FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 12

CONTENTS

Last day: smoothness=regularity=nonsingularity, Zariski tangent space and related notions, Nakayama's Lemma.

Today: Jacobian criterion, Euler test, characterizations of discrete valuation rings = dimension 1 Noetherian regular local rings

1. "SMOOTHNESS" = REGULARITY = NONSINGULARITY, CONTINUED

Last day, I defined the Zariski tangent space. Suppose A is a ring, and $\mathfrak{m}$ is a maximal ideal, with residue field $k = A/\mathfrak{m}$. Then $\mathfrak{m}/\mathfrak{m}^2$, a vector space over k, is the **Zariski cotangent space**. The dual is the **Zariski tangent space**. Elements of the Zariski cotangent space are called **cotangent vectors** or **differentials**; elements of the tangent space are called **tangent vectors**.

I tried to convince you that this was a reasonable definition. I also asked you what your private definition of tangent space or cotangent space was, so I could convince you that this is the right algebraic notion. A couple of you think of tangent vectors as *derivations*, and in this case, the connection is very fast. I've put it in the Class 11 notes, so please check it out if you know what derivations are.

Last day, I stated the following proposition.

1.1. *Proposition. — Suppose* $(A, \mathfrak{m})$ *is a Noetherian local ring. Then* $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.

We'll prove this in a moment.

If equality holds, we say that A is **regular** at $\mathfrak{m}$. If A is a local ring, then we say that A is a **regular local ring**. If A is regular at all of its primes, we say that A is a **regular ring**.

A scheme X is **regular** or **nonsingular** or **smooth** at a point p if the local ring $\mathcal{O}_{X,p}$ is regular. It is **singular** at the point otherwise. A scheme is **regular** or **nonsingular** or

Date: Friday, November 4, 2005. Minor update January 31, 2007.

smooth if it is regular at all points. It is **singular** otherwise (i.e. if it is singular at *at least one* point).

1.2. Exercise. Show that if A is a Noetherian local ring, then A has finite dimension. (*Warning:* Noetherian rings in general could have infinite dimension.)

In order to prove Proposition 1.1, we're going to use Nakayama's Lemma, which hopefully you've looked at.

The version we'll use is:

1.3. 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 $\mathfrak{m}$.) Translation: if we have a set of generators of a *finitely generated* module modulo a finite ideal, then they generate the entire module.

Proof of Proposition 1.1: Note that $\mathfrak{m}$ is finitely generated (as R is Noetherian), so $\mathfrak{m}/\mathfrak{m}^2$ is a finitely generated $R/\mathfrak{m} = k$-module, hence finite-dimensional. Say $\dim_k \mathfrak{m}/\mathfrak{m}^2 = n$. Choose n elements of $\mathfrak{m}/\mathfrak{m}^2$, and lift them to elements $f_1, \dots, f_n$ of $\mathfrak{m}$. Then by Nakayama's lemma, $(f_1, \dots, f_n) = \mathfrak{m}$.

Problem B6 on problem set 4 (newest version!) includes the following: Suppose $X = \operatorname{Spec} R$ where R is a Noetherian domain, and Z is an irreducible component of $V(f_1, \dots, f_n)$, where $f_1, \dots, f_n \in R$. Show that the height of Z (as a prime ideal) is at most n.

In this case, $V((f_1, \dots, f_n)) = V(\mathfrak{m})$ is just the point $[\mathfrak{m}]$, so the height of $\mathfrak{m}$ is at most n. Thus the longest chain of prime ideals containing $\mathfrak{m}$ is at most $n + 1$. But this is also the longest chain of prime ideals in X (as $\mathfrak{m}$ is the unique maximal ideal), so $n \geq \dim X$. $\square$

Computing the Zariski-tangent space is actually quite hands-on, because you can compute it in a multivariable calculus way.

For example, last day I gave some motivation, by saying that $x + y + 3z + y^3 = 0$ and $2x + z^3 + y^2 = 0$ cut out a curve in $\mathbb{A}^3$, which is nonsingular at the origin, and that the tangent space at the origin is cut out by $x + y + 3z = 2x = 0$. This can be made precise through the following exercise.

1.4. *Important exercise.* Suppose A is a ring, and $\mathfrak{m}$ a maximal ideal. If $f \in \mathfrak{m}$, show that the dimension of the Zariski tangent space of $\operatorname{Spec} A$ at $[\mathfrak{m}]$ is the dimension of the Zariski tangent space of $\operatorname{Spec} A/(f)$ at $[\mathfrak{m}]$, or one less. (Hint: show that the Zariski tangent space of $\operatorname{Spec} A/(f)$ is "cut out" in the Zariski tangent space of $\operatorname{Spec} A$ by the linear equation $f \pmod{\mathfrak{m}^2}$.)

1.5. *Exercise.* Find the dimension of the Zariski tangent space at the point $[(2, x)]$ of $\mathbb{Z}[2i] \cong \mathbb{Z}[x]/(x^2 + 4)$. Find the dimension of the Zariski tangent space at the point $[(2, x)]$ of $\mathbb{Z}[\sqrt{2}i] \cong \mathbb{Z}[x]/(x^2 + 2)$.

1.6. *Exercise (the Jacobian criterion for checking nonsingularity).* Suppose k is an algebraically closed field, and X is a finite type k-scheme. Then locally it is of the form $\operatorname{Spec} k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$. Show that the Zariski tangent space at the closed point p (with residue field k, by the Nullstellensatz) is given by the cokernel of the Jacobian map $k^r \to k^n$ given by the Jacobian matrix

$$J = \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(p) & \cdots & \frac{\partial f_r}{\partial x_1}(p) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial x_n}(p) & \cdots & \frac{\partial f_r}{\partial x_n}(p) \end{pmatrix}. \tag{1}$$

(This is just making precise our example of a curve in $\mathbb{A}^3$ cut out by a couple of equations, where we picked off the linear terms.) Possible hint: "translate p to the origin," and consider linear terms. See also the exercise two previous to this one.

You might be alarmed: what does $\frac{\partial f}{\partial x_1}$ mean?! Do you need deltas and epsilons? No! Just define derivatives formally, e.g.

$$\frac{\partial}{\partial x_1}(x_1^2 + x_1 x_2 + x_2^2) = 2x_1 + x_2.$$

1.7. Exercise: Dimension theory implies the Nullstellensatz. In the previous exercise, l is necessarily only a finite extension of k, as this exercise shows. (a) Prove a microscopically stronger version of the weak Nullstellensatz: Suppose $R = k[x_1, \ldots, x_n]/I$, where k is an algebraically closed field and I is some ideal. Then the maximal ideals are precisely those of the form $(x_1 - a_1, \ldots, x_n - a_n)$, where $a_i \in k$.
(b) Suppose $R = k[x_1, \ldots, x_n]/I$ where k is not necessarily algebraically closed. Show every maximal ideal of R has residue field that are finite extensions of k. (Hint for both: the maximal ideals correspond to dimension 0 points, which correspond to transcendence degree 0 extensions of k, i.e. finite extensions of k. If $k = \overline{k}$, the maximal ideals correspond to surjections $f : k[x_1, \ldots, x_n] \to k$. Fix one such surjection. Let $a_i = f(x_i)$, and show that the corresponding maximal ideal is $(x_1 - a_1, \ldots, x_n - a_n)$.) This exercise is a bit of an aside — it belongs in class 8, and I've also put it in those notes.

1.8. Exercise. Show that the singular *closed* points of the hypersurface $f(x_1, \ldots, x_n) = 0$ in $\mathbb{A}^n_k$ are given by the equations $f = \frac{\partial f}{\partial x_1} = \cdots = \frac{\partial f}{\partial x_n} = 0$.

1.9. Exercise. Show that $\mathbb{A}^1$ and $\mathbb{A}^2$ are nonsingular. (Make sure to check nonsingularity at the non-closed points! Fortunately you know what all the points of $\mathbb{A}^2$ are; this is trickier for $\mathbb{A}^3$.)

In the previous exercise, you'll use the fact that the local ring at the generic point of $\mathbb{A}^2$ is dimension 0, and the local ring at generic point at a curve in $\mathbb{A}^2$ is 1.

Let's apply this technology to an arithmetic situation.

1.10. Exercise. Show that $\operatorname{Spec} \mathbb{Z}$ is a nonsingular curve.

Here are some fun comments: What is the derivative of 35 at the prime 5? Answer: 35 $\pmod{25}$, so 35 has the same "slope" as 10. What is the derivative of 9, which doesn't vanish at 5? Answer: the notion of derivative doesn't apply there. You'd think that you'd want to subtract its value at 5, but you can't subtract "4 $\pmod 5$)" from the integer 9. Also, 35 $\pmod 2$)5 you might *think* you want to restate as 7 $\pmod 5$, by dividing by 5, but that's morally wrong — you're dividing by a particular choice of generator 5 of the maximal ideal of the 5-adics $\mathbb{Z}_5$; in this case, one appears to be staring you in the face, but in general that won't be true. Follow-up fun: you can talk about the derivative of a function only for functions vanishing at a point. And you can talk about the second derivative of a function only for functions that vanish, and whose first derivative vanishes. For example, 75 has second derivative 75 $\pmod 1$)25 at 5. It's pretty flat.

1.11. Exercise. Note that $\mathbb{Z}[i]$ is dimension 1, as $\mathbb{Z}[x]$ has dimension 2 (problem set exercise), and is a domain, and x^2+1 is not 0, so $\mathbb{Z}[x]/(x^2+1)$ has dimension 1 by Krull. Show that $\operatorname{Spec} \mathbb{Z}[i]$ is a nonsingular curve. (This is intended for people who know about the primes of the Gaussian integers $\mathbb{Z}[i]$.)

1.12. Exercise. Show that there is one singular point of $\operatorname{Spec} \mathbb{Z}[2i]$, and describe it.

1.13. Handy Exercise (the Euler test for projective hypersurfaces). There is an analogous Jacobian criterion for hypersurfaces $f = 0$ in $\mathbb{P}^n_k$. Show that the singular *closed* points correspond to the locus $f = \frac{\partial f}{\partial x_1} = \cdots = \frac{\partial f}{\partial x_n} = 0$. If the degree of the hypersurface is not divisible by the characteristic of any of the residue fields (e.g. if we are working over a field of characteristic 0), show that it suffices to check $\frac{\partial f}{\partial x_1} = \cdots = \frac{\partial f}{\partial x_n} = 0$. (Hint: show that f lies in the ideal $(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$). (Fact: this will give the singular points in general. I don't want to prove this, and I won't use it.)

1.14. Exercise. Suppose k is algebraically closed. Show that $y^2 z = x^3 - xz^2$ in $\mathbb{P}^2_k$ is an irreducible nonsingular curve. (This is for practice.) Warning: I didn't say $\operatorname{char} k = 0$.

1.15. Exercises. Find all the singular closed points of the following plane curves. Here we work over a field of characteristic 0 for convenience.

(a) $y^2 = x^2 + x^3$. This is called a *node*.
(b) $y^2 = x^3$. This is called a *cusp*.
(c) $y^2 = x^4$. This is called a *tacnode*.

(I haven't given precise definitions for node, cusp, or tacnode. You may want to think about what they might be.)

1.16. Exercise. Show that the twisted cubic $\operatorname{Proj} k[w, x, y, z]/(wz - xy, wy - x^2, xz - y^2)$ is nonsingular. (You can do this by using the fact that it is isomorphic to $\mathbb{P}^1$. I'd prefer you to do this with the explicit equations, for the sake of practice.)

1.17. Exercise. Show that the only dimension 0 Noetherian regular local rings are fields. (Hint: Nakayama.)

2. Dimension 1 Noetherian regular local rings = discrete valuation rings

The case of dimension 1 is also very important, because if you understand how primes behave that are separated by dimension 1, then you can use induction to prove facts in arbitrary dimension. This is one reason why Krull is so useful.

A dimension 1 Noetherian regular local ring can be thought of as a "germ of a curve". Two examples to keep in mind are $k[x]_{(x)} = \{f(x)/g(x) : x \not| g(x)\}$ and $\mathbb{Z}_{(5)} = \{a/b : 5 \not| b\}$.

The purpose of this section is to give a long series of equivalent definitions of these rings.

Theorem. *Suppose* $(R, \mathfrak{m})$ *is a Noetherian dimension* 1 *local ring. The following are equivalent.*
(a) R *is regular.*

Informal translation: R is a germ of a smooth curve.

(b) $\mathfrak{m}$ *is principal.* If R is regular, then $\mathfrak{m}/\mathfrak{m}^2$ is one-dimensional. Choose any element $t \in \mathfrak{m} - \mathfrak{m}^2$. Then t generates $\mathfrak{m}/\mathfrak{m}^2$, so generates $\mathfrak{m}$ by Nakayama's lemma. Such an element is called a *uniformizer*. (Warning: we needed to know that $\mathfrak{m}$ was finitely generated to invoke Nakayama — but fortunately we do, thanks to the Noetherian hypothesis!)

Conversely, if $\mathfrak{m}$ is generated by one element t over R, then $\mathfrak{m}/\mathfrak{m}^2$ is generated by one element t over $R/\mathfrak{m} = k$.

(c) All ideals are of the form $\mathfrak{m}^n$ *or* 0. Suppose $(R, \mathfrak{m}, k)$ is a Noetherian regular local ring of dimension 1. Then I claim that $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for any n. Proof: Otherwise, $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \mathfrak{m}^{n+2} = \cdots$. Then $\cap_i \mathfrak{m}^i = \mathfrak{m}^n$. But $\cap_i \mathfrak{m}^i = (0)$. **(I'd given a faulty reason for this. I owe you this algebraic fact.)** Then as $t^n \in \mathfrak{m}^n$, we must have $t^n = 0$. But R is a domain, so $t = 0$ — but $t \in \mathfrak{m} - \mathfrak{m}^2$.

I next claim that $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is dimension 1. Reason: $\mathfrak{m}^n = (t^n)$. So $\mathfrak{m}^n$ is generated as as a R-module by one element, and $\mathfrak{m}^n/(\mathfrak{m}\mathfrak{m}^n)$ is generated as a $(R/\mathfrak{m} = k)$-module by 1 element, so it is a one-dimensional vector space.

So we have a chain of ideals $R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^3 \supset \cdots$ with $\cap \mathfrak{m}^i = (0)$. We want to say that there is no room for any ideal besides these, because "each pair is "separated by dimension 1", and there is "no room at the end". Proof: suppose $I \subset R$ is an ideal. If $I \neq (0)$, then there is some n such that $I \subset \mathfrak{m}^n$ but $I \not\subset \mathfrak{m}^{n+1}$. Choose some $u \in I - \mathfrak{m}^{n+1}$. Then $(u) \subset I$. But u generates $\mathfrak{m}^n/\mathfrak{m}^{n+1}$, hence by Nakayama it generates $\mathfrak{m}^n$, so we have

$\mathfrak{m}^n \subset I \subset \mathfrak{m}^n$, so we are done. Conclusion: in a Noetherian local ring of dimension 1, regularity implies all ideals are of the form $\mathfrak{m}^n$ or (0).

Conversely, suppose we have a dimension 1 Noetherian local domain that is not regular, so $\mathfrak{m}/\mathfrak{m}^2$ has dimension at least 2. Choose any $u \in \mathfrak{m} - \mathfrak{m}^2$. Then $(u, \mathfrak{m}^2)$ is an ideal, but $\mathfrak{m} \subsetneq (u, \mathfrak{m}^2) \subsetneq \mathfrak{m}^2$. We've thus shown that (c) is equivalent to the previous cases.

(d) R is a principal ideal domain. I didn't do this in class. **Exercise.** Show that (d) is equivalent to (a)–(c).

(e) R is a discrete valuation ring. I will now define something for you that will be a very nice way of describing such rings, that will make precise some of our earlier vague ramblings. We'll have to show that this definition accords with (a)–(d) of course.

Suppose K is a field. A *discrete valuation* on K is a *surjective homomorphism* $\nu : K^* \to \mathbb{Z}$ (homomorphism: $\nu(xy) = \nu(x) + \nu(y)$) satisfying

$$\nu(x + y) \geq \min(\nu(x), \nu(y)).$$

Suggestive examples: (i) *(the 5-adic valuation)* $K = \mathbb{Q}$, $\nu(r)$ is the "power of 5 appearing in r", e.g. $\nu(35/2) = 1$, $\nu(27/125) = -3$.

(ii) $K = k(x)$, $\nu(f)$ is the "power of x appearing in f".

Then $0 \cup \{x \in K^* : \nu(x) \geq 0\}$ is a ring. It is called the *valuation ring* of ν.

2.1. Exercise. Describe the valuation rings in those two examples. Hmm — they are familiar-looking dimension 1 Noetherian local rings. What a coincidence!

2.2. Exercise. Show that $0 \cup \{x \in K^* : \nu(x) \geq 1\}$ is the unique maximal ideal of the valuation ring. (Hint: show that everything in the complement is invertible.) Thus the valuation ring is a local ring.

An integral domain A is called a *discrete valuation ring* if there exists a discrete valuation ν on its fraction field $K = \mathrm{Frac}(A)$.

Now if R is a Noetherian regular local ring of dimension 1, and t is a uniformizer (generator of $\mathfrak{m}$ as an ideal = dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space) then any non-zero element r of R lies in some $\mathfrak{m}^n - \mathfrak{m}^{n+1}$, so $r = t^n u$ where u is a unit (as t^n generates $\mathfrak{m}^n$ by Nakayama, and so does r), so $\mathrm{Frac}\, R = R_t = R[1/t]$. So any element of $\mathrm{Frac}\, R$ can be written uniquely as ut^n where u is a unit and $n \in \mathbb{Z}$. Thus we can define a valuation $\nu(ut^n) = n$, and we'll quickly see that it is a discrete valuation (**exercise**). Thus (a)-(c) implies (d).

Conversely, suppose $(R, \mathfrak{m})$ is a discrete valuation ring. Then I claim it is a Noetherian regular local ring of dimension 1. **Exercise.** Check this. (Hint: Show that the ideals are all of the form (0) or $I_n = \{r \in R : \nu(r) \geq n\}$, and I_1 is the only prime of the second sort. Then we get Noetherianness, and dimension 1. Show that I_1/I_2 is generated by any element of $I_1 - I_2$.)

Exercise/Corollary. There is only one discrete valuation on a discrete valuation ring.

Thus whenever you see a regular local ring of dimension 1, we have a valuation on the fraction field. If the valuation of an element is $n > 0$, we say that the element has a *zero of order* n. If the valuation is $-n < 0$, we say that the element has a *pole of order* n.

So we can finally make precise the fact that 75/34 has a double zero at 5, and a single pole at 2! Also, you can easily figure out the zeros and poles of $x^3(x+y)/(x^2+xy)^3$ on $\mathbb{A}^2$. Note that we can only make sense of zeros and poles at *nonsingular points of codimension* 1.

Definition. More generally: suppose X is a locally Noetherian scheme. Then for any regular height(=codimension) 1 points (i.e. any point p where $\mathcal{O}_{X,p}$ is a regular local ring of dimension 1), we have a valuation ν. If f is any non-zero element of the fraction field of $\mathcal{O}_{X,p}$ (e.g. if X is integral, and f is a non-zero element of the function field of X), then if $\nu(f) > 0$, we say that the element has a *zero of order* $\nu(f)$, and if $\nu(f) < 0$, we say that the element has a *pole of order* $-\nu(f)$.

Exercise. Suppose X is a regular integral Noetherian scheme, and $f \in \operatorname{Frac}(\Gamma(X, \mathcal{O}_X))^*$ is a non-zero element of its function field. Show that f has a finite number of zeros and poles.

Finally:

(f) $(R, \mathfrak{m})$ *is a unique factorization domain,*

(g) R *is integrally closed in its fraction field* $K = \operatorname{Frac}(R)$.

(a)-(e) clearly imply (f), because we have the following stupid unique factorization: each non-zero element of r can be written uniquely as ut^n where $n \in \mathbb{Z}^{\geq 0}$ and u is a unit.

(f) implies (g), because checked earlier that unique factorization domains are always integrally closed in its fraction field.

So it remains to check that (g) implies (a)-(e). This is straightforward, but for the sake of time, I'm not going to give the proof in class. But in the interests of scrupulousness, I'm going to give you a full proof in the notes. It will take us less than half a page. This is the only tricky part of this entire theorem.

2.3. Fact. Suppose $(S, \mathfrak{n})$ is a Noetherian local domain of dimension 0. Then $\mathfrak{n}^n = 0$ for some n. (I had earlier given this as an exercise, with an erroneous hint. I may later add a proof to the notes.)

2.4. Exercise. Suppose A is a subring of a ring B, and $x \in B$. Suppose there is a faithful $A[x]$-module M that is finitely generated as an A-module. Show that x is integral over A.

(Hint: look carefully at the proof of Nakayama's Lemma version 1 in the Class 11 notes, and change a few words.)

Proof that (f) implies (b). Suppose $(R, \mathfrak{m})$ is a Noetherian local domain of dimension 1, that is integrally closed in its fraction field $K = \mathrm{Frac}(R)$. Choose any $r \in R \neq 0$. Then $S = R/(r)$ is dimension 0, and is Noetherian and local, so if $\mathfrak{n}$ is its maximal ideal, then there is some n such that $\mathfrak{n}^n = 0$ but $\mathfrak{n}^{n-1} \neq 0$ by Exercise 2.3. Thus $\mathfrak{m}^n \subseteq (r)$ but $\mathfrak{m}^{n-1} \not\subset (r)$. Choose $s \in \mathfrak{m}^{n-1} - (r)$. Consider $x = r/s$. Then $x^{-1} \notin R$, so as R is integrally closed, x^{-1} is not integral over R.

Now $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$ (or else $x^{-1}\mathfrak{m} \subset \mathfrak{m}$ would imply that $\mathfrak{m}$ is a faithful $R[x^{-1}]$-module, contradicting Exercise 2.4). But $x^{-1}\mathfrak{m} \subset R$. Thus $x^{-1}\mathfrak{m} = R$, from which $\mathfrak{m} = xR$, so $\mathfrak{m}$ is principal. □

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