ELLIPTIC CURVES

Contents

These notes are from a course taught by Professor Bao Le Hung at Nortwestern University during the winter quarter of the 20/21 academic year. The note taker is responsible for any mistakes or inaccuracies that occur.

1. Lecture 1 (Monday 1/11)

This is a topics class about **elliptic curves**. The goal of today is to give an overview.

A quick and concrete definition:

Definition 1. Let k be a field. An *elliptic curve* E/k is a smooth projective plane cubic determined by an affine equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where $a_i \in k$, i. e. E is the closure of this affine curve in $\mathbb{P}^2$, *and* the data of a rational point $0 \in E(k)$.

In other words, if $\mathbb{P}^2$ has homogeneous coordinates $[X : Y : Z]$, then E is the curve in $\mathbb{P}^2$ determined by the equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

For this to be *smooth*, there is a condition $\Delta(a_1, a_2, \dots) \neq 0$, where Δ is a polynomial in the a_i. (The precise formula can be found in Silverman.) In the case where the equation is

$$y^2 = x^3 + ax + b, \tag{2}$$

we have $\Delta(a, b) = -4a^3 - 27b^2$. By the way, Equation 1 is called the *Weierstrass equation*, and Equation 2 is called the *short Weierstrass equation.*

1.1. **Why study elliptic curves?** Firstly, the plane cubics in $\mathbb{P}^2$ are exactly the smooth projective genus 1 curves. Being genus 1 is between being genus 0, i. e. $\mathbb{P}^1$, and of genus > 1, of “general type”. In the theory of curves, there is a trichotomy where the geometry behaves very differently based on whether the genus is 0, 1, or higher than 1.

Secondly, an elliptic curve is exactly a proper group variety of dimension 1. There is a multiplication map $m\colon E \times E \to E$, and inversion map $\mathrm{inv}\colon E \to E$, and an identity map $0\colon \operatorname{Spec} k \to E$, satisfying a bunch of commutative diagrams. The point is that these maps are algebraic maps.

Being a proper group variety means that we have direct access to cohomological invariants of E. For example the *Tate module.* The interaction between the group structure and algebraic variety structure implies many things.

Themes:

(1) Study nature of the abelian group $E(k)$. (We will see later on that *abelian* is a formal consequence of being proper.)
(2) See how cohomological invariant control $E(k)$. More or less everything you want to know about $E(k)$ will be controlled by cohomological invariants, namely the Tate module.

1.2. **Examples.**

(1) $k = \mathbb{C}$. In this case, $E/\mathbb{C}$ is a compact Riemann surface of genus 1. By the uniformization, a genus 1 Riemann surface has universal cover $\mathbb{C}$, hence $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where $\Lambda \subseteq \mathbb{C}^2$ is a lattice. These are all complex tori. It turns out that the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ can be made to respect the group structure.

More canonically, $\Lambda \cong \pi_1(E(\mathbb{C}), 0) = H_1(E(\mathbb{C}), \mathbb{Z})$. We can understand $\mathbb{C}$ as the Lie algebra of E, and the exponential map $\mathrm{Lie}(E) \to E(\mathbb{C})$ corresponds to the quotient map $\mathbb{C} \to \mathbb{C}/\Lambda$. We have $\mathrm{Lie}(E) = T_0E(\mathbb{C}) = \{$invariant global vector fields on $E(\mathbb{C}\} = H^0\left(E(\mathbb{C}), \Omega^1\right)^*$.

Note that the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ is complex analytic, and the x, y that show up in the Weierstrass equation correspond to some doubly periodic meromorphic functions on $\mathbb{C}$. These are so-called *elliptic functions.*

The n-torsion $E[n](\mathbb{C}) \cong \frac{1}{n}\Lambda/\Lambda \cong \mathbb{Z}/n \times \mathbb{Z}/n$. For a prime p, *Tate module* T_pE is defined as

$$T_p(E) = \varprojlim_{\times p} E[p^k](\mathbb{C}) = \varprojlim \left(E[p] \leftarrow E[p^2] \leftarrow \cdots\right).$$

Canonically, in this case

$$T_pE = \varprojlim \frac{1}{p^k}\Lambda/\Lambda = \varprojlim_{\text{projection}} \Lambda/p^k\Lambda = \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p = H_1(E(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

the p-adic completion of $\Lambda = H_1(E(\mathbb{C}), \mathbb{Z})$.

For the first theme, we have seen that $E(\mathbb{C})$ is an divisible uncountable abelian group. For the second, E is completely determined by the pair $(\mathrm{Lie}\, E, H_1(E, \mathbb{Z})) = \left(H^0\left(E, \Omega^1\right)^*, H_1(E, \mathbb{Z})\right)$. Here, $H_1(E, \mathbb{Z})$ is a free $\mathbb{Z}$-module, and $H^0\left(E, \Omega^1\right)^*$ is a line in $H_1(E, \mathbb{Z})^* \otimes_{\mathbb{Z}} \mathbb{C}$. This is the data of a *Hodge structure* of weight -1. The interesting fact here is that a nonlinear thing like E is determined by just linear algebrac data that can be extracted from E by cohomological data.

(2) $k = \mathbb{F}_q$ a finite field. Now $E(\mathbb{F}_q)$ is a finite abelian group. A basic fact is that if $a = q+1-\#E(\mathbb{F}_q)$, then $|a| \leq 2\sqrt{q}$. This is known as the *Hasse bound*. We have a double cover

$$E \to \mathbb{P}^1$$
$$(x, y) \mapsto x$$

which should mean that the number of rational points of E is roughly the same as the number of points of $\mathbb{P}^1$, which is $q+1$. The discrepancy is of order $\sqrt{q}$, and the heuristic is that the Hasse bound is as if $\#E(\mathbb{F}_q)$ is "random" (subject to some natural constraints).

How do the cohomological invariants come into play? We don't have singular cohomology, but we do have the Tate module $T_l(E)$, where $l \neq p = \operatorname{char} q$. It is defined as

$$T_l E = \varprojlim E[l^n](\overline{\mathbb{F}_q}).$$

There are two important facts about this Tate module. The first is that $E[l^n]\left(\overline{\mathbb{F}_q}\right) \cong \mathbb{Z}/l^n \times \mathbb{Z}/l^n$ as in the complex case, and consequently $T_l E \cong \mathbb{Z}_l^2$. The second is that $T_l E$ has a natural action of $\operatorname{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right)$. This Galois group is simple, namely procyclic $\cong \hat{\mathbb{Z}}$, as topologically it is generated by the Frobenius Frob_q. In sum, $T_l E$ is a free $\mathbb{Z}_l$-module of rank two with an action of Frob_q. The meaning of a from before is that $a = \operatorname{tr} \operatorname{Frob}_q$. (Note that this does not hold for $l = p$.)

In the general context, for algebraic varieties over finite fields you don't have singular cohomology, but you do have l-adic or étale cohomology. Secretly, $T_l E \cong H_1\left(E/\overline{\mathbb{F}_q}, \mathbb{Z}_l\right)$, the l-adic homology of E. One advantage of working with the Tate module is that it is elementaryto define, whereas defining l-adic cohomology is rather complicated.

In the finite field case, E is almost recovered from the action of Frob_q on $T_l E$. The problem is the choice of l: If you know this action for all l, even $l = p$, then you can indeed recover E. Compared to the complex case, we only work with homology and we have no Hodge structure. However, we do have an action of the Galois group as a substitute for the Hodge structure. This is a recurring theme.

(3) k a local field, i. e. a finite extension of $\mathbb{Q}_p$. Let's stick with $k = \mathbb{Q}_p$ for simplicity, but this will not impact the results. Now $E(\mathbb{Q}_p)$ is a p-adic manifold, i. e. has charts that are isomorphic to p-adic balls $\mathbb{Z}_p$, and in fact a p-adic Lie groups. One feature of $\mathbb{Q}_p$ is the existence of a good integral structure: There is a maximal compact subring $\mathbb{Z}_p \subseteq \mathbb{Q}_p$, and one can comtemplate if there are integral models $\mathcal{E}/\mathbb{Z}_p$ for $E/\mathbb{Q}_p$. We can obtain one such integral model cheaply by clearing denominators in a Weierstrass equation, but it is a subtle question to get the "optimal" one, and this is given by the Néron model. The source of the subtlety is that if $\mathcal{E}$ is proper, then $\mathcal{E}(\mathbb{Z}_p) = E(\mathbb{Q}_p)$, but $\mathcal{E}$ may not have a group structure. It may be impossible for $\mathcal{E}$ to be proper and have a group structure at the same time, but the Néron model $\mathcal{E}$ has a group structure and still satisfies $\mathcal{E}(\mathbb{Z}_p) = E(\mathbb{Q}_p)$. If E has *good reduction* we can take $\mathcal{E}$ to be proper and have a group structure. This implies that we have an exact sequence

$$0 \to \underbrace{\hat{\mathcal{E}}(\mathbb{Z}_p)}_{\text{formal group}} \to E(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Z}_p) \to \underbrace{\mathcal{E}(\mathbb{F}_p)}_{\text{finite group}} \to 0.$$

The formal group on the left, whatever it is, is a pro-p-group.

Insert picture

$\operatorname{Spec} \mathbb{Z}_p$ has two points, namely the generic point $\operatorname{Spec} \mathbb{Q}_p$ and $\operatorname{Spec} \mathbb{F}_p$. The elliptic curve E lives over $\operatorname{Spec} \mathbb{Q}_p$, and the integral model $\mathcal{E}$ is a way too expand E over the other point $\operatorname{Spec} \mathbb{F}_p$. Any point of $E(\mathbb{Q}_p)$ then corresponds to a "section" $\operatorname{Spec} \mathbb{Z}_p \to \mathcal{E}$, which specializes to a point $\mathcal{E}(\mathbb{F}_p)$. We can interpret the exact sequence as decomposing $E(\mathbb{Q}_p)$ into p-adic balls.

The Tate module $T_l E$, which is defined as before, has an action of $\operatorname{Gal}\left(\overline{\mathbb{Q}_p}/\mathbb{Q}_p\right)$, a much more complicated Galois group than in the case of finite fields. The Tate module with the Galois action does not quite determine E as strongly as in the case of finite fields, however it does determine many things about $\mathcal{E}$. In particular, it can recognize when E has good reduction. This is the criterion of *Néron-Ogg-Shafarevich.*

(4) k is a number field, i. e. a finite extension of $\mathbb{Q}$, and let us for simplicity consider the case $k = \mathbb{Q}$.

Theorem 2 (Mordell-Weil)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group.*

In other words, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$. The number r is the *rank* of E.

Remark 3. Let $C/\mathbb{Q}$ be a smooth projective curve of genus g. If $g = 0$, then $C(\mathbb{Q})$ is either ∞ or $\emptyset$. If $g > 1$, then $C(\mathbb{Q})$ is finite by Faltings' Theorem. If $g = 1$, then $C(\mathbb{Q})$ can be $\emptyset$, finite, or infinite.

Computing $E(\mathbb{Q})$ is interesting from an arithmetic point of view. As an example, take the *congruent number problem*: An integer $n \in \mathbb{Z}$ that is square-free is a *congruent number* if there is a triple $a, b, c \in \mathbb{Q}$ with $a^2+b^2=c^2$ and $n=\frac{1}{2}ab$, or in geometric terms a right-angled triangle with rational sides a, b, c and area n. Equivalently, we can ask about an arithmetic progression α^2, $\beta^2=\alpha^2+n$, $\gamma^2=\beta^2+n$. For example, $n=1$ is not congruent, as shown by Fermat. On the other hand $n=5$ is congruent, because we can take $a=\frac{20}{3}$, $b=\frac{3}{2}$.

Proposition 4. *Let E_n be the elliptic curve given by $y^2=x^3-n^2x$. Then n is a congruent number if and only if $\operatorname{rank} E_n(\mathbb{Q})>0$, i. e. if and only if $E_n(\mathbb{Q})$ is infinite.*

Explanation. If (x,y) is a rational point on E, then $a=\frac{x^2-n^2}{y}$, $b=2n\frac{x}{y}$, $c=\frac{x^2+n^2}{y}$ realizes n as a congruent number. This gives a bijection between triples (a,b,c) realizing n as a congruent number and $(x,y)\in E(\mathbb{Q})$ such that $y \neq 0$. To prove the proposition, we check that $E_n(\mathbb{Q})_{\mathrm{tors}} \subseteq \{y=0\}$, which strongly uses the exact sequence from before.

How does T_lE control $E(\mathbb{Q})$? The function

$$L(E,s)=\prod_{p \text{ prime of good reduction}} \frac{1}{1-a_pp^{-s}+p^{1-2s}} \prod_{p \text{ prime of bad reduction}} (\cdots),$$

where $a_p=p+1-\#E(\mathbb{F}_p)$. assembles all possible point counts of E modulo p.

Conjecture 5 (Birch-Swinnerton-Dyer)**.** *$L(E,s)$ has holomorphic continuation to all $s\in\mathbb{C}$, and $\operatorname{ord}_{s=1} L(E,s)=\operatorname{rank} E$.*

For the congruent number problem, $L(E,s)$ is “easy” and there exists an explicit formula for $L(E,1)$ involving some ternary quadratic forms.

2. Lecture 2 (Wednesday 1/13)

Last time, we outlined the basic material. Today, we start proving things.

There are three characterizations of what an elliptic curve is. Let k be a field. When convenient we will make the simplifying assumption that the characteristic of k is 2 or 3.

Proposition 6. *There are three equivalent ways of defining an elliptic curve:*

- *(A) As a smooth projective genus 1 curve E, with a rational point $O\in E(k)$.*
- *(B) As plane cubic given by the equation*

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

  in $\mathbb{P}^2$, where $a_i\in k$ and discriminant $\Delta(a_1,a_2,a_3,a_4,a_5,a_6)\neq 0$. (The point O corresponds to $[0:1:0]$.)
- *(C) (E,O) is a proper group variety of dimension 1 with identity O. (Recall that a group variety is a variety with group structure such that multiplication and inversion are algebraic maps, i. e. a group object in a certain category.)*

Last time we started with (B), which is the most concrete. Today we will establish the equivalence of (A) and (B), which is the study of projective geometry of genus 1 curves. The equivalence of (A), (B), and (C) will be established next time.

The general way to study a smooth projective curve is to map it into projective space, and such a map is given by a line bundle with a generating set of global sections.

2.1. Reminder on projective geometry of curves.

If C is a smooth projective curve, $v\in C$ a closed points, we can measure the order of functions on C along v using that $\mathcal{O}_{C,v}$ is a DVR. We have

$$\operatorname{Prin}(C)=\{\operatorname{div} f, f\in K(C)\}\subset \operatorname{Div}(C)=\bigoplus_{v \text{ closed point}} \mathbb{Z}v,$$

where $K(C)$ is the field of rational functions on C, i. e. functions that are defined away from finitely many points, and $\operatorname{div}(f)=\sum_{v\in C}\operatorname{ord}_v fv$. The class group of C is $\operatorname{Cl}(C)=\operatorname{Div}(C)/\operatorname{Prin}(C)$, and there is a degree map deg: $\operatorname{Cl}(C)\to\mathbb{Z}$ given by $\sum n_v v\mapsto\sum n_v$. In our situation there is an isomorphism

$\mathrm{Cl}(C) \cong \mathrm{Pic}(C)$, where $\mathrm{Pic}(C)$ is the Picard group of isomorphism classes of line bundles on C. Via this isomorphism, a divisor $D \in \mathrm{Cl}(C)$ corresponds to the line bundle $\mathcal{O}(D)$ given by

$$\mathcal{O}(D)(U) = \{f \in K(C) : \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

For doing projective geometry the Picard group $\mathrm{Pic}(C)$ is important because it "controls" maps of C into projective space. The reason is that if we have a set of elements $s_0, s_1, \ldots, s_d \in H^0(C, \mathcal{L})$ that generate $\mathcal{L}$, we get a map

$$\begin{aligned} C &\to \mathbb{P}^d \\ v &\mapsto [s_0(v) : \cdots : s_d(v)]. \end{aligned}$$

Although the value $s_i(v)$ is not well-defined, the common ratio of the $s_i(v)$ is well-defined as an element of $\mathbb{P}^d$. The way this could go wrong is if all the s_i vanish at a point, but the assumption that they generate $\mathcal{L}$ is precisely the condition that this doesn't happen.

Remark 7. More intrinsically, we get a map to projective space by sending $v \in C$ to the hyperplane of sections in $H^0(C, \mathcal{L})$ vanishing at v. Depending on conventions, this is a map $C \to \mathbb{P}\left(H^0(C, \mathcal{L})\right)$ or $C \to \mathbb{P}\left(H^0(C, \mathcal{L})^\vee\right)$.

Because of the relation between line bundles and maps to projective space, the dimension of $H^0(C, \mathcal{L})$ gives an upper bound for the dimension d of projective space that we can map into. Riemann-Roch provides the main tool for computing the dimension of global sections of line bundles.

If $\mathcal{F}$ is a sheaf on C, then the Euler characteristic is

$$\chi(\mathcal{F}) = \dim H^0(C, \mathcal{F}) - \dim H^1(C, \mathcal{F}).$$

The cohomology groups $H^i(C, \mathcal{F})$ are finite dimensional over k because C is projective, and vanish for $i > 1$ because C is a curve.

The Euler characteristic χ is additive on short exact sequences of sheaves. For example, if $v \in C$ is a closed point there is an exact sequence $0 \to \mathcal{O}_C \to \mathcal{O}(v) \to k_v \to 0$, where k_v is the skyscraper sheaf with value k supported at v, so $\chi(\mathcal{O}(v)) = \chi(\mathcal{O}_C) + \deg v$. More generally,

$$\chi(\mathcal{O}(D)) = \chi(\mathcal{O}_C) + \deg D. \tag{3}$$

Whereas additivity of Euler characteristics is purely formal, *Serre duality* is a fundamental fact which says that

$$H^1(C, \mathcal{L}) \cong H^0\left(C, \Omega^1 \otimes \mathcal{L}^{-1}\right)^\vee, \tag{4}$$

where Ω^1 is the sheaf of differentials.

Combining Equations (3) and (4),

$$\dim_k H^0(C, \mathcal{O}(D)) - \dim_k H^0\left(C, \Omega^1 \otimes \mathcal{O}(-D)\right) = \chi(\mathcal{O}(D)) = \chi(\mathcal{O}_C) + \deg D = 1 - g + \deg D, \quad \text{(Riemann-Roch)}$$

where $g = \dim H^1(C, \mathcal{O}_C) = \dim H^0\left(C, \Omega^1\right)$ is the *genus* of C.

Remark 8. If C is a proper curve, but not necessarily smooth, then everything above works except for Serre duality. The number $\dim H^1(C, \mathcal{O}_C)$ is the *arithmetic genus* of C.

In order to apply Riemann-Roch, we will use:

Easy fact. If $\deg \mathcal{L} \leq 0$ and $\mathcal{L} \ncong \mathcal{O}_C$, then $\dim H^0(C, \mathcal{L}) = 0$.

2.2. Back to elliptic curves.

Let E be a genus 1 smooth projective curve, and $O \in E(k)$. The idea of going from (A) to (B) is to study maps from E into projective space determined by sections of the line bundles $\mathcal{O}(nO)$. Being genus 1 implies that

(i) Riemann-Roch becomes $\dim_k H^0(E, \mathcal{O}(nO)) - \dim_k H^0\left(E, \Omega^1 \otimes \mathcal{O}(-nO)\right) = n$.

(ii) We have $\Omega^1 \cong \mathcal{O}_C$. This is because first of all, $\dim H^0\left(E, \Omega^1\right) = g = 1$, and second, because by Riemann-Roch $\deg \Omega^1 = 2g - 2 = 0$. Hence the statement follows from the "easy fact".

Combining (i) and (ii), we obtain $\dim_k H^0(E, \mathcal{O}(nO)) - \dim_k H^0(E, \mathcal{O}(-nO)) = n$. Using the "easy fact" that $H^0(E, \mathcal{O}(D)) = 0$ if $\deg D < 0$, it follows that

$$\dim_k H^0(E, \mathcal{O}(nO)) = \begin{cases} 1, & n = 0, \\ n, & n > 0. \end{cases}$$

Note that $H^0(E, \mathcal{O}(0O)) \subseteq H^0(E, \mathcal{O}(O)) \subseteq H^0(E, \mathcal{O}(2O)) \subseteq \cdots$. The constant function $1 \in H^0(E, \mathcal{O}(0))$ is a non-zero element. Since $H^0(E, \mathcal{O}(2O))$ has dimension 2 there is an element $x \in H^0(E, \mathcal{O}(2O))$ that is not a scalar multiple of 1. And since $H^0(E, \mathcal{O}(3O))$ has dimension 3 there is an element $y \in H^0(E, \mathcal{O}(3O))$ that is not a linear combination of 1 and x.

Claim 9. *The map*

$$\begin{aligned} E &\to \mathbb{P}^2 \\ v &\mapsto [x(v) : y(v) : 1] \end{aligned}$$

is an embedding, and the image is a smooth plane cubic given by a Weierstrass equation.

There are two things to check, namely that the map is an *embedding* and that the image is a smooth plane cubic.

To guess the image, we find relations between monomials in $x, y, 1$. In this case, the target projective space is 2-dimensional, so to identify the image it will suffice to find one relation, as this cuts out a 1-dimensional object.

Note that $x^3, x^2, x, y, y^2, xy, 1 \in H^0(E, \mathcal{O}(6O))$. So we have 7 elements of a 6-dimensional space, so there exists a non-trivial linear relation between them. Because pole orders are distinct except for x^3, y^2, this relation has to involve x^3 and y^2. After rescaling x, y, we can make this relation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Remark 10. This linear relation is essentially unique, because if we throw out x^3 or y^2 the remaining elements constitute a basis.

Let $\widetilde{E}$ denote the plane cubic described by this Weierstrass equation. In order to establish Claim 9, it remains to show that

(i) $\widetilde{E}$ is smooth,
(ii) The map $\pi\colon E \to \widetilde{E}$ is an isomorphism.

To do this, we have to do one basic computation. The idea is to first show that π is birational, and then compute the arithmetic genus.

Claim 11. *π is birational, i. e. induces an isomorphism of function fields.*

Proof. To prove this claim, we compute the (scheme-theoretic) fiber of a point $[0 : 1 : 0] \in \widetilde{E}$. An affine chart around $[0 : 1 : 0]$ is $\left[\frac{X}{Y} : 1 : \frac{Z}{Y}\right]$, so $\widetilde{E}$ in this chart is given by

$$\frac{Z}{Y} + a_1\frac{X}{Y}\frac{Z}{Y} + a_3\left(\frac{Z}{Y}\right)^2 = \left(\frac{X}{Y}\right)^3 + a_2\left(\frac{X}{Y}\right)^2\frac{Z}{Y} + a_4\frac{X}{Y}\left(\frac{Z}{Y}\right)^2 + a_6\left(\frac{Z}{Y}\right)^3.$$

The term $\frac{Z}{Y}$ is linear whereas the other terms are quadratic or cubic, and this implies that the point $[0 : 1 : 0]$ is smooth. The inverse image $\pi^{-1}\{[0 : 1 : 0]\}$ is the locus in E where $\frac{x}{y}$ and $\frac{1}{y}$ has zeros. By construction, y only has poles at O, and therefore $\pi^{-1}\{[0 : 1 : 0]\} = \{O\}$. There is no multiplicity because $\operatorname{ord}_O \frac{x}{y} = \operatorname{ord}_O x - \operatorname{ord}_O y = 1$. This shows that π is birational. □

There are now two ways to proceed. Silverman's approach is to show that a singular plane cubic is birational to $\mathbb{P}^1$, which is a contradiction because E is a genus 1 curve which is not birational to $\mathbb{P}^1$. The map π is finite, so we have a short exact sequence of structure sheaves

$$0 \to \mathcal{O}_{\widetilde{E}} \to \pi_*\mathcal{O}_E \to \text{skyscrapers} \to 0,$$

the cokernel being a sum of skyscraper sheaves since π is birational (and the first map is an isomorphism over an open set). Since π is finite, cohomology commutes with π_*, so in particular $\chi(\pi_*\mathcal{O}_E) = \chi(\mathcal{O}_E) = 1 - 1 = 0$. Additivity of Euler characteristics applied to the short exact sequence yields

$$\chi(\mathcal{O}_{\widetilde{E}}) + \chi(\text{skyscrapers}) = \chi(\pi_*\mathcal{O}_E) = 0.$$

On the other hand, there is a short exact sequence

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-3) \to \mathcal{O}_{\mathbb{P}^2} \to i_*\mathcal{O}_{\widetilde{E}} \to 0,$$

where the first map is multiplication by the cubic defining $\widetilde{E}$, and $i\colon \widetilde{E} \hookrightarrow \mathbb{P}^2$ is the inclusion. Again, additivity of Euler characteristics imply that

$$\chi(\mathcal{O}_{\mathbb{P}^2}(-3)) + \chi(\mathcal{O}_{\widetilde{E}}) = \chi(\mathcal{O}_{\mathbb{P}^2}),$$

from which we can compute that $\chi(\mathcal{O}_{\widetilde{E}}) = 0$.

Exercise 1. Generalize this last argument to show that if C is a plane curve of degree d in $\mathbb{P}^2$, then $\chi(\mathcal{O}_C) = 1 - \frac{(d-1)(d-2)}{2}$.

The conclusion is that $H^0(E, \text{skyscrapers}) = \chi(\text{skyscrapers}) = 0$, so in fact the map

$$\mathcal{O}_{\widetilde{E}} \to \pi_*\mathcal{O}_E$$

must be an isomorphism. This concludes our proof of "(A) implies (B)". But the computation of $\chi(\mathcal{O}_{\widetilde{E}})$ also shows that "(B) implies (A)".

To sum up, we started with (E, O) as in (1) and produced a cubic curve given by a Weierstrass equation. But (E, O) can produce many such Weierstrass equations depending of choices of x, y. The choice is only unique up to an action of an upper triangular 3×3-matrix. This is because we chose the basis in such a way as to be compatible with the filtration

$$H^0(E, \mathcal{O}_E) \subset H^0(E, \mathcal{O}(2O)) \subset H^0(E, \mathcal{O}(3O)),$$

i. e. we can replace $x \mapsto ux + \alpha$ and $y \mapsto vy + \beta x + \gamma$, and this is encoded by an upper triangular matrix. In the end, we have

$$\{(E, O)\}/\text{iso} \cong \left(k^5\right)^{\Delta \neq 0}/B(k).$$

If $\operatorname{char} k \neq 2, 3$, we can further simplify this quotient, by choosing x, y such that $a_1, a_3, a_2 = 0$. In the Weierstrass equation, we can complete the square on the left hand side and complete the cube on the right hand side:

$$y^2 + a_1xy + a_3y = \left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 + \text{quadratic polynomial in } x,$$
$$x^3 + a_2x^2 + a_4x + a_6 = \left(x + \frac{a_2}{3}\right)^3 + \text{linear polynomial in } x.$$

This gets rid of a_1, a_3, a_2. So if $\operatorname{char} k \neq 2, 3$,

$$\{(E, O)\}/\text{iso} \cong \left(k^2\right)^{\Delta \neq 0}/k^\times = \left\{(a_4, a_6) : 4a_4^3 + 27a_6^2 \neq 0\right\}/k^\times,$$

where as we'll see next time the action of $u \in k^\times$ is given by $u(a_4, a_6) = \left(u^{-4}a_4, u^{-6}a_6\right)$.

3. Lecture 3 (Friday 1/15)

Last time we showed that the following data are equivalent:

(1) (E, O), where E is a genus 1 curve and $O \in E(k)$.
(2) A Wierestrass equation $Y^2Z + a_1XYZ + a_3XZ^2 = x^3 + a_2X^2Z + a_4XZ + a_6$ describing a smooth cubic in $\mathbb{P}^2$.

To go from (1) to (2), we analyzed $H^0(E, \mathcal{O}(nO))$. We took $x \in H^0(E, \mathcal{O}(2O))$ non-constant, $y \in H^0(E, \mathcal{O}(3O))$ not in the span of 1 and x, and from these we produced a Weierstrass equation.

The pair (E, O) in fact gives rise to many Weierstrass equations. The question is how many? The choice of $y, x, 1$ is well-defined up to replacing y by $\alpha y + \beta x + \gamma$ and x by $\alpha' x + \beta'$ (with some relation between α and α'). This substitution turns a Weierstrass equation into another Weierstrass equation (with different coefficients a_i). These substitution corresponds to an action of some subgroup of upper triangular matrices on Weierstrass equations. We have a map

$$\{(E,O)\}\,/\cong \to \{\text{Weierstrass equations}\}\,/\text{action}.$$

If $\operatorname{char} k \neq 2,3$ we can choose a Weierstrass equation with $a_1 = a_2 = a_3 = 0$, and the action of changing such Weierstrass equations is just an action of $k^\times$. The map above then takes the form

$$\{(E,O)\}\,/\cong \to \{(a_4,a_6)\}\,/k^\times.$$

For a Weierstrass equation $y^2 = x^3 + a_4x + a_6 = f(x)$ the following are equivalent

$$\begin{aligned}\text{the curve described by the Weierstrass equation is smooth} &\iff f \text{ and } f' \text{ are coprime}\\ &\iff f(x) = (x-\alpha_0)(x-\alpha_1)(x-\alpha_2), \alpha_i \neq \alpha_j \in \overline{k}\\ &\iff \Delta = \underbrace{\prod(\alpha_i - \alpha_j)^2}_{\in \mathbb{Z}[a_4,a_6]} \neq 0.\end{aligned}$$

In fact, $\Delta = -16(4a_4^3 + 27a_6^2)$. We are allowed to substitute

$$(\alpha y + \beta x + \gamma)^2 = (\alpha' x + \beta')^3 + a_4(\alpha' x + \beta') + a_6,$$

where $\alpha, \alpha' \neq 0$. In order for this to be a short Weierstrass equation, we need $\alpha^2 = \alpha'^3 \neq 0$, $2\alpha\beta = 0$, $2\alpha\gamma = 0$, $3\alpha'^2\beta' = 0$, and therefore $\beta = \beta' = \gamma = 0$. So the substition must be of the form $y \mapsto \alpha y$ and $x \mapsto \alpha' x$. The effect of this substitution on a short Weierstrass equations is to replace (a_4,a_6) with $(u^{-4}a_4, u^{-6}a_6)$, where $u^2 = \alpha'$. To summarize:

Proposition 12. *Suppose* $\operatorname{char} k \neq 2,3$. *Then there is a bijection*

$$\{(E,O)\}\,/\cong \to \left\{(a_4,a_6) : 4a_4^3 + 27a_6^2 \neq 0\right\}/k^\times,$$

where $u \in k^\times$ *acts by* (a_4,a_6) *via* $u(a_4,a_6) = \left(u^{-4}a_4, u^{-6}a_6\right)$.

We now define a "universal" function on the pairs (a_4,a_6).

Definition 13 (j-invariant)**.** We define

$$j(E) = \frac{1728a_4^3}{4a_4^3 + 27a_6^2}.$$

The 1728 is a normalizing factor that you can ignore for now. The j-invariant has the important features that

(1) The denominator does not vanish.
(2) It is invariant under the action of $k^\times$.

Hence j is defined on the sets of the proposition above.

Remark 14. Without the assumption $\operatorname{char} k \neq 2,3$ we can still carry out the above analysis, but it is less pleasant because not every Weierstrass equation is equivalent to a short one.

Proposition 15. *If* $k = \overline{k}$ *and* $\operatorname{char} k \neq 2,3$, *then* $j\colon (E,O)\,/\cong \to k$ *is a bijection.*

Proof. Let E_1, E_2 be elliptic curves given by Weierstrass equations $y^2 = x^3 + a_4x + a_6$ and $y^2 = x^3 + a_4'x + a_6'$, respectively. It suffices to show that if $j(E_1) = j(E_2) = j$, then there is a $u \in k^\times$ with $(a_4,a_6) = u(a_4',a_6')$. Either the common value $j = 0$, in which case $a_4 = 0 = a_4'$, so with $u = (a_6'/a_6)^{1/6}$ we have $u(a_4',a_6') = (0, u^{-6}a_6') = (0,a_6) = (a_4,a_6)$. Or the common value $j \neq 0$, in which case the equality of j-invariants imply that

$$\frac{a_6^2}{a_4^3} = \frac{a_6'^2}{a_4'^3} \implies \left(\frac{a_6}{a_6'}\right)^2 = \left(\frac{a_4}{a_4'}\right)^3.$$

Taking $u = \left(\frac{a_4}{a_4'}\right)^{1/4}$, we see that $\frac{a_6}{a_6'} = \pm u^6$. Adjusting u by a fourth root of unity, if necessary, we get a u that works. □

Note that the above proposition is not true if $k \neq \overline{k}$: There exists E_1, E_2 such that $E_1 \ncong E_2$ over k, but $E_1 \cong E_2$ over $\overline{k}$. In this case, we say that E_2 is a *twist* of E_1.

Example 16. Let $E_n : y^2 = x^3 - n^2$. Then $E_n \cong E_{n'}$ over $\mathbb{Q}$ if and only if $n^2/n'^2 \in \left(\mathbb{Q}^\times\right)^4$, if and only if $n/n' \in \left(\mathbb{Q}^\times\right)^2$.

3.1. **Elliptic curves as proper smooth group varieties of dimension 1.** The goal for the remainder of today is to prove that the data of an elliptic curve (E, O) is equivalent to the data of a proper smooth group variety of dimension 1.

There are two ways to get a group structure on (E, O):

(A) Geometrically by chord and tangent.
(B) By identification of E with $\operatorname{Pic}^0 E$.

We will not follow either approach strictly, but combine the easy parts from both. Approach (A) has the merit that it is clearly algebraic, but not obviously a group operation. Method (B) has the opposite problem, namely that it is obviously a group, but not necessarily given by regular functions. The path with minimal resistance is to define both operations and check that they are equal. The common operation is then algebraic and a group operation.

For method (A), consider the example of $y^2 = x^3 + x$.

Insert picture

The group operation is given as follows. Given closed points $P, Q \in E$, let l_{PQ} be the line in $\mathbb{P}^2$ passing through P, Q. Then $l_{PQ} \cap E$ consists of three points: P, Q and another point R'. Now the line passing through R' and O again intersects E in three points O, R', R, and we define

$$P \oplus Q = R.$$

The resulting map $(P, Q) \mapsto P \oplus Q$ is clearly algebraic, as we will now show. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Then $l_{PQ} : y = \lambda x + \mu$, where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\mu = y_1 - \lambda$. To get the third point R', note that $x(R')$ is the third root of $(\lambda x + \mu)^2 = x^3 + a_4 x + a_6$. This has roots x_1, x_2 by design, so

$$x(R') = -x_1 - x_2 + \lambda^2.$$

And $y = \lambda x + \mu$, so this is clearly algebraic.

For method (B), we will define an operation on $E(\overline{k})$.

Proposition 17. *The Abel-Jacobi map*

$$\begin{aligned} \mathrm{AJ} \colon E(\overline{k}) &\to \operatorname{Pic}^0 E = \left\{\mathcal{L} \text{ line bundle on } E_{\overline{k}}\right\}/iso \\ P &\mapsto \mathcal{O}\left(P - O\right) \end{aligned}$$

is a bijection.

Remark 18. If C is a positive genus curve, and $O \in C$, then we can define the Abel-Jacobi map in the same way as above, and it is always an injection. In fact, the reason why the Abel-Jacobi map is not manifestly algebraic is that $\operatorname{Pic}^0 C$ is only an abstract group. It is a fact that one can promote the Picard group $\operatorname{Pic}^0 C$ to a group variety, and the general theory will tell you that the Abel-Jacobi map is a closed embedding. But it is never a bijection if the C has genus $g > 1$.

Proof. For injectivity, suppose $P, Q \in E(\overline{k})$ with the properties that $\mathcal{O}\left(P - O\right) \cong \mathcal{O}\left(Q - O\right)$. Then $\mathcal{O}\left(P - Q\right) \cong \mathcal{O}_E$, so $H^0\left(E_{\overline{k}}, \mathcal{O}\left(P - Q\right)\right) = \overline{k}$. So there exists $f \in K(E)$ such that $\operatorname{div}(f) + P - Q \geq 0$. But the $\deg f = 0$, so the map $f \colon E \to \mathbb{P}^1$ has $f^{-1}\left\{0\right\} = \left\{Q\right\}$ and $f^{-1}\left\{\infty\right\} = \left\{P\right\}$, both the zero and pole of multiplicity one. This tells you that f is an isomorphism, because f is of degree 1. This is a contradiction.

For surjectivity, let $\mathcal{L} = \mathcal{O}(D)$ with $\deg D = 0$. We need to find P such that $\mathcal{L} \cong \mathcal{O}\left(P - O\right)$. Consider $\mathcal{O}\left(D + O\right)$, which is of degree 1. By Riemann-Roch, using the fact that E has genus 1,

$\dim H^0(E, \mathcal{O}(D+O)) = 1$. So there exists $f \in K(E)$ such that $\operatorname{div} f + D + O \geq 0$. The degree of this divisor is 1, so the only possibility is that $\operatorname{div} f + D + O = P$ for some $P \in E(\overline{k})$. This tells you that $\mathcal{O}(D) \cong \mathcal{O}(P - O)$. □

The conclusion is that we have a group operation on $E(\overline{k})$ characterized by $R = P \oplus Q$ if and only if $\mathcal{O}(R - O) \cong \mathcal{O}(P - O) \otimes \mathcal{O}(Q - O)$, if and only if $\mathcal{O}(P + Q - R) \cong \mathcal{O}(3O)$. Equivalently, the group operation is characterized by $P \oplus Q \oplus R' = 0$ if and only if $\mathcal{O}(P + Q + R') \cong \mathcal{O}(3O)$.

It remains to check that the operation $(P, Q) \mapsto P \oplus_B Q$ coincides with $(P, Q) \mapsto P \oplus_A Q$. The operation $\oplus_A$ is characterized by the property that $P \oplus_A Q \oplus_A R' = 0$ if and only if P, Q, R are colinear.

Insert picture

Recall the embedding $E \hookrightarrow \mathbb{P}\left(H^0(E, \mathcal{O}(3O))\right)$. A global section of $H^0(E, \mathcal{O}(3O))$ describes a hyperplane H in this projective space. Now $E \cap H$ is the zero locus of the corresponding section, and any two such intersections are linearly equivalent, because the ratio of two global sections is a meromorphic function. Thus, P, Q, R are colinear in $\mathbb{P}^2$ if and only if $P + Q + R = \operatorname{div} f + 3O$.

For the remainder, let us sketch why a proper smooth group variety of dimension 1 must have genus 1. The idea is that for a Lie group, the tangent bundle is trivial, because given a basis for the tangent space at a point can be translated using the group operation to a basis for the tangent space at any other point. If G is a curve which is a group, the algebro geometric version of this statement is that $\Omega^1_G \cong \mathcal{O}_G$, or equivalently the tangent sheaf $\left(\Omega^1_G\right)^\vee$ is trivial. And the genus is the dimension of global sections of that, which is 1.

4. Lecture 4 (Wednesday 1/20)

Let us recap what we defined the group law on an elliptic curve in two different ways:

(1) Via chords and tangents. To add two points P and Q, take the line through P, Q and let R' be the point where this line intersects E. Now take the line through O, R' and let R be the point where this line intersects E. Then $P \oplus Q = R$.
(2) More intrinsic description. Now $P \oplus Q$ is characterized by $\mathcal{O}(O) \otimes \mathcal{O}(P \oplus Q) \cong \mathcal{O}(P) \otimes \mathcal{O}(Q)$, i. e. the map $E \to \operatorname{Pic}^0 E$ given by $P \mapsto \mathcal{O}(P - O)$ is a group homomorphism.

We saw that these group laws coincide, by verifying that both operations are characterized by

$$P \oplus Q \oplus R = 0 \text{ if and only if } P, Q, R \text{ are colinear.}$$

We also made the claim:

Proposition 19. *The only proper smooth group variety of dimensioon 1 are elliptic curves.*

Properness is essential, because $\mathbb{G}_m$ and $\mathbb{G}_a$ satisfy the other properties.

Proof. We'll show that $\Omega^1_{G/k} \cong \mathcal{O}_G$. As the case of Lie groups, the idea is to choose a trivialization at a point and translate this to any other point using the group operation.

$$\begin{tikzcd}
G \times G \arrow[r, "(\mathrm{pr}_1, m)", "\cong"'] \arrow[dr, "\mathrm{pr}_1"'] & G \times G \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\mathrm{pr}_1"] & G \arrow[d] \\
& G \arrow[r] & \operatorname{Spec} k
\end{tikzcd}$$

The right hand square is clearly Cartesian, so we get another Cartesian square using the isomorphism on the left. Now use the fact that formation of relative differentials commutes with base change:

$$\Omega^1_{G \times G/\mathrm{pr}_1} \cong \mathrm{pr}_2^* \, \Omega^1_{G/k} \qquad \text{(inner square)}$$
$$\Omega^1_{G \times G/\mathrm{pr}_1} \cong m^* \Omega^1_{G/k}. \qquad \text{(outer square)}$$

In sum, $m^*\Omega^1_{G/k} \cong \mathrm{pr}_2^*\,\Omega^1_{G/k}$. Now pull back via the map $\phi\colon G \to G \times G$, with $\phi(g) = (g, e)$. Since $\mathrm{pr}_2 \circ \phi = e$ is constant and $m \circ \phi = \mathrm{id}$, we obtain finally

$$e^*\mathcal{O}_G \cong \phi^*\,\mathrm{pr}_2^*\,\Omega^1_{G/k} \cong \phi^* m^* \Omega^1_{G/k} \cong \Omega^1_{G/k}.$$

If G is smooth, then $e^*\Omega^1_{G/k} \cong \mathcal{O}_G^{\oplus d}$, where $d = \dim G$. □

Remark 20. The proof shows that $\Omega^1_{G/k}$ is a trivial vector bundle of rank $\dim T_e G$. Properness is only needed to show that G has genus 1.

4.1. **Isogenies.**

Definition 21. An *isogeny* $\phi\colon (E, O) \to (E', O')$ is a morphism of curves $\phi\colon E \to E'$ such that $\phi(O) = O'$.

Remark 22. Some people insist that isogenies must be non-constant.

There are two basic cases:

(1) ϕ is constant, in which case $\phi(E) = \{O'\}$.
(2) ϕ is non-constant. Then ϕ is necessarily finite, flat, surjective, and $\phi\colon E \to E'$ is a branched covers of curves.

For a branched cover of curves, there is anotion of degree:

$$\begin{aligned} \deg\phi &= \dim_k \phi^{-1}\{x\} && \text{for any } x \in E' \\ &= \text{total degree of points in } \phi^{-1}\{x\} \text{ counted with multiplicity} \\ &= \dim\,(\phi_*\mathcal{O}_E)_x \otimes_{\mathcal{O}_{E',x}} \kappa(x) \\ &= \operatorname{rank}\phi_*\mathcal{O}_E. \end{aligned}$$

Degree is multiplicative: $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$.

Example 23. Let $E : y^2 = x^3 + x$, and define $\phi\colon E \to E$ by $(x, y) \mapsto (-x, iy)$. This is well-defined because $(iy)^2 = -y^2 = -x^3 - x = (-x)^3 + (-x)$. This isogeny has degree 1 because it is an automorphism. Indeed, $\phi = [i]$ is "multiplication by i", and $\phi^2 = [i]^2 = [-1]$, which sends $(x, y) \mapsto (x, -y)$.

Example 24. Multiplication by $[2]\colon E \to E$ given by $P \mapsto P \oplus P$. If E is given by $y^2 = x^3 + ax + b$, and in Silverman you can find the formula for this map in coordinates:

$$(x, y) \mapsto \left(\frac{(3x^2 + a)^2 - 8xy^2}{4y^2}, \frac{42xy^2\left(3x^2 + a\right) - (3x^2 + a)^3 - 8y^5}{8y^3} \right).$$

We have a commutative diagram

$$\begin{tikzcd} E \arrow[r, "{[2]}"] \arrow[d, "x"] & E \arrow[d, "x"] \\ \mathbb{P}^1 \arrow[r] & \mathbb{P}^1, \end{tikzcd}$$

where the bottom map is

$$x \mapsto \frac{(3x^2 + a^2) - 2x}{4(x^3 + ax + b)}.$$

This map has degree 4, because it is given by the ratio of two degree 4 polynomials that are coprime. The degree of x is 2 (because for a given x there are generically two choices for y), so by multiplicativity of degree it follows that

$$\deg[2] = 4.$$

This is still true if $\mathrm{char}\, k = 2$.

Example 25. Suppose $\operatorname{char} k = p > 0$. If X is a scheme over k, then the *absolute Frobenius* $F_X : X \to X$ raises all functionos to the p'th power. This is a morphism of schemes, but it is not defined over k. Instead we have the commutative diagram

$$\begin{tikzcd}
X \arrow[r, "F_X"] \arrow[d] & X \arrow[d] \\
\operatorname{Spec} k \arrow[r, "F_k"] & \operatorname{Spec} k.
\end{tikzcd}$$

There is now another commutative diagram

$$\begin{tikzcd}
X \arrow[r, dashed, "F_{X/k}"] \arrow[rr, bend left, "F_X"] \arrow[dr] & X^{(p)} \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner"] & X \arrow[d] \\
 & \operatorname{Spec} k \arrow[r, "F_k"] & \operatorname{Spec} k,
\end{tikzcd}$$

where $X^{(p)}$ is defined to be the pullback in the right hand square, and $F_{X/k}$ is the unique map making the diagram commute. The map $F_{X/k}$ is called the *relative Frobenius*, and it *is* defined over k.

As a concrete example, consider an elliptic curve $E : y^2 = x^3 + ax + b$. The standard affine open is then Spec of $\frac{k[x,y]}{(y^2 - x^3 - ax - b)}$. The corresponding affine chart for $E^{(p)}$ is Spec of

$$\frac{k[x,y]}{(y^2 - x^3 - ax - b)} \otimes_{k,F_k} k \cong \frac{k[x,y]}{y^2 - x^3 - a^p x - b^p}.$$

In other words, $E^{(p)} : y^2 = x^3 + a^p x + b^p$. The relative Frobenius map is

$$\begin{aligned} F_{X/k} \colon E &\to E^{(p)} \\ (x,y) &\mapsto (x^p, y^p). \end{aligned}$$

Note that

$$(y^p)^2 = (y^2)^p = (x^3 + ax + b)^p = (x^p)^3 + a^p x^p + b^p,$$

so this is indeed well defined.

Note also that $F_{E/k}^{-1}\{O\}$ is supported at O.

The same technique we used to prove that [2] had degree 4 can be used to show that $F_{E/k}$ has degree p, using the fact that $\mathbb{P}^1 \to \mathbb{P}^1$, $x \mapsto x^p$ has degree p. We are in the situation that the for any point $z \in E^{(p)}$, the preimage $F_{E/k}^{-1}\{z\}$ is supported at a single point of E. (The reason is essentially that in $\overline{k}$ any element has a *unique* p-th root.) It follows that $\dim_k F_{E/k}^{-1}\{z\} = p$ for any $z \in E^{(p)}$. In particular, $F_{X/k}$ is ramified everywhere! (Note that this can't happen in characteristic zero.) In fact, $F_{X/k}$ is the minimal isogeny with this property, in the sense that if $\phi \colon E \to E'$ is another isogeny that is ramified at a point (or equivalently ramified everywhere, as we will see), then there is a unique dashed arrow making the diagram

$$\begin{tikzcd}
E \arrow[rr, "\phi"] \arrow[dr, "F_{E/k}"'] & & E' \\
 & E' \arrow[ur, dashed] &
\end{tikzcd}$$

commute. Such a ϕ is known as an *inseparable isogeny.*

Recall that there is a dictionary between irreducible smooth projective curves over k and function fields over k, i. e. finitely generated field extensions of k of transcendence degree 1:

$$\begin{gathered} C \mapsto K(C) \\ [\phi \colon C \to C' \text{ non-constant}] \mapsto [\phi^* \colon K(C') \hookrightarrow K(C)] \end{gathered}$$

Definition 26. An isogeny $\phi \colon E \to E'$ is *(in)separable* if $\phi^* \colon K(E') \hookrightarrow K(E)$ is (in)separable. *Purely inseparable* means that for all $f \in K(E)$, some $f^{p^n} \in K(E')$.

Under this dictionary, the Frobenius $F_{C/k} \colon C \to C^{(p)}$ corresponds to $F_{C/k}^* K(C^{(p)}) = K(C)^p \subseteq K(C)$, which indeed has degree p.

Corollary 27. *Any inseparable map $C \to D$ factors through Frobenius.*

Proof. If $K(D) \subseteq K(C)$ is inseparable, then $K(D) \subseteq K(C)^p \subseteq K(C)$. □

4.2. **Rigidity.**

Proposition 28. *Any isogeny $\phi\colon E \to E'$ is a group homomorphism. That is, $\phi\,(P \oplus Q) = \phi\,(P) \oplus \phi\,(Q)$.*

Key input:

Lemma 29 (Rigidity)**.** *Let X, Y be irreducible proper varieties over k. Fix $x_0 \in X$ and $y_0 \in Y$. If $f\colon X \times_k Y \to Z$ satisfies $f\,(X \times_k \{y_0\}) = f\,(\{x_0\} \times_k Y) = z_0$, then f is constant.*

This implies the proposition, because the map

$$\begin{aligned} f\colon E \times E &\to E' \\ (P, Q) &\mapsto \phi(P \oplus Q) \ominus \phi(P) \ominus \phi(Q) \end{aligned}$$

has the property that $f(E \times \{O\}) = f(\{O\} \times E) = \{O'\}$, so is constant by the Rigidity Lemma.

Proof of Rigidity Lemma.

Proof by picture

Let $U \subseteq Z$ be an affine open containing z_0. Then $f^{-1}U \subseteq X \times_k Y$ is an open containing $X \times_k \{y_0\}$. Since Y is proper, $\mathrm{pr}_2\left(X \times Y \setminus f^{-1}U\right)$ is closed in Y, Therefore, there is an open $V \subseteq Y$ containing y_0 such that the tube $X \times V \subseteq f^{-1}U$. For any $v \in V$, the image $f(X \times \{v\})$ is a point because there are no non-constant maps from a proper variety to an affine variety. This constant must be $f(x_0, v) = z_0$. This shows that that $f(X \times V) = \{z_0\}$.

Now observe that $\{y \in Y : f(X \times \{y\}) = \{z_0\}\}$ is closed, and open by the above argument. So it must be a connected component of Y, which is all of Y. □

Corollary 30. *Any proper group smooth group variety is commutative.*

Proof. The commutator map

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto ghg^{-1}h^{-1} \end{aligned}$$

collapses $G \times \{e\}$ and $\{e\} \times G$ to $\{e\}$. □

Corollary 31. *The group variety structure on an elliptic curve (E, O) is unique.*

Proof. Suppose $(E, \oplus_1)$ and $(E, \oplus_2)$ are group variety structures with the same identity O. Then the identity map $\mathrm{id}\colon E \to E$ sends O to O, so it is a group homomorphism by the proposition. □

5. Lecture 5 (Friday 1/22)

Last time we introduced the notion of an *isogeny* of elliptic curves, which is a map of curves $\phi\colon E \to E'$ such that $\phi(O) = O'$. There is a unique constant isogeny with $\phi(E) = O'$, and a non-constant isogeny $\phi\colon E \to E'$ is automatically surjective, finite, and flat.

By rigidity an isogeny is automatically a group homomorphism: $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$. A consequence of this is that

$$\ker \phi = \phi^{-1}\{O'\} = E \times_{E'} O'$$

is a subgroup of E. Another consequence is that a non-constant isogeny is "homogeneous", in the sense that for any $x \in E'$ we have $\phi^{-1}x \cong \phi^{-1}O$, with the isomorphism being realized by translation by a point $y \in E$ with $\phi(y) = x$. In particular, if ϕ is ramified at some point, then ϕ is ramified everywhere.

This can't happen in characteristic zero, but as we saw last time the Frobenius is such a everywhere ramified isogeny in characteristic p.

Remark 32. Any map of curves $\phi\colon E \to E'$ can be factored as $\phi = \text{translation} \circ \text{isogeny}$. In particular, $\operatorname{Aut}_{\text{curve}}(E) = E \rtimes \operatorname{Aut}_{\text{group variety}}(E)$.

Recall the definition of an (in)separable isogeny $\phi\colon E \to E'$: it is an isogeny for which the corresponding field extension $\phi^*\colon K(E') \hookrightarrow K(E)$ is (in)separable.

Proposition 33. *Let $\phi\colon E \to E'$ be a non-constant isogeny. The following are equivalent:*

(1) ϕ is separable.
(2) ϕ is unramified, i. e. étale.
(3) $d\phi_O\colon T_O E \to T_{O'} E$ is an isomorphism.
(4) $\# \ker \phi(\overline{k}) = \deg \phi$, i. e. $\ker \phi$ is reduced.
(5) $\overline{k}(E)/\phi^* \overline{k}(E)$ is a Galois extension (with Galois group $\ker \phi(\overline{k})$).

Proof. (2) is equivalent to (3). Let $y \in E$, $x = \phi(y)$, and let π_y, π_x be uniformizers at y, x. Then there exists an integer e such that $\phi^* \pi_x = \text{unit} \cdot \pi_y^e$, and ϕ being unramified at y means that $e = 1$. We have to check that ϕ is unramified at O if and only if $d\phi_O \neq 0$. But $d\phi_O$ is dual to $\phi^*\colon \pi_{O'}/\pi_{O'}^2 \to \pi_O/\pi_O^2$, so $e > 1$ if and only if $d\phi_O = 0$. Once ϕ is unramified at O, ϕ is unramified everywhere by using translations.

(2) implies (4). If ϕ is unramified, then $\#\phi^{-1}\left\{x\right\} = \deg \phi$, because the degree counts the number of points in the fiber with multiplicity, and being unramified means that there is no multiplicity.

(4) implies (5). We have seen that $\overline{k}(E)/\phi^* \overline{k}(E')$ is an extension of degree $\deg \phi$. Note that translation by $p \in \ker \phi(\overline{k})$, denoted t_p, induces an automorphism of the map ϕ:

$$\begin{tikzcd}
E \arrow[rr, "t_p", "\cong"'] \arrow[dr, "\phi"'] & & E \arrow[dl, "\phi"] \\
& E'. &
\end{tikzcd}$$

Therefore, we get a map $G = \ker \phi(\overline{k}) \to \operatorname{Aut}\left(\overline{k}(E)/\phi^* \overline{k}(E)\right)$. Distinct p induces different automorphisms, so this map is injective. The order of G is $\deg \phi$, which is the order of the extension $\overline{k}(E)/\phi^* \overline{k}(E)$, so G must be an isomorphism and the extension Galois.

(5) implies (1). Clear, because Galois extensions are separable.

(1) implies (2)/(3). Note that ϕ being separable is equivalent to the preimage of the generic point $\phi^{-1}\left\{\overline{k}(E')\right\}$ being reduced. This is because in general, a finite extension $\operatorname{Spec} L \to \operatorname{Spec} K$, then L/K is separable if and only if $L \otimes_K \overline{K}$ is reduced. So if ϕ is separable, then it is unramified at the generic point, and therefore unramified everywhere.

Alternatively, ϕ being separable is equivalent to the trace pairing $\overline{k}(E) \otimes \overline{k}(E) \to \phi^* \overline{k}(E')$ being non-degenerate. Once this is non-degenerate, we can find an affine open $\operatorname{Spec} R \subseteq E'$ with inverse image $\operatorname{Spec} S \subseteq E$ such that $\operatorname{tr}\colon R \otimes R \to S$ is also non-degenerate, i. e. $\operatorname{disc}_{R/S} \in S^\times$. □

Corollary 34. *The multiplication by n map $[n]\colon E \to E$ is a separable isogeny if and only if n is coprime to* $\operatorname{char} k$.

Proof. Let $m\colon E \times E \to E$ be the multiplication map. Then

$$\begin{aligned} dm_{(O,O)}\colon T_O E \times T_O E &\to T_O E \\ (u, v) &\mapsto u + v \end{aligned}$$

is the addition map, because it is linear and restricts to the identity on $T_O E \times 0$ and $0 \times T_O E$. It follows that $d[n]_O$ is precisely multiplication by n. □

Note that we don't know yet when $[n]$ is non-constant if $\operatorname{char} k$ divides n.

Remark 35. The proof of the above proposition shows that

$$\{\text{separable isogenies } \phi\colon E \to E' \text{ over } \overline{k}\} \cong \{\text{finite subgroups } G \subseteq E(\overline{k})\}$$

$$\{\text{separable isogenies } \phi\colon E \to E' \text{ over } k\} \cong \left\{ \begin{array}{l} \text{finite subgroups } G \subseteq E(\overline{k}) \text{ which are} \\ \text{stable under the action of } \operatorname{Gal}(\overline{k}/k) \end{array} \right\}$$

$$\phi \mapsto \ker \phi(\overline{k})$$

$$\overline{k}(E)/\overline{k}(E)^G \leftarrow\!\shortmid G.$$

Actually, this bijection can be extended to cover inseparable isogenies as well, if you enhance the right hand side to finite subgroup schemes $G \subseteq E$. (The reason is that *reduced* schemes are determined by $\overline{k}$-points.) The main subtelty in this correspondence is that given $G \subseteq E$ a finite subgroup scheme, we need to construct the categorical quotient $E' = E/G$. In particular, this gives a convenient way to check when something factors through $\varphi\colon E \to E/G$. That is, a map $f\colon E \to C$ factors through φ if and only if $f(x+p)f(x)$ for all $p \in \ker \phi$. Note that E/G is necessarily of genus 1, because $\chi(E) = \deg \varphi \chi(E/G) = 0$.

Definition 36. Define $\operatorname{Hom}(E, E') = \{\text{isogenies } \varphi\colon E \to E'\}$ and $\operatorname{End}(E) = \{\text{isogenies } \varphi\colon E \to E\}$. These inherit a group structure from the target, and moreover $\operatorname{End}(E)$ is a ring. Also, define $\operatorname{Hom}^0(E, E') = \operatorname{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\operatorname{End}^0(E) = \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 37. $\operatorname{End}^0(E)$ *is a characteristic zero domain.*

Proof. It is clear that this is a domain, because $\deg\colon \operatorname{End}(E) \to \mathbb{Z}_{\geq 0}$ is multiplicative and $\deg \phi = 0$ if and only if $\deg \phi$ is constant. That it is characteristic zero means that $[n] \neq 0$ for all $n \in \mathbb{Z}_{>0}$. The "immoral" proof of this fact is the following. We already showed that $\deg[2] = 4$. Suppose that $[n] = 0$. Then we can factor out powers of 2 dividing n, and assume that n is odd. But then n divides some $2^M - 1$, in which case $[2^M] = [1]$, which is a contradiction because the degrees don't match. □

At this point, we don't know what $\deg[n]$ is! It turns out that $\deg[n] = n^2$. To show this, we need to analyze the effect of isogenies on line bundles.

The basic question is the following: Given an isogeny $\phi\colon E \to E'$, what does $\phi^*\colon \operatorname{Pic} E' \to \operatorname{Pic} E$ do? This is not obvious!

$$\phi^*\mathcal{O}(x) = \mathcal{O}(\phi^{-1}x))???$$

In particular,

$$(\phi + \psi)^* \mathcal{O}(x) = \mathcal{O}\left((\phi + \psi)^{-1}\{x\}\right)???$$

This does not interact nicely with $\phi^{-1}\{x\}$ and $\psi^{-1}\{x\}$. There is one fundamental fact that allows you to deal with this for elliptic curves and more generally abelian varieties.

Theorem 38 (of the Square)**.** *If $\phi, \psi\colon E \to E'$ and $\mathcal{L} \in \operatorname{Pic}(E')$, then*

$$(\phi + \psi)^*\mathcal{L} \otimes (\phi - \psi)^*\mathcal{L} \cong (\phi^*\mathcal{L})^{\otimes 2} \otimes \psi^*\mathcal{L} \otimes (-\psi)^*\mathcal{L}.$$

Remark 39. This is actually a consequence of the Theorem of the Cube. In higher dimensions, the proof of the Theorem of the Square is to prove the Theorem of the Cube.

Remark 40. The Theorem of the Square will be crucial to understand the effect of $(\phi + \psi)^*$.

Remark 41. Why is it called the Theorem of the Square? Because ϕ^* is like a quadratic function, and the Theorem of the Square is like the parallelogram law: $(\phi + \psi)^2 + (\phi + \psi)^2 = 2\phi^2 + \psi^2 + (-\psi)^2$.

Corollary 42. *(1) If $\mathcal{L}$ is symmetric, meaning that $[-1]^*\mathcal{L} \cong \mathcal{L}$, then $[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes n^2}$.*

(2) If $\mathcal{L}$ is anti-symmetric, meaning that $[-1]^*\mathcal{L} \cong \mathcal{L}^{\otimes(-1)}$ (and which turns out to be equivalent to $\deg \mathcal{L} \geq 0$), then $(\phi + \psi)^*\mathcal{L} \cong \phi^*\mathcal{L} \otimes \psi^*\mathcal{L}$.

Proof.

(1) If $\phi = [n]$ and $\psi = [-1]$, the Theorem of the Square becomes

$$[n+1]^*\mathcal{L} \otimes [n-1]^*\mathcal{L} \cong ([n]^*\mathcal{L})^{\otimes 2} \otimes \mathcal{L}^{\otimes 2}.$$

In particular, for $n = 1$, we see that $[2]^*\mathcal{L} \cong \mathcal{L}^{\otimes 4}$, and inductively we can show that $[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes n^2}$.

What does this have to do with the degree of ϕ? Simply apply the above to a symmetric line bundle of positive degree. For example, if $\mathcal{L} = \mathcal{O}(P)$, we can "symmetrize" this line bundle by considering

$$\mathcal{L} \otimes [-1]^*\mathcal{L} \cong \mathcal{O}\left(P + (\ominus P)\right),$$

which has degree 2. So we can take a symmetric line bundle $\mathcal{L}$ of positive degree, and then

$$\deg \phi \deg \mathcal{L} = \deg \phi^*\mathcal{L} = \deg \mathcal{L}^{\otimes n^2} = n^2 \deg \mathcal{L},$$

so $\deg \phi = n^2$.

Remark 43. For an abelian variety of dimension d, $\deg[n] = n^{2d}$.

(2) If $\mathcal{L}$ is anti-symmetric, then

$$-\deg \mathcal{L} = \deg \mathcal{L}^{-1} = \deg[-1]^*\mathcal{L} = \deg \mathcal{L},$$

so $\deg \mathcal{L} = 0$. (The converse is also true for elliptic curves, because $[-1]^*\mathcal{O}(P - O) \cong \mathcal{O}((\ominus P) - O) \cong \mathcal{O}(P - O)^{\otimes(-1)}$.) The Theorem of the Square in this case becomes

$$(\phi + \psi)^*\mathcal{L} \otimes (\phi - \psi)^*\mathcal{L} \cong (\phi^*\mathcal{L})^{\otimes 2}.$$

If $A = \phi + \psi$ and $B = \phi - \psi$ this says that

$$A^*\mathcal{L} \otimes B^*\mathcal{L} \cong \left(\frac{A+B}{2}\right)^* \mathcal{L}.$$

What does it take for arbitrary A, B to be of the above form? If we can divide by 2, we could set $\phi = \frac{A+B}{2}$ and $\psi = \frac{A-B}{2}$. So (2) is at least true for *even* A, B, meaning for A, B of the form $A = 2A'$ and $B = 2B'$. But this implies the statement in general, because for *arbitrary* A, B, we have $(2A + 2B)^*\mathcal{L} \cong (2A)^*\mathcal{L} \otimes (2B)^*\mathcal{L}$, we know the effect of multiplying by 2, and since multiplication by 2 is surjective any degree zero line bundle $\mathcal{L} \cong \mathcal{O}\left(P - O\right)$ has a square root, that is there is a line bundle $\mathcal{L}'$ such that $\mathcal{L} \cong (\mathcal{L}')^{\otimes 2}$. □

6. Lecture 6 (Monday 1/25)

Last time we gave various characterizations for an isogeny to be separable. The most convenient one was that an isogeny $\phi\colon E \to E'$ is separable if and only if $(d\phi)_O \colon T_O E \to T_{O'} E'$ is non-zero (or equivalently an isomorphism because we are dimension 1). This is equivalent to $\phi\colon E \to E'$ being an unramified Galois cover (with Galois group $\ker \phi(\overline{k})$).

In general, $\phi\colon E \to E'$ identifies E' as the quotient $E/\ker\phi$. In the diagram

$$\begin{tikzcd} E \arrow[rr, "\phi"] \arrow[dr, "f"'] & & E' \arrow[dl, dashed] \\ & C & \end{tikzcd}$$

the dashed arrow exists if and only if f is invariant under translation by elements of $\ker\phi$.

We showed that $\mathrm{End}(E) = \{\text{isogenies } \phi\colon E \to E\}$ is a characteristic zero domain, and $[n] \neq 0$. To analyze $[n]$ further we studied the effect of $\phi^*\colon \mathrm{Pic}(E') \to \mathrm{Pic}(E)$. There are two basic cases:

(1) If $\mathcal{L}$ is symmetric, $[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes n^2}$.
(2) If $\mathcal{L}$ is anti-symmetric, $(\phi + \psi)^*\mathcal{L} \cong \phi^*\mathcal{L} \otimes \psi^*\mathcal{L}$.

Both facts are proved using the Theorem of the Square: If $\phi, \psi\colon E \to E'$, then pulling back behaves like a quadratic function, and we have a "parallelogram law"

$$(\phi + \psi)^*\mathcal{L} + (\phi - \psi)^*\mathcal{L} \cong (\phi^*\mathcal{L})^{\otimes 2} \otimes \psi^*\mathcal{L} \otimes (-\psi)^*\mathcal{L}.$$

Proof of the Theorem of the Square. The first step is reduction to a "universal case". Consider the 4 maps $p_1, p_2, d, m\colon E \times E \to E$ given by projections p_i, the difference $d(P, Q) = P \ominus Q$ and addition $m(P, Q) = P \oplus Q$.

Claim 44. *Let $\mathcal{L} \in \mathrm{Pic}(E)$. Then*

$$m^*\mathcal{L} \otimes d^*\mathcal{L} \cong (p_1^*\mathcal{L})^{\otimes 2} \otimes p_2^*\mathcal{L} \otimes (-p_2)^*\mathcal{L}.$$

This implies the Theorem of the Square, by pulling back the isomorphism via $(\phi, \psi)\colon E \to E' \times E'$. So it remains to prove the claim.

Let

$$\widetilde{\mathcal{L}} = m^*\mathcal{L} \otimes d^*\mathcal{L}(p_1^*\mathcal{L})^{\otimes(-2)} \otimes (p_1^*\mathcal{L})^{\otimes(-1)} \otimes ((-p_1)^*\mathcal{L})^{\otimes(-1)}.$$

We must prove that $\widetilde{\mathcal{L}}$ is trivial. Given a point Q in E, note that

$$\widetilde{\mathcal{L}}|_{E\times\{Q\}} \cong t_Q^*\mathcal{L} \otimes t_{-Q}^*\mathcal{L} \otimes \mathcal{L}^{\otimes(-2)},$$

where $t_{\pm Q}\colon E \to E$ is translation by $\pm Q$. A necessary condition of $\widetilde{\mathcal{L}}$ to be trivial is that $\widetilde{\mathcal{L}}|_{E\times\{Q\}}$ is trivial. And this is indeed holds: It suffices to cheack for $\mathcal{L} = \mathcal{O}(P)$, and

$$\begin{aligned}
t_Q^*\mathcal{O}(P) \otimes t_{-Q}^*\mathcal{O}(P) &\cong \mathcal{O}(P \oplus Q) \otimes \mathcal{O}(P \ominus Q)\\
&\cong \mathcal{O}(P \oplus Q - O) \otimes \mathcal{O}(P \ominus Q - O) \otimes \mathcal{O}(O)^{\otimes 2}\\
&\cong \mathcal{O}(P - O) \otimes \mathcal{O}(Q - O) \otimes \mathcal{O}(P - O) \otimes \mathcal{O}(Q - O)^{\otimes(-1)} \otimes \mathcal{O}(O)^{\otimes 2}\\
&\cong \mathcal{O}(P)^{\otimes 2},
\end{aligned}$$

as needed. In fact, we checked that for any map $i\colon \operatorname{Spec} K \to E$, where K is a field, $(1 \times i)^*\widetilde{\mathcal{L}}$ is trivial on $E \times \operatorname{Spec} K$. In particular, for $i\colon \operatorname{Spec} K(E) \to E$ the generic point of E.

Insert picture

So there is an isomorphism $\mathcal{O}_{E\times\operatorname{Spec} K(E)} \cong \widetilde{\mathcal{L}}|_{E\times\operatorname{Spec} K(E)}$. It follows that there exists an open dense $U \subseteq E$ such that $\mathcal{O}_{E\times U} \cong \widetilde{\mathcal{L}}_{E\times U}$. In other words, $\widetilde{\mathcal{L}}$ is trivial away from finitely many points $E \times \{P_i\}$. Therefore, the divisor class of $\widetilde{\mathcal{L}}$ is of the class of $\sum_i n_i E \times \{P_i\}$, and it follows that $\widetilde{\mathcal{L}} \cong p_2^*\mathcal{O}\left(\sum_i n_i P_i\right)$.

We have shown that $\widetilde{\mathcal{L}} \cong p_2^*\mathcal{N}$ for a line bundle $\mathcal{N} \in \operatorname{Pic}(E)$. But then

$$\mathcal{N} \cong \widetilde{\mathcal{L}}|_{\{O\}\times E} \cong \mathcal{L} \otimes [-1]^*\mathcal{L} \otimes \mathcal{L}^{\otimes(-1)} \otimes [-1]^*\mathcal{L}^{\otimes(-1)} \cong \mathcal{O}.$$

So $\widetilde{\mathcal{L}} \cong p_2^*\mathcal{O} \cong \mathcal{O}$. □

Remark 45. The same argument shows that whenever X, Y are irreducible smooth, $\mathcal{L}$ is a line bundle on $X \times Y$ such that $\mathcal{L}|_{X\times\eta}$ is trivial, where $\eta \in Y$ is the generic point, then $\mathcal{L} \cong p_2^*\mathcal{N}$ for some $\mathcal{N} \in \operatorname{Pic}(Y)$.

There is a better version of this statement, namely the *See-saw Theorem*: Let X be proper and Y finite type, reduced, connected. Let $\mathcal{L}$ be a line bundle on $X \times Y$. Then $\mathcal{L} \cong p_2^*\mathcal{N}$ if and only if $\mathcal{L}|_{X\times\{s\}}$ is trivial for every closed point s of Y.

Note that a line bundle on $X \times Y$ corresponds to a map $Y \to \operatorname{Pic}(X)$. So the See-saw Theorem is a statement about separatedness of $\operatorname{Pic}(X)$.

6.1. **Dual isogenies.** Let $\phi\colon E \to E'$ be an isogeny. There is an induced map $\phi^*\colon \operatorname{Pic}^0(E') \to \operatorname{Pic}^0(E)$ with $\mathcal{L} \mapsto \phi^*\mathcal{L}$. The Abel-Jacobi map gave an isomorphism $E(\overline{k}) \cong \operatorname{Pic}^0(E)$. So there is a unique $\hat{\phi}$ fitting into the diagram

Definition 46. The map $\hat{\phi}$ above is the *dual isogeny* of ϕ.

We should justify the terminology. Namely, we have described $\hat{\phi}$ on points, but we should verify that it is an isogeny.

Proposition 47. *There exists a unique isogeny $\hat{\phi}\colon E' \to E$ such that $\hat{\phi}|_{E(\overline{k})}$ agrees with the above definition.*

Remark 48. If we had promoted the Abel-Jacobi map to a morphism of *schemes*, this would be completely transparent.

Proof. The idea is to characterize $\hat{\phi}$ by

$$[\deg\phi] = \hat{\phi} \circ \phi.$$

Let us check that our definition satisfies this: Choose $P \in E(\overline{k})$, and let $Q = \phi(P)$. Then

$$\hat{\phi}(Q) = \mathrm{AJ}^{-1} \circ \phi^* \circ \mathrm{AJ}(Q) = \mathrm{AJ}^{-1}\left(\phi^* \mathcal{O}(Q - O)\right).$$

Now, using the fact that fibers of ϕ differ by translations via elements of $\ker \phi$,

$$\phi^*\mathcal{O}(Q-O) = \mathcal{O}(\phi^{-1}Q - \phi^{-1}O') = \mathcal{O}(\sum n_R(R \oplus P) - \sum n_R R) = \mathcal{O}(P-O)^{\otimes(\sum n_R)} = \mathrm{AJ}(P)^{\otimes \deg \phi}.$$

Taking AJ^{-1}, we see that our definition satisfies the condition.

To see that $\hat{\phi}$ exists, we have to show that $\hat{\phi}$ exists in the diagram

$$\begin{tikzcd}
E \arrow[rr, "\phi"] \arrow[dr, "{[\deg \phi]}"'] & & E' \arrow[dl, dashed, "\hat{\phi}"] \\
& E. &
\end{tikzcd}$$

This is equivalent to showing that $[\deg \phi]$ is invariant under translation by $\ker \phi$, i. e. that $[\deg \phi](\ker \phi) = 0$. But this is Lagrange's Theorem! In the separable case it is literally Lagrange's Theorem. One could also make sense of Lagrange's Theorem in the inseparable case, but alternatively, if $\phi = \mathrm{Frob}$ we can directly factorize,

$$\begin{tikzcd}
E \arrow[rr, "\mathrm{Frob}"] \arrow[dr, "{[p]}"'] & & E^{(p)} \arrow[dl, dashed, "\exists!"] \\
& E. &
\end{tikzcd}$$

The existence of $\hat{\phi}$ is stable under composition: $\widehat{\phi \circ \psi} = \hat{\phi} \circ \hat{\psi}$. And any ϕ is the composition of an inseparable and Frobenius. □

Summary of properties of the dual isogeny:

(1) $\widehat{\phi \circ \psi} = \hat{\phi} \circ \hat{\psi}$
(2) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.
(3) $\phi \circ \hat{\phi}, \hat{\phi} \circ \phi = [\deg \phi]$.
(4) $\deg \hat{\phi} = \deg \phi$

In particular, $\mathrm{End}(E)$ has a positive anti-involution $\hat{\cdot}$.

Remark 49. In higher dimension, given $\phi \colon A \to B$ there is a dual isogeny $\mathrm{Pic}^0(B) = \hat{B} \to \hat{A} = \mathrm{Pic}^0(A)$. But there are not isomorphisms $A \cong \hat{A}$ and $B \cong \hat{B}$ in general; this is a feature of dimension 1.

6.2. **Example: The Poncelet Porism.** Assume $\mathrm{char}\, k \neq 2$. Let $C_1, C_2 \subseteq \mathbb{P}^2$ be smooth conics (i. e. of degree 2) which are not tangent to each other. Let $P_1 \in C_1$, and consider the following process. Given P_k, draw the line l through P_k that is tangent to C_2, and let P_{k+1} be the other intersection point of l with C_1.

Insert picture

Proposition 50. *Whterh this process is periodic is independent of P.*

Example 51. Start with an equilateral triangle, let P be a vertex, C_1 the circumscribed circle and C_2 the inscribed circle. Then the process is evidently periodic (with period 3). The same is true if we had started with a regular n-gon instead of a triangle. More interestingly, if we started with say a random quadrilateral that has an incribed and circumscribed circle, this is still true, but not for obvious symmetry reasons.

Example 52. Take two circles centered at the same point. Then the process is not periodic for most ratios of radii.

Proof. Consider $\check{\mathbb{P}}^2 = \left\{\text{lines in } \mathbb{P}^2\right\}$. The dual conic to C_2 is

$$\check{C}_2 = \{\text{lines tangent to } C_2\} \subseteq \check{\mathbb{P}}^2,$$

which is also a smooth conic. Now consider

$$\widetilde{C} = \left\{(P,l) \in C_1 \times \check{C}_2 : P \in l\right\} \subseteq \mathbb{P}^2 \times \check{\mathbb{P}}^2.$$

In other words, $\widetilde{C}$ is the intersection of $C_1 \times \check{C}_2$ with the incidence plane $H = \left\{(P,l) \in \mathbb{P}^2 \times \check{\mathbb{P}}^2 : P \in l\right\}$. The point now is that

(1) $\widetilde{C}$ is a smooth projective curve.
(2) The genus of $\widetilde{C}$ is 1.

To check this, consider the projection map $\pi \colon \widetilde{C} \to C_1$. The fiber over a point $P \in C_1$ is given by

$$\pi^{-1}\{P\} = \{(P,l) : l \text{ tangent to } C_2 \text{ and } P \in l\}.$$

There are two lines l_1, l_2 tangent to C_2 that pass through P. So $\pi^{-1}\{P\}$ has two distinct points, unless $P \in C_1 \cap C_2$. In fact, π is a branched cover of degree 2, ramified at the 4 points where C_1 and C_2 intersect. The Riemann-Hurwitz formula then tells you that the genus of $\widetilde{C}$ is 1.

We can now describe the above process as follows: Consider the automorphism

$$\begin{aligned} \tau \colon \widetilde{C} &\to \widetilde{C} \\ (P,l) &\mapsto (P',l) \end{aligned}$$

that sends (P,l) to the other intersection of C_1 with l. The key point is now that τ has no fixed points (because C_1 is not tangent to C_2). Therefore, $\tau = t_M$ for some $M \in \widetilde{C}(\bar{k})$. Now $\tau^N = t_{[N]M}$. Either $\tau^N = \mathrm{id}$ for some N (or equivalently, M is torsion), or τ^N has no fixed points for all N. These two situations correspond to whether the process we described is periodic or not. □