# 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

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

$$\mathcal{O}(q - p) \longmapsfrom q$$

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 $\infty$, 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 $\lambda$-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 $\lambda$ under this map, where necessarily $\lambda \neq 0, 1, \infty$.

The value $\lambda$ 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 $\lambda$ 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 $\lambda$ should satisfy a sextic polynomial over $k(\lambda)$, as for each j-invariant, there are six values of $\lambda$ 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 $\lambda$) 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 $\lambda$ 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 $\lambda$ is some fixed small number (say $1/2$), the sum of squares is some small real number, while when $\lambda$ 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:

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

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. □

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. □

**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. □

**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