FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 41

RAVI VAKIL

CONTENTS

Welcome back!

Let's now use what we have developed to study something explicit — curves. Our motivating question is a loose one: what are the curves, by which I mean nonsingular irreducible separated curves, finite type over a field k? In other words, we'll be dealing with geometry, although possibly over a non-algebraically closed field.

Here is an explicit question: are all curves (say reduced, even non-singular, finite type over given k) isomorphic? Obviously not: some are affine, and some (such as $\mathbb{P}^1$) are not. So to simplify things — and we'll further motivate this simplification in Class 42 — are all projective curves isomorphic? Perhaps all nonsingular projective curves are isomorphic to $\mathbb{P}^1$? Once again the answer is no, but the proof is a bit subtle: we've defined an invariant, the genus, and shown that $\mathbb{P}^1$ has genus 0, and that there exist nonsingular projective curves of non-zero genus. Are all (nonsingular) genus 0 curves isomorphic to $\mathbb{P}^1$? We know there exist nonsingular genus 1 curves (plane cubics) — is there only one? If not, "how many" are there?

In order to discuss interesting questions like these, we'll develop some theory. We first show a useful result that will help us focus our attention on the projective case.

1. NORMALIZATION

I now want to tell you how to normalize a reduced Noetherian scheme, which is roughly how best to turn a scheme into a normal scheme. More precisely, a **normalization** of a scheme X is a morphism $\nu : \tilde{X} \to X$ from a normal scheme, where ν induces a bijection of irreducible components of $\tilde{X}$ and X, and ν gives a birational morphism on each of the components. It will be nicer still, as it will satisfy a universal property. (I drew a picture of a normalization of a curve.)

Date: Tuesday, April 1, 2008.

Let's begin with the case where X is irreducible, and hence integral. (We will then deal with the more general case, and also discuss normalization in a function field extension.)

In this case of X irreducible, the normalization $\nu : \tilde{X} \to X$ is an affine and surjective map, such that given any dominant morphism f from an irreducible normal scheme to X, this morphism factors uniquely through ν:

$$\begin{tikzcd} Y \arrow[rr, dotted, "\exists!"] \arrow[dr] & & \tilde{X} \arrow[dl, "\nu"] . \\ & X & \end{tikzcd}$$

Thus if the normalization exists, then it is unique up to unique isomorphism. We now have to show that it exists, and we do this in the usual way. We deal first with the case where X is affine, say $X = \operatorname{Spec} A$, where A is an integral domain. Then let $\tilde{A}$ be the *integral closure* of A in its fraction field $\mathrm{FF}(A)$.

1.A. EXERCISE. Show that $\nu : \operatorname{Spec} \tilde{A} \to \operatorname{Spec} A$ is surjective. (Hint: use the Going-up Theorem.)

1.B. EXERCISE. Show that $\nu : \operatorname{Spec} \tilde{A} \to \operatorname{Spec} A$ satisfies the universal property.

1.C. EXERCISE. Show that normalizations exist in general.

1.D. EXERCISE. Show that $\dim \tilde{X} = \dim X$ (hint: see the discussion around the notes for the Going-Up Theorem).

1.E. EXERCISE. Explain how to generalize the notion of normalization to the case where X is a reduced Noetherian scheme (with possibly more than one component). This basically requires defining a universal property. I'm not sure what the "perfect" definition, but all reasonable universal properties should be equivalent.

1.F. EXERCISE. Show that the normalization map is an isomorphism on an open dense subset of X.

Now might be a good time to see some examples.

1.G. EXERCISE. Show that $\operatorname{Spec} k[t] \to \operatorname{Spec} k[x,y]/(y^2 - x^2(x+1))$ given by $(x,y) \mapsto (t^2-1, t(t^2-1))$ (see Figure 1) is a normalization. (Hint: show that $k[t]$ and $k[x,y]/(y^2 - x^2(x+1))$ have the same fraction field. Show that $k[t]$ is integrally closed. Show that $k[t]/k[x,y]/(y^2 - x^2(x+1))$ is an integral extension.)

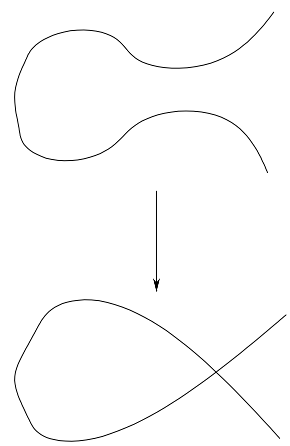

FIGURE 1. The normalization $\operatorname{Spec} k[t] \to \operatorname{Spec} k[x,y]/(y^2 - x^2(x+1))$ given by $(x,y) \mapsto (t^2-1, t(t^2-1))$

You will see that once we guess what the normalization is, it isn't hard to verify that it is indeed the normalization. Perhaps a few words are in order as to where the polynomials t^2-1 and $t(t^2-1)$ arose in the previous exercise. The key idea is to guess $t = y/x$. (Then $t^2 = x+1$ and $y = xt$ quickly.) The key idea comes from three possible places. We begin by sketching the curve, and noticing the node at the origin. (a) The function y/x is well-defined away from the node, and at the node, the two branches have "values" $y/x = 1$ and $y/x = -1$. (b) We can also note that if $t = y/x$, then t^2 is a polynomial, so we'll need to adjoin t in order to obtain the normalization. (c) The curve is cubic, so we expect a general line to meet the cubic in three points, counted with multiplicity. (We'll make this precise when we discuss Bezout's Theorem.) There is a $\mathbb{P}^1$ parametrizing lines through the origin (with co-ordinate equal to the slope of the line, y/x), and most such lines meet the curve with multiplicity two at the origin, and hence meet the curve at precisely one other point of the curve. So this "co-ordinatizes" most of the curve, and we try adding in this co-ordinate.

1.H. EXERCISE. Find the normalization of the cusp $y^2 = x^3$.

1.I. EXERCISE. Find the normalization of the tacnode $y^2 = x^4$.

Notice that in the previous examples, normalization "resolves" the singularities of the curve. In general, it will do so in dimension one (in reasonable Noetherian circumstances, as normal Noetherian domains of dimension one are all Discrete Valuation Rings), but won't do so in higher dimension (we'll see that the cone $z^2 = x^2 + y^2$ is normal).

1.J. EXERCISE. Suppose $X = \operatorname{Spec} \mathbb{Z}[15i]$. Describe the normalization $\tilde{X} \to X$. (Hint: it isn't hard to find an integral extension of $\mathbb{Z}[15i]$ that is integrally closed.) Over what points of X is the normalization not an isomorphism?

The following fact is useful.

1.1. *Theorem (finiteness of integral closure).* — *Suppose* A *is a domain,* $K = FF(A)$, L/K *is a finite separable field extension, and* B *is the integral closure of* A *in* L *("the integral closure of* A *in the field extension* L/K*", i.e. those elements of* L *integral over* A*).*
(a) if A *is integrally closed, then* B *is a finitely generated* A*-module.*
(b) if A *is a finitely generated* k*-algebra, then* B *(the integral closure of* A *in its fraction field) is a finitely generated* A*-module.*

I hope to type up a proof of these facts at some point to show you that they are not that bad. Much of part (a) was proved by Greg Brumfiel in 210B.

Warning: (b) does *not* hold for Noetherian A in general. I find this very alarming. I don't know an example offhand, but one is given in Eisenbud's book. This is a sign that this Theorem is not easy.

1.K. EXERCISE. Show that if X is an integral finite-type k-scheme, then its normalization $\nu : \tilde{X} \to X$ is a finite morphism.

1.L. EXERCISE. (This is an important generalization!) Suppose X is an integral scheme. Define the *normalization of* X, $\nu : \tilde{X} \to X$, *in a given finite field extension of the function field of* X. Show that $\tilde{X}$ is normal. (This will be hard-wired into your definition.) Show that if either X is itself normal, or X is finite type over a field k, then the normalization in a finite field extension is a finite morphism. Again, this is a finite morphism. (Again, for this we need finiteness of integral closure 1.1.)

Let's try this in a few cases.

1.M. EXERCISE. Suppose $X = \operatorname{Spec} \mathbb{Z}$ (with function field $\mathbb{Q}$). Find its integral closure in the field extension $\mathbb{Q}(i)$. (There is no "geometric" way to do this; it is purely an algebraic problem, although the answer should be understood geometrically.)

A finite extension K of $\mathbb{Q}$ is called a *number field*, and the integral closure of $\mathbb{Z}$ in K the *ring of integers of* K, denoted $\mathcal{O}_K$. (This notation is a little awkward given our other use of the symbol $\mathcal{O}$.) By the previous exercises, $\operatorname{Spec} \mathcal{O}_K$ is a Noetherian normal domain of dimension 1 (hence regular). This is called a *Dedekind domain*. We think of it as a smooth curve.

1.N. EXERCISE. (a) Suppose $X = \operatorname{Spec} k[x]$ (with function field $k(x)$). Find its integral closure in the field extension $k(y)$, where $y^2 = x^2 + x$. (Again we get a Dedekind domain.)
(b) Suppose $X = \mathbb{P}^1$, with distinguished open $\operatorname{Spec} k[x]$. Find its integral closure in the field extension $k(y)$, where $y^2 = x^2 + x$. (Part (a) involves computing the normalization over one affine open set; now figure out what happens over the "other" affine open set.)

2. Extending maps to projective schemes over smooth codimension one points: the "clear denominators" theorem

2.1. *The "curve to projective" extension Theorem. — Suppose* C *is a pure dimension* 1 *Noetherian scheme over a base* S, *and* $p \in C$ *is a nonsingular closed point of it. Suppose* Y *is a projective* S-*scheme. Then any morphism* $C - p \to Y$ *extends to* $C \to Y$.

I often called this the "clear denominators" theorem because it reminds me of the central simple idea in the proof. Suppose you have a map from $\mathbb{A}^1 - \{0\}$ to projective space, and you wanted to extend it to $\mathbb{P}^n$. Say for example the map was given by $t \mapsto [t^4 + t^{-3}; t^{-2} + 4t]$. Then of course you would "clear the denominators", and replace the map by $t \mapsto [t^7 + 1; t + t^4]$.

In practice, we'll use this theorem when $S = k$, and C is a k-variety.

Note that if such an extension exists, then it is unique: The non-reduced locus of C is a closed subset (we checked this earlier for any Noetherian scheme), not including p, so by replacing C by an open neighborhood of p that is reduced, we can use the theorem that maps from reduced schemes to separated schemes are determined by their behavior on a dense open set.

I will give three proofs, which I find enlightening in different ways.

Proof 1. By restricting to an affine neighborhood of C, we can reduce to the case where C is affine. We can similarly assume S is affine.

We next reduce to the case where $Y = \mathbb{P}^n_S$. Choose a closed immersion $Y \to \mathbb{P}^n_S$. If the result holds for $\mathbb{P}^n$, and we have a morphism $C \to \mathbb{P}^n$ with $C - p$ mapping to Y, then C must map to Y as well. Reason: we can reduce to the case where the source is an affine open subset, and the target is $\mathbb{A}^n_k \subset \mathbb{P}^n_k$ (and hence affine). Then the functions vanishing on $Y \cap \mathbb{A}^n_k$ pull back to functions that vanish at the generic point of C and hence vanish everywhere on C, i.e. C maps to Y.

Choose a uniformizer $t \in \mathfrak{m} - \mathfrak{m}^2$ in the local ring of C at p. By discarding the points of the vanishing set $V(t)$ aside from p, and taking an affine open subset of p in the remainder we reduce to the case where t cuts out precisely $\mathfrak{m}$ (i.e. $\mathfrak{m} = (y)$). Choose a dense open subset U of $C - p$ where the pullback of $\mathcal{O}(1)$ is trivial. Take an affine open neighborhood $\operatorname{Spec} A$ of p in $U \cup \{p\}$. Then the map $\operatorname{Spec} A - p \to \mathbb{P}^n$ corresponds to $n+1$ functions, say $f_0, \dots, f_n \in A_{\mathfrak{m}}$, not all zero. Let m be the smallest valuation of all the f_i. Then $[t^{-m} f_0; \dots; t^{-m} f_n]$ has all entries in A, and not all in the maximal ideal, and thus is defined at p as well. $\square$

Proof 2. We first extend the map $\operatorname{Spec} FF(C) \to Y$ to $\operatorname{Spec} \mathcal{O}_{C,p} \to Y$. We do this as follows. Note that $\mathcal{O}_{C,p}$ is a discrete valuation ring. We show first that there is a morphism $\operatorname{Spec} \mathcal{O}_{C,p} \to \mathbb{P}^n$. The rational map can be described as $[a_0; a_1; \cdots; a_n]$ where $a_i \in \mathcal{O}_{C,p}$. Let m be the minimum valuation of the a_i, and let t be a uniformizer of $\mathcal{O}_{C,p}$ (an element of valuation 1). Then $[t^{-m}a_0; t^{-m}a_1; \dots t^{-m}a_n]$ is another description of the morphism $\operatorname{Spec} \mathrm{FF}(\mathcal{O}_{C,p}) \to \mathbb{P}^n$, and each of the entries lie in $\mathcal{O}_{C,p}$, and not all entries lie in $\mathfrak{m}$ (as one of the entries has valuation 0). This same expression gives a morphism $\operatorname{Spec} \mathcal{O}_{C,p} \to \mathbb{P}^n$.

Our intuition now is that we want to glue the maps $\operatorname{Spec} \mathcal{O}_{C,p} \to Y$ (which we picture as a map from a germ of a curve) and $C - p \to Y$ (which we picture as the rest of the curve). Let $\operatorname{Spec} R \subset Y$ be an affine open subset of Y containing the image of $\operatorname{Spec} \mathcal{O}_{C,p}$. Let $\operatorname{Spec} A \subset C$ be an affine open of C containing p, and such that the image of $\operatorname{Spec} A - p$ in Y lies in $\operatorname{Spec} R$, and such that p is cut out scheme-theoretically by a single equation (i.e. there is an element $t \in A$ such that (t) is the maximal ideal corresponding to p. Then R and A are domains, and we have two maps $R \to A_{(t)}$ (corresponding to $\operatorname{Spec} \mathcal{O}_{C,p} \to \operatorname{Spec} R$) and $R \to A_t$ (corresponding to $\operatorname{Spec} A - p \to \operatorname{Spec} R$) that agree "at the generic point", i.e. that give the same map $R \to \mathrm{FF}(A)$. But $A_t \cap A_{(t)} = A$ in $\mathrm{FF}(A)$ (e.g. by algebraic Hartogs' theorem — elements of the fraction field of A that don't have any poles away from t, nor at t, must lie in A), so we indeed have a map $R \to A$ agreeing with both morphisms. $\square$

Proof 3. As $Y \to S$, by the valuative criterion of properness, the map $\operatorname{Spec} \mathrm{FF}(C) \to Y$ extends to $\operatorname{Spec} \mathcal{O}_{C,p} \to Y$. Then proceed as in Proof 2. $\square$

The third proof is quite short, and indeed extends the statement of Theorem 2.1 to the proper case. The only downside is that the previous proofs are straightforward, while the proof of the valuative criterion is highly nontrivial.

2.A. EXERCISE (USEFUL PRACTICE!). Suppose X is a Noetherian k-scheme, and Z is an irreducible codimension 1 subvariety whose generic point is a nonsingular point of X (so the local ring $\mathcal{O}_{X,Z}$ is a discrete valuation ring). Suppose $X \dashrightarrow Y$ is a rational map to a projective k-scheme. Show that the domain of definition of the rational map includes a dense open subset of Z. In other words, rational maps from Noetherian k-schemes to projective k-schemes can be extended over nonsingular codimension 1 sets. (By the easy direction of the valuative criterion of separatedness, or the theorem of uniqueness of extensions of maps from reduced schemes to separated schemes.) this map is unique.)

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

FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 42

RAVI VAKIL

CONTENTS

Last day we saw three proofs of:

0.1. *The "curve to projective" extension Theorem. — Suppose* C *is a pure dimension* 1 *Noetherian scheme over a base* S*, and* $p \in C$ *is a nonsingular closed point of it. Suppose* Y *is a projective* S*-scheme. Then any morphism* $C - p \to Y$ *extends to* $C \to Y$.

We now use the "Curve-to-projective" Extension Theorem 0.1 to show the following.

0.2. *Theorem. — If* C *is an irreducible nonsingular curve over a field* k*, then there is an open immersion* $C \hookrightarrow C'$ *into some projective nonsingular curve* C' *(over* k*).*

We'll use make particular use of the fact that one-dimensional Noetherian schemes have a boring topology.

Proof. We begin by finding a nonconstant map to $\mathbb{P}^1$. Given a nonsingular irreducible k-curve C, take a non-empty (=dense) affine open set, and take any non-constant function f on that affine open set to get a rational map $C \dashrightarrow \mathbb{P}^1$ given by $[1; f]$. As a dense open set of a dimension 1 scheme consists of everything but a finite number of points, by the "Curve-to-projective" Extension Theorem 0.1, this extends to a morphism $C \to \mathbb{P}^1$.

We now take the normalization of $\mathbb{P}^1$ in the function field $FF(C)$ of C (a finite extension of $FF(\mathbb{P}^1)$), to obtain $C' \to \mathbb{P}^1$. (Normalization in a field extension was discussed in Exercise last day.)

Now C' is normal, hence nonsingular (as nonsingular = normal in dimension 1). By the finiteness of integral closure, $C' \to \mathbb{P}^1$ is a finite morphism. Moreover, finite morphisms are projective, so by considering the composition of projective morphisms $C' \to \mathbb{P}^1 \to \operatorname{Spec} k$, we see that C' is projective over k. Thus we have an isomorphism $FF(C') \to FF(C)$, hence a rational map $C \dashrightarrow C'$, which extends to a morphism $C \to C'$ by the "Curve-to-Projective" Extension Theorem 0.1.

Date: Thursday, April 3, 2008.

Finally, I claim that $C \to C'$ is an open immersion. If we can prove this, then we are done. I note first that this is an injection of sets:

- the generic point goes to the generic point
- the closed points of C correspond to distinct valuations on $FF(C)$ (as C is separated, by the easy direction of the valuative criterion of separatedness)

Thus as sets, C is C' minus a finite number of points. As the topology on C and C' is the "cofinite topology" (i.e. the open sets include the empty set, plus everything minus a finite number of closed points), the map $C \to C'$ of topological spaces expresses C as a homeomorphism of C onto its image $\mathrm{im}(C)$. Let $f : C \to \mathrm{im}(C)$ be this morphism of schemes. Then the morphism $\mathcal{O}_{\mathrm{im}(C)} \to f_* \mathcal{O}_C$ can be interpreted as $\mathcal{O}_{\mathrm{im}(C)} \to \mathcal{O}_C$ (where we are identifying C and $\mathrm{im}(C)$ via the homeomorphism f). This morphism of sheaves is an isomorphism of stalks at all points $p \in \mathrm{im}(C)$ (the stalks are both isomorphic to the discrete valuation ring corresponding to $p \in C'$), and is hence an isomorphism. Thus $C \to \mathrm{im}(C)$ is an isomorphism of schemes, and thus $C \to C'$ is an open immersion. $\square$

1. Various categories of "curves" are all essentially the same

1.1. *Theorem. — The following categories are equivalent.*

(i) *irreducible nonsingular projective curves* $/k$*, and surjective* k*-morphisms.*
(ii) *irreducible nonsingular projective curves* $/k$*, and dominant* k*-morphisms.*
(iii) *irreducible nonsingular projective curves* $/k$*, and dominant rational maps* $/k$*.*
(iv) *irreducible reduced* $/k$ *curves, and dominant rational maps* $/k$*.*
(v) *the opposite category of fields of transcendence degree* 1 *over* k*, and* k*-homomorphisms.*

For simplicity of notation, all morphisms and maps in the following discussion are assumed to be defined over k.

This Theorem has a lot of implications. For example, each quasiprojective reduced curve is birational to precisely one projective nonsingular curve. Also, we now see that transcendence degree 1 field extensions have a genus, through their equivalence to curves. Thus we know for the first time that there exist transcendence degree 1 extensions of k that are not generated by a single element.

1.A. Exercise. Show that all nonsingular proper curves are projective. (Hint: suppose C is such a curve. It admits an open immersion $i : C \hookrightarrow C'$. Argue that i is proper, and hence has closed image.)

The interested reader can tweak the proof below to show the following variation of the theorem: in (i)–(iv), consider only geometrically irreducible curves, and in (v), consider only fields K such that $\overline{k} \cap K = k$ in $\overline{K}$. This variation allows us to exclude "weird" curves we may not want to consider. For example, if $k = \mathbb{R}$, then we are allowing curves such as $\mathbb{P}^1_{\mathbb{C}}$ which are not geometrically irreducible (as $\mathbb{P}^1_{\mathbb{C}} \times_{\mathbb{R}} \mathbb{C} \cong \mathbb{P}^1_{\mathbb{C}} \coprod \mathbb{P}^1_{\mathbb{C}}$).

Proof. Any surjective morphism is a dominant morphism, and any dominant morphism is a dominant rational map, and each nonsingular projective curve is a quasiprojective curve, so we've shown (i) $\to$ (ii) $\to$ (iii) $\to$ (iv). To get from (iv) to (i), we first note that the nonsingular points on a quasiprojective reduced curve are dense. (One way to see this: normalization is an isomorphism away from a closed subset, an Exercise last day.) Given a dominant rational map between quasiprojective reduced curves $C \to C'$, we get a dominant rational map between their normalizations, which in turn gives a dominant rational map between their projective models $D \dashrightarrow D'$. The dominant rational map is necessarily a morphism by the "Curve-to-Projective" Extension Theorem 0.1, and then this morphism is necessarily projective and hence closed, and hence surjective (as the image contains the generic point of D', and hence its closure). Thus we have established (iv) $\to$ (i).

It remains to connect (v). Each dominant rational map of quasiprojective reduced curves indeed yields a map of function fields of dimension 1 (their fraction fields). Each function field of dimension 1 yields a reduced affine (hence quasiprojective) curve over k, and each map of two such yields a dominant rational map of the curves. $\square$

1.2. Degree of a morphism between projective nonsingular curves.

You might already have a reasonable sense that a map of compact Riemann surfaces has a well-behaved degree, that the number of preimages of a point of C' is constant, so long as the preimages are counted with appropriate multiplicity. For example, if f locally looks like $z \mapsto z^m = y$, then near $y = 0$ and $z = 0$ (but not *at* $z = 0$), each point has precisely m preimages, but as y goes to 0, the m preimages coalesce.

We now show the algebraic version of this fact. Suppose $f : C \to C'$ is a surjective (or equivalently, dominant) map of nonsingular projective curves. We will show that f has a well-behaved degree, in a sense that we will now make precise.

Then f is finite, as f is a projective morphism with finite fibers. Alternatively, we can see the finiteness of f as follows. Let C'' be the normalization of C' in the function field of C. Then we have an isomorphism $FF(C) \cong FF(C'')$ which leads to birational maps $C \dashleftarrow\dashrightarrow C''$ which extend to morphisms as both C and C'' are nonsingular and projective. Thus this yields an isomorphism of C and C''. But $C'' \to C$ is a finite morphism by the finiteness of integral closure.

1.3. *Proposition. — Suppose that $\pi : C \to C'$ is a surjective finite morphism, where C is an integral curve, and C' is an integral nonsingular curve. Then $\pi_* \mathcal{O}_C$ is locally free of finite rank.*

As π is finite, $\pi_* \mathcal{O}_C$ is a finite type sheaf on $\mathcal{O}'_C$.

Before proving the proposition. I want to remind you what this means. Suppose d is the rank of this allegedly locally free sheaf. Then the fiber over any point of C with residue field K is the Spec of an algebra of dimension d over K. This means that the number of points in the fiber, counted with appropriate multiplicity, is always d.

As a motivating example, consider the map $\mathbb{Q}[y] \to \mathbb{Q}[x]$ given by $x \mapsto y^2$. (We've seen this example before.) I picture this as the projection of the parabola $x = y^2$ to the x-axis.

(i) The fiber over $x = 1$ is $\mathbb{Q}[y]/(y^2 - 1)$, so we get 2 points.
(ii) The fiber over $x = 0$ is $\mathbb{Q}[y]/(y^2)$ — we get one point, with multiplicity 2, arising because of the nonreducedness.
(iii) The fiber over $x = -1$ is $\mathbb{Q}[y]/(y^2+1) \cong \mathbb{Q}[i]$ — we get one point, with multiplicity 2, arising because of the field extension.
(iv) Finally, the fiber over the generic point $\operatorname{Spec} \mathbb{Q}(x)$ is $\operatorname{Spec} \mathbb{Q}(y)$, which is one point, with multiplicity 2, arising again because of the field extension (as $\mathbb{Q}(y)/\mathbb{Q}(x)$ is a degree 2 extension).

We thus see three sorts of behaviors (as (iii) and (iv) are the same behavior). Note that even if you only work with algebraically closed fields, you will still be forced to this third type of behavior, because residue fields at generic points tend not to be algebraically closed (witness case (iv) above).

Note that we need C' to be nonsingular for this to be true. Otherwise, the normalization of a nodal curve (Figure 1) shows an example where most points have one preimage, and one point (the node) has two.

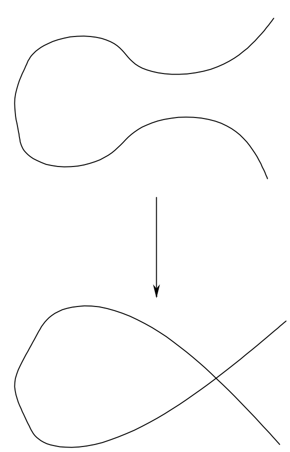

FIGURE 1. Normalization of a node shows that degree need not be well-behaved if the target is not smooth

Proof of Proposition 1.3. (For experts: we will later see that what matters here is that the morphism is finite and *flat*. But we don't yet know about flatness.)

The question is local on the target, so we may assume that C' is affine. Note that $\pi_* \mathcal{O}_C$ is torsion-free (as $\Gamma(C, \mathcal{O}_C)$ is an integral domain). Our plan is as follows: by an important exercise from ages ago, if the rank of the coherent sheaf $\pi_* \mathcal{O}_C$ is constant, then (as C' is reduced) $\pi_* \mathcal{O}_C$ is locally free. We'll show this by showing the rank at any closed point p of C' is the same as the rank at the generic point.

The notion of "rank at a point" behaves well under base change, so we base change to the discrete valuation ring $\mathcal{O}_{C',p}$. Then $\pi_* \mathcal{O}_C$ is a finitely generated module over a discrete valuation ring which is torsion-free. By the classification of finitely generated modules over a principal ideal domain, any finitely generate module over a principal ideal domain A is a direct sum of modules of the form $A/(d)$ for various $d \in A$. But if A is a discrete valuation ring, and $A/(d)$ is torsion-free, then $A/(d)$ is necessarily A (as for example all ideals of A are of the form 0 or a power of the maximal ideal). Thus we are done. $\square$

Remark. Degrees maps of complex algebraic curves in this algebro-geometric sense agrees with the usual topological degree, which can after all be computed in the same way, by "counting preimages" appropriately.

1.B. EXERCISE. Suppose $f : C \to C'$ is a degree d morphism of integral projective nonsingular curves, and $\mathcal{L}$ is an invertible sheaf on C'. Show that $\deg_C f^* \mathcal{L} = d \deg_{C'} \mathcal{L}$. (Hint: compute $\deg_{\mathcal{L}}$ using any non-zero rational section s of $\mathcal{L}$, and compute $\deg f^* \mathcal{L}$ using the rational section $f^* s$ of $f^* \mathcal{L}$. Note that zeros pull back to zeros, and poles pull back to poles.)

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

FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 43

RAVI VAKIL

CONTENTS

1. FACTS WE'LL SOON KNOW ABOUT CURVES

We almost know enough to say a lot of interesting things about curves. There are a few more notions and facts that are very helpful, and I'll state them now as "black boxes" to take for granted. We'll prove everything in due course, and hopefully after seeing how useful they are, you'll be highly motivated to learn more.

For this topic, we will assume that all curves are projective, geometrically integral, nonsingular curves over a field k.

We will sometimes add the hypothesis that k is algebraically closed. Most people are happy with working over algebraically closed fields, and those people should ignore the adverb "geometrically" in the previous paragraph.

1.1. Differentials on curves.

Riemann surfaces (and complex manifolds more generally) support the notion of a *differential*, things which can be locally interpreted as $f(z)dz$, where z is a local parameter.

Similarly, there is a sheaf of differentials on a curve C, denoted Ω_C, which is an invertible sheaf. In general, a nonsingular k-variety X of dimension d will have a sheaf of differentials Ω_X that will be locally free of rank d. Its determinant is called the *canonical bundle* $\mathcal{K}_X$. In our case, $X = C$ is a curve, so $\mathcal{K}_C = \Omega_C$, and from here on in, we'll use $\mathcal{K}$ instead of Ω_C.

1.2. Serre duality.

The canonical bundle $\mathcal{K}$ is also an example of a *dualizing sheaf* because of its role in Serre duality. Serre duality states that (i) $H^1(C, \mathcal{K}) \cong k$. (ii) Further, for any coherent sheaf $\mathcal{F}$, the natural map

$$\boxed{H^0(C, \mathcal{F}) \otimes_k H^1(C, \mathcal{K} \otimes \mathcal{F}^\vee) \to H^1(C, \mathcal{K}) \cong k}$$

Date: Tuesday, April 8, 2008.

is a perfect pairing. (This is our first black box! — remember this, as we will use it repeatedly!) Thus in particular, $h^0(C, \mathcal{F}) = h^1(C, \mathcal{K} \otimes \mathcal{F}^\vee)$. Recall we defined the arithmetic genus of a curve to be $h^1(C, \mathcal{O}_C)$. Hence $h^0(C, \mathcal{K}) = g$ as well: there is a g-dimensional family of differentials.

1.3. *Proposition.* — $\deg \mathcal{K} = 2g - 2$.

Proof. Recall that Riemann-Roch for a invertible sheaf $\mathcal{L}$ states that

$$h^0(C, \mathcal{L}) - h^1(C, \mathcal{L}) = \deg \mathcal{L} - g + 1.$$

Applying this to $\mathcal{L} = \mathcal{K}$, we get

$$\deg \mathcal{K} = h^0(C, \mathcal{K}) - h^1(C, \mathcal{K}) + g - 1 = h^1(C, \mathcal{O}) - h^0(C, \mathcal{O}) + g - 1 = g - 1 + g - 1 = 2g - 2.$$

□

1.4. *Example.* If $C = \mathbb{P}^1$, then the above Proposition implies $\mathcal{K} \cong \mathcal{O}(-2)$. Here is a heuristic which will later be made precise. On the affine open subset $x_0 \neq 0$, given by $\operatorname{Spec} k[x_{1/0}]$, we expect $dx_{1/0}$ to be a differential, which has no poles or zeros. Let's analyze this as a differential on an open subset of the other affine open subset, $\operatorname{Spec} k[x_{0/1}]$, where $x_{0/1} = 1/x_{1/0}$. If differentials behave the way we are used to, then $dx_{1/0} = -(1/x_{0/1}^2)dx_{0/1}$. Thus we expect that the rational differential $dx_{1/0}$ on $\mathbb{P}^1$ to have no zeros, and a pole at order 2 "at ∞", so the line bundle of differentials must be isomorphic to $\mathcal{O}(-2)$.

Part (i) of Serre duality certainly holds: $h^1(\mathbb{P}^1, \mathcal{O}(-2)) = 1$. Moreover, we also have a natural perfect pairing

$$H^0(\mathbb{P}^1, \mathcal{O}(n)) \times H^1(\mathbb{P}^1, \mathcal{O}(-2-n)) \to k.$$

If $n < 0$, both factors on the left are 0, so we assume $n > 0$. Then $H^0(\mathbb{P}^1, \mathcal{O}(n))$ corresponds to homogeneous degree n polynomials in x and y, and $H^1(\mathbb{P}^1, \mathcal{O}(-2-n))$ corresponds to homogeneous degree $-2-n$ Laurent polynomials in x and y so that the degrees of x and y are both at most $n-1$. You can quickly check that the dimension of both vector spaces are $n+1$. The pairing is given as follows: multiply the polynomial by the Laurent polynomial, to obtain a Laurent polynomial of degree -2. Read off the co-efficient of $x^{-1}y^{-1}$.

1.5. The Riemann-Hurwitz formula.

Differentials pull back: any surjective morphism of curves $f : C \to C'$ induces a natural map $f^*\Omega_{C'} \to \Omega_C$.

Suppose $f : C \to C'$ is a dominant morphism. Then it turns out $f^*\Omega_{C'} \hookrightarrow \Omega_C$ is an inclusion of invertible sheaves. (This is a case when inclusions of invertible sheaves does not mean what people normally mean by inclusion of line bundles, which are always isomorphisms.) The fact that this is injective arises from the fact that Ω_C is a line bundle, and hence torsion-free, and thus has no non-zero torsion subsheaves. But $f^*\Omega_{C'} \to \Omega_C$ is non-zero at the generic point, so the kernel is necessarily torsion.

Its cokernel is supported in dimension 0:

$$0 \to f^*\Omega_{C'} \to \Omega_C \to [\text{dimension } 0] \to 0.$$

The divisor R corresponding to those points (with multiplicity), is called the **ramification divisor**.

By an Exercise from the last couple of classes, the degree of the pullback of an invertible sheaf is the degree of the map times the degree of the original invertible sheaf. Thus if d is the degree of the cover, $\deg \Omega_C = d \deg \Omega_{C'} + \deg R$. Hence if $C \to C'$ is a degree d cover of curves, then

$$\boxed{2g_c - 2 = d(2g_{C'} - 2) + \deg R}$$

This is our second black box. Remember it!

Let's now figure out how to measure $\deg R$. We can study this in local coordinates. We don't have the technology to describe this precisely yet, so we'll stick to the case where $\operatorname{char} k = 0$ and k is algebraically closed whenever we use the Riemann-Hurwitz formula, until we formally prove things. Heuristically, if the map at $q \in C'$ looks like $u \mapsto u^n = t$, then $dt \mapsto d(u^n) = nu^{n-1}du$, so dt when pulled back vanishes to order $n-1$. Thus branching of this sort $u \mapsto u^n$ contributes $n-1$ to the ramification divisor. (More correctly, we should look at the map of Spec's of discrete valuation rings, and then u is a uniformizer for the stalk at q, and t is a uniformizer for the stalk at $f(q)$, and t is actually a unit times u^n. But the same argument works.)

1.A. EASY BUT CRUCIAL EXERCISE. Suppose $C \to C'$ is a degree d map of nonsingular projective curves over k ($\operatorname{char} k = 0$ and $k = \overline{k}$), and the closed points $p \in C'$ has e preimages (set-theoretically). Show that the amount of ramification above p (the degree of the part of the ramification divisor supported in the preimage of p) is $d - e$.

Here are some applications.

1.B. EXERCISE. Show that there is no nonconstant map from a genus 2 curve to a genus 3 curve. (Hint: $\deg R \geq 0$.)

1.6. *Example: Hyperelliptic curves..* Hyperelliptic curves are curves that are double covers of $\mathbb{P}^1_k$. If they are genus g, then they are branched over $2g+2$ points, as each ramification can happen to order only 1. (Warning: we are in characteristic 0!) You may already have heard about genus 1 complex curves double covering $\mathbb{P}^1$, branched over 4 points.

1.7. *Example.* For any map, the degree of R is even: any cover of a curve must be branched over an even number of points (counted with multiplicity).

1.8. *Example.* The only connected unbranched cover of $\mathbb{P}^1_k$ is the isomorphism. Reason: if $\deg R = 0$, then we have $2 - 2g_C = 2d$ with $d \geq 1$ and $g_c \geq 0$, from which $d = 1$ and $g_C = 0$.

1.9. *Example: Lüroth's theorem..* Suppose $g(C) = 0$. Then from the Riemann-Hurwitz formula, $g(C') = 0$. (Otherwise, if $g_{C'}$ were at least 1, then the right side of the Riemann-Hurwitz formula would be non-negative, and thus couldn't be -2, which is the left side. This has a non-obvious algebraic consequence, by our identification of covers of curves with field extensions. All subfields of $k(x)$ containing k are of the form $k(y)$ where $y = f(x)$. (It turns out that the hypotheses that $\operatorname{char} k = 0$ and $k = \overline{k}$ are not necessary; we'll remove them in due course.)

1.10. A criterion for when a morphism is a closed immersion.

The third fact we need is a criterion for when something is a closed immersion. This won't need to be a black box — we'll be able to prove it. To help set it up, let's recall some facts about closed immersions. Suppose $f : X \to Y$ is a closed immersion. Then f is projective, and it is injective on points. This is not enough to ensure that it is a closed immersion, as the example of the normalization of the cusp shows (Figure 1). Another example is the *Frobenius morphism* from $\mathbb{A}^1$ to $\mathbb{A}^1$, given by $k[t] \to k[u]$, $u \to t^p$, where k has characteristic p.

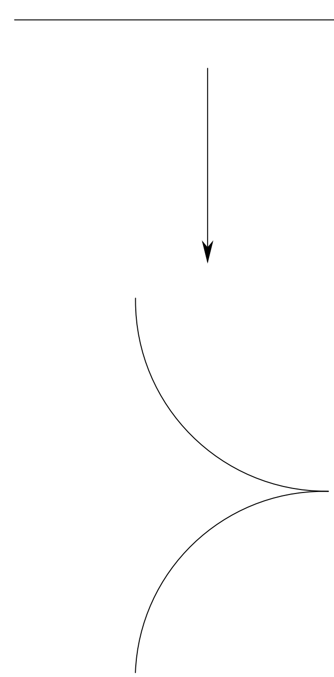

FIGURE 1. Projective morphisms that are injective on points need not be closed immersions

The additional information you need is that the tangent map is an isomorphism at all closed points.

1.C. EXERCISE. Show that in the two examples described above (the normalization of a cusp and the Frobenius morphism), the tangent map is *not* an isomorphism at all closed point.

1.11. *Theorem. — Suppose* $k = \overline{k}$, *and* $f : X \to Y$ *is a projective morphism of finite-type* k-*schemes that is injective on closed points and injective on tangent vectors at closed points. Then* f *is a closed immersion.*

(Remark: this is the definition of an *unramified* map in this situation. We will later define this in more generality.)

The example $\operatorname{Spec} \mathbb{C} \to \operatorname{Spec} \mathbb{R}$ shows that we need the hypothesis that k is algebraically closed. For those of you who are allergic to algebraically closed fields: still pay attention, as we'll use this to prove things about curves over k where k is *not* necessarily algebraically closed.

We need the hypothesis of projective morphism, as shown by the example of Figure 2. It is the normalization of the node, except we erase one of the preimages of the node. We map $\mathbb{A}^1$ to the plane, so that its image is a curve with one node. We then consider the morphism we get by discarding one of the preimages of the node. Then this morphism is an injection on points, and is also injective on tangent vectors, but it is not a closed immersion. (In the world of differential geometry, this fails to be an embedding because the map doesn't give a homeomorphism onto its image.)

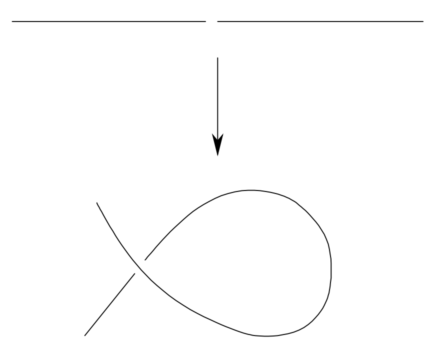

FIGURE 2. We need the projective hypothesis in Theorem 1.11

Suppose $f(p) = q$, where p and q are closed points. We will use the hypothesis that X and Y are finite type k-schemes where k is algebraically closed at only one point of the argument: that the map induces an isomorphism of residue fields at p and q.

This is the hardest result of today. We will kill the problem in old-school French style: death by a thousand cuts.

Proof. The property of being a closed immersion is local on the base, so we may assume that Y is affine, say $\operatorname{Spec} B$.

I next claim that f has finite fibers, not just finite fibers above closed points: the fiber dimension for projective morphisms is upper-semicontinuous (an earlier exercise), so the locus where the fiber dimension is at least 1 is a closed subset, so if it is non-empty, it must contain a closed point of Y. Thus the fiber over any point is a dimension 0 finite type scheme over that point, hence a finite set.

Hence f is a projective morphism with finite fibers, thus finite (an earlier corollary).

So far this argument is a straightforward sequence of reduction steps and facts we know well. But things now start to get weird.

Thus X is affine too, say $\operatorname{Spec} A$, and f corresponds to a ring morphism $B \to A$. We wish to show that this is a surjection of rings, or (equivalently) of B-modules. We will show that for any maximal ideal $\mathfrak{n}$ of B, $B_{\mathfrak{n}} \to A_{\mathfrak{n}}$ is a surjection of $B_{\mathfrak{n}}$-modules. (This will show that $B \to A$ is a surjection. Here is why: if K is the cokernel, so $B \to A \to K \to 0$, then we wish to show that $K = 0$. Now A is a finitely generated B-module, so K is as well, being a homomorphic image of A. Thus $\operatorname{Supp} K$ is a closed set. If $K \neq 0$, then $\operatorname{Supp} K$ is non-empty, and hence contains a closed point $[\mathfrak{n}]$. Then $K_{\mathfrak{n}} \neq 0$, so from the exact sequence $B_{\mathfrak{n}} \to A_{\mathfrak{n}} \to K_{\mathfrak{n}} \to 0$, $B_{\mathfrak{n}} \to A_{\mathfrak{n}}$ is not a surjection.)

If $A_{\mathfrak{n}} = 0$, then clearly $B_{\mathfrak{n}}$ surjects onto $A_{\mathfrak{n}}$, so assume otherwise. I claim that $A_{\mathfrak{n}} = A \otimes_B B_{\mathfrak{n}}$ is a local ring. Proof: $\operatorname{Spec} A_{\mathfrak{n}} \to \operatorname{Spec} B_{\mathfrak{n}}$ is a finite morphism (as it is obtained by base change from $\operatorname{Spec} A \to \operatorname{Spec} B$), so we can use the going-up theorem. $A_{\mathfrak{n}} \neq 0$, so $A_{\mathfrak{n}}$ *has* a prime ideal. Any point p of $\operatorname{Spec} A_{\mathfrak{n}}$ maps to some point of $\operatorname{Spec} B_{\mathfrak{n}}$, which has $[\mathfrak{n}]$ in its closure. Thus there is a point q in the closure of p that maps to $[\mathfrak{n}]$. But there is only one point of $\operatorname{Spec} A_{\mathfrak{n}}$ mapping to $[\mathfrak{n}]$, which we denote $[\mathfrak{m}]$. Thus we have shown that $\mathfrak{m}$ contains all other prime ideals of $\operatorname{Spec} A_{\mathfrak{n}}$, so $A_{\mathfrak{n}}$ is a local ring.

Here things get weirder still. We apply Nakayama, using two *different* local rings.

Injectivity of tangent vectors *means* surjectivity of cotangent vectors, i.e. $\mathfrak{n}/\mathfrak{n}^2 \to \mathfrak{m}/\mathfrak{m}^2$ is a surjection, i.e. $\mathfrak{n} \to \mathfrak{m}/\mathfrak{m}^2$ is a surjection. I claim that $\mathfrak{n}A_{\mathfrak{n}} \to \mathfrak{m}A_{\mathfrak{n}}$ is an isomorphism. Reason: Using Nakayama's lemma for the local ring $A_{\mathfrak{n}}$ and the $A_{\mathfrak{n}}$-*module* $\mathfrak{m}A_{\mathfrak{n}}$, we conclude that $\mathfrak{n}A_{\mathfrak{n}} = \mathfrak{m}A_{\mathfrak{n}}$.

Next apply Nakayama's Lemma to the $B_{\mathfrak{n}}$-*module* $A_{\mathfrak{n}}$. The element $1 \in A_{\mathfrak{n}}$ gives a generator for $A_{\mathfrak{n}}/\mathfrak{n}A_{\mathfrak{n}} = A_{\mathfrak{n}}/\mathfrak{m}A_{\mathfrak{n}}$, which equals $B_{\mathfrak{n}}/\mathfrak{n}B_{\mathfrak{n}}$ (as both equal k), so we conclude that 1 also generates $A_{\mathfrak{n}}$ as a $B_{\mathfrak{n}}$-module as desired. $\square$

1.D. EXERCISE. Use this to show that the dth Veronese morphism from $\mathbb{P}^n_k$, corresponding to the complete linear series $|\mathcal{O}_{\mathbb{P}^n_k}(d)|$, is a closed immersion. Do the same for the Segre morphism from $\mathbb{P}^m_k \times_{\operatorname{Spec} k} \mathbb{P}^n_k$. (This is just for practice for using this criterion. This is a weaker result than we had before; we've earlier checked this over an arbitrary base ring, and we are now checking it only over algebraically closed fields.)

Although Theorem 1.11 requires k to be algebraically closed, the following exercise will enable us to use it for general k.

1.E. EXERCISE. Suppose $f : X \to Y$ is a morphism over k that is affine. Show that f is a closed immersion if and only if $f \times_k \overline{k} : X \times_k \overline{k} \to Y \times_k \overline{k}$ is. (The affine hypothesis is certainly not necessary for this result, but it makes the proof easier, and this is the situation in which we will most need it.)

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

FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 44

RAVI VAKIL

CONTENTS

1. A SERIES OF CRUCIAL OBSERVATIONS

We are now ready to start understanding curves in a hands on way. We will repeatedly make use of the following series of crucial remarks, and it will be important to have them at the tip of your tongue.

In what follows, C will be a projective, nonsingular, geometrically integral, over a field k. (Often, what matters is integrality rather than geometric integrality, but most readers aren't worrying about this distinction, and those that are can weaken hypotheses as they see fit.) $\mathcal{L}$ is an invertible sheaf on C.

1.1. *Negative degree line bundles have no section.* $h^0(C, \mathcal{L}) = 0$ if $\deg \mathcal{L} < 0$. Reason: $\deg \mathcal{L}$ is the number of zeros minus the number of poles (suitably counted) of any rational section. If there is a regular section (i.e. with no poles), then this is necessarily non-negative. Refining this argument gives:

1.2. *Degree 0 line bundles, and recognizing when they are trivial.* $h^0(C, \mathcal{L}) = 0$ or 1 if $\deg \mathcal{L} = 0$, and if $h^0(C, \mathcal{L}) = 1$ then $\mathcal{L} \cong \mathcal{O}_C$. Reason: if there is a section s, it has no poles and hence no zeros. Then s gives a trivialization for the invertible sheaf. (Recall how this works: we have a natural bijection for any open set $\Gamma(U, \mathcal{L}) \leftrightarrow \Gamma(U, \mathcal{O}_U)$, where the map from left to right is $s' \mapsto s'/s$, and the map from right to left is $f \mapsto sf$.) So if there is a section, $\mathcal{L} \cong \mathcal{O}$. But we've already checked that for a geometrically integral projective variety, $h^0(\mathcal{O}) = 1$.

1.3. *Twisting $\mathcal{L}$ by a (degree 1) point changes h^0 by at most 1.* Suppose p is any closed point of degree 1 (i.e. the residue field of p is k). Then $h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p)) = 0$ or 1. Reason:

Date: Thursday, April 10, 2008.

consider $0 \to \mathcal{O}_C(-p) \to \mathcal{O}_C \to \mathcal{O}_p \to 0$, tensor with $\mathcal{L}$ (this is exact as $\mathcal{L}$ is locally free) to get

$$0 \to \mathcal{L}(-p) \to \mathcal{L} \to \mathcal{L}|_p \to 0.$$

Then $h^0(C, \mathcal{L}|_p) = 1$, so as the long exact sequence of cohomology starts off

$$0 \to H^0(C, \mathcal{L}(-p)) \to H^0(C, \mathcal{L}) \to H^0(C, \mathcal{L}|_p),$$

we are done.

1.4. *Numerical criterion for $\mathcal{L}$ to be base-point-free.* Suppose for this remark that k is algebraically closed. (In particular, *all* closed points have degree 1 over k.) Then if $h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p)) = 1$ for *all* closed points p, then $\mathcal{L}$ is base-point-free, and hence induces a morphism from C to projective space. Reason: given any p, our equality shows that there exists a section of $\mathcal{L}$ that does not vanish at p.

1.5. Next, suppose p and q are distinct (closed) points of degree 1. Then $h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p-q)) = 0, 1$, or 2 (by repeating the argument of Remark 1.3 twice). If $h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p-q)) = 2$, then necessarily

$$h^0(C, \mathcal{L}) = h^0(C, \mathcal{L}(-p)) + 1 = h^0(C, \mathcal{L}(-q)) + 1 = h^0(C, \mathcal{L}(-p-q)) + 2. \tag{1}$$

Then the linear system $\mathcal{L}$ separates points p and q, i.e. the corresponding map f to projective space satisfies $f(p) \neq f(q)$. Reason: there is a hyperplane of projective space passing through p but not passing through q, or equivalently, there is a section of $\mathcal{L}$ vanishing at p but not vanishing at q. This is because of the last equality in (1).

1.6. By the same argument as above, if p is a (closed) point of degree 1, then $h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-2p)) = 0$, 1, or 2. I claim that if this is 2, then map corresponds to $\mathcal{L}$ (which is already seen to be base-point-free from the above) separates the tangent vectors at p. To show this, I need to show that the cotangent map is *surjective*. To show surjectivity onto a one-dimensional vector space, I just need to show that the map is non-zero. So I need to give a function on the target vanishing at the image of p that pulls back to a function that vanishes at p to order 1 but not 2. In other words, I want a section of $\mathcal{L}$ vanishing at p to order 1 but not 2. But that is the content of the statement $h^0(C, \mathcal{L}(-p)) - h^0(C, \mathcal{L}(-2p)) = 1$.

1.7. *Criterion for $\mathcal{L}$ to be a closed immersion.* Combining some of our previous comments: suppose C is a curve over an *algebraically closed* field k, and $\mathcal{L}$ is an invertible sheaf such that for *all* closed points p and q, *not necessarily distinct*, $h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}(-p-q)) = 2$, then $\mathcal{L}$ gives a *closed immersion into projective space*, as it separates points and tangent vectors, by Theorem 1.11 from last day (Class 43).

1.8. *We know h^0 if the degree is sufficiently high.* We now bring in Serre duality. I claim that $\deg \mathcal{L} > 2g - 2$ implies

$$\boxed{h^0(C, \mathcal{L}) = \deg \mathcal{L} - g + 1.}$$

We know $h^0(C, \mathcal{L})$ if $\deg \mathcal{L} \gg 0$. *This is important — remember this!* Reason: $h^1(C, \mathcal{L}) = h^0(C, \mathcal{K} \otimes \mathcal{L}^\vee)$; but $\mathcal{K} \otimes \mathcal{L}^\vee$ has negative degree (as $\mathcal{K}$ has degree $2g-2$), and thus this invertible sheaf has no sections. Thus Riemann-Roch gives us the desired result.

1.A. EXERCISE. Suppose that k is algebraically closed, so the previous remark applies. Show that $C - p$ is affine. (Hint: Show that if $k \gg 0$, then $\mathcal{O}(kp)$ is base-point free and has at least two linearly independent sections, one of which has divisor kp. Use these two sections to map to $\mathbb{P}^1$ so that the preimage of ∞ is (set-theoretically) p. Argue that the map is finite, and that $C - p$ is the preimage of $\mathbb{A}^1$.)

1.B. FOLLOW-UP EXERCISE. Show that any non-projective integral curve over a field k (not necessarily algebraically closed) is affine.

1.C. USEFUL EXERCISE (RECOGNIZING $\mathcal{K}$ AMONG DEGREE $2g-2$ LINE BUNDLES). Suppose $\mathcal{L}$ is a degree $2g-2$ invertible sheaf. Show that it has $g-1$ or g sections, and it has g sections if and only if $\mathcal{L} \cong \mathcal{K}$.

1.9. Conclusion. We can combine much of the above discussion to give the following useful fact. If k is algebraically closed, then $\deg \mathcal{L} \geq 2g$ implies that $\mathcal{L}$ is basepoint free (and hence determines a morphism to projective space). Also, $\deg \mathcal{L} \geq 2g+1$ implies that this is in fact a closed immersion. Remember this!

1.D. EXERCISE. Show that the statements in the previous paragraph even without the hypothesis that k is algebraically closed. (Hint: to show one of the facts about some curve C and line bundle $\mathcal{L}$, consider instead $C \otimes_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$. Then somehow show that if the pullback of $\mathcal{L}$ here has sections giving you one of the two desired properties, then there are sections downstairs with the same properties. You may want to use facts that we've used, such as the fact that the h^0 is preserved by extension of k, or that the property of an affine morphism being a closed immersion holds if and only if it does after an extension of k, Exercise 1.E from the previous class, Class 43.)

We're now ready to take these facts and go to the races.

2. CURVES OF GENUS 0

We are now ready to (in some form) answer the question: what are the curves of genus 0?

We have seen a genus 0 curve (over a field k) that was *not* isomorphic to $\mathbb{P}^1$: $x^2+y^2+z^2 = 0$ in $\mathbb{P}^2_{\mathbb{R}}$. We have already observed that this curve is *not* isomorphic to $\mathbb{P}^1_{\mathbb{R}}$, because it doesn't have an $\mathbb{R}$-valued point. On the other hand, we haven't seen a genus 0 curve over an algebraically closed field with this property. This isn't a coincidence: the lack of an existence of a k-valued point is the only obstruction to a genus 0 curve being $\mathbb{P}^1$.

2.1. *Claim. — Suppose* C *is genus* 0*, and* C *has a* k*-valued (degree* 1*) point. Then* $C \cong \mathbb{P}^1_k$*.*

Thus we see that all genus 0 (integral, nonsingular) curves over an algebraically closed field are isomorphic to $\mathbb{P}^1$.

Proof. Let p be the point, and consider $\mathcal{L} = \mathcal{O}(p)$. Then $\deg \mathcal{L} = 1$, so we can apply what we know above: first, $h^0(C, \mathcal{L}) = 2$ (Remark 1.8), and second, these two sections give a closed immersion into $\mathbb{P}^1_k$ (Remark 1.9). But the only closed immersion of a curve into $\mathbb{P}^1_k$ is an isomorphism! □

As a fun bonus, we see that the weird real curve $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2_{\mathbb{R}}$ has no *divisors* of degree 1 over $\mathbb{R}$ (*effective* divisors); otherwise, we could just apply the above argument to the corresponding line bundle.

This weird curve shows us that over a non-algebraically closed field, there can be genus 0 curves that are not isomorphic to $\mathbb{P}^1_k$. The next result lets us get our hands on them as well.

2.2. *Claim. — All genus* 0 *curves can be described as conics in* $\mathbb{P}^2_k$*.*

Proof. Any genus 0 curve has a degree -2 line bundle — the canonical bundle $\mathcal{K}$. Thus any genus 0 curve has a degree 2 line bundle: $\mathcal{L} = \mathcal{K}^\vee$. We apply Remark 1.9: $h^0(C, \mathcal{L}) = 3 \geq 2g + 1$, so this line bundle gives a closed immersion into $\mathbb{P}^2$. □

2.A. EXERCISE. Suppose C is a genus 0 curve (projective, geometrically integral and nonsingular). Show that C has a point of degree at most 2.

We will use the following result later.

2.3. *Claim. — Suppose* C *is not isomorphic to* $\mathbb{P}^1_k$ *(with no restrictions on the genus of* C*), and* $\mathcal{L}$ *is an invertible sheaf of degree* 1*. Then* $h^0(C, \mathcal{L}) < 2$*.*

Proof. Otherwise, let s_1 and s_2 be two (independent) sections. As the divisor of zeros of s_i is the degree of $\mathcal{L}$, each vanishes at a single point p_i (to order 1). But $p_1 \neq p_2$ (or else s_1/s_2 has no poles or zeros, i.e. is a constant function, i.e. s_1 and s_2 are dependent). Thus we get a map $C \to \mathbb{P}^1$ which is basepoint free. This is a finite degree 1 map of nonsingular curves, which induces a degree 1 extension of function fields, i.e. an isomorphism of function fields, which means that the curves are isomorphic. But we assumed that C is not isomorphic to $\mathbb{P}^1_k$. □

2.B. EXERCISE. Show that if k is algebraically closed, then C has genus 0 if and only if all degree 0 line bundles are trivial.

3.1. *Why not do curves of genus* 1 *now?.* It might make most sense to jump to genus 1 at this point, but the theory of elliptic curves is especially rich and beautiful, so we'll leave it for later.

In general, curves have quite different behaviors (topologically, arithmetically, geometrically) depending on whether $g = 0$, $g = 1$, or $g > 2$. This trichotomy extends to varieties of higher dimension. I gave a very brief discussion of this trichotomy for curves. For example, arithmetically, genus 0 curves can have lots and lots of points, genus 1 curves can have lots of points, and by Faltings' Theorem (Mordell's Conjecture) any curve of genus at least 2 has at most finitely many points. (Thus we knew before Wiles that $x^n + y^n = z^n$ in $\mathbb{P}^2$ has at most finitely many solutions for $n \geq 4$, as such curves have genus $\binom{n-1}{2} > 1$.) Geometrically, Riemann surfaces of genus 0 are positively curved, Riemann surfaces of genus 1 are flat, and Riemann surfaces of genus 1 are negatively curved. We will soon see that curves of genus at least 2 have finite automorphism groups, while curves of genus 1 have some automorphisms (a one-dimensional family), and the unique curve of genus 0 (over an algebraically closed field) have a three-dimensional automorphism group.

3.2. *Back to curves of genus* 2*.*

Over an algebraically closed field, there is only one genus 0 curve. We haven't yet seen *any* curves of genus 2 — how many are there? How can we get a hold of them.

Fix a curve C of genus $g = 2$. Then $\mathcal{K}$ is degree $2g - 2 = 2$, and has 2 sections (Exercise 1.C). I claim that $\mathcal{K}$ is base-point-free. We may assume k is algebraically closed, as base-point-freeness is independent of field extension of k. If $\mathcal{K}$ is not base-point-free, then if p is a base point, then $\mathcal{K}(-p)$ is a degree 1 invertible sheaf with 2 sections, and we just showed (Claim 2.3) that this is impossible. Thus we canonically constructed a double cover of $\mathbb{P}^1$ (unique up to automorphisms of $\mathbb{P}^1$). Conversely, any double cover $C \to \mathbb{P}^1$ arises from a degree 2 invertible sheaf with at least 2 sections, so if $g(C) = 2$, this invertible sheaf must be the canonical bundle (as the only degree 2 invertible sheaf on a genus 2 curve with at least 2 sections is $\mathcal{K}_C$, Exercise 1.C).

Hence we have a natural bijection between genus 2 curves and genus 2 double covers of $\mathbb{P}^1$.

Thus if we could classify genus 2 double covers of $\mathbb{P}^1$, we could classify all genus 2 curves. We'll do that next day, at least in the case where k is algebraically closed and characteristic 0. While we're doing that, we may as well study double covers of $\mathbb{P}^1$ instead — the theory of *hyperelliptic curves*.

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

FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 45

RAVI VAKIL

CONTENTS

1. HYPERELLIPTIC CURVES

A curve C of genus at least 2 is **hyperelliptic** if it admits a degree 2 cover of $\mathbb{P}^1$. This map is often called the **hyperelliptic map**.

1.A. EXERCISE. Verify that a curve C of genus at least 1 admits a degree 2 cover of $\mathbb{P}^1$ if and only if it admits a degree 2 invertible sheaf $\mathcal{L}$ with $h^0(C, \mathcal{L}) = 2$. Possibly in the course of doing this, verify that if C is a curve, and $\mathcal{L}$ has a degree 2 invertible sheaf with at least 2 (linearly independent) sections, then $\mathcal{L}$ has precisely two sections, and that this $\mathcal{L}$ is base-point free and gives a hyperelliptic map.

The degree 2 map $C \to \mathbb{P}^1$ gives a degree 2 extension of function fields $\mathrm{FF}(C)$ over $\mathrm{FF}(\mathbb{P}^1) \cong k(t)$. If the characteristic is not 2, this extension is necessarily Galois, and the involution on C induces (via the equivalence of various categories of curves, Class 42 Theorem 1.1) an involution on C is called the **hyperelliptic involution**.

1.1. *Proposition. — If $\mathcal{L}$ corresponds to a hyperelliptic cover $C \to \mathbb{P}^1$, then $\mathcal{L}^{\otimes(g-1)} \cong \mathcal{K}_C$.*

Proof. Compose the hyperelliptic map with the $(g-1)$th Veronese map:

$$C \xrightarrow{\mathcal{L}} \mathbb{P}^1 \xrightarrow{\mathcal{O}_{\mathbb{P}^1}(g-1)} \mathbb{P}^{g-1}.$$

The composition corresponds to $\mathcal{L}^{\otimes(g-1)}$. This invertible sheaf has degree $2g-2$, and the image is nondegenerate in $\mathbb{P}^{g-1}$, and hence has at least g sections. But by Exercise 1.C of Class 44, the only invertible sheaf of degree $2g-2$ with (at least) g sections is the canonical sheaf. $\square$

Date: Tuesday, April 15, 2008.

1.2. *Proposition.* — *Any curve* C *of genus at least* 2 *admits at most one double cover of* $\mathbb{P}^1$. *In other words, a curve can be in "only one way".*

Proof. If C is hyperelliptic, then we can recover the hyperelliptic map by considering the canonical linear system given by $\mathcal{K}$ (the *canonical map*, which we'll use again soon): it is a double cover of a degree $g-1$ rational normal curve (by the previous Proposition), and this double cover is the hyperelliptic cover (also by the proof of the previous Proposition). $\square$

Next, we invoke the Riemann-Hurwitz formula. In order to do so, we need to assume $\operatorname{char} k = 0$, and $k = \overline{k}$. However, when we actually discuss differentials, and prove the Riemann-Hurwitz formula, we will see that we can just require $\operatorname{char} k \neq 2$ (and $k = \overline{k}$).

The Riemann-Hurwitz formula implies that hyperelliptic covers have precisely $2g+2$ (distinct) branch points. These branch points determine the cover:

1.3. *Claim.* — *Assume* $\operatorname{char} k \neq 2$ *and* $k = \overline{k}$. *Given* n *distinct points* $r_1, \ldots, r_n \in \mathbb{P}^1$, *there is precisely one cover branched at precisely these points if* n *is even, and none if* n *is odd.*

Proof. The result when n is odd is immediate from the Riemann-Hurwitz formula, so assume n is even.

Pick a point of $\mathbb{P}^1$ distinct from the n branch points, so all n branch points are in the "complementary" $\mathbb{A}^1$. Suppose we have a double cover of $\mathbb{A}^1$, $C \to \mathbb{A}^1$, where x is the coordinate on $\mathbb{A}^1$. This induces a quadratic field extension K over $k(x)$. As $\operatorname{char} k \neq 2$, this extension is Galois. Let σ be the hyperelliptic involution. Let y be an element of K such that $\sigma(y) = -y$, so 1 and y form a basis for K over the field $k(x)$, and are eigenvectors of σ. Now $\sigma(y^2) = y^2$, so $y^2 \in k(x)$. We can replace y by an appropriate $k(x)$-multiple so that y^2 is a polynomial, with no repeated factors, and monic. (This is where we use the hypothesis that k is algebraically closed, to get leading coefficient 1.)

Thus $y^2 = x^N + a_{N-1}x^{N-1} + \cdots + a_0$, where the polynomial on the right (call it $f(x)$) has no repeated roots. The Jacobian criterion implies that this curve C' in $\mathbb{A}^2$ (with co-ordinates x and y) is nonsingular. then C' is normal and has the same function field as C — but so is C. Thus C' and C are both normalizations of $\mathbb{A}^1$ in the finite field extension generated by y, and hence are isomorphic. Thus we have identified C in terms of an explicit equation!

The branch points correspond to those values of x for which there is exactly one value of y, i.e. the roots of $f(x)$. In particular, $N = n$, and $f(x) = (x - r_1) \cdots (x - r_n)$ (where the r_i are interpreted as elements of $\overline{k}$).

Having mastered the situation over $\mathbb{A}^1$, we return to the situation over $\mathbb{P}^1$. We have identified the function field extension K of $\mathrm{FF}(\mathbb{P}^1) = k(x)$ corresponding to any C double-covering $\mathbb{P}^1$ over the n points — there is only one up to isomorphism, given by adjoining y with $y^2 = (x - r_1) \cdots (x - r_n)$. There is a unique curve branched over $r_1, \ldots, r_n$: the normalization of $\mathbb{P}^1$ in the field extension $K/k(x)$. (You might fear that we haven't accidentally acquired a branch point at the missing point $\infty = \mathbb{P}^1 - \mathbb{A}^1$. But the total number of branch points is even, and we already have an even number of points, so there is no branching at ∞.) $\square$

We can now extract a lot of useful information.

1.4. *Curves of every genus.* For the first time, we see that there are curves of every genus $g \geq 0$ over an algebraically closed field of characteristic 0: to get a curve of genus g, consider the branched cover branched over $2g+2$ distinct points. The unique genus 0 curve is of this form, and we have seen above that every genus 2 curve is of this form. We'll soon see that every genus 1 curve is too. But it is too much to hope that all curves are of this form, and in Exercise 2.A we'll see that there are genus 3 curves that are *not* hyperelliptic, and we'll get heuristic evidence that "most" genus 3 curves are not hyperelliptic. We'll later get heuristic evidence that "most" genus g curves are not hyperelliptic if $g > 2$.

We can also classify hyperelliptic curves. Hyperelliptic curves of genus g correspond to precisely $2g + 2$ points on $\mathbb{P}^1$ modulo S_{2g+2}, and modulo automorphisms of $\mathbb{P}^1$. Thus "the space of hyperelliptic curves" has dimension

$$2g + 2 - \dim \operatorname{Aut} \mathbb{P}^1 = 2g - 1.$$

This is not a well-defined statement, because we haven't rigorously defined "the space of hyperelliptic curves" — and example of a *moduli space*. For now, take it as a plausibility statement. It is also plausible that this space is irreducible and reduced — it is the image of something irreducible and reduced.

1.5. *Genus* 2 *in particular.* In particular, if $g = 2$, we see that we have a "three-dimensional space of genus 2 curves". This isn't rigorous, but we can certainly show that there are an infinite number of non-isomorphic genus 2 curves.

1.B. EXERCISE. Fix an algebraically closed field k of characteristic 0. Show that there are an infinite number of (pairwise) non-isomorphic genus 2 curves k.

1.6. *If k is not algebraically closed.* If k is not algebraically closed (but of characteristic not 2), the above argument shows that if we have a double cover of $\mathbb{A}^1$, then it is of the form $y^2 = af(x)$, where f is monic, and $a \in k^*/(k^*)^2$. You may be able to use this to show that (assuming the $k^* \neq (k^*)^2$) a double cover is *not* determined by its branch points. Moreover, see that this failure is classified by $k^*/(k^*)^2$. Thus we have lots of curves that are not isomorphic over k, but become isomorphic over $\overline{k}$. These are often called *twists* of each other.

(In particular, even though haven't talked about elliptic curves yet, we definitely have two elliptic curves over $\mathbb{Q}$ with the same j-invariant, that are not isomorphic.)

2. Curves of genus 3

Suppose C is a curve of genus 3. Then $\mathcal{K}$ has degree $2g - 2 = 4$, and has $g = 3$ sections.

2.1. *Claim. — $\mathcal{K}$ is base-point-free, and hence gives a map to $\mathbb{P}^2$.*

Proof. We check base-point-freeness by working over the algebraic closure $\overline{k}$. For any point p, by Riemann-Roch,

$$h^0(C, \mathcal{K}(-p)) - h^0(C, \mathcal{O}(p)) = \deg(\mathcal{K}(-p)) - g + 1 = 3 - 3 + 1 = 1.$$

But $h^0(C, \mathcal{O}(p)) = 1$ by Claim 2.3 of Class 44, so

$$h^0(C, \mathcal{K}(-p)) = 2 = h^0(C, \mathcal{K}) - 1.$$

Thus p is not a base-point of $\mathcal{K}$ for any p, so by Criterion 1.4 of Class 44 for base-point-freeness, $\mathcal{K}$ is base-point-free. $\square$

The next natural question is: Is this a closed immersion? Again, we can check over algebraic closure. We use our "closed immersion test" (again, see our useful facts). If it *isn't* a closed immersion, then we can find two points p and q (possibly identical) such that

$$h^0(C, \mathcal{K}) - h^0(C, \mathcal{K}(-p - q)) = 2,$$

i.e. $h^0(C, \mathcal{K}(-p - q)) = 2$. But by Serre duality, this means that $h^0(C, \mathcal{O}(p + q)) = 2$. We have found a degree 2 divisor with 2 sections, so C is hyperelliptic. (Indeed, I could have skipped that sentence, and made this observation about $\mathcal{K}(-p - q)$, but I've done it this way in order to generalize to higher genus.) Conversely, if C is hyperelliptic, then we already know that $\mathcal{K}$ gives a double cover of a nonsingular conic in $\mathbb{P}^2$ (also known as a rational normal curve of degree 2), and hence $\mathcal{K}$ does not give a closed immersion.

Thus we conclude that if (and only if) C is not hyperelliptic, then the canonical map describes C as a degree 4 curve in $\mathbb{P}^2$.

Conversely, any quartic plane curve is canonically embedded. Reason: the curve has genus 3 (we can compute this — see our discussion of Hilbert functions), and is mapped by an invertible sheaf of degree 4 with 3 sections. But by Exercise 1.C of Class 44, the only invertible sheaf of degree $2g - 2$ with g sections is $\mathcal{K}$.

In particular, each non-hyperelliptic genus 3 curve can be described as a quartic plane curve in only one way (up to automorphisms of $\mathbb{P}^2$).

In conclusion, there is a bijection between non-hyperelliptic genus 3 curves, and plane quartics up to projective linear transformations.

2.A. Exercise. Show that there are non-hyperelliptic genus 3 curves.

2.B. EXERCISE. Give a heuristic (non-rigorous) argument that the nonhyperelliptic curves of genus 3 form a family of dimension 6. (Hint: Count the dimension of the family of nonsingular quartics, and quotient by $\operatorname{Aut} \mathbb{P}^2 = \mathsf{PGL}(3)$.)

The genus 3 curves thus seem to come in two families: the hyperelliptic curves (a family of dimension 5), and the nonhyperelliptic curves (a family of dimension 6). This is misleading — they actually come in a single family of dimension 6.

In fact, hyperelliptic curves are naturally limits of nonhyperelliptic curves. We can write down an explicit family. (This explanation necessarily requires some hand-waving, as it involves topics we haven't seen yet.) Suppose we have a hyperelliptic curve branched over $2g + 2 = 8$ points of $\mathbb{P}^1$. Choose an isomorphism of $\mathbb{P}^1$ with a conic in $\mathbb{P}^2$. There is a nonsingular quartic meeting the conic at precisely those 8 points. (This requires Bertini's theorem, so I'll skip that argument.) Then if f is the equation of the conic, and g is the equation of the quartic, then $f^2 + t^2 g$ is a family of quartics that are nonsingular for most t (nonsingular is an open condition as we will see). The $t = 0$ case is a double conic. Then it is a fact that if you normalize the family, the central fiber (above $t = 0$) turns into our hyperelliptic curve. Thus we have expressed our hyperelliptic curve as a limit of nonhyperelliptic curves.

I then discussed the 28 bitangents to any smooth quartic curve, and their relationship to other interesting geometry, for example the 6 branch points of a genus 2 hyperelliptic cover (both are examples of theta characteristics) and the 27 lines on any smooth cubic surface (and the link to the Weyl groups of E_7 and E_6). I likely won't type those up in these notes.

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

FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 46

RAVI VAKIL

CONTENTS

1. CURVES OF GENUS 4 AND 5

We begin with two exercises in general genus, and then go back to genus 4.

1.A. EXERCISE. Suppose C is a genus g curve. Show that if C is not hyperelliptic, then the canonical bundle gives a closed immersion $C \hookrightarrow \mathbb{P}^{g-1}$. (In the hyperelliptic case, we have already seen that the canonical bundle gives us a double cover of a rational normal curve.) Hint: follow the genus 3 case. Such a curve is called a **canonical curve**, and this closed immersion is called the **canonical embedding** of C.

1.B. EXERCISE. Suppose C is a curve of genus $g > 1$, over a field k that is not algebraically closed. Show that C has a closed point of degree at most $2g - 2$ over the base field. (For comparison: if $g = 1$, it turns out that there is no such bound independent of k!)

We next consider nonhyperelliptic curves C of genus 4. Note that $\deg \mathcal{K} = 6$ and $h^0(C, \mathcal{K}) = 4$, so the canonical map expresses C as a sextic curve in $\mathbb{P}^3$. We shall see that all such C are complete intersections of quadric surfaces and cubic surfaces, and conversely all nonsingular complete intersections of quadrics and cubics are genus 4 nonhyperelliptic curves, canonically embedded.

By Riemann-Roch,

$$h^0(C, \mathcal{K}^{\otimes 2}) = \deg \mathcal{K}^{\otimes 2} - g + 1 = 12 - 4 + 1 = 9.$$

We have the restriction map $H^0(\mathbb{P}^3, \mathcal{O}(2)) \to H^0(C, \mathcal{K}^{\otimes 2})$, and $\dim \operatorname{Sym}^2 \Gamma(C, \mathcal{K}) = \binom{4+1}{2} = 10$. Thus there is at least one quadric in $\mathbb{P}^3$ that vanishes on our curve C. Translation: C lies on at least on quadric Q. Now quadrics are either double planes, or the union of two planes, or cones, or nonsingular quadrics. (They corresponds to quadric forms of rank 1, 2, 3, and 4 respectively.) But C can't lie in a plane, so Q must be a cone or nonsingular. In particular, Q is irreducible.

Date: Thursday, April 17, 2008.

Now C can't lie on *two* (distinct) such quadrics, say Q and Q'. Otherwise, as Q and Q' have no common components (they are irreducible and not the same!), $Q \cap Q'$ is a curve (not necessarily reduced or irreducible). By Bezout's theorem, $Q \cap Q'$ is a curve of degree 4. Thus our curve C, being of degree 6, cannot be contained in $Q \cap Q'$. (Do you see why?)

We next consider cubics surface. By Riemann-Roch again, $h^0(C, \mathcal{K}^{\otimes 3}) = \deg \mathcal{K}^{\otimes 3} - g + 1 = 18 - 4 + 1 = 15$. Now $\dim \operatorname{Sym}^3 \Gamma(C, \mathcal{K})$ has dimension $\binom{4+2}{3} = 20$. Thus C lies on at least a 5-dimensional vector space of cubics. Now a 4-dimensional subspace come from multiplying the quadric Q by a linear form $(?w + ?x + ?y + ?z)$. But hence there is still one cubic K whose underlying form is not divisible by the quadric form Q (i.e. K doesn't contain Q.) Then K and Q share no component, so $K \cap Q$ is a complete intersection. By Bezout's theorem (the degree of a complete intersection of hypersurfaces is the product of the degrees of the hypersurfaces), we obtain a curve of degree 6. Our curve C has degree 6. This suggests that $C = K \cap Q$. In fact, $K \cap Q$ and C have the same Hilbert polynomial, and $C \subset K \cap Q$. Hence $C = K \cap Q$ by the following exercise.

1.C. EXERCISE. Suppose $X \subset Y \subset \mathbb{P}^n$ are a sequence of closed subschemes, where X and Y have the same Hilbert polynomial. Show that $X = Y$. Hint: consider the exact sequence

$$0 \to \mathcal{I}_{X/Y} \to \mathcal{O}_Y \to \mathcal{O}_X \to 0.$$

Show that if the Hilbert polynomial of $\mathcal{I}_{X/Y}$ is 0, then $\mathcal{I}_{X/Y}$ must be the 0 sheaf. (Handy trick: For $m \gg 0$, $\mathcal{I}_{X/Y}(m)$ is generated by global sections and is also 0. This of course applies with $\mathcal{I}$ replaced by *any* coherent sheaf.)

We now show the converse, and that any nonsingular complete intersection C of a quadric surface with a cubic surface is a canonically embedded genus 4 curve. By an earlier exercise on computing the genus of a complete intersection (in our discussion of Hilbert functions), such a complete intersection has genus 4.

1.D. EXERCISE. Show that $\mathcal{O}_C(1)$ has at least 4 sections. (Translation: C doesn't lie in a hyperplane.)

The only degree $2g-2$ invertible sheaf with (at least) g sections is the canonical sheaf (we've used this fact many times), so $\mathcal{O}_C(1) \cong \mathcal{K}_C$, and C is indeed canonically embedded.

1.E. EXERCISE. Give a heuristic argument suggesting that the nonhyperelliptic curves of genus 4 "form a family of dimension 9".

On to genus 5!

1.F. EXERCISE. Suppose C is a nonhyperelliptic genus 5 curve. Show that the canonical curve is degree 8 in $\mathbb{P}^4$. Show that it lies on a three-dimensional vector space of quadrics (i.e. it lies on 3 linearly independent independent quadrics). Show that a nonsingular complete intersection of 3 quadrics is a canonical genus 5 curve.

In fact a canonical genus 5 is always a complete intersection of 3 quadrics.

1.G. EXERCISE. Give a heuristic argument suggesting that the nonhyperelliptic curves of genus 5 "form a family of dimension 12".

We have now understand curves of genus 3 through 5 by thinking of canonical curves as complete intersections. Sadly our luck has run out.

1.H. EXERCISE. Show that if $C \subset \mathbb{P}^{g-1}$ is a canonical curve of genus $g \geq 6$, then C is *not* a complete intersection. (Hint: Bezout's theorem.)

2. CURVES OF GENUS 1: THE BEGINNING

To avoid dividing up these notes too much, I've moved these into the Class 47 notes.

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

FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 47

RAVI VAKIL

CONTENTS

1. CURVES OF GENUS 1

Finally, we come to the very rich case of curves of genus 1. It will be fun to present the theory by thinking about line bundles of steadily increasing degree.

1.1. Line bundles of degree 0.

Suppose C is a genus 1 curve. Then $\deg \mathcal{K}_C = 2g - 2 = 0$ and $h^0(C, \mathcal{K}_C) = g = 1$, (by Exercise 1.C of Class 44). But the only degree 0 invertible sheaf with a section is the trivial sheaf, so we conclude that $\mathcal{K} \cong \mathcal{O}$.

Next, note that if $\deg \mathcal{L} > 0$, then Riemann-Roch in high degree gives

$$h^0(C, \mathcal{L}) = \deg \mathcal{L} - g + 1 = \deg \mathcal{L}.$$

1.2. Line bundles of degree 1.

Each degree 1 (k-valued) point q determines a line bundle $\mathcal{O}(q)$, and two distinct points determine two distinct line bundles (as a degree 1 line bundle has only one section, up to scalar multiples). Conversely, any degree 1 line bundle $\mathcal{L}$ is of the form $\mathcal{O}(q)$ (as $\mathcal{L}$ has a section — then just take its divisor of zeros), and it is of this form in one and only one way.

Thus we have a canonical bijection between degree 1 line bundles and degree 1 (closed) points. (If k is algebraically closed, as all closed points have residue field k, this means that we have a canonical bijection between degree 1 line bundles and closed points.)

Define an **elliptic curve** to be a genus 1 curve E with a choice of k-valued point p. The choice of this point should always be considered part of the definition of an elliptic curve — "elliptic curve" is not a synonym for "genus 1 curve". (Note: a genus 1 curve need not

Date: Tuesday, April 22, 2008.

have any k-valued points at all! However, if $k = \overline{k}$, then any closed point is k-valued.) We will often denote elliptic curves by E rather than C.

If (E, p) is an elliptic curve, then there is a canonical bijection between the set of degree 0 invertible sheaves (up to ismorphism) and the set of degree 1 points of E: simply the twist the degree 1 line bundles by $\mathcal{O}(-p)$. Explicitly, the bijection is given by

$$\mathcal{L} \longmapsto \operatorname{div}(\mathcal{L}(p))$$

$$\mathcal{O}(q - p) \longleftarrow\!\shortmid\; q$$

But the degree 0 invertible sheaves form a group (under tensor product), so have proved:

1.3. *Proposition (the group law on the degree 1 points of an elliptic curve). — The above bijection defines an abelian group structure on the degree 1 points of an elliptic curve, where p is the identity.*

From now on, we will conflate closed points of E with degree 0 invertible sheaves on E.

For those of you familiar with the complex analytic picture, this isn't surprising: E is isomorphic to the complex numbers modulo a lattice: $E \cong \mathbb{C}/\Lambda$.

This is currently just a bijection of sets. Given that E has a much richer structure (it has a generic point, and the structure of a variety), this is a sign that there should be a way of defining some *scheme* $\operatorname{Pic}^0(E)$, and that this should be an isomorphism of schemes. We'll soon show (when discussing degree 3 line bundles) that this group structure on the degree 1 points of E comes from a group variety structure on E.

1.4. Line bundles of degree 2.

Note that $\mathcal{O}_E(2p)$ has 2 sections, so E admits a double cover of $\mathbb{P}^1$ (Class 43 Exercise 1.A). One of the branch points is $2p$: one of the sections of $\mathcal{O}_E(2p)$ vanishes to p of order 2, so there is a point of $\mathbb{P}^1$ consists of p (with multiplicity 2). Assume now that $k = \overline{k}$ and $\operatorname{char} k \neq 2$, so we can use the Riemann-Hurwitz formula. Then the Riemann-Hurwitz formula shows that E has 4 branch points (p and three others). Conversely, given 4 points in $\mathbb{P}^1$, there exists a unique double cover branched at those 4 points (Class 45, Claim 1.3). Thus elliptic curves correspond to 4 distinct points in $\mathbb{P}^1$, where one is marked p, up to automorphisms of $\mathbb{P}^1$. Equivalently, by placing p at ∞, elliptic curves correspond to 3 points in $\mathbb{A}^1$, up to affine maps $x \mapsto ax + b$.

1.A. EXERCISE. Show that the other three branch points are precisely the (non-identity) 2-torsion points in the group law. (Hint: if one of the points is q, show that $\mathcal{O}(2q) \cong \mathcal{O}(2p)$, but $\mathcal{O}(q)$ is not congruent to $\mathcal{O}(p)$.)

Thus (if the $\operatorname{char} k \neq 2$ and $k = \overline{k}$) every elliptic curve has precisely four 2-torsion points. If you are familiar with the complex picture $E \cong \mathbb{C}/\Lambda$, this isn't surprising.

Follow-up remark. An elliptic curve with *full level* n*-structure* is an elliptic curve with an isomorphism of its n-torsion points with $(\mathbb{Z}/n)^2$. (This notion will have problems if n is divisible by $\operatorname{char} k$.) Thus an elliptic curve with *full level 2 structure* is the same thing as an elliptic curve with an ordering of the three other branch points in its degree 2 cover description. Thus (if $k = \overline{k}$) these objects are parametrized by the λ-line.

Follow-up to the follow-up. There is a notion of moduli spaces of elliptic curves with full level n structure. Such moduli spaces are smooth curves (where this is interpreted appropriately), and have smooth compactifications. A *weight* k *level* n *modular form* is a section of $\mathcal{K}^{\otimes k}$ where $\mathcal{K}$ is the canonical sheaf of this "modular curve".

1.5. *The cross-ratio and the* j*-invariant.* If the three other points are temporarily labeled q_1, q_2, q_3, there is a unique automorphism of $\mathbb{P}^1$ taking p, q_1, q_2 to $(\infty, 0, 1)$ respectively (as $\operatorname{Aut} \mathbb{P}^1$ is three-transitive). Suppose that q_3 is taken to some number λ under this map, where necessarily $\lambda \neq 0, 1, \infty$.

The value λ is called the **cross-ratio** of the four-points (p, q_1, q_2, q_3) of $\mathbb{P}^1$, first defined by Pascal in 1640.

1.B. EXERCISE. Show that isomorphism class of four ordered distinct points on $\mathbb{P}^1$, up to projective equivalence (automorphisms of $\mathbb{P}^1$), are classified by the cross-ratio.

We have not defined the notion of *moduli space*, but the previous exercise illustrates the fact that $\mathbb{P}^1 - \{0, 1, \infty\}$ (the image of the cross-ratio map) is the moduli space for four ordered distinct points of $\mathbb{P}^1$ up to projective equivalence.

Notice:

- If we had instead sent p, q_2, q_1 to $(\infty, 0, 1)$, then q_3 would have been sent to $1 - \lambda$.
- If we had instead sent p, q_1, q_3 to $(\infty, 0, 1)$, then q_2 would have been sent to $1/\lambda$.
- If we had instead sent p, q_3, q_1 to $(\infty, 0, 1)$, then q_2 would have been sent to $1 - 1/\lambda = (\lambda - 1)/\lambda$.
- If we had instead sent p, q_2, q_3 to $(\infty, 0, 1)$, then q_2 would have been sent to $1/(1 - \lambda)$.
- If we had instead sent p, q_3, q_2 to $(\infty, 0, 1)$, then q_2 would have been sent to $1 - 1/(1 - \lambda) = \lambda/(\lambda - 1)$.

Thus these six values (which correspond to S_3) yield the same elliptic curve, and this elliptic curve will (upon choosing an ordering of the other 3 branch points) yield one of these six values.

Thus the elliptic curves over k corresponds to k-valued points of $\mathbb{P}^1 - \{0, 1, \lambda\}$, modulo the action of S_3 on λ given above. Consider the subfield of $k(\lambda)$ fixed by S_3. By Lüroth's theorem (see the discussion of Curves of Genus 0), it must be of the form $k(j)$ for some $j \in k(\lambda)$. Note that λ should satisfy a sextic polynomial over $k(\lambda)$, as for each j-invariant, there are six values of λ in general.

Here is the formula for the j-invariant that everyone uses:

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}. \tag{1}$$

You can readily check that $j(\lambda) = j(1/\lambda) = \cdots$, and that as j has a degree 6 numerator and degree < 6 denominator, j indeeds determines a degree 6 map from $\mathbb{P}^1$ (with co-ordinate λ) to $\mathbb{P}^1$ (with co-ordinate j). But this complicated-looking formula begs the question: where did this formula come from? How did someone think of it? We'll largely answer this, but we'll ignore the 2^8 (which, as you might imagine, arises from characteristic 2 issues, and to get this discussion started using Riemann-Hurwitz, we have been assuming $\operatorname{char} k \neq 2$).

Rather than using the formula handed to us, let's try to guess what j is. We won't necessarily expect to get the same formula as (1), but our answer will differ by an automorphism of the j-line ($\mathbb{P}^1$), i.e. we'll get $j' = (aj + b)/(cj + d)$ for some a, b, c, d.

We are looking for some $j(\lambda)$ such that $j(\lambda) = j(1/\lambda) = \cdots$. Hence we want some expression in λ that is invariant under this S_3-action. A first possibility would be to take the product of the six numbers

$$\lambda \cdot (1 - \lambda) \cdot \frac{1}{\lambda} \cdot \frac{\lambda - 1}{\lambda} \cdot \frac{1}{1 - \lambda} \cdot \frac{\lambda}{\lambda - 1}$$

This is silly, as the product is obviously 1.

A better idea is to add them all together:

$$\lambda + (1 - \lambda) + \frac{1}{\lambda} + \frac{\lambda - 1}{\lambda} + \frac{1}{1 - \lambda} + \frac{\lambda}{\lambda - 1}$$

This also doesn't work, as they add to 3 (the six terms come in pairs adding to 1).

But you'll undoubtedly have another idea immediately. One good idea is to take the second symmetric function in the six roots. An equivalent one that is easier to do by hand is to add up the squares of the six terms. Even before doing the calculation, we can see that this will work: it will clearly produce a fraction whose numerator and denominator have degree at most 6, and it is not constant, as when λ is some fixed small number (say $1/2$), the sum of squares is some small real number, while when λ is a large real number, the sum of squares will have to be some large real number (different from the value when $\lambda = 1/2$).

When you add up the squares by hand (which isn't hard), you will get

$$j' = \frac{2\lambda^6 - 6\lambda^5 + 9\lambda^4 - 8\lambda^3 + 9\lambda^2 - 6\lambda + 2}{\lambda^2(\lambda - 1)^2}.$$

Indeed $k(j) \cong k(j')$: you can check (again by hand) that

$$2j/2^8 = \frac{2\lambda^6 - 6\lambda^5 + 12\lambda^4 - 14\lambda^3 + 12\lambda^2 - 6\lambda + 2}{\lambda^2(\lambda-1)^2}.$$

Thus $2j/2^8 - j' = 3$.

1.6. Line bundles of degree 3.

In the last section 1.4, we assumed k was algebraically closed, and $\operatorname{char} k \neq 2$, in order to invoke the Riemann-Hurwitz formula. In this section, we'll start with no assumptions, and add them as we need them. In this way, you'll see what partial results hold with weaker assumptions.

Consider the degree 3 invertible sheaf $\mathcal{O}_E(3p)$. By Riemann-Roch in high degree, $h^0(E, \mathcal{O}_E(3p)) = \deg(3p) - g + 1 = 3$. As $\deg E > 2g$, this gives a closed immersion. Thus we have a closed immersion $E \hookrightarrow \mathbb{P}^2_k$ as a cubic curve. Moreover, there is a line in $\mathbb{P}^2_k$ meeting E at point p with multiplicity 3, corresponding to the section of $\mathcal{O}(3p)$ vanishing precisely at p with multiplicity 3. (A line in the plane meeting a smooth curve with multiplicity at least 2 is said to be a **tangent line**. A line in the plane meeting a smooth curve with multiplicity at least 3 is said to be a **flex line**.)

Choose projective coordinates on $\mathbb{P}^2_k$ so that p maps to $[0;1;0]$, and the flex line is the line at infinity $z = 0$. Then the cubic is of the following form:

$$\begin{array}{ccccccccccc}
?x^3 & + & 0x^2y & + & 0xy^2 & + & 0y^3 & & & & \\
+ & ?x^2z & + & ?xyz & + & ?y^2z & & & & & \\
 & + & ?xz^2 & + & ?yz^2 & & & & & & \\
 & & + & ?z^3 & & & & & & & = 0
\end{array}$$

The co-efficient of x is not 0 (or else this cubic is divisible by z). Dividing the entire equation by this co-efficient, we can assume that the coefficient of x^3 is 1. The coefficient of y^2z is not 0 either (or else this cubic is singular at $x = z = 0$). We can scale z (i.e. replace z by a suitable multiple) so that the coefficient of y^2z is 1. If the characteristic of k is not 2, then we can then replace y by $y + ?x + ?z$ so that the coefficients of xyz and yz^2 are 0, and if the characteristic of k is not 3, we can replace x by $x + ?z$ so that the coefficient of x^2z is also 0. In conclusion, if $\operatorname{char} k \neq 2, 3$, the elliptic curve may be written

$$y^2z = x^3 + ax^2z + bz^3. \tag{2}$$

This is called **Weierstrass normal form.**

We see the hyperelliptic description of the curve (by setting $z = 1$, or more precisely, by working in the distinguished open set $z \neq 0$ and using inhomogeneous coordinates). In particular, we can compute the j-invariant.

1.C. EXERCISE. Compute the j-invariant of the curve (2) in terms of a and b. (I'm not sure how messy this is.)

Here is the geometric explanation of why the double cover description is visible in the cubic description.

I drew a picture of the projective plane, showing the cubic, and where it met the z-axis (the line at infinity) — where the z-axis and x-axis meet — it has a flex there. I drew the lines through that point — vertical lines. Equivalently, you're just taking 2 of the 3 sections: x and z. These are two sections of $\mathcal{O}(3p)$, but they have a common zero — a base point at p. So you really get two sections of $\mathcal{O}(2p)$.

1.D. EXERCISE. Show that the flexes of the cubic are the 3-torsion points in the group E. (In fact, if k is algebraically closed and $\operatorname{char} k \neq 3$, there are nine of them. This won't be surprising if you are familiar with the complex story, $E = \mathbb{C}/\Lambda$.)

1.7. Elliptic curves are group varieties.

So far, we know little about the structure of the the group law on the (closed) points of an elliptic curve. For example, for all we know (so far), the group operations (addition, inverse) may be horribly discontinuous on a complex elliptic curve. But this is happily not the case: the morphisms are even algebraic. We can get this rather cheaply using what we already know. Let's start with the inverse.

1.8. *Proposition. — There is a morphism of varieties $E \to E$ sending a (degree 1) point to its inverse.*

In other words, the "inverse map" in the group law actually arises from a morphism of schemes — it isn't just a set map. This is another clue that $\operatorname{Pic}^0(E)$ really wants to be a scheme.

Proof. It is the hyperelliptic involution $y \mapsto -y$! Here is why: if q and r are "hyperelliptic conjugates", then $q + r = 2p = 0$ in the group law. $\square$

We can describe addition in the group law using the cubic description. (Here a picture is absolutely essential, and at some later date, I hope to add it.) To find the sum of q and r on the cubic, we draw the line through q and r, and call the third point it meets s. Then we draw the line between p and s, and call the third point it meets t. Then $q + r = t$. Here's why: $q + r + s = p + s + t$ gives $(q - p) + (r - p) = (s - p)$.

(When the group law is often defined on the cubic, this is how it is done. Then you have to show that this is indeed a group law, and in particular that it is associative. We don't need to do this — $\mathrm{Pic}^0 E$ is a group, so it is automatically associative.)

Note that this description works in all characteristics; we haven't required the cubic to be in Weierstrass normal form. Similarly, the description of the inverse map (stated correctly) also works in all characteristics.

1.9. *Proposition. — There is a morphism of varieties* $E \times E \to E$ *that on degree* 1 *points sends* (q, r) *to* $q + r$.

Proof. We have to show that there are algebraic formulas describing this construction on the cubic. This looks daunting, as you should expect the formulas to be hideous, and indeed they are. (And they are even worse if the characteristic is 2 or 3, and we have to work with something messier than the Weierstrass normal form.)

But we don't need to actually write down the formulas — we need only show they exist. We define a map $E \times E \to E$, where if the input is (a, b), the output is the third point where the cubic meets the line, with the natural extension if the line doesn't meet the curve at three distinct points. You should convince yourself that this can be done, without actually doing it. (Possible hint: if you know two of there roots of a cubic $x^3 + ax^2 + bx + c = 0$ are d and e, then you know the third is $-a - d - e$.) Then we can use this to construct addition on the cubic. This gives an algebraic map $E \times E \to E$, and by construction it agrees with our addition rule on closed points. $\square$

1.10. *Proposition. — The inverse and addition rules above give* E *the structure of an abelian group scheme (or group variety).*

Proof. We need to check that the addition and inverse satisfy the desired axioms of a group scheme. We'll do associativity as an example.

First assume that k is algebraically closed. Consider $a : E \times E \times E \to E$ given by

$$(q, r, s) \mapsto ((q + r) + s) - (q + (r + s))$$

(i.e. this morphism is obtained by using the addition and inverse morphisms in this way). Then this map sends all closed points to the identity. Since the degree 1 (= closed) points are dense, and E is reduced, this means that the map is the constant map (with image the identity, p).

For the case of general k, base change to the algebraic closure. Then if a is the morphism of the above paragraph, $a \otimes_k \overline{k}$ is the constant map with image p, so a is too. $\square$

1.11. *Features of this construction.* The most common derivation of the properties of an elliptic curve are to describe it as a cubic, and describe addition using the explicit construction with lines. Then one has to work hard to prove that the multiplication described is associative.

Instead, we started with something that was patently a group (the degree 0 line bundles). We interpreted the maps used in the definition of the group (addition and inverse) geometrically using our cubic interpretation of elliptic curves. This allowed us to see that these maps were algebraic. We managed to avoid doing any messy algebra.

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

FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 48

RAVI VAKIL

CONTENTS

1. A LITTLE MORE ABOUT CUBIC PLANE CURVES

1.A. IMPORTANT EXERCISE: A DEGENERATE ELLIPTIC CURVE. Consider the genus 1 curve $C \subset \mathbb{P}^2_k$ given by $y^2 z = x^3 + x^2 z$, with the point $p = [0;1;0]$. Emulate the above argument to show that $C - [0;0;1]$ is a group variety. Show that it is isomorphic to $\mathbb{G}_m$ (the multiplicative group) with co-ordinate $t = y/x$, by showing an isomorphism of schemes, and showing that multiplication and inverse in both group varieties agree under this isomorphism.

1.B. EXERCISE: AN EVEN MORE DEGENERATE ELLIPTIC CURVE. Consider the genus 1 curve $C \subset \mathbb{P}^2_k$ given by $y^2 z = x^3$, with the point $p = [0;1;0]$. Emulate the above argument to show that $C - [0;0;1]$ is a group variety. Show that it is isomorphic to $\mathbb{A}^1$ (with additive group structure) with co-ordinate $t = y/x$, by showing an isomorphism of schemes, and showing that multiplication/addition and inverse in both group varieties agree under this isomorphism.

I then gave proofs of Pappas' Theorem and Pascal's "Mystical Hexagon" theorem.

2. LINE BUNDLES OF DEGREE 4, AND PONCELET'S PORISM

The story doesn't stop in degree 3. In the same way that we showed that a canonically embedded nonhyperelliptic curve of genus 4 is the complete intersection in $\mathbb{P}^3_k$ of a quadric and a cubic, we can show the following.

2.A. EXERCISE. Show that the complete linear system for $\mathcal{O}(4p)$ embeds E in $\mathbb{P}^3$ as the complete intersection of two quadrics. (Hint: Show the image of E is contained in at least

Date: Thursday, April 24, 2008.

2 linearly independent quadrics. Show that neither can be reducible, so they share no components. Use Bezout's theorem.)

We can use this to prove a beautiful fact in classical geometry: Poncelet's porism. Suppose C and D are two ellipses in the real plane, with C containing D. Choose any point p_0 on C. Choose one of the two tangents ℓ_1 from p to D. Then ℓ_1 meets C at two points in total: p_0 and another points p_1. From p_1, there are two tangents to D, ℓ_1 and another line ℓ_2. The line ℓ_2 meets C at some other point p_2. Continue this to get a sequence of points $p_0, p_1, p_2, \dots$. Suppose this sequence starting with p_0 is periodic, i.e. $p_0 = p_n$ for some n. Then it is periodic with *any* starting point $p \in C$. I drew a picture of this.

Let's see what this has to do with elliptic curves. We work over the complex numbers and at the end consider what our results over the real numbers. For the rest of this discussion, we assume that k is an algebraically closed field of characteristic not 2.

2.B. EXERCISE. Suppose D is a nonsingular conic in the plane $\mathbb{P}^2_k$. Suppose p is a point on the plane not on D. Then there are precisely 2 tangents to D containing p.

Thus we have verified one of the implicit statements in the set-up for Poncelet's porism.

Next, suppose Q is a nonsingular quadric in $\mathbb{P}^3$, and q is a point not on Q. Then the projection from q to $\mathbb{P}^2$ describes Q as a branched double-cover of $\mathbb{P}^2$. We should be explicit about what we mean about "branching": the lines through q correspond to the (closed) points of $\mathbb{P}^2$. Most lines meet Q in 2 points. The branch points in $\mathbb{P}^2$ correspond to those that meet Q in only one point (with multiplicity 2 of course).

2.C. EXERCISE. Show that this double cover is branched over a nonsingular conic D in $\mathbb{P}^2$. (If it helps, choose explicit co-ordinates.)

Side remark: we have stated earlier that $\mathrm{Pic}(\mathbb{P}^2 - D) \cong \mathbb{Z}/2$, and that this was related to the fact that (over the complex numbers) $\pi_1(\mathbb{P}^2 - C) = \mathbb{Z}/2$. This latter fact implies that the universal cover of $\mathbb{P}^2 - C$ is a double cover. We have now produced the double cover: the quadric Q minus the branch divisor. We can even use this to prove that $\pi_1(\mathbb{P}^2 - C) = \mathbb{Z}/2$: please ask me for the short argument.

Since Q is a nonsingular quadric over an algebraically closed field of characteristic not 2, $Q \cong \mathbb{P}^1 \times \mathbb{P}^1$, and has two rulings. What are the images of the lines in each ruling in $\mathbb{P}^2$? Suppose ℓ is a line in $\mathbb{P}^2$. Then the preimage of ℓ in $\mathbb{P}^3$ is a plane Π in $\mathbb{P}^3$ containing q. Q meets this plane Π in a conic.

If this conic $Q \cap \Pi$ is nonsingular, then we are precisely in the situation of Exercise 2.B, and this may help you see that the degree of the branch curve is 2 (Exercise 2.C). Also, since $Q \cap \Pi$ is not singular at any point (i.e. the germ of the equation of $Q \cap P$ at any point r is not contained in the square of the maximal ideal at r), $Q \cap \Pi$ is not a tangent plane to Q.

On the other hand, if $Q \cap \Pi$ is singular, then Π is a tangent plane to Q. And this singular conic is the union of two lines. (Why can't it be a double line?) Thus the two lines consist of one of each ruling.

Conversely, if l is a line in a ruling on Q, then the plane Π spanned by l and q must be tangent to Q: the conic $\Pi \cap Q$ contains a line and is thus singular.

We thus conclude that the image of any line on Q is a tangent line to D, and conversely the preimage of each tangent line on D is two lines on Q, one from each ruling.

We have recovered part of the picture of Poncelet: we have a nonsingular conic D in the plane. Let $C \subset \mathbb{P}^2$ be another conic in the plane, not tangent to D. Let $G \subset \mathbb{P}^3$ be the quadric surface that is the cone over C with vertex q. (Can you make this precise?)

2.D. EXERCISE. Show that $G \cap C$ is a nonsingular curve.

The complete intersection E of two quadric surfaces in $\mathbb{P}^3$ has genus 1. Choose any point of it, so E have an elliptic curve. By considering E as a subset of $Q \cong \mathbb{P}^1 \times \mathbb{P}^1$, we have two maps $E \to \mathbb{P}^1$, one corresponding to each factor. Both are degree 2. Let D_1 and D_2 be the two degree 2 divisors corresponding to these two double covers. If p'_0 is a point of E, each ruling through p'_0 meets E at one other point: the point $D_1 - p$ for the first ruling, and the point $D_2 - p$ for the second ruling. The image of p'_0, the two lines, and $D_1 - p$ and $D_2 - p$ in the plane is a point p_0 in the plane, the two tangents to D from p_0, and the two points on C also on those two tangents.

Thus if we start at p'_0, choose the other point of E on the line in the first ruling to obtain $p'_1 = D_1 - p_0$, and then choose the other point of E through p'_1 on a line in the second ruling, we obtain the point $p'_2 = D_2 - p'_1 = p'_0 + (D_2 - D_1)$: a translation of p'_0 by an amount independent of p'_0. Thus $p'_{2n} = p'_0 + n(D_2 - D_1)$. In particular, if $p'_{2n} = p'_0$ for one choice of p'_0, then this would still hold for *any* choice of p'_0.

2.E. EXERCISE. Put the above pieces together to prove Poncelet's porism.

3. FUN COUNTEREXAMPLES USING ELLIPTIC CURVES

We now give some fun counterexamples using our understanding of elliptic curves.

3.1. An example of a scheme that is locally factorial near a point p, but such that no affine open neighborhood of p has ring that is a Unique Factorization Domain.

Suppose E is an elliptic curve over $\mathbb{C}$ (or some other uncountable field). Consider $p \in E$. The local ring $\mathcal{O}_{E,p}$ is a Discrete Valuation Ring and hence a Unique Factorization Domain. Then an open neighborhood of E is of the form $E - q_1 - \cdots - q_n$. I claim that its Picard group is nontrivial. Recall the exact sequence:

$$\mathbb{Z}^n \xrightarrow{(a_1,\dots,a_n)\mapsto a_1 q_1+\cdots+a_n q_n} \operatorname{Pic} E \longrightarrow \operatorname{Pic}(E - q_1 - \cdots - q_n) \longrightarrow 0\ .$$

But the group on the left is countable, and the group in the middle is uncountable, so the group on the right is non-zero.

3.2. Counterexamples using the existence of a non-torsion point.

We next give a number of counterexamples using the existence of a non-torsion point of a complex elliptic curve. We show the existence of such a point.

We have a "multiplication by n" map $[n] : E \to E$, which sends p to np. If $n = 0$, this has degree 0. If $n = 1$, it has degree 1. Given the complex picture of a torus, you might not be surprised that the degree of $\times n$ is n^2. If $n = 2$, we have almost shown that it has degree 4, as we have checked that there are precisely 4 points q such that $2p = 2q$. All that really shows is that the degree is at least 4. (We could check by hand that the degree is 4 is we really wanted to.)

3.3. *Proposition. — For each $n > 0$, the "multiplication by n" map has positive degree. In other words, there are only a finite number of n torsion points, and the $[n] \neq [0]$.*

Proof. We prove the result by induction; it is true for $n = 1$ and $n = 2$.

If n is odd, then assume otherwise that $nq = 0$ for all closed points q. Let r be a non-trivial 2-torsion point, so $2r = 0$. But $nr = 0$ as well, so $r = (n-2[n/2])r = 0$, contradicting $r \neq 0$.

If n is even, then $[\times n] = [\times 2] \circ [\times(n/2)]$, and by our inductive hypothesis both $[\times 2]$ and $[\times(n/2)]$ have positive degree. □

In particular, the total number of torsion points on E is countable, so if k is an uncountable field, then E has an uncountable number of closed points (consider an open subset of the curve as $y^2 = x^3 + ax + b$; there are uncountably many choices for x, and each of them has 1 or 2 choices for y).

Thus *almost all* points on E are non-torsion. I'll use this to show you some pathologies.

3.4. An example of an affine open set that is not distinguished.

We can use this to see another example of an affine scheme X and an affine open subset Y that is not distinguished in X. (Our earlier example was $X = \mathbb{P}^2$ minus a conic, and $Y = X$ minus a line.) Let $X = E - p$, which is affine (easy, and an earlier exercise).

Let q be another point on E so that $q - p$ is non-torsion. Then $E - p - q$ is affine (we've shown all nonprojective nonsingular curves are affine). Assume that it is distinguished. Then there is a function f on $E - p$ that vanishes on q (to some positive order d). Thus

f is a rational function on E that vanishes at q to order d, and (as the total number of zeros minus poles of f is 0) has a pole at p of order d. But then $d(p-q) = 0$ in $\operatorname{Pic}^0 E$, contradicting our assumption that $p - q$ is non-torsion.

3.5. Example of variety with non-finitely-generated space of global sections.

We next show an example of a complex variety whose ring of global sections is not finitely generated. This is related to Hilbert's fourteenth problem, although I won't say how.

We begin with a preliminary exercise.

3.A. EXERCISE. Suppose X is a scheme, and L is the total space of a line bundle corresponding to invertible sheaf $\mathcal{L}$, so $L = \operatorname{Spec} \oplus_{n \geq 0} (\mathcal{L}^\vee)^{\otimes n}$. Show that $H^0(L, \mathcal{O}_L) = \oplus H^0(X, (\mathcal{L}^\vee)^{\otimes n})$.

Let E be an elliptic curve over some ground field k, N a degree 0 non-torsion invertible sheaf on E, and P a positive-degree invertible sheaf on E. Then $H^0(E, N^m \otimes P^n)$ is nonzero if and only if either (i) $n > 0$, or (ii) $m = n = 0$ (in which case the sections are elements of k). Thus the ring $R = \oplus_{m,n \geq 0} H^0(E, N^m \otimes P^n)$ is not finitely generated.

Now let X be the total space of the vector bundle $N \oplus P$ over E. Then the ring of global sections of X is R.

3.6. A proper nonprojective surface.

We finally sketch an example of a proper surface S over $\mathbb{C}$ that is not projective. We will see that the construction will work over uncountable fields, and (modulo an fact unproved here) $\mathbb{Q}$. We will construct it as a "fibration" $f : S \to C$ where C is a projective curve, and f is "locally projective", by which I mean that there is an open cover of C such that over each open set, f is projective. In particular, we will show that projectivity in the sense it is usually defined (without the data of a line bundle on the source, as we define it) is not a Zariski-local property.

As a result, we'll see some other interesting behavior, about the difficulty of gluing a scheme to itself (not typed up in the notes).

This is the simplest example I know. There are no examples of curves, as all proper curves are projective. This example is singular; in fact all proper nonsingular surfaces are projective.

Let C be two $\mathbb{P}^1$'s (C_1 and C_2) glued together at two points p and q, as shown in Figure 1. For example, consider a general conic union a line in $\mathbb{P}^2$. Clearly C is projective (over $\mathbb{C}$).

Let E be any complex elliptic curve, and r a non-torsion point on it. We construct an "E-bundle" over C as follows. over $C - p$, the family is trivial: $E \times (C - p)$. Similarly, over

$C - q$, the family is trivial. We glue these families together via the identity over C_1, and via translation by r over C_2. Call the resulting fibration $f : S \to C$.

Now E is proper, so f is proper over $C - p$ and $C - q$, and hence (by Zariski-locality of properness) f is a proper morphism. As C is proper, and properness is preserved by composition, S is a proper surface.

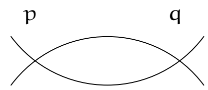

FIGURE 1. The $\mathbb{P}^1$'s glued together at two points

Suppose that S were projective, and that there was a closed immersion $S \to \mathbb{P}^n$ into projective space. Choose a hyperplane not containing the fiber of f over either p or q. This gives an effective Cartier divisor on S. Perhaps this effective Cartier divisor contains some fibers; if so, subtract them, to get another effective Cartier divisor containing no fibers. (There is no issue with subtracting these fibers, as away from the fibers over p and q, S is smooth, so on this locus, effective Weil divisors and effective Cartier divisors are the same.)

We will show that this is impossible.

I'll finish typing this in when I get a chance...

All we needed to make this argument work was the existence of a non-torsion point. Thus this argument works over any uncountable field. It also works over $\mathbb{Q}$ once one verifies that there is an elliptic curve over $\mathbb{Q}$ with a non-torsion point. This is a good excuse to mention the *Mordell-Weil Theorem*: for any elliptic curve E over $\mathbb{Q}$, the $\mathbb{Q}$-points of E form a *finitely generated* abelian group. By the classification of finitely generated abelian groups, the $\mathbb{Q}$-points are a direct sum of a torsion part, and of a free $\mathbb{Z}$-module. The rank of the $\mathbb{Z}$-module is called the *Mordell-Weil rank*. Thus this construction works once we have verified that there is an elliptic curve with positive Mordell-Weil rank.

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

FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 50

RAVI VAKIL

CONTENTS

1. DIFFERENTIALS: MOTIVATION AND GAME PLAN

Differentials are an intuitive geometric notion, and we're going to figure out the right description of them algebraically. I find the algebraic manifestation a little non-intuitive, so I always like to tie it to the geometry. So please don't tune out of the statements. Also, I want you to notice that although the algebraic statements are odd, none of the proofs are hard or long. You'll notice that this topic could have been done as soon as we knew about morphisms and quasicoherent sheaves.

I prefer to introduce new ideas with a number of examples, but in this case I'm going to spend a fair amount of time discussing theory, and only then get to a number of examples.

Suppose X is a "smooth" k-variety. We intend to define a tangent bundle. We'll see that the right way to do this will easily apply in much more general circumstances.

• We'll see that cotangent is more "natural" for schemes than tangent bundle. This is similar to the fact that the Zariski *cotangent* space is more natural than the *tangent space* (i.e. if A is a ring and $\mathfrak{m}$ is a maximal ideal, then $\mathfrak{m}/\mathfrak{m}^2$ is "more natural" than $(\mathfrak{m}/\mathfrak{m}^2)^\vee$). Both of these notions are because we are understanding "spaces" via their (sheaf of) functions on them, which is somehow dual to the geometric pictures you have of spaces in your mind.

So we'll define the cotangent sheaf first. An element of the (co)tangent space will be called a **(co)tangent vector**.

• Our construction will automatically apply for general X, even if X is not "smooth" (or even at all nice, e.g. finite type). The cotangent sheaf won't be locally free, but it will still be a quasicoherent sheaf.

• Better yet, this construction will naturally work "relatively". For *any* $X \to Y$, we'll define $\Omega_{X/Y}$, a quasicoherent sheaf on X, the sheaf of *relative differentials*. The fiber of this sheaf

Date: Thursday, May 1, 2008.

at a point will be the cotangent vectors of the fiber of the map. This will specialize to the earlier case by taking $Y = \operatorname{Spec} k$. The idea is that this glues together the cotangent sheaves of the fibers of the family. Figure 1 is a sketch of the relative tangent space of a map $X \to Y$ at a point $p \in X$ — it is the tangent to the fiber. (The tangent space is easier to draw than the cotangent space!) An element of the relative (co)tangent space is called a **vertical** or **relative (co)tangent vector**.

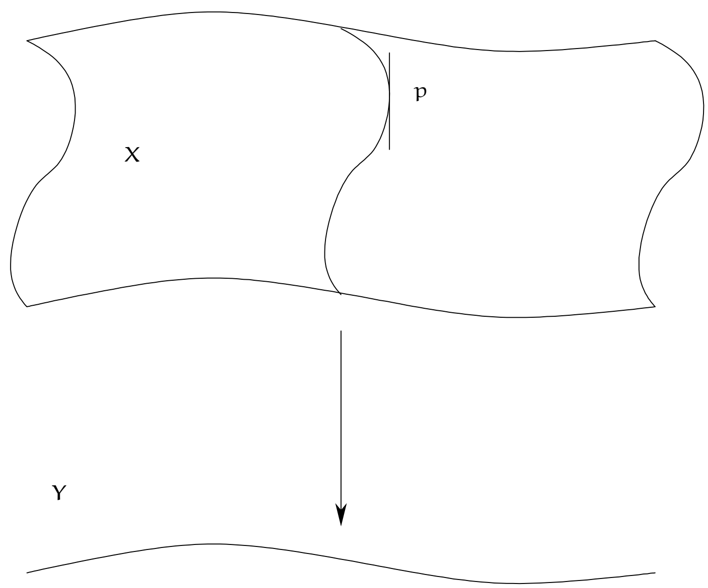

FIGURE 1. The relative tangent space of a morphism $X \to Y$ at a point p

2. THE AFFINE CASE: TWO OF THREE DEFINITIONS

We'll first study the affine case. Suppose A is a B-algebra, so we have a morphism of rings $\phi : B \to A$ and a morphism of schemes $\operatorname{Spec} A \to \operatorname{Spec} B$. I will define an A-module $\Omega_{A/B}$ in three ways. This is called the **module of relative differentials** or the **module of Kähler differentials**. The module of differentials will be defined to be this module, as well as a map $d : A \to \Omega_{A/B}$ satisfying three properties.

(i) **additivity.** $da + da' = d(a + a')$
(ii) **Leibniz.** $d(aa') = a\ da' + a'da$
(iii) **triviality on pullbacks.** $db = 0$ for $b \in \phi(B)$.

2.A. TRIVIAL EXERCISE. Show that d is B-linear. (In general it will not be A-linear.)

2.B. EXERCISE. Prove the quotient rule: if $b = as$, then $da = (s\ db - b\ ds)/s^2$.

2.C. EXERCISE. State and prove the chain rule for $d(f(g))$ where f is a polynomial with B-coefficients, and $g \in A$. (As motivation, think of the case $B = k$. So for example, $da^n = na^{n-1} da$, and more generally, if f is a polynomial in one variable, $df(a) = f'(a)\ da$, where f' is defined formally: if $f = \sum c_i x^i$ then $f' = \sum c_i i x^{i-1}$.)

I'll give you three definitions of the module of Kähler differentials, which will soon "sheafifiy" to the sheaf of relative differentials. The first definition is a concrete hands-on definition. The second is by universal property. And the third will globalize well, and will allow us to define $\Omega_{X/Y}$ conveniently in general.

2.1. First definition of differentials: explicit description. We define $\Omega_{A/B}$ to be finite A-linear combinations of symbols "da" for $a \in A$, subject to the three rules (i)–(iii) above. For example, take $A = k[x, y]$, $B = k$. Then a sample differential is $3x^2\ dy + 4\ dx \in \Omega_{A/B}$. We have identities such as $d(3xy^2) = 3y^2\ dx + 6xy\ dy$.

Key fact. Note that if A is generated over B (as an algebra) by $x_i \in A$ (where i lies in some index set, possibly infinite), subject to some relations r_j (where j lies in some index set, and each is a polynomial in the x_i), then the A-module $\Omega_{A/B}$ is generated by the dx_i, subject to the relations (i)—(iii) and $dr_j = 0$. In short, we needn't take every single element of A; we can take a generating set. And we needn't take every single relation among these generating elements; we can take generators of the relations.

2.D. EXERCISE. Verify the above key fact.

In particular:

2.2. *Proposition.* — *If A is a finitely generated B-algebra, then $\Omega_{A/B}$ is a finite type (=finitely generated) A-module. If A is a finitely presented B-algebra, then $\Omega_{A/B}$ is a finitely presented A-module.*

An algebra A is **finitely presented** over another algebra B if it can be expressed with finite number of generators (=finite type) and finite number of relations:

$$A = B[x_1, \dots, x_n]/(r_1(x_1, \dots, x_n), \dots, r_j(x_1, \dots, x_n)).$$

If A is Noetherian, then the two hypotheses are the same, so most of you will not care.)

Let's now see some examples. Among these examples are three particularly important kinds of ring maps that we often consider: adding free variables; localizing; and taking quotients. If we know how to deal with these, we know (at least in theory) how to deal with any ring map.

2.3. Example: taking a quotient. If $A = B/I$, then $\Omega_{A/B} = 0$ basically immediately: $da = 0$ for all $a \in A$, as each such a is the image of an element of B. This should be believable; in this case, there are no "vertical tangent vectors".

2.4. Example: adding variables. If $A = B[x_1, \dots, x_n]$, then $\Omega_{A/B} = A dx_1 \oplus \cdots \oplus A dx_n$. (Note that this argument applies even if we add an arbitrarily infinite number of indeterminates.) The intuitive geometry behind this makes the answer very reasonable. The cotangent bundle should indeed be trivial of rank n.

2.5. Example: two variables and one relation. If $B = \mathbb{C}$, and $A = \mathbb{C}[x, y]/(y^2 - x^3)$, then $\Omega_{A/B} = (A\ dx \oplus A\ dy)/(2y\ dy - 3x^2\ dx)$.

2.6. Example: localization. If S is a multiplicative set of B, and $A = S^{-1}B$, then $\Omega_{A/B} = 0$. Reason: the quotient rule holds, Exercise 2.B, so if $a = b/s$, then $da = (s\ db - b\ ds)/s^2 = 0$. If $A = B_f$ for example, this is intuitively believable; then $\operatorname{Spec} A$ is an open subset of $\operatorname{Spec} B$, so there should be no vertical (co)tangent vectors.

2.E. EXERCISE. Suppose k is a field, and K is a separable algebraic extension of k. Show that $\Omega_{K/k} = 0$. (Warning: do not assume that K/k is a finite extension!)

2.7. *Exercise (Jacobian description of $\Omega_{A/B}$).* — Suppose $A = B[x_1, \dots, x_n]/(f_1, \dots, f_r)$. Then $\Omega_{A/B} = \{\oplus_i A dx_i\}/\{df_j = 0\}$ maybe interpreted as the cokernel of the Jacobian matrix $J : A^{\oplus r} \to A^{\oplus n}$.

I now want to tell you two handy (geometrically motivated) exact sequences. The arguments are a bit tricky. They are useful, but a little less useful than the foundation facts above.

2.8. *Theorem (relative cotangent sequence, affine version).* — *Suppose $C \to B \to A$ are ring homomorphisms. Then there is a natural exact sequence of A-modules*

$$A \otimes_B \Omega_{B/C} \to \Omega_{A/C} \to \Omega_{A/B} \to 0.$$

The proof will be quite straightforward algebraically, but the statement comes fundamentally from geometry, and that is how I remember it. Figure 2 is a sketch of a map $X \xrightarrow{f} Y$. Here X should be interpreted as $\operatorname{Spec} A$, Y as $\operatorname{Spec} B$, and $\operatorname{Spec} C$ is a point. (If you would like a picture with a higher-dimensional $\operatorname{Spec} C$, just take the "product" of Figure 2 with a curve.) In the Figure, Y is "smooth", and X is "smooth over Y" — roughly, all fibers are smooth. p is a point of X. Then the tangent space of the fiber of f at p is certainly a subspace of the tangent space of the total space of X at p. The cokernel is naturally the pullback of the tangent space of Y at $f(p)$. This short exact sequence for each p should be part of a short exact sequence of sheaves

$$0 \to T_{X/Y} \to T_{X/Z} \to f^* T_{Y/Z} \to 0$$

on X Dualizing this yields

$$0 \to f^* \Omega_{Y/Z} \to \Omega_{X/Z} \to \Omega_{X/Y} \to 0.$$

This is precisely the statement of the Theorem, except we also have left-exactness. This discrepancy is because the statement of the theorem is more general; we'll may later see that in the "smooth" case, we'll indeed have left-exactness.

2.9. *Unimportant aside.* As always, whenever you see something right-exact, you should suspect that there should be some sort of (co)homology theory so that this is the end of a long exact sequence. This is indeed the case, and this exact sequence involves *André-Quillen homology*. You should expect that the next term to the left should be the first homology corresponding to A/B, and in particular shouldn't involve C. So if you already suspect that you have exactness on the left in the case where A/B and B/C are "smooth" (whatever that means), and the intuition of Figure 2 applies, then you should expect further that all that is necessary is that A/B be "smooth", and that this would imply that the first André-Quillen homology should be zero. Even though you wouldn't precisely know what all the words meant, you would be completely correct!

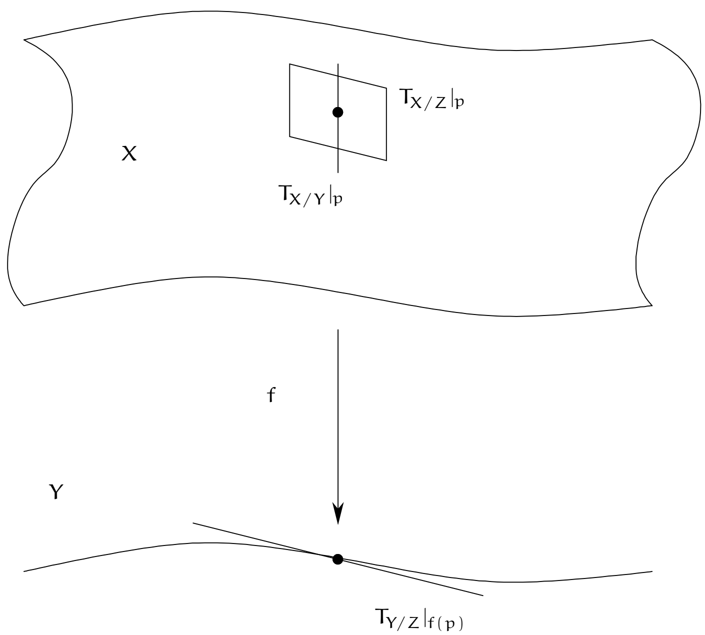

FIGURE 2. A sketch of the geometry behind the relative cotangent sequence

Proof of the relative cotangent sequence (affine version) 2.8.

First, note that surjectivity of $\Omega_{A/C} \to \Omega_{A/B}$ is clear, as this map is given by $da \mapsto da$ ($a \in A$).

Next, the composition over the middle term is clearly 0, as this composition is given by $db \to db \to 0$.

Finally, we wish to identify $\Omega_{A/B}$ as the cokernel of $A \otimes_B \Omega_{B/C} \to \Omega_{A/C}$. Now $\Omega_{A/B}$ is exactly the same as $\Omega_{A/C}$, except we have extra relations: $db = 0$ for $b \in B$. These are precisely the images of $1 \otimes db$ on the left. $\square$

2.10. *Theorem (conormal exact sequence, affine version). — Suppose* B *is a* C*-algebra,* I *is an ideal of* B*, and* $A = B/I$*. Then there is a natural exact sequence of* A*-modules*

$$I/I^2 \xrightarrow{\delta: i \mapsto 1 \otimes di} A \otimes_B \Omega_{B/C} \xrightarrow{a \otimes db \mapsto a\, db} \Omega_{A/C} \longrightarrow 0.$$

Before getting to the proof, some discussion may be helpful. First, the map δ needs to be rigorously defined. It is the map $1 \otimes d : B/I \otimes_B I \to B/I \otimes \Omega_{B/C}$.

As with the relative cotangent sequence, the conormal exact sequence is fundamentally about geometry. To motivate it, consider the sketch of Figure 3. In the sketch, everything is "smooth", X is one-dimensional, Y is two-dimensional, j is the inclusion $j : X \hookrightarrow Y$, and Z (omitted) is a point. Then at a point $p \in X$, the tangent space $T_X|_p$ clearly injects into the tangent space of $j(p)$ in Y, and the cokernel is the normal vector space to X in Y at p. This should give an exact sequence of bundles on X:

$$0 \to T_X \to j^* T_Y \to N_{X/Y} \to 0.$$

dualizing this should give

$$0 \to N_{X/Y}^{\vee} \to j^* \Omega_Y/Z \to \Omega_X/Z \to 0.$$

This is precisely what appears in the statement of the Theorem, except we see I/I^2 rather than $N^{\vee}_{\operatorname{Spec} A/\operatorname{Spec} B}$, and the exact sequence in algebraic geometry is not necessary exact on the left.

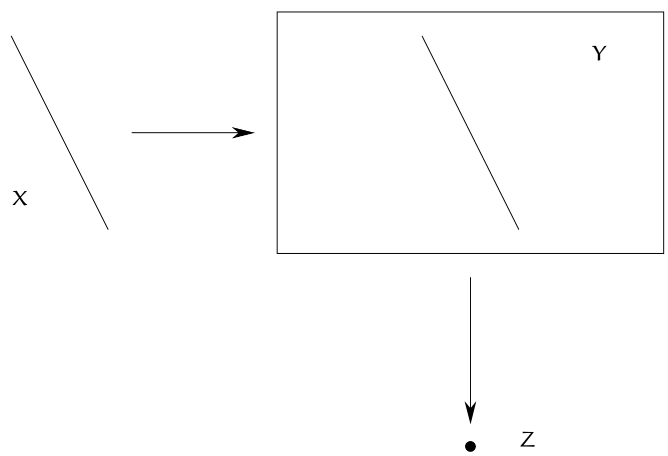

FIGURE 3. A sketch of the geometry behind the conormal exact sequence

2.11. We resolve the first issue by declaring I/I^2 to be the *conormal module*, and indeed we'll soon see the obvious analogue as the *conormal sheaf*. (Further evidence that I/I^2 deserves to be called the conormal bundle: if $\operatorname{Spec} A$ is a closed point of $\operatorname{Spec} B$, we expect the conormal space to be precisely the cotangent space. And indeed if $A = B/\mathfrak{m}$, the Zariski cotangent space is $\mathfrak{m}/\mathfrak{m}^2$.)

And we resolve the second by expecting that the seqeunce of Theorem 2.10 is exact on the left if X/Y and Y/Z (and hence X/Z) are "smooth" whatever that means. This is indeed the case. (If you enjoyed Remark 2.9, you might correctly guess several things. The next term on the left should be the André-Quillen homology of A/C, so we should only need that A/C is smooth, and B should be irrelevant. Also, if $A = B/I$, then we should expect that I/I^2 is the first André-Quillen homology of A/B.)

Proof of the conormal exact sequence (affine version) 2.10. We need to identify the cokernel of $\delta : I/I^2 \to A \otimes_B \Omega_{B/C}$ with $\Omega_{A/C}$. Consider $A \otimes_B \Omega_{B/C}$. As an A-module, it is generated by db ($b \in B$), subject to three relations: $dc = 0$ for $c \in \phi(C)$ (where $\phi : C \to B$ describes B as a C-algebra), additivity, and the Leibniz rule. Given any relation *in* B, d of that relation is 0.

Now $\Omega_{A/C}$ is defined similarly, except there are more relations *in* A; these are precisely the elements of $i \in B$. Thus we obtain $\Omega_{A/C}$ by starting out with $A \otimes_B \Omega_{B/C}$, and adding the additional relations di where $i \in I$. But this is precisely the image of δ! $\square$

2.12. Second definition: universal property. Here is a second definition that is important philosophically, by universal property. Technically, it isn't a definition: by universal property nonsense, it shows that if the module exists (with the d map), then it is unique up to unique isomorphism, and then one still has to construct it to make sure that it exists.

Suppose A is a B-algebra, and M is a A-module. An *B-linear derivation of A into M* is a map $d : A \to M$ of B-modules (*not necessarily A-modules*) satisfying the Leibniz rule: $d(fg) = f\ dg + g\ df$. As an example, suppose $B = k$, and $A = k[x]$, and $M = A$. Then an example of a k-linear derivation is d/dx. As a second example, if $B = k$, $A = k[x]$, and $M = k$. Then an example of a k-linear derivation is $d/dx|_0$.

Then $d : A \to \Omega_{A/B}$ is defined by the following universal property: any other B-linear derivation $d' : A \to M$ factors uniquely through d:

$$\begin{tikzcd} A \arrow[rr, "d'"] \arrow[dr, "d"'] & & M \\ & \Omega_{A/B} \arrow[ur, "f"'] & \end{tikzcd}$$

Here f is a map of A-modules. (Note again that d and d' are not! They are only B-linear.) By universal property nonsense, if it exists, it is unique up to unique isomorphism. The candidate I described earlier clearly satisfies this universal property (in particular, it is a derivation!), hence this is it. [Thus Ω is the "unversal derivation". I should rewrite this paragraph at some point. Justin points out: the map defined earlier is a derivation, but I never really say that; thus the original map, together with Ω, is a universal derivation.]

The next result will give you more evidence that this deserves to be called the (relative) cotangent bundle.

2.13. *Proposition.* *Suppose* B *is a* k*-algebra, with residue field* k*. Then the natural map* $\delta : \mathfrak{m}/\mathfrak{m}^2 \to \Omega_{B/k} \otimes_B k$ *is an isomorphism.*

Proof. By the conormal exact sequence 2.10 with $I = \mathfrak{m}$ and $A = C = k$, δ is a surjection (as $\Omega_{k/k} = 0$), so we need to show that it is injection, or equivalently that $\mathrm{Hom}_k(\Omega_{B/k} \otimes_B k, k) \to \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k)$ is a surjection. But any element on the right is indeed a derivation from B to k (an earlier exercise from back in the dark ages on the Zariski tangent space), which is precisely an element of $\mathrm{Hom}_B(\Omega_{B/k}, k)$ (by the universal property of $\Omega_{B/k}$), which is canonically isomorphic to $\mathrm{Hom}_k(\Omega_{B/k} \otimes_B k, k)$ as desired. $\square$

Remark. As a corollary, this (in combination with the Jacobian exercise 2.7 above) gives a second proof of an exercise from the first quarter, showing the Jacobian criterion for nonsingular varieties over an algebraically closed field.

Depending on how your brain works, you may prefer using the first (constructive) or second (universal property) definition to do the next two exercises.

2.F. EXERCISE. (a) *(pullback of differentials)* If

$$\begin{tikzcd} A' & A \arrow[l] \\ B' \arrow[u] & B \arrow[l] \arrow[u] \end{tikzcd}$$

is a commutative diagram, show that there is a natural homomorphism of A'-modules $A' \otimes_A \Omega_{A/B} \to \Omega_{A'/B'}$. An important special case is $B = B'$.
(b) *(differentials behave well with respect to base extension, affine case)* If furthermore the above diagram is a tensor diagram (i.e. $A' \cong B' \otimes_B A$) then show that $A' \otimes_A \Omega_{A/B} \to \Omega_{A'/B'}$ is an isomorphism.

2.G. EXERCISE: LOCALIZATION (STRONGER FORM). If S is a multiplicative set of A, show that there is a natural isomorphism $\Omega_{S^{-1}A/B} \cong S^{-1}\Omega_{A/B}$. (Again, this should be believable from the intuitive picture of "vertical cotangent vectors".) If T is a multiplicative set of B, show that there is a natural isomorphism $\Omega_{S^{-1}A/T^{-1}B} \cong S^{-1}\Omega_{A/B}$ where S is the multiplicative set of A that is the image of the multiplicative set $T \subset B$. [Ziyu used the relative cotangent sequence.]

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