FOUNDATIONS OF ALGEBRAIC GEOMETRY BONUS HANDOUT: PROOFS OF "HARTOGS" AND KRULL

RAVI VAKIL

I said earlier that I hoped to give you proofs of (i) "Hartogs' Theorem" for normal Noetherian schemes, (ii) Krull's Principal Ideal Theorem, and (iii) the fact that if $(R, \mathfrak{m})$ is a Noetherian ring, then $\cap \mathfrak{m}^i = 0$ (corresponding to the fact that a function that is analytically zero at a point is zero in a neighborhood of that point).

You needn't read these; but you may appreciate the fact that the proofs aren't that long. Thus there are very few statements in this class (beyond Math 210) that we actually used, but didn't justify.

I am going to repeat the Nakayama statements, so the entire argument is in one place.

0.1. *Nakayama's Lemma version 1. — Suppose R is a ring, I an ideal of R, and M is a finitely-generated R-module. Suppose $M = IM$. Then there exists an $a \in R$ with $a \equiv 1 \pmod{I}$ with $aM = 0$.*

Proof. Say M is generated by $m_1, \dots, m_n$. Then as $M = IM$, we have $m_i = \sum_j a_{ij} m_j$ for some $a_{ij} \in I$. Thus

$$(\mathrm{Id}_n - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0 \tag{1}$$

where Id_n is the $n \times n$ identity matrix in R, and $A = (a_{ij})$. We can't quite invert this matrix, but we almost can. Recall that any $n \times n$ matrix M has an adjoint matrix $\operatorname{adj}(M)$ such that $\operatorname{adj}(M) M = \det(M) \mathrm{Id}_n$. The coefficients of $\operatorname{adj}(M)$ are polynomials in the coefficients of M. (You've likely seen this in the form of a formula for M^{-1} when there *is* an inverse.) Multiplying both sides of (1) on the left by $\operatorname{adj}(M)$, we obtain

$$\det(\mathrm{Id}_n - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

But when you expand out $\det(\mathrm{Id}_n - A)$, you get something that is $1 \pmod{I}$. $\square$

Here is why you care: Suppose I is contained in all maximal ideals of R. (The intersection of all the maximal ideals is called the *Jacobson radical*, but I won't use this phrase. For comparison, recall that the nilradical was the intersection of the *prime ideals* of R.) Then I claim that any $a \equiv 1 \pmod{I}$ is invertible. For otherwise $(a) \neq R$, so the ideal (a) is

Date: Thursday, December 15, 2005. Minor update Dec. 16.

contained in some maximal ideal $\mathfrak{m}$ — but $a \equiv 1 \pmod{\mathfrak{m}}$, contradiction. Then as a is invertible, we have the following.

0.2. *Nakayama's Lemma version 2. — Suppose* R *is a ring,* I *an ideal of* R *contained in all maximal ideals, and* M *is a finitely-generated* R*-module. (The most interesting case is when* R *is a local ring, and* I *is the maximal ideal.) Suppose* $M = IM$*. Then* $M = 0$*.*

0.3. Important exercise (Nakayama's lemma version 3). Suppose R is a ring, and I is an ideal of R contained in all maximal ideals. Suppose M is a *finitely generated* R-module, and $N \subset M$ is a submodule. If $N/IN \hookrightarrow M/IM$ an isomorphism, then $M = N$.

0.4. Important exercise (Nakayama's lemma version 4). Suppose $(R, \mathfrak{m})$ is a local ring. Suppose M is a finitely-generated R-module, and $f_1, \dots, f_n \in M$, with (the images of) $f_1, \dots, f_n$ generating $M/\mathfrak{m}M$. Then $f_1, \dots, f_n$ generate M. (In particular, taking $M = \mathfrak{m}$, if we have generators of $\mathfrak{m}/\mathfrak{m}^2$, they also generate $\mathfrak{m}$.)

0.5. *Important Exercise that we will use soon.* Suppose S is a subring of a ring R, and $r \in R$. Suppose there is a faithful $S[r]$-module M that is finitely generated as an S-module. Show that r is integral over S. (Hint: look carefully at the proof of Nakayama's Lemma version 1, and change a few words.)

We are ready to prove "Hartogs' Theorem".

0.6. *"Hartogs' theorem". — Suppose* A *is a Noetherian normal domain. Then in* $\mathrm{Frac}(A)$*,*

$$A = \cap_{\mathfrak{p} \textit{ height } 1} A_{\mathfrak{p}}.$$

More generally, if A *is a product of Noetherian normal domains (i.e.* $\operatorname{Spec} A$ *is Noetherian normal scheme), then in the ring of fractions of* A*,*

$$A = \cap_{\mathfrak{p} \textit{ height } 1} A_{\mathfrak{p}}.$$

I stated the special case first so as to convince you that this isn't scary.

Proof. Obviously the right side is contained in the left. Assume we have some x in all A_P but not in A. Let I be the "ideal of denominators":

$$I := \{r \in A : rx \in A\}.$$

(The ideal of denominators arose in an earlier discussion about normality.) We know that $I \neq A$, so choose $\mathfrak{q}$ a minimal prime containing I.

Observe that this construction behaves well with respect to localization (i.e. if $\mathfrak{p}$ is any prime, then the ideal of denominators x in $A_{\mathfrak{p}}$ is the $I_{\mathfrak{p}}$, and it again measures the failure of "'Hartogs' Theorem" for x,' this time in $A_{\mathfrak{p}}$). But Hartogs' Theorem is vacuously true for dimension 1 rings, so hence no height 1 prime contains I. Thus $\mathfrak{q}$ has height at least 2. By localizing at $\mathfrak{q}$, we can assume that A is a local ring with maximal ideal $\mathfrak{q}$, and that $\mathfrak{q}$ is the only prime containing I. Thus $\sqrt{I} = \mathfrak{q}$, so there is some n with $I \subset \mathfrak{q}^n$. Take a minimal such n, so $I \not\subset \mathfrak{q}^{n-1}$, and choose any $y \in \mathfrak{q}^{n-1} - \mathfrak{q}^n$. Let $z = yx$. Then $z \notin A$ (so $\mathfrak{q}z \notin \mathfrak{q}$), but $\mathfrak{q}z \subset A$: $\mathfrak{q}z$ is an ideal of A.

I claim $\mathfrak{q}z$ is not contained in $\mathfrak{q}$. Otherwise, we would have a finitely-generated A-module (namely $\mathfrak{q}$) with a faithful $A[z]$-action, forcing z to be integral over A (and hence in A) by Exercise 0.5.

Thus $\mathfrak{q}z$ is an ideal of A not contained in $\mathfrak{q}$, so it must be A! Thus $\mathfrak{q}z = A$ from which $\mathfrak{q} = A(1/z)$, from which $\mathfrak{q}$ is principal. But then $\operatorname{ht} Q = \dim A \leq \dim_{A/Q} Q/Q^2 \leq 1$ by Nakayama's lemma 0.4, contradicting the fact that $\mathfrak{q}$ has height at least 2. $\square$

We now prove:

0.7. *Krull's Principal Ideal Theorem. — Suppose A is a Noetherian ring, and $f \in A$. Then every minimal prime $\mathfrak{p}$ containing f has height at most 1. If furthermore f is not a zero-divisor, then every minimal prime $\mathfrak{p}$ containing f has height precisely 1.*

0.8. *Lemma. — If R is a Noetherian ring with one prime ideal. Then R is Artinian, i.e., it satisfies the descending chain condition for ideals.*

The notion of Artinian rings is very important, but we will get away without discussing it much.

Proof. If R is a ring, we define more generally an *Artinian R-module*, which is an R-module satisfying the descending chain condition for submodules. Thus R is an Artinian ring if it is Artinian over itself as a module.

If $\mathfrak{m}$ is a maximal ideal of R, then any finite-dimensional $(R/\mathfrak{m})$-vector space (interpreted as an R-module) is clearly Artinian, as any descending chain

$$M_1 \supset M_2 \supset \cdots$$

must eventually stabilize (as $\dim_{R/\mathfrak{m}} M_i$ is a non-increasing sequence of non-negative integers).

Exercise. Show that for any n, $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is a finitely-dimensional $R/\mathfrak{m}$-vector space. (Hint: show it for $n = 0$ and $n = 1$. Use the dimension for $n = 1$ to bound the dimension for general n.) Hence $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is an Artinian R-module.

As $\sqrt{0}$ is prime, it must be $\mathfrak{m}$. As $\mathfrak{m}$ is finitely generated, $\mathfrak{m}^n = 0$ for some n. **Exercise.** Prove this. (Hint: suppose $\mathfrak{m}$ can be generated by m elements, each of which has kth power 0, and show that $\mathfrak{m}^{m(k-1)+1} = 0$.)

Exercise. Show that if $0 \to M' \to M \to M'' \to 0$ is an exact sequence of modules. then M is Artinian if and only if M' and M'' are Artinian.

Thus as we have a finite filtration

$$R \supset \mathfrak{m} \supset \cdots \supset \mathfrak{m}^n = 0$$

all of whose quotients are Artinian, so R is Artinian as well. $\square$

Proof of Krull's principal ideal theorem 0.7. Suppose we are given $x \in A$, with $\mathfrak{p}$ a minimal prime containing x. By localizing at $\mathfrak{p}$, we may assume that A is a local ring, with maximal ideal $\mathfrak{p}$. Suppose $\mathfrak{q}$ is another prime strictly containing $\mathfrak{p}$.

$$\begin{tikzcd} x \arrow[dr, hook] & & \\ & \mathfrak{p} \arrow[r, hook] & A \\ \mathfrak{q} \arrow[ur, hook] & & \end{tikzcd}$$

For the first part of the theorem, we must show that $A_\mathfrak{q}$ has dimension 0. The second part follows from our earlier work: if any minimal primes are height 0, f is a zero-divisor, by our identification of the associated primes of a ring as the union of zero-divisors.

Now $\mathfrak{p}$ is the only prime ideal containing (x), so $A/(x)$ has one prime ideal. By Lemma 0.8, $A/(x)$ is Artinian.

We invoke a useful construction, the *nth symbolic power of a prime ideal*: if R is a ring, and $\mathfrak{q}$ is a prime ideal, then define

$$\mathfrak{q}^{(n)} := \{r \in R : rs \in \mathfrak{q}^n \text{ for some } s \in R - \mathfrak{q}\}.$$

We have a descending chain of ideals in A

$$\mathfrak{q}^{(1)} \supset \mathfrak{q}^{(2)} \supset \cdots,$$

so we have a descending chain of ideals in $A/(x)$

$$\mathfrak{q}^{(1)} + (x) \supset \mathfrak{q}^{(2)} + (x) \supset \cdots$$

which stabilizes, as $A/(x)$ is Artinian. Say $\mathfrak{q}^{(n)} + (x) = \mathfrak{q}^{(n+1)} + (x)$, so

$$\mathfrak{q}^{(n)} \subset \mathfrak{q}^{(n+1)} + (x).$$

Hence for any $f \in \mathfrak{q}^{(n)}$, we can write $f = ax + g$ with $g \in \mathfrak{q}^{(n+1)}$. Hence $ax \in \mathfrak{q}^{(n)}$. As $\mathfrak{p}$ is minimal over x, $x \notin \mathfrak{q}$, so $a \in \mathfrak{q}^{(n)}$. Thus

$$\mathfrak{q}^{(n)} = (x)\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}.$$

As x is in the maximal ideal $\mathfrak{p}$, the second version of Nakayama's lemma 0.2 gives $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$.

We now shift attention to the local ring $A_\mathfrak{q}$, which we are hoping is dimension 0. We have $\mathfrak{q}^{(n)}A_\mathfrak{q} = \mathfrak{q}^{(n+1)}A_\mathfrak{q}$ (the symbolic power construction clearly construction commutes with respect to localization). For any $r \in \mathfrak{q}^n A_\mathfrak{q} \subset \mathfrak{q}^{(n)}A_\mathfrak{q}$, there is some $s \in A_\mathfrak{q} - \mathfrak{q}A_\mathfrak{q}$ such that $rs \in \mathfrak{q}^{n+1}A_\mathfrak{q}$. As s is invertible, $r \in \mathfrak{q}^{n+1}A_\mathfrak{q}$ as well. Thus $\mathfrak{q}^n A_\mathfrak{q} \subset \mathfrak{q}^{n+1}A_\mathfrak{q}$, but as $\mathfrak{q}^{n+1}A_\mathfrak{q} \subset \mathfrak{q}^n A_\mathfrak{q}$, we have $\mathfrak{q}^n A_\mathfrak{q} = \mathfrak{q}^{n+1}A_\mathfrak{q}$. By Nakayama's Lemma version 4 (Exercise 0.4),

$$\mathfrak{q}^n A_\mathfrak{q} = 0.$$

Finally, any local ring $(R, \mathfrak{m})$ such that $\mathfrak{m}^n = 0$ has dimension 0, as $\operatorname{Spec} R$ consists of only one point: $[\mathfrak{m}] = V(\mathfrak{m}) = V(\mathfrak{m}^n) = V(0) = \operatorname{Spec} R$. □

Finally:

0.9. *Proposition. — If* $(A, \mathfrak{m})$ *is a Noetherian local ring, then* $\cap_i \mathfrak{m}^i = 0$.

It is tempting to argue that $\mathfrak{m}(\cap_i \mathfrak{m}^i) = \cap_i \mathfrak{m}^i$, and then to use Nakayama's lemma 0.4 to argue that $\cap_i \mathfrak{m}^i = 0$. Unfortunately, it is not obvious that this first equality is true: product does not commute with infinite intersections in general. I heard this argument from Kirsten Wickelgren, who I think heard it from Greg Brumfiel. We used it in showing an equivalence in that big chain of equivalent characterizations of discrete valuation rings.

Proof. Let $I = \cap_i \mathfrak{m}^i$. We wish to show that $I \subset \mathfrak{m}I$; then as $\mathfrak{m}I \subset I$, we have $I = \mathfrak{m}I$, and hence by Nakayama's Lemma 0.4, $I = 0$. Fix a primary decomposition of $\mathfrak{m}I$. It suffices to show that $\mathfrak{p}$ contains I for any $\mathfrak{p}$ in this primary decomposition, as then I is contained in all the primary ideals in the decomposition of $\mathfrak{m}I$, and hence $\mathfrak{m}I$.

Let $\mathfrak{q} = \sqrt{\mathfrak{p}}$. If $\mathfrak{q} \neq \mathfrak{m}$, then choose $x \in \mathfrak{m} - \mathfrak{q}$. Now x is not nilpotent in $R/\mathfrak{p}$, and hence is not a zero-divisor. But $xI \subset \mathfrak{p}$, so $I \subset \mathfrak{p}$.

On the other hand, if $\mathfrak{q} = \mathfrak{m}$, then as $\mathfrak{m}$ is finitely generated, and each generator is in $\sqrt{\mathfrak{p}}$, there is some a such that $\mathfrak{m}^a \subset \mathfrak{p}$. But $I \subset \mathfrak{m}^a$, so we are done. □

E-mail address: vakil@math.stanford.edu