FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 36

RAVI VAKIL

CONTENTS

Last day: More fun with curves: hyperelliptic curves; curves of genus at least 2; elliptic curves take 1.

Today: elliptic curves; the Picard variety; "the moduli space of curves has dimension $3g - 3$."

This is the last class of the quarter! We'll finish off using what we know (and a little of what we'll know soon) to learn a great deal about curves.

There will be one more homework out early next week, due Thursday of the week after, covering this week's notes. We may well have a question-and-answer question on the last morning of class.

Once again, I'm going to use those important facts that we proved a couple of days ago, so I'll refer you to the class 34 crib sheet.

Let me first give you an exercise I should have given you last day.

Exercise. (a) Suppose C is a projective curve. Show that $C - p$ is affine. (Hint: show that $n \gg 0$, $\mathcal{O}(np)$ gives an embedding of C into some projective space $\mathbb{P}^m$, and that there is some hyperplane H meeting C precisely at p. Then $C - p$ is a closed subscheme of $\mathbb{P}^n - H$.) (b) If C is a geometrically integral nonsingular curve over a field k (i.e. all of our standing assumptions, minus projectivity), show that it is projective or affine.

Date: Thursday, March 2, 2006. Minor update January 30, 2007.

We're in the process of studying elliptic curves, i.e. curves E (projective, geometrically integral and nonsingular, over a field k) of genus 1, with a choice of a k-valued point p. (It is typical to use the letter E for the curve rather than C.)

So far we have seen that they admit double covers of $\mathbb{P}^1$, and that if $k = \overline{k}$, then the elliptic curves are classified by the j-invariant. The double cover corresponded to the invertible sheaf $\mathcal{O}_E(2p)$. We'll now consider $\mathcal{O}_E(np)$ for larger n.

1.1. **Degree 3.** Consider the degree 3 invertible sheaf $\mathcal{O}_E(3p)$. We consult our useful facts. By Riemann-Roch, $h^0(E, \mathcal{O}_E(3p)) = \deg(3p) - g + 1 = 3$. 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. (Remark: 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*.)

We can 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). We can scale x so that the coefficient of x^3 is 1. The coefficient of y^2z is not 0 either (or else this cubic is singular at $x = z = 0$). As k is algebraically closed, we can scale y so that the coefficient of y^2z is 1. (More precisely, we are changing variables, say $y' = ay$ for some $a \in k$.) 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 k is algebraically closed of characteristic not 2 or 3, we can write our elliptic curve in the form

$$y^2z = x^3 + ax^2z + bz^3.$$

This is called *Weierstrass normal form.* (If only some of the "bonus hypotheses" $k = \overline{k}$, $\operatorname{char} k \neq 2, 3$ is true, then we can perform only some of the reductions of course.)

Notice that 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.

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 $\mathcal{O}(2p)$.

Exercise. Show that $\mathcal{O}(4p)$ embeds E in $\mathbb{P}^3$ as the complete intersection of two quadrics.

1.2. The group law.

1.3. *Theorem. — The closed points of* E *are in natural bijection with* $\operatorname{Pic}^0(E)$*, via* $x \leftrightarrow x - p$*. In particular, as* $\operatorname{Pic}^0(E)$ *is a group, we have endowed the closed points of* E *with a group structure.*

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.

Proof. For injectivity: $\mathcal{O}(x-p) \cong \mathcal{O}(y-p)$ implies $\mathcal{O}(x-y) \cong \mathcal{O}$. But as E is not genus 0, this is possible only if $x = y$.

For surjectivity: any degree 1 invertible sheaf has a section, so if $\mathcal{L}$ is any degree 0 invertible sheaf, then $\mathcal{O}(\mathcal{L}(p)) \cong \mathcal{O}(x)$ for some x. □

Note that more naturally, $\operatorname{Pic}^1(E)$ is in bijection with the points of E (without any choice of point p).

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

Remark. The 2-torsion points in the group are the branch points in the double cover! Reason: q is a 2-torsion point if and only if $2q \sim 2p$ if and only if there is a section of $\mathcal{O}(2p)$ vanishing at q to order 2. (This is characteristic-independent.) Now assume that the characteristic is 0. (In fact, we'll only be using the fact that the characteristic is not 2.) By the Riemann-Hurwitz formula, there are 3 non-trivial torsion points. (Again, given 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 (see the discussion last day).

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".

But let's get back down to earth.

1.4. *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 $\mathrm{Pic}^0(E)$ 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 $q + r \sim 2p = 0$. □

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.

1.5. *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 just have to write down formulas for the construction on the cubic. This is no fun, so I just want to convince you that it can be done, rather than writing down anything explicit. They key idea is to define another 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. Then we can use this to construct addition on the cubic. □

Aside: Discussion on group varieties and group schemes.

A *group variety* X over k is something that can be defined as follows: We are given an element $e \in X(k)$ (a k-valued point of X), and maps $i : X \to X$, $m : X \times X \to X$. They satisfy the hypotheses you'd expect from the definition of a group.

(i) associativity:

$$\begin{array}{ccc} X \times X \times X & \xrightarrow{(m,id)} & X \times X \\ \downarrow{\scriptstyle (id,m)} & & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow{m} & X \end{array}$$

commutes.

(ii) $X \xrightarrow{e,id} X \times X \xrightarrow{m} X$ and $X \xrightarrow{id,e} X \times X \xrightarrow{m} X$ are both the identity.

(iii) $X \xrightarrow{i,id} X \times X \xrightarrow{m} X$ and $X \xrightarrow{id,i} X \times X \xrightarrow{m} X$ are both e.

More generally, a *group scheme over a base* B is a scheme $X \to B$, with a section $e : B \to X$, and B-morphisms $i : X \to X$, $m : X \times_B X \to X$, satisfying the three axioms above.

More generally still, a *group object in a category* $\mathcal{C}$ is the above data (in a category $\mathcal{C}$), satisfying the same axioms. The e map is from the final object in the category to the group object.

You can check that a group object in the category of sets is in fact the same thing as a group. (This is symptomatic of how you take some notion and make it categorical. You write down its axioms in a categorical way, and if all goes well, if you specialize to the category of sets, you get your original notion. You can apply this to the notion of "rings" in an exercise below.)

1.6. *The functorial description.* It is often cleaner to describe this in a functorial way. Notice that if X is a group object in a category $\mathcal{C}$, then for any other element of the category, the set $\mathrm{Hom}(Y, X)$ is a group. Moreover, given any $Y_1 \to Y_2$, the induced map $\mathrm{Hom}(Y_2, X) \to \mathrm{Hom}(Y_1, X)$ is group homomorphism.

We can instead define a group object in a category to be an object X, along with morphisms $m : X \times X \to X$, $i : X \to X$, and e : final object $\to X$, such that these induce a natural group structure on $\mathrm{Hom}(Y, X)$ for each Y in the category, such that the forgetful maps are group homomorphisms. This is much cleaner!

Exercise. Verify that the axiomatic definition and the functorial definition are the same.

Exercise. Show that (E, p) is a group scheme. (Caution! we've stated that only the closed points form a group — the group Pic^0. So there is something to show here. The main idea is that with varieties, lots of things can be checked on closed points. First assume that $k = \overline{k}$, so the closed points are dimension 1 points. Then the associativity diagram is commutative on closed points; argue that it is hence commutative. Ditto for the other categorical requirements. Finally, deal with the case where k is not algebraically closed, by working over the algebraic closure.)

We've seen examples of group schemes before. For example, $\mathbb{A}^1_k$ is a group scheme under addition. $\mathbb{G}_m = \mathrm{Spec}\, k[t, t^{-1}]$ is a group scheme.

Easy exercise. Show that $\mathbb{A}_k^1$ is a group scheme under addition, and $\mathbb{G}_m$ is a group scheme under multiplication. You'll see that the functorial description trumps the axiomatic description here! (Recall that $\mathrm{Hom}(X, \mathbb{A}_k^1)$ is canonically $\Gamma(X, \mathcal{O}_X)$, and $\mathrm{Hom}(X, \mathbb{G}_m)$ is canonically $\Gamma(X, \mathcal{O}_X)^*$.)

Exercise. Define the group scheme $GL(n)$ over the integers.

Exercise. Define μ_n to be the kernel of the map of group schemes $\mathbb{G}_m \to \mathbb{G}_m$ that is "taking nth powers". In the case where n is a prime p, which is also $\mathrm{char}\, k$, describe μ_p. (I.e. how many points? How "big" = degree over k?)

Exercise. Define a *ring scheme*. Show that $\mathbb{A}_k^1$ is a ring scheme.

1.7. *Hopf algebras.* Here is a notion that we'll certainly not use, but it is easy enough to define now. Suppose $G = \mathrm{Spec}\, A$ is an affine group scheme, i.e. a group scheme that is an affine scheme. The categorical definition of group scheme can be restated in terms of the ring A. Then these axioms define a *Hopf algebra*. For example, we have a "comultiplication map" $A \to A \otimes A$. *Exercise.* As $\mathbb{A}_k^1$ is a group scheme, $k[t]$ has a Hopf algebra structure. Describe the comultiplication map $k[t] \to k[t] \otimes_k k[t]$.

2. Fun counterexamples using elliptic curves

We have a morphism $(\times n) : E \to E$ that is "multiplication by n", 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.

2.1. *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.*

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 nontrivial 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.

An example of an affine open set that is not distinguished. I can give you an affine scheme X and an affine open subset Y that is not distinguished in X. Let $X = E - p$, which is affine (easy, or see Exercise).

Let q be another point on E so that $q-p$ is non-torsion. Then $E-p-q$ is affine (Exercise). 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.

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

Consider $p \in E$. 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.

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

This is related to Hilbert's fourteenth problem, although I won't say how.

Before we begin we have a preliminary exercise.

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. More serious stuff

I'll conclude the quarter by showing the following.

- If C has genus g, then "$\operatorname{Pic}^0(C)$ has dimension g".
- "The moduli space of curves of genus g "is dimension $3g - 3$."

We'll work over an algebraically closed field k. We haven't yet made the above notions precise, so what follows are just plausibility arguments. (It is worth trying to think of a way of making these notions precise! There are several ways of doing this usefully.)

3.1. The Picard group has dimension g: "$\dim \operatorname{Pic}^0 C = g$". There are quotes around this equation because so far, $\operatorname{Pic}^0 C$ is simply a set, so this will just be a plausibility argument. Let p be any (closed, necessarily degree 1) point of C. Then twisting by p gives an isomorphism of $\operatorname{Pic}^d C$ and $\operatorname{Pic}^{d+1} C$, via $\mathcal{L} \leftrightarrow \mathcal{L}(p)$. Thus we'll consider $\operatorname{Pic}^d C$, where $d \gg 0$ (in fact $d > \deg \mathcal{K} = 2g - 2$ will suffice). Say $\dim \operatorname{Pic}^d C = h$. We ask: how many degree d *effective divisors* are there (i.e. what is the dimension of this family)? The answer is clearly d, and C^d surjects onto this set (and is usually $d!$-to-1).

But we can count effective divisors in a different way. There is an h-dimensional family of line bundles by hypothesis, and each one of these has a $(d - g + 1)$-dimensional family of non-zero sections, each of which gives a divisor of zeros. But two sections yield the same divisor if one is a multiple of the other. Hence we get: $h + (d - g + 1) - 1 = h + d - g$.

Thus $d = h + d - g$, from which $h = g$ as desired.

Note that we get a bit more: if we believe that Pic^d has an algebraic structure, we have a fibration $(C^d)/S_d \to \operatorname{Pic}^d$, where the fibers are isomorphic to $\mathbb{P}^{d-g}$. In particular, Pic^d is reduced, and irreducible.

3.2. The moduli space of genus g curves has dimension $3g - 3$. Let $\mathcal{M}_g$ be the set of nonsingular genus g curves, and pretend that we can give it a variety structure. Say $\mathcal{M}_g$ has dimension p. By our useful Riemann-Roch facts, if $d \gg 0$, and D is a divisor of degree d, then $h^0(C, \mathcal{O}(D)) = d - g + 1$. If we take two general sections s, t of the line bundle $\mathcal{O}(D)$, we get a map to $\mathbb{P}^1$, and this map is degree d. Conversely, any degree d cover $f : C \to \mathbb{P}^1$ arises from two linearly independent sections of a degree d line bundle. Recall that (s, t) gives the same map to $\mathbb{P}^1$ as (s', t') if and only (s, t) is a scalar multiple of (s', t'). Hence the number of maps to $\mathbb{P}^1$ arising from a fixed curve C and a fixed line bundle $\mathcal{L}$ correspond to the choices of two sections ($2(d - g + 1)$), minus 1 to forget the scalar multiple, for a total of $2d - 2g + 1$. If we let the the line bundle vary, the number of maps from a fixed curve is $2d - 2g + 1 + \dim \operatorname{Pic}^d(C) = 2d - g + 1$. If we let the curve also vary, we see that the number of degree d genus g covers of $\mathbb{P}^1$ is $\boxed{p + 2d - g + 1}$.

But we can also count this number using the Riemann-Hurwitz formula. I'll need one believable fact: there are a finite number of degree d covers with a given set of branch points. (In the complex case, this is believable for the following reason. If $C \to \mathbb{P}^1$ is a branched cover of $\mathbb{P}^1$, branched over $p_1, \ldots, p_r$, then by discarding the branch points and their preimages, we have an unbranched cover $C' \to \mathbb{P}^1 - \{p_1, \ldots, p_r\}$. Then you can check that (i) the original map $C \to \mathbb{P}^1$ is determined by this map (because C is the normalization of $\mathbb{P}^1$ in this function field extension $\mathsf{FF}(C')/\mathsf{FF}(\mathbb{P}^1)$), and (ii) there are a finite number of such covers (corresponding to the monodromy data around these r points; we have r elements of S_d once we take branch cuts). This last step is where the characteristic 0 hypothesis is necessary.)

By the Riemann-Hurwitz formula, for a fixed g and d, the total amount of branching is $2g + 2d - 2$ (including multiplicity). Thus if the branching happens at no more than $2g + 2d - 2$ points, and if we have the simplest possible branching at $2g + 2d - 2$ points, the covering curve is genus g. Thus

$$p + 2d - g + 1 = 2g + 2d - 2,$$

from which $\boxed{p = 3g - 3}$.

Thus there is a $3g-3$-dimensional family of genus g curves! (By showing that the space of branched covers is reduced and irreducible, we could again "show" that the moduli space is reduced and irreducible.)

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