INTRODUCTION TO ALGEBRAIC GEOMETRY, CLASS 16

RAVI VAKIL

Contents

Problem sets back. 2 points extra to everyone who did the last problem set, because of the $\mathbb{A}^1$ issue. If you didn't do problems 5 and 6 (on Hilbert polynomials), come ask me about it.

Warning: a morphism of varieties that gives a bijection of points isn't necessarily an isomorphism. Example 1: the morphism from $\mathbb{A}^1$ to the cuspidal curve $y^2 = x^3$, given by $t \mapsto (t^2, t^3)$. Example 2: Frobenius morphism from $\mathbb{A}^1$ to $\mathbb{A}^1$, over a field of characteristic p, given by $t \mapsto t^p$.

1. Valuation rings (and non-singular points of curves)

Get rid of zero-valuation problem. Valuation examples: I should have said that you have valuations over $\overline{k}$.

Dimension 1 varieties, or curves, are particularly simple, and most of the rest of the course will concentrate on them.

We saw that nonsingularity has to do with local rings, so we'll discuss *one-dimensional local rings.*

First we'll recall some facts about discrete valuation rings and Dedekind domains.

Definition. Let K be a field. A *discrete valuation* of K is a map $v : K \setminus \{0\} \to \mathbb{Z}$ such that for all x, y non-zero in K, we have: $v(xy) = v(x) + v(y)$, $v(x + y) \geq \min(v(x), v(y))$. *It is* **trivial** *if it is the 0-valuation. From now on, assume all discrete valuations are non-trivial. Then the image of v is of the form $\mathbb{Z}n$ for some non-zero n; by dividing by n, we may as well consider the image of v to be all of $\mathbb{Z}$ from now on.* Notice that the set $R = \{x \in K | v(x) \geq 0\} \cup \{0\}$ is a subring of K; call this the *discrete valuation ring*, or *DVR*, of K. The subset

Date: Tuesday, November 2, 1999.

$\mathfrak{m} = \{x \in K | v(x) > 0\} \cup \{0\}$ is an ideal in R, and $(R, \mathfrak{m})$ is a local ring. A *discrete valuation ring* is an integral domain which is the discrete valuation ring of some valuation of its quotient field. If $\overline{k}$ is a subfield of K such that $v(x) = 0$ for all $x \in \overline{k} \setminus \{0\}$, then we say v is a *discrete valuation of* $K/\overline{k}$, and R is a *discrete valuation ring of* $K/\overline{k}$.

Example. Let $K = \overline{k}(t)$, and for $f \in K$, let $v(f)$ be the order of the zero of f at $t = 0$ (negative if f has a pole). Check all properties. Notice that *discrete valuation ring* of of v are those quotients of polynomials whose denominator doesn't vanish at 0, i.e. $\overline{k}[t]_{(t)}$. In geometric language, it is the stalk of the structure sheaf of $\mathbb{A}^1$ at the origin.

Similarly, $\overline{k}[t]_{(t)}$ is a discrete valuation ring: it is indeed an integral domain, and it is the valuation ring of some valuation in its quotient field $\overline{k}(t)$.

Similarly, we could get other valuations by replacing 0 with any other element of $\overline{k}$. Have we found all the valuations? No:

Example. Let $K = \overline{k}(t)$ as before. For $f \in K$, write f in terms of $u = 1/t$, and let $v(f)$ be the order of zero of f at $u = 0$. Again, it is indeed a valuation, and it has geometric meaning. (Ask them.) It corresponds to the point of $\mathbb{P}^1$ "at ∞" (when looking at it with respect to the t-coordinate).

Roya pointed out that $v(f(t)/g(t)) = \deg g - \deg f$.

Exercise. These are all the non-trivial valuations of $\overline{k}(t)$ over $\overline{k}$, the function field of $\mathbb{P}^1$. They naturally correspond to the points of $\mathbb{P}^1$. Hint: if v is a valuation, consider the possible values of $v(t - a)$ be for all $a \in \overline{k}$.

Example. Let $K = \mathbb{Q}$. If $f \in \mathbb{Q}$, let $v(x)$ be the highest power of 2 dividing x, so $v(14) = 2$, $v(3) = 0$, $v(13/12) = -2$. Check all properties. What's the discrete valuation ring? Those fractions with no 2's in the denominators. Geometrically, $\mathbb{Q}$ is the function field of $\operatorname{Spec} \mathbb{Z}$, and the valuations turn out to correspond to the maximal prime ideals of $\mathbb{Z}$, i.e. the "closed points" of $\operatorname{Spec} \mathbb{Z}$.

Remark. Every element x of a local ring R that isn't in the maximal ideal $\mathfrak{m}$ is invertible. Reason: the ideal (x) is either all of R, or it isn't. If it isn't, then it is contained in a maximal ideal — but there's only one, and x isn't contained in $\mathfrak{m}$. Hence $(x) = R$, so $1 \in (x)$, so $1 = fx$ for some $f \in R$, i.e. x is invertible.

Another example. Consider the ring $\overline{k}[[t]]$ of power series in one variable over $\overline{k}$. It's a discrete valuation ring, with valuation given by $v(f)$ is the largest power of t dividing f. Its quotient field is denoted $\overline{k}((t))$; you can check that elements of the quotient field are of the form $t^{-n}g$, where n is some integer, and $g \in \overline{k}[[t]]$.

This example looks very much like the example $\overline{k}[t]_{(t)} \subset \overline{k}(t)$ above. You can make this precise by talking about *completions*.

1.1. **Completions.** Suppose R is a ring, and $\mathfrak{m}$ is a maximal ideal. (Think: R is a DVR.) Then the completition $\hat{R}$ is defined to be the inverse limit $\lim_{\leftarrow n} R/\mathfrak{m}^n$.

What this means: you can consider elements of $\hat{R}$ to be elements $(x_1, x_2, \dots) \in R/\mathfrak{m} \times R/\mathfrak{m}^2 \times \dots$ such that $x_i \equiv x_j \mod \mathfrak{m}^j$ (if $j > i$).

Note that there is a homomorphism $R \to \hat{R}$. Caution: This isn't always injective! But I think it is if R is a domain.

Example: completion of $\overline{k}[t]$ *at* (t) *is* $\overline{k}[[t]]$. Let $R = \overline{k}[t]$, and $\mathfrak{m}$ the maximal ideal (t). The function $1/(1-t)$ defined near $t = 0$ is (after some work): $(1, 1+t, 1+t+t^2, \dots) \in R/\mathfrak{m} \times R/\mathfrak{m}^2 \times \dots$ in the completion. For convenience, we write this as $1 + t + t^2 + \dots$.

Example. What's -1 in the 5-adics? In the power-series representation? What is 1/3 in the ring $\mathbb{Z}_2$?

More on completitions appears in class 17; that should have been introduced here.

1.2. **A big result from commutative algebra.** We'll need an amazing result from commutative algebra. The proof will come up in Commutative Algebra, but as usual, you can treat it as a black box.

Theorem. Let $(R, \mathfrak{m})$ be a noetherian local domain of dimension one. Then the following are equivalent.

(i) R is a discrete valuation ring;
(ii) R is integrally closed (I'll speak about integral closures next day);
(iii) R is a regular local ring;
(iv) $\mathfrak{m}$ is a principal ideal.

To get you used to these idea, let's see what this gives us.

Now $\mathfrak{m}$ is principal by (iv), so let x be a generator of $\mathfrak{m}$. (It is often called a *uniformizer*.) Note that $v(x)$ must be 1. Note that $\mathfrak{m}^n = (x^n)$.

Next, $\mathfrak{m}^n = \{r \in R | v(r) \geq n\}$. You can see this by induction. This is true when $n = 0$ and 1. Clearly $\mathfrak{m}^n = (x^n) \subset \{r \in R | v(r) \geq n\}$, so take any $r \in R$ such that $v(r) \geq n$. Then $r \in \mathfrak{m}$, so r is a multiple of x, so $r = xs$ for some s. Then $v(s) \geq n - 1$, and by induction, $s \in \mathfrak{m}^{n-1}$. Hence $r \in \mathfrak{m}^n$.

Next, $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is a $\overline{k}$-vector space of dimension 1: it is an R-module generated by x, and $\mathfrak{m}$ annihilates it, so it is a $R/\mathfrak{m}$-module generated by x, i.e. a $\overline{k}$-vector space generated by x. So its dimension is either 0 or 1. But x^n gives a non-zero element of $\mathfrak{m}^n/\mathfrak{m}^{n+1}$, so the dimension of this space must be 1.

So here's our picture: we have nested subsets $\mathfrak{m}^n$ of R, and the difference between two adjacent ones is one-dimensional. You can see this in each of our examples.

The following lemma will let you know, partially, how to think about discrete valuation rings that come up geometrically.

Lemma. If $(R, \mathfrak{m})$ is a discrete valuation ring over $\overline{k}$, such that $R/\mathfrak{m} \cong \overline{k}$, and there is an inclusion $\overline{k} \hookrightarrow R$ such that the composition $\overline{k} \to R \to R/\mathfrak{m} \cong \overline{k}$ is an isomorphism, then $\hat{R} \cong \overline{k}[[t]]$.

Note: these hypotheses are satisfied by $\overline{k}[t]_{(t)}$, but not $\mathbb{Z}_p$.

Proof. Fix an element $r \in R$. I claim that for each n, there are unique elements $a_0, \ldots, a_{n-1}$ such that

$$r \equiv a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \pmod{\mathfrak{m}^n}.$$

This is certainly true if $n = 1$, so we work by induction.

First we show existence. Suppose

$$r \equiv a_0 + \cdots + a_{n-1}x^{n-1} \pmod{\mathfrak{m}^n}.$$

Call this polynomial f. Then $r - f \in \mathfrak{m}^n$; hence $r - f \equiv a_n x^n \pmod{\mathfrak{m}^{n+1}}$ (for a *unique* a_n). Hence

$$r \equiv a_0 + a_1 x + \cdots + a_n x^n \pmod{\mathfrak{m}^{n+1}}.$$

Thus we have existence.

Now for uniqueness. If $r \equiv b_0 + \cdots + b_n x^n \pmod{\mathfrak{m}^{n+1}}$, then by reducing modulo $\mathfrak{m}^n$, we see that $b_0 = a_0, \ldots, b_{n-1} = a_{n-1}$. Finally, $b_n = a_n$ by the comment in the last paragraph.

Thus we've shown that r can be written in this unique way. Then its image in the completion can be written as

$$\hat{r} = (a_0, a_0 + a_1 x, a_0 + a_1 x + a_2 x^2, \ldots)$$

for uniquely chosen $a_i \in \overline{k}$. At this point, it's clear what the isomorphism with the power series ring $\overline{k}[[t]]$, whose elements can be uniquely written as

$$(a_0, a_0 + a_1 t, a_0 + a_1 t + a_2 t^2, \ldots).$$

We just need to check that the ring structures are the same, i.e. when you add r and s in our ring R, you end up adding the corresponding power series, and the same for multiplication. Addition is clear, and for multiplication: notice that if $\hat{s} = (b_0, \ldots)$, then

$$\hat{rs} = (a_0 b_0, a_0 b_0 + (a_1 b_0 + a_0 b_1)x, \ldots)$$

which is the same multiplication rule as for power series. $\square$

In conclusion any one of these nice local rings you can informally imagine as power series, although you lose some information in doing so.

Fact. Completion of dimension n regular local ring with this property (that the residue field is contained in ring) is isomorphic to $\overline{k}[[t_1, \ldots, t_n]]$.

Mild generalization to the p-adics: You don't need $\overline{k}$ to lie in R for this to work (or indeed for $\overline{k}$ to be algebraically closed). All you really need is a map $\sigma : k \to R$ — not a ring map or anything, just a map of sets — such that the composition $k \to R \to R/\mathfrak{m}$ is an isomorphism. *(Explain more.)*

Example. Let p be a nonsingular point on a curve Y. Then $\mathcal{O}_{Y,p}$ is a regular local ring of dimension 1. Hence it is a valuation of $k(Y)/\overline{k}$. What's the valuation? Essentially, it's the same thing we say in the case of $\overline{k}[t]$. The maximal ideal $\mathfrak{m}$ is the ideal of functions vanishing at p, and $\mathfrak{m}$ is generated by a single element (often called the *uniformizer*). In a way that can soon be made precise, given a regular function on a curve, its valuation is the order of vanishing at the point p.

If you're willing to think analytically, over the complex numbers, you can already see it: there are classical neighbourhoods of nonsingular points look just like open sets in $\mathbb{C}$, and functions there can have zeroes or poles at p. And if you're thinking analytically, you'll want to think in terms of power series, which is precisely what the above Lemma allows you to do.

How to think of the map $R \to \hat{R}$ or $R_{\mathfrak{m}} \to \hat{R}$. This is expanding out a locally defined function as a power series. Any function in a Zariski neighbourhood is an element of the localization. Any element of the localization is an element of the completition.

Smaller and smaller neighbourhoods of a point p in a variety V: Zariski-neighbourhoods (denominators are powers of some f). Local ring (denominators are functions not vanishing at p. (Etale neighbourhoods.) Analytic neighbourhoods (convergent power series). Formal neighbourhoods (formal power series).

For example, all nonsingular varieties (of dimension n) look the same formally.

Coming next: *Integral closure and Dedekind domains.* Definition of integral closure. Two examples: $\mathbb{Z}$ and $\overline{k}[t]$. Integral closure is a "local property". Definition of Dedekind domain.