ALGEBRA III
NOVEMBER 30, 2004

GABRIEL C. DRUMMOND-COLE

I want to get back to integral closure. Just to give you the plan for what's left, I want to finish with integral closure. From this I can sketch a three line proof of a general Nullstellenstatz, and then talk about one dimensional rings, which account for Riemann surfaces and dedekind rings, and that's probably about all of what I can say. So most of the books just list some results at the beginning and I'll mention some of those. They relate dimension with some other characterizations.

We started with integral dependence. We proved last time the theorem which I called

Theorem 1. *Cayley Hamilton Theorem*
Let $I \subset R$ an ideal and M an R-module generated by n elements, and $\phi : M \to M$ an R-map such that $\phi(M) \subset IM$.

Then there exists a monic polynomial $p(x) = x^n + \sum_1^n a_i x^{n-i}$ with $a_i \in I^i$ and $p(\phi) = 0$. It's called Cayley Hamilton because it would be exactly that over a vector space.

I'm just recalling, since it's been a while and I will be using this at least four times today.

Corollary 1. *Let M be finitely generated and $I \subset R$ with $IM = M$. Then there exists an $x \equiv 1 \mod I$ such that $xM = 0$.*

Just use $\phi = id$.

Corollary 2. *Nakayama Lemma*
Let M be a finitely generated, $I \subset R$ such that $I \subset \cap m$, the intersection being the Jacobson radical $Jac(R)$, ranging over maximal ideals, and $IM = M$ then $M = 0$.

This is an application of the last result. $X - 1$ sits in every maximal ideal so if X was in a maximal ideal then 1 would be.

This is like invariance of dimension.

The special case used a lot is when R is a local ring, and I is contained in the unique maximal ideal. If I is in that maximal ideal and $IM = M$ then $M = 0$. That's usually one of the special cases. The other special case which is not a corollary but the proof is the same, is the following, an exercise:

Exercise 1. *Let $R = \oplus_{i=0}^{\infty} R_i$ be a graded ring and $m = \oplus_{i>0}^{\infty} R_i$ a maximal ideal. Then if $I \subset m$ is graded and M a finitely generated R-graded module, and $IM = M$, then $M = 0$.*

This is a graded version of Nakayama. The idea is to use homogeneity to prove things degree by degree. It's a good exercise. This one is used a lot in projective geometry, the other is used a lot in, say, algebra.

Let's try to improve the Nakayama lemma.

Corollary 3. *Let M be a finitely generated module, $N \subset M$ a submodule. Say $I \subset Jac(R)$ and $M = IM + N$. Then $M = N$.*

Keep in mind that R is not noetherian, there are even good examples if you play at home with R noncommutative.

If you think a little bit, this is a more general version of what we used to prove that the dimension was the same modulo an ideal.

How do you prove this? Consider M/N. Apply the Nakayama lemma for M/N. No matter what N does the quotient is finitely generated, and the maximal ideals are still the same.

Is this clear? Okay. One of the versions to use a lot is the following:

Corollary 4. *Let (R, m) be a local ring, $k = R/m$ the residue field, and M a finitely generated (you can improve this but to be honest with what I can prove here, I need to say only this case) R-module. Then M/mM is an $R/m = k$-module (k vector space). One of the nicest invariants of a vector space is its dimension.*

If $\bar{x}_1, \ldots, \bar{x}_n$ generate M/mM as a k vector space then $x_1, \cdots, x_n$ generate M as an R-module.

I'm pretty sure you've seen this. Any idea how we prove this? Let N be the submodule of M generated by $x_1, \cdots, x_n$. Then $M = mM + N$, since if I reduce mod m these things generate N.

Let's see a couple more consequences.

Corollary 5. *Let R be a ring, M a finitely generated R-module.*

(1) *If $\phi : M \to M$ is an epimorphism then ϕ is an isomorphism!*
This you know for vector spaces but it is also true for finitely generated modules.

(2) *If M is a free module isomorphic to R^n then any n elements of M that generate M form a basis. In particular you can't be isomorphic to R^n and R^m. So $rk(M)$ is well-defined.*

This fails even for vector spaces if you don't have finite generation. Let's prove this.

The first part can be proven in many ways. You could localize, you could check it for every maximal or every prime. I'll let you do it that way at home. But you can prove it directly with Cayley Hamilton by writing an explicit inverse. Look to M as an $R[t]$-module. How do you do this? t acts on M by ϕ. Then I is (t). If ϕ is an epimorphism then $IM = tM = \phi(M) = M$. So I have a finitely generated module over a ring and I have an endomorphism that does this. Then Cayley Hamilton for the identity tells you that there is a polynomial which is monic so that you get $(1 - q(t)t)M = 0$. I had to take the polynomial and apply it to the identity to get a 0 map. But how does $q(t)t$ act? This is $(1 - q(\phi)\phi)M = 0$. Then $q(\phi)\phi = id$. If you look carefully this is Cramer's rule.

So I got a map which multiplies with ϕ to give the identity so it's an isomorphism. Keep in mind that 1 gives the identity map.

Now part two is very easy. Take a set of generators. You know that M is isomorphic to R^n so pick generators. Let me prove this in two steps. First take n elements that generate M. Then this gives you a surjective map $\beta : R^n \to M$. I want to apply part one. Since M is free I have some isomorphism $\gamma : M \to R^n$. So $\beta\gamma$ is a surjective R-map so it is an isomorphism. Then $\gamma^{-1}(\beta\gamma)^{-1}$ is an inverse for β.

Now I will show that the rank is well-defined. It will follow from this but it's not quite immediate.

The second part says that $R^m \cong R^n$ for $m < n$ is impossible. What can we do? I'm going to let you do this part. You need to localize at any prime and you need to show that a basis can be extended to a system of generators. At the end you have to prove that the number of elements in a basis here is the same. But there are many ways of doing this.

You can also do the following, where you take any maximal ideal p and then if you have an isomorphism you can tensor with R/p over R. Then these become vector spaces.

Definition 1. *If $R \subset S$ then $x \in S$ is integral over R if x satisfies a monic equation with coefficients in R.*

So it's like an algebraic dependence but I'm requiring monicity.

We could have $R = \mathbb{Z}, S = \mathbb{Q}$. Say $x = p/q, (p, q) = 1$. Then you clear denominators and get $p^n + a_1p^{n-1}q + \cdots + a_nq^n = 0$. So this is $p^n + qr = 0$. This can only happen if $q = \pm 1$, so that p/q is integral over $\mathbb{Z}$ if and only if $p/q \in \mathbb{Z}$.

If I look to $\mathbb{Z} \subset \mathbb{R}$ then $\sqrt{2}$ is integral since it satisfies $X^2 - 2 = 0$. You could also be brave and go to the complex numbers, then i is integral over $\mathbb{Z}$.

We'll discuss quadratic extensions in a moment. Why are these interesting? Because of Fermat you go to bigger rings and try to factorize. You have $\mathbb{Z} \subset \mathbb{Q} \hookrightarrow K$, this could be $\mathbb{Q}(\sqrt[n]{1})$. So you get something like

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, hook] \arrow[d, "\subset"'] & Q_k \arrow[d, "\subset"] \\
\mathbb{Q} \arrow[r, hook] & K
\end{tikzcd}$$

How do you know that this is a ring? This is from Cayley Hamilton.

Proposition 1. *The following are equivalent, for $x \in S \supset R$:*

1. *x is integral over R.*
2. *$R[x]$ is a finitely generated R-module.*
3. *$R[x] \subset C \subset S$, where C is a subring of S which is a finitely generated R module*
4. *There exists a faithful ($Ann(M) = 0$) $R[x]$ module M such that M is finitely generated as an R-module.*

Let's apply this first to see something.

Corollary 6. *If $R \subset S$ then the collection of integral elements of S over R forms a subring.*

It's hard to come up with an equation for the sum of two elements, given their individual equations.

We did something like this with Gr obner bases, you could use resultants. That formula would prove this on the spot. But you can prove it without producing these polynomials with this material.

What you do is the following. Pick x and y integral over R in S. Look now to the ring $R[x, y] \subset S$. This, I hope you remember, is $R[x][y]$. Now x is integral so $R[x]$ is a finitely generated R module. Then y is integral over $R[x]$ so $R[x][y]$ is finitely generated over $R[x]$. Then it is finitely generated over R. Then we are done. I found a finitely generated module $R[x][y]$ which is a subring of S contining $R[x + y]$ and $R[xy]$.

Which implications are easy? $R[x]$ is generated by powers of x, and then the polynomial which x satisfies makes the powers above n redundant.

How do you prove two to three? Take $C = R[x]$.

For three to four, let C be your $R[x]$-module. Then since C contains 1 the module is faithful.

The last one needs Cayley Hamilton. Let ϕ be multiplication by x (over R). Then $\phi(M) = xM \subset M$. Then there exists a monic polynomial p with coefficients in R such that $p(\phi) = 0$, so that $p(x)M = 0$. But since M is faithful, $p(x) = 0$, which is your integral dependence relation.

We'll continue next time; think about the following at home. How about $\mathbb{Q}(\sqrt{d})$ and $O_{\mathbb{Q}(\sqrt{d})}$, what is that? $\mathbb{Z}[\sqrt{d}]$ is always contained but only sometimes equal. We'll finish here.