus pA'}$

are computable. Then by Lemma 0.3, a primary decomposition and associated primes of $I_{A' \setminus pA'} \cap R$ are computable. By Lemma 0.3 it remains to compute a primary decomposition and associated primes of $I + (b^m)$. By the assumption that $I \cap A'$ is not zero-dimensional, since $b \in A[X_j] \setminus pA[X_j]$, it follows that $I + (b^m)$ strictly contains I. If it is the whole ring, we are done, otherwise we either repeat this case or the following case on this new ideal $I + (b^m)$. The repetition will happen at most finitely many times by the Noetherian hypothesis.

Case $\mathbf{n > 0}$, $\mathbf{I \cap A}$ primary to a maximal ideal $\mathbf{(p)}$, $\dim(\mathbf{R/I}) = \mathbf{0}$: Set $R' = A[X_1, \ldots, X_{n-1}]$. Then $A/(I \cap A) \subseteq R'/(I \cap R') \subseteq R/I$. As $A/(I \cap A)$ and R/I are zero-dimensional and R, R' are finitely generated A-algebras, it follows that $\dim(R'/(I \cap R')) = 0$. By Lemma 0.2 we may assume that $I \cap R'$ is primary, to a maximal ideal M. As R/MR is a principal ideal domain, $I(R/MR)$ is a principal ideal. From the given generators of I one can compute $g \in I$ such that $g(R/MR) = I(R/MR)$. Observe that $g \notin MR$. Then $I \subseteq gR + MR = gR + (\sqrt{I \cap R'})R \subseteq \sqrt{I}$, whence $\sqrt{gR + (I \cap R')R} = \sqrt{I}$. By our factorization assumption, there are computable elements $g_1, \ldots, g_s \in R$ such that their images in R/MR are distinct irreducible elements and $g = \prod g_j^{k_j}$ modulo MR. Observe that the ideals $g_j R + MR$ are distinct maximal ideals in R and that $g_j^{l_j} R + I$ is primary to $g_j R + MR$ for all $l_j \in \mathbb{N}$. Furthermore, any prime ideal in R containing I contains M and g, hence is one of the $g_j R + MR$. Thus it remains to find the $(g_j R + MR)$-primary component of I. But this is just $I_{f_j} \cap R$, where $f_j = \prod_{i \neq j} g_i$. Thus a primary decomposition of I is computable.

10. Complexity of associated primes

There are aspects of complexity of associated primes and complexity of primary decompositions other than their computability. This section describes some of them.

For example, the main motivation for Theorem 0.4 came from the theory of tight closure. Here is the set-up: let p be a prime integer and R a ring of characteristic p. For any ideal I and any power $q = p^e$ of p, define $I^{[q]}$ to be the ideal $(i^q \mid i \in I)$. This ideal is called the eth *Frobenius power* of I. Hochster and Huneke developed the theory of tight closure and proved many results in commutative algebra with it. But one basic question about tight closure is still open: does tight closure commute with localization? A partial answer to the question would be provided with a positive answer to the following question:

Question 10.1. For every ideal I in a Noetherian ring of characteristic p, does there exist an integer k such that for all $q = p^e$ there exists a primary decomposition

$$I^{[q]} = q_1 \cap \cdots \cap q_l$$

with $\sqrt{q_i}^{k[q]} \subseteq q_i$ for all i?

In case when I is one-generated, its Frobenius powers are ordinary powers, and then the answer to the question above is yes by Theorem 0.4.

If R is a regular ring, the answer to the question is yes, as then the Frobenius map is flat (see Kunz). A set-back to finding an affirmative answer to the question above in general was provided by the following example of Katzman :

Example 10.2. Let k be a field of positive characteristic p, t, x, y variables over k and $R = k(t)[x, y]/(xy(x - y)(x - ty))$. Then $\bigcup\limits_q \operatorname{Ass}(R/I^{[q]})$ is an infinite set.

This is not giving a negative answer to the question. In fact, Smith and Swanson showed in that Katzman's ideal satisfies the condition in the question. Nevertheless, Katzman's example shows that primary decompositions of Frobenius powers are fairly complex, and that resolving the question above will not be easy.

An example similar to Katzman's, but over an integral domain, was provided by Singh and Swanson :

Example 10.3. Let k be a field of positive characteristic p,

$$R = \frac{K[r, t, u, v, w, x, y, z]}{\left(u^2x^2 + v^2y^2 + tuxvy + rw^2z^2\right)},$$

and $I = (x, y, z)R$. Then R is an F-regular unique factorization domain, and the set

$$\bigcup_q \operatorname{Ass} \frac{R}{I^{[q]}} = \bigcup_q \operatorname{Ass} \frac{R}{(I^{[q]})^*}$$

has infinitely many maximal elements. (Superscript $*$ denotes tight closure, and F-regularity is a notion from tight closure. I leave these terms undefined here.)

Thus even in very good rings associated primes of Frobenius powers run wild.

Another aspect of complexity is the degree of generators of primary components of an ideal in a graded ring. Grete Hermann proved that in a polynomial ring in n variables over a field, if an ideal I has k generators and all have degree at most d, then the primary components of I are all generated in degrees which are at most doubly exponential in n. Hermann proved a few other doubly exponential bounds, such as for the ideal membership problem and the degrees of the generators of the syzygy module. Mayr and Meyer proved that the doubly exponential degree bounds are achieved for the ideal membership problem: let $J(n, d)$ be the ideal generated by the following polynomials in the polynomial ring in $10n+2$ variables over a field:

$$\begin{aligned}
&c_{0i}\left(s - fb_{0i}^d\right), i = 1, 2, 3, 4;\\
&s_r - s_{r-1}c_{r-1,1}, r = 1, \ldots, n,\\
&f_r - s_{r-1}c_{r-1,4}, r = 1, \ldots, n,\\
&f_{r-1}c_{r-1,1} - s_{r-1}c_{r-1,2}, r = 1, \ldots, n,\\
&f_{r-1}c_{r-1,4} - s_{r-1}c_{r-1,3}, r = 1, \ldots, n,\\
&s_{r-1}\left(c_{r-1,3} - c_{r-1,2}\right), r = 1, \ldots, n,\\
&f_{r-1}\left(c_{r-1,2}b_{r-1,1} - c_{r-1,3}b_{r-1,4}\right), r = 1, \ldots, n,\\
&f_{r-1}\left(c_{r-1,2}b_{r-1,1} - c_{r-1,3}b_{r-1,4}\right), r = 1, \ldots, n,\\
&f_{r-1}c_{r-1,2}c_{ri}\left(b_{r-1,2} - b_{ri}b_{r-1,3}\right), i = 1, \ldots, 4, r = 1, \ldots, n-1,\\
&f_{n-1}c_{n-1,2}\left(b_{n-1,2} - b_{n-1,3}\right).
\end{aligned}$$

Note that the generators have degrees at most $\max\{d + 2, 4, 5\delta_{n\geq 2}\}$. (Here, δ_P is 1 if P is true, and is 0 otherwise.) The degree 1 element $s_n - f_n$ of S is in $J(n, d)$, and when written as a linear combination of the given generators, the coefficient of $c_{04}(s_0 - f_0b_{01}^d)$ has degree which is doubly exponential in n (see).

It is not yet known if for every primary decomposition of the Mayr-Meyer ideals, the bound on the degrees of the generators of primary components is indeed doubly exponential. It is known that the number of minimal components is $nd^2 + 20$, and that the number of embedded primes is least $31 + 15d + (d^2 - d)\delta_{n=2} + (n-1)(d^3 - d)\delta_{n>2}$ and possibly doubly exponential in n (see ,). Bayer, Huneke, and Stillman asked whether the doubly exponential behaviour of the Mayr-Meyer ideals is due to the structure of one component or to the number of components. One could ask the same of the family of ideals $J(n,d) + (c_{ri}, s_r, f_r)^2$, which have much higher height than the $J(n,d)$, yet the same doubly exponential behaviour.

And one more aspect of complexity of primary decompositions is the number of associated or minimal primes over an ideal. Here is an example of permanental ideals: let A be an $n \times n$ matrix. In a Laplace expansion of the determinant of A change all the minus signs to plus. The obtained formula is the *permanent* of A.

Now let m and n be arbitrary positive integers and A an $m \times n$ matrix of indeterminates over a field. It is well-known that the ideal generated by determinants of all the $r \times r$ submatrices of A is a prime ideal. Not much is known for the corresponding results for permanents. Here is a special, and a wild, case, reflecting the computational complexity of permanents versus determinants via primary decompositions and associated primes:

Proposition 10.4. (Laubenbacher-Swanson) Let k be field of characteristic other than 2. Let $m, n \geq 2$ be integers and A an $m \times n$ matrix of indeterminates over k. Let I be the ideal generated by the permanents of all the 2×2 submatrices of A. Then the number of minimal primes over I is $n\delta_{m\geq 3} + m\delta_{n\geq 3} + \binom{n}{2}\binom{m}{2}$. Also, I has an embedded component if and only if $m, n \geq 3$, and the number of embedded components is exactly one.

And yet another aspect of the complexity of associated primes has to do with local cohomology: if R is a Noetherian ring, M a finitely generated module, and I an ideal, when do the local cohomology modules $H^i_I(M)$ have finitely many associated primes? If R is a regular ring containing a field, all such local cohomology modules have only finitely many associated primes. This was proved by Huneke and Sharp in case of positive characteristic, and by Lyubeznik otherwise. Lyubeznik also proved that the local cohomology modules have finitely many associated primes if R is an unramified regular local ring of mixed characteristic. Marley proved that if R is a Noetherian local ring and M a finitely generated R-module of dimension at most three, then any local cohomology module $H^i_I(M)$ has only finitely many associated primes. Khashyarmanesh and Salarian and Brodmann and Lashgari Faghani proved that if i is the smallest integer such that $H^i_I(M)$ is not finitely generated, then $H^i_I(M)$ has only finitely many associated primes. Singh constructed the first example for which $H^i_I(M)$ does not have finitely many associated primes. Katzman constructed such an example over a local ring containing a field, and Singh and Swanson constructed an example over a local unique factorization domain.

Acknowledgement. I thank the Bhaskaracharya Pratishthana and Harish-Chandra Research Institutes for the hospitality and a great conference, and the NSF for partial support. I thank Bruce Olberding and Kamran Divaani-Aazar for the careful reading of the first version of these notes and for improving the non-Noetherian parts. I thank Winfried Bruns and H. S. Hassanzadeh for their comments and corrections.

11. Exercises

Exercises have double numbers: the first number corresponds to the section with that number, the second number simply counts the exercises. Exercises with first number 0 cover some background.

0.1: Let P be a prime ideal, and $q_1, \dots, q_s$ arbitrary ideals. If P contains $q_1 \cap \dots \cap q_s$, prove that P contains one of the q_i. If $P = q_1 \cap \dots \cap q_s$, prove that P equals some q_i.

0.2: Let I and J be ideals in a ring R. Prove that $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

0.3: Let I and J be ideals and x an element in a ring R. Prove that $(I \cap J) : x = (I : x) \cap (J : x)$.

0.4: Let I be an ideal and U a multiplicatively closed subset in a ring R. Prove that $\sqrt{I}U^{-1}R = \sqrt{IU^{-1}R}$.

0.5: Let R be a ring, $N \subseteq M$ R-modules, and U a multiplicatively closed subset of R. Assume that M is finitely generated over R or that N is Noetherian. Prove that $U^{-1}(N :_R M) = U^{-1}N :_{U^{-1}R} U^{-1}M$.

0.6: Let R be a ring, $N \subseteq M$ R-modules, I an ideal in R, and U a multiplicatively closed subset of R. Assume that I is finitely generated or that N is Noetherian. Prove that $U^{-1}(N :_M I) = U^{-1}N :_{U^{-1}M} U^{-1}I$.

0.7: (Prime Avoidance) Let R be a ring, $P_1, \dots, P_s$ ideals in R, at most two of which are not prime ideals. Let I be an ideal such that $I \not\subseteq P_i$ for $i = 1, \dots, s$. Then I is not contained in $P_1 \cup \dots \cup P_s$.
Furthermore, if R is graded by a totally ordered abelian monoid and $P_1, \dots, P_s$ and I are homogeneous, then there exists a homogeneous element $r \in I$ such that $r \notin P_1 \cup \dots \cup P_s$.

2.8: Find an example of a primary ideal I such that for some integer n, I^n is not primary.

2.9: Let R be a ring, P a prime ideal, M and M' R-modules, N a P-primary submodule of M, and N' a P-primary submodule of M'. Then $N \oplus N'$ is a P-primary submodule of $M \oplus M'$.

2.10: Let R be a Noetherian ring, P a prime ideal in R, and M an R-module. Assume that P is minimal over $0 :_R m$ for some $m \in M$. Prove that $P = 0 :_R n$ for some $n \in N$.

2.11: Let R be the ring $\mathbb{R}[X, Y]/(X^2 - Y^2 - X^3)$ localized at (X, Y), and S the completion of R in the (X, Y)-adic topology. Then S is a faithfully flat extension of R. Verify that there are prime ideals in R which are not primary in S.

3.12: Let R be a Noetherian ring and M a finitely generated R-module. Prove that the different notions of primes associated to M as in Remark 0.11 are all the same.

3.13: Let R be a Noetherian ring, and M an R-module (not necessarily Noetherian). Prove that $\text{Ass}_R(M) = \widetilde{\text{Ass}}_R(M)$.

3.14: Find a ring R and a module M such that the different notions of primes associated to M (as in Remark 0.11) are all distinct.

3.15: Let R be a ring, M, M' both R-modules.

(i) Prove or disprove: $\mathrm{Ass}(M \oplus M') = \mathrm{Ass}(M) \cup \mathrm{Ass}(M')$.

(ii) Assume that M, M' are contained in an R-module. Prove or disprove: $\mathrm{Ass}(M + M') = \mathrm{Ass}(M) \cup \mathrm{Ass}(M')$.

3.16: Let R be a ring and M an R-module. An R-submodule N of M is said to be *irreducible* if whenever N' and N'' are R-submodules of M such that $N = N' \cap N''$, then either $N = N'$ or $N = N''$.

(i) Prove that every irreducible submodule of a Noetherian module is primary.

(ii) Prove that every submodule of a Noetherian submodule can be written as a finite intersection of irreducible submodules. (This generalizes Theorem 0.4.)

3.17: Let R be a ring, I an ideal and X a variable over R. Let $I = q_1 \cap \cdots \cap q_s$ be a (minimal, irredundant) primary decomposition. Prove that $IR[X] = q_1R[X] \cap \cdots \cap q_sR[X]$ is a (minimal, irredundant) primary decomposition.

3.18: Let R be a ring, I an ideal, J a finitely generated ideal in R, and P a prime ideal. Prove that if $P \in \mathrm{Ass}_R(R/(I : J))$, then $P \in \mathrm{Ass}_R(R/I)$.

3.19: (From Dan Katz) Let R be a Noetherian ring, and I an ideal containing a non-zerodivisor. Let n_0 be a positive integer such that for all $n \geq n_0$, $I^{n+1} : I = I^n$.[1] Prove that for all $n \geq n_0$, $\mathrm{Ass}_R(R/I^n) \subseteq \mathrm{Ass}_R(R/I^{n+1})$. (Thus if you know that $\bigcup\limits_n \mathrm{Ass}_R(R/I^n)$ is finite, then for all large n, $\mathrm{Ass}_R(R/I^n) = \mathrm{Ass}_R(R/I^{n+1})$. Cf. Proposition 0.5 and Exercise 7.35.)

3.20: Find an example of an ideal I and a primary decomposition $I = q_1 \cap \cdots \cap q_s$ such that for some positive integer n, $I^n \neq q_1^n \cap \cdots \cap q_s^n$.

3.21: Let R be a Noetherian ring, M a finitely generated R-module, and N an R-module. Prove that

$$\mathrm{Ass}_R \mathrm{Hom}_R(M, N) = \mathrm{Ass}_R(N) \cap \mathrm{Supp}_R(M).$$

3.22: Let R be a ring, P a prime ideal, and $E_R(R/P)$ the injective envelope of R/P. Prove that $\widetilde{\mathrm{Ass}}\, E_R(R/P) = \{P\}$.

3.23: Let R be a Noetherian ring and M a finitely generated R-module.

(i) Prove that there exists a filtration of R-modules

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M$$

[1] Such n always exists. A proof can be found in McAdam's book , Lemma 1.1 (b), applied to ideals which contain a non-zerodivisor. Namely, let $S = \mathrm{gr}_I(R) = R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots$. Then S is a Noetherian $\mathbb{N}$-graded ring. The ideal $0 :_S I/I^2$ is finitely generated, in degrees at most some integer l. For all $n > l$, $(0 :_S I/I^2) \cap I^n/I^{n+1} = 0$. Conclude that for all $n \geq l$, $(I^{n+1} : I) \cap I^l = I^n$. Now let x be a non-zerodivisor in I. Then for all n, $I^n : I \subseteq I^n : r$. By the Artin-Rees lemma, there exists an integer k such that for all $n \geq k$, $I^n \cap (r) \subseteq rI^{n-k}$. As r is a non-zerodivisor, for all $n \geq k$, $I^n : r \subseteq I^{n-k}$. Hence for $n \geq k + l$, $I^{n+1} : I \subseteq I^{n+1} : r \subseteq I^{n+1-k} \subseteq I^l$, whence $I^{n+1} : I \subseteq (I^{n+1} : I) \cap I^l = I^n$.

such that for all $i = 1, \ldots, n$, M_i/M_{i-1} is isomorphic to R/P_i for some prime ideal P_i in R.

(ii) Prove that if P is associated to M, then $P = P_i$ for some i.

3.24: (Yassemi) Let R be a ring and M an R-module. Prove that $\widetilde{\operatorname{Ass}}_R(M)$ is a finite set if and only if there exists a filtration of R-modules

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M$$

such that for all $i = 1, \ldots, n$, $\widetilde{\operatorname{Ass}}_R\, M_i/M_{i-1}$ consists of one prime ideal which is in addition weakly associated to M.

3.25: (Yassemi) Let R be a ring, I a proper ideal, and M an R-module. Prove that $\bigcup\limits_n \widetilde{\operatorname{Ass}}_R(M/I^nM) = \bigcup\limits_n \widetilde{\operatorname{Ass}}_R(I^{n-1}M/I^nM)$.

3.26: (Heinzer, Ratliff, Shah) Let $(R, \mathfrak{m})$ be a Noetherian local ring such that $\mathfrak{m} \in \operatorname{Ass} R \setminus \operatorname{Min} R$. Let S be the set of all $\mathfrak{m}$-primary components of (0) which are not contained properly in any other $\mathfrak{m}$-primary component of (0). Prove that S is an infinite set.

3.27: Let R be a ring, M, N R-modules, and $P \in \operatorname{Ass}_R(M)$. Prove that $\operatorname{Ass}_R(N/PN) \subseteq \operatorname{Ass}_R(M \otimes_R N)$. (I saw this exercise in .)

3.28: (Ortiz, , cf. Theorem 0.2) Let R be a Noetherian ring, and M a finitely generated R-module. For each $P \in \operatorname{Ass}_R M$, and each P-primary component N of 0 in M, set

$$\operatorname{nil}_N(P) = \min\{n \mid P^n \subseteq N :_R M\},$$
$$\operatorname{nil}(P) = \min\{\operatorname{nil}_N(P) \mid N \text{ is a } P\text{-primary component of } 0\}.$$

Prove that there exists a unique irredundant primary decomposition $0 = \bigcap\limits_{i=1}^{s} N_i$ of 0 in M such that

(i) For each i, with $P_i = \sqrt{N_i :_R M}$, $\operatorname{nil}_{N_i}(P_i) = \operatorname{nil}(P_i)$.

(ii) If $0 = \bigcap\limits_{i=1}^{s} N'_i$ is any other irredundant primary decomposition, then after relabelling without loss of generality for each $i = 1, \ldots, s$, $P_i = \sqrt{N'_i :_R M}$. If $\operatorname{nil}_{N'_i}(P_i) = \operatorname{nil}(P_i)$, then $N_i \subseteq N'_i$.

4.29: Let R be a Noetherian ring and I an ideal in R. Prove that for any $x \in R$, $\operatorname{Ass}(R/I) \subseteq \operatorname{Ass}(R/(I : x)) \cup \operatorname{Ass}(R/(I + xR))$. (Hint: use Proposition 0.4.)

4.30: Let R be a Noetherian ring and $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ a short exact sequence of finitely generated R-modules. Prove that

$$\operatorname{Ass} M'' \subseteq \operatorname{Ass} M \cup \{P \in \operatorname{Spec} R \mid \operatorname{depth}_{R_P} M'_P = 1\}.$$

5.31: (Krull's intersection theorem) Let R be a Noetherian ring and I an ideal in R. Prove that $\bigcap\limits_n I^n$ is the intersection of those primary components

q of 0 which satisfy the property $q+I=R$. (Hint: you may need to use that $I\bigcap\limits_n I^n=\bigcap\limits_n I^n$.)

5.32: (Yassemi) Let R be a ring, S an R-algebra, and M an S-module. Prove that $\{P\cap R \mid P\in \operatorname{Ass}_S(M)\}\subseteq \operatorname{Ass}_R(M)$.

5.33: Let R be a ring and x a non-zerodivisor in R. Assume that 0 and (x) have primary decompositions. If $P\in \operatorname{Ass}(R/(x))$ and $y\in P$ a non-zerodivisor, then P is associated to some power of (y). If P is finitely generated, then P is associated to (y).

5.34: Let R be a Noetherian $\mathbb{N}^n$-graded ring generated over R_0 by elements of total degree 1. Let M be a finitely generated $\mathbb{N}^n$-graded R-module. Prove that there exists $g_0\in\mathbb{N}^n$ such that for all $g\in\mathbb{N}^n$, if g is componentwise larger than g_0, then $\operatorname{Ass}_{R_0} M_g=\operatorname{Ass}_{R_0} M_{g_0}$.

7.35: Let R be a Noetherian ring and I an ideal. Then $\bigcup\limits_n \operatorname{Ass}(R/I^n)$ is a finite set. (Hint: this of course follows from Proposition 0.5, which proves more. Try a more elementary approach? Compare with the following two exercises.)

7.36: Let R be a Noetherian ring of prime characteristic p and I an ideal of finite projective dimension such that $\operatorname{Min} R/I=\operatorname{Ass}_R(R/I)$. Prove that for every $q=p^e$, $\operatorname{Ass}_R(R/I^{[q]})=\operatorname{Min} R/I$, where $I^{[q]}=(i^q \mid i\in I)$.

7.37: Let R be a Noetherian ring and I an ideal generated by a regular sequence. Prove that for all n, $\operatorname{Ass}_R(R/I^n)=\operatorname{Ass}_R(R/I)$.

7.38: Let R be a ring, and $I_1,\ldots,I_s$ ideals in R. The *multi-Rees algebra* of $I_1,\ldots,I_s$ is the subalgebra of $R[t_1,\ldots,t_s]$, where $t_1,\ldots,t_s$ are variables over R, generated over R by all elements of the form a_it_i, as a_i varies over the elements of I_i. This algebra is also denoted $R[I_1t_1,\ldots,I_st_s]$. The *extended multi-Rees algebra* of $I_1,\ldots,I_s$ is the subalgebra of $R[t_i,t_i^{-1} \mid i=1,\ldots,s]$ generated over R by the t_i^{-1} and all elements of the form a_it_i, as a_i varies over the elements of I_i. The extended Rees algebra is also denoted $R[It,t^{-1}]$. $R[I_1t_1,\ldots,I_st_s,t_1^{-1},\ldots,t_s^{-1}]$

(i) Prove that for all non-negative integers $n_1,\ldots,n_s$,

$$t_1^{-n_1}\cdots t_s^{-n_s}R[I_1t_1,\ldots,I_st_s,t_1^{-1},\ldots,t_s^{-1}]\cap R=I_1^{n_1}\cdots I_s^{n_s}.$$

(ii) Assume that M is an R-module. If S denotes the (extended) Rees algebra of $I_1,\ldots,I_s$, prove that MS is an $\mathbb{N}^s$-graded S-module. In particular, S is a graded.

7.39: Let R be a Noetherian ring, $I_1,\ldots,I_s$ ideals, and M a finitely generated R-module. Let S be the (extended) Rees algebra of $I_1,\ldots,I_s$.

(i) Prove that $\bigcup\limits_e \operatorname{Ass}(MS)_e$ is a finite set, as e varies over s-tuples in $\mathbb{N}^s$.

(ii) Use the shorthand notation $I^e=I_1^{e_1}\cdots I_s^{e_s}$. Prove that $\bigcup\limits_e \operatorname{Ass}(I^eM)$ is a finite set.

(iii) Similarly, prove that $\bigcup_{e,i} \mathrm{Ass}(I^e M/I^e I_i M)$ is a finite set.

(iv) Prove that $\mathrm{Ass}(I^e M)$ is independent of e for e componentwise large enough.

8.40: Let R be a Noetherian ring, $I_1, \ldots, I_s$ ideals and M a finitely generated R-module. Then there exists a positive integer k such that for all positive integers $n_1, \ldots, n_s$ there exists a primary decomposition

$$I_1^{n_1} M \cap \cdots \cap I_s^{n_s} M = N_1 \cap N_2 \cap \cdots \cap N_l$$

such that for all i, $\sqrt{N_i : M}^{kn} M \subseteq N_i$.

9.41: Let $R = \mathbb{Q}[X, Y]$ endowed with the lexicographic ordering. Let $I = (X^2, XY - Y^2)$.

(i) Prove that $\mathrm{in}(I) = (X^2, XY, Y^3)$.

(ii) Show that $\mathrm{in}(I) \neq (\mathrm{in}(X^2), \mathrm{in}(XY - Y^2)) = (X^2, XY)$.

(iii) Let $G = \{X^2, XY - Y^2\}$. Reduce X^2Y with respect to G in two different ways.

9.42: Let k be a perfect field, $X_1, \ldots, X_n$ variables over k, $R = k[X_1, \ldots, X_n]$. Let I be a zero-dimensional ideal in R. For each $j = 1, \ldots, n$, set $F_j k[X_j] = I \cap k[X_j]$. Let G_j be the square-free part of F_j. Prove that $\sqrt{I} = I + (G_1, \ldots, G_n)$.

9.43: Let k be an infinite field, $X_1, \ldots, X_n$ variables over k, and I a zero-dimensional ideal in $R = k[X_1, \ldots, X_n]$. Assume that I is not primary.

(i) Prove that after a generic linear change of coordinates, i.e., after a mapping $X_j \mapsto \sum_i a_{ij} X_i$, with $a_{ij} \in k$ sufficiently general, I contracted to $k[X_1]$ is not primary.

(ii) Give an example showing that without the generic linear change it can happen that $I \cap k[X_j]$ is primary for all j.

Bibliography

[1] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra.* Addison-Wesley Publishing Company, 1969.

[2] M. Brodmann. Asymptotic stability of $\mathrm{Ass}(M/I^n M)$. *Proc. Amer. Math. Soc.* **74** (1979), 16-18.

[3] M. P. Brodmann and A. Lashgari Faghani. A finiteness result for associated primes of local cohomology modules. *Proc. Amer. Math. Soc.* **128** (2000), 2851-2853.

[4] W. Bruns and U. Vetter. *Determinantal Rings.* Lecture Notes in Mathematics no. 1327, Springer-Verlag, 1988.

[5] J. H. Davenport, Y. Siret and E. Tournier. *Computer algebra. Systems and algorithms for algebraic computation.* Second edition. With a preface by Daniel Lazard. Translated from the French by A. Davenport and J. H. Davenport. With a foreword by Anthony C. Hearn. Academic Press, Ltd., London, 1993.

[6] W. Decker, G.-M. Greuel and G. Pfister. Primary decomposition: algorithms and comparisons. Algorithmic algebra and number theory (Heidelberg, 1997), 187–220, Springer, Berlin, 1999.

[7] K. Divaani-Aazar and M. Tousi. A new definition of associated prime ideals. *Ital. J. Pure Appl. Math.* **8**, (2000), 99–113.

[8] L. Ein, R. Lazarsfeld and K. E. Smith. Uniform bounds and symbolic powers on smooth varieties. *Invent. Math.* **144** (2001), 241-252.

[9] D. Eisenbud, C. Huneke and W. Vasconcelos. Direct methods for primary decomposition. *Invent. math.* **110** (1992), 207-235.

[10] L. Fuchs, W. Heinzer and B. Olberding. Commutative ideal theory without finiteness conditions: primal ideals. *Trans. Amer. Math. Soc.* **357** (2005), 2771-2798.

[11] P. Gianni, B. Trager and G. Zacharias. Gröbner bases and primary decompositions of polynomial ideals. *J. Symbolic Comput.* **6** (1988), 149-167.

[12] D. Grayson and M. Stillman. Macaulay2. 1996. A system for computation in algebraic geometry and commutative algebra, available via anonymous `ftp` from `math.uiuc.edu`.

[13] G.-M. Greuel, G. Pfister and H. Schönemann. Singular. 1995. A system for computation in algebraic geometry and singularity theory. Available via anonymous `ftp` from `helios.mathematik.uni-kl.de`.

[14] W. Heinzer, L. J. Ratliff, Jr. and K. Shah. On the embedded primary components of ideals, I. *J. Algebra* **167** (1994), 724-744.

[15] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.* **95** (1926), 736-788.

[16] L. T. Hoa and N. V. Trung. On the Castelnuovo-Mumford regularity and the arithmetic degree of monomial ideals. *Math. Z.* **229** (1998), 519-537.

[17] M. Hochster and C. Huneke. Comparison of symbolic and ordinary powers of ideals. *Invent. Math.* **147** (2002), 349-369.

[18] S. Hoşten and R. R. Thomas. The associated primes of initial ideals of lattice ideals. *Math. Res. Lett.* **6** (1999), 83–97.

[19] C. Huneke and R. Y. Sharp. Bass numbers of local cohomology modules. *Trans. Amer. Math. Soc.* **339** (1993), 765-779.

[20] J. Iroz and D. E. Rush. Associated prime ideals in non-Noetherian rings. *Can. J. Math.* **36** (1984), 344-360.

[21] M. Katzman. Finiteness of $\cup_e \mathrm{Ass}\, F^e(M)$ and its connections to tight closure. *Illinois J. Math.* **40** (1996), no.2, 330-337.

[22] M. Katzman. An example of an infinite set of associated primes of a local cohomology module. *J. Alg.* **252** (2002), 161-166.

[23] K. Khashyarmanesh and Sh. Salarian. On the associated primes of local cohomology modules. *Comm. Alg.* **27** (1999), 6191-6198.

[24] D. Kirby. Artinian modules and Hilbert polynomials. *Quart. J. Math. Oxford (2)*, **24** (1973), 47-57.

[25] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1.* Springer-Verlag, 2000.

[26] T. Krick and A. Logar. An algorithm for the computation of the radical of an ideal in the ring of polynomials. AAECC9, Springer LNCS 539 (1991), 195-205.

[27] E. Kunz. Characterizations of regular local rings of characteristic p. *Amer. J. Math.* **91** (1969), 772-784.

[28] R. C. Laubenbacher and I. Swanson. Permanental ideals. *J. Symbolic Comput.* **30** (2000), 195-205.

[29] G. Lyubeznik. Finiteness properties of local cohomology modules (an application of D-modules to commutative algebra). *Invent. Math.* **113** (1993), 41-55.

[30] G. Lyubeznik. Finiteness properties of local cohomology modules for regular local rings of mixed characteristic: the unramified case. *Comm. Alg.* **28** (2000), 5867-5882.

[31] T. Marley. The associated primes of local cohomology modules over rings of small dimension. *Manuscripta Math.* **104** (2001), 519-525.

[32] E. Mayr and A. Meyer. The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. Math.* **46** (1982), 305-329.

[33] S. McAdam. *Asymptotic Prime Divisors.* Lecture Notes in Mathematics 1023, Springer-Verlag, 1983.

[34] S. McAdam and P. Eakin. The asymptotic Ass. *J. Algebra* **61** (1979), 71-81.

[35] C. Monico. Computing the primary decomposition of zero-dimensional ideals. *J. Symbolic Comput.* bf 34 (2002), 451-459.

[36] V. Ortiz. Sur une certaine decomposition canonique d'un idéal en intersection d'idéaux primaires dans un anneau noetherien commutatif. *C. R. Acad. Sci. Paris* **T. 248, n. 24** (1959), 3385-3387.

[37] L. J. Ratliff, Jr.. On prime divisors of I^n, n large. *Michigan Math. J.* **23** (1976), 337-352.

[38] E. W. Rutman. Gröbner bases and primary decomposition of modules. *J. Symbolic Comput.* **14** (1992), 483-503.

[39] E. W. Rutman. Primary decomposition of modules: two variables over a field. *J. Symbolic Comput.* **15** (1993), 267-275.

[40] D. Savitt. Associated Primes and Primary Decomposition. Available electronically at `www.math.harvard.edu/~dsavitt/250b/primary2.ps`.

[41] R. Y. Sharp. Injective modules and linear growth of primary decompositions. *Proc. Amer. Math. Soc.* **128** (2000), 717-722.

[42] T. Shimoyama and K. Yokoyama. Localization and primary decomposition of polynomial ideals. *J. of Symbolic Comput.* **22** (1996), 247-277.

[43] A. K. Singh. p-torsion elements in local cohomology modules. *Math. Res. Lett.* **7** (2000), 165-176.

[44] A. K. Singh and I. Swanson. Associated primes of local cohomology modules and of Frobenius powers. *International Mathematics Research Notices* **30** (2004), 1703-1733.

[45] K. E. Smith and I. Swanson. Linear bounds on growth of associated primes. *Comm. Algebra* **25** (1997), 3071-3079.

[46] I. Swanson. Powers of ideals: primary decompositions, Artin-Rees lemma and regularity. *Math. Annalen* **307** (1997), 299-313.

[47] I. Swanson. Linear equivalence of ideal topologies. *Math. Zeit.* **234** (2000), 755-775.

[48] I. Swanson. The minimal components of the Mayr-Meyer ideals. *J. Algebra* **267** (2003), 127-155.

[49] I. Swanson. On the embedded primes of the Mayr-Meyer ideals. *J. Algebra* **275** (2004), 143-190.

[50] J. von zur Gathen and J. Gerhard. *Modern computer algebra.* Second edition. Cambridge University Press, Cambridge, 2003.

[51] D. Wang. An elimination method based on Seidenberg's theory and its applications. Computational algebraic geometry (Nice, 1992), 301-328, Progr. Math., 109, Birkheuser Boston, Boston, MA, 1993.

[52] Y. Yao. Primary decomposition: compatibility, independence and linear growth. *Proc. Amer. Math. Soc.* **130** (2002), 1629–1637.

[53] S. Yassemi. Weakly associated primes under change of rings. *Comm. Algebra* **26** (1998), 2007-2018.

[54] S. Yassemi. Weakly associated prime filtration. *Acta Math. Hungar.* **92** (2001), 179-183.

Some solutions

2.8: There are many examples. Here is a large class of examples: let k be a field, X_{ij} indeterminates over k, where $i = 1, \dots, m$ and $j = 1, \dots, n$. Let $R = k[X_{IJ} \mid i, j]$ and I an ideal generated by the determinants of all the $r \times r$ submatrices of $[X_{ij}]$. Then I is always a prime ideal, but powers of I are rarely primary. See Bruns-Vetter .

3.13: Use Exercise 2.10.

5.31: Set $K = \bigcap\limits_n I^n$, $L = \bigcap\limits_q q$, where q varies over all primary components of 0 satisfying $q + I \neq R$, $M = \bigcap\limits_q q$, where q varies over the rest of the primary components. As M is a finite intersection, $M + I = R$, and there exist $m \in M$, $i \in I$ such that $m + i = 1$. Then for any $x \in L$, $x = xm + xi = xi$, and similarly for all positive integers n, $x = xi^n \in I^n$. Hence $L \subseteq K$. As $IK = K$, by determinantal trick, there exists $r \in R$ such that $rK = 0$ and $r - 1 \in I$. If r is in an associated prime ideal P of 0, then from $r - 1 \in I$ we deduce that $P + I = R$. Thus $K \subseteq 0 : r$ is contained in the intersection of the primary components q of 0 for which $q + I \neq R$, which proves that $K \in L$, and hence $K = L$.

5.33: By Proposition 0.1 there exists a non-zerodivisor r such that P is minimal over $(x) : r$. Then $ry^n \in (x)$ for some positive integer n, so there exists $s \in R$ such that $ry^n = sx$. Set $Q = (y^n) : s$. If $z \in P$, then $z^m r = ax$ for some $a \in R$ and $m \in \mathbb{N}$. Thus $srz^m = asx = ary^n$. As r is a non-zerodivisor, $sz^m = ay^n$. Hence z is in the radical of $(y^n) : s = Q$. Conversely, let z be in $(y^n) : s$. Write $zs = ay^n$ for some $a \in R$. Then $zsr = ay^n r = asx$. But s is also a non-zerodivisor, as $sx = ry^n$ is a product of non-zerodivisors. Thus $rz = ax$, so that $z \in (x) : r$. This proves that $Q \subseteq P$, so that P is associated to (y).

7.35: Let $S = R[It, t^{-1}]$. Then t^{-1} is a non-zerodivisor in S. By Corollary 0.2, $\mathrm{Ass}(S/(t^{-1})) = \mathrm{Ass}(S/(t^{-n}))$ for all $n \in \mathbb{N}$. In particular, $\bigcup\limits_n \mathrm{Ass}(S/(t^{-n})$ is a finite set. But then by Lemma 0.3 and the fact that $I^n = t^{-n}S \cap R$, $\bigcup\limits_n \mathrm{Ass}(R/I^n)$ is a finite set.

Index