LECTURE 4-7

We now give the definition of primary submodule in a general context, following Chapter 4 of Atiyah-Macdonald (including the exercises in this chapter). Let M be any module over any ring R. Call a submodule N of N *primary* if every zero-divisor on M/N is nilpotent, where $x \in R$ is (defined to be) a zero-divisor on M/N if there is $y \in M/N, y \neq 0$ with $xy = 0$, while x is nilpotent if there is an integer k with $x^k(M/N) = 0$. By the binomial theorem, which holds for any commutative ring, the set of nilpotent element in R on any fixed module M' is an ideal; if this coincides with the set of zero-divisors on M', this ideal is prime. We therefore more precisely call N *P-primary* if it is primary and the set of zero-divisors on M/N is the prime ideal P. It is not difficult to check that if M is finitely generated and R is Noetherian, then a P-primary submodule in this sense is the same as a P-primary module in the earlier sense (but not in general). It is easy to check that a finite intersection of P-primary submodules is again P-primary, so given a submodule N that is a finite intersection $\cap N_i$ of primary submodules then we can combine terms and assume that each N_i is P_i-primary where the P_i are distinct primes. We may further assume, omitting terms as necessary, that no N_i contains the intersection of the others. The prime ideals P_i are said to *belong* to N; recall that the minimal primes among the P_i are called isolated and the others embedded.

Call a submodule N of M *decomposable* if it has a primary decomposition, i.e. it is the intersection of finitely many primary submodules (called its primary components). In general, submodules are not decomposable, but we have seen that any submodule of a finitely generated module over a Noetherian ring is decomposable. Even when they exist, primary decompositions need not be unique; but it turns out that they satisfy two important uniqueness properties. First, given a submodule N realized as in the previous paragraph as a finite intersection $\cap N_i$ where the submodule N_i is P_i-primary, the P_i are distinct prime ideals, and no N_i contains the intersection of the others, then the set of prime ideals P_i arising in this way (both isolated and embedded ones) is uniquely determined by N. To see this we may pass to the quotient and assume that $N = 0$. Then the annihilator $I(m)$ of m is the intersection of the annihilators $I_i(m)$ of the images of m in the quotients M/N_i and in turn the radical $\sqrt{I(m)}$ is the intersection of the radicals $\sqrt{I_i(m)}$. If $\sqrt{I(m)}$ is prime, this forces it to coincide with P_i for some i; conversely any P_i arises as $\sqrt{I(m)}$ for any m chosen to lie in the intersection of the N_j for $j \neq i$ but not in N_i. Hence the P_i are exactly the prime ideals of the form $\sqrt{I(m)}$ for $m \in M$ and so are determined by M alone; note that this result also gives us some idea of where to look for submodules N_i that could realize the submodule N as decomposable (having a finite primary decomposition), if we do not yet know whether N is decomposable or not.

The other uniqueness result pertains to the isolated primes $Q_1, \ldots, Q_j$ among the P_i: *the primary component N_i of N corresponding to any Q_i is uniquely determined by N.* This follows since it is easy to check that the localization N_S of any P-primary submodule N of M by a multiplicatively closed subset S of R is 0 if S meets P, while otherwise it is an $S^{-1}P$-primary submodule of $S^{-1}M$ intersecting M in N. Hence by localizing N by the complement of any isolated prime belonging to it and intersecting with M we recover the corresponding isolated component uniquely.

The failure of the embedded components to be unique is illustrated rather graphically by the following simple example. Let $R = K[x]_{(x)}$ be the localization of the polynomial ring $K[x]$ in one variable x over a field K at the complement of the prime ideal (x) and set $M = R \oplus R/(x)$. Here there are just two associated primes of M, namely 0 and (x); the isolated component of 0 in M is uniquely determined as Re, where e is a generator of the second summand. Even if we restrict to embedded components of M that are as large as possible, we find that the submodule generated by $(1, ue)$ for any $u \in K$ can be taken to be an embedded component; clearly no choice of such a component can be canonical as one can send any choice to any other by an automorphism of R.

Turning now to ideals in R, we find that any ideal I whose radical M is maximal in R is M-primary, for in this case the image of M in R/I is the only prime ideal and R/I consists only of units (not in this image) and nilpotent elements in it, so that every zero divisor is nilpotent. But in general even the powers P^n of a prime ideal P need not be P-primary; for example, if R is the quotient $K[x, y, z]/(xy - z^2)$, then the images xz of $x, z \in R$ generate a prime ideal P but $xy = z^2 \in P^2$ and $x, y^n \notin P$ for any n, since $y \notin \sqrt{P^2} = P$. Instead the powers P^n of P have P-primary components not equal to P^n in general; in the above case $P^2 = (x) \cap (y, z)$ is a primary decomposition with P-primary component (x). We denote the P-primary component of P^n by $P^{(n)}$ and call it the nth *symbolic power* of P.