ALGEBRA III
NOVEMBER 18, 2004

GABRIEL C. DRUMMOND-COLE

No class next week. I'll be at MIT.

I want to convince you that primary decomposition and localization are friends.

Let M be finitely generated over Noetherian R. Say $(0) = \cap_{i=1}^{n} M_i$ is a primary decomposition, minimal and irredundant. Let $p_1, \ldots, p_n$ be the associated primes. Because of irredundancy all the primes are associated; because of minimality each occurs once.

Now $p_i \supset ann(M)$ is minimal (minimal associated prime). The M_i corresponding to p is uniquely determined. So the M_i primary with respect to the associated primes are uniquely determined as the kernel of the localization map $M \to M_p$.

The rest are not unique, and the reason is simple. The nonminimal primes are essentially complements. You intersect them with the associated primes and get zero. If you don't have minimal ones then the complement is not unique.

So the only thing that is frozen is the geometric information. All I keep, all I think about, is the collection of p_i.

What else is frozen? If I take the intersection of all top dimensional components, that's perfectly well-defined. If you want to be as general as possible, there is a more general tool that captures what is unique in such a picture, and it is called "local cohomology."

Now, let me say in a word, every time you take the M_i and look for the p_i that are not contained in a given locus, that is still well-defined.

Let me define, for an ideal R which we think of as an algebraic set, $H_I^0(M) = \{m \in M | I^n m = 0 for n >> 0\} \subset M$. This is the zeroth local cohomology of M with support in I. What is this gadget? It looks kind of far-fetched. This is a functor from modules to modules. It has the following nice property; this is an exercise:

Exercise 1. *If* $0 \to M' \to M \to M'' \to 0$ *is exact then* $0 \to H_I^0(M') \to H_I^0(M) \to H_I^0(M'') \to ?$ *is exact.*

So $H_I^0(\cdot)$ is left exact.

In a certain sense the long exact sequence that is the obstruction to exactness of this functor is like sheaf cohomology. $H_I^i(M)$ is just like the $i-1$ cohomology of M.

This depends not on I but on $\sqrt{I}$; you care what the zero locus is.

Exercise 2. $H_I^0(M) = H_J^0(M)$ *if* $\sqrt{I} = \sqrt{J}$.

$H^0_I(M) = (0 :_M I^\infty) = \cup_{n\geq 0}(0 :_M I^n)$ is another way to write this.

Proposition 1. (1) *Bits and pieces are proved in Eisenbud and Matsamura and so on. Let $I \subset R, A = \{p \in Ass(M) : p \supset I\}$. If I have a primary decomposition then $H^0_I(M) = \cap_{j|p_j \notin A} M_j$. This is independent of the choice of the decomposition.*

What is the connection with localization. Primary decomposition and localization are morally equivalent. How much so?

(2) *There exists $f \in I$ such that $p \in A$ if and only if $P \in Ass(M)$ and $f \in p$; $H^0_I(M) = \ker(M \to M_f)$.*

[When M is projective is there a better result?]

Well, over a polynomial ring those will be free.

It's not very hard to prove; maybe I'm going to sketch it.

For the first part it's rather simple. What is $H^0_I(M)$? It's $(\cap_{i=1}^n M_i :_M I^\infty) = \cap(M_i : MI^\infty)$. We know that M/M_i is p_i-coprimary so the associator is p_i and a power of p_i vanishes it.

So either $p_i \supset I$ so that $(M_i :_M I^\infty) = M$. Then I can put it in the intersection without harm. So remember that $p_i \supset I$ if and only if $p_i \in A$, so I can drop these.

What about $p_i \not\supseteq I$. Then I claim $(M_i :_M I^\infty) = M_i$. This is because I contains a nonzero divisor modulo M_i. So this colon cannot be M and has to be M_i.

So this looks to the components which do not sit in the zero locus of I. This infinite colon does this.

For the second part, which is also easy, the f is, well, it's the same argument as before, but let me tell you what f is. I have a collection $p_i \notin A$ implies $p_i \not\supseteq I$ implies $I \notin \cup_{p_j \notin A} p_j$ by prime avoidance. If I is in a union of p_j it is in one of them.

Then I can find an $f \in I \setminus \cup_{p_j \notin A} p_j$. So the first part is clear. Now look at the kernel N of $M \to M_f$. This is $(0 :_M f^\infty)$.

I claim that the same proof as before shows that $N = \cap_{p_j \notin A} M_j$.

Exercise 3. *This is useful in some situations, not in what we did. Amuse yourself to take $Ass(H^0_I(M))$. This is finite length.*

Show that this is A.

(2) $Ass(M/H^0_I(M)) = Ass(M) \setminus A$.

This is not fundamental, it's just to test you know the definition.

Derived functors involve taking injective resolutions and then the cohomology. Do $0 \to M \to I^0 \to \cdots$; Here each I^i is injective and this is exact except at I^0, which has kernel M. Such a thing always exists, using injective hulls.

So in general when you have a funny functor, injectives will give you the right answers, but projectives will not.

Then $H^i_I(M)$ is the $\ker(H^0_I(J^i) \to H^0_I(J^{i+1}))/im(H^0_I(J^{i-1} \to H^0_I(J^i))$. This is a cohomology, not a homology; it has a cup product.

I don't want to get into this, it's complicated stuff and has to be built carefully.

So let's go back to simple things, integral dependence. Remember we argued something like $R_f = R[x]/(xf-1)$. I'm not going to remind you of the conditions. You attach something to R which satisfies something of degree one with coefficients in R. What happens to elements that satisfy an algebraic equation over I. When I have a finite covering, like a function, a branched cover. This boils down to looking, well, I have $R \subset S$. Then $x \in S$ is integral over R if it satisfies a monic polynomial with coefficients in I, $p(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$.

So $\mathbb{Z} \hookleftarrow \mathbb{Z}[i]$. Then i is integral over $\mathbb{Z}$ since it's a solution to x^2+1. Many rings in number theory are integral over other rings.

It generalizes localization and many other things. There is another phenomena. You want to add, starting from R, to its field of fractions $Q(R)$. From here you'd like to add everything that's integral. Why? Look to $\mathbb{Z}[2i]$. This is a nice ring. It's not the Gaussian integers; it's contained in them. So $\mathbb{Z}[2i]$ is not a UFD.

From the point of view of algebraic geometry, this usually tells you you have simple geometry; if you are factorial you have no interesting Picard group. Typically this improves geometry.

What makes this very much interesting is that the collection of all elements in S integral over R it forms a subring.

We'll come back but I need to make a detour. Let's rewrite the Cayley Hamilton theorem.

Theorem 1. *Cayley-Hamilton Let R be a ring, commutative with unit, I an ideal in R, M an R-module that can be generated by n elements.*

Let $\phi : M \to M$ satify $\phi(M) \subset IM$. Then there exists a monic polynomial $p(X)$ of degree n where $p_j \in I^j$ such that $p(\phi) = 0$.

Hard to recognize this as the Cayley Hamilton theorem.

So M is generated by $m_1, \ldots, m_n$. Also $\phi(m_i) \in IM$ so it can be written $\sum a_{ij} m_j$, with $a_{ij} \in I$.

So I can write $(\delta\phi - a_{ij}) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$

I could replace ϕ by x and say this is true if M is an $R[x]$ module and x acts on M by ϕ.

So now let's multiply this matrix, which we call N by N^*, so that $det(\delta x - a_{ij})$ applied to anything yields zero. Then $p(\phi) = 0$. So p is a characteristic polynomial. It's monic up to a sign because δ is ± 1.

So this is a polynomial whose coefficients are the traces of the wedge products.

Why is this important? It's one of the cheapest tricks for some of the most important lemmas, such as the Nakayama lemma, which is used maybe every second day in algebra.

Corollary 1. *If M is finitely generated, $I \subset R$ such that $IM = M$ then there exists x equal to $1 \mod I$ such that $xM = 0$.*

Let $\phi = id$. Then $\phi(M) = M \subset IM$, so that $(1 + \sum p_i)M = 0$. So this is $1 \mod I$.

Corollary 2. *(Nakayama's lemma)*
Suppose $IM = M$ and moreover that $I \subset \cap_{m \ maximal} m$, the Jacobson radical of R, then M is 0.

There is an x congruent to 1 mod I that multiplies M to zero. Now x does not lie in a maximal ideal because then 1 would lie in that maximal ideal, since $I+1$ does. So the element is invertible and multiplies M to zero, so M is zero.

This will tell you that there is a rank for any module, and if you have a module over a local ring, and you reduce to a vector space, generators you find will be generators for the original thing.

The same situation is here. Take an epimorphism ϕ as above. Then it is an isomorphism. There are a number of funny consequences. Again, no class next Tuesday. So we meet in a while. I recommend for those who want to read a little bit about Cayley-Hamilton, page five or six of Atiyah and MacDonald. It's half a page.

Some of you gave me some homework, but some of you did not. If you're registered for the class you should try to do something.