INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY. CABLE: CENTRATOM TRIESTE

SMR.761/9

Workshop on Commutative Algebra
and its Relation to
Combinatorics and Computer Algebra

(16 - 27 May 1994)

Associated Primes and Primary Decomposition

from
Commutative Algebra with a view toward
Algebraic Geometry

D. Eisenbud
Brandeis University
Waltham, MA 02254
U.S.A.

From Commutative Algebra with A View Toward Algebraic Geometry by David Eisenbud. (Springer-Verlag, Oct. 1994).

Chapter 3: Associated Primes and Primary Decomposition

As we have suggested above, the earliest impulse toward the development of what is now commutative algebra came from the desire of the number theorists to make use of unique factorization in rings of integers in number fields other than $\mathbb{Q}$. When it became clear that unique factorization did not always hold, the search for the strongest available alternative began. The theory of primary decomposition is the direct result of that search. Given an ideal I in a Noetherian ring R, the theory identifies a finite set of "associated" prime ideals of R, and tells how to "decompose" I as an intersection of ideals called primary ideals that are closely connected with these prime ideals. More generally, the theory produces such a set of associated primes and a decomposition of any submodule of a finitely generated R-module.

In the geometric setting, where $R = k[x_1, \dots, x_r]$ is a polynomial ring over an algebraically closed field, part of the geometric significance of primary decomposition may be seen as follows: Call an algebraic set X in affine r-space **irreducible** if it cannot be expressed as the union of two properly smaller algebraic sets. If $I \subset k[x_1, \dots, x_r]$ is the ideal of X, then I is prime iff X is irreducible -- that is, not the union of two smaller algebraic sets (Proof: If X is irreducible and $fg \in I$, then $Z(I,f) \cup Z(I,g) = X$, so f or g must vanish on X and be in I. Conversely suppose $X = X_1 \cup X_2$. If each X_i is an algebraic set smaller than X, then there is a function f_i vanishing on X_i but not X. Since $f_1 f_2$ vanishes on X we have $f_1 f_2 \in I$ though neither f_i is in I.) If X is any algebraic set, then I is the intersection of prime ideals. In this case the primary decomposition of I is the unique minimal expression of I as a finite intersection of primes. This corresponds to writing X in a unique way as a minimal union of irreducible algebraic sets X_i. We may think of it as specifying I as the set of polynomials that vanish on each of the X_i. More generally, given any ideal $I \subset k[x_1, \dots, x_r]$, the theory produces a finite set of irreducible algebraic sets X_i -- possibly with some embedded in others -- and says that I can be specified as the set of

polynomial functions with certain "higher" vanishing conditions at the "generic points" of the X_i.

One measure of the significance of the associated primes is that they determine many homological properties, via the theory of depth that we shall develop in Chapters 17 and 18.

Two simple examples will be useful to bear in mind while studying the theory below:

1) Corresponding to the unique prime factorization

$$n = \pm p_1^{d1} \cdots p_t^{dt}$$

of an integer in $\mathbb{Z}$ into powers of distinct primes we may write the ideal (n) as

$$(n) = (p_1^{d1}) \cap \dots \cap (p_t^{dt}).$$

(Proof: By induction on t we have $J := (p_2^{d2} \cdots p_t^{dt}) = (p_2^{d2}) \cap \dots \cap (p_t^{dt})$, and it suffices to show that if $I = (p_1^{d1})$ then $IJ = I \cap J$. If I, J $\subset$ R are ideals in any commutative ring, then $IJ \subset I \cap J$, but generally the containment is strict. However, if $I+J = R$, as in our case, we can write $1 = i+j$ with $i \in I$ and $j \in J$. Thus if $f \in I \cap J$ then $f = 1f = if + jf \in IJ + JI = IJ$, so $I \cap J = IJ$. For a generalization, see Exercise A3.17.)

In this case we shall see that the associated primes are the primes (p_i).

2) The ideal $(x^2, xy) \subset k[x,y]$ may be written as

$$(x^2, xy) = (x) \cap (x^2, xy, y^2),$$

and described as the ideal of polynomials vanishing along the line x=0 *and* vanishing to order at least two at the point x = y = 0.

Note that the given decomposition is not unique: we could also write $(x^2,xy) = (x) \cap (x^2,y)$, which corresponds to saying that a polynomial f is in (x^2,xy) if it vanishes along the line x = 0 and its derivative $\partial f/\partial x$ vanishes at the point x=y=0.

In this case we shall see that the associated primes are the primes (x) and (x,y).

Besides the search for an analog of unique prime factorization, there is another reason why primary decomposition is historically important in commutative algebra. Lasker formulated the theory originally only for affine rings and convergent power series rings. The proofs, by induction on the number of variables, used complicated arguments from elimination theory. Emmy Noether rewrote the subject in her classic paper [1921]. Here she developed the general theory of primary decomposition from the ascending chain condition alone. This paper and her subsequent paper on Dedekind domains [1927] were the first to show the importance of the rings now named for her.

Associated Primes

Let R be a ring and let M be an R-module.

Definitions : A prime P of R is **associated** to M if P is the annihilator of an element of M. The set of all primes associated to M is written $\mathbf{Ass_R\ M}$ or simply **Ass M** when there can be no confusion.

Tradition dictates one exception to this terminology: If I is an ideal of R, then the associated primes of the module R/I are called associated primes of I. Confusion rarely arises in this way, since the associated primes of I as a module are usually not interesting. For example, if R is a domain then the only associated prime of the module I is 0.

From the definition we see that P is an associated prime of M iff R/P is isomorphic to a submodule of M. Clearly all the associated primes of M contain the annihilator of M.

The central result about associated primes is:

Theorem 3 1: Let R be a Noetherian ring and let M be a finitely generated nonzero R-module.

a) Ass M is a finite, nonempty set of primes, each containin ann M. The set Ass M includes all the primes minimal among primes containing ann M.

b) The union of the associated primes of M consists of 0 and the set of zerodivisors on M.

c) The formation of the set Ass M commutes with localization at an arbitary multiplicatively closed set U, in the sense that

$$\text{Ass } M[U^{-1}] = \{\, PR[U^{-1}] \mid P \in \text{Ass } M \text{ and } P \cap U = \varnothing. \,\}$$

The proof will be given after a series of preliminary results and corollaries.

Essentially because of the second part of conclusion a), the primes minimal among those primes containing a given ideal I appears rather often in what follows. To simplify our language, we usually call them **primes minimal over I.**

The primes of Ass M that are not minimal are called **embedded** primes of M. If M=R/I corresponds to a subscheme X = Spec R/I of Spec R, then the varieties associated to minimal primes over I are called **isolated components** of X, and the varieties associated to other associated primes are called **embedded components** of X

(geometrically, they occur "embedded in" the isolated components). We shall draw some pictures after we have discussed primary decomposition.

If R is a graded ring Noetherian ring and M is a finitely generated graded R-module, then the associated primes of R are homogeneous, as we shall see in Proposition 3 12. This allows one to make graded versions of Theorem 3 1 and all the other results in this chapter.

One important consequence of Theorem 3 1 is:

Corollary 3 2: Let R be a Noetherian ring and let M be a finitely generated nonzero R-module. Every ideal consisting entirely of zerodivisors on M actually annihilates some element of M.

To prove this we need to know that an ideal contained in a union of primes is contained in one of them. This somewhat surprising but elemenentary fact often goes under the name "prime avoidance":

Prime Avoidance

Lemma 3 3 (Prime Avoidance) : Suppose that $I_1, \ldots, I_n$, J are ideals of a ring R, and suppose that $J \subset \cup_j I_j$. If R contains an infinite field or if at most 2 of the I_j are not prime, then J is contained in one of the I_j.

If R is graded, J is generated by homogeneous elements of degree > 0, and all the I_j are prime, then it is enough to assume that the homogeneous elements of J are contained in $\cup_j I_j$.

Despite the odd hypotheses, the Lemma is rather sharp; see Exercise 3 17. The name "Prime Avoidance" comes from the following typical application: if an ideal I is not contained in any of a finite number of primes P_j, then there is an element of I that "avoids" being contained in any of the P_j. In the geometric setting we can translate this by saying that if a finite number of

subvarieties X_j of a variety X are given, along with polynomial functions $f_1, \ldots, f_s$ on X, not all vanishing on any of the X_j, then there is some polynomial linear combination $f = \Sigma g_i f_i$ that does not vanish on any of the X_j. The last part will be used in Chapter 14. In fact, the first of the g_i can often be chosen to be 1; see Exercise 3 19 for this and a refinement, and McAdam [1974] for further refinements and a history of the ring theoretic formulations of this result.

Proof of Lemma 3 3: If R contains an infinite field, the result is trivial: No vector space over an infinite field can be a finite union of proper subspaces.

In the other case, we do induction on n, the case n=1 being trivial. By induction we may suppose that J is not contained in any smaller union of the I_j, so we can find elements $x_i \in J$, x_i not in $\cup_{j \neq i} I_j$. Supposing that $J \subset \cup I_j$, we must have $x_i \in I_i$.

If n=2, then x_1+x_2 is in neither I_1 nor I_2, contradicting the supposition. If on the other hand $n > 2$ then we may assume that I_1 is prime, and $x_1+x_2x_3\ldots$ is not in any of the I_j, again a contradiction.

For the graded case we can use the same proof after raising the x_i to a power, chosen so that x_1 and the product $x_2x_3\ldots$ have the same degree. We need the hypothesis that each I_j is prime to ensure that for each j the powers of x_i are not in I_j for $j \neq i$.//

Note that in Lemma 3 3 we did not assume that R was Noetherian; we shall have occasion to use the result in a (possibly) non-Noetherian case in Proposition 13.10. Also, in the cases not involving a ground field, the proof given above uses only that J is a subring -- without unit-- of R.

Proof of Corollary 3 2: By Theorem 3 1 an ideal consisting of zerodivisors on M is contained in the union of the associated primes of M. By Lemma 3 3, it is in one of them.//

Theorem 3 1 clearly implies that if M is nonzero then Ass M is nonempty. For example, since the intersection of a descending chain of primes is certainly prime, there are (even without Noetherian hypotheses) always primes minimal over a given ideal. The first step in the proof is to establish the existence of an associated prime directly:

Proposition 3 4: Let R be a ring and let M be an R-module. If I is an ideal of R maximal among all ideals of R that are annihilators of elements of M, then I is prime (and thus belongs to Ass M). In particular, if R is a Noetherian ring then Ass M is nonempty.

Proof: If $rs \in I$ and $s \notin I$ then we must show $r \in I$. If $m \in M$ is an element with ann m = I, then rsm = 0 but sm ≠ 0; Thus (r,I) is contained in the annihilator of sm, and since I was maximal, (r)+I = I. Thus $r \in I$.//

Proposition 3 4 is the basis for one of the characteristic applications of the theory of associated primes. If $x \in M$ is an element of any module over any (not necessarily Noetherian) ring R, then by Lemma 2.8 we can test whether x = 0 by seeing whether x goes to 0 in the localization Mp for each prime, or even each maximal ideal P. Now we see that if R is Noetherian we can restrict our attention to the associated primes. If M is finitely generated there will be only finitely many of these, a great improvement.

Corollary 3 5: Suppose that M is a module over a Noetherian ring R.

a) If $m \in M$, then m = 0 iff m goes to 0 in Mp for each of the maximal associated primes of M.

b) If $K \subset M$ is a submodule, then K = 0 iff Kp = 0 for all $P \in$ Ass M.

c) If $\varphi: M \to N$ is a homomorphism from M to an R-module N, then φ is a monomorphism iff the localization $\varphi_P: M_P \to N_P$ is a monomorphism for each associated prime P of M.

Proof: a) Suppose m ≠ 0. Since R is Noetherian, there is a prime maximal among the annihilators of elements of M that contain ann m, and this prime is an associated prime of M by Proposition 3 4. Thus ann m is contained in a maximal associated prime P, so m/1 ≠ 0 in Mp.

b) If K = 0 then clearly Kp = 0 for all P. If K ≠ 0, choose $0 \neq m \in K$ and apply i).

c) By Proposition 2.5, $(\ker \varphi)_P = \ker(\varphi_P)$. The result follows by putting $K = \ker \varphi$ in part ii). //

Proposition 3 4 makes the proof of part b) of the Theorem immediate: if r annihilates a nonzero element of M, then r is contained in a maximal annihilator ideal.

To prove part a) we shall apply the following tool:

Lemma 3 6: a) If $M = M' \oplus M''$ then Ass M = (Ass M') ∪ (Ass M").

b) More generally, if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then Ass M' ⊂ Ass M ⊂ (Ass M') ∪ (Ass M").

Proof: b) The first containment is clear from the definition. For the second, suppose that $P \in$ Ass M - Ass M'. If $x \in M$ has annihilator P, so that $Rx \cong R/P$, then since P is prime every nonzero submodule of Rx also has annihilator P. It follows that $Rx \cap M' = 0$, so Rx is isomorphic to its image in M". Thus $P \in$ Ass M" as required.

a) Given part b), it is enough to observe that Ass M" ⊂ Ass M.//

The first exact sequences on which we shall use Lemma 3 6 are produced as follows:

Proposition 3 7: If R is a Noetherian ring and M is a finitely generated R-module, then M has a filtration

$$0 = M_0 \subset M_1 \subset \dots \subset M_n = M$$

with each $M_{i+1}/M_i \cong R/P_i$ for some prime ideal P_i.

Proof: By Proposition 3 4, M has at least one associated prime, say P_1, so that there is a submodule $M_1 \cong R/P_1$. Appl/ing this reasoning again to M/M_1 we produce M_2, and continue in this way. The process must come to an end because the submodules of M satisfy the ascending chain condition, and this means that some $M_n = M$, as required.//

Using Lemma 3 6 inductively, we see that the associated primes of M are among the primes P_i appearing in Proposition 3 7. This proves the finiteness statement of Theorem 3 1.

One might ask which modules M admit a filtration as in 3 7, where in addition, every P_i is an associated prime of M. Such modules are called **clean**. For example, when R is a domain and M is torsion-free but not free, M is not clean, as the reader may verify. Unfortunately I know (1994) of no interesting characterization of cleanliness -- perhaps the reader will find one! An interesting class of filtrations where the associated primes do split up nicely is provided by Proposition 3 13.

Conclusion of the Proof of Theorem 3 1: We first prove part c): If $P \in \text{Ass } M$, then there is an inclusion $R/P \subset M$. Localizing, we get an injection $R[U^{-1}]/PR[U^{-1}] \subset M[U^{-1}]$. Thus if $PR[U^{-1}]$ is a prime ideal of $R[U^{-1}]$ -- that is, if $P \cap U = \varnothing$ so $PR[U^{-1}]$ is still a proper ideal -- then $PR[U^{-1}] \in \text{Ass } M[U^{-1}]$.

Conversely, suppose Q is a prime of $R[U^{-1}]$ that is associated to $M[U^{-1}]$. We may write $Q = PR[U^{-1}]$ with P a prime of R and $P \cap U = \varnothing$. There is an injection $\varphi: R[U^{-1}]/PR[U^{-1}] \to M[U^{-1}]$. Since P is finitely generated, we have

$$\text{Hom}_{R[U^{-1}]}(R[U^{-1}]/PR[U^{-1}] , M[U^{-1}]) = \text{Hom}_R(R/P , M)[U^{-1}]$$

by Proposition 2.10 so we may write $\varphi = u^{-1}f$ for some $f \in \text{Hom}_R(R/P , M)$ and $u \in U$. Since u is a nonzerodivisor on R/P, it follows that f is an injection, concluding the proof of c).

It remains to show that if P is any prime minimal over ann M then $P \in \text{Ass } M$. By part c), we may localize and suppose that R is local with maximal ideal P. By Proposition 3 4 the set Ass M is nonempty, and since P is the only prime that contains ann M, it follows that $P \in \text{Ass } M$.//

Primary Decomposition

To avoid endlessly repeating the hypotheses, **we shall assume throughout the rest of this Chapter that R is a Noetherian ring, and we shall assume that M is a finitely generated R-module.**

If n is an integer, then the associated primes of $(n) \subset \mathbf{Z}$ in the ring of integers are just the ideals generated by the primes dividing n. But for the factorization of n, we need powers of these primes. Instead of writing $n = p_1^{e_1} \dots p_n^{e_n}$ for the prime factorization, we may write the ideal (n) as a product, $(n) = (p_1^{e_1}) \cdots (p_n^{e_n})$, or, if the p_i are distinct primes, even as an intersection, $(n) = (p_1^{e_1}) \cap \dots \cap (p_n^{e_n})$. Primary decomposition is an extension of prime factorization to arbitrary rings, which consists in writing an ideal as the intersection of certain ideals that play the role of prime powers: these are called primary ideals.

As often happens, it is advantageous to work with modules instead of ideals, and we shall define primary decompositions for a submodule M' of a finitely generated module M: That is, we shall write M' as the intersection of certain submodules M_i that correspond to the prime powers above. These are defined as follows: A submodule N of a module M is **primary** if Ass(M/N) consists of just a one prime; if Ass(M/N) = {P}, we say that N is **P-primary** Since this is really a condition on M/N, it is convenient to say that a module M is **coprimary** if 0 is a primary submodule -- that is, if Ass(M) consists of just one prime ideal.

From Lemma 3 6 we easily see that an intersection of P-primary submodules is P-primary:

Corollary 3 8: Suppose that P is a prime ideal of a ring R and $N_1,\ldots,N_t \subset M$ are R-modules. If each N_i is a P-primary submodule of M then $\cap_i N_i$ is P-primary.

Proof: First suppose that t = 2. By hypothesis M/N_1 and M/N_2 are P-coprimary. Lemma 3 6 a) shows that P is the only associated prime of $M/N_1 \oplus M/N_2$. Since $M/(N_1 \cap N_2)$ injects into $M/M_1 \oplus M/M_2$, Lemma 3 6 b) shows that $M/(N_1 \cap N_2)$ is also coprimary.//

Definitions : M is **coprimary** if it has exactly one associated prime. If Ass M = {P}, then M is called P-coprimary. A submodule $M' \subset M$ is called **primary** (or P-primary) if M/M' is co-primary (or P-coprimary).

The results of Theorem 3 1 lead to the following interpretation of this condition:

Proposition 3 9: Let P be a prime ideal of R. The following are equivalent:

a) M is P-coprimary.

b) P is minimal over ann M, and every element not in P is a nonzerodivisor on M.

c) A power of P annihilates M, and every element not in P is a nonzerodivisor on M.

Proof: a) ⇒ b): Since P is the only associated prime of M, Theorem 3 1 a) shows that P is minimal over ann M, and Theorem 3 1 b) shows that every element not in P is a nonzerodivisor on M.

b) ⇒ c): Since the elements not in P are nonzerodivisors on M, it suffices to prove the statement after localizing at P, so we may assume that R is a local ring with maximal ideal P. Since P is minimal over ann M, it follows by Corollary 2.12 that P is the radical of ann M, so P is nilpotent modulo ann M.

c) ⇒ a): Since P is nilpotent modulo ann M, it is certainly minimal among primes containing ann M, and is an associated prime of M by Theorem 3 1 a). Since every element outside of P is a nonzerodivisor, every associated prime of M is contained in P by Theorem 3 1 b). Thus P is the only associated prime of M.//

The most important case is the one where M = R/I, for some ideal I of R. In this setup, Proposition 3 9 c) shows that I is P-primary iff I contains a power of P and for every r,s ∈ R, the conditions rs ∈ I and r ∉ P imply s ∈ I. This is the classical definition.

It is often convenient to think of the definitions above in terms of localizations: Proposition 3 9, b) shows that M is P-coprimary iff P is minimal over the annihilator of M and M injects into M_P. In general, if M is any module and P is a minimal prime over the annihilator of M, then the submodule $M' \subset M$ defined by

$$M' = \ker (M \to M_P).$$

is P-primary because M/M' injects into $(M/M')_P = M_P$. In this situation, M' is called **the P-primary component** of 0 in M. Note that it depends only on M and on P.

Primary decomposition consists in writing an arbitrary submodule M' of M as the intersection of primary submodules:

Theorem 3 10: Let R be a Noetherian ring, and let M be a finitely generated R-module. Any proper submodule M' of M is the intersection of primary submodules. Further, if $P_1, \ldots, P_n$ are prime ideals and we write $M' = \bigcap_{i=1}^{n} M_i$ with M_i a P_i-primary submodule, then

a) Every associated prime of M/M' occurs among the P_i.

b) If the intersection is **irredundant** (meaning no M_i can be dropped) then the P_i are precisely the associated primes of M/M'.

c) If the intersection is **minimal**, in the sense that there is no such intersection with fewer terms, then each associated prime of M/M' is equal to P_i for exactly one index i. In this case, if P_i is minimal over the annihilator of M/M', then M_i is the P_i-primary component of M'.

d) Minimal primary decompositions localize in the following sense: Suppose that $M' = \bigcap_{i=1}^{n} M_i$ is a minimal primary decomposition. If U is any multiplicatively closed set of R, and $P_1, \ldots, P_t$ are the primes among the P_i that do not meet U, then

$$M'[U^{-1}] = \bigcap_{i=1}^{t} M_i[U^{-1}]$$

is a minimal primary decomposition over $R[U^{-1}]$.

Proof: We first prove the existence of a slightly finer but less canonical decomposition. We shall say that a submodule $N \subset M$ is **irreducible** if N is not the intersection of two strictly larger

submodules. We first claim -- and this is Emmy Noether's fundamental observation -- that every submodule of M can be expressed as the intersection of irreducible submodules. Otherwise, by the ascending chain condition on submodules of M, we could choose a submodule $N \subset M$ maximal among those submodules that are not the intersection of irreducible submodules. In particular, N is not itself irreducible, so it is the intersection of two strictly larger submodules N_1 and N_2. By the maximality of N, both the N_i are intersections of irreducible submodules, and it follows that N is too. The contradiction proves our claim, and shows that there is an irreducible decomposition $M = \cap_i M_i$ with each M_i irreducible.

We next show that every irreducible decomposition is a primary decomposition. That is, we show that any irreducible submodule $N \subset M$ is primary, or equivalently that M/N is coprimary. Otherwise, M/N would have at least two associated primes, P and Q say, so it would contain a submodule isomorphic to R/P and another isomorphic to R/Q. The annihilator of every nonzero element of R/P is P, and similarly for Q, so these two submodules of M/N can only meet in 0. Thus 0 is reducible. Taking preimages of these submodules in M, we see that N is reducible, a contradiction. This proves that M/N is coprimary, and thus that irreducible decompositions are primary decompositions.

Since a)-d) are really statements about M/M'. To simplify the notation, we begin by factoring out M', and assume henceforward that M' = 0.

a) Now suppose that $0 = \bigcap_i M_i$ is a primary decomposition. Note that $M \subset \oplus M/M_i$ so by Lemma 3 6 every prime in Ass M occurs among the primes P_i. This proves assertion a).

b) Next suppose that the given decomposition is irredundant, so that for each j, $\bigcap_{i \neq j} M_i \neq 0$. Note that because $M_j \cap \bigcap_{i \neq j} M_i = 0$ we have

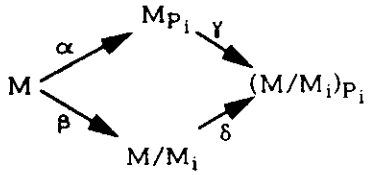
$$\bigcap_{i\neq j} M_i = (\bigcap_{i\neq j} M_i) / (M_j \cap \bigcap_{i\neq j} M_i)$$

$$\cong (\bigcap_{i\neq j} M_i + M_j)/M_j \subset M/M_j.$$

As this module is P_j-coprimary, so is $\bigcap_{i\neq j} M_i$. By Lemma 3 6, P_j is an associated prime of M. Together with a), this proves b).

c) Finally, suppose that the given decomposition is minimal. By Corollary 3 8 the intersection of P-primary submodules is P-primary, so minimality implies that the primes P_i are distinct. With b), this proves the first statement of c).

For the last statement, suppose that P_i is minimal over the annihilator of M. We must show that M_i is the kernel of the localization map $\alpha: M \to M_{P_i}$. Consider the commutative diagram



where β is the projection map, δ is the localization map, and γ is the projection of M_{P_i} to $M_{P_i}/M_{iP_i} = (M/M_i)_{P_i}$. The kernel of β is M_i. To show that the kernel of α is also M_i, it suffices to show that both γ and δ are monomorphisms. Since M_i is P_i-primary, this is immediate for δ.

Since $\cap_j M_j = 0$ the natural map $\varphi: M \to \oplus M/M_j$ is a monomorphism. By Proposition 2.5 localization preserves monomorphisms, so $\varphi_{P_i}: M_{P_i} \to \oplus(M/M_j)_{P_i}$ is a monomorphism. The map γ is the i^{th} component of φ_{P_i}. Because P_i is minimal over the annihilator of M we know that P_j is not contained in P_i for $j \neq i$. Since M/M_j is P_j-coprimary, we have $(M/M_j)_{P_i} = 0$ for $j \neq i$, so the j^{th} component of φ_{P_i} vanishes, and we see that γ is a monomorphism as required.

d) If $U \cap P_i = \varnothing$ then $P_i[U^{-1}]$ is a prime ideal of $R[U^{-1}]$, and by Theorem 3 1 c), $M_i[U^{-1}]$ is $P_i[U^{-1}]$ primary. We see from Proposition 3 9 c) that $M_i[U^{-1}] = M[U^{-1}]$. Thus

$$0 = \bigcap_{i=1}^{t} M_i[U^{-1}]$$

is a primary decomposition. To see that it is minimal, it suffices by part b) to show that the associated primes of $M[U^{-1}]$ are the associated primes of M that do not meet U, and this also follows from Theorem 3 1 c). //

In Exercise A3.6 we present a different view of primary decomposition: It is the reflection, in M, of the fact that the injective envelope of M decomposes in a nice way. This point of view also explains the meaning of the irreducible decompositions defined in the proof above.

Primary Decomposition And Factoriality

It is easy to express the relationship between primary decomposition and unique factorization in the classical sense:

Proposition 3 11: Let R be a Noetherian domain.

a) If $f \in R$ and $f = u\Pi p_i^{e_i}$, in such a way that u is a unit of R, the p_i are primes generating distinct ideals (p_i), and each e_i is a positive integer, then $(f) = \cap(p_i^{e_i})$ is the minimal primary decomposition of (f).

b) R is factorial iff every prime ideal minimal over a principal ideal is itself principal.

Proof: a) First we show that $(p_i^{e_i})$ is a (p_i)-primary ideal. If Q is an associated prime of $(p_i^{e_i})$ then since Q contains a power of p we

have $Q \supset (p_i)$. If q is any element of Q, then q annihilates some element of $R/(p_i^{e_i})$, that is for some $f \notin (p_i^{e_i})$ we have $qf = p_i^{e_i}g$. Since $p_i^{e_i}$ divides qf but not f, and since p_i is prime, we see that p_i divides q. this shows $Q \subset (p_i)$ as required.

Clearly we have $(f) \subset \cap(p_i^{e_i})$; we wish to show equality. By induction on the number of primes p_i involved, it suffices to show that if g is not divisible by a prime p, then $(g)\cap(p^e) = (gp^e)$. But if $fg \in (p^e)$, then since p does not divide g and p is prime, p must divide f, and $(f/p)g \in (p^{e-1})$. Repeating this argument, we eventually see that p^e divides f, so $fg \in (gp^e)$.

We now see that $(f) = \cap(p_i^{e_i})$ is an primary decomposition. Thus every prime of Ass R/(f) is one of the (p_i). Each (p_i) is contained in an associated prime of (f) because p_i is a zerodivisor modulo (f): For p_i divides f and $p_i(f/p_i) \in (f)$. Thus the given primary decomposition is minimal.

b) Suppose R is factorial. If $f = u\Pi p_i^{e_i}$ is the prime factorization of an element, then by part a) the associated primes of (f), and thus in particular the minimal primes of R that contain f, are the principal primes (p_i).

Converely, suppose that every prime ideal minimal over a principal ideal is itself principal. To prove that R is factorial, the argument given in Chapter 0 shows that, since R is Noetherian, it is enough to check that any irreducible element $f \in R$ is prime. But if P is a prime minimal over (f) then by hypothesis we may write P = (p) for some $p \in R$, and $f \in P$ becomes f = rp for some $r \in R$. Since f is irreducible, r must be a unit, so (f) = (p) = P is prime.//

We shall sharpen this result a little in Chapter 10.

Primary Decomposition In The Graded Case

If R is a graded Noetherian ring and M a finitely generated graded R-module then the associated primes of M are homogeneous, a primary decomposition of 0 in M can be made in terms of homogeneous modules, and M has a filtration as in Proposition 3 7 where the M_i and P_i are homogeneous. The proofs of these things involve only one new idea, given in Proposition 3 12 below, and we leave the details to the reader. We state the Proposition here for ordinary graded rings $R = R_0 \oplus R_1 \oplus \ldots$, but in fact it holds (with the same proof!) for $\mathbb{Z}$-graded rings and modules, and much more generally. See Exercise 3 5.

Proposition 3 12: Suppose that $R = R_0 \oplus R_1 \oplus \ldots$ is a graded ring, and M is a graded R-module. Let $m \in M$ be any element, and set P = ann m $\subset$ R. If P is prime, then P is homogeneous and P is the annihilator of a homogeneous element.

Proof: Any $f \in R$ may be expressed in a unique way as a sum $f = \Sigma_{i=1}^{s} f_i$, where each f_i is nonzero and homogeneous of some degree d_i, and $d_1 < \ldots < d_s$. We may prove that P is homogeneous by showing that if $f \in P$ then $f_i \in P$ for each i. By induction on s it suffices to show that $f_1 \in P$. Thus we suppose that fm = 0 and we wish to prove that $f_1 m = 0$.

We may also write $m = \Sigma_{i=1}^{t} m_i$, in a unique way so that each m_i is nonzero and homogeneous of some degree e_i, and $e_1 < \ldots < e_t$. We do induction on the number of terms t. Since $fm = f_0m_0$+(terms of higher degree), we see that $f_1m_1 = 0$. Thus if t = 1 we are done. Suppose t > 1, and that the result has been proven for all smaller values of t.

The element $f_1m = \Sigma_{i=2}^{t} f_1m_i$ is a sum of fewer homomgeneous terms than is m. Set I = ann f_1m. Note that P $\subset$ I. If P = I then P is homogenous by the induction, and we are done. Otherwise we may choose an element $g \in I$, such that $g \notin P$. We have $gf_1m = 0$, so $gf_1 \in$ ann m = P. Since $g \notin P$, and P is prime, we have $f_1 \in P$ as claimed, proving that P is homogeneous.

From the fact that P is homogeneous it follows that $Pm_i = 0$ for each i. Since $P = \text{ann } m \supset \cap_i(\text{ann } m_i) \supset P$, we see that $P = \cap_i(\text{ann } m_i) \supset \Pi_i(\text{ann } m_i)$. Since P is prime, we have $P \supset \text{ann } m_i$ for some i, whence $P = \text{ann } m_i$, and we are done. //

Extracting Information From Primary Decomposition

We maintain the assumptions **that R is a Noetherian ring, and we shall assume that M is a finitely generated R-module.**

We have already seen that if $0 = \cap_i M_i$ is the minimal primary decomposition, then the M_i corresponding to minimal primes of Ass M, are uniquely determined by M, and thus might be expected to shed some light on the structure of M, whereas the M_i corresponding to embedded primes are not in general uniquely determined (we shall analyze this phenomenon in a moment). The same mechanism that leads to the uniqueness of the M_i corresponding to the minimal primes carries us a little further, and shows that certain intersections of primary components are well-defined. It turns out that these intersections correpond to the sets of associated primes containing a given ideal -- that is, to the closed subsets of Spec A in the Zariski topology introduced in Chapter 1.

To express the intersections above, we shall make the following definition: For any ideal $I \subset R$, we set

$$H_I^0(M) = \{ m \in M \mid I^n m = 0 \text{ for } n \gg 0\},$$

the set of elemen s annihilated by some power of I. The notation comes from local cohomology; see Appendix 4, in which functors $H_I^i(M)$ are defined for all i. (Pursuing the analogy with sheaf theory from which local cohomology arises, some authors also write $\Gamma_I(M)$ for what we have called $H_I^0(M)$.)

The set $H_I^0(M)$ is easily seen to be a submodule of M. It actually depends only on the radical of I, in the sense that $H_I^0(M) = H_J^0(M)$ if $\text{rad}(I) = \text{rad}(J)$.

Proposition 3 13: Let I be an ideal of R, and let

$$A = \{P \in \text{Ass } M \mid P \supset I\}.$$

a) Let $0 = \cap_i M_i$ be a primary decomposition of $0 \subset M$, and suppose M_i is P_i-primary. The submodule $H_I^0(M)$ is the intersection of those M_i such that $P_i \notin A$. In particular, this intersection is independent of the primary decomposition chosen.

b) There is an element $f \in I$ such that $P \in A$ iff $P \in \text{Ass } M$ and $f \in P$. For any such f we have

$$H_I^0(M) = \ker (M \to M[f^{-1}]).$$

c) We have $\text{Ass } H_I^0(M) = A$, and $\text{Ass } M/H_I^0(M) = (\text{Ass } M) - A$. These properties characterize $H_I^0(M)$ uniquely.

Proof: a) We may write $H_I^0(M) = (0 :_M I^\infty) := \cup_n(0 :_M I^n)$, where $(0 :_M I^n) = \{m \in M \mid I^n m = 0\}$. Using the given primary decomposition we get

$$H_I^0(M) = ((\cap_i M_i) :_M I^\infty) = \cap_i (M_i :_M I^\infty).$$

A power of P_i annihilates M/M_i so if $P_i \supset I$ then $(M_i :_M I^\infty) = M$, and we may drop this component from the intersection. On the other hand, if $P_i \not\supset I$ then I contains a nonzerodivisor on M/M_i, so $(M_i :_M I^\infty) = M_i$. The desired formula for $H_I^0(M)$ follows.

b) By Prime Avoidance we may choose $f \in I$ not in any of the finitely many primes $Q \in (\text{Ass } M) - A$. Set $N = \ker (M \to M[f^{-1}])$. By Proposition 2.1 we have $N = (0 :_M f^\infty)$. By the argument of part a),

applied to the ideal (f) in place of I, this is the intersection of those M_i such that $P \not\supset f$, the same as $H^0_I(M)$.

c) By part a) the primary decomposition of $H^0_I(M)$ in M is

$$H^0_I(M) = \cap_{i \text{ such that } P_i \notin A} M_i.$$

If we choose the primary decomposition $0 = \cap_i M_i$ to be irredundant, then we get an irredundant primary decompostion of $H^0_I(M)$, and it follows from Theorem 3 10 that Ass $M/H^0_I(M)$ = (Ass M) - A. Further, by Lemma 3 6 b) we see that Ass $H^0_I(M)$ is a subset of primes of Ass M that contains (Ass M) - A. Since every element of $H^0_I(M)$ is annihilated by a power of I, it follows that the primes of Ass $H^0_I(M)$ all contain I. Thus Ass $H^0_I(M) = A$.

Conversely, let N be any submodule of M such that Ass N = A and Ass M/N = Ass M - A. If we choose f as in part b), then a power of f annihilates N and f is a nonzerodivisor on M/N. If follows that N = ker $(M \to M[f^{-1}])$, so $N = H^0_I(M)$ by part b). //

The mechanism of part b) could be applied with any localization, but it does not yield any submodules other than the $H^0_I(M)$. See Exercise 3 12.

A typical application of part a) of the Proposition is to show that the intersection of all primary components corresponding to primes of dimension $\geq$ some number d is well defined. (See Chapter 9 for the definition of dimension.)

The most interesting case of Proposition 3 13 occurs when the ideal I is a prime P. The module $H^0_P(M)_P \subset M_P$ is then the unique largest submodule of finite length. It's length is called the **multiplicity of P in M.** We see from the Proposition (or directly from Theorem 3 1) that P is associated to M iff the multiplicity of P in M is nonzero. In general, one may think of the multiplicity as measuring "how associated" P is to M.

Somewhat surprisingly, there seems no general way to extract "invariant" information about M from a primary decomposition that is not covered by Proposition 3 13 (but in some special circumstances there is -- see for example Exercise 3 11). This has led some people to the view that one should ignore primary decomposition entirely; localization and the set of associated primes are together enough.

Why Primary Decomposition Is Not Unique

We take a moment to "explain why" the terms in a primary decomposition corresponding to embedded primes are not unique, and to explore some related ideas. Assume for simplicity that R is a local Noetherian ring, and that the finitely generated module M has two associated primes, a minimal prime Q and the maximal ideal P itself. If we write a minimal primary decompostion $0 = M' \cap M''$, where M' is Q-primary and M'' is P-primary, then by Theorem 3 10 c) $M' = \ker (M \to M_Q)$ is uniquely determined. However, as the reader may easily check, M'' may be taken to be any submodule such that

a) For some integer d, $M'' \supset P^d M$

and

b) $M'' \cap M' = 0$.

In particular, we could simply take $M'' = P^d M$ for any sufficiently large d.

One may try to avoid the problem by taking M'' maximal satisfying properties a,b. However, uniqueness is prevented even then, essentially by the fact that the complement of a vector space is not unique. For example, let k be a field and let $R = k[x]_{(x)}$ be a

localization of the polynomial ring in one variable. Let $M = R \oplus R/(x)$, and let e be a generator for the second summand. With notation as above, $Q = 0$, $P = (x)$, and $M' = Re$, the second summand. Here M", may be any nonzero submodule meeting Re in 0. The maximal choices for M" are precisely the complements of the second summand, Re; these are the modules generated by elements of the form (1,ue), with $u \in k$. Since any two such elements are carried into one another by an automorphism of M, there is no distinguished choice for M". (Some more examples are given in Exercise 3 10.)

In situations where "nice" subspaces have distinguished complements (for example in the presence of a suitable group action) there are sometimes distinguished primary decompositions, however. See Exercise 3 11.

Geometric Interpretation Of Primary Decomposition

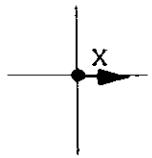
If k is an algebraically closed field and $I \subset S = k[x_1, \ldots, x_r]$ is an ideal, we can hope to "see" some of the meaning of a primary decomposition of I. Let $I = \cap_j I_j$ be a minimal primary decomposition. It follows of course that $Z(I) = \cup_j Z(I_j)$. If I is a radical ideal, then each of the I_j is a prime ideal minimal over I, and the primary decomposition simply expresses the algebraic set Z(I) as the union of the irreducible algebraic sets (algebraic varieties) $Z(I_j)$. But in more general cases the algebra suggests more. What we shall do here informally is formalized in the theory of schemes; see for example Eisenbud-Harris [1992] for an expository treatment in the spirit of this text, and Hartshorne [1977, Ch. 2] for more technical detail.

Let us begin with the case of an ideal $I \subset S = k[x,y]$ that is primary to the maximal ideal (x,y), so that Z(I) is the origin in the affine plane. For example, what geometric object X should be associated with the primary ideal (x^2,y)? The idea is that X should be that geometric object that determines the coordinate ring S/I. If

$$f = a_0 + a_1x + a_2y + a_3x^2 + a_4xy + a_5y^2 + a_6x^3 + \ldots$$

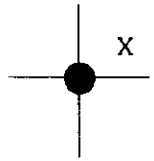
is a polynomial, then the class of f modulo (x^2,y) we can read off the scalars $a_0 = f(0,0)$ and $a_1 = \partial f/\partial x(0,0)$. That is, if we restrict a function to X, then we "see" the value of the function at the origin -- so the point (0,0) should be "in" X -- and the value of the first derivative of f in the horizontal direction. There is a standard geometric object of this kind: it is the origin plus the horizontal tangent vector at the origin!

$I = (x^2,y)$ corresponds to X, a point with tangent vector



In a similar way, if we take $I = (x^2, xy, y^2)$, then the class of f modulo I reveals the value of f at 0 and the value of the first derivative of f in any direction. Thus it is natural to think of the corresponding X as the whole first order infinitesimal neighborhood of the origin in the plane,

$I = (x^2, xy, y^2)$ corresponds to X, the first-order infinitesimal neighborhood of (0,0).

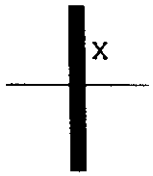


If we replace I by, for example, the n^{th} power $(x,y)^n$, then all the derivatives of f up to order n-1 are visible modulo I, so the corresponding geometric object X is the n^{th} infinitesimal neighborhood.

Similar considerations are suggestive in higher-dimensional cases, too. For example, the ideal $(x) \subset k[x,y]$ corresponds to Z((x)), the vertical line in the plane, while modulo (x^2) one can see the values of a function f(x,y) at every point on the vertical line together with

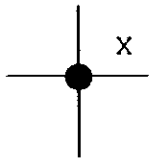
the values of it's first derivatives in the horizontal direction at any point of the line. Thus (x^2) corresponds to the vertical line with all the horizontal tangent vectors at points of the line -- that is the first order neighborhood of the vertical line:

$I = (x^2)$ corresponds to X, the first-order infinitesimal neighborhood of the vertical line.



From these ideas it is easy to see how to interpret more or less arbitary primary decompositions. For example, $I = (x) \cap (x^2, xy, y^2)$ corresponds to the vertical line together with the first order neighborhood at the origin

$I = (x) \cap (x^2, xy, y^2)$ corresponds to X, the vertical line plus the first-order infinitesimal neighborhood of (0,0).



Here the primary decomposition is not unique, and we could also write $I = (x^2, xy) = (x) \cap (x^2, y)$, corresponding to the fact that the only information about a function f that is available on the first order infinitesimal neighborhood of the origin but not on the vertical line is the derivative of the function in the horizontal direction.

Symbolic Powers and Functions Vanishing to High Order

If P is a maximal ideal of R and I is any proper ideal containing a power of P, then I is P-primary: for in this case P is the only prime containing the annihilator I of R/I, so Theorem 3 1 a) shows that Ass $R/I = \{P\}$. This generalizes the fact that any power of a prime in the integers is primary.

In particular, the powers of a maximal ideal are all primary. One would be tempted to hope that a power of any prime ideal P would be P-primary, but this is not the case. In general, the P-primary component of the n^{th} power of P is called the **n^{th} symbolic power** of P, and is written $P^{(n)}$. In the geometric case, the symbolic powers of P have a nice geometric description, due to Zariski and Nagata:

Suppose that k is an algebraically closed field of characteristic 0 and $S = k[x_1, \ldots, x_r]$ is a polynomial ring. Let X be the variety corresponding to the prime ideal $P \subset S$, so that P is the set of all polynomials vanishing on X. For $n \geq 1$, let

$$P^{\langle n \rangle} = \{f \in S \mid f \text{ vanishes to order} \geq n \text{ at every point of } X\}.$$

The condition that f vanishes to order n at a point $x \in \mathbf{A}^r$ means that if $\mathfrak{m}_x$ is the maximal ideal of S consisting of functions vanishing at x, then $f \in \mathfrak{m}_x^n$; equivalently, the Taylor expansion of f around x begins with terms of order $\geq n$. Thus we may also write

$$P^{\langle n \rangle} = \cap_{x \in X} \mathfrak{m}_x^n.$$

If the characteristic of k is 0, then $P^{\langle n \rangle}$ can be defined in another way as well: it is the set of polynomials that vanish together with their partial derivatives of orders $< n$ at all the points of X. (In characteristic p, this is a weaker condition, and not so interesting: the derivatives of order $\geq p$ of the function x_1^m are identically 0.) We have:

Theorem 3 14 (Zariski, Nagata): Suppose that k is an algebraically closed field and S is a polynomial ring over k. If P is a prime ideal of S, then $P^{\langle n \rangle} = P^{(n)}$, the n^{th} symbolic power.

Theorem 3 14 is true (with suitable interpretation) in a much broader setting. See Eisenbud-Hochster [1979] for history and

details.

Partial Proof: We shall prove in characteristic 0 that $P^{\langle n\rangle}$ is P-primary and contains P^n. It follows that $P^{\langle n\rangle}$ contains $P^{(n)}$. We only sketch the opposite inclusion; for a full proof see the paper mentioned above, and the references there. It is obvious that $P^{\langle n\rangle}$ is an ideal and that $P^{\langle n\rangle} \supset P^n$. To show that $P^{\langle n\rangle}$ is P-primary we must show that if $r \notin P$, but $rs \in P^{\langle n\rangle}$ then $s \in P^{\langle n\rangle}$.

If $\mathfrak{m}$ is a maximal ideal of S containing P such that $r \notin \mathfrak{m}$ then since $rs \in \mathfrak{m}^n$ and $\mathfrak{m}^n$ is $\mathfrak{m}$-primary we must have $s \in \mathfrak{m}^n$. It follows that the derivatives of order $< n$ of s all vanish on the set $Y = \{x \in X \mid r(x) \neq 0\}$. Let g be such a derivative. Since rg vanishes at every point of X, we have $rg \in P$ by the Nullstellensatz. Since $r \notin P$ by hypothesis, it follows that $g \in P$. Under the hypothesis that k has characteristic 0 we deduce that s vanishes to order $\geq n$ on X, proving that $P^{\langle n\rangle}$ is P-primary. Because of the uniqueness of primary components associated to minimal associated primes, we deduce also $P^{\langle n\rangle} \supset P^{(n)}$.

Here is the idea of the proof that $P^{\langle n\rangle} \subset P^{(n)}$: Since $P^{(n)}$ is P-primary, it is enough to show that $(P^{\langle n\rangle})[U^{-1}] \subset (P^{(n)})[U^{-1}]$ for some multiplicatively closed set U not meeting P. We shall later show that there exists an element $u \in P$ such that for any point $x \in X$ with $u(x) \neq 0$, with corresponding maximal ideal $\mathfrak{m} = \mathfrak{m}_x$, there is a set of generators $y_1, \ldots, y_r$ of $\mathfrak{m}_{\mathfrak{m}}$ such that $P_{\mathfrak{m}}$ is generated by a subset of the y_i. Under these circumstances the y_i act like a set of "variables" (see Corollary 10.14 and Exercise 17.13).

To see how the argument should go, we shift to the simpler case where P is generated by a subset of variables: $P = (y_1, \ldots, y_c) \subset k[y_1, \ldots, y_r]$. The polynomials $f(y_1, \ldots, y_r)$ all of whose derivatives of order $< n$ are in $(y_1, \ldots, y_c)$ are precisely the polynomials whose terms are all of degree at least n in $y_1, \ldots, y_c$ -- that is, the n^{th} power of P, and $P^{\langle n\rangle} = P^n$. The n^{th} power of $(y_1, \ldots, y_c)$ is also primary by Exercise 3 6, so $P^n = P^{(n)}$. The analogous statements are

also true in the original case. In particular, after inverting u we have $P^{\langle n\rangle} = P^n = P^{(n)}$, concluding the sketch. //

A Determinantal Example

These ideas suggest an explicit example of a prime whose square is not equal to its symbolic square (and we shall check the example directly). A good general reference for the material that follows is the book of Bruns and Vetter [1988], and the example we shall give is very close to the paper of DeConcini-Eisenbud-Procesi [1982]; in particular, all the unproved assertions encountered below are proved in these sources.

Consider the polynomial ring in 9 variables $S = k[(x_{ij})_{1\leq i,j\leq 3}]$ and the generic 3×3 matrix $G = (x_{ij})$ over S. Let P be the radical of the ideal $I_2(G)$ generated by the 2×2 minors of G. The algebraic set X defined by $I_2(G)$ in the set $M_3 = \mathbb{A}^9$ of all 3×3 matrices is the set of 3×3 matrices of rank ≤ 1. This set is irreducible, so that P is prime, as the following very typical geometric argument shows:

First, the algebraic set

$$Y := GL(3,k) = \{(g,y) \subset \mathbb{A}^9 \times \mathbb{A}^1 \mid g \text{ a } 3\times 3 \text{ matrix and } (\det g)y = 1\}$$

is irreducible because the corresponding ring is $k[(x_{ij})_{1\leq i,j\leq 3}][(\det g)^{-1}]$, a localization of the polynomial ring in 9 variables. The same is true of the algebraic set $Y\times Y \subset \mathbb{A}^{20}$; its ring is a localization of the ring of polynomials in 18 variables. Let $M_3 = \mathbb{A}^9$ be the set of 3×3 matrices over k. Choose any matrix m of rank exactly 1, and consider the morphism $Y\times Y \to M_3$ defined by $(g,h) \mapsto gmh$. Because any two nonzero matrices of rank 1 differ only by a change of basis in source and target, the image of φ is exactly X. If $X = X_1 \cup X_2$, with X_1 and X_2 algebraic subsets of X, then $\varphi^{-1}(X_1) \cup \varphi^{-1}(X_2) = Y\times Y$. Since $Y\times Y$ is irreducible, either $\varphi^{-1}(X_1) = Y\times Y$ or $\varphi^{-1}(X_2) = Y\times Y$, and thus $X_1 = X$ or $X_2 = X$, showing that X is

irreducible, too.

It is obvious that no linear form vanishes on all rank 1 matrices, so P contains no linear form. In fact $I_2(G)$ is prime, so $P = I_2(G)$ is the prime ideal of functions vanishing on the set of rank 1 matrices, but we shall not need this here.

Let $g = \det G$, the determinant of G. We claim that $g \in P^{(2)}$. Since P contains no linear forms P^2 is generated by forms of degree ≥ 4 and g is of degree 3, so this will show that $P^2 \neq P^{(2)}$.

Checking Theorem 3 14 against this example, we note that the partial derivatives of g with respect to the variables x_{ij} are 2×2 minors of G, so $g \in P^{<2>}$. If k has characteristic 0, then Theorem 3 14 applies to show that $g \in P^{(2)}$ as claimed.

We now give a direct proof. We must show that g becomes an element of P^2 after we localize at P. Now $x_{11} \notin P$, so it suffices to show that $x_{11}g \in I_2(G)^2$. This is easy to check: after multiplying the second and third columns of G by x_{11}, which changes the determinant to $x_{11}^2 g$, we may add multiples of the first column to the two other columns (not changing the determinant) to make the 1,2 and 1,3 elements of the matrix 0, as in Figure 3.1:

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} \mapsto \begin{bmatrix} x_{11} & x_{11}x_{12} & x_{11}x_{13} \\ x_{21} & x_{11}x_{22} & x_{11}x_{23} \\ x_{31} & x_{11}x_{32} & x_{11}x_{33} \end{bmatrix} \mapsto$$

$$\begin{bmatrix} x_{11} & 0 & 0 \\ x_{21} & x_{11}x_{22}-x_{12}x_{21} & x_{11}x_{23}-x_{13}x_{21} \\ x_{31} & x_{11}x_{32}-x_{12}x_{31} & x_{11}x_{33}-x_{13}x_{31} \end{bmatrix}.$$

Figure 3.1

Thus the determinant $x_{11}^2 g$ is the product of x_{11} and the determinant of the lower 2×2 submatrix

$$G' = \begin{bmatrix} x_{11}x_{22}-x_{12}x_{21} & x_{11}x_{23}-x_{13}x_{21} \\ x_{11}x_{32}-x_{12}x_{31} & x_{11}x_{33}-x_{13}x_{31} \end{bmatrix},$$

so that $x_{11}g = \det G'$. Since the entries of G' are 2×2 minors of the original matrix, $\det G' \in I_2(G)^2$, and thus $g \in P^{(2)}$.

In fact, it is known that $P^{(2)} = (P^2, g)$, and that a primary decomposition of P^2 is $P^2 = P^{(2)} \cap \mathfrak{m}^4$, where $\mathfrak{m}$ is the ideal generated by all the x_{ij}.

Here is a geometric proof that g vanishes to order ≥ 2 at any point $a \in X$. Since we are in characteristic 0, it suffices to show that the partial derivative $\partial g/\partial x_{ij}$ vanishes at a for every i,j. If we write e_{ij} for the matrix which has all its entries equal to 0 except for the i,j entry, and whose i,j entry is 1, then $\partial g/\partial x_{ij} = dg(a+te_{ij})/dt$, where t is a new variable. But since both a and e_{ij} have rank 1, every matrix of the form $a+te_{ij}$ has rank ≤ 2. Thus g vanishes identially on matrices of the form $a+te_{ij}$, and we see that the derivative is 0 as required.

More generally, we might ask for the primary decomposition of any power of any "determinantal" ideal. To be specific, if $G = (x_{ij})$ is the "generic" p×q matrix over the ring $S = k[x_{ij1\leq i\leq p, 1\leq j\leq q}]$ then for each n the ideal P_n generated by the n×n minors of G is prime. If $1 < n < \min(p,q)$ then the powers of P_n are not primary; however, the symbolic powers of P_n are known -- they are generated by certain products of minors of various orders -- and a primary decomposition of the powers has the form

$$*) \quad P_n^m = P_n^{(m)} \cap P_{n-1}^{(2m)} \cap \ldots \cap P_1^{(nm)}.$$

The decomposition *) can be made minimal by taking only the first $\alpha(k,n)$ terms for a certain function $\alpha(k,n)$ -- see DeConcini-Eisenbud-Procesi [1982] for a precise statement, proof, and history of these matters.

Exercises

Exercise 3 1 : Let $R = \mathbf{Z}$, the ring of integers. Identify the associated primes of a finitely generated abelian group ($\mathbf{Z}$-module) in terms of the usual structure theory of finitely generated abelian groups.

Exercise 3 2 : If $M' = M_1 \cap M_2$ are submodules of a module M, show that $\operatorname{Ass} M/M' \subset \operatorname{Ass} M/M_1 \cup \operatorname{Ass} M/M_2$.

Exercise 3 3 *: If R is Noetherian and M and N are finitely generated R-modules, show that

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

where Supp M is the set of all primes containing the annihilator of M. (Hint: Show that it suffices to assume R is local and prove that the maximal ideal is in the set on the left hand side iff it is in the set on the right hand side. You will need to use Nakayama's Lemma.) Taking $M = R/I$, and setting $(0 :_N I) = \{n \in N \mid In=0\}$, show that $\operatorname{Hom}_R(M,N) = (0 :_N I)$, and thus

$$\operatorname{Ass} (0 :_N I) = \operatorname{Ass} N \cap \{P \subset R \mid P \text{ is a prime ideal and } I \subset P\}.$$

Exercise 3 4 * (Gauss' Lemma): Let R be any ring, and set $S = R[x_1, \dots, x_r]$, the polynomial ring in r variables. If $f \in S$ is a polynomial write Content(f) for the ideal generated by the coefficients of f.

a) If $f,g \in S$ then

$$\operatorname{Content}(fg) \subset \operatorname{Content}(f)\operatorname{Content}(g) \subset \operatorname{rad}(\operatorname{Content}(fg)).$$

Deduce that if Content(f) contains a nonzerodivisor of R, then f is a nonzerodivisor of S.

b) If R is Noetherian and f is a nonzerodivisor of S, show conversely that Content(f) contains a nonzerodivisor of R.

c) We say that f is **primitive** if Content(f) = (1). Gauss proved, in the case $R = \mathbf{Z}$ and r = 1, that the product of primitive polynomials is primitive, essentially to prove that if a primitive polynomial is irreducible in $\mathbf{Q}[x]$ then it is irreducible in $\mathbf{Z}[x]$. Prove that if R is a factorial domain with quotient field K, and if f is irreducible in R[x], then f is irreducible in K[x]. Then show that R[x] is again factorial. (The key step is Gauss' Lemma, applied to products of primitive polynomials.)

General Graded Primary Decomposition

Exercise 3 5 : Let Γ be an abelian monoid (that is, a set with a commutative associative addition operation posessing an identity element 0), and let $R = \oplus_{\gamma \in \Gamma} R_\gamma$ be a ring graded by Γ, in the sense that each R_γ is an abelian group and $R_\gamma R_{\gamma'} \subset R_{\gamma+\gamma'}$. We say that Γ acts on a set Λ if we are given a map $\Gamma \times \Lambda \to \Lambda$, denoted $(\gamma,\lambda) \mapsto \gamma+\lambda$ and the associative law $\gamma+(\gamma'+\lambda) = (\gamma+\gamma')+\lambda$ holds. We say that Γ acts freely on Λ if $\gamma+\lambda = \lambda$ only when $\gamma = 0$. If M is an R-module, we say that M is graded by Λ if $M = \oplus_{\lambda \in \Lambda} M_\lambda$ as abelian groups and $R_\gamma M_\lambda \subset M_{\gamma+\lambda}$ for any $\gamma \in \Gamma$, $\lambda \in \Lambda$. An element of R is called homogeneous if it belongs to one of the R_λ, and similarly for M. Every element of R or M can be written as a sum of nonzero homogeneous elements in a unique way; these are called its homogeneous components. An ideal $I \subset R$ is called homogeneous if it can be generated by homogeneous elements. Show that I is homogeneous iff I contains the homogeneous components of each of its elements.

a) Suppose that both Γ and Λ are totally ordered sets and that Γ acts freely on Λ in such a way that if $\gamma \le \gamma' \in \Gamma$ and $\lambda \le \lambda' \in \Lambda$ then $\gamma+\lambda \le \gamma'+\lambda'$. Prove that with this notation, if $\gamma \le \gamma'$, $\lambda \le \lambda'$ and $\gamma+\lambda = \gamma'+\lambda'$, then $\gamma = \gamma'$ and $\lambda = \lambda'$. We say that the action of Γ on Λ is

compatible with the orders.

b) Suppose that Γ is a totally ordered abelian monoid and R is a ring graded by Γ. Suppose also that M is an R-module, graded by a totally ordered set Λ on which Γ acts freely in a way compatible with the order. If $P \subset R$ is a prime ideal that is the annihilator of an element of M adapt the argument of Proposition 3 12 to show that P is homogeneous and that P is in fact the annihilator of a homogeneous element of M.

c) Suppose that R is a Noetherian ring, M is a finitely generated R-module, and that R and M are graded as in part b). Show that Ass M consists of homogeneous prime ideals. Show that $0 \subset M$ has a primary decomposition into homogeneous submodules. Show that in the filtration of Proposition 3 7 the M_i and the P_i may be taken to be homogeneous.

d) Let $R = k[x,y]$, Let Γ be the abelian group $\mathbf{Z}/(2)$ with elements written 0 and 1. We give R a grading by Γ, letting R_0 be the set of polynomials whose terms all have even degree in y, and R_1 the set of all polynomials whose terms have odd degree in y. The element x^2+y^2 is homogeneous of degree 0. Let $M = R/(x^2+y^2)$. Show that M is also graded by Γ. Show that the prime ideal $P = (x-y)$ is the annihilator of an element of M, but that P is not homogeneous. (By part b), this shows that $\mathbf{Z}/(2)$ cannot be ordered in such a way that the action of $\mathbf{Z}/(2)$ on itself is compatible with the order. Prove this directly.) Show that $0 \subset M$ does not have a primary decomposition by homogeneous submodules of M.

Primary Decomposition Of Monomial Ideals:

Computing the primary decomposition of the ideal generated by an arbitrary set of polynomials is quite difficult. See for example Eisenbud-Huneke-Vasconcelos [1992] for algorithms and references. But for monomial ideals the job is relatively easy. See Heinzer,

Ratliff, and Shah [***] and Sturmfels, Trung and Vogel [***] for further information on monomial primary decomposition. See Eisenbud and Sturmfels [***] for the case of binomial ideals.

Let k be a field (or any domain). A **monomial ideal** is an ideal $I \subset k[x_0,\ldots,x_r]$ generated by monomials in the variables $x_0,\ldots,x_r$. .

Exercise 3 6 *: Which monomial ideals are prime? Irreducible? Radical? Primary?

Exercise 3 7 *: Find an algorithm for computing the radical of a monomial ideal.

Exercise 3 8 *: Find an algorithm for computing an irreducible decomposition, and thus a primary decomposition, of a monomial ideal.

Exercise 3 9 *: **Products of linear primes**

a) Let $I = (x_0)\cdot(x_0,x_1)\cdot \ldots \cdot(x_0,\ldots,x_r)$. Show that the associated primes of I are $(x_0), (x_0,x_1), \ldots, (x_0,\ldots,x_r)$.

b) More generally, for any subset $I \subset \{0, \ldots ,r\}$ let P(I) be the prime ideal generated by $\{x_i | i \in I\}$. Let $I_1, \ldots ,I_t$ be subsets of $\{0, \ldots ,r\}$, and set $I = \Pi_j P(I_j)$. Let Γ be the "incidence graph", whose vertices are the sets I_j, with an edge joining I_i and I_j iff $I_i \cap I_j \neq \emptyset$. Show that the associated primes of I are precisely those primes that may be expressed as $P(I_{j_1} \cup \ldots \cup I_{j_s})$ where $I_{j_1}, \ldots ,I_{j_s}$ forms a connected subgraph of Γ. (It may not be easiest to use the general algorithm above.)

The Question Of Uniqueness

Exercise 3 10 : a)* Let $R = k[a,b]/I$ where $I = (a) \cap (a,b)^2 = (a^2, ab)$. Show that (b^n) is (a,b)-primary in R, and that

$0 = (a) \cap (b^n)$

is a minimal primary decomposition of 0 in R for any $n \geq 1$.

b) Show that $(a+\lambda b^n)$ is also (a,b) primary for any nonzero $\lambda \in k$, and that

$0 = (a) \cap (a+\lambda b^n)$.

Show that each $(a+\lambda b^n)$ is maximal among those ideals $J \subset R$ with

$0 = (a) \cap J$;

thus the length of the rings R/J, for J a "maximal (a,b)-primary component of 0", is actually unbounded.

c) It may be objected that example b is unnatural in the sense that it gives an inhomogeneous primary decomposition of a homogeneous ideal. However, it can be "homogenized" as follows: Let $S = R[c]$. Show that $0 = (a) \cap (ac^{n-1}+\lambda b^n)$ are primary decompositions of 0 in S, and that $(ac^{n-1}+\lambda b^n)$ is maximal among homogeneous ideals that can be used as primary components.

d)* (Huneke, unpublished): For maximal associated primes in the homogeneous case there is a small positive result: Let $I \subset k[x_1, \ldots, x_r]$ be a homogeneous ideal and suppose that $R = k[x_1, \ldots, x_r]/I$ has the maximal ideal $(x_1, \ldots, x_r)$ as an associated prime. Show that there exists a number B such that if

$0 = J_1 \cap J_2 \cap \ldots$

is a primary decomposition of I by homogeneous ideals, and J_1 is maximal among the homogeneous ideals that can appear as an $(x_1, \ldots, x_r)$-primary component, then the length of the ring R/J_1 is bounded above by B.

Exercise 3 11 *: Uniqueness of maximal monomial primary decomposition (Bayer, Galligo, Stillman, unpublished): Show that if $I \subset k[x_1, \ldots, x_r]$ is a monomial ideal, then there is a unique minimal primary decomposition $I = \cap I_j$ of I for which each I_j is a monomial ideal, primary to an ideal P_j generated by a subset of the variables, and I_j is maximal among the possible monomial P_j-primary components.

Exercise 3 12 : Let M be a finitely generated module over the Noetherian ring R. Given any multiplicatively closed set $U \subset R$, the intersection of the primary components of 0 in M corresponding to those primes of Ass M not meeting U is the kernel of the localization map $M \to M[U^{-1}]$, and is thus independent of the primary decomposition chosen. Any such kernel may be written as $H^0_I(M)$ for some ideal $I \subset R$.

Determinantal Ideals

Exercise 3 13 : a) Let $M_r = \mathbb{A}^{r^2}$ be the affine space of r×r matrices over an algebraically closed field k. Show that if a polynomial f vanishes on all the matrices of rank s in M_r, then it must vanish on all matrices of rank s-1.

b) Use part a) and the idea of the proof given in the text for the case of 3×3 matrices of rank 1 to show that the set of r×r matrices of rank $\leq$ s is irreducible. (In fact the ideal of (s+1)×(s+1) minors of the generic r×r matrix is prime -- but this is somewhat harder to prove: see for example Bruns-Vetter [1988].)

c) Now show that, if P is the radical of the ideal of (s+1)×(s+1) minors of the generic r×r matrix, then the (s+2)×(s+2) minors are in the symbolic square of P.

Total Quotients

Exercise 3 14 : Use the finiteness of the set of associated primes of a Noetherian ring R to show that the total quotient ring K(R) has only finitely many maximal ideals -- they are the localizations of the maximal associated primes.

Exercise 3 15 : The construction of the ring of total quotients K(R) of a ring R (obtained from R by inverting all the nonzerodivisors of R) commutes with localization if the ring is reduced, but not in the general case. The problem has to do with embedded primes:

a)* If R is a reduced ring, show that for any multiplicatively closed set $U \subset R$ we have $K(R[U^{-1}]) = K(R)[U^{-1}]$.

b) If R is any ring and U is any multiplicatively closed subset, show that $K(R[U^{-1}]) = K(\ K(R)[U^{-1}]\ )$ is a localization of $K(R)[U^{-1}]$

c) Let k be a field, let $R = k[x,y,z]/(x^2, xy, xz)$, and let $P = (x,y)$. Show that

$K(R) = R_{(x,y,z)}$;
$R_P = k[y,z]_{(y)}$;
$K(R_P) = k(y,z)$;

and thus $K(R_P) \neq R_P \otimes K(R) = R_P$.

Exercise 3 16 : Give an example of an extension of finitely generated abelian groups for which the second inclusion of Lemma 3 6 b) is proper.

Prime Avoidance

Exercise 3 17 : The Prime Avoidance Lemma 3 3 is sharp:

a) Show that if $k = \mathbb{Z}/(2)$ then the ideal $(x,y) \subset k[x,y]$ is the union of 3 properly smaller ideals.

b) Let k be any field. In the ring $k[x,y]/(xy, y^2)$, consider the ideals $I_1 = (x)$, $I_2 = (y)$, and $J = (x^2, y)$. Show that the homogeneous elements of J are contained in $I_1 \cup I_2$, but that $J \not\subset I_1$ and $J \not\subset I_2$. Note that one of the I_j is prime.

Exercise 3 18 : Prime avoidance usually fails for infinite sets of primes -- but not always.

a) Show that in k[x,y] the ideal (x,y) is contained in an infinite union of primes P_i such that no P_i contains (x,y).

b) Suppose that $R = k[(x_j)_{j \in A}]$ is a polynomial ring with infinitely many variables indexed by a set A. Let $(A_i)_{i \in B}$ be a (possibly) infinite collection of mutually disjoint subsets of A, and for each $i \in B$ let P_i be the prime ideal generated by $(x_j)_{j \in A_i}$. Show that any ideal contained in the union of the P_i is contained in one of them. Conclude that if U is the multiplicative set $U = R - \cup_{i \in B} P_i$ then the maximal ideals of $S = R[U^{-1}]$ are precisely the ideals SP_i. See Exercise 9.6 for more about this example.

Exercise 3 19 * **(Refinements of prime avoidance):** Prove the following useful variants of Prime Avoidance:

a) Suppose R is a ring containing a field k, and let $I_1, \ldots, I_n$ be ideals of R. If $(f_1, \ldots, f_n) \not\subset I_i$ for $i = 1, \ldots, s$, then there is a nonzero homogeneous polynomial $g(t_1, \ldots, t_n) \in k[t_1, \ldots, t_n]$ with the property that

(*) $\sum a_i f_i \notin \cup_j I_j$
for all $(a_1, \ldots, a_n) \in k^n$ such that $g(a_1, \ldots, a_n) \neq 0$.

In particular, if k is infinite, then there is an element $(a_2, \ldots, a_n) \in k^{n-1}$ so that $f_1 + \sum_{i=2}^n a_i f_i \notin \cup_j I_j$.

b) Suppose R is a ring, and let $I_1, \ldots, I_n$ be prime ideals of R. If $f \in R$ and J is an ideal of R such that $f+J \not\subset I_i$ for $i = 1, \ldots, n$, then there is an element $g \in J$ with the property that

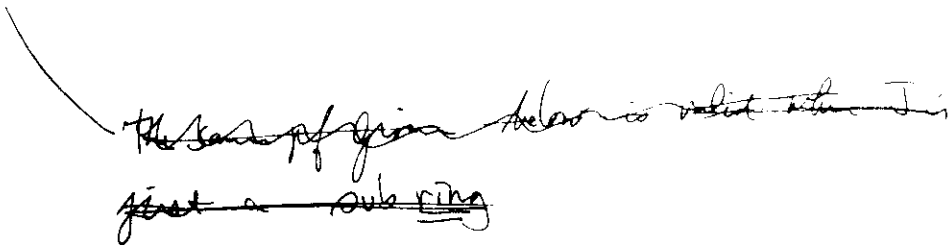
$$f + g \notin \cup_j I_j.$$

In particular, if $(f_1, \ldots, f_s) \not\subset I_i$ for $i = 1, \ldots, n$, then there is an element $(a_2, \ldots, a_n) \in R^{n-1}$ so that $f_1 + \Sigma_{i=2}^{n} a_i f_i \notin \cup_j I_j$.

Exercise 3 20 : Let M be a finitely generated module M over a Noetherian ring R. Proposition 3 4 immediately implies that the set of elements of R that are zerodivisors on M is a union of primes. Here is a method, due to Kaplansky, for showing directly that this set is a finite union of primes: Consider

$$\mathfrak{P} = \{(P,m) \mid P \text{ is a maximal annihilator ideal and } P = \operatorname{ann} m\}.$$

Let $M' \subset M$ be the submodule generated by all the m's that occur as second members of pairs in $\mathfrak{P}$. Let $m_1, \ldots, m_n$ be a finite set of these m_i that generate M', and let $P_1, \ldots, P_n$ be the corresponding primes. Show that the set of zerodivisors on M is $P_1 \cup \ldots \cup P_n$.



Hints

Exercise 3 3 : Since all the sets of primes involved behave well with respect to localization, it suffices to prove that if R is a local ring then a prime P is in $\operatorname{Ass} \operatorname{Hom}_R(M,N)$ iff it is in $\operatorname{Supp} M \cap \operatorname{Ass} N$. If P is in Supp M, show using Nakayama's Lemma that there is a surjection $M \twoheadrightarrow R/P$. If P is also in Ass N, there is an inclusion $R/P \subset N$. The composition $\varphi \in \operatorname{Hom}_R(M,N)$ of these two maps is annihilated by P, so $P \in \operatorname{Ass} \operatorname{Hom}_R(M,N)$. Conversely, if $P \in \operatorname{Ass} \operatorname{Hom}_R(M,N)$, then we can choose $0 \neq \varphi \in \operatorname{Hom}_R(M,N)$ with annihilator P. It follows that $M \neq 0$, so $P \in \operatorname{Supp} M$, and that $\operatorname{im} \varphi \subset N$ is annihilated by P, so $P \in \operatorname{Ass} N$.

Exercise 3 4 : a) The inequality $\operatorname{Content}(fg) \subset \operatorname{Content}(f)\operatorname{Content}(g)$ is obvious. To prove the second inequality, it is enough to show that if a prime $P \subset R$ contains Content(fg) then it contains Content(f)Content(g). Factoring out P, we may assume that R is a domain and P is 0, and we must show that if $fg = 0$ then f or $g = 0$. Since S is now a domain, this is obvious.

b) If R is Noetherian and Content(f) consists of zerodivisors, then Content(f) annihilates a nonzero element of R by Theorem 3 1. It follows that f annihilates this same element viewed as an element of S.

≡≡ Cited Item Has Been Deleted ≡≡ : To show that R is factorial, it suffices to show that irreducible elements are prime.

Exercise 3 6 : Answers: Ideals generated by subsets of the variables; ideals generated by powers of some of the variables; ideals generated by square-free (that is, multilinear) monomials; ideals containing a power of each of a certain subset of the variables, and generated by elements involving no further variables.

Exercise 3 7 , Exercise 3 8 : Let I be a monomial ideal. The key point is that if m is a minimal generator of I, and we can factor m

into relatively prime parts $m = m' m''$ then $I = (I + (m')) \cap (I + (m''))$. It is also useful to note that a monomial n is in I iff it is divisible by one of the minimal generators of I.

Exercise 3 9 : a) Do induction on r, inverting x_r and using Theorem 3 1.

b) With an induction as in the Hint for part a, it suffices to show that $\mathfrak{m} = (x_0, \ldots, x_r)$ is an associated prime iff Γ is connected. If Γ is connected, let T be a spanning tree (that is, a connected subgraph of Γ containing all the vertices, and whose edges form no loops). For each edge e of T, let i_e be an element of the intersection of the two sets corresponding to the vertices incident to e. Show that $\mathfrak{m}$ is associated by showing that $\mathfrak{m} \prod_{e \in T} x_{i_e} \subset I$. Conversely, if Γ is not connected, we may partition Γ into two subgraphs Γ_1 and Γ_2 that are not connected to each other. Let I_1 and I_2 be the corresponding subproducts of primes, so that $I = I_1 I_2$, and I_1 and I_2 involve disjoint subsets of the variables. Show that $I_1 I_2 = I_1 \cap I_2$, and thus the associated primes of R/I are those of I_1 (which involve only the first set of variables) and those of I_2, involving only the second.

Exercise 3 10 a): As a vector space the ring R is $k[b] \oplus ka$.

d) J_1 must contain all forms of degree $\geq d$, where d is the maximal degree of a nonzero homogeneous element of $(0 : (x_1, \ldots, x_r))$.

Exercise 3 11 : First, let $\delta = x_1, \ldots, x_s$ be a subset of the variables $x_1, \ldots, x_r$. Relating each monomial ideal to its minimal set of monomial generators, observe that there is a one to one correspondence between monomial ideals primary to (δ) and monomial ideals primary to the irrelevant ideal in $K[x_1, \ldots, x_s]$, where $K = k(x_{s+1}, \ldots, x_r)$ is the field of rational functions in the remaining variables.

Use this observation, together with the fact that primary decompositions localize, to reduce the problem to the following special case:

Let $\mathfrak{m}$ be the irrelevant ideal of $S = k[x_1, \ldots, x_r]$. Suppose that if I is a monomial ideal of S, and $I = I' \cap J$ where I' is a monomial ideal having no $\mathfrak{m}$-primary component and J is an $\mathfrak{m}$-primary monomial ideal. In this case the unique maximal monomial choice of J is the ideal generated by all those monomials NOT dividing any of the finitely many monomials in I' but not in I. (The finiteness of this set implies that J contains a power of each variable -- and is thus $\mathfrak{m}$-primary).

Exercise 3 15 **a)**: In this case all the prime ideals of K(R) are maximal ideals of K(R).

Exercise 3 18 : Suppose that $f \in \cup_{i \in B} P_i$ and suppose that

$$\{P_1, \ldots, P_n\} = \{ P_i \mid \text{some monomial of } f \text{ is in } P_i\}.$$

Show that if g is a polynomial such that g and f+g are in $\cup_{i \in B} P_i$, then $g \in \cup_{m=1}^{n} P_m$. Conclude that if $f \in I \subset \cup_{i \in B} P_i$, then $I \subset \cup_{m=1}^{n} P_m$ and thus I is contained in one of the $P_1, \ldots, P_n$.

Exercise 3 19 : a) Regard the subspace in R generated by $f_1, \ldots, f_n$ as an image of an n-dimensional vector space V. Let W_j be the preimage of I_j in V, and write $f_1, \ldots, f_n$ again for the basis elements of V. Let m_j be the dimension of W_j. Consider the $n \times (m_j+1)$ matrix M_j whose first column is $(t_1, \ldots, t_n)$ and whose other m_j columns represent a basis for W_j. The $(m_j+1) \times (m_j+1)$ minors of M_j are linear forms in the t_i. For each j, the condition $\Sigma a_i f_i \notin W_j$ is the condition that one of these forms is nonzero at $(a_1, \ldots, a_n)$. Since not all the f_i are in W_j, one of these linear form is not identically 0; call it L_j. The polynomial g may be taken to be $\prod_j L_j$.

b) We do induction on n, the case $n = 1$ being trivial. We may suppose that none of the primes $I_1, \dots, I_n$ contains another of the I_j. By induction we may choose $j_1 \in J$ such that $f + j_1 \notin \cup_{k=2}^{n} I_k$. If $f+j_1 \notin I_1$ we are done, so suppose that $f+j_1 \in I_1$.

Since $f + j_1 + J = f+J \not\subset I_1$ we must have $J \not\subset I_1$. Since I_1 is prime we therefore have $J \cap \cap_{k=2}^{n} I_k \not\subset I_1$. Let $j_2 \in J \cap \cap_{k=2}^{n} I_k$ be an element outside I_1. It is easy to see that $f + j_1 + j_2 \notin \cup_{k=1}^{n} I_k$.