FOUNDATIONS OF ALGEBRAIC GEOMETRY CLASS 35

RAVI VAKIL

CONTENTS

Last day: More fun with curves: Serre duality, criterion for closed immersion, a series of useful remarks, curves of genus 0 and 2.

Today: hyperelliptic curves; curves of genus at least 2; elliptic curves take 1.

Last day we started studying curves in detail, using things we'd proved. Today, we'll continue to use these things. (See the "Class 34 crib sheet" for a reminder of what we know.)

1. HYPERELLIPTIC CURVES

As usual, we begin by working over an arbitrary field k, and specializing only when we need to. 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*.

Equivalently, C is hyperelliptic if it admits a degree 2 invertible sheaf $\mathcal{L}$ with $h^0(C, \mathcal{L}) = 2$.

1.1. *Exercise..* Verify that these notions are the same. 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 induced involution on C is called the *hyperelliptic involution*.

Date: Tuesday, February 28, 2006. Superficial update June 25, 2007.

1.2. *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 one of our useful facts (and indeed an exercise) was that the only invertible sheaf of degree $2g-2$ with (at least) g sections is the canonical sheaf. $\square$

1.3. *Proposition. — If a curve (of genus at least 2) is hyperelliptic, then it is hyperelliptic in "only one way". In other words, it admits only one double cover of* $\mathbb{P}^1$.

Proof. If C is hyperelliptic, then we can recover the hyperelliptic map by considering the canonical map: 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. We assume the $\operatorname{char} k = 0$, and $k = \overline{k}$, so we can invoke this black box. 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. We will see in a moment that the branch points determine the curve (Claim 1.4).

Assuming this, we see that 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

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

(As usual, this is not a well-defined statement, because as yet we don't know what we mean by "the space of hyperelliptic curves". For now, take it as a plausibility statement.) If we believe that the curves of genus g form a family of dimension $3g-3$, we have shown that "most curves are not hyperelliptic" if $g > 2$ (or on a milder note, there exists a hyperelliptic curve of each genus $g > 2$).

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

In particular, the branch points determine the hyperelliptic curve. (We also used this fact when discussing genus 2 curves last day.)

Proof. 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 $y^2 \in k(x)$, so 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 $y^2 = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. The branch points correspond to those values of x for which there is exactly one value of y, i.e. the roots of the polynomial. As we have no double roots, the curve is nonsingular. Let this cover be $C' \to \mathbb{A}^1$. Both C and C' are normalizations of $\mathbb{A}^1$ in this field extension, and are thus isomorphic. Thus every double cover can be written in this way, and in particular, if the branch points are $r_1, \dots, r_n$, the cover is $y^2 = (x - r_1) \cdots (x - r_n)$.

We now consider the situation over $\mathbb{P}^1$. A double cover can't be branched over an odd number of points by the Riemann-Hurwitz formula. Given an even number of points r_1, $\dots$, r_n in $\mathbb{P}^1$, choose an open subset $\mathbb{A}^1$ containing all n points. Construct the double cover of $\mathbb{A}^1$ as explained in the previous paragraph: $y^2 = (x - r_1) \cdots (x - r_n)$. Then take the normalization of $\mathbb{P}^1$ in this field extension. Over the open $\mathbb{A}^1$, we recover this cover. We just need to make sure 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 ∞. $\square$

Remark. 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 $a \in k^*/(k^*)^2$. So (assuming the field doesn't contain all squares) a double cover does *not* determine the same curve. 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 $h^0(C, \mathcal{O}(p)) = 0$ by one of our useful facts, so

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

Thus p is not a base-point of $\mathcal{K}$, so $\mathcal{K}$ 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).

Thus we conclude that 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. Once again, we use the useful fact saying that the only invertible sheaf of degree $2g-2$ with g sections is $\mathcal{K}$.

Exercise. Show 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 $\operatorname{Aut}\mathbb{P}^2 = PGL(3)$.)

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 next paragraph will necessarily require 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.

3. Genus at least 3

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

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*.

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 $g = 1$, there is no such bound!)

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 vice versa.

By Riemann-Roch, $\mathcal{K}^{\otimes 2}$ has $\deg \mathcal{K}^{\otimes 2} - g + 1 = 12 - 4 + 1 = 9$ sections. That's one less than $\dim \operatorname{Sym}^2 \Gamma(C, \mathcal{K}) = \binom{4+1}{2}$. 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.) Note that C can't lie in a plane, so Q must be a cone or nonsingular. In particular, Q is irreducible.

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, it is a curve of degree 4. Thus our curve C, being of degree 6, cannot be contained in $Q \cap Q'$.

We next consider cubics. By Riemann-Roch, $\mathcal{K}^{\otimes 3}$ has $\deg \mathcal{K} \otimes 3 - g + 1 = 18 - 4 + 1 = 15$ sections. 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. Admittedly 4 of them 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, 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.

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.

We now consider the converse, and who that any nonsingular complete intersection C of a quadric surface with a cubic surface is a canonically embedded genus 4 curve. It is not hard to check that it has genus 3 (again, using our exercises involving Hilbert functions). *Exercise.* Show that $\mathcal{O}_C(1)$ has 4 sections. (Translation: C doesn't lie in a hyperplane.) Hint: long exact sequences! Again, the only degree $2g - 2$ invertible sheaf with g sections is the canonical sheaf, so $\mathcal{O}_C(1) \cong \mathcal{K}_C$, and C is indeed canonically embedded.

Exercise. Conclude that nonhyperelliptic curves of genus 4 "form a family of dimension $9 = 3g - 3$". (Again, this isn't a mathematically well-formed question. So just give a plausibility argument.)

On to genus 5!

Exercise. Suppose C is a nonhyperelliptic genus 5 curve. 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 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.

Exercise. Show that the complete intersections of 3 quadrics in $\mathbb{P}^4$ form a family of dimension $12 = 3g - 3$.

This suggests that the nonhyperelliptic curves of genus 5 form a dimension 12 family.

So we've managed to understand curves of genus up to 5 (starting with 3) by thinking of canonical curves as complete intersections. Sadly our luck has run out.

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.)

4. Genus 1

Finally, we come to the very rich case of curves of genus 1.

Note that $\mathcal{K}$ is an invertible sheaf of degree $2g - 2 = 0$ with $g = 1$ section. 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 and Serre duality gives

$$h^0(C, \mathcal{L}) = h^0(C, \mathcal{L}) - h^0(C, \mathcal{K} \otimes \mathcal{L}^\vee) = h^0(C, \mathcal{L}) - h^0(C, \mathcal{L}^\vee) = \deg \mathcal{L}$$

as an invertible sheaf $\mathcal{L}^\vee$ of negative degree necessarily has no sections.

An *elliptic curve* is a genus 1 curve E with a choice of k-valued point p. (Note: it is *not* the same as a genus 1 curve — some genus 1 curves have no k-valued points. However, if $k = \overline{k}$, then any closed point is k-valued; but still, the choice of a closed point should always be considered part of the definition of an elliptic curve.)

Note that $\mathcal{O}_E(2p)$ has 2 sections, so the argument given in the hyperelliptic section shows that E admits a double cover of $\mathbb{P}^1$. 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 $k = \overline{k}$, 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 $\mathbb{P}^1$, we get a map ($y^2 = \cdots$). This determines C (as shown in the hyperelliptic section). Thus elliptic curves correspond to 4 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 $x \mapsto ax + b$.)

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. Notice that $\lambda \neq 0, 1, \infty$.

- 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 (in bijection with 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 Luroth's theorem, 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.

At this point I should just give you j:

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

But this begs the question: where did this formula come from? How did someone think of it?

Far better is to guess what j is. We want to come up with 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 silly choice would be the product of the six numbers $\lambda(1/\lambda) \cdots$ as this is 1.

A better idea is to add them all together. Unfortunately, if you do this, you'll get 3. (Here is one reason to realize this can't work: if you look at the sum, you'll realize that you'll get something of the form "degree at most 3" divided by "degree at most 2" (before cancellation). Then if $j' = p(\lambda)/q(\lambda)$, then λ satisfies (at most) a cubic over j. But we said that λ should satisfy a sextic over j'. The only way we avoid a contradiction is if $j' \in k$.

Our next attempt is to add up the six squares. When you do this by hand (it isn't hard), you get

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

This works just fine: $k(j) \cong k(j'')$. If you really want to make sure that I'm not deceiving you, you can check (again by hand) that

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

The difference is 3.

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