Elliptic Curves

Hahn Lheem
Taught by Javier Fresán

Nov-Dec 2024

Contents

0 Preface

This class is one of the "Cours Fondamentaux I" of the M2 Mathématiques Fondamentales program at Sorbonne Université. Course times are Mondays from 9-11am and 1-3pm, and the TD (*travaux dirigés*) sessions are on Tuesdays from 4:10-6:10pm. The lectures are held at Sorbonne Université, Jussieu/Pierre and Marie Curie Campus. The main textbook is Silverman's *The Arithmetic of Elliptic Curves*. There will be a final exam for this course.

There are inevitably some errors in these notes. Any errors should be attributed to me, not the professor. If you see anything wrong or unclear, let me know at hahnlheem@gmail.com!

1 11/04 - Complex Elliptic Curves

1.1 Why do we care?

[1] It is difficult to understate the importance of elliptic curves in modern number theory. Andrew Wiles's proof of Fermat's Last Theorem boiled down to proving a statement about elliptic curves; in particular, he proved that every so-called semistable elliptic curve over $\mathbb{Q}$ "comes from" a modular form. One of the Millenium Problems, the Birch and Swinnerton-Dyer Conjecture, poses that the order of zero at $s = 1$ of the L-function $L(E, s)$ attached to an elliptic curve E over some number field K is equal to the rank of the group of K-points $E(K)$ on the elliptic curve. This is still a wide-open problem, although the cases where the order (and thus the rank) is 0 or 1 are proven using quite advanced machinery.

These two examples alone suggest that lots of unexpected arithmetic information can be extracted from the geometry of elliptic curves and the analytic properties of its L-functions. Considering elliptic curves over different kinds of fields ($\mathbb{C}$, finite extensions of $\mathbb{F}_p$, $\mathbb{Q}$, $\mathbb{Q}_p$) each yield their own beautiful and unexpected stories. We will study elliptic curves in these various settings, beginning with $\mathbb{C}$.

1.2 Elliptic Functions

First, we offer a definition of an elliptic curve, although we will not explain all terms just yet.

Definition 1.1 (Elliptic Curve)**.** An **elliptic curve** over a field K is a smooth projective curve over K of genus 1.

If $K = \mathbb{C}$, then how may one produce a smooth complex curve of genus 1? From topology, one example is a complex torus, which we can form by taking some paral-

[1] I actually missed this part of lecture, but I am supplying my own (terse) motivations here.

lelogram and identifying opposite edges. We can identify a parallelogram in $\mathbb{C}$ as the space of representatives for $\mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is some lattice. A good way to study some space is to study functions on that space, so we seek to understand meromorphic functions on $\mathbb{C}/\Lambda$. This is equivalent to studying meromorphic functions on $\mathbb{C}$ which are periodic with respect to some lattice. We now define these words.

Definition 1.2 (Lattice)**.** A **lattice** $\Lambda \subset \mathbb{C}$ is a discrete subgroup which contains an $\mathbb{R}$-basis of $\mathbb{C}$.

Let $\Lambda \subset \mathbb{C}$ be a lattice. By the above, we can write $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ for some $\mathbb{R}$-basis $\{\omega_1, \omega_2\}$ of $\mathbb{C}$. In other words, we require $\omega_1/\omega_2 \notin \mathbb{R}$.

Definition 1.3 (Fundamental Domain)**.** A **fundamental domain** for a lattice $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ is a subset of $\mathbb{C}$ of the form

$$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_i < 1,\ a \in \mathbb{C}\}.$$

Note by construction that every $z \in \mathbb{C}$ has a unique representative $z' \in D$ such that $z \equiv z' \pmod{\Lambda}$.

Definition 1.4 (Elliptic Function)**.** An **elliptic function** with respect to Λ is a meromorphic function f on $\mathbb{C}$, i.e., $f : \mathbb{C} \to \mathbb{P}^1(\mathbb{C})$, such that $f(z + \omega) = f(z)$ for all $z \in \mathbb{C}$, $\omega \in \Lambda$. We denote $\mathbb{C}(\Lambda)$ as the set of all such functions; this is a field.

Note that we study meromorphic functions because holomorphic elliptic functions are very restrictive. In fact, any elliptic function without a pole (resp., without a zero) is constant. This is because f is periodic with respect to Λ, so

$$\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\overline{D}} |f(z)| < \infty,$$

where the inequality follows because $\overline{D}$ is compact. The claim now follows from Liouville's Theorem.

The elliptic criterion comes with enough restrictions of its own, which lends to the study of complex elliptic curves being so elegant.

Theorem 1.5. Let $f \in \mathbb{C}(\Lambda)^\times$ and D be a fundamental domain for Λ. Then,

1. $\sum_{x\in D} \operatorname{Res}_x(f) = 0$;
2. $\sum_{x\in D} \operatorname{ord}_x(f) = 0$;
3. $\sum_{x\in D} \operatorname{ord}_x(f) \cdot x \in \Lambda$.

Proof. Note that f is defined the same for all choices of fundamental domain, we can arbitrarily choose D. We will choose D such that there are no zeros or poles on ∂D.

(This is possible because the poles and zeros should be isolated by standard complex analysis.) Let the vertices of D be $\{a, a+\omega_1, a+\omega_2, a+\omega_1+\omega_2\}$.

The first statement is an application of the Residue Theorem, which tells us

$$\sum_{x\in D} \mathrm{Res}_x(f) = \frac{1}{2\pi i}\int_{\partial D} f(z)\,dz,$$

which we can decompose as

$$\int_{\partial D} f(z)\,dz = \int_a^{a+\omega_1} f(z)\,dz + \int_{a+\omega_1}^{a+\omega_1+\omega_2} f(z)\,dz + \int_{a+\omega_1+\omega_2}^{a+\omega_2} f(z)\,dz + \int_{a+\omega_2}^{a} f(z)\,dz.$$

Consider the second integral on the right. Translating by $-\omega_1$ gives

$$\int_{a+\omega_1}^{a+\omega_1+\omega_2} f(z)\,dz = \int_a^{a+\omega_2} f(z-\omega_1)\,dz = \int_a^{a+\omega_2} f(z)\,dz,$$

which cancels out with the fourth integral. Likewise, the third integral cancels with the first, so indeed $\sum \mathrm{Res}_x(f) = 0$.

The second statement follows directly from the first. Indeed, if f is elliptic, then f'/f is also elliptic, and the result follows from $\mathrm{Res}_x(f'/f) = \mathrm{ord}_x(f)$.

For the third statement, the key idea is to use the fact $\mathrm{ord}_x(f)\cdot x = \mathrm{Res}_x(z\cdot f'(z)/f(z))$. Note that the function inside the parentheses on the right is not an elliptic function! But by the Residue Theorem, we always have

$$\begin{aligned}\sum_{x\in D} \mathrm{ord}_x(f)\cdot x &= \frac{1}{2\pi i}\int_{\partial D} z\frac{f'(z)}{f(z)}dz \\ &= \frac{\omega_1}{2\pi i}\int_a^{a+\omega_2}\frac{f'(z)}{f(z)}dz - \frac{\omega_2}{2\pi i}\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}dz.\end{aligned}$$

It must be true that $\frac{1}{2\pi i}\int_a^{a+\omega_2}\frac{f'(z)}{f(z)}dz \in \mathbb{Z}$. This is the case because if $\gamma:[0,1]\to\mathbb{C}^\times$ is a closed loop, then $\int_\gamma \frac{dz}{z} \in 2\pi i\mathbb{Z}$. We then use this on the path $\gamma(t) = f(a+t\omega_2)$ to get $\sum \mathrm{ord}_x(f) \in \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \Lambda$. □

Corollary 1.6. *A non-constant elliptic functions has at least two poles, counting multiplicity.*

Proof. If f has only one simple pole at x, then $\mathrm{Res}_x(f) = 0$ by formula (1) above. Thus, f is holomorphic, hence constant. □

1.3 The Weierstrass $\wp$-function

Let $\Lambda \subset \mathbb{C}$ be a lattice. Define the **Eisenstein series of weight** $2k$ as

$$G_{2k}(\Lambda) = \sum_{0\neq w\in\Lambda} \frac{1}{w^{2k}}.$$

This is clearly elliptic. The problem with this when $k = 1$ is that we can no longer guarantee convergence. We get around this by defining the special function which is the **Weierstrass $\wp$-function**:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{0 \neq w \in \Lambda} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Proposition 1.7. These functions are absolutely convergent. In particular,

1. $G_{2k}(\Lambda)$ absolutely converges for $k > 1$.
2. $\wp_\Lambda$ absolutely and uniformly converges on all compact subsets of $\mathbb{C} - \Lambda$.
3. $\wp_\Lambda$ is an even elliptic function with a double pole of residue 0 on all lattice points of Λ.

Proof. For absolute convergence of the Eisenstein series, we will write

$$G_{2k}(\Lambda) = \sum_{0<|w|<1} \frac{1}{w^{2k}} + \sum_{|w| \geq 1} \frac{1}{w^{2k}}.$$

The first sum clearly converges (it is a finite sum), while we can bound the second by

$$\sum_{|w| \geq 1} \frac{1}{|w|^{2k}} \leq \sum_{N=1}^{\infty} \frac{\#\{w \in \Lambda : N \leq |w| < N+1\}}{N^{2k}}.$$

But the numerator can be bounded linearly in terms of N (roughly, this follows from $(N+1)^2 - N^2$ being linear in N), so the sum on the right in turn is bounded above by $\sum_{N \geq 1} c/N^{2k-1}$, which we know converges for $k > 1$.

For (2), we employ something similar. We split up the sum into two sums, the first ranging over $|w| \leq 2|z|$ and the second over $|w| > 2|z|$. Again, the first sum is finite, while for $|w| > 2|z|$, we have

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| = \frac{|z||2z-w|}{|w|^2|z-w|^2} \leq \frac{10|z|}{|w|^3}$$

since $|w| > 2|z| \implies |z-w| \geq |w|/2$ and $|2w - z| \leq \frac{5}{2}|w|$. On compact subsets, $|z|$ is bounded, and the result follows because the sum $\sum_{0 \neq w \in \Lambda} |w|^{-3}$ converges absolutely and uniformly.

For the last part, the evenness and statement about the double poles with residue 0 are evident. It remains to show $\wp_\Lambda(z)$ is elliptic. We do this by showing that the derivative $\wp'(z)$ is elliptic first. We have

$$\wp'_\Lambda(z) = -2 \sum_{w \in \Lambda} \frac{1}{(z-w)^3},$$

which is clearly elliptic. Thus, we have $\wp_\Lambda(z+w) = \wp_\lambda(z) + C(w)$ for some function C on w. But using $z = -w/2$ gives $\wp_\Lambda(w/2) = \wp_\Lambda(-w/2) + C(w)$; from evenness of $\wp_\Lambda$, it follows that $C(w) = 0$ so $\wp_\Lambda$ is elliptic. □

Just like how all singly-periodic functions can be written in terms of sin and cos, we can write all doubly periodic functions using $\wp_\Lambda$ and $\wp'_\Lambda$. Also, I will start dropping the Λ from $\wp_\Lambda$ if it is well-understood.

Theorem 1.8. $\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda(z), \wp'_\Lambda(z))$. In other words, any elliptic function can be written as

$$\frac{R(\wp_\Lambda(z), \wp'_\Lambda(z))}{Q(\wp_\Lambda(z), \wp'_\Lambda(z))}, \qquad R, Q \in \mathbb{C}[X, Y].$$

Proof. Note first that we can write any elliptic function f as

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.$$

The first summand is an even elliptic function, while the second is odd elliptic. Note that if g is odd elliptic, then $\wp'(z) \cdot g$ is even elliptic. It now suffices to show that any even elliptic function is rational in $\wp(z)$.

Suppose f is even. This means (1) $\operatorname{ord}_x(f) = \operatorname{ord}_{-x}(f)$, and (2) if $2x \in \Lambda$, then $\operatorname{ord}_x(f)$ is even. (For the latter, note in general that $f^{(n)}(z) = (-1)^n f^{(n)}(-z)$, but if $2x \in \Lambda$, then by invariance of f and its derivatives under the translation $z \mapsto z - 2x$, we have $f^{(n)}(x) = f^{(n)}(-x)$. This forces $f^{(n)}(x) = 0$ when n is odd, so $\operatorname{ord}_x(f)$ must be even.)

Let D denote the fundamental domain with vertices a, $a+\omega_1$, $a+\omega_2$, and $a+\omega_1+\omega_2$, and let H denote the lower half with vertices a, $a+\omega_1$, $a+\frac{\omega_2}{2}$, and $a+\omega_1+\frac{\omega_2}{2}$. Define

$$g(z) = \prod_{w \in H - \{0\}} (\wp(z) - \wp(w))^{n_w}, \qquad n_w = \begin{cases} \operatorname{ord}_x(f) & \text{if } 2x \notin \Lambda \\ \frac{1}{2}\operatorname{ord}_x(f) & \text{if } 2x \in \Lambda \end{cases}.$$

Note that this is a finite product as there are only finitely many poles (and thus zeros) in H.

We claim that $g(z) = f(z)$. Observe that the function $\wp(z) - \wp(w)$ has a double pole at 0, and thus it has two zeros by $\sum \operatorname{ord}_x(f) = 0$. By evenness of $\wp(z)$, we see that the two zeros are $z = w$ and $z = -w$.

But then by construction, f and g have the same poles and zeros with the same multiplicity, including at $x = 0$. Thus, $f(z)/g(z)$ is elliptic and holomorphic, meaning it is constant. The conclusion then follows. □

We now calculate the Laurent series of $\wp_\Lambda(z)$ around $z = 0$. If $|z| < |w|$, then for

all $w \in \Lambda$, we have

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{1}{w^2}\left(\frac{1}{\left(1-\frac{z}{w}\right)^2} - 1\right) = \frac{1}{w^2}\sum_{n=1}^{\infty}(n+1)\left(\frac{z}{w}\right)^n,$$

which we can do as $|z| < |w| \implies |z/w| < 1$. We thus deduce that around $z = 0$,

$$\begin{aligned}\wp_\Lambda(z) &= \frac{1}{z^2} + \sum_{0\neq w\in\Lambda}\sum_{n=1}^{\infty}\frac{(n+1)}{w^{n+2}}z^n \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}(\Lambda)z^n \\ &= \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k},\end{aligned}$$

so the coefficients of the Laurent series are given by the Eisenstein series.

Since $\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda(z), \wp'_\Lambda(z))$, we must be able to express $\wp'_\Lambda(z)^2$, which is even, in terms of $\wp_\Lambda(z)$. This is the algebraic relation, which gives a model (the **Weierstrass model**) of an elliptic curve:

Proposition 1.9. For all $z \in \mathbb{C} - \Lambda$, we have

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4(\Lambda)\wp(z) - 140G_6(\Lambda).$$

Remark 1.10. We denote $g_2(\Lambda) \coloneqq 60G_4(\Lambda)$ and $g_3(\Lambda) \coloneqq 140G_6(\Lambda)$.

Proof. We can explicitly compute

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3G_4z^2 + \cdots \\ \wp(z)^3 &= \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + \cdots \\ \wp'(z)^2 &= \frac{4}{z^6} - \frac{24G_4}{z^4} - 80G_6 - \cdots.\end{aligned}$$

We see then that

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6 = O(z^2),$$

but any holomorphic elliptic function is constant, and checking the constant term ensures the error term is indeed 0. □

Consequently, we obtain a holomorphic map

$$\begin{aligned}\mathbb{C} - \Lambda &\to \{(x,y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2x - g_3\} \\ z &\mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)),\end{aligned}$$

which extends to

$$\mathbb{C} \to \{[x:y:z] \in \mathbb{P}^2(\mathbb{C}) : y^2z = 4x^3 - g_2xz^2 - g_3z^3\}$$
$$z \mapsto \begin{cases} [\wp(z) : \wp'(z) : 1] & \text{if } z \notin \Lambda \\ [0:1:0] & \text{if } z \in \Lambda. \end{cases}$$

We want this map to be bijective and for the image to be smooth, in which case this lattice Λ would somehow give us a one-dimensional curve in $\mathbb{P}^2(\mathbb{C})$.

Proposition 1.11. The polynomial $4x^3 - g_2x - g_3$ does not have a double root. Equivalently,

$$\Delta(\Lambda) = g_2^3 - 27g_3^2 \neq 0.$$

Proof. Take periods ω_1, ω_2, and let $\omega_3 = \omega_1 + \omega_2$. Since $\wp'$ is odd, we know

$$\wp'(\omega_1/2) = \wp'\left(\frac{\omega_1}{2} - \omega_1\right) = \wp'(-\omega_1/2) = -\wp'(\omega_1/2),$$

so $\wp'(\omega_1/2) = 0$. Likewise, $\wp'(w_2/2) = \wp'(w_3/2) = 0$. Since $\wp'$ has a triple pole at $0 \in \mathbb{C}/\Lambda$, the roots of $\wp'$ are the nonzero 2-torsion points of $\mathbb{C}/\Lambda$. Thus, from the Weierstrass model $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, we get that the roots of $4x^3 - g_2x - g_3$ are exactly $\wp(\omega_i/2)$ for $i \in \{1,2,3\}$. It just suffices now to show that the $\wp(\omega_i/2)$ values are all distinct.

But note that the function $\wp(z) - \wp(\omega_i/2)$ is elliptic with a double pole at $z = 0$, and its roots are at $\omega_i/2$ and $-\omega_i/2 \equiv \omega_i/2$. Hence, it has a double zero at $z = \omega_i/2$, meaning any other $z = \omega_j/2$ cannot be a root. □

Proposition 1.12. The map

$$\begin{aligned} \varphi : \mathbb{C}/\Lambda &\to E \subset \mathbb{P}^2(\mathbb{C}) \\ 0 &\mapsto [0:1:0] \\ z &\mapsto [\wp(z) : \wp'(z) : 1], \end{aligned}$$

where E is given by the homogeneous polynomial $y^2z = 4x^3 - g_2xz^2 - g_3z^3$, is a biholomorphism.

Proof. This is really a fact about compact Riemann surfaces. We already established this function is holomorphic, so we just demonstrate it is bijective.

We first prove injectivity. Suppose $\varphi(z_1) = \varphi(z_2)$, so $\wp(z_1) = \wp(z_2)$ and $\wp'(z_1) = \wp'(z_2)$. If $2z_1 \notin \Lambda$, the function $\wp(z) - \wp(z_1)$ must have roots at $z_1, -z_1, z_2$, which are all distinct by assumption. But it can only admit two roots, so $z_2 \equiv \pm z_1 \bmod \Lambda$. Now use $\wp'(z_1) = \wp'(z_2)$ to deduce the positive sign. If $2z_1 \in \Lambda$, then $\wp(z) - \wp(z_1)$ has a double zero at z_1, so automatically we get $z_1 = z_2$ in $\mathbb{C}/\Lambda$.

Now we prove surjectivity. Suppose $(x, y) \in \mathbb{C}^2$ satisfies $y^2 = 4x^3 - g_2x - g_3$. The function $\wp(z) - x$ is a non-constant elliptic function, so it must have zeros at $z = \pm a$ for some $a \in \mathbb{C}$. Thus, $x = \wp(a)$, which makes $y^2 = \wp'(a)^2$. We can replace a with $-a$ if necessary to get $(x, y) = (\wp(a), \wp'(a))$, done. □

We now determine whether $E \subset \mathbb{P}^2(\mathbb{C})$ is smooth. Recall that a curve given by $f(x, y, z) = 0$ in $\mathbb{P}^2(\mathbb{C})$ is **smooth** (**non-singular**) if and only if $\partial f/\partial x$, $\partial f/\partial y$, $\partial f/\partial z$, and f do not have any common roots. But note that the only root of $\partial f/\partial y = 0$ is $2y = 0 \implies y = 0$, which means $4x^3 - g_2x - g_3$ must have a double root, which we established is not the case. So in fact the curves we have produced from a given lattice Λ are smooth projective curves. Noting that $\mathbb{C}/\Lambda$ is a complex torus and hence has genus 1, we assert that the curve defined by the Weierstrass equation is an elliptic curve.

1.4 Uniformization Theorem

So far, we have described a way to construct an elliptic curve given a lattice. It turns out that **all** elliptic curves arise from lattices.

> **Theorem 1.13** (Uniformization Theorem for Elliptic Curves)**.** For all $a, b \in \mathbb{C}$ with $a^3 - 27b^2 \neq 0$, there exists $\Lambda \subset \mathbb{C}$ such that $a = g_2(\Lambda)$ and $b = g_3(\Lambda)$.

More explicitly, the map $\mathbb{C}/\Lambda \xrightarrow{\sim} E$ sending $z \mapsto [\wp(z) : \wp'(z) : 1]$ admits an inverse map given by

$$\begin{aligned} E &\to \mathbb{C} \\ P &\mapsto \int_0^P \frac{dx}{y}. \end{aligned}$$

We can see where the dx/y comes from: if we take the parametrization $x = \wp(z)$ and $y = \wp'(z)$, then $\frac{dx}{y} = \frac{\wp'(z)dz}{\wp'(z)} = dz$, so we would just be taking the length from 0 to P.

However, the integral depends on the choice of path from 0 to P! Let us describe this dependence more carefully. Let γ_1 and γ_2 be two closed loops generating the complex torus E. (If we start with $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, we can take the paths from the origin to ω_1 and ω_2, respectively.) Then, this integral is *well-defined modulo*

$$\mathbb{Z}\int_{\gamma_1} \frac{dx}{y} \oplus \mathbb{Z}\int_{\gamma_2} \frac{dx}{y}.$$

We call the two integrals $\int_{\gamma_i} \frac{dx}{y}$ the **periods** of the elliptic curve. These two periods define a lattice Λ, so we have a map $E \to \mathbb{C}/\Lambda$ sending $P \mapsto \int_0^P \frac{dx}{y} \bmod \Lambda$. **This is the inverse of φ from above.**

Remark 1.14. The one-dimensional analogue of this is familiar: the group morphism $\mathbb{C} \to \mathbb{C}^\times$ sending $z \mapsto e^z$ induces an isomorphism $\mathbb{C}/2\pi i\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^\times$, which has an inverse $\log z = \int_1^z \frac{dt}{t}$.

1.5 Moprhisms of Complex Elliptic Curves

The Uniformization Theorem tells us that all complex elliptic curves are of the form $\mathbb{C}/\Lambda$ for a lattice $\Lambda \subset \mathbb{C}$. We wish to express morphisms between complex elliptic curves in terms of their respective lattices. Let $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ be two lattices. If $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$, then

$$\begin{aligned} f_\alpha : \mathbb{C}/\Lambda_1 &\to \mathbb{C}/\Lambda_2 \\ z &\mapsto \alpha z \end{aligned}$$

is a holomorphic map with $f_\alpha(0) = 0$.

Theorem 1.15. The map between $\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\}$ and holomorphic functions $f : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $f(0) = 0$ given by $\alpha \mapsto f_\alpha$ is a bijection.

Proof. For injectivity, we have $f_\alpha = f_\beta \implies \alpha z \equiv \beta z \bmod \Lambda_2$ for all $z \in \mathbb{C}$. But then this means the multiplication-by-$(\alpha - \beta)$ map is a continuous map between $\mathbb{C}$ (connected) and Λ_2 (discrete), so it must be the constant zero map. Thus, $\alpha = \beta$.

For surjectivity, first denote π_i as the projection map $\mathbb{C} \to \mathbb{C}/\Lambda_i$. Can we find some $\widetilde{f} : \mathbb{C} \to \mathbb{C}$ such that $f \circ \pi_1 = \pi_2 \circ \widetilde{f}$? For this, we use the lifting property, which says that given $Y \xrightarrow{h} X$ and $X' \xrightarrow{p} X$ (with $h(y_0) = p(x_0') = x_0$), the map h factors through p if and only if $h_*(\pi_1(Y, y_0)) \subset p_*(\pi_1(X', x_0'))$. In particular, we can always lift if $\pi_1(Y, y_0) = 0$, aka when Y is simply connected.

Given this lift, we have $\widetilde{f}(z + w) \equiv \widetilde{f}(z) \bmod \Lambda_2$ for all $z \in \mathbb{C}$ and $w \in \Lambda_1$. But then the difference $\widetilde{f}(z+w) - \widetilde{f}(z)$, as a function in z, has image contained in Λ_2, so it is constant since $\widetilde{f}$ is continuous. Continuing, we now have $\widetilde{f}'(z + w) = \widetilde{f}'(z)$, meaning $\widetilde{f}'$ is elliptic (periodic with respect to Λ_1) and holomorphic, hence constant. Thus, we may write $\widetilde{f}(z) = \alpha z + \gamma$ for some $\alpha, \gamma \in \mathbb{C}$. The condition $\widetilde{f}(0) = 0$ forces $\gamma = 0$, so $\widetilde{f}(z) = \alpha z$ and so $f = f_\alpha$, as desired. □

Corollary 1.16. *$\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic (by a map which sends 0 to 0) if and only if there exists some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 = \Lambda_2$.*

Our discussion of complex elliptic curves has been quite nice so far because we can express everything in terms of lattices in $\mathbb{C}$. But although these lattices are nice to work with, they don't seem to exhibit much structure collectively. But we have a very nice way of parametrizing these lattices.

Consider the Poincaré upper half-plane $\mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$. This admits an $\mathrm{SL}_2(\mathbb{R})$-action by linear fractional transformations.

Proposition 1.17. We have a bijection

$$\mathbb{H}/\operatorname{SL}_2(\mathbb{Z}) \leftrightarrow \{\text{lattices in } \mathbb{C}\}/\mathbb{C}^\times$$
$$\tau \mapsto \mathbb{Z} \oplus \mathbb{Z}\tau.$$

Proof. Suppose $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$. Then, as ω_1', ω_2' both belong in the first lattice, we have $a, b, c, d \in \mathbb{Z}$ such that

$$\omega_1' = a\omega_1 + b\omega_2, \quad \omega_2' = c\omega_1 + d\omega_2 \implies \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix}.$$

Likewise, since ω_1, ω_2 both lie in the second lattice, we have $a', b', c', d' \in \mathbb{Z}$ such that

$$\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}.$$

It follows that $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \operatorname{SL}_2(\mathbb{Z})$, and that $\gamma \cdot (\omega_1/\omega_2) = \omega_1'/\omega_2'$. Thus, if $\mathbb{Z} \oplus \mathbb{Z}\tau \sim \mathbb{Z} \oplus \mathbb{Z}\tau'$ are equivalent up to scaling by $\mathbb{C}^\times$, then there must exist some $\gamma \in \operatorname{SL}_2(\mathbb{Z})$ such that $\gamma \cdot \tau = \tau'$.

The converse can be easily checked: if $\tau' = \gamma\tau$ for some $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \operatorname{SL}_2(\mathbb{Z})$, then $\mathbb{Z} \oplus \mathbb{Z}\tau' \simeq \mathbb{Z}(a\tau + b) \oplus \mathbb{Z}(c\tau + d) \subseteq \mathbb{Z} \oplus \mathbb{Z}\tau$, and equality is achieved since γ is invertible. This completes the proof of the bijection. □

1.6 Aside: Complex Multiplication

This is inspired from one of the TD problems, so it was not part of the lecture. Let $\Lambda_1 = \Lambda_2 = \Lambda$, and let $E = \mathbb{C}/\Lambda$. The above tells us that $\operatorname{End}(E) = \{\alpha \mid \alpha\Lambda \subseteq \Lambda\}$. It is clear that any $\alpha \in \mathbb{Z}$ works, so $\mathbb{Z} \subset \operatorname{End}(E)$ automatically. In fact, one can note that $\operatorname{End}(E)$ is an endomorphism *ring* (addition is clear, multiplication is composition), so it must include $\mathbb{Z}$.

Most often, it turns out we have equality $\mathbb{Z} = \operatorname{End}(E)$. Elliptic curves with admit more endomorphisms than just $\mathbb{Z}$ are said to have **complex multiplication**. We can give a taste to what these elliptic curves with complex multiplication look like.

Suppose $\alpha \in \mathbb{C} - \mathbb{Z}$ satisfies $\alpha\Lambda \subseteq \Lambda$. Write $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$. This means that there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\alpha\tau = a\tau + b, \quad \alpha = c\tau + d \implies (c\tau + d)\tau = a\tau + b,$$

so τ satisfies some quadratic relation. Even better, taking the characteristic polynomial of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ gives a *monic* quadratic relation for α, explicitly $(a - \alpha)(d - \alpha) - bc = 0$. So $\operatorname{End}(E)$ is an order of the ring of integers $\mathcal{O}_K$ of some imaginary quadratic field K. If $\alpha \in \mathbb{H}$ such that $\alpha \in \operatorname{End}(E)$ for some elliptic curve E, then we call α a **CM point**.

If we were to find elliptic curves that admit *automorphisms* besides $\{\pm 1\} \subset \mathbb{Z}$, then we have even fewer options. Using the same as above, the equality $\alpha\Lambda = \Lambda$ forces $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$, and so the characteristic polynomial becomes

$$(a-\alpha)(d-\alpha) - bc = \alpha^2 - (a+d)\alpha + (ad-bc) = \alpha^2 - (a+d)\alpha + 1 = 0.$$

In order for $\alpha \in \mathbb{C} - \mathbb{R}$, we need $(a+d)^2 < 4$, which restricts our possibilities to (1) $\alpha^2 + 1 = 0$, (2) $\alpha^2 - \alpha + 1 = 0$, and (3) $\alpha^2 + \alpha + 1 = 0$. Equivalently, we have either $\alpha = i$, $\alpha = \omega = \frac{-1+\sqrt{-3}}{2}$, or $\alpha = \rho = \frac{1+\sqrt{-3}}{2}$.

If α is any of the above values, then note that $\alpha \cdot 1 \in \Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$. One can check that the lattice $\mathbb{Z} \oplus \mathbb{Z}i$ admits an automorphism given by multiplication by i, and the lattice $\mathbb{Z} \oplus \mathbb{Z}\omega = \mathbb{Z} \oplus \mathbb{Z}\rho$ admits two given by multiplication by ω and ρ.

In general, suppose $E = \mathbb{C}/\Lambda$ admits an automorphism given by multiplication by i. Then, we can consider the Eisenstein series $G_6(\Lambda)$; the sum of $1/\lambda^6$ over each orbit given by multiplication-by-i is 0, and so $G_6(\Lambda) = 0$. This means E has a Weierstrass equation of the form $y^2 = 4x^3 - g_2 x$, which after scaling gives $y^2 = x^3 - x$. Indeed, one can check $(x, y) \mapsto (-x, iy)$ is an automorphism. Likewise, if $E = \mathbb{C}/\Lambda$ has an automorphism given by multiplication by ρ (and hence by $\rho^2 = \omega$), then we can consider the sum of $1/\lambda^4$ over all orbits from multiplication-by-ω to conclude $G_4(\Lambda) = 0$. Thus, the Weierstrass equation for E is $y^2 = 4x^3 - g_3$, which clearly has an automorphism $(x, y) \mapsto (\omega x, y)$.

The property that $\mathrm{End}(E) \supsetneq \mathbb{Z}$ may not seem remarkable at first, but elliptic curves with complex multiplication satisfy some beautifully remarkable properties. For instance, the j-invariant of E with CM is guaranteed to be an *algebraic integer*. Furthermore, if $\mathrm{End}(E) \otimes \mathbb{Q} = K$ (we already established K must be imaginary quadratic), then $j(E)$ *generates the Hilbert class field of* K. One can tie these facts to show that transcendental numbers like $e^{\pi\sqrt{163}}$ are very close to an integer. It is quite the remarkable (and still expanding) story!

2 11/12 - Generalizing the Theory of Riemann Surfaces

Author's Note 2.1. Monday, November 11 was a holiday, so the usual TD session on Tuesday was replaced with a lecture. TDs will resume next week, and the missed lectures will be made up on December 16.

The study of compact Riemann surfaces, as we have already seen, is key to studying elliptic curves over $\mathbb{C}$. We seek to generalize results of Riemann surfaces to allow us to work with elliptic curves over other fields. Luckily, the most important theorem about Riemann surfaces holds in much greater generality:

Theorem 2.2 (Riemann-Roch)**.** Let C be a smooth projective curve of genus g over an algebraically closed field $K = \overline{K}$. Let D be a divisor on C. We have an equality

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Usually, we will be working in the case where an elliptic curve C lies over a *perfect field* K such that $\overline{K}/K$ is a Galois field extension. (Note by perfectness, it is automatically separable.)

In this spirit, let C be a smooth projective curve over a perfect field K. Denote $\overline{K}(C)$ as the field of rational functions on C. Explicitly, it is given set-wise as equivalence classes of pairs (U, f) where $U \subset C$ is Zariski-open and $f \in \mathcal{O}(U)$ is a continuous $f : U \to \overline{K}$. We have the inclusions

$$\mathfrak{m}_p \subset \mathcal{O}_{C,p} \subset \overline{K}(C),$$

where $\mathcal{O}_{C,p}$ is the local ring at p given by the set of germs at p, and $\mathfrak{m}_p$ is the maximal ideal of $\mathcal{O}_{C,p}$ given by all germs vanishing at p. Note we have $\overline{K}(C) = \mathrm{Frac}(\mathcal{O}_{C,p})$ and $\mathcal{O}_{C,p}/\mathfrak{m}_p \simeq \overline{K}$.

We have an algebraic way of expressing the smoothness condition. We say C is **smooth** if for all $p \in C$,

$$\dim \mathcal{O}_{C,p} = \dim(\mathfrak{m}_p/\mathfrak{m}_p^2) = 1,$$

where the left is the Krull dimension (length of maximal chain of prime ideals) and $\mathfrak{m}_p/\mathfrak{m}_p^2$ on the right can be seen as the dual of the tangent space at p. This agrees with our geometric understanding of smoothness.

2.1 Divisors

Definition 2.3 (Divisor, etc.)**.** A **divisor** on C is a formal linear combination of the form

$$D = \sum_{P \in C(\overline{K})} n_P[P], \qquad n_P \in \mathbb{Z},\ n_P = 0 \text{ for all but finitely many } P \in C(\overline{K}).$$

We denote the free abelian group of divisors on C as $\mathrm{Div}(C)$. The **degree** of a divisor is $\deg(D) = \sum_P n_P$. (Note this is a finite sum of integers.) A divisor is **effective** if $n_P \geq 0$ for all $P \in C(\overline{K})$, in which case we write $D \geq 0$. This defines a partial ordering on $\mathrm{Div}(C)$ where $D_1 \geq D_2 \iff D_1 - D_2 \geq 0$.

If C is defined over K, then we can access K from $\overline{K}$ by considering the Galois action $\mathrm{Gal}(\overline{K}/K)$ on $C(\overline{K})$. This Galois action extends to an action on $\mathrm{Div}(C)$ in the obvious way: $\sigma(D) = \sum_P n_P[\sigma(P)]$. We say that a divisor D is defined over K if it is fixed by this Galois action, i.e., if $\sigma(D) = D$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. In particular, we can access $C(K)$ by looking at the fixed points of $C(\overline{K})$ under the Galois action.

Example 2.4. Let $C = \mathbb{P}^1$; it is clearly defined over $\mathbb{Q}$. Over $\overline{\mathbb{Q}}$, we see the divisor $D = [(\sqrt{2} : 1)] + [(-\sqrt{2} : 1)]$ is defined over $\mathbb{Q}$, as any Galois action either fixes each term in the sum or swaps them.

We can associate a function $f \in \overline{K}(C)$ with a divisor. The key is that, up to scaling, a function on a compact Riemann surface is determined by its poles and zeros, counting multiplicity. For elliptic curves over $\mathbb{C}$, this follows from the fact that any entire elliptic function is constant. In the general setting where $\mathbb{C}$ is replaced by any perfect field K, we attempt to draw up a similar lexicon. Let C again be a smooth projective curve over perfect K. Define the following "**order**" map by

$$\begin{aligned} \operatorname{ord}_p : \mathcal{O}_{C,p} &\to \mathbb{Z}_{\geq 0} \cup \{\infty\} \\ f &\mapsto \max\{d \mid f \in \mathfrak{m}_p^d\}. \end{aligned}$$

Note that we have the properties

$$\operatorname{ord}_p(fg) = \operatorname{ord}_p(f) + \operatorname{ord}_p(g), \qquad \operatorname{ord}_p(f+g) \geq \min\{\operatorname{ord}_p(f), \operatorname{ord}_p(g)\}.$$

This makes $\mathcal{O}_{C,p}$ into a **discrete valuation ring** with valuation given by the ord map. We can extend this valuation to the fraction field $\overline{K}(C) = \operatorname{Frac}(\mathcal{O}_{C,p})$ by $\operatorname{ord}_p(f/g) = \operatorname{ord}_p(f) - \operatorname{ord}_p(g)$. This turns our order map into

$$\begin{aligned} \operatorname{ord}_p : \overline{K}(C) &\to \mathbb{Z} \cup \{\infty\} \\ f/g &\mapsto \operatorname{ord}_p(f) - \operatorname{ord}_p(g). \end{aligned}$$

Definition 2.5 (Regular, Zero, Pole)**.** If $\operatorname{ord}_p(f) \geq 0$, we say f is **regular** at P and one can evaluate $f(p) \in \overline{K}$. If $\operatorname{ord}_p(f) > 0$, we say f has a **zero** at p. Otherwise, if $\operatorname{ord}_p(f) < 0$, then we say f has a **pole** at p.

Note that there are a finite number of zeros and poles, i.e., given $f \in \overline{K}(C)^\times$, the set of points $P \in C(\overline{K})$ with $\operatorname{ord}_P(f) \neq 0$ is finite. This is because the set of zeros $\{p \mid f(p) = 0\}$ is Zariski-closed, hence finite, and so the number of poles is also finite by considering $1/f$.
Now we are able to define the divisor of a function.

Definition 2.6 (Divisor of Function)**.** Let $f \in \overline{K}(C)^\times$. The **divisor of** f is

$$\operatorname{div}(f) = \sum_{P \in C(\overline{K})} \operatorname{ord}_P(f) \cdot [P].$$

Proposition 2.7. If C is a projective curve and $f \in \overline{K}(C)^\times$, then $\deg(\operatorname{div}(f)) = 0$.

We have exhibited a Galois action of $\mathrm{Gal}(\overline{K}/K)$ on $C(\overline{K})$. We can now define it on $\overline{K}(C)$ (or on the structure sheaf $\mathcal{O}_C$) as follows. Given some $f : U \to \overline{K}$ (i.e., $f \in \mathcal{O}(U)$), we define the Galois action as $\sigma(f)(x) \coloneqq f(\sigma(x))$. Note that if $\sigma(x) \in U$, then $x \in \sigma^{-1}(U)$, so $\sigma(f) \in \mathcal{O}(\sigma^{-1}(U))$. Note that one can directly show

$$\mathrm{div}(\sigma(f)) = \sigma(\mathrm{div}(f)).$$

Thus, if $f \in K(C)$, then the divisor $\mathrm{div}(f)$ is well-defined as a divisor over K since $\sigma(f) = f$.

Definition 2.8. Let $D \in \mathrm{Div}(C)$. Denote

$$\mathcal{L}(D) \coloneqq \{f \in \overline{K}(C)^\times \mid \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

This is a $\overline{K}$-vector space.

Example 2.9. If $D = n \cdot [P]$, then the nonzero elements of $\mathcal{L}(D)$ are the functions f which are regular outside of P and has a pole of order at most n at P.

Lemma 2.10. *If C is projective, then $\mathcal{L}(D)$ has finite dimension over $\overline{K}$.*

Proof. If $D_1 \leq D_2$, then $\mathrm{div}(f) \geq -D_1$ implies $\mathrm{div}(f) \geq -D_2$, so $\mathcal{L}(D_1) \subset \mathcal{L}(D_2)$. It thus suffices to prove the statement for $D \geq 0$. We will show in particular that

$$\dim \mathcal{L}(D) \leq \deg D + 1.$$

We do this by induction on $\deg D$. If $\deg D = 0$, then $D = 0$ since $D \geq 0$ by assumption, meaning $\mathcal{L}(D) = \mathcal{O}(C) = \overline{K}$. Now if $D > 0$, then there exists $P \in C(\overline{K})$ such that $D - [P] \geq 0$. If $\mathcal{L}(D) = \mathcal{L}(D - [P])$, then we are done by induction. Otherwise, we have $\mathcal{L}(D - [P]) \subsetneq \mathcal{L}(D)$. In this case, we can choose a **uniformizer** t in P such that t generates $\mathfrak{m}_p$. In particular, we have $\mathrm{ord}_P(t) = 1$. Denoting n_P as the multiplicity of P in D, we define a map

$$\begin{aligned} \mathcal{L}(D) &\to \overline{K} \\ g &\mapsto (t^{n_P} g)(P). \end{aligned}$$

This is surjective, as it is a nonzero $\overline{K}$-linear map. Note that $\mathcal{L}(D - [P])$ lies in the kernel of this map. Thus, as $\overline{K}$-vector spaces, we have $\mathcal{L}(D) = \mathcal{L}(D - [P]) \oplus \overline{K} \cdot f$ where $f \in \mathcal{L}(D) - \mathcal{L}(D - [P])$. Now we may conclude by the inductive hypothesis on $\mathcal{L}(D - [P])$. □

Remark 2.11. These vector spaces $\mathcal{L}(D)$ in the context of Riemann surfaces can be realized via sheaf cohomology. The cohomology may vary depending on the context, but in principle we have $\mathcal{L}(D) = H^0(C, \mathcal{O}(D))$.

Remark 2.12. If $\deg D < 0$, then $\mathcal{L}(D) = \{0\}$.

A group of particular interest to us is the **Picard group**, given as $\mathrm{Pic}(C) = \mathrm{coker}(\overline{K}(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(C))$. In other words, if $\mathrm{Prin}(C)$ is the group of **principal divisors**, i.e., divisors of the form $\mathrm{div}(f)$, then we have $\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Prin}(C)$. It fits into the following exact sequence:

$$1 \to \overline{K}^\times \to \overline{K}(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}(C) \to \mathrm{Pic}(C) \to 0.$$

Note that $\mathcal{L}(D)$ is invariant under action by $\mathrm{Prin}(C)$. Explicitly, for any $g \in \overline{K}(C)^\times$, we have $\mathcal{L}(D + \mathrm{div}(g)) \simeq \mathcal{L}(D)$ given by $f \mapsto fg$. This is well-defined because $\mathrm{div}(f) \geq -D - \mathrm{div}(g) \implies \mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g) \geq -D$. In other words, we see that $\dim \mathcal{L}(D)$ depends only on the equivalence class of D in $\mathrm{Pic}(C)$.

Lemma 2.13. *Let C be a smooth projective curve defined over K. If D is a divisor defined over K, then $\mathcal{L}(D)$ admits a basis of functions in $K(C)$.*

Proof. Note that $\mathcal{L}(D)$ admits a $\mathrm{Gal}(\overline{K}/K)$-action since for $f \in \mathcal{L}(D)$, we have $\sigma(f) \in \mathcal{L}(\sigma(D)) = \mathcal{L}(D)$. The result now follows from the following lemma:

Lemma 2.14. *Let V be a $\overline{K}$-vector space with a continuous semilinear Galois action. (These are defined below.) Let*

$$V^{\mathrm{Gal}(\overline{K}/K)} := \{v \in V \mid \sigma(v) = v \text{ for all } \sigma \in \mathrm{Gal}(\overline{K}/K)\}$$

be the subspace of Galois-invariant vectors. Then, we have an isomorphism

$$\begin{aligned} V^{\mathrm{Gal}(\overline{K}/K)} \otimes_K \overline{K} &\xrightarrow{\simeq} V \\ v \otimes \lambda &\mapsto \lambda v. \end{aligned}$$

Definition 2.15 (Continuous, Semilinear Action)**.** We say the Galois action is **continuous** if for all $v \in V$, the subgroup $\{\sigma \in \mathrm{Gal}(\overline{K}/K) \mid \sigma(v) = v\}$ has finite index. It is **semilinear** if it satisfies $\sigma(\lambda v) = \sigma(\lambda)\sigma(v)$.

For the proof, I will denote V^G as shorthand for $V^{\mathrm{Gal}(\overline{K}/K)}$ since the (Galois) group is well-understood.

Proof. It suffices to show that any $v \in V$ can be written as a $\overline{K}$-linear combination of elements of V^G.

Let $H = \{\sigma \in \mathrm{Gal}(\overline{K}/K) \mid \sigma(v) = v\} \subset G$. Since H has finite index in G by continuity, the fixed field $\overline{K}^H$ is a finite extension of K. Let L be its Galois closure. We now choose a K-basis $\alpha_1, \ldots, \alpha_n$ of L. Writing $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$, we define a vector

$$w_i = \sum_{j=1}^{n} \sigma_j(\alpha_i v).$$

By construction, we have $\sigma(w_i) = w_i$ for all $\sigma \in G$, so $w_i \in V^G$. By semilinearity, we can thus write

$$w_i = \sum_{j=1}^{n} \sigma_j(\alpha_i)\sigma_j(v).$$

But the matrix $(\sigma_j(\alpha_i))_{i,j}$ is invertible! (One way to obtain this is by letting $L = K(\alpha)$ by the Primitive Element Theorem, then the basis $\alpha_i = \alpha^{i-1}$ turns the matrix $(\sigma_j(\alpha_i))_{i,j}$ into a Vandermonde matrix, whose determinant we can explicitly compute to be non-zero.) This means that all $\sigma_j(v)$, and in particular v itself, can be written as a $\overline{K}$-linear combination of w_i. □

To show that $\mathcal{L}(D)$ indeed has a $\overline{K}$-basis contained in $K(C)$, we just need to show that the Galois action on $\mathcal{L}(D)$ is continuous semilinear. For continuous, note that divisors are finite sums, so the stabilizer of some divisor in $\mathcal{L}(D)$ must fix some finite extension of K. As the action is evidently semilinear, we may conclude. □

3 11/19 - Differential Forms

3.1 Differential Forms

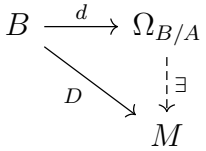
We also develop the notion of differential forms algebraically.

Definition 3.1 (Kähler Differentials)**.** Let $A \to B$ be a ring morphism. The **module of Kähler differentials**, denoted $\Omega_{B/A}$, is the quotient of the free B-module generated by the symbols db for all $b \in B$ by the sub-module generated by the elements of the following form:

1. $d(b + b') - db - db'$ (linear);
2. $d(bb') - b\,db' - b'\,db$ (Leibniz);
3. da for all $a \in A$ ("constants").

Definition 3.2 (Derivation)**.** We call any A-linear map $B \to M$ satisfying the three above conditions an ***A*-derivation**.

We have a natural B-module morphism $d : B \to \Omega_{B/A}$ given by $b \mapsto db$. By definition, this is an A-derivation. It satisfies the following universal property:



Here, M is a B-module and D is an A-derivation. The induced map is a B-module morphism.

Let's look at several explicit examples.

Example 3.3 (Differentials on Polynomial Ring)**.** If $B = A[x_1, \ldots, x_n]$, then we have $\Omega_{B/A} = B\,dx_1 \oplus \cdots \oplus B\,dx_n$ with a map

$$\begin{aligned} d : B &\to \Omega_{B/A} \\ f &\mapsto df = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} dx_i \end{aligned}$$

If we consider a quotient, i.e., $B = A[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$, then we have

$$\Omega_{B/A} = B\,dx_1 \oplus \cdots \oplus B\,dx_n \Big/ (df_1, \ldots, df_m),$$

with a similar map $B \to \Omega_{B/A}$ as above. These follow from the exercise below.

Exercise 3.4. (from TD3) Let B be generated by $(x_i)_{i\in I}$ as an A-algebra. Then, $\Omega_{B/A}$ is generated as an B-module by $(dx_i)_{i\in I}$.

Proof. For $d \geq 0$, let $B_d \subset B$ be the A-module generated by all polynomials in the x_i's of degree at most d. We can prove using induction that

$$d(B_d) \subset \sum_{i\in I} B\,dx_i.$$

This would imply equality $d(B) = \sum_I B\,dx_i$, since clearly the right is contained in the left.

The base case $d = 0$ is clear, so suppose it is true for $d-1$. Let $g \in B_d$; we can write $g = c + \sum_I x_i g_i$, where $c \in A$ is constant and $g_i \in B_{d-1}$. Then, we have

$$dg = \sum_{i\in I} d(x_i g_i) = \sum_{i\in I} g_i\,dx_i + \sum_{i\in I} x_i\,dg_i.$$

As both sums on the right are in $\sum_I B\,dx_i$, the inductive step is done. □

To make the connection with the above example explicit, let us determine $\Omega_{B/A}$ when $B = A[x_1, \ldots, x_n]$. By the exercise, we know $\Omega_{B/A}$ is generated by $(dx_1, \ldots, dx_n)$. We want to show that this module is free. But we see that for each i, we have the derivation $\partial x_i : B \xrightarrow{d} \Omega_{B/A} \xrightarrow{\delta_i} B\,dx_i$, where $\delta_i(dx_j) = \delta_{ij}$. Thus, if $0 = \sum_{i=1}^n a_i\,dx_i$, then applying δ_i would force $a_i = 0$, so this module is free.

Example 3.5 (Differentials of Field Extension)**.** Let $f \in \mathbb{Q}[x]$ be a polynomial with no double root, and consider $K = \mathbb{Q}[x]/(f) \supset \mathbb{Q}$. Then, $\Omega_{K/\mathbb{Q}}$ is generated by dx modulo $df = f'(x)\,dx$. But as f and f' are coprime to each other, we can find $P, Q \in \mathbb{Q}[x]$ such that $Pf + Qf' = 1$. In particular, this means $Qf' \equiv 1 \bmod (f)$, i.e., f' is invertible in K. Thus, $dx = 0$ in $\Omega_{K/\mathbb{Q}}$, and so $\Omega_{K/\mathbb{Q}} = 0$.

In general, if L/K is a finite field extension, then $\Omega_{L/K} = 0$ iff L/K is separable. For an example of a inseparable extension, one can show that $\Omega_{\mathbb{F}_p(t)/\mathbb{F}_p(t^p)} = \mathbb{F}_p(t)\,dt$.

Example 3.6 (Differential on Curve)**.** Consider the plane curve $X = \mathbb{A}^1_K - \{0\} \hookrightarrow \mathbb{A}^2_K$ given by $xy - 1 = 0$, and let $B = K[x,y]/(xy-1) = K[x,x^{-1}]$ be the field of functions on X. Then, we have

$$\Omega_{B/K} = K[x,x^{-1}]\,dx \oplus K[x,x^{-1}]\,dy \Big/ (x\,dy + y\,dx).$$

Well, we can explicitly compute from $y = 1/x$ that $dy = -y\frac{dx}{x} = -\frac{dx}{x^2}$, so in conclusion $\Omega_{B/K} = K[x,x^{-1}]\,dx$.

Example 3.7 (Differential on Elliptic Curve)**.** Let $X \subset \mathbb{A}^2_K$ be given by $y^2 = f(x) = x^3 + ax + b$, and suppose f does not have a double root. Let $B = K[x,y]/(y^2 - f(x))$. Like in Example 3.5, we can find $P, Q \in K[x,y]$ such that $Pf + Qf' = 1$. Note from $y^2 = f(x)$ we have $2y\,dy = f'(x)\,dx$. Consider the differential

$$\omega = Py\,dx + 2Q\,dy.$$

We claim $\Omega_{B/K} = B \cdot \omega$. Indeed, we can explicitly construct dx and dy from ω:

$$\begin{aligned} y\omega &= Py^2\,dx + 2Qy\,dy \\ &= Pf\,dx + Qf'\,dx \\ &= dx, \\ f'\omega &= Pf'y\,dx + 2Qf'\,dy \\ &= 2Py^2\,dy + 2Qf'\,dy \\ &= 2\,dy, \end{aligned}$$

as desired.

Of course, we are interested in the examples regarding (smooth) curves over some field, so we will continue studying differentials on such curves. One should assume in the following that K is algebraically closed.

Definition 3.8 (Meromorphic Differentials)**.** Let C be a smooth curve over K. We define the **space of meromorphic differential forms on C** as the $K(C)$-vector space

$$\Omega_C \coloneqq \Omega_{K(C)/K}.$$

In the case when we consider the differential on a local ring, the differential generating the Kähler module is given by the uniformizer of the local ring.

Proposition 3.9. Let C be a smooth curve over K and $P \in C(K)$. Let t be a uniformizer at P. Then, the module of Kähler differentials $\Omega_{\mathcal{O}_{C,P}/K}$ is a free $\mathcal{O}_{C,P}$-module generated by dt.

More generally, these modules $\Omega_{B/A}$ behave nicely with respect to localization.

Exercise 3.10. (from TD) Suppose we have a ring map $A \to B$ and $S \subset B$ is multiplicative. Then,

$$\Omega_{S^{-1}B/A} = S^{-1}\Omega_{B/A} = \Omega_{S^{-1}B/(S\cap A)^{-1}A}.$$

Proof. We first show the first isomorphism. We have the following commutative diagram by the universal property of localization:

$$\begin{array}{ccc} \Omega_{B/A} & \longrightarrow & S^{-1}\Omega_{B/A} \\ & \searrow & \downarrow \exists g \\ & & \Omega_{S^{-1}B/A} \end{array}$$

We wish to show that the induced map is an isomorphism. Consider also the universal property of the Kähler module:

$$\begin{array}{ccc} S^{-1}B & \xrightarrow{d} & \Omega_{S^{-1}B/A} \\ & \searrow^{\delta} & \downarrow \exists h \\ & & S^{-1}\Omega_{B/A} \end{array}$$

Here, δ is the derivation defined by

$$\delta\left(\frac{b}{s}\right) \coloneqq \frac{1}{s}d(b) - \frac{b}{s^2}d(s).$$

This comes from the Leibniz rule computation $\delta(b) = \delta(s \cdot b/s) = s \cdot \delta(b/s) + b/s \cdot \delta(s)$, and we want to force $\delta = d$ on B. One can manually check $g \circ h = \mathrm{id}_{\Omega_{S^{-1}B/A}}$ and $h \circ g = \mathrm{id}_{S^{-1}\Omega_{B/A}}$, so they are isomorphic. (This is basically by construction.)

To show the second isomorphism, it suffices to show $d((S \cap A)^{-1}A) = 0$. Let $s \in S \cap A$. Then, we have

$$0 = d(a) = d(s \cdot a/s) = s\,d(a/s) + a/s \cdot \cancel{d(s)} \implies d(a/s) = 0,$$

as desired. □

We also have

Exercise 3.11. (from TD) If $A \to B \to C$ is an an exact sequence of rings, then

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

is also exact.

Proof. This is just abstract play. We will use two facts:

(i) The sequence of A-modules $M' \to M \to M'' \to 0$ is exact iff for all A-modules N, the sequence

$$0 \to \mathrm{Hom}_A(M'', N) \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N)$$

is exact.

(ii) By the universal property, we have an isomorphism

$$\mathrm{Hom}_B(\Omega_{B/A}, N) \cong \mathrm{Der}_A(B, N).$$

Applying this to our given exact sequence and noting that $\mathrm{Hom}_C(C \otimes_B \Omega_{B/A}, N) = \mathrm{Hom}_B(\Omega_{B/A}, N) \cong \mathrm{Der}_A(B, N)$, we get that the given sequence is exact iff

$$0 \to \mathrm{Der}_B(C, N) \to \mathrm{Der}_A(C, N) \to \mathrm{Der}_A(B, N)$$

is exact for any A-module N. But this is clearly true. □

Corollary 3.12. *Let C be a smooth curve. Then, Ω_C is a $K(C)$-vector space of dimension* 1.

Proof. We use the second exercise. Take $A = K$, $B = \mathcal{O}_{C,P}$, $S = \mathcal{O}_{C,P} - \{0\}$, and $C = S^{-1}B$. Note that $\Omega_{S^{-1}B/B} = 0$, as any $d(b_1/b_2)$ can be written as a linear combination in terms of $d(B)$. Thus, the second exercise gives an isomorphism

$$\Omega_{K(C)/K} = \Omega_{S^{-1}B/A} = \Omega_{B/A} \otimes_B S^{-1}B = \Omega_{\mathcal{O}_{C,P}/K} \otimes_{\mathcal{O}_{C,P}} K(C).$$

The right hand side as a $K(C)$-vector space has dimension equal to the rank of $\Omega_{\mathcal{O}_{C,P}/K}$ as a $\mathcal{O}_{C,P}$-module. But we established that this is just 1, as it is generated as an $\mathcal{O}_{C,P}$-module by dt for t a uniformizer of C at P. □

3.2 Divisors of Differential Forms

Like how we defined $\mathrm{div}(f)$ for $f \in K(C)^\times$, we can do something similar for $\Omega_C - \{0\}$.

Let $\omega \in \Omega_C - \{0\}$. Take $P \in C(K)$ and t a uniformizer at P. Then, the above shows that there exists $g \in K(C)^\times$ such that $\omega = g\,dt$. We now define

$$\mathrm{ord}_P(\omega) \coloneqq \mathrm{ord}_P(g).$$

Note that this does not depend on the choice of uniformizer. Indeed, if t, t' are both uniformizers of $\mathcal{O}_{C,P}$, then we have $dt' \in \mathcal{O}_{C,P}\,dt$ and likewise $dt \in \mathcal{O}_{C,P}\,dt'$, and so $dt' \in \mathcal{O}_{C,P}^\times\,dt$ which does not change $\mathrm{ord}_P(g)$.

It is clear now, from our understanding of $K(C)$, that the set $\{P \in C(K) \mid \mathrm{ord}_P(\omega) \neq 0\}$ is finite. We can thus define without issue

$$\mathrm{div}(\omega) \coloneqq \sum_{P \in C(K)} \mathrm{ord}_P(\omega) \cdot [P].$$

This is the **divisor of** ω.

If $\omega_1, \omega_2 \in \Omega_C$ are non-zero, then there exists $f \in K(C)^\times$ with $\omega_1 = f\,\omega_2$ as Ω_C has dimension 1 over $K(C)$. We can thus write $\operatorname{div}(\omega_1) = \operatorname{div}(\omega_2) + \operatorname{div}(f)$. Thus, any choice of $\omega \in \Omega_C$ is equivalent modulo principal divisors, i.e., the class of $\operatorname{div}(\omega)$ in $\operatorname{Pic}(C)$ is independent of our choice of ω. This class has a special name.

Definition 3.13 (Canonical Divisor)**.** The **canonical divisor** K_C of a smooth curve C is the class of $\operatorname{div}(\omega)$ in $\operatorname{Pic}(C)$.

One may recognize this from the statement of Riemann-Roch. In that spirit, one can now actually *define* the genus of a curve:

Definition 3.14 (Genus of Curve)**.** Let C be a smooth projective curve over K. The **genus** of C is $g = \ell(K_C) = \dim \mathcal{L}(K_C)$.

We can interpret the genus g as the dimension (over K) of the space of holomorphic differential forms. Here, we mean ω is holomorphic if $\operatorname{ord}_P(\omega) \geq 0$ for all $P \in C(K)$. Indeed, if $f \in \mathcal{L}(K_C)$, then $\operatorname{div}(f) \geq -\operatorname{div}(\omega)$, or $\operatorname{div}(f\omega) \geq 0$, meaning $f\omega$ is holomorphic.

Example 3.15 (Projective Line)**.** Let $C = \mathbb{P}^1$ with homogeneous coordinates $[X : Y]$. Consider the affine coordinate $t = X/Y$ over $C - \infty$ (with $\infty = [1 : 0]$ per usual). We will compute $\operatorname{div}(dt)$.

For $P \in \mathbb{A}^1(K)$, we have that $t - P$ is a uniformizer at P, meaning $\operatorname{ord}_P(t - P) = 1$. Note $dt = d(t - P)$, so $\operatorname{ord}_P(dt) = \operatorname{ord}_P(t - P) - 1 = 0$. For $P = \infty$, we consider the uniformizer $u = 1/t$. We have $du = -1/t^2\,dt$, so $dt = -t^2\,du = -1/u^2\,du$, and so $\operatorname{ord}_\infty(dt) = -2$. Taking all of this together, we get

$$\operatorname{div}(dt) = -2 \cdot [\infty].$$

So note that divisors of differential forms need not be degree 0.

Now we show the genus of $\mathbb{P}^1$ is 0 as expected. Let $\omega \in \Omega_C$ be non-zero. We can write $\omega = f\,dt$, and so $\operatorname{div}(\omega) = \operatorname{div}(f) + \operatorname{div}(dt)$. But $\deg \operatorname{div}(f) = 0$ and $\operatorname{div}(dt) = -2[\infty]$ from above, so $\operatorname{div}(\omega) \not\geq 0$. In other words, ω cannot be holomorphic, so there are no holomorphic differential forms on $\mathbb{P}^1$. It follows that $g(\mathbb{P}^1) = 0$.

Example 3.16 (Elliptic Curve)**.** Assume here $\operatorname{char} K \neq 2, 3$. Choose distinct values $e_1, e_2, e_3 \in K$, and let $C \subset \mathbb{P}^2$ be the curve given by the equation

$$Y^2Z = (X - e_1Z)(X - e_2Z)(X - e_3Z).$$

This is a smooth curve which passes through the four points $P_i = [e_i : 0 : 1]$ and $\infty = [0 : 1 : 0]$.

Now consider the affine plane $\mathbb{A}^2 \subset \mathbb{P}^2$ with coordinates $x = X/Z$ and $y = Y/Z$. Our curve C in $\mathbb{A}^2$ is given by $y^2 = f(x) \coloneqq (x - e_1)(x - e_2)(x - e_3)$. We now proceed

to compute $\operatorname{div}(y)$. Note that we only need to consider the points P_i and ∞, as $y = 0$ only at the points P_i and y is a pole only at ∞.

Consider when $P = P_i$. The maximal ideal $\mathfrak{m}_P$ is generated by $(x - e_i)$ and y. Clearly, $y \in \mathfrak{m}_P$, but

$$\mathfrak{m}_P^2 = ((x-e_i)^2, (x-e_i)y, y^2) \subset (x - e_i)$$

since $y^2 = f(x) \in (x - e_i)$. As $y \notin (x - e_i)$, we conclude $\operatorname{ord}_{P_i}(y) = 1$. In order to ensure $\deg \operatorname{div}(y) = 0$, we also conclude $\operatorname{ord}_\infty(y) = -3$. Collecting gives

$$\operatorname{div}(y) = [P_1] + [P_2] + [P_3] - 3[\infty].$$

In a similar fashion, we can also show

$$\operatorname{div}(x - e_i) = 2[P_i] - 2[\infty].$$

Now we can calculate $\operatorname{div}(dx)$. If $P = [x_0 : y_0 : 1]$ with $x_0 \neq e_i$, then $x - x_0$ is a uniformizer at P. We see now that from $dx = d(x - x_0)$, we get $\operatorname{ord}_P(dx) = 0$. At $P = P_i$, we no longer have $x - e_i$ as a uniformizer at P_i. Instead, we know $\operatorname{ord}_{P_i}(x - e_i) = 2$ from above. Letting t be a uniformizer at P_i, we get $x - e_i = c \cdot t^2$ for some constant c, and so $dx = d(x - e_i) = 2ct\,dt$. We thus conclude $\operatorname{ord}_{P_i}(dx) = 1$.

Finally, we consider $P = \infty$. Let t be a uniformizer at ∞. As $\operatorname{ord}_\infty(x) = -2$, we can do two change of variables ($x \mapsto 1/x \mapsto 1/t^2$) to conclude

$$\operatorname{ord}_\infty(dx) = \operatorname{ord}_{x=0}\left(-x^2\, d(1/x)\right) = \operatorname{ord}_{t=0}(-2t^3\, d(1/t)) = 3,$$

and so

$$\operatorname{div}(dx) = [P_1] + [P_2] + [P_3] - 3[\infty].$$

But this is exactly $\operatorname{div}(y)$! Thus, we conclude $\operatorname{div}(dx) = 0$ in $\operatorname{Pic}(C)$, so $g(C) = \dim \mathcal{L}(K_C) = \dim \mathcal{L}(0) = \dim_K K = 1$. We also have $\operatorname{ord}_P(dx/y) = 0$ for any $P \in C(K)$, so dx/y is a holomorphic differential. In fact, since $g = 1$, it is the only holomorphic differential up to scalar. This now justifies why we consider the integral of $\frac{dx}{y}$ when constructing an elliptic curve from a lattice $\Lambda \subset \mathbb{C}$ in the uniformization of complex elliptic curves. (See §1.4.)

Now we can make sense of all components of the Riemann-Roch Theorem, which we know restate.

Theorem 3.17 (Riemann-Roch)**.** Carrying over all notation from above, we have

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Some immediate observations we can make. First, if $D = K_C$, then $\ell(K_C) = \ell(0) = \deg K_C - g + 1$. But $\ell(K_C) = g$ by definition and $\ell(0) = 1$, so $\deg K_C = 2g - 2$. If $\deg D > 2g-2$, then $\ell(K_C - D) = 0$ since $\deg(K_C - D) < 0$, and so $\ell(D) = \deg D - g + 1$. Finally, if $g = 1$, then we can use Riemann-Roch to show that C must be of the form given in Example 3.16, so $K_C = 0$. Thus, we have $\ell(D) - \ell(-D) = \deg D$.

Remark 3.18. Proving this is hard, of course. Whereas in the case of Riemann surfaces, one may hope to construct functions explicitly satisfying certain order conditions, there is little hope to do this over an arbitrary field. The interpretation Serre came up with is to see $\ell(D)$ as the dimension of some zeroth sheaf cohomology and $\ell(K_C - D)$ as dimension of the first cohomology, and this is how Grothendieck was able to prove Riemann-Roch in the general setting.

4 11/19 - Elliptic Curves (at last)

4.1 Elliptic Curves

We can finally talk about elliptic curves in generality, not just over $\mathbb{C}$. Let K be a perfect field with algebraic closure $\overline{K}$.

Definition 4.1 (Elliptic Curve)**.** An **elliptic curve** over K is a smooth projective curve E of genus 1 with a specified K-rational point $O \in E(K)$.

Example 4.2 (Legendre Form)**.** Let $\lambda \in K - \{0, 1\}$. Then, the curve $E_\lambda \subset \mathbb{P}^2_K$ defined by $Y^2Z = X(X - Z)(X - \lambda Z)$ with $O = [0 : 1 : 0]$ is an elliptic curve.

We have some non-examples as well:

Example 4.3 (Curve with Singularity)**.** The curve given by the affine equation $y^2 = x^3$ has a singularity at $P = (0, 0)$. Indeed, one can compute that the dimension of the tangent space at P, i.e., $\dim \mathfrak{m}_P/\mathfrak{m}_P^2$, is 2, with basis $\{x, y\}$.

Example 4.4 (Quartic)**.** Let $f \in K[x]$ be a degree-4 polynomial without a double root. The affine curve given by $y^2 = f(x)$ is smooth, but the projective curve $Y^2Z^2 = f(X, Z)$ is singular at ∞. (Take partial derivatives and evaluate at $[0 : 1 : 0]$.) Thus, for instance, the curve over $\mathbb{Q}$ given by $y^2 = -x^4 - 1$ is not an elliptic curve.

We can consider the normalization of such a curve, but it no longer embeds into $\mathbb{P}^2$. Instead, we can consider the curve $C \subset \mathbb{P}^3$, with coordinates $[x : y : z : t]$, defined by $y^2 = f(x)$ and $z = x^2$. This curve has genus 1, but it does not necessarily have K-rational points.

Proposition 4.5 (Abel-Jacobi Map)**.** Let (E, O) be an elliptic curve. The **Abel-Jacobi map**

$$\begin{aligned} AJ : E(\overline{K}) &\to \mathrm{Pic}^0(E) \\ P &\mapsto \text{class of } [P] - [O] \end{aligned}$$

is a bijection, equivariant under the $\mathrm{Gal}(\overline{K}/K)$-action.

Proof. Since $O \in E(K)$, we have $\sigma(O) = O$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Thus, we have

$$AJ(\sigma(P)) = [[\sigma(P)] - [O]] = [[\sigma(P)] - [\sigma(O)]] = \sigma \cdot [[P] - [O]] = \sigma \cdot AJ(P),$$

showing $\mathrm{Gal}(\overline{K}/K)$-equivariance.

For injectivity, suppose $AJ(P) = AJ(Q)$ for $P, Q \in E(\overline{K})$. Equality in $\mathrm{Pic}^0(E)$ means there exists some $f \in \overline{K}(E)$ such that $\mathrm{div}(f) = [P] - [Q]$. As $[P] - [Q] \geq -[Q]$, we have $f \in \mathcal{L}([Q])$. But by Riemann-Roch, we cam compute

$$\ell([Q]) - \ell(K_E - [Q]) = \deg[Q] - g + 1.$$

We have $\ell(K_E - [Q]) = 0$ since $\deg(K_E - [Q]) = -1$, and we know $\deg[Q] - g = 1 - 1 = 0$. Thus, $\ell([Q]) = 1$, meaning $\mathcal{L}([Q]) = \overline{K}$, so f is constant. This forces $[P] - [Q] = \mathrm{div}(f) = 0$, hence $P = Q$.

For surjectivity, let $D \in \mathrm{Div}^0(E)$. By Riemann-Roch, we have

$$\ell(D + [O]) = \ell(D + [O]) - \ell(K_E - D - [O]) = \deg(D + [0]) - g + 1 = 1,$$

so $\ell(D + [O]) = 1$. Choose any nonzero $f \in \mathcal{L}(D + [O])$; by definition, it must satisfy

$$\mathrm{div}(f) + D + [O] \geq 0.$$

The left side is an effective divisor of degree 1, aka of the form $[P]$, and so we get $\mathrm{div}(f) + D = [P] - [O]$ for some $P \in E(\overline{K})$. This means $D = [P] - [O]$ in $\mathrm{Pic}^0(E)$, as desired. □

This Abel-Jacobi map is remarkable because it now allows us to put an *abelian group structure on $E(\overline{K})$ that has a natural $\mathrm{Gal}(\overline{K}/K)$-action.* In general, we can define an Abel-Jacobi map to a family of varieties called **abelian varieties**, of which elliptic curves are the ones with dimension 1. More explicitly, we can define a *group law* on $E(\overline{K})$ where given $P, Q \in E(\overline{K})$, the point $P + Q$ is the unique point such that $[P + Q] \sim [P] + [Q] - [O]$.

Theorem 4.6. Let (E, O) be an elliptic curve over K.

1. There exist $x, y \in K(E)$ which induces an isomorphism between E and the smooth projective curve given by the (Weierstrass) equation

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

   where $x = X/Z$, $y = Y/Z$, and $a_i \in K$. This isomorphism sends O to $[0 : 1 : 0]$.

2. Two such equations define isomorphic elliptic curves if and only if there exists

a change of variables of the form

$$x' = u^2 x + r$$
$$y' = u^3 y + u^2 s x + t$$

with $u, r, s, t \in K$ and $u \neq 0$.

Proof of (1). The first statement begins with a slick application of Riemann-Roch. We can use Riemann-Roch on $D = n[O]$ for $n \geq 1$ to compute $\ell(n[O]) = n$. For small values of n, we can explicitly find a basis for $\mathcal{L}(n[O])$:

$$\mathcal{L}([O]) = \langle 1 \rangle, \qquad \mathcal{L}(2[O]) = \langle 1, x \rangle, \qquad \mathcal{L}(3[O]) = \langle 1, x, y \rangle.$$

We thus conclude $\operatorname{ord}_O(x) = -2$ and $\operatorname{ord}_O(y) = -3$. But now when considering $\mathcal{L}(6[O])$, which has dimension 6, we can produce 7 distinct elements: $1, x, y, x^2, xy, y^2, x^3$. Thus, they must be linearly dependent, so there exist $A_1, \ldots, A_7 \in K$ such that

$$0 = A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3.$$

Consider the order of the pole at 0, we get that $\operatorname{ord}_O(x^3) = \operatorname{ord}_O(y^2) = -6$. These must cancel, so we require $A_6 = -A_7 \neq 0$. (If both were 0, then we would require $A_i = 0$ else 0 has a pole at 0 of order i, which is nonsense.) Replacing x with $-A_6 A_7^2 x$ and y with $A_6 A_7^2 y$, we can divide by $A_6^3 A_7^4$ to get the desired form, albeit still in affine form (dehomogenized).

But we can extend the map $\varphi : E - \{0\} \to \mathbb{P}^2$ sending $P \mapsto [x(P) : y(P) : 1]$ to a morphism of algebraic varieties $\varphi : E \to C \subset \mathbb{P}^2$ which sends 0 to $[0 : 1 : 0]$. Here, C is the curve defined by the homogenized form of the equation as given in the theorem statement. It remains to show that φ is an isomorphism, and that the curve given by the Weierstrass equation is smooth.

Let $\varphi : C \to C'$ be a non-constant morphism. Recall we define the **degree** of φ as the degree of the field extension $[\overline{K}(C) : \varphi^* \overline{K}(C')]$, and that φ is an isomorphism iff $\deg \varphi = 1$. (Here, $\varphi^* : \overline{K}(C') \to \overline{K}(C)$ denotes the pullback, which is injective since φ must be surjective. It is always true that this field extension is finite, hence we can make sense of the degree.) Also recall that the degree can also be determined by the ramification indices: if the ramification index of φ at P is defined as $e_\varphi(P) \coloneqq \operatorname{ord}_P(\varphi^* t_{\varphi(P)})$, where $t_{\varphi(P)}$ is a uniformizer at $\varphi(P)$, then

$$\deg \varphi = \sum_{\varphi(P) = Q} e_\varphi(P).$$

(Note that we always have $e_\varphi(P) \geq 1$ by $(\varphi^* t_{\varphi(P)})(P) = 0$.)

We can now show that $\deg \varphi = 1$ if and only if $\overline{K}(E) = \overline{K}(x, y)$. Note by default that $\overline{K}(x, y) \subseteq \overline{K}(E)$. First, we can show $[\overline{K}(E) : \overline{K}(x)] = 2$ and $[\overline{K}(E) : \overline{K}(y)] = 3$.

For the former, we just need to compute the degree of the morphism $x : E \to \mathbb{P}^1$. This is just

$$\deg x = e_x(0) = -\operatorname{ord}_O(x) = 2.$$

Likewise, $\deg(y : E \to \mathbb{P}^1) = -\operatorname{ord}_O(y) = 3$. By multiplicativity of field extension degrees, we have $[\overline{K}(E) : \overline{K}(x, y)] \mid 2, 3$, which forces $[\overline{K}(E) : \overline{K}(x, y)] = 1$. Hence, φ is an isomorphism.

The one final check to show is that our projective curve is indeed smooth. Denote our equation as $F(X, Y, Z) = 0$. We see that our curve C is smooth at $[0 : 1 : 0]$ because $\frac{\partial F}{\partial Z}(O) \neq 0$. Note now that if C is singular, then there must exist a singularity in some affine chart. Translating appropriately, we may suppose it has a singularity at $(0, 0)$. The Jacobian criterion then forces the affine equation to look like

$$C : y^2 + a_1xy - a_2x^2 - x^3 = 0.$$

Now consider the map $C \to \mathbb{P}^1$ sending $(x, y) \mapsto [x : y]$. We can show that it admits an inverse, and hence is of degree 1. We claim that the map

$$\begin{aligned} \mathbb{P}^1 &\to C \\ [1 : t] &\mapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t) \end{aligned}$$

is the inverse, where $t = y/x$. I will omit the computation, but just plug in $t = y/x$ into the above expression and you should recover (x, y).

The punchline is that $\deg \varphi = 1$ implies $E \simeq \mathbb{P}^1$, which is absurd since $g(E) = 1$ but $g(\mathbb{P}^1) = 0$. Hence, C has no singularities, so E is smooth. □

Proof of (2). Note that for two Weierstrass equations, one given by variables $\{x, y\}$ and the other by $\{x', y'\}$, we have $\{1, x\}$ and $\{1, x'\}$ are both bases of $\mathcal{L}(2[O])$, and that $\{1, x, y\}$ and $\{1, x', y'\}$ are both bases of $\mathcal{L}(3[O])$. Thus, there exist $\lambda, \mu, r, s, t \in K$ (with $\lambda, \mu \neq 0$) such that

$$\begin{aligned} x' &= \lambda x + r \\ y' &= \mu y + sx + t. \end{aligned}$$

For the coefficients to be the same, we can compute that $\lambda^3 = \mu^2$. Now, taking $u = \lambda/\mu$, we get $\lambda = u^2$ and $\mu = u^3$, as desired. □

5 11/25 - Group Law on Elliptic Curve

We now interpret the group law on $E(K)$ geometrically.

Proposition 5.1. Let (E, O) be an elliptic curve and $P, Q, R \in E$. The following conditions are equivalent:

1. $P + Q + R = O$.
2. There exists a line $L \subset \mathbb{P}^2$ such that $[E \cap L] = [P] + [Q] + [R]$.

Denoting L_p as the equation of L at p (which usually just means take the affine equation for L on an affine containing p), the term $[E \cap L]$ is the **intersection divisor**, defined as

$$[E \cap L] \coloneqq \sum_{p \in E \cap L} \dim_K(\mathcal{O}_{E,p}/L_p)[p]$$

Proof. We first show (1) implies (2). Note that under the map $E \to \mathrm{Pic}^0(E)$ taking $P \mapsto [[P] - [O]]$ (I will also denote it as $\overline{[P] - [O]}$), the assumption from (1) gives us

$$[P] - [O] + [Q] - [O] + [R] - [O] \sim 0.$$

Thus, there exists some $f \in K(E)^\times$ such that

$$\mathrm{div}(f) = [P] + [Q] + [R] - 3[O].$$

In particular, as $f \in \mathcal{L}(3[O])$, there exists coefficients $a, b, c \in K$ such that $f = ax + by + c$, since $\{1, x, y\}$ forms a basis of $\mathcal{L}(3[O])$. Therefore, we may take the line with equation $L : aX + bY + cZ = 0$ and now show (2) holds. Let $s \in E \cap L$.

First, suppose $s \neq O$, and WLOG take $s \in \mathbb{P}^2 - \{Z = 0\}$. Dehomogenizing $x = X/Z$, $y = Y/Z$, we obtain the affine equation for $E - \{O\}$ as $g(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0$, and for $L - \{Z = 0\}$ as $f = ax + by + c = 0$. Now, note that

$$\dim_K K[x, y]_s/(f, g(x, y)) = \mathrm{ord}_s(f),$$

and so on $E - \{O\}$, we have

$$[E \cap L]|_{E-\{O\}} = \sum_{s \in E - \{O\}} \mathrm{ord}_s(f)[s].$$

Now suppose $s = O$. Now dehomogenize via $u = X/Y$ and $v = Z/Y$ to get affine equations

$$\begin{aligned} E \setminus \{Y = 0\} &: v + a_1uv + a_3v^2 - u^3 - a_2u^2v - a_4uv^2 - a_6v^3 = 0 \\ L &: au + b + cv = 0. \end{aligned}$$

Now we consider

$$K[u, v]/(au + b + cv, v + a_1uv + \cdots).$$

We will now determine the valuation of $au + b + cv$ at the point $s = O$. Taking $au + b + cv = a\frac{X}{Z}\frac{Z}{Y} + b + c\frac{Z}{Y}$, we have

$$\begin{aligned} au + b + cv &= a\frac{X}{Z}\frac{Z}{Y} + b + c\frac{Z}{Y} \\ &= a\frac{x}{y} + b + \frac{c}{y} \\ &= y^{-1}f. \end{aligned}$$

Thus, the part of $[E \cap L]$ supported on O is given by $\mathrm{ord}_O(y^{-1}f) = \mathrm{ord}_O(f) + 3[O]$. Enumerating in total, we now get

$$\begin{aligned} [E \cap L] &= \sum_{s \in E} \mathrm{ord}_s(f)[s] + 3[O] \\ &= \mathrm{div}(f) + 3[O] \\ &= [P] + [Q] + [R], \end{aligned}$$

as desired.

We now prove (2) implies (1). Let $L : aX+bY+cZ = 0$ be a line. Let $f \coloneqq ax+by+c$. In a similar manner to above, we can show

$$[E \cap L] = \mathrm{div}(f) + 3[O],$$

and so

$$\mathrm{div}(f) = [P] + [Q] + [R] - 3[O] = ([P] - [O]) + ([Q] - [O]) + ([R] - [O]).$$

Taking the inverse of the Abel-Jacobi map and noting that $\mathrm{div}(f) = 0$ in $\mathrm{Pic}^0(E)$, we get $P + Q + R = O$ as desired. □

We hope that we can equip E with an *algebraic group* structure, since it seems to admit both an algebraic variety structure and a group law. We need to check that multiplication and the inverse map are both K-variety morphisms.

Theorem 5.2. The group law $E \times E \to E$ is a morphism of K-varieties.

We must prove a few lemmata beforehand.

Lemma 5.3. *Let $P = (x_0, y_0) \in E - \{O\}$. Then, $-P = (x_0, y_0')$ and y_0, y_0' are roots of a polynomial of the form $y^2 + (a_1x_0 + a_3)y + C = 0$ for some constant C.*

Proof. Let $L : aX + bY + cZ = 0$ be the line in $\mathbb{P}^2$ that passes through the points O and P. As L passes through $O = [0 : 1 : 0]$, we have $b = 0$. As L passes through P, we get $ax_0 + c = 0$. We can thus write L as

$$L : X - x_0Z = 0.$$

Additionally, we know $-P$ is a point on L by the above proposition, so by the above equation for L, the x-coordinate for $-P$ must be x_0. Thus, we have $-P = (x_0, y_0')$ for some $y_0' \in K$. The fact that both $P = (x_0, y_0)$ and $-P = (x_0, y_0')$ satisfy the affine Weierstrass equation gives us the polynomial condition, where the constant term is $C = -(x_0^3 + a_2x_0^2 + a_4x_0 + a_6)$. □

We now show that the inverse map is an automorphism of K-varieties, as we sought. Additionally, translation is an automorphism as well.

Lemma 5.4. *Let (E, O) be an elliptic curve over K.*

1. *The inverse map $E \to E$ sending $R \mapsto -R$ is an involution (automorphism) defined over K.*
2. *For all $Q \in E(K)$, the translation map $t_Q : E \to E$ sending $R \mapsto R + Q$ is an automorphism of varieties defined over K.*

Proof. Let $P, Q \in E$. We consider the divisor $[P]+[Q]$, which has degree $2 \geq 2g-1 = 1$. Thus, Riemann-Roch tells us that $\mathcal{L}([P] + [Q])$ has dimension 2 over K, meaning there must exist some nonconstant $f \in \mathcal{L}([P] + [Q])$. Even more, it must have a pole at both P and Q – if it only had one pole, then it must be constant via $\ell([P]) = \ell([Q]) = 1$.

Now consider the map $\varphi_f : E \to \mathbb{P}^1_K$ given by f. Since P and Q are the only poles, and they are simple, we have

$$\varphi_f^*([\infty]) = [P] + [Q] \implies \deg \varphi_f = 2 = [K(E) : K(f)].$$

We assert that φ_f must be separable. If it were inseparable, then we must have $K(E) = K(f^{1/2})$, which would imply $E \simeq \mathbb{P}^1$. But this is impossible because they have different genus.

But now we have φ_f is a degree-2 separable map, so it must be Galois. Thus, any $\sigma \in \mathrm{Gal}(K(E)/K(f))$ uniquely corresponds to some automorphism $\sigma_{P,Q} : E \to E$ which preserves φ_f, i.e., it satisfies $\varphi_f \circ \sigma_{P,Q} = \varphi_f$. As φ_f is Galois, $\sigma_{P,Q}$ acts transitively on each fiber of φ_f, meaning in particular that $\sigma_{P,Q}(P) = Q$.

Suppose $R \in E \setminus \{P, Q\}$. Considering the function $f - f(R) \in K(f)$, we have that

$$\mathrm{div}(f - f(R)) = [R] + [\sigma(R)] - [P] - [Q],$$

so $[R] + [\sigma(R)] \sim [P] + [Q]$ in $\mathrm{Pic}(E)$. Now we are ready to prove the lemma.

For (1), we take $P = Q = O$, and so for any $R \neq O$, we have $[R] + [\sigma_{O,O}(R)] \sim 2[O]$. By our above proposition/Abel-Jacobi, we conclude $\sigma_{O,O}(R) = -R$. Since $\sigma_{O,O}$ is a morphism of K-varieties, this proves (1).

For (2), we take $P = O$ and $Q \neq O$. Then, we get $\sigma_{O,Q}(R) = Q - R = -t_{-Q}(R)$, so

$$\sigma_{O,Q} \circ \sigma_{O,O}(R) = \sigma_{O,Q}(-R) = -t_{-Q}(-R) = t_Q(R),$$

so $t_Q = \sigma_{O,Q} \circ \sigma_{O,O}$ is a morphism of K-varieties. □

Now we will prove Theorem 5.2.

Proof of Theorem 5.2. First, suppose $P, Q \in E - \{O\}$ and that $P \neq \pm Q$. The latter assumption ensures that the line passing through P and Q (a) is well-defined (since $P \neq Q$) and (b) does not pass through O (as otherwise $P = -Q$ by Proposition 5.1). Denote this line L_{PQ}, and give it an equation $L_{PQ} : aX + bY + cZ = 0$. Also write $P = [x(P) : y(P) : 1]$ and likewise for Q. We thus have

$$ax(P) + by(P) + c = ax(Q) + by(Q) + c = 0.$$

We may choose values $a = y(P) - y(Q)$, $b = x(P) - x(Q)$, and $c = x(Q)y(P) - x(P)y(Q)$. Note that as $O = [0 : 1 : 0] \notin L_{PQ}$, we necessarily have $b \neq 0$.

Let $[x_0 : y_0 : 1]$ be a point of intersection between E and L_{PQ}. Substituting $y_0 = -\frac{a}{b}x_0 - \frac{c}{b}$ into the affine Weierstrass equation for E, we obtain

$$0 = x_0^3 + \left(a_2 - \frac{a^2}{b^2} + \frac{a}{b}a_1\right) x_0^2 + O(x_0).$$

Note that the only points in $E \cap L_{PQ}$ are P, Q, and $-(P+Q)$, and so the roots of the above cubic are $x(P)$, $x(Q)$, and $x(-(P+Q)) = x(P+Q)$ (by Lemma 5.3). Using our chosen values for a and b, we now have

$$x(P+Q) = -a_2 + \left(\frac{y(P) - y(Q)}{x(P) - x(Q)}\right)^2 + a_1 \left(\frac{y(P) - y(Q)}{x(P) - x(Q)}\right) - x(P) - x(Q),$$

which gives us the addition law for the x-coordinate. Using now $y_0 = -\frac{a}{b}x_0 - \frac{c}{b}$, we also have the addition law for the y-coordinate:

$$\begin{aligned} y(P+Q) &= -a_1 x(P+Q) - a_3 - y(-(P+Q)) && \text{Lemma 5.3} \\ &= -a_1 x(P+Q) - a_3 + \frac{y(P) - y(Q)}{x(P) - x(Q)} x(P+Q) + \frac{x(Q)y(P) - x(P)y(Q)}{x(P) - x(Q)} \\ &= \left(-a_1 + \frac{y(P) - y(Q)}{x(P) - x(Q)}\right) x(P+Q) + \left(-a_3 + \frac{x(Q)y(P) - x(P)y(Q)}{x(P) - x(Q)}\right). \end{aligned}$$

Now we pass to the general setting. Note that we have been working in the Zariski-open

$$U = \{(P, Q) \in (E - \{O\})^2 \mid P \neq \pm Q\} \subset E(K).$$

In general, we have $P + Q = t_{-R}(t_R(P) + Q)$. Then, $+ = t_{-R} \circ + \circ (t_R \times \mathrm{id})$ defines the group law on $V_R \coloneqq (t_R \times \mathrm{id})^{-1}(U)$. This now allows us to define the group law on all of E, as $\{V_R\}$ is an open cover of E. □

Example 5.5. Let $E/\mathbb{Q}$ be given by the equation $y^2 = x^3 + 17$. By trying out small values, we can find some integral points

$$P_1 = (-2, 3), \quad P_2 = (-1, 4), \quad P_3 = (2, 5), \quad P_4 = (4, 9), \quad P_5 = (8, 23), \ldots$$

One can compute explicitly $P_5 = -2P_1$, $P_4 = P_1 - P_3$, etc. We can also compute sums such as

$$P_2 + P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

In fact, it turns out that P_1 and P_3 generate all of $E(\mathbb{Q})$, and so $E(\mathbb{Q}) = \mathbb{Z}P_1 \oplus \mathbb{Z}P_3 \simeq \mathbb{Z} \times \mathbb{Z}$.

6 11/26 - Morphisms of Elliptic Curves

We will primarily study $E(K)$, its finite subgroups, and $\mathrm{End}(E)$. Most notable of the finite subgroups are the subgroups of n-torsion points, denoted $E(K)[n]$. Over $\mathbb{C}$, we have $E(\mathbb{C}) = \mathbb{C}/\Lambda$, and so $E(\mathbb{C})[n] = \frac{1}{n}\Lambda/\Lambda \simeq (\mathbb{Z}/n\mathbb{Z})^2$. We hope to replicate results just as nice for arbitrary K.

6.1 Morphism as Group Morphism

We naturally want to study morphisms between elliptic curves. Such a morphism should respect both the variety structure of E as well as the group structure of $E(K)$. Fortunately, the latter comes for free.

Lemma 6.1. *Let (E, O) and (E', O') be elliptic curves over K. Let $\varphi : E \to E'$ be a morphism of K-varieties with $\varphi(O) = O'$. Then, φ is also a group morphism.*

Proof. Note that φ induces a morphism on the divisor groups

$$\begin{aligned} \varphi_* : \mathrm{Div}(E') &\to \mathrm{Div}(E) \\ [P] &\mapsto \sum_{Q \in \varphi^{-1}(P)} e_\varphi(Q)[Q]. \end{aligned}$$

One can see from the definition that $\deg(\varphi_* D) = \deg(\varphi) \deg D$. In particular, φ_* induces a map $\mathrm{Div}^0(E) \to \mathrm{Div}^0(E')$.

If $f \in \overline{K}(E)^\times$, then $\varphi_*(\mathrm{div}\, f) = \mathrm{div}(\varphi_* f)$. Thus, φ_* sends $\mathrm{Prin}(E) \to \mathrm{Prin}(E')$, meaning it induces a morphism $\mathrm{Pic}(E) \to \mathrm{Pic}(E')$. For $P \in E(K)$, we have $\varphi_*([P] - [O]) = [\varphi_*(P)] - [\varphi_*(O)]$. The latter term is just $[O']$, and so φ_* is a group morphism. □

6.2 Isogeny

Because the group morphism structure comes for free so long as $O \mapsto O'$ (Lemma 6.1), we can take the following as our definition of morphisms:

Definition 6.2 (Morphism, Isogeny)**.** A **morphism** of elliptic curves is a morphism of K-varieties $\varphi : E \to E'$ with $\varphi(O) = O'$. A nonconstant morphism between elliptic curves is called an **isogeny**.

Note that the set of morphisms $\mathrm{Hom}(E, E')$ form an abelian group via $(\varphi+\psi)(P) \coloneqq \varphi(P) + \psi(P)$, where addition on the right is taken in $E'(K)$. Even better, the set of endomorphisms $\mathrm{End}(E)$ forms an **endomorphism ring**, where the multiplication rule is composition.

Proposition 6.3 (Finite subgroups as kernels)**.** The kernel of an isogeny is a finite subgroup of $E(K)$, and any finite subgroup is the kernel of some isogeny.

Proof. Let φ be an isogeny. The fact that $\ker\varphi$ is a subgroup comes from Lemma 6.1 since then φ is a group homomorphism. It is finite because $\ker\varphi = \varphi^{-1}(O')$ and fibers of nonconstant maps are finite. (It is a closed proper subset of E under the Zariski topology.)

Now suppose $H \subset E(K)$ is a finite subgroup. Consider the translation map $t_h : E \to E$ mapping $P \mapsto P + h$ for all $h \in H$. Reformulating in terms of function fields, t_h corresponds to some $\sigma_h \in \mathrm{Aut}(K(E))$, and we can identify H with the subgroup $\{\sigma_h \mid h \in H\} \subset \mathrm{Aut}(K(E))$, which we also call H.

Let $K(E)^H$ be the subfield of $K(E)$ fixed by H. By the Fundamental Theorem of Galois Theory, this is a Galois extension with Galois group H. But the equivalence between function fields and smooth projective curves guarantees such a curve C with $K(C) \cong K(E)^H$, and the extension $K(E)^H \subset K(E)$ corresponds to a morphism $\varphi : E \to C$.

We now claim that this is an isogeny, with $\ker\varphi = H$. We must show, in particular, that C is an elliptic curve, i.e., it has genus 1.

As φ is Galois, we have $|H| = \deg(\varphi) = e_P(\varphi)\cdot|\varphi^{-1}(P)|$ for all $P \in C$. Furthermore, we claim that φ is constant on the H-orbits in E. Suppose we had some $h \in H$ such that $\varphi(h + P) \neq \varphi(P)$. Then, we could find some $f \in K(C)$ with a pole at P but not at $h + P$. This would contradict the invariance of $K(C)$ under action by H, so we conclude φ is constant on its fibers. In particular, this means that $|\varphi^{-1}(P)| \geq |H|$ since the size of any H-orbit is H. The above equality forces $|\varphi^{-1}(P)| = |H|$, meaning $e_P(\varphi) = 1$ and hence φ is unramified everywhere. Riemann-Hurwitz then tells us

$$0 = 2g(E) - 2 = \deg(\varphi)(2g(C) - 2) = |H| \cdot (2g(C) - 2).$$

This forces $2g(C) - 2 = 0$, so $g(C) = 1$ as desired. Taking $O' = \varphi(O)$ makes (C, O') into an elliptic curve and $\varphi : E \to C$ into an isogeny. But now we can see $H \cong \varphi^{-1}(O')$ where $h \mapsto h + O$, so indeed $H = \ker\varphi$ as sought. □

Example 6.4 (Multiplication-by-m)**.** We can take the subgroup of m-torsion points in E, denoted $E[m]$. What isogeny has kernel $E[m]$? Consider the multiplication-by-m map

$$[m] : E \to E.$$

This is special because it is an endomorphism. The aside in §1.6 tells us that, when $K \subset \mathbb{C}$, these are usually the only endomorphisms of E, and that elliptic curves which admit endomorphisms beyond just $\mathbb{Z}$ have very special properties.

Claim 6.5. Suppose $\operatorname{char} K \neq 2$ and $|E(K)| > 4$. The multiplication-by-m map $[m] : E \to E$ is not trivial, and hence non-constant.

Proof. It suffices to show this for prime m. When m is odd, it suffices to show there exists a point in $E(\overline{K})$ of order 2, as if P has order 2, then $[m]P = [2k+1]P = [k][2]P + P = P \neq O$. We employ an argument similar to that in the proof of Lemma 5.4. Let $P = Q = O$, take $x \in \mathcal{L}(2[O]) - \overline{K}$, and consider $\varphi_x : E \to \mathbb{P}^1_K$. This is separable whose fibers are of the form $\{P, -P\}$. (If $P = (x, y)$ is in the fiber, then so is $(x, -y) = -P$.) Since $\deg \varphi_x = 2$, we have the ramification degree at any point is at most 2. Invoking Riemann-Hurwitz again, we have

$$\begin{aligned} 0 = 2g(E) - 2 &= (2g(\mathbb{P}^1_K) - 2) \cdot 2 + \sum_{P \in E} (e_{\varphi_x}(P) - 1) \\ &= -4 + \sum_{P \in E} (e_{\varphi_x}(P) - 1), \end{aligned}$$

hence there are exactly 4 points which are ramified (where $e = 2$). Equivalently, there are 4 points such that $P = -P$, so this guarantees a 2-torsion points.

Furthermore, all points except 4 are not 2-torsion. Assuming $|E(K)| > 4$, this means we have a point which is not 2-torsion, hence [2] is also nontrivial. This exhausts all cases. □

Example 6.6 (Isogenies over $\mathbb{F}_p$)**.** If E is an elliptic curve over $\mathbb{F}_p$, then observe that $E(\mathbb{F}_p)$ is itself finite! We can consider it as a finite subgroup of $E(\overline{\mathbb{F}_p})$. Note that we can obtain $E(\mathbb{F}_p)$ by looking at the fixed points of the **Frobenius** Frob_p, and so

$$\operatorname{id} - \operatorname{Frob}_p : E \to E$$

is an isogeny. In particular, this means that whereas most elliptic curves over $K \subset \mathbb{C}$ do not have complex multiplication, all elliptic curves over finite fields have complex multiplication because of the Frobenius map.

Let $\varphi : E \to E'$ be an isogeny. We'd like to determine more information about $\ker \varphi$, as these give the finite subgroups. We will obtain $|\ker \varphi|$.

Lemma 6.7. *Let $\varphi : E \to E'$ be an isogeny, and take points $P \in E$ and $Q = \varphi(P)$. Then, $e_\varphi(P) = \deg_i(\varphi)$, where $\deg_i(\varphi)$ denotes the degree of the inseparable part of φ.*

Proof. We first prove this when φ is separable, i.e., when $\deg_i(\varphi) = 1$. Riemann-Hurwitz tells us

$$2g(E) - 2 = \deg \varphi \cdot (2g(E') - 2) + \sum_{P \in E} (e_\varphi(P) - 1).$$

Since $g(E) = g(E') = 1$, we get the sum on the right is 0. Hence, $e_\varphi(P) = 1 = \deg_i(\varphi)$ for all $P \in E$, and the statement is proven.

Now consider the general case. Recall that if $K \subset F$ is a finite field extension, then there exists an intermediate extension $K \subset L \subset F$ such that L/K is separable and F/L is purely inseparable. If $\operatorname{char} K = 0$, then F/K is purely separable. If $\operatorname{char} K = p$ and K is perfect, then there exists some h such that $F^{p^h} = L$. Thus, φ can be decomposed as $\varphi = \psi \circ \varphi_q$, where ψ is separable, $q = p^h$, and φ_q is the q-Frobenius morphism. This is ramified with ramification index q, but $\deg_i \varphi = \deg_i \varphi_q = q$, so equality holds. □

Now we can see $\deg \varphi$ in two different ways. First, we can break φ down into its separable and purely inseparable part, so $\deg(\varphi) = \deg_i(\varphi) \deg_s(\varphi)$. On the other hand, we have $\deg(\varphi) = e(Q|O')|\varphi^{-1}(O')| = \deg_i(\varphi) \cdot |\varphi^{-1}(O')|$, and so we conclude:

Proposition 6.8. Let $\varphi : E \to E'$ be an isogeny. We have

$$\#\ker \varphi = \deg_s \varphi.$$

We know that the following are separable isogenies, although we will prove them later.

Theorem 6.9. The isogeny $[m]$ is separable iff $(m, \operatorname{char} K) = 1$. Additionally, $\mathrm{id} - \mathrm{Frob}_p$ is always separable.

Author's Note 6.10. We provided a proof of each statement in different, later lectures. I am going ahead and proving the second statement here in more detail (the proof we did in class assumed the following lemma). The first statement is proved in the proof of Corollary 7.8.

To prove that these are separable, we will use the following separability criterion for maps between curves.

Lemma 6.11. *Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. Then, ϕ is separable if and only if the map $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is injective.*

Proof. We have to backfill on some things about differentials here. Proposition 3.9 tells us that each space of differentials is one-dimensional, so ϕ^* being injective is equivalent to being nonzero. Choose some $y \in \overline{K}(C_2)$ such that dy generates Ω_{C_2}. We can show that this is equivalent to the finite extension $\overline{K}(C)/\overline{K}(y)$ being separable. Indeed, Example 3.5 tells us $\overline{K}(C)/\overline{K}(y)$ is separable iff $\Omega_{\overline{K}(C)/\overline{K}(y)} = 0$. Then, taking $C/B/A = \overline{K}(C)/\overline{K}(y)/\overline{K}$, the exact sequence

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

tells us that $\overline{K}(C) \otimes_{\overline{K}(y)} \Omega_{\overline{K}(y)/\overline{K}} \twoheadrightarrow \Omega_{\overline{K}(C)/\overline{K}}$ is surjective. But the former has dimension 1 over $\overline{K}(C)$ with basis dy, so its image $dy \in \Omega_{\overline{K}(C)/\overline{K}}$ must be nonzero.

To summarize, since dy is a basis of Ω_{C_2}, we necessarily have $\overline{K}(C_2)/\overline{K}(y)$ is finite separable from the above, so $\phi^*\overline{K}(C_2)$ is separable over $\phi^*\overline{K}(y) = \overline{K}(\phi^* y)$.

Now we execute our proof. By definition, ϕ is separable iff $\overline{K}(C_1)/\phi^*\overline{K}(C_2)$ is separable. But this is separable iff $\overline{K}(C_1)/\overline{K}(\phi^* y)$ is separable, which in turn is separable iff $d(\phi^* y)$ is a basis for Ω_{C_1}, i.e., $d(\phi^* y) \neq 0$. This means ϕ^* is nonzero, as desired. □

Proof of Theorem 6.9. As mentioned before, we leave the proof of the first statement in the proof of Corollary 7.8. (The reason why we can't do it presently is because the map $[m]^*$ is very difficult to describe explicitly – the explicit formula for $m = 2$ (duplication of a point) was messy enough!)

For the Frobenius, note $\mathrm{Frob}_p^*(dx) = d(x^p) = p \cdot x^{p-1} d(x) = 0$. Thus, for any $0 \neq \omega \in \Omega_E$, we have

$$(\mathrm{id} - \mathrm{Frob}_p)^* \omega = \omega - \mathrm{Frob}_p^* \omega = \omega \neq 0,$$

so $\mathrm{id} - \mathrm{Frob}_p$ is separable by the lemma. □

6.3 Aside: Discriminant and j-invariant

Consider the Weierstrass equation ($A, B \in K$)

$$W_{AB} = W(x, y) : y^2 = x^3 + Ax + B.$$

Suppose $\mathrm{char}(K) \neq 2, 3$, in which case all elliptic curves can be written in this form. Furthermore, we showed that the only change of variables which preserve the Weierstrass equation are $(x, y) \mapsto (u^2 x, u^3 y)$ for $u \in K^\times$.

Definition 6.12 (Discriminant, j-invariant)**.** Define the **discriminant** of W_{AB} as

$$\Delta := -16(4A^3 + 27B^2).$$

The j-invariant of W_{AB} is given as

$$j := -1728 \frac{4A^3}{\Delta}.$$

Remark 6.13. Under the change of variables $(x, y) \mapsto (u^2 x, u^3 y)$, we have the following change of values:

$$A' = u^4 A, \quad B' = u^6 B, \quad \Delta' = u^{12} \Delta, \quad j' = j.$$

Consequently, the j-invariant does not depend on the specific Weierstrass equation, hence the name.

Proposition 6.14. The discriminant and j-invariant have the following properties:

1. The Weierstrass equation W_{AB} is not singular if and only if $\Delta \neq 0$.
2. If K is algebraically closed, then two elliptic curves with the same j-invariant are isomorphic.

3. Given $j_0 \in \overline{K}$, there exists an elliptic curve defined over $K(j_0)$ with j-invariant j_0.

Proof of (1). Consider the associated homogeneous equation in $\mathbb{P}^2_K$:

$$f(X,Y,Z) = Y^2Z - (X^3 + AXZ^2 + BZ^3) = 0.$$

We can show explicitly that $O = [0:1:0]$ is never singular: in particular, $\partial f/\partial Z$ at O is always 1.

Let $P = (x_0, y_0) \in E - \{O\}$ be a singular point. Then, we require the partial derivatives in both x and y to vanish at P, which comes out to $A = -3x_0^2$ and $y_0 = 0$. Plugging into the affine Weierstrass equation, we get

$$0 = y_0^2 = x_0^3 + Ax_0 + B = x_0^3 - 3x_0^3 + B,$$

so $B = 2x_0^3$. Calculating Δ given the explicit formula, we have

$$\Delta = -16(4A^3 + 27B^2) = -16(-4(3x_0^2)^3 + 27(2x_0^3)^2) = 0.$$

This demonstrates that E is non-singular if $\Delta \neq 0$.

Conversely, the above computation shows that the singular points of E, if there are any, must be of the form $(x_0, 0)$, and x_0 must be a double root of $P(x) = x^3 + Ax + B$. But this happens if and only if $\Delta = \mathrm{disc}(P) = 0$, so we conclude (1). □

The rest were completed in a separate TD session, but I did not transcribe. The proofs can be found under Proposition III.1.4 in Silverman.

7 12/2 - Special Morphisms

7.1 Frobenius Morphism

In the last lecture, we noted that the Frobenius morphism for elliptic curves over $\mathbb{F}_p$ always gives rise to an endormorphism not in $\mathbb{Z}$, meaning that all elliptic curves over finite fields have "complex multiplication" ($\mathrm{End}(E) \neq \mathbb{Z}$). We will now study this morphism in a more general setting, namely for any (perfect) field of characteristic $p > 0$.

As setup, let p be a prime number, K a perfect field of characteristic p, $q = p^r$ some prime power of p, $f \in K[X_0, \ldots, X_n]$ written as $f = \sum a_I X^I$ for $a_I \in K$, and $f^{(q)} = \sum a_I^q X^I$.

Let C be a projective curve over K. Consider the homogeneous ideal $I(C)$ of C, which is just

$$I(C) = \{f \in \overline{K}[X_0, \ldots, X_n] \mid f \text{ homogeneous}, f(P) = 0 \text{ for all } P \in C\}.$$

Definition 7.1. $C^{(q)}$ is the projective curve with homogeneous ideal $I(C^{(q)}) = \{f^{(q)} \mid f \in I(C)\}$.

This is a projective curve over K. We can now construct the **Frobenius morphism**

$$\varphi_q : C \to C^{(q)}$$
$$[X_0 : \cdots : X_n] \mapsto [X_0^q : \cdots : X_n^q].$$

One can check this is well-defined by construction. Indeed, let $P = [X_0 : \cdots : X_n] \in C$ and $f \in I(C)$ (so $f^{(q)} \in I(C^{(q)})$ by definition). Then, we have

$$f^{(q)}(\varphi_q(P)) = f^{(q)}(X_0^q, \ldots, X_n^q) = (f(X_0, \ldots, X_n))^q = 0$$

and so $\varphi_q(P) \in C^{(q)}$.

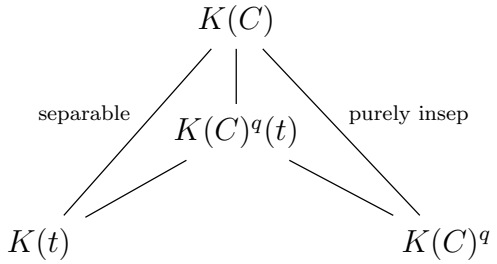
Proposition 7.2. Let φ_q be the Frobenius morphism defined above. It satisfies the following properties:

1. $\varphi_q^* K(C^{(q)}) = K(C)^q := \{f^q \mid f \in K(C)\}$.
2. φ_q is purely inseparable.
3. $\deg \varphi_q = q$.

Proof. For (1), we know that $K(C)$ is the set of all f/g, where $f, g \in K[X_0, \ldots, X_n]$ are homogeneous of the same degree and $g \notin I(C)$, modulo the standard equivalence $f/g \sim f'/g' \iff fg' - f'g \in I(C)$. Thus, every element in $\varphi_q^* K(C^{(q)})$ is of the form $f^{(q)}(X_0^q, \ldots, X_n^q)/g^{(q)}(X_0^q, \ldots, X_n^q)$. But $\operatorname{char} K = p$ and K is perfect, so both the numerator and denominator can be written in the form $f_0(X_0, \ldots, X_n)^q / g_0(X_0, \ldots, X_n)^q$ for some $f_0, g_0 \in K(C)$. This proves (1).

For (2), we really just need to invoke the following fact, which we have used before: every finite extension L/K can be split into a separable and purely inseparable part $L/K^{\text{sep}}/K$. Furthermore, $[L : K^{\text{sep}}] = p^n$ for some n, so for any $\alpha \in L$, there exists $n \geq 1$ such that $\alpha^{p^n} \in K^{\text{sep}}$. Here, we have φ_q is purely inseparable iff $K(C)/\varphi_q^* K(C^{(q)})$ is purely inseparable. We just showed $\varphi_q K(C^{(q)}) = K(C)^q$, so for any $f \in K(C)$, we have $f^q \in \varphi_q^* K(C^{(q)})$. Hence the extension is purely inseparable.

For (3), let $P \in C$ be a smooth point. Let t be a uniformizer at P. We have the following field extensions:



Note again that the bottom right is $K(C)^q = \varphi_q^* K(C)$ by (1). We know the big extension on the right is purely inseparable by (2). We also know the left extension $K(C)/K(t)$ is separable; this is shown in the proof of Lemma 6.11. (The proof outline: $K(C)/K(t)$ separable iff $\Omega_{K(C)/K(t)} = 0$ iff $dt \neq 0$, which is evident as it generates Ω_C. A more elementary proof that doesn't use differentials is in Silverman, Proposition II.1.4.) As a consequence, the extension $K(C)/K(C)^q(t)$ is an intermediate extension of both a separable and purely inseparable one. This is only possible if $K(C) = K(C)^q(t)$.

Now we have $\deg \varphi_q = [K(C) : \varphi_q^* K(C)] = [K(C)^q(t) : K(C)^q]$; it suffices to show that this degree extension is exactly q. Note first that $\deg \varphi_q \mid q$ since $t^q \in K(C)^q$. Since q is just some power of p, it suffices to show that $t^{q/p} \notin K(C)^q$. If we assume the contrary, then $t^{q/p} = f^q$ for some $f \in K(C)$. But then

$$q/p = \operatorname{ord}_P(f^q) = q \cdot \operatorname{ord}_P(f)$$

which would imply $\operatorname{ord}_P(f) = 1/p$. This is clearly not possible, and hence $\deg \varphi_q = q$ as desired. □

Corollary 7.3. *Let $\psi : C_1 \to C_2$ be a morphism between smooth curves over a field K with $\operatorname{char} K = p$. Then, we can decompose ψ as*

$$\psi : C_1 \xrightarrow{\varphi_q} C_1^{(q)} \xrightarrow{\lambda} C_2$$

with $q = \deg_i \psi$ and λ is separable.

In other words, the "only" inseparable morphism between smooth curves is the Frobenius morphism. Of course, we assume $\operatorname{char} K > 0$, as all morphisms are separable when $\operatorname{char} K = 0$.

Proof. Just look at the corresponding function field extension. We have $\deg \psi = [K(C_1) : \psi^* K(C_2)]$, and we can split this into $K(C_1)/\psi^* K(C_2)^{\text{sep}}/\psi^* K(C_2)$. Denote $F = \psi^* K(C_2)^{\text{sep}}$. We know that $K(C_1)/F$ is purely inseparable of degree $\deg_i \psi = q$. This means $K(C_1)^q \subset F$. But we also have $[K(C_1) : F] = [K(C_1) : K(C_1)^q] = q$, so the inclusion must be an equality. Thus, $F = K(C_1)^q = \varphi_q^* K(C_1)$, with the second equality coming from part (1) of the above proposition. The rest of the proof is just reformulating the fact about splitting a field extension into a separable and purely inseparable part for the morphism ψ. □

7.2 Dual Isogeny

Let E, E' be elliptic curves over some perfect field K, and let $\varphi : E \to E'$ be an isogeny. Although isogenies clearly do not need to be isomorphisms, we have a rough notion of an "inverse" given by the *dual isogeny*. This extra structure on $\operatorname{Hom}(E, E')$ allows us to prove many useful facts about isogenies, as we will see. For instance, it turns out that the composition of an isogeny ϕ and its dual $\widehat{\phi}$ gives the multiplication-by-$\deg(\phi)$ map, so we get a nice handle of the degree with other benefits (e.g., Corollary 7.11).

Recall the Abel-Jacobi map $E(\overline{K}) \to \mathrm{Pic}^0(E)$ sending P to the class of $[P]-[O]$. Now looking at divisors, we have the pullback map

$$\begin{aligned}\varphi^* : \mathrm{Pic}^0(E') &\to \mathrm{Pic}^0(E)\\ [P] &\mapsto \sum_{\varphi(Q)=P} e_\varphi(Q)[Q].\end{aligned}$$

This allows us to construct a map $\widehat{\varphi} : E'(\overline{K}) \to E(\overline{K})$ via

$$\widehat{\varphi} : E'(\overline{K}) \xrightarrow{AJ} \mathrm{Pic}^0(E') \xrightarrow{\varphi^*} \mathrm{Pic}^0(E) \xrightarrow{AJ^{-1}} E(\overline{K}).$$

What is this map, and how exactly does it relate to φ? We answer this now.

Let us closely track what $\widehat{\varphi}$ actually does. Let $Q \in E'(\overline{K})$. Then, considering $\widehat{\varphi}$ as a map on the Picard groups, we see $\widehat{\varphi}(Q)$ satisfies

$$[\widehat{\varphi}(Q)] - [O] = \varphi^*([Q]-[O']).$$

We will simplify the right hand side. Let $P \in E(\overline{K})$ with $\varphi(P) = Q$. Just by definition, we have

$$\varphi^*([Q]-[O']) = \sum_{T\in\varphi^{-1}(Q)} e_\varphi(T)[T] - \sum_{R\in\ker\varphi} e_\varphi(R)[R].$$

But note we can write $\varphi^{-1}(Q) = P + \ker\varphi$, so any $T \in \varphi^{-1}(Q)$ is of the form $P+R$ for some $R \in \ker\varphi$. But then in $\mathrm{Pic}^0(E)$, we have

$$[P+R]-[R] \sim [P]+[R]-[O]-[R] \sim [P]-[O].$$

Recall from Lemma 6.7 that the ramification index for an isogeny is the same for every point, namely $e_\varphi(R) = e_\varphi(T) = \deg_i\varphi$. We also have Proposition 6.8 which says $\#\ker\varphi = \deg_s\varphi$. Using both, we get

$$\begin{aligned}\varphi^*([Q]-[O']) &= \sum_{T\in\varphi^{-1}(Q)} e_\varphi(T)[T] - \sum_{R\in\ker\varphi} e_\varphi(R)[R]\\ &= \sum_{R\in\ker\varphi} e_\varphi(P+R)[P+R] - e_\varphi(R)[R]\\ &= \sum_{R\in\ker\varphi} \deg_i\varphi\cdot([P+R]-[R])\\ &= \deg_i\varphi\cdot(\#\ker\varphi)\cdot([P]-[O])\\ &= \deg_i\varphi\cdot\deg_s\varphi\cdot([P]-[O])\\ &= \deg\varphi\cdot([P]-[O]),\end{aligned}$$

thus $\widehat{\varphi}(Q) = [\deg\varphi]\cdot(P)$. Remembering $Q = \varphi(P)$, we are really saying $\widehat{\varphi}\circ\varphi = [\deg\varphi]$.

This is our dual isogeny, except we are missing one crucial fact: *we do not yet know this is an isogeny.* Indeed, finding a P such that $\varphi(P) = Q$ involves taking roots, so we cannot say that φ is a rational map. This requires us to define the dual isogeny in a slightly different way:

Theorem 7.4. Let $\varphi : E \to E'$ be an isogeny of degree m. Then, there exists a unique isogeny $\widehat{\varphi} : E' \to E$ such that

$$\widehat{\varphi} \circ \varphi = [m]_E.$$

In addition, it also satisfies $\varphi \circ \widehat{\varphi} = [m]_{E'}$ and $\widehat{\psi \circ \varphi} = \widehat{\varphi} \circ \widehat{\psi}$.

Definition 7.5 (Dual Isogeny)**.** Let $\varphi : E \to E'$ be an isogeny. The isogeny $\widehat{\varphi} : E' \to E$ satisfying the above is called the **dual isogeny** to φ.

Proof. We first prove uniqueness. If $\widehat{\varphi}'$ were another isogeny with the three given properties, then we would have

$$(\widehat{\varphi} - \widehat{\varphi}') \circ \varphi = \widehat{\varphi} \circ \varphi - \widehat{\varphi}' \circ \varphi = [m]_E - [m]_E = 0.$$

As φ is an isogeny, it is non-constant, hence surjective. It follows then that $\widehat{\varphi} - \widehat{\varphi}' = 0$.

Assuming existence of $\widehat{\varphi}$ satisfying the first condition, we have that $\varphi \circ \widehat{\varphi} \circ \varphi = \varphi \circ [m]_E = [m]_{E'} \circ \varphi$, and so $\varphi \circ \widehat{\varphi} = [m]_{E'}$. (The multiplication-by-m maps commute with φ because φ is a group homomorphism.) This proves the second condition.

Assuming $\widehat{\varphi}$ and $\widehat{\psi}$ exist (here, $\varphi : E \to E'$ and $\psi : E' \to E''$), we may compute

$$\begin{aligned}(\widehat{\varphi} \circ \widehat{\psi}) \circ (\psi \circ \varphi) &= \widehat{\varphi} \circ [\deg \psi]_{E'} \circ \varphi \\ &= (\widehat{\varphi} \circ \varphi) \circ [\deg \psi]_E \\ &= [\deg(\varphi) \deg(\psi)]_E \\ &= [\deg(\varphi \circ \psi)]_E \\ &= \widehat{\psi \circ \varphi} \circ (\psi \circ \varphi),\end{aligned}$$

and the third condition is proven.

Now we prove existence of $\widehat{\varphi}$ satisfying the first condition. Corollary 7.3 tells us we can decompose φ into $\varphi : E \xrightarrow{\varphi_q} E^{(q)} \xrightarrow{\lambda} E'$ where λ is a separable isogeny and $q = \deg_i \varphi$. (If $\operatorname{char} K = 0$, then there is no Frobenius morphism, and the map is separable.) Because we showed this $\widehat{\cdot}$ dual is compatible with composition, it suffices to prove the cases where either φ is (purely) separable or purely inseparable.

Suppose φ is separable. Then, $\#\ker \varphi = \deg_s \varphi = \deg \varphi = m$, so $\ker \varphi \subset \ker([m]_E)$. Looking at the function fields, we have the extension $\overline{K}(E)/\varphi^*\overline{K}(E')$. We have the following useful lemma:

Lemma 7.6. *If $\varphi : E \to E'$ is an isogeny, then we have an isomorphism of groups*

$$\ker \varphi \xrightarrow{\sim} \operatorname{Aut}(\overline{K}(E)/\varphi^*\overline{K}(E')).$$

If φ is separable, then $\overline{K}(E)/\varphi^*\overline{K}(E')$ is Galois.

Proof. If $P \in E(\overline{K})$, denote $t_P : E(\overline{K}) \to E(\overline{K})$ as the translation map $x \mapsto x + P$. This now gives us a map $E(\overline{K}) \to \mathrm{Aut}(E(\overline{K}))$, which upon restricting to $\ker \varphi$ and looking at functions fields gives

$$\begin{aligned} \ker \varphi &\to \mathrm{Aut}(\overline{K}(E)/\varphi^*\overline{K}(E')) \\ P &\mapsto t_P^*. \end{aligned}$$

Note that indeed any t_P^* fixes $\varphi^*\overline{K}(E')$ for $P \in \ker \varphi$ because, for $f \in \overline{K}(E')$, we have

$$t_P^*\varphi^* f = (\varphi \circ t_P)^* f = \varphi^* f,$$

where the second equality follows from $\varphi \circ t_P(x) = \varphi(x+P) = \varphi(x)+\varphi(P) = \varphi(x)+O$. We also check this is a group morphism, as $t_{P+Q} = t_P \circ t_Q = t_Q \circ t_P$.

Now we prove that this is indeed an isomorphism. Note that $|\ker \varphi| = \deg_s \varphi$, but $|\mathrm{Aut}(\overline{K}(E)/\varphi^*\overline{K}(E))| \leq \deg_s \varphi$ by Galois theory. (It is less than the degree of the separable part of $\overline{K}(E)/\varphi^*\overline{K}(E)$, which is exactly $\deg_s \varphi$.) It thus suffices to show that the map is injective. Suppose $t_P^* = \mathrm{id}$ on $\overline{K}(E)$. This means that for all $f \in \overline{K}(E)$, we have $f(x + P) = f(x)$ for all $x \in E(\overline{K})$. But this is only possible if $P = O$, as desired. □

As φ is separable, the field extension is Galois, so the above lemma gives us the isomorphism

$$\ker \varphi \simeq \mathrm{Gal}(\overline{K}(E)/\varphi^*\overline{K}(E')).$$

Likewise, we have $\ker([m]_E) \simeq \mathrm{Gal}(\overline{K}(E)/[m]^*\overline{K}(E'))$, and this gives us an inclusion of Galois extensions

$$\overline{K}(E) \supset \varphi^*\overline{K}(E') \supset [m]_E^*\overline{K}(E).$$

Now, the latter extension $\varphi^*\overline{K}(E') \supset [m]_E^*\overline{K}(E)$ produces a well-defined map $\overline{K}(E) \to \overline{K}(E')$ given by $(\varphi^*)^{-1} \circ [m]_E^*$. We **define** $\widehat{\varphi} : E' \to E$ to be the morphism whose corresponding map on function fields is $(\varphi^*)^{-1} \circ [m]_E^*$. We see then that

$$\varphi^* \circ \widehat{\varphi}^*\overline{K}(E) = \varphi^* \circ ((\varphi^*)^{-1} \circ [m]_E^*)\overline{K}(E) = [m]_E^*\overline{K}(E),$$

and so $\widehat{\varphi} \circ \varphi = [m]_E$. It remains to check that $\widehat{\varphi}$ is indeed an isogeny. We already see it is nonconstant, and we check easily that

$$\widehat{\varphi}(O') = \widehat{\varphi}(\varphi(O)) = [m]_E(O) = O,$$

completing the proof in the separable case.

Now assume φ is purely inseparable. In this case, we must have $\varphi = \varphi_q$ for some prime power $q = p^f$. From construction of the Frobenius map, we have $\varphi_q = (\varphi_p)^{\circ f}$. Again, as we've seen taking the dual is compatible with composition, we are reduced to the case where $\varphi = \varphi_p$. Note $\deg \varphi_p = p$.

The multiplication-by-p map $[p] : E \to E$ is an inseparable isogeny because of Lemma 6.11 and the fact that any $\omega \in \Omega_E$ satisfies $[p]^*\omega = 0$ in characteristic p. We can see this from the fact that Ω_E is generated by dx/y, and we can compute

$$[p]^*\frac{dx}{y} = \frac{d(px)}{\text{stuff}} = p\frac{dx}{\text{stuff}} = 0.$$

This means we can factorize $[p] : E \to E$ as $[p] : E \xrightarrow{\varphi_p^r} E^{(p^r)} \xrightarrow{\lambda} E$ where $r \geq 1$ and λ is separable. We now **define** $\widehat{\varphi_p} \coloneqq \lambda \circ \varphi_p^{r-1}$, and we can see that $[p] = \widehat{\varphi_p} \circ \varphi_p$ as desired. □

Theorem 7.7. Let $\varphi, \psi : E \to E'$ be isogenies. Then, $\widehat{\cdot}$ is an endomorphism on the group of isogenies $\operatorname{Hom}(E, E')$. In particular, we have

$$\widehat{\varphi + \psi} = \widehat{\varphi} + \widehat{\psi}.$$

We will save the proof for later, once we have the Weil pairing at our disposal; see Proof 8.2.

Corollary 7.8. *Let $m \geq 1$ be an integer. Then,*

1. $\deg([m]_E) = m^2$ *and* $\widehat{[m]} = [m]$.
2. *If* $(m, \operatorname{char} K) = 1$, *then*
$$E(\overline{K})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$
3. *If* $\operatorname{char} K = p$, *then* $E(\overline{K})[p^n]$ *is either (a)* $\{0\}$ *for all* n *or (a)* $\mathbb{Z}/p^n\mathbb{Z}$ *for all* n.

Definition 7.9 (Supersingular)**.** Elliptic curves over $\overline{K}$ for which $E(\overline{K})[p^n] = \{0\}$ for all n (case (a) in Statement 3 above) are called **supersingular elliptic curves**. These are *very rare*!

Proof. For (1), note the first statement follows from the second immediately from $\widehat{\varphi} \circ \varphi = [\deg \varphi]$. We prove $\widehat{[m]} = [m]$ by induction. Clearly $\widehat{[m]} = [m]$ is true for $m = 1$. For the inductive step, we have

$$\widehat{[m+1]} = \widehat{[m] + \mathrm{id}} = \widehat{[m]} + \widehat{\mathrm{id}} = [m] + \mathrm{id} = [m+1],$$

where the second equality follows from Theorem 7.7 and the third from the inductive hypothesis.

For (2), we begin by supposing $(m, \operatorname{char} K) = 1$. We can quickly justify $[m]$ is a separable isogeny. (Note this finally completes the proof of Theorem 6.9 – and in one sentence, too!) If $[m]$ were not separable, it would have an inseparable part given by

some Frobenius, but the coprimality condition forces the Frobenius to be trivial. This means that

$$|E(\overline{K})[m]| = |\ker([m])| = \deg_s([m]) = \deg([m]) = m^2,$$

so $E(\overline{K})[m]$ is a finite abelian group of order m^2.

Note if $m = \prod_i p_i^{k_i}$, then we have $E(\overline{K})[m] \simeq \prod_i E(\overline{K})[p_i^{k_i}]$. (This is from the classification of abelian groups.) Thus, it suffices to prove the case when $m = \ell^r$ for some $\ell \neq p = \operatorname{char} K$, and then the general statement will follow.

First consider $r = 1$. Then, we have two possibilities: either $\mathbb{Z}/\ell^2\mathbb{Z}$ or $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. But the former is impossible, as there does not exist an element of order ℓ^2 in $E(\overline{K})[\ell]$. In general, if we have

$$E(\overline{K})[\ell^r] = \langle Q_1 \rangle \times \cdots \times \langle Q_s \rangle$$

where $Q_i \in E(\overline{K})$ has order ℓ^{e_i}, then

$$E(\overline{K})[\ell] = \left\langle \ell^{e_1 - 1} Q_1 \right\rangle \times \cdots \times \left\langle \ell^{e_s - 1} Q_s \right\rangle = (\mathbb{Z}/\ell\mathbb{Z})^2,$$

so we force $s = 2$. But now we have

$$E(\overline{K})[\ell^r] = \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z},$$

and since this has order ℓ^{2r}, we require $a + b = 2r$. But there cannot be an element of order greater than ℓ^r, so we must have $a = b = r$, as desired.

For (3), recall from the end of the proof of Theorem 7.4 that $[p]_E = \widehat{\varphi_p} \circ \varphi_p$. Because $\varphi_p \circ \widehat{\varphi_p}$ as well from the theorem, we get more generally $[p^n]_E = \widehat{\varphi_p}^n \circ \varphi_p^n$. Thus,

$$|E(\overline{K})[p^n]| = \deg_s([p^n]_E) = \deg_s(\widehat{\varphi_p}^n) \cdot \deg_s(\varphi_p^n) = \deg_s(\widehat{\varphi_p}^n)$$

since φ_p is purely inseparable. Noting $\deg \widehat{\varphi_p} = p = \deg_i(\widehat{\varphi_p}) \cdot \deg_s(\widehat{\varphi_p})$, we naturally split into two cases: either $\widehat{\varphi_p}$ is purely inseparable, or it is separable.

If $\widehat{\varphi_p}$ is purely inseparable, then $\widehat{\varphi_p}^n$ is as well, and so $\deg_s \widehat{\varphi_p}^n = 1$. This forces $E(\overline{K})[p^n] = \{O\}$, giving the supersingular case. Otherwise, if $\widehat{\varphi_p}$ is separable, then $\deg \widehat{\varphi_p} = \deg_s \widehat{\varphi_p} = p$, so $|E(\overline{K})[p^n]| = p^n$.

We prove now that it is exactly $\mathbb{Z}/p^n\mathbb{Z}$. This is obvious for $n = 1$. Since $[p] : E \to E$ is non-constant, it is surjective, so for any $P \in E(\overline{K})$ we may find some $Q \in E(\overline{K})$ such that $p \cdot Q = P$. Thus, by induction we can show that $E(\overline{K})[p^n]$ always contains an element of order p^n, in which case $E(\overline{K})[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z}$ as desired. □

We now show that the degree gives a quadratic form. We quickly define a quadratic form:

Definition 7.10. A function $d : A \to \mathbb{R}$ on an abelian group A is a **quadratic form** if (i) $d(x) = d(-x)$ for all $x \in A$ and (ii) the map $(x, y) \mapsto d(x + y) - d(x) - d(y)$ is $\mathbb{Z}$-bilinear.

Corollary 7.11 (Degree as Quadratic Form)**.** *The* ***degree*** *map*

$$\begin{aligned}\mathrm{Hom}(E, E') &\to \mathbb{Z}_{\geq 0}\\ \varphi &\mapsto \deg \varphi\end{aligned}$$

defines a positive definite quadratic form.

Proof. Clearly, $\deg(\varphi) = \deg(-\varphi)$ and $\deg\varphi \geq 0$ with equality iff $\varphi = 0$. It remains to only show the $\mathbb{Z}$-bilinearity of $(\varphi, \psi) \mapsto \deg(\varphi+\psi) - \deg\varphi - \deg\psi$. Seeing $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ via $m \mapsto [m]$, we have

$$\begin{aligned}[\deg(\varphi+\psi)]_E - [\deg\varphi]_E - [\deg\psi]_E &= (\widehat{\psi} + \widehat{\varphi}) \circ (\varphi+\psi) - \widehat{\varphi}\circ\varphi - \widehat{\psi}\circ\psi\\ &= \widehat{\psi}\circ\varphi + \widehat{\varphi}\circ\psi,\end{aligned}$$

which is indeed bilinear by Theorem 7.7. □

On the note of bilinear forms, we will prove this nice result here. This will be the crux of the main result in the next section (Theorem 7.13).

Lemma 7.12. *Let $d : A \to \mathbb{Z}$ be a positive definite quadratic form on an abelian group A. Then,*

$$|d(x-y) - d(x) - d(y)| \leq 2\sqrt{d(x)d(y)}.$$

Proof. Denote B as the $\mathbb{Z}$-bilinear form $B(x,y) = d(x-y) - d(x) - d(y)$ on $A \times A$. By positive-definiteness, we have

$$0 \leq d(mx - ny) = m^2 d(x) + mnB(x,y) + n^2 d(y)$$

for all $m, n \in \mathbb{Z}$. Letting $m = -B(x,y)$ and $n = 2d(x)$, we get

$$0 \leq d(x)\cdot(4d(x)d(y) - B(x,y)),$$

and the result follows. □

7.3 Elliptic Curves over Finite Fields

We now restrict our attention to the case where $K = \mathbb{F}_q$. Let p be prime, $q = p^f$ some prime power, and $K = \mathbb{F}_q$. Let E be an elliptic curve over K. The affine equation for E is, as always, given by

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

where $a_i \in K$.

We are interested in counting K-points on E. Accounting for the point at infinity, we have $|E(K)|$ is one plus the number of solutions $(x,y) \in K^2$ to the above affine equation.

One naïve upper bound we can take is $|E(K)| \leq 1 + 2q$. For any choice of $x \in K$, we would have at most 2 solutions for y.

We can try to approximate better. If we choose some $x \in K$, then we have a quadratic in y. There is heuristically a $1/2$ probability that the quadratic will have a solution $y \in K$. This means that morally, $|E(K)|$ should be on the order of magnitude of $q + 1$. How far off are we? Here is a great result by Hasse:

Theorem 7.13 (Hasse Bound)**.** If $|K| = q$ and E is an elliptic curve over K, then

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

Remark 7.14 (Sato–Tate Conjecture)**.** Let E be an elliptic curve over $\mathbb{Q}$. We can consider the "error" term $a_p(E) \coloneqq p + 1 - \#E(\mathbb{F}_p)$. From the Hasse bound, we have that $|a_p(E)/2\sqrt{p}| \leq 1$ when E has good reduction over p, i.e., when $E(\mathbb{F}_p)$ is still smooth. (See Definition 9.10.) Given this, we can assign an angle $\theta_p \in [0, \pi]$ such that

$$\cos\theta_p = \frac{a_p(E)}{2\sqrt{p}}.$$

Then, the Sato–Tate Conjecture claims that if E does not have complex multiplication, then the angles θ_p are equidistributed in $[0, \pi]$ with probability measure $\frac{2}{\pi}\sin^2\theta\, d\theta$. I find this so wild!! This has been proven in specific cases (e.g., when $j(E) \notin \mathbb{Z}$) by Clozel, Harris, Shepherd-Barron, and Taylor.

Proof. Consider the Frobenius map $\varphi_q : E(\overline{K}) \to E(\overline{K})$ sending $(x, y) \mapsto (x^q, y^q)$. It is well-known that $\mathrm{Gal}(\overline{K}/K) \simeq \widehat{\mathbb{Z}}$ is generated by the Frobenius $x \mapsto x^q$, so $E(K) \subset E(\overline{K})$ are exactly the fixed points of φ_q. This means that if $P \in E(K)$, then $\varphi_q(P) = P = \mathrm{id}(P)$, so $P \in \ker(\mathrm{id} - \varphi_q)$. (We've seen this already in Example 6.6.) Thus, we get the map

$$\begin{aligned} \mathrm{id} - \varphi_q : E(\overline{K}) &\to E(\overline{K}) \\ P &\mapsto P - \varphi_q(P), \end{aligned}$$

which is indeed an isogeny since $(\mathrm{id} - \varphi_q)(O) = O$ and it is non-constant. Furthermore, Theorem 6.9 tells us that φ_q is separable. (It shows it for $q = p$, but the proof is exactly the same for powers of p.) Thus, we have the equalities

$$|E(K)| = |\ker(\mathrm{id} - \varphi_q)| = \deg(\mathrm{id} - \varphi_q).$$

Writing this in terms of degree is great, because we can now use the fact that degree gives a quadratic form. Namely, we want to use Lemma 7.12, which looks very reminiscent to the statement of Hasse's theorem.

Indeed, applying this lemma gets us to the finish line directly. We have $|E(K)| = \deg(\mathrm{id} - \varphi_q)$, as well as the standard $\deg \mathrm{id} = 1$ and $\deg \varphi_q = q$. The lemma gives us

$$\begin{aligned} |\#E(K) - 1 - q| &= |\deg(\mathrm{id} - \varphi_q) - \deg \mathrm{id} - \deg \varphi_q| \\ &\leq 2\sqrt{\deg(\mathrm{id}) \deg(\varphi_q)} \\ &\leq 2\sqrt{q}, \end{aligned}$$

as desired. □

Although this Hasse bound may not seem that significant, it actually has very astounding consequences. In fact, one can say this is the analogue of the Riemann Hypothesis over finite fields! This will be explained more in §8.3.

8 12/9 - Tate Module and Weil Pairing

8.1 Tate Module

Let E be an elliptic curve over a perfect field K, and let $m \geq 2$ be an integer relatively prime to $\mathrm{char}\, K$. Recall that $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. We will investigate the absolute Galois action on the torsion points.

We have a natural action of $\mathrm{Gal}(\overline{K}/K)$ on $E[m]$ as follows: if $P \in E(\overline{K})[m]$, then as $[m](\sigma(P)) = \sigma([m]P) = \sigma(O) = O$, we conclude $\sigma(P) \in E(\overline{K})[m]$ as well. This gives us a Galois representation

$$\begin{aligned} \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]) &\simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\mapsto (P \mapsto \sigma(P)). \end{aligned}$$

However, studying representations over $\mathbb{Z}/m\mathbb{Z}$ is not so interesting, so we will do better by looking at prime powers and their compatible Galois actions. This is the appropriate, two-dimensional analogy of studying the ℓ-adic numbers.

Definition 8.1 (ℓ-adic Tate Module)**.** Let $\ell \neq p$ be a prime (here $p = \mathrm{char}\, K$ if $\mathrm{char}\, K > 0$). The **ℓ-adic Tate module** of E is the inverse limit

$$T_\ell(E) = \varprojlim_n E[\ell^n].$$

The elements in this Tate module are systems $(P_n)_n$ such that $P_n \in E[\ell^n]$ and $[\ell]P_n = P_{n-1}$. One can check that $T_\ell(E)$ is a module over $\mathbb{Z}_\ell$, and in fact is isomorphic to

$$T_\ell(E) = \varprojlim_n E[\ell^n] \simeq \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

This means that, upon choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$, we have $\mathrm{Aut}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$, so we get a *Galois representation*

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell) \subset \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Remark 8.2. If $\ell = p = \mathrm{char}\, K$, then we can define the p-adic Tate module in the same way and get

$$T_p(E) = \begin{cases} \mathbb{Z}_p & E \text{ is ordinary} \\ 0 & E \text{ is supersingular} \end{cases}$$

Remark 8.3. The construction of $T_\ell(E)$ is functorial, meaning if $\varphi : E_1 \to E_2$ is an isogeny, then as $\varphi \circ [\ell^n]_{E_1} = [\ell^n]_{E_2} \circ \varphi$, we have that φ induces a map on the respective ℓ^n-torsion points. Taking the inverse limit gives us $\varphi_\ell : T_\ell(E_1) \to T_\ell(E_2)$ where $(P_n)_n \mapsto (\varphi(P_n))_n$.

For intuition, we can look at the case when $K = \mathbb{C}$. There, we know $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ for some lattice Λ, and then $T_\ell(E) \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. We also have the homology $H_1(E(\mathbb{C}), \mathbb{Z}) \simeq \Lambda$. So it is good to think of the Tate module as $H_1(E)$ over some ℓ-adic field.

Theorem 8.4. The map

$$\begin{aligned} \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell &\to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) \\ \varphi &\mapsto \varphi_\ell \end{aligned}$$

is injective.

Remark 8.5. A weaker version of this statement is that the map $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ is an injection. One can prove this directly: observe that $\varphi_\ell \equiv 0$ means $E_1[\ell^n] \subset \ker \varphi$ for all n, in which case we can argue that φ factors through $[\ell^n]$, which is impossible for large enough n by a degree argument.

Remark 8.6. The map is surjective if K is a finite field or if K is a number field. In general, this is known as the "Tate Conjecture," and it was proven for finite fields by Tate and for number fields by Faltings.

Proof. I unfortunately could not jot this down, but this is Theorem III.7.4 of Silverman. I personally find the proof a bit weird and unenlightening, so I don't feel so bad omitting it from these notes. □

8.2 Weil Pairing

As above, let E be an elliptic curve over K and $m \in \mathbb{N}$ coprime to $\mathrm{char}\, K$ if $\mathrm{char}\, K = p > 0$. We would like a way to study the Tate module, or more down-to-earth, the torsion points $E[m]$. This will come in the form of a bilinear pairing $E[m] \times E[m] \to \mu_m(\overline{K})$.

To start, recall that $D = \sum n_P[P] \in \mathrm{Div}(E)$ is principal iff the following two conditions are satisfied: (1) $\sum n_P \in \mathbb{Z}$ and (2) $\sum [n_P](P) = O_E$.

Now let $T \in E[m]$. By the above, there exists some $f \in \overline{K}(E)^\times$ such that $\operatorname{div} f_T = m[T] - m[O]$. Let $T' \in E(\overline{K})$ such that $[m]T' = T$. Then, we have

$$\begin{aligned}[m]^*([T'] - [O]) &= \sum_{R \in E[m]} ([T' + R] - [R]) \\ &\sim \sum_{R \in E[m]} ([T'] - [O]) \\ &\sim m^2([T'] - [O]) \sim O_E,\end{aligned}$$

where the first line is because $[m]$ is unramified, the third line because $|E[m]| = m^2$, and the last equivalence because $[m^2]T' = O$. From this, there exists some $g_T \in \overline{K}(E)^\times$ with $\operatorname{div} g_T = [m]^*([T] - [O])$. We can compare g_T^m and $f_T \circ [m]$ as follows:

$$\begin{aligned}\operatorname{div} g_T^m &= m \operatorname{div} g_T = m([m]^*([T] - [O])) \\ &= [m]^*(m([T] - [O])) = [m]^* \operatorname{div} f_T \\ &= \operatorname{div}(f_T \circ [m]).\end{aligned}$$

After scaling appropriately, we can therefore assume $g_T^m = f_T \circ [m]$.

We now get to defining the Weil pairing. Let $S \in E[m]$. Then for all $X \in E(\overline{K})$, we have

$$g_T(X + S)^m = f_T([m]X + [m]S) = f_T([m]X) = g_T(X)^m,$$

so g_T^m is *invariant under translation by* S. This leads to the following definition:

Definition 8.7 (Weil Pairing)**.** Let $S, T \in E[m]$. Using the notation above, we define a function

$$\begin{aligned}e_m : E[m] \times E[m] &\to \mu_m(\overline{K}) \\ (S, T) &\mapsto \frac{g_T(X + S)}{g_T(X)}.\end{aligned}$$

We will prove that it is bilinear, as well as several other nice properties, below. First, though, we must make clear that the pairing does not depend on our choice of X. The reason is very simple: the morphism

$$\begin{aligned}E &\to \mathbb{P}^1 \\ X &\mapsto \frac{g(X + S)}{g(X)}\end{aligned}$$

is not surjective, as it must be in μ_m, so it must be constant.

Proposition 8.8. The Weil pairing

$$\begin{aligned} e_m : E[m] \times E[m] &\to \mu_m \\ (S,T) &\mapsto e_m(S,T) \end{aligned}$$

satisfies the following properties:

1. *Bilinearity*: we have $e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T)$ and $e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2)$.
2. *Alternating*: we have $e_m(T,T) = 1$, and thus $e_m(S,T) = e_m(T,S)^{-1}$. (Consider $e_m(S+T,S+T)$.)
3. *Non-degenerate*: If $e_m(S,T) = 1$ for all $S \in E[m]$, then $T = O$.
4. *Compatible with Galois action*: If $\sigma \in \mathrm{Gal}(\overline{K}/K)$, then $e_m(\sigma(S),\sigma(T)) = \sigma(e_m(S,T))$.
5. *Compatible with multiplication in m*: If $S \in E[mm']$ and $T \in E[m] \subset E[mm']$, then $e_{mm'}(S,T) = e_m([m']S,T)$.
6. *Dual Isogeny is Adjoint*: Let $\varphi : E_1 \to E_2$ be an isogeny and $\widehat{\varphi} : E_2 \to E_1$ be its dual. Then, for all $S \in E_1[m]$, $T \in E_2[m]$, we have $e_m(S,\widehat{\varphi}(T)) = e_m(\varphi(S),T)$. In other words, φ and $\widehat{\varphi}$ are adjoint with respect to the Weil pairing e_m.

If you don't care about these details and want to skip to something very cool, skip to §8.3. Because of time, we only prove (1) and (6) here.

Proof. We start with **(6)**, namely φ and $\widehat{\varphi}$ are adjoint with respect to e_m. By definition, recall

$$e_m(\varphi(S),T) = \frac{g_T(X+\varphi(S))}{g_T(X)},$$

where $\mathrm{div}(f_T) = m[T] - m[O]$ and g_T is defined to satisfy $g_T^m = f_T \circ [m]$. Recall also that if $\varphi^*([T]-[O]) = \sum_P n_P[P] \in \mathrm{Div}(E_1)$, then $\widehat{\varphi}(T) = \sum_P [n_P](P)$. From this fact, we see that the divisors $\varphi^*([T]-[O])$ and $[\widehat{\varphi}(T)]-[O]$ have the same degree, so there must exists some $h \in \overline{K}(E)^\times$ such that

$$\varphi^*([T]-[O]) = [\widehat{\varphi}(T)] - [O] + \mathrm{div}(h).$$

We thus have

$$\begin{aligned} \mathrm{div}\left(\frac{f_T \circ \varphi}{h^m}\right) &= \mathrm{div}(f_T \circ \varphi) - m\,\mathrm{div}(h) \\ &= \varphi^* \mathrm{div}(f_T) - m\,\mathrm{div}(h) \\ &= \varphi^*(m[T]-m[O]) - \varphi^*(m[T]-m[O]) - m[O] + m[\widehat{\varphi}(T)], \end{aligned}$$

and after canceling like terms on the right, we get

$$\operatorname{div}\left(\frac{f_T \circ \varphi}{h^m}\right) = m[\widehat{\varphi}(T)] - m[O].$$

We also have from $g_T^m = f_T \circ [m]$ the equality

$$\left(\frac{g_T \circ \varphi}{h \circ [m]}\right)^m = \frac{f_T \circ [m] \circ \varphi}{(h \circ [m])^m} = \left(\frac{f_T \circ \varphi}{h^m}\right) \circ [m],$$

and thus

$$\begin{aligned} e_m(S, \widehat{\varphi}(T)) &= \frac{\left(\frac{g_T \circ \varphi}{h \circ [m]}\right)(X+S)}{\left(\frac{g_T \circ \varphi}{h \circ [m]}\right)(X)} \\ &= \frac{g_T(\varphi(X)+\varphi(S))}{g_T(\varphi(X))} \cdot \frac{h([m]X)}{h([m]X + \cancel{[m]S})} \\ &= \frac{g_T(\varphi(X)+\varphi(S))}{g_T(\varphi(X))} = e_m(\varphi(S), T), \end{aligned}$$

as sought.

Now we prove bilinearity **(1)**. Linearity in the first component is not so bad, as we can write

$$\begin{aligned} e_m(S_1+S_2, T) &= \frac{g_T(X+(S_1+S_2))}{g_T(X)} \frac{g_T(X+S_1)}{g_T(X+S_1)} \\ &= \frac{g_T(X+(S_1+S_2))}{g_T(X+S_1)} \frac{g_T(X+S_1)}{g_T(X)} \\ &= e_m(S_2, T) e_m(S_1, T). \end{aligned}$$

For the second component, we first note that

$$\begin{aligned} \operatorname{div}\left(\frac{g_{T_1+T_2}}{g_{T_1} g_{T_2}}\right) &= [m]^*([T_1+T_2] - [O] - [T_1] - [T_2] + 2[O]) \\ &= [m]^*([T_1+T_2] - [T_1] - [T_2] + [O]) \\ &= [m]^* \operatorname{div}(h) = \operatorname{div}(h \circ [m]) \end{aligned}$$

for some $h \in \overline{K}(E)^\times$. Thus, we can write $g_{T_1+T_2} = c \cdot g_{T_1} g_{T_2} \cdot (h \circ [m])$ for some $c \in \overline{K}^\times$. This now allows us to compute

$$\begin{aligned} e_m(S, T_1+T_2) &= \frac{g_{T_1+T_2}(X+S)}{g_{T_1+T_2}(X)} \\ &= \frac{g_{T_1}(X+S) g_{T_2}(X+S) h([m]X + [m]S)}{g_{T_1}(X) g_{T_2}(X) h([m]X)} \\ &= e_m(S, T_1) e_m(S, T_2), \end{aligned}$$

as we have $[m]S = O$ since $S \in E[m]$ by definition. □

As a consequence, we can obtain a pairing on the Tate module by taking the inverse limit over powers of ℓ:

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu).$$

Indeed, the bilinearity tells us that $e_{\ell^n}([\ell]S, [\ell]T) = e_{\ell^{n+1}}(S,T)^\ell$, so the Weil pairings e_{ℓ^n} respect the transition maps $[\ell] : E[\ell^{n+1}] \to E[\ell^n]$ and $(\cdot)^\ell : \mu_{\ell^{n+1}} \to \mu_{\ell^n}$ for $T_\ell(E)$ and $T_\ell(\mu)$, respectively.

Proof of Theorem 7.7. Suppose $\varphi, \psi : E_1 \to E_2$. We wish to show $\widehat{\varphi+\psi} = \widehat{\varphi} + \widehat{\psi}$. If $\mathrm{char}(K) \neq 2$, we know that $[2^n]$ has degree $(2^n)^2$. We now consider the Weil pairing e_{2^n}. For all $S \in E_1[2^n]$ and $T \in E_2[2^n]$, we have

$$\begin{aligned}
e_{2^n}(S, \widehat{(\varphi+\psi)}(T) - \widehat{\varphi}(T) - \widehat{\psi}(T)) &= e_{2^n}(S, \widehat{(\varphi+\psi)}(T)) e_{2^n}(S, \widehat{\varphi}(T))^{-1} e_{2^n}(S, \widehat{\psi}(T))^{-1} \\
&\qquad \text{(bilinearity)} \\
&= e_{2^n}((\varphi+\psi)(S), T) e_{2^n}(\varphi(S), T)^{-1} e_{2^n}(\psi(S), T)^{-1} \\
&\qquad \text{(adjoint)} \\
&= e_{2^n}((\varphi+\psi)(S) - \varphi(S) - \psi(S), T) \\
&= e_{2^n}(O, T) = 1.
\end{aligned}$$

But as this is true for all $S \in E_1[2^n]$, we have by non-degeneracy that $\widehat{(\varphi+\psi)}(T) = \widehat{\varphi}(T) + \widehat{\psi}(T)$ for all $T \in E_2[2^n]$. But $\bigcup_{n\geq 1} E_2[2^n]$ is an infinite set, so it is Zariski dense in E_2. Thus, by continuity it must be true that $\widehat{(\varphi+\psi)}(T) = \widehat{\varphi}(T) + \widehat{\psi}(T)$ for all $T \in E_2(\overline{K})$. □

8.3 Weil Conjectures

With the Weil pairing in hand, we can now discuss the Weil conjectures for elliptic curves!

Let K be a finite field wtih q elements, and denote K_n/K as the unique degree n extension in $\overline{K}$. Let E be an elliptic curve defined over K. Consider the generating series

$$Z(E/K, T) = \exp\left(\sum_{n=1}^{\infty} |E(K_n)| \frac{T^n}{n}\right) \in \mathbb{Q}[[T]].$$

We call this the **zeta function of E**.

Theorem 8.9 (Weil "Conjecture")**.** There exists $a \in \mathbb{Z}$ such that the zeta function of E is rational of the form

$$Z(E/K, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}.$$

Furthermore,

1. We can factor
$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$$
with $|\alpha| = |\beta| = \sqrt{q}$ and $\alpha\beta = q$.
2. It satisfies the *functional equation*
$$Z\left(E/K, \frac{1}{qT}\right) = Z(E/K, T).$$

Exercise 8.10. This is really a statement about smooth projective varieties over finite fields in general. Construct the zeta function for $X = \mathbb{P}^N$, express it as a rational function, and show it satisfies a functional equation.

Remark 8.11. This is really a statement about cohomology. To give some taste, the $(1 - T)$ term in the denominator corresponds to $\dim H^0(E) = 1$, the $(1 - qT)$ term corresponds to $\dim H^2(E) = 1$, and the numerator corresponds to $\dim H^1(E) = 2$. Here, the cohomology is étale cohomology, although since we only need to access up to H^2, we don't need all the formalism and can just look at the Tate module and, in effect, Tate cohomology.

Remark 8.12. Via the change of variable $T = q^{-s}$, we get
$$\zeta(E/K, s) = \frac{1 - aq^{-s} + q^{1-2s}}{(1 - q^{-s})(1 - q^{1-s})}.$$
The functional equation now becomes
$$\zeta(E/K, 1 - s) = \zeta(E/K, s),$$
and the property $|\alpha| = |\beta| = \sqrt{q}$ says that the zeros of $\zeta(E/K, s)$ satisfy $|q^s| = \sqrt{q}$, and hence $\mathrm{Re}(s) = 1/2$. This is exactly the Riemann Hypothesis for elliptic curves over finite fields!

So how does one prove such a thing? We will show its beginning. Let $\ell \neq \mathrm{char}(K)$ be a prime. We've observed from earlier (Remark 8.5) that we have an injection
$$\begin{aligned} \mathrm{End}(E) &\hookrightarrow \mathrm{End}(T_\ell(E)) \\ \varphi &\mapsto \varphi_\ell. \end{aligned}$$

If we choose a basis of $T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, we can express φ_ℓ as a matrix, and in particular we can define the **trace** and **determinant** $\mathrm{Tr}(\varphi_\ell), \det(\varphi_\ell) \in \mathbb{Z}_\ell$.

Proposition 8.13. We have
$$\begin{aligned} \det(\varphi_\ell) &= \deg(\varphi) \\ \mathrm{Tr}(\varphi_\ell) &= 1 + \deg(\varphi) - \deg(\mathrm{id} - \varphi). \end{aligned}$$

In particular, $\det(\varphi_\ell), \mathrm{Tr}(\varphi_\ell) \in \mathbb{Z}$ are *independent of* ℓ.

Proof. Let $\{v_1, v_2\}$ be a $\mathbb{Z}_\ell$-basis of $T_\ell(E)$, and express $\varphi_\ell = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with respect to this basis. Taking the Weil pairing e on $T_\ell(E)$, we have

$$\begin{aligned} e(v_1, v_2)^{\deg \varphi} &= e(\deg(\varphi) v_1, v_2) \\ &= e(\widehat{\varphi}_\ell \varphi_\ell v_1, v_2) \\ &= e(\varphi_\ell v_1, \varphi_\ell v_2) && \text{(adjoint)} \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{\det(\varphi_\ell)}. \end{aligned}$$

Thus, by non-degeneracy of e, we have $\deg(\varphi) = \det(\varphi_\ell)$. Now for the trace, we use $\deg \varphi = \det \varphi_\ell$ and $\varphi_\ell = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to compute

$$\begin{aligned} 1 + \det \varphi_\ell - \det(\mathrm{id} - \varphi_\ell) &= 1 + (ad - bc) - (1 - a)(1 - d) + bc \\ &= a + d = \mathrm{Tr}(\varphi_\ell), \end{aligned}$$

as desired. □

Now returning to the specific case of E being defined over a finite field, let $\varphi = \varphi_q : E \to E$ be the q^{th}-power Frobenius morphism. We know $\mathrm{id} - \varphi^n$ is separable, hence $\#\ker(\mathrm{id} - \varphi^n) = \deg(\mathrm{id} - \varphi^n)$. But the kernel is just $E(K_n)$, and thus

$$|E(K_n)| = \deg(\mathrm{id} - \varphi^n).$$

Now from the above proposition, we have that $\det(T - \varphi_\ell) = T^2 - \mathrm{Tr}(\varphi_\ell)T + \det(\varphi_\ell) \in \mathbb{Z}[T]$. Thus, we can find complex roots

$$\mathbb{Z}[T] \ni \det(T - \varphi_\ell) = (T - \alpha)(T - \beta), \quad \alpha, \beta \in \mathbb{C}.$$

But at the same time, we compute directly

$$\det\left(\frac{m}{n} - \varphi_\ell\right) = \frac{\det(m \,\mathrm{id} - n\varphi_\ell)}{n^2} = \frac{\deg(m \,\mathrm{id} - n\varphi)}{n^2} \geq 0$$

for all $m/n \in \mathbb{Q}$. This restricts our possibility for α, β. In particular,

1. If $\alpha, \beta \in \mathbb{R}$, then we must have $\alpha = \beta$ (else we can find some $m/n \in \mathbb{Q}$ with $\det(m/n - \varphi_\ell) < 0$).
2. If $\alpha, \beta \notin \mathbb{R}$, then they must be complex conjugates since $(T - \alpha)(T - \beta) \in \mathbb{Z}$. In particular, we have $\alpha\beta = \det(\varphi_\ell) = \deg(\varphi) = q$, and so $|\alpha| = |\beta| = \sqrt{q}$.

Since we can consider φ_ℓ as the diagonal matrix with entries α and β, we deduce the characteristic polynomial for φ_ℓ^n is

$$\det(T - \varphi_\ell^n) = (T - \alpha^n)(T - \beta^n),$$

and thus

$$\begin{aligned} |E(K_n)| &= \deg(\mathrm{id} - \varphi_\ell^n) = \det(\mathrm{id} - \varphi_\ell^n) \\ &= (1 - \alpha^n)(1 - \beta^n) = 1 - \alpha^n - \beta^n + q^n. \end{aligned}$$

We now prove the Weil Conjecture for elliptic curves in earnest.

Proof of Weil Conjecture (Theorem 8.9). Consider the log

$$\log Z(E/K, T) = \sum_{n=1}^{\infty} |E(K_n)| \frac{T^n}{n}.$$

Using $|E(K_n)| = 1 - \alpha^n - \beta^n + q^n$ obtained above, as well as noting the standard $\sum_{n\geq 1} \frac{T^n}{n} = -\log(1 - T)$, we have

$$\log Z(E/K, T) = -\log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T) - \log(1 - qT),$$

and so

$$Z(E/K, T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}.$$

We check that Z satisfies the claimed functional equation. We expand

$$\begin{aligned} Z\left(E/K, \frac{1}{qT}\right) &= \frac{\left(1 - \frac{\alpha}{qT}\right)\left(1 - \frac{\beta}{qT}\right)}{\left(1 - \frac{1}{qT}\right)\left(1 - \frac{q}{qT}\right)} \\ &= \frac{(qT - \alpha)(qT - \beta)}{(qT - 1)(qT - q)} \\ &= \frac{q(1 - (\alpha + \beta)T + qT^2}{q(1 - T)(1 - qT)} \\ &= \frac{1 - aT + qT^2}{(1 - T)(1 - qT)} = Z(E/K, T), \end{aligned}$$

where the last line follows from $\alpha + \beta = a$ by definition of α, β. □

9 12/16 - Mordell–Weil Theorem

Last class! As the section title suggests, we will discuss the Mordell–Weil Theorem.

Let K be a number field and E an elliptic curve over K. Then, the Mordell–Weil Theorem states:

Theorem 9.1 (Mordell–Weil Theorem)**.** The group $E(K)$ is a **finitely generated** abelian group, so it can be decomposed as

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\text{tors}},$$

where $r \in \mathbb{Z}_{\geq 0}$ is the **rank** of $E(K)$ and $E(K)_{\text{tors}}$ is a finite group.

There are many natural questions one can ask here, including:

1. What are the possibilities for the torsion group?
2. What are the possible ranks of an elliptic curve over K?
3. What is the distribution of the ranks?
4. What arithmetic information does the rank contain?

Each of these questions begets very involved and rich discussions. Professor Fresàn alluded to the history of some of them, but frankly I did not understand his spoken French. We will elaborate more on these throughout the lecture though, I presume.

9.1 Weak Mordell–Weil

How does one go about proving such a statement? It involves two very different steps. The first gives us, as a consequence, the finiteness of the rank.

Theorem 9.2 (Weak Mordell–Weil)**.** Let E be an elliptic curve over a number field K. Let $m \geq 2$ be an integer. Then, $E(K)/mE(K)$ is a finite group.

Remark 9.3. Oftentimes, it is convenient to study the case $m = 2$, as we understand the 2-torsion of $E(K)$ relatively well.

We first start by reducing to the scenario $E[m] \subset E(K)$, which will come in handy in the proceeding steps. We do this via the following lemma.

Lemma 9.4. *Let L/K be a finite Galois extension. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is finite as well.*

Proof. Consider the exact sequence

$$0 \to (E(K) \cap mE(L))/mE(K) \to E(K)/mE(K) \to E(L)/mE(L).$$

Denote Φ as the second term in the sequence. It suffices to show Φ is finite.

For $P \in \Phi$, let $Q_P \in E(L)$ be a point such that $[m]Q_P = P$. We define a map (just as sets – this is not a group morphism!)

$$\begin{aligned} \lambda_p : \mathrm{Gal}(L/K) &\to E[m] \\ \sigma &\to \sigma(Q_P) - Q_P. \end{aligned}$$

This is well-defined because $[m](\sigma(Q_P) - Q_P) = \sigma([m]Q_P) - [m]Q_P = \sigma(P) - P = O$. Note that this in turn gives us a map $\lambda : \Phi \to \mathrm{Mor}(\mathrm{Gal}(L/K), E[m])$ where $P \mapsto \lambda_P$. Note again that the set on the right consists of morphisms of *sets*, not as groups.

We show that λ is injective. Observe that if $\lambda_P = \lambda_{P'}$, then $\sigma(Q_P) - Q_P = \sigma(Q_{P'}) - Q_{P'}$, i.e., $\sigma(Q_P - Q_{P'}) = Q_P - Q_{P'}$. But this is true for all $\sigma \in \mathrm{Gal}(L/K)$, hence $Q_P - Q_{P'} \in E(K)$. Thus,

$$P - P' = [m](Q_P - Q_{P'}) \in mE(K),$$

so $P = P'$ in Φ as desired.

Now we can quickly show Φ is finite. We know now that λ provides an injection $\Phi \hookrightarrow \mathrm{Mor}(\mathrm{Gal}(L/K), E[m])$, and the latter set of morphisms is finite because both $\mathrm{Gal}(L/K)$ and $E[m]$ are finite. As stated before, this then implies $E(K)/mE(K)$ is finite since $\Phi = \ker(E(K)/mE(K) \to E(L)/mE(L))$. □

Remark 9.5. One can see this λ map is the analogue of Kummer theory for elliptic curves! I don't know the details, but here are some remarks that gesture towards Kummer theory:

1. In Kummer theory, we consider something like $\sigma(\sqrt[m]{x})/\sqrt[m]{x}$. Above, division is subtraction in $E[m]$, and the m^{th} root is what we're doing when we consider $[m]Q_P = P$.

2. Although λ_P is not a group homomorphism, it is a *cocycle*. (This is easy to check, just write it out!) So we are really looking at the *first group cohomology* of $\mathrm{Gal}(L/K)$ with values in $E[m]$, and Φ is in some sense measuring a certain kind of obstruction.

Since $E[m]$ is finite, we can guarantee $E[m] \subset E(L)$ for some finite extension L/K. Lemma 9.4 now tells us that proving $E(L)/mE(L)$ is finite implies $E(K)/mE(K)$ is finite. Thus, we may assume from now on that $E[m] \subset E(K)$.

We now introduce something called the Kummer pairing. (The choice of name fortifies Remark 9.5.)

Definition 9.6 (Kummer Pairing)**.** The **Kummer pairing**

$$\kappa : E(K) \times \mathrm{Gal}(\overline{K}/K) \to E[m]$$

is defined as follows. Let $P \in E(K)$, and let $Q \in E(\overline{K})$ such that $[m]Q = P$. We let

$$\kappa(P, \sigma) = \sigma(Q) - Q.$$

Proposition 9.7. The Kummer pairing satisfies the following (expected) properties:

1. It is well-defined;
2. It is bilinear;
3. Its left kernel (in $E(K)$) is $mE(K)$.
4. Its right kernel (in $\mathrm{Gal}(\overline{K}/K)$) is $\mathrm{Gal}(\overline{K}/L)$, where $L = K([m]^{-1}E(K))$, i.e., L is the compositum of all residue fields $K' = K(Q)$ for $Q \in E(\overline{K})$ satisfying $[m]Q \in E(K)$.

Remark 9.8. Note that in (4), L/K is Galois since $\mathrm{Gal}(\overline{K}/K)$ sends $[m]^{-1}E(K)$ to itself.

Corollary 9.9. *Taking the appropriate kernel on both sides, this means that the induced pairing*

$$\kappa : E(K)/mE(K) \times \mathrm{Gal}(L/K) \to E[m]$$

is perfect. In particular, this means

$$E(K)/mE(K) \simeq \mathrm{Mor}(\mathrm{Gal}(L/K), E[m]).$$

Proof of Proposition. Well-definedness (1) requires two checks. First, we have

$$[m]\kappa(P,\sigma) = [m](\sigma(Q) - Q) = \sigma([m]Q) - [m]Q = O.$$

We also show that κ is independent of our choice of Q. Observe that if $[m]Q' = P$ as well, then it is of the form $Q + T$ for some $T \in E[m]$, in which case

$$\sigma(Q+T) - (Q+T) = \sigma(Q) - Q + \sigma(T) - T = \sigma(Q) - Q$$

since we assumed $E[m] \subset E(K)$.

We show bilinearity (2) routinely: we have linearity in the first component by definition, and linearity in the second follows from the computation

$$\begin{aligned}\kappa(P, \sigma\tau) &= (\sigma \circ \tau)(Q) - Q \\ &= (\sigma \circ \tau)(Q) - \sigma(Q) + \sigma(Q) - Q \\ &= \sigma(\kappa(P,\tau)) + \kappa(P,\sigma) \\ &= \kappa(P,\tau) + \kappa(P,\sigma),\end{aligned}$$

where the last equality follows again from $\kappa(P,\tau) \in E[m]$ and $E[m] \subset E(K)$ by assumption.

We now prove (3). If $P \in mE(K)$, then for any $Q \in E(K)$ such that $[m]Q = P$, we clearly have $\sigma(Q) - Q = O$. Thus, the kernel contains $mE(K)$. We want to show

the reverse inclusion. Suppose $\kappa(P,\sigma) = 0$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. But $\sigma(Q) = Q$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ implies $Q \in E(K)$, and hence $P \in mE(K)$.

Finally, we prove (4). The kernel clearly contains $\sigma \in \mathrm{Gal}(\overline{K}/L)$ since by construction, each Q with $[m]Q = P$ lives in $E(L)$, and hence $\sigma(Q) = Q$. Conversely, suppose $\kappa(P,\sigma) = 0$ for all $P \in E(K)$. This means $\sigma(Q) = Q$ for all $Q \in E(\overline{K})$ with $[m]Q = P$. But these are exactly the points of $E(L)$, so $\sigma(Q) = Q$ for all $Q \in E(L)$ implies $\sigma \in \mathrm{Gal}(\overline{K}/L)$ as desired. □

Let's recall what we want to show. We want to show the Weak Mordell–Weil Theorem (9.2), which states that $E(K)/mE(K)$ is finite for $m \geq 2$. We showed that if L/K is finite Galois, then $E(L)/mE(L)$ is finite implies $E(K)/mE(K)$ is finite. Thus, we can safely assume $E[m] \subset E(K)$. We also showed from the Kummer pairing that $E(K)/mE(K) \simeq \mathrm{Mor}(\mathrm{Gal}(L/K), E[m])$ where $L = K([m]^{-1}E(K))$. If we want to show $E(K)/mE(K)$ is finite, it suffices to show that $\mathrm{Gal}(L/K)$ is finite. This is our present objective.

9.2 Elliptic Curves over Local Fields

What we're going to do now is transition from elliptic curves over global fields to those over local fields by taking completions. The upshot of this is that studying local fields often amounts to studying the corresponding (finite) residue fields, which we understand well. This will inform us about our Galois extension of global fields, which is our present scenario.

Denote M_K as the set of absolute values over K, up to equivalence. We can write $M_K = M_K^0 \cup M_K^\infty$, where M_K^0 are the finite places of K and M_K^∞ are the infinite (archimedean) ones. For each $\nu \in M_K^0$, consider the completion K_ν of K with respect to ν. Define $\mathcal{O}_\nu$ and $\mathfrak{m}_\nu$ as standard, and denote $\kappa_\nu = \mathcal{O}_\nu/\mathfrak{m}_\nu$ as the residual field at ν.

If E is an elliptic curve over K, then it admits a Weierstrass equation

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

where the $a_i \in K$. But $K \subset K_\nu$, and after an appropriate change of variables, we can force $a_i \in \mathcal{O}_\nu$. We call such a Weierstrass equation a **minimal Weierstrass equation** if $\nu(\Delta)$ is minimal over all Weierstrass equations for E with coefficients in $\mathcal{O}_\nu$.

Definition 9.10 (Good and Bad Reduction)**.** We say E is **good reduction** at ν if the curve

$$\widetilde{E}_\nu : y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6},$$

where the $\overline{a_i}$'s are all reductions mod $\mathfrak{m}_\nu$, is smooth, i.e., $\widetilde{E}_\nu$ is an elliptic curve over κ_ν. Otherwise, we say E has **bad reduction** at ν.

Remark 9.11. An elliptic curve E over K can only have finitely many places with bad reduction.

Theorem 9.12. Let $\nu \in M_K^0$ and let $m \in \mathbb{N}$ be relatively prime to $\operatorname{char} \kappa_\nu$. Suppose E is an elliptic curve over K with good reduction at ν. Then, the reduction map

$$E(K) \to \widetilde{E}_\nu(\kappa_\nu)$$

induces an isomorphism $E[m] \xrightarrow{\simeq} \widetilde{E}_\nu(\kappa_\nu)[m]$.

Remark 9.13. Why can we have such a map? Let $[x : y : z] \in E(K) \subset \mathbb{P}^2_K \subset \mathbb{P}^2_{K_\nu}$. Why can we assume it is contained in $\mathbb{P}^2(\mathcal{O}_\nu)$? This follows from the valuation criterion for properness for schemes.

Proof. See Professor Dat's notes for the proof. □

We now return to the setting where $L = K([m]^{-1}E(K))$. We will prove some properties about the extension L/K.

Proposition 9.14. Let K be a number field, E an elliptic curve over K, and $m \geq 2$ an integer. Denote $L = K([m]^{-1}E(K))$. Then,

1. $\operatorname{Gal}(L/K)$ is abelian, and the order of every element divides m.
2. Let S be the (finite) set of places given by

   $$S = \{\nu \in M_K^0 \mid E \text{ has bad reduction at } \nu\} \cup \{\nu \in M_K^0 \mid |m|_\nu \neq 1\} \cup M_K^\infty.$$

   Then, L/K is unramified outside of S.

Proof. For (1), first recall Corollary 9.9, which gives us an isomorphism

$$\operatorname{Gal}(L/K) \simeq \operatorname{Mor}(E(K)/mE(K), E[m]).$$

The statement now follows because the group on the right is abelian and the order of any point in $E[m]$ divides m.

For (2), let $\nu \in M_K - S$. Let $Q \in E(\overline{K})$ such that $[m]Q \in E(K)$. It suffices to show that $K' = K(Q)$ is unramified at ν. Consider any place $\nu' \in M_{K'}$ lying over ν, and consider the completion $K'_{\nu'}$. We then have an extension of residue fields $\kappa'_{\nu'}/\kappa_\nu$.

Definition 9.15 (Inertia Group)**.** The **inertia group** with respect to ν'/ν is the kernel of the reduction map

$$I_{\nu'/\nu} = \ker\left(\operatorname{Gal}(K'_{\nu'}/K_\nu) \to \operatorname{Gal}(\kappa'_{\nu'}/\kappa_\nu)\right).$$

We say the extension K'/K is **unramified** at ν if $I_{\nu'/\nu} = \{1\}$.

So we wish to show that $I_{\nu'/\nu} = \{1\}$, in which case we show K'/K is unramified, and hence L/K is unramified.

Consider the reduction map $\widetilde{\cdot} : E(K') \to \widetilde{E}_{\nu'}(\kappa'_{\nu'})$. Let $\sigma \in I_{\nu'/\nu} \subset \mathrm{Gal}(K'/K)$, where the inclusion is possible after a choice of embedding $K' \hookrightarrow K'_{\nu'}$. By definition of the inertia group, we have

$$\widetilde{\sigma(Q) - Q} = \sigma(\widetilde{Q}) - \widetilde{Q} = \widetilde{Q} - \widetilde{Q} = \widetilde{O}.$$

As $\widetilde{\cdot}$ is injective on $E[m]$ (see Theorem 9.12), it suffices to show that $\sigma(Q) - Q \in E[m]$, in which case we would force $\sigma(Q) = Q$ and hence the inertia is trivial. But this follows from the computation

$$[m](\sigma(Q) - Q) = \sigma([m]Q) - [m]Q = \sigma(P) - P = 0,$$

so indeed $\sigma(Q) - Q \in E[m]$. □

The upshot of this proposition is that we can invoke the following theorem from algebraic number theory to obtain that L/K is finite.

Theorem 9.16. Let K be a number field and $S \subset M_K$ a finite set of absolute values containing M_K^∞. Let $m \in \mathbb{N}$. Suppose L/K is an extension satisfying:

1. $\mathrm{Gal}(L/K)$ is abelian,
2. The order of every element divides m,
3. L/K is unramified outside of S.

Then, L/K is finite.

To recap on how this finishes the proof: we want to show that $E(K)/mE(K) \simeq \mathrm{Mor}(\mathrm{Gal}(L/K), E[m])$ is finite. But $E[m]$ is clearly finite and the above theorem dictates that $\mathrm{Gal}(L/K)$ is finite, so $E(K)/mE(K)$ is finite as desired. This completes the proof of Weak Mordell–Weil!

9.3 Heights

Now how do we go from Weak Mordell–Weil to Mordell–Weil? Note that we need some notion of $E(K)$ being "discrete." To illustrate, we have $\mathbb{R}/m\mathbb{R}$ is trivial, but clearly $\mathbb{R}$ is not finite. So we want to rule out such scenarios.

To do this, we will introduce this notion of a **height function** which, as we will see shortly, gets us directly to the finite generatedness of the Mordell–Weil group. We will first speak in generalities, so we start with some abelian group A, but we really care about $A = E(K)$.

Theorem 9.17 (Height Function implies Finitely Generated)**.** Let A be an abelian group and let $m \geq 2$ be an integer such that A/mA is finite. Suppose there exists a function

$$h : A \to \mathbb{R}$$

with the following properties:

1. Let $Q \in A$. There exists $c_1 = c_1(A, Q)$ such that, for all $P \in A$,
$$h(P + Q) \leq 2h(P) + c_1.$$
2. There exists $c_2 = c_2(A)$ such that, for all $P \in A$,
$$h(mP) \geq m^2 h(P) - c_2.$$
3. For all c_3, the set
$$\{P \in A \mid h(P) \leq c_3\}$$
is finite.

Then, A is of finite type, i.e., it is finitely generated.

Proof. Let $Q_1, \ldots, Q_r$ be representatives of A/mA. Let $P \in A$. For each $1 \leq j \leq r$, choose $i_j \in \{1, 2\}$, and define P_i inductively like

$$\begin{aligned} P &= mP_1 + Q_{i_1} \\ P_1 &= mP_2 + Q_{i_2} \\ &\vdots \\ P_{n-1} &= mP_n + Q_{i_n}. \end{aligned}$$

By conditions 2 (first line) and 1 (third line), we have

$$\begin{aligned} h(P_j) &\leq \frac{1}{m^2}\left(h(mP_j) + c_2\right) \\ &\leq \frac{1}{m^2}\left(h(P_{j-1} - Q_{i_j}) + c_2\right) \\ &\leq \frac{1}{m^2}\left(2h(P_{j-1}) + c_1' + c_2\right), \end{aligned}$$

where $c_1' = \max\{c_1(A, Q_{i_\ell}\}$. Repeating inductively, we get

$$\begin{aligned} h(P_n) &\leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \cdots + \frac{2^{n-1}}{m^2}\right)(c_1' + c_2) \\ &< \left(\frac{2}{m^2}\right)^n h(P) + \frac{c_1' + c_2}{m^2 - 2} \\ &\leq \frac{1}{2^n} h(P) + \frac{1}{2}(c_1' + c_2). \end{aligned}$$

For n large enough, this gives us $h(P_n) \leq 1 + \frac{1}{2}(c_1' + c_2)$. From condition 3, this means that the P_n's are contained in some finite set, so we conclude by the equality

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}$$

that we can write any P as a linear combination of the Q_i's and points in the finite set $\{Q \in A \mid h(Q) \leq 1 + \frac{1}{2}(c_1' + c_2)\}$. □

To prove the Mordell–Weil Theorem, all we have to do now is construct a height function $h : E(K) \to \mathbb{R}$ with the three properties above. When $K = \mathbb{Q}$, we can pick the following. We first define a height function on $\mathbb{Q}$.

Definition 9.18 (Height on $\mathbb{Q}$)**.** Let $t = p/q \in \mathbb{Q}$ where p, q are relatively prime. The **height of t** is defined as

$$H(t) = \max(|p|, |q|).$$

Definition 9.19 (Height on $E(\mathbb{Q})$)**.** Let E be an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation $y^2 = x^3 + Ax + B$. For $P = (x, y) \in E(\mathbb{Q})$, we define the **height of P** via the function

$$\begin{aligned} h_x : E(\mathbb{Q}) &\to \mathbb{R} \\ P &\mapsto \begin{cases} \log H(x(P)) & P \neq O \\ 0 & P = O. \end{cases} \end{aligned}$$

Remark 9.20 (Height for $E(K)$)**.** For an arbitrary number field K, we look at the minimal polynomial of t, say

$$P_t(X) = \sum_{j=0}^{d} a_j X^j, \quad a_j \in \mathbb{Z}.$$

We define the *height on K* via

$$H(t) = \max_j\{|a_j|\}.$$

We check that this function h_x satisfies the three desired properties. It satisfies (3) because the set $\{t \in \mathbb{Q} \mid H(t) \leq C\}$ is finite (bounded above by $(2C+1)^2$) and for each x, there is at most two values of y such that $(x, y) \in E(\mathbb{Q})$. For the first two conditions, one can look at Silverman, Chapter VIII, Lemma 4.2, which says

$$\begin{aligned} h_x(P+Q) &\leq 2h_x(P) + c_1 \\ h_x([2]P) &\geq 4h_x(P) - c_2. \end{aligned}$$

We have therefore constructed a height function for $E(K)$. Combining with Weak Mordell–Weil (9.2) and Theorem 9.17 gives the Mordell–Weil Theorem.

9.4 Birch and Swinnerton-Dyer Conjecture

Let's get a taste of what arithmetic information we can get from the Mordell–Weil group. In particular, a lot is left to learn about the *rank* of an elliptic curve.

Suppose $E/\mathbb{Q}$ has good reduction at p. From the Weil Conjectures (now proven), we know that the reduction $\widetilde{E}_p/\mathbb{F}_p$ has a zeta function

$$Z(\widetilde{E}_p/\mathbb{F}_p, T) = \frac{1 - a_pT + pT^2}{(1-T)(1-pT)}$$

which satisfies nice analytic properties (e.g., functional equation). We can patch up these local parts together to get the L-function of an elliptic curve

$$L(E/\mathbb{Q}, s) = \prod_{p \text{ good red}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

which is holomorphic on $\mathrm{Re}(s) > 1 + \frac{1}{2}$. We want L-functions to have nice analytic properties, namely meromorphic continuation and analytic functions. Wiles proved that $L(E/\mathbb{Q}, s)$ can be holomorphically continued to all of $\mathbb{C}$. Even better, there exists some newform $f \in S_2(\Gamma_0(N))$ such that $L(E, s) = L(f, s)$.

The Birch and Swinnerton-Dyer Conjecture claims

$$\boxed{\mathrm{rank}(E(\mathbb{Q})) \stackrel{?}{=} \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)}.$$

This has been proven in the case where both the "arithmetic" rank on the left and the "analytic" rank on the right are either 0 or 1. The case where rank $= 1$ is due to the influential works of Kolyvagin and Gross–Zagier, and these methods (Euler systems, Gross–Zagier formulae) continue to be studied in great depth. Beyond $r = 1$, though, there has been quite little progress.