Math 7370. Topics in Number Theory: Elliptic Curves and Arithmetic Geometry

Taught by David Zywina

Notes by Linus Setiabrata

Please let me know if you spot any mistakes! There are probably lots of typos. Things in [blue font square brackets] are personal comments. Things in [red font square brackets] are (important) announcements.

Last edited May 20, 2020. Theorem numbering unchanged since May 12, 2020.

Contents

1 Preliminaries

1.1 Jan 21, 2020

[The standard reference is Silverman's *The arithmetic of elliptic curves*. We'll discuss the material in the book and hopefully some advanced topics at the end.]

Fix a field K with characteristic not equal to 2 or 3. Choose an algebraic closure $\overline{K}$ of K. (Some nice examples are $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Q}_p, \mathbb{F}_p$.)

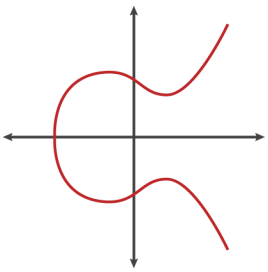
Definition 1.1.1 (Preliminary)**.** An *elliptic curve* E over K is the (projective) curve defined by $y^2 = x^3 + ax + b$ with $a, b \in K$ and $\Delta := -16(4a^3 + 27b^2) \neq 0$. △

The K-points of E are

$$E(K) \stackrel{\text{def}}{:=} \{(x, y) \in K^2 \colon y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is the "point at infinity".

For $K = \mathbb{R}$, a typical elliptic curve has $\mathbb{R}$-points that look like



where, as usual in projective geometry, $\mathcal{O}$ is vertically "up at infinity".

The condition $\Delta \neq 0$ ensures that our curve is nonsingular. Indeed, suppose E is singular at $(x_0, y_0) \in \overline{K}^2$. This means that for $f = y^2 - (x^3 + ax + b)$, we have

$$\begin{aligned} f(x_0, y_0) &= 0 \\ f_x(x_0, y_0) &= 0 \\ f_y(x_0, y_0) &= 0. \end{aligned}$$

The third equation says $2y_0 = 0$, and the first two equations say $f(x, 0)$ has a double root. This means $\operatorname{disc} f(x, 0) = 0$; one can verify that $\operatorname{disc} f(x, 0) = \Delta/16$.

Example 1.1.2. Let's consider $E/\mathbb{Q}$ given by $y^2 = x^3 - 2$. Some $\mathbb{Q}$-points are $\mathcal{O}$, $(3, 5)$, and $(3, -5)$. There are more, but they're hard to find! But we can apply the following theorem:

Theorem 1.1.3 (Bachet, 1621)**.** *Fix a $c \in \mathbb{Z} \setminus \{0\}$ and let $E/\mathbb{Q}$ be the curve $y^2 = x^3 + c$. If $(x, y) \in E(\mathbb{Q})$ with $y \neq 0$, then*

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{x^6 + 20cx^3 - 8c^2}{8y^2}\right) \in E(\mathbb{Q})$$

is a solution.

For the curve in our example,

$$(3, 5) \rightsquigarrow \left(\frac{129}{100}, \frac{-383}{1000}\right) \rightsquigarrow \left(\frac{2340922881}{58675600}, \frac{113259286337279}{449455096080}\right) \rightsquigarrow \dots.$$

We'd get an infinite sequence of distinct rational points this way. (But the number of digits grows exponentially!)

There is a geometric interpretation of this operation: we may consider the tangent line to E at $(3,5)$, namely, $y = \frac{27}{10}x - \frac{31}{10}$. The tangent line intersects the curve E at another point: we have

$$\left(\frac{27}{10}x - \frac{31}{10}\right)^2 = x^3 - 2,$$

or equivalently

$$0 = x^3 - \frac{729}{100}x^2 + \frac{837}{50}x - \frac{1161}{100} = (x-3)^2\left(x - \frac{129}{100}\right).$$

Here the factorization is not an accident: $x = 3$ is a double root of the cubic because the tangent line intersects the elliptic curve "twice" at $x = 3$; the third root of the cubic is rational because its coefficients and two of its roots are rational. We obtain

$$R = \left(\frac{129}{100}, \frac{383}{1000}\right)$$

and we negate the y-coordinate. △

Fact 1.1.4. *Consider $y^2 = x^3 + c$ with $c \in \mathbb{Z} \setminus \{0\}$ and 6-th power free, i.e. if $n^6 | c$ then $n = \pm 1$. If $(x, y) \in E(\mathbb{Q})$ with $xy \neq 0$ and $c \notin \{1, -432\}$, then Bachet's formula gives infinitely many points in $E(\mathbb{Q})$.*

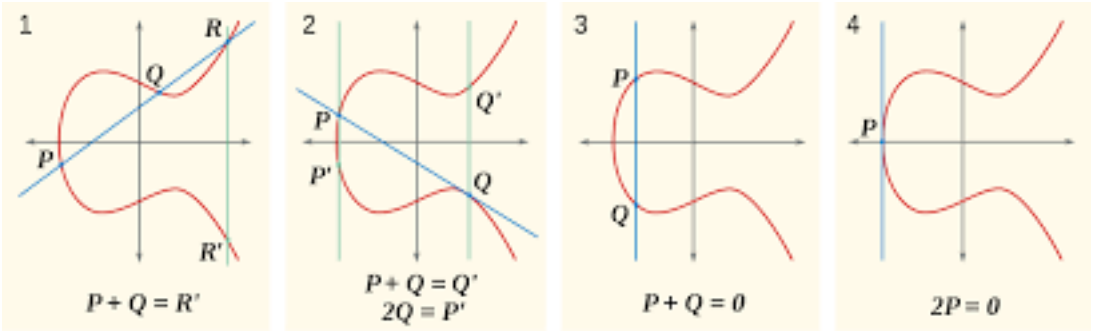
The assumption that c is 6-th power free is essentially without loss of generality, since

$$y^2 = x^3 + c \rightsquigarrow \left(\frac{y}{n^3}\right)^2 = \left(\frac{x}{n^2}\right)^3 + \frac{c}{n^6}.$$

For $c = -432$, Bachet's formula interchanges $(12, 36)$ and $(12, -36)$. For this elliptic curve, applying the change of variables $u = \frac{36-y}{6x}$ and $v = \frac{36+y}{6x}$ transforms E into $u^3 + v^3 = 1$, for which Euler proved in 1760 that the only solutions in $\mathbb{Q}$ are $(1, 0)$ and $(0, 1)$. So it's good that there are not infinitely many points to find in this case.

Let's return to a general $E/K : y^2 = x^3 + ax + b$. Our goal is to use geometry and give $E(K)$ a group law. Then $E(K)$ will be an abelian group with identity $\mathcal{O}$.

Take any points $P, Q \in E(K)$. If $P = Q$, let L be the tangent line of E at P. If $P \neq Q$, let L be the unique line through P and Q. The line L intersects E at three points P, Q, R. (Although $R \in E(\overline{K})$, it turns out that since $P, Q \in E(K)$ then $R \in E(K)$.) Let L' be the line through R and $\mathcal{O}$. Then L' intersects E at 3 points: $R, \mathcal{O}$, and the point which we define to be $P \oplus R$.



Fact 1.1.5. *The set $E(K)$ with $\oplus$ is an abelian group with identity $\mathcal{O}$. This is straightforward, except for associativity.*

We'll give a conceptual proof of associativity later. (Secretly, $E(K) \cong \mathrm{Pic}^0_K(E)$.) As we become more comfortable, we'll replace $\oplus$ with $+$ and $\mathcal{O}$ with 0.

Let's take $P_1, P_2 \in E(K)$. We can assume they are not $\mathcal{O}$, so they have coordinates $P_i = (x_i, y_i) \in K^2$. Then:

- If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 \oplus P_2 = \mathcal{O}$.
- If $x_1 \neq x_2$, then L is $y = \lambda x + \nu$ where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = y_1 - \lambda x_1 = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$$

- If $x_1 = x_2$ and $y_1 = y_2$, then L is $y = \lambda x + \nu$ with

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad \text{and} \quad \nu = \frac{-x_1^3 + ax_1 + 2b}{2y_1}.$$

In the final two cases, $P_3 = P_1 \oplus P_2 = (x_3, y_3)$ is given by

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = -\lambda x_3 - \nu.$$

Prof. Zywina will later post some code that may be useful for these.

Exercise 1: Let $E/\mathbb{Q} : y^2 = x^3 - 25x$. The points $\mathcal{O}$, $(0,0)$, $(\pm 5, 0)$, and $(4, \pm 6)$ are in $E(\mathbb{Q})$. Find some more.

Exercise 2: Let $E/\mathbb{Q} : y^2 = x^3 - 432x + 8208$. Let $P = (24, 108) \in E(\mathbb{Q})$. Compute $5P = P+P+P+P+P$.

Theorem 1.1.6 (Mordell). *For an elliptic curve $E/\mathbb{Q}$, the abelian group $E(\mathbb{Q})$ is finitely generated.*

This implies $E(\mathbb{Q}) \cong A \times \mathbb{Z}^r$ where A is finite and $r \geq 0$.

Theorem 1.1.7 (Mazur, 1978). *The group A is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 12$ with $n \neq 11$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $n = 2, 4, 6, 8$.*

The number $r = r(E)$ is called the *rank* of E. It's a deep invariant, and it's unknown whether $r(E)$ is computable. The BSD conjecture makes an analytic formula for r. It's also unknown whether or not r is bounded. Elkies gave an example with rank at least 28.

Example 1.1.8. For $E/\mathbb{Q} : y^2 = x^3 + 875x$, we have $r = 0$ and in fact $E(\mathbb{Q}) = \{\mathcal{O}, (0,0)\} \cong \mathbb{Z}/2\mathbb{Z}$. △

Example 1.1.9. For $E/\mathbb{Q} : y^2 = x^3 + 877x$. The BSD conjecture (and other things, e.g. Selmer groups) predicts that $r = 1$. In fact, $E(\mathbb{Q}) = \langle (0,0), (x_0, y_0) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ with

$$x_0 = \frac{3754945281271621931055040699420927923462 01}{621598777687150542546322078069723804 4100}.$$

The y-coordinate is worse, but you can find it from x_0. [Update:

$$y_0 = \frac{2562562679889268093887768340455130896486691532043566034647869 49}{490078023219787588959802933995928925096061616470779979261000}$$

seems to work.]

To find rational points on E as large as (x_0, y_0), one needs to make use of secret ingredients (as opposed to brute force). In this case, the secret ingredient is Heegner points. △

Let C be a smooth projective geometrically irreducible curve over $\mathbb{Q}$. (These are mild assumptions; e.g. one can blow up at finitely many singular points to get smoothness.) Let g denote the genus of C. Then:

- If $g = 0$, then $C(\mathbb{Q}) = \emptyset$ or $C \cong \mathbb{P}^1_{\mathbb{Q}}$, which has lots of $\mathbb{Q}$-points.
- (due to Faltings) If $g \geq 2$ we know that $C(\mathbb{Q})$ is finite. (This used to be the Mordell conjecture.)
- If $g = 1$, and $C(\mathbb{Q}) \neq \emptyset$, we may choose $P \in C(\mathbb{Q})$. Then there exists an embedding

$$C \hookrightarrow \mathbb{P}^2_{\mathbb{Q}}$$

whose image is an elliptic curve $E : y^2 = x^2 + ax + b$ such that $P \mapsto \mathcal{O}$. (This leads to another definition of elliptic curves, as we'll see later.)

Thus elliptic curves occupy a Goldilocks zone in the study of smooth projective geometrically irreducible curves over $\mathbb{Q}$.

1.2 Jan 23, 2020

[Again, a basic reference is Silverman's Arithmetic of Elliptic Curves]

Today will be an algebraic geometry review or crash course.

Definition 1.2.1 (Definitions; K algebraically closed)**.** Fix $n \geq 1$ and let K be an algebraically closed field. (We would like to eventually drop this, for number theoretic purposes.)

Affine n-space is $\mathbb{A}^n \stackrel{\text{def}}{=} K^n$ (so n-tuples of elements of K). *Projective n-space* is $\mathbb{P}^n = (K^{n+1} \setminus \{\mathbf{0}\})/\sim$ where $\mathbf{a} \sim \mathbf{b}$ if $\mathbf{a} = \lambda \mathbf{b}$ for some $\lambda \in K^\times$. The equivalence class of $(x_0, \dots, x_n)$ is denoted $[x_0, \dots, x_n]$.

For a set I of polynomials in $K[x_1, \dots, x_n]$, the (affine) *variety* defined by I is

$$V_I \stackrel{\text{def}}{=} \{P \in \mathbb{A}^n | f(P) = 0 \text{ for all } f \in I\} \subseteq \mathbb{A}^n.$$

The set V_I is unchanged if we replace I by the ideal it generates. For a set $I \subseteq K[x_0, \dots, x_n]$ of homogeneous polynomials, the (projective) *variety* defined by I is

$$V_I \stackrel{\text{def}}{=} \{P \in \mathbb{P}^n | f(P) = 0 \text{ for all homogeneous } f \in I\}.$$

(Note that V_I is well defined because $f(\lambda \mathbf{b}) = \lambda^d f(\mathbf{b})$.) As before, the set V_I is unchanged if we replace I by the ideal it generates.

The sets $\mathbb{A}^n$ and $\mathbb{P}^n$ have the *Zariski topology*; the closed sets are the V_I. Then V_I gets a topology induced from $\mathbb{A}^n$ or $\mathbb{P}^n$.

We say $V = V_I$ is *irreducible* if whenever $V = V_1 \cup V_2$ for closed V_1, V_2, then $V = V_1$ or $V = V_2$.

The *dimension* of an irreducible V is the largest $d \geq 0$ such that

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_d$$

with V_i irreducible.

Consider an affine variety $V \subseteq \mathbb{A}^n$. We may define its *ideal*

$$I(V) \stackrel{\text{def}}{=} \{f \in K[x_1, \dots, x_n] | f(P) = 0 \text{ for } P \in V\}$$

and its *coordinate ring*

$$K[V] \stackrel{\text{def}}{=} K[x_1, \dots, x_n]/I(V).$$

These give distinct functions $V \to K$ (by evaluation).

Note that V is irreducible if and only if $I(V)$ is a prime ideal, if and only if $K[V]$ is an integral domain. If V is irreducible, the *function field* $K(V)$ of V is the fraction field of $K[V]$. In this case, $\dim V = \text{trdeg} K(V)$ is the *transcendence degree* of $K(V)$.

For $P \in V$, the *local ring* of V at P is

$$K[V]_P \stackrel{\text{def}}{=} \left\{ \frac{f}{g} \colon f, g \in K[V], g(P) \neq 0 \right\}$$

consisting of elements of $K(V)$ which are defined ("are *regular*") at P. We can also define

$$\begin{aligned} K[V]_P &\to K \\ f &\mapsto f(P) \end{aligned}$$

with kernel $\mathfrak{m}_P$. Then V is *non-singular* at P if and only if $\dim_K \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim V$.

If V is irreducible and has dimension 1 (e.g. elliptic curves) and $P \in V$ is non-singular, then $K[V]_P$ is a discrete valuation ring (this means that the ideals of $K[V]_P$ are $\mathfrak{m}_P^0, \mathfrak{m}_P, \mathfrak{m}_P^2, \dots$ and $\{0\}$). In particular, there is $\text{ord}_P \colon K[V]_P \to \{0, 1, 2, \dots\} \cup \{\infty\}$ such that for $f \in K[V]_P \setminus \{0\}$, the number $\text{ord}_P(f)$ is the smallest $e \geq 0$ such that $f \in \mathfrak{m}_p^e$.

We may extend ord_P to a map $\text{ord}_P \colon K(V) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ by $\text{ord}_P(f/g) = \text{ord}_P(f) - \text{ord}_P(g)$. The idea is for $f \in K(V)$ we may define a map

$$\begin{aligned} V &\dashrightarrow K \\ P &\longmapsto f(P) \end{aligned}$$

If $\mathrm{ord}_P(f) \geq 0$, it is the order of the zero at P. If $\mathrm{ord}_P(f) < 0$, then $-\mathrm{ord}_P(f)$ is the order of the pole at P. $\triangle$

Definition 1.2.2 (Definitions; K perfect)**.** Consider a perfect field K. (This contains characteristic zero, finite, and algebraically closed fields.) This assumption simplifies the algebraic geometry greatly.

For $K = \mathbb{Q}$, we asserted last time (Example 1.1.8) that the only solutions of $y^2 - (x^3 + 875x) = 0$ in $\mathbb{Q}$ are $(x, y) = (0, 0)$. There's no interesting geometry here, so something has to be done:

Fix an algebraic closure $\overline{K}$ of K. Define $\mathrm{Gal}_K = G_{\overline{K}/K}$ to be the group of automorphisms of $\overline{K}$ that fixes K. Then $\mathrm{Gal}_K \circlearrowright \overline{K}$, and the fixed points $\overline{K}^{\mathrm{Gal}_K} = K$, since K is perfect.

For $I \subseteq K[x_1, \ldots, x_n]$, we may define

$$V = V_I \stackrel{\mathrm{def}}{=} \{P \in \overline{K}^n | f(P) = 0 \text{ for } f \in I\}.$$

Note that $\mathrm{Gal}_K \circlearrowright \overline{K}^n$ and fixes K^n. For $\sigma \in \mathrm{Gal}_K$, $f \in I$, and $P \in V$, we have

$$0 = \sigma(f(P)) = \sigma(f)(\sigma(P)) = f(\sigma P),$$

so $\mathrm{Gal}_K \circlearrowright V$. It follows that

$$V^{\mathrm{Gal}_K} = \{P \in K^n | f(P) = 0 \text{ for } f \in I\}.$$

Then $\mathrm{Gal}_K \circlearrowright \overline{K}[x_1, \ldots, x_n]$ with $\overline{K}[x_1, \ldots, x_n]^{\mathrm{Gal}_K} = K[x_1, \ldots, x_n]$. Also, $\mathrm{Gal}_K \circlearrowright I(V)$ with

$$I(V)^{\mathrm{Gal}_K} = \{f \in K[x_1, \ldots, x_n] | f(P) = 0 \text{ for } P \in V\}.$$

We denote by $I(V/K) \stackrel{\mathrm{def}}{=} I(V)^{\mathrm{Gal}_K}$.

We may also define

$$K[V] \stackrel{\mathrm{def}}{=} \underbrace{K[x_1, \ldots, x_n]/I(V/K)}_{=\overline{K}[V]^{\mathrm{Gal}_K}} \hookrightarrow \overline{K}[V].$$

For a set $V \subseteq \overline{K}^n$ with a Galois action $\mathrm{Gal}_K \circlearrowright V$, we may ask whether V is "defined over K" (i.e., if it comes from a set $I \subseteq K[x_1, \ldots, x_n]$). The answer (or definition) is that $I(V)$ is generated by $I(V/K) = I(V) \cap K[x_1, \ldots, x_n]$.

We may summarize these sets and their fixed points in the following table:

Set with Galois action	Fixed points
$\overline{K}^n$	K^n
$V = \{P \in \overline{K}^n \mid f(P) = 0 \text{ for } f \in I\}$	$\{P \in K^n \mid f(P) = 0 \text{ for } f \in I\}$
$\overline{K}[x_1, \ldots, x_n]$	$K[x_1, \ldots, x_n]$
$I(V) = \{f \in \overline{K}[x_1, \ldots, x_n] \mid f(P) = 0 \text{ for } P \in V\}$	$I(V/K) = \{f \in K[x_1, \ldots, x_n] \mid f(P) = 0 \text{ for } P \in V\}$
$\overline{K}[V]$	$K[V] = K[x_1, \ldots, x_n]/I(V/K)$

There is also a Galois action $\mathrm{Gal}_K \circlearrowright \mathbb{P}^n(\overline{K})$, with fixed points $\mathbb{P}^n(\overline{K})^{\mathrm{Gal}_K} = \mathbb{P}^n(K)$. (For $K = \mathbb{Q}$, observe that $[\sqrt{2}, \sqrt{8}] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is stable under the $\mathrm{Gal}_{\mathbb{Q}}$ action. But in this case, $[\sqrt{2}, \sqrt{8}] = [1, 2]$.)

For a projective variety $V \subseteq \mathbb{P}^n$, $I(V)$ is the ideal of $\overline{K}[x_0, \ldots, x_n]$ generated by homogeneous $f \in \overline{K}[x_0, \ldots, x_n]$ such that $f(P) = 0$ for all $P \in V$.

Then V is "defined over K" if $I(V)$ is generated by homogeneous $f \in I(V) \cap K[x_0, \ldots, x_n]$.

For a point $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{K})$, we have $x_i \neq 0$ for some i, so $P = [x_0/x_i, \ldots, 1, \ldots, x_n/x_i]$. Then $K(P) \stackrel{\mathrm{def}}{=} K(x_0/x_i, \ldots, x_n/x_i)$ is the *minimal field of definition* of P. $\triangle$

Let's consider a projective variety $V \subseteq \mathbb{P}^n$. Again, V is irreducible if and only if $I(V)$ is prime. We can cover $\mathbb{P}^n$ with $\mathbb{A}^n$'s. Indeed, for $0 \leq i \leq n$, we have a map

$$\mathbb{A}^n \hookrightarrow \mathbb{P}^n$$
$$(a_1, \ldots, a_n) \mapsto [a_1, \ldots, 1, \ldots, a_n]$$

where the 1 appears in the i-th coordinate. The image of this map is open in $\mathbb{P}^n$. For a fixed $0 \leq i \leq n$, we may restrict V to $\mathbb{A}^n \cap V \subseteq \mathbb{A}^n$; this is an affine variety. Conversely, $V \subseteq \mathbb{A}^n$ gives rise to its *projective closure* $\overline{V} \subseteq \mathbb{P}^n$, which is the closed set containing V. Then $\overline{V} \cap \mathbb{A}^n = V$.

Example 1.2.3 (Elliptic curves)**.** For example, for $i = n = 2$ we have

$$\begin{aligned} \mathbb{A}^2 &\hookrightarrow \mathbb{P}^2 \\ (x,y) &\mapsto [x,y,1] \end{aligned}$$

We may consider the variety $V \subseteq \mathbb{A}^2$ defined by $y^2 = x^3 + ax + b$ for $a, b \in K$. Its projective closure $\overline{V}$ is defined by $Y^2Z = X^3 + aXZ^2 + bZ^3$. Take a point $[x,y,z] \in \overline{V}$. If $z \neq 0$, then we may assume $z = 1$ and $y^2 = x^3 + ax + b$. On the other hand, if $z = 0$ then $x = 0$, and $[x,y,z] = [0,1,0]$, which was our point at infinity $\mathcal{O}$. $\triangle$

If $V \subseteq \mathbb{P}^2$ is irreducible, then $K(V)$ is the function field of $V \cap \mathbb{A}^n$. A better definition is that $K(V)$ consists of $\frac{f}{g}$ with $f, g \in K[x_0, \dots, x_n]$ homogeneous of the same degree and $g \notin I(V)$; then $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ if and only if $f_1 g_2 - f_2 g_1 \in I(V)$.

Definition 1.2.4 (Morphisms)**.** Let K be algebraically closed and let $V_1 \subseteq \mathbb{P}^m$ and $V_2 \subseteq \mathbb{P}^n$ be irreducible varieties. A *rational map* $\varphi \colon V_1 \dashrightarrow V_2$ is given by functions $f_0, \dots, f_n \in K(V_1)$ (not all zero) such that $\varphi(P) = [f_0(P), \dots, f_n(P)]$ is in V_2 for all $P \in V_1$ where all f_i are defined.

The map φ is *regular* at $P \in V$ if there is $g \in K(V_1)$ such that gf_i are regular at P and $(gf_i)(P) \neq 0$ for some i. In that case,

$$\varphi(P) \stackrel{\text{def}}{=} [(gf_0)(P), \dots, (gf_n)(P)].$$

The map φ is a *morphism* if it is regular at all $P \in V$. $\triangle$

Example 1.2.5. Suppose the characteristic of K is not 2. Consider $V \subseteq \mathbb{P}^2$ defined by $x^2 + y^2 = z^2$. We have

$$\begin{aligned} \varphi \colon \mathbb{P}^1 &\dashrightarrow V \\ [x,y] &\longmapsto \left[\frac{2xy}{x^2+y^2}, \frac{x^2-y^2}{x^2+y^2}, 1\right]. \end{aligned}$$

This map is regular if $x^2 + y^2 \neq 0$. On the other hand, φ is also the map

$$[x,y] \mapsto \left[1, \frac{x^2-y^2}{2xy}, \frac{x^2+y^2}{2xy}\right]$$

This is regular if $xy \neq 0$. Since $x^2 + y^2 = 0$ and $xy = 0$ cannot simultaneously happen (unless $[x,y]$ is the illegal point "$[0,0]$"), we have verified that φ is a morphism.

We may check that it has an inverse $V \to \mathbb{P}^1$ given by $[a,b,c] \mapsto [\frac{c+b}{a}, 1]$. $\triangle$

Next time we will talk specifically about curves.

1.3 Jan 28, 2020

[There will be chill OH on Thursdays 1:00–2:30 PM in MLT 555.]

Fix a perfect field K and an algebraic closure $\overline{K}$. We have defined $\mathbb{A}^n = \overline{K}^n$ and $\mathbb{P}^n = (\overline{K}^{n+1} \setminus \{0\})/\sim$. A set of polynomials $S \subseteq \overline{K}[x_1, \dots, x_n]$ or $\overline{K}[x_0, \dots, x_n]$ gives rise to an affine variety

$$V = \{P \in \mathbb{A}^n | f(P) = 0 \text{ for all } f \in S\} \subseteq \mathbb{A}^n$$

and a projective variety

$$V = \{P \in \mathbb{P}^n | f(P) = 0 \text{ for all homogeneous } f \in S\} \subseteq \mathbb{P}^n$$

respectively. We'll say that V is *defined over* K if the ideal $I(V)$ is generated by $I(V/K) = I(V) \cap K[\mathbf{x}]$.

Equivalent formulations of *defined over* K include:

- The absolute Galois group $\mathrm{Gal}_K = \mathrm{Gal}(\overline{K}/K)$, acting on $\overline{K}[\mathbf{x}]$, acts on $I(V)$. There is a notion of *Galois descent of vector spaces* which gives $I(V)^{\mathrm{Gal}_K} \otimes_K \overline{K} \xrightarrow{\sim} I(V)$.
- The absolute Galois group Gal_K, acting on $\mathbb{A}^n$ or $\mathbb{P}^n$, acts on V.

We use notation $\mathbb{A}^n_K$ and $\mathbb{P}^n_K$ to remind ourselves that our affine and projective space is defined over K. We'll talk about curves today.

Notation. A variety V defined over K is *nice* if it's smooth, projective, and (geometrically) irreducible.

Let's consider a nice curve C over K (so C is 1-dimensional). For a point $P \in C$, recall that

$$\overline{K}[C]_P = \{f \in \overline{K}(C) | f \text{ is regular at } P\} \subseteq \overline{K}(C)$$

is a discrete valuation ring with corresponding valuation $\mathrm{ord}_P \colon \overline{K}(C) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$. (Warning: in general, Gal_K does not necessarily act on $\overline{K}[C]_P$ if $P \notin C(K)$. Indeed, $\mathrm{ord}_P(f) = \mathrm{ord}_{\sigma(P)}(\sigma(f))$, so one should really consider the conjugates of P.)

Definition 1.3.1. A *uniformizer* at P is a $t \in \overline{K}(C)$ such that $\mathrm{ord}_P(t) = 1$. (One can in fact take $t \in K(C)$.) △

Observation 1.3.2. Consider a rational map $\varphi \colon C \dashrightarrow V$ with $V \subseteq \mathbb{P}^n$ projective. Then φ is a morphism!

Indeed, consider $\varphi = [f_0, \dots, f_n]$ with $f_i \in \overline{K}(C)$. Then $\varphi(P) = [f_0(P), \dots, f_n(P)]$, when defined, is in V. Now take any point $P \in C$ and let $m = \min_{0 \le i \le n} \mathrm{ord}_P(f_i)$. Since $\varphi = [t^{-m} f_0, \dots, t^{-m} f_n]$, and $\mathrm{ord}_P(t^{-m} f_i) \ge 0$ for all i with equality for at least one i. It follows that $\varphi(P) = [(t^{-m} f_0)(P), \dots, (t^{-m} f_n)(P)]$ is a well defined point in projective space. △

Example 1.3.3. For $f \in K(C)$, we have $C \dashrightarrow \mathbb{P}^1_K$ given by $P \mapsto [f(P), 1]$. This gives a morphism $f \colon C \to \mathbb{P}^1_K$ given by

$$f(P) = \begin{cases} [f(P), 1] & \text{if } \mathrm{ord}_P(f) \ge 0 \\ [1, 0] & \text{otherwise.} \end{cases}$$

In other words, we obtain a bijection

$$\{\text{morphisms } C \to \mathbb{P}^1_K \text{ defined over } K\} \longleftrightarrow K(C) \cup \{\infty\},$$

where $\{\infty\}$ corresponds to the constant morphism $[1, 0]$. △

Fact 1.3.4. *If $\varphi \colon C_1 \to C_2$ is a morphism of nice curves, then it is constant or surjective. If $\varphi \colon C_1 \to C_2$ is a non-constant morphism of nice curves over K, we get a homomorphism*

$$\begin{aligned} \varphi^* \colon K(C_2) &\to K(C_1) \\ f &\mapsto f \circ \varphi \end{aligned}$$

of fields fixing K.

Fact 1.3.5 (Facts)**.**

- *The field extension*

$$\begin{array}{c} K(C_1) \\ | \\ \varphi^*(K(C_2)) \end{array}$$

has finite degree; its degree is the degree *of φ and is denoted $\deg \varphi$. This extension factors*

$$\begin{array}{c} K(C_1) \\ | \\ L \\ | \\ \varphi^*(K(C_2)) \end{array}$$

where $K(C_1)/L$ is purely inseparable and $L/\varphi^*K(C_2)$ is separable. We denote the degrees of these extensions by $\deg_i \varphi$ and $\deg_s \varphi$ respectively, and we say φ is separable *if $\deg_s \varphi = \deg \varphi$. (Warning: if K has positive characteristic, then $K(C_i)$ is* not *perfect.)*

- *Any homomorphism $i\colon K(C_2) \to K(C_1)$ of fields that fixes K is of the form φ^* for a unique $\varphi\colon C_1 \to C_2$.*
- *Fix a finite index subfield $F \subseteq K(C_1)$ containing K. There is a nice curve C_2 over K (unique up to isomorphism) and a morphism $\varphi\colon C_1 \to C_2$ such that $\varphi^*(K(C_2)) = F$. Thus we get an equivalence of categories between curves and function fields (see Silverman for details).*

Let $\varphi\colon C_1 \to C_2$ be a nonconstant morphism of nice curves over K. For $P \in C_1$,We define the *ramification index of φ at P* to be

$$e_\varphi(P) \stackrel{\text{def}}{=} \operatorname{ord}_P(\varphi^* t),$$

where $t \in K(C_2)$ is a uniformizer of $\varphi(P)$. We say φ is *unramified* in P if $e_\varphi(P) = 1$.

Fact 1.3.6 (Facts)**.**

- *When φ is separable, we have $e_\varphi(P) = 1$ for all but finitely many $P \in C_1$.*
- *For $Q \in C_2$,*

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi.$$

- *For all but finitely many $Q \in C_2$, $\#\varphi^{-1}(Q) = \deg_s \varphi$.*

Divisors.
Let's fix a nice curve C/K.

Definition 1.3.7 (Divisors)**.** The *divisor group* of C, denoted $\operatorname{Div}(C)$, is the free abelian group on the set of points of C.

An element is a *divisor*, i.e. a formal sum

$$D = \sum_{P \in C} n_P P$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P. When C is an elliptic curve, we may write

$$D = \sum_{P \in C} n_P (P)$$

to distinguish divisors from the group law on the elliptic curves. The *degree* of D is

$$\deg D = \sum_{P \in C} n_P,$$

and $\mathrm{Div}^0(G) \stackrel{\text{def}}{=} \ker(\mathrm{Div}(C) \xrightarrow{\deg} \mathbb{Z})$.

The group of divisors of C over K is

$$\mathrm{Div}_K(C) = \mathrm{Div}(C)^{\mathrm{Gal}_K},$$

where $\mathrm{Gal}_K \circlearrowright \mathrm{Div}(C)$ by $\sigma(\sum n_P P) = \sum n_P \sigma(P)$. Note that $\mathrm{Div}_K(C)$ is *not* generated by $C(K)$. Indeed, given $P \in C$, adding the orbits under the Gal_K action gives an element of $\mathrm{Div}_K(C)$. (This produces a basis of $\mathrm{Div}_K(C)$.)

We also define

$$\begin{aligned}\mathrm{Div}^0_K(C) &= \mathrm{Div}^0(C)^{\mathrm{Gal}_K} \\ &= \mathrm{Div}^0(C) \cap \mathrm{Div}_K(C).\end{aligned}$$

Take $f \in \overline{K}(C)^\times$. Its *divisor* is $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$. △

Fact 1.3.8. *We have* $\deg(\mathrm{div}(f)) = 0$*, and* $\mathrm{div}(f) = 0$ *if and only if* $f \in \overline{K}^\times$*. If* $f \in K(C)$*, then* $\mathrm{div}(f) \in \mathrm{Div}_K(C)$.

Example 1.3.9. Suppose K does not have characteristic 2. Take $C \subseteq \mathbb{P}^2_K$ given by an affine model $y^2 = f(x)$ with $f(x) \in K[x]$ cubic, monic, and separable. This implies C is a nice curve.

Take $x, y \in K(C)$. Let's compute $\mathrm{div}(y)$. Note that C has a single point $\mathcal{O} = [0, 1, 0]$ which is "at ∞".

Take $f(x) = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in \overline{K}$ distinct. Define $P_i = (e_i, 0) \in C$.

We claim that $\mathrm{ord}_{P_i}(y) = 1$. Let's consider $i = 1$. Note that the discrete valuation ring $\overline{K}[C]_{P_i} \supseteq \mathfrak{m}$ contains a unique maximal ideal $\mathfrak{m} = \langle x - e_1, y \rangle$. Since

$$x - e_1 = \frac{y^2}{(x - e_2)(x - e_3)},$$

where $(x - e_2)(x - e_3)$ is a unit in $\overline{K}[C]_{P_1}$, it follows that $\mathfrak{m} = \langle y \rangle$. In other words, y is a uniformizer.

It follows that that $\mathrm{div}(y) = P_1 + P_2 + P_3 - 3\mathcal{O}$. △

Next time we'll state Riemann-Roch and get to elliptic curves.

1.4 Jan 30, 2020

[OH on 1:00–2:30PM in MLT 555 today is *canceled*. There will be an extra one next Tuesday. By the way, a canvas page exists.]

Let C be a *nice* curve over a perfect field K. (Here, *nice* means smooth, projective, and geometrically irreducible.) We defined the *divisor group* $\operatorname{Div}(C)$, which is the free abelian group on C (ie. on $\overline{K}$-points). Thus a divisor D is of the form

$$D = \sum_{P \in C} n_P P = \sum_{P \in C} n_P (P).$$

The brackets (P) are to distinguish divisors from the group law on an elliptic curve. Only finitely many n_P can be nonzero. We also defined

$$\operatorname{Div}_K(C) = \operatorname{Div}(C)^{\operatorname{Gal}(\overline{K}/K)}.$$

We had a degree map $\deg\colon \operatorname{Div}(C) \to \mathbb{Z}$, which is a homomorphism of groups; it sends each point $P \mapsto \deg(P) = 1$. We have $\operatorname{Div}^0(C) = \ker(\deg)$ and Div^0_K, which can be defined in either of the reasonable ways one might define it. There is a homomorphism

$$\begin{aligned} \operatorname{div}\colon \overline{K}(C)^\times &\to \operatorname{Div}^0(C) \\ f &\mapsto \sum_{P \in C} \operatorname{ord}_P(f) \cdot P. \end{aligned}$$

The map restricts to $K(C)^\times \xrightarrow{\operatorname{div}} \operatorname{Div}^0_K(C)$. Let's get to Riemann-Roch now.

Definition 1.4.1. A divisor $D = \sum n_P P$ is *effective* if $n_P \geq 0$ for all $P \in C$. We write $D \geq 0$.

We say $D \geq D'$ if $D - D' \geq 0$, or equivalently if $n_P \geq n'_P$ for every P, where n_P is the coefficient of P in D and n'_P is the coefficient of P in D'.

For $D \in \operatorname{Div}_K(C)$, define

$$\mathcal{L}(D) = \{f \in K(C)^\times \colon \operatorname{div}(f) + D \geq 0\} \cup \{0\}. \qquad \triangle$$

Note that $\mathcal{L}(D)$ is a vector space over K. (It's closed under addition since $\operatorname{ord}_P(f+g) \geq \min\{\operatorname{ord}_P(f), \operatorname{ord}_P(g)\}$.)

If $D = \sum_{P \in C} n_P P$, then

$$f \in \mathcal{L}(D) \iff \operatorname{ord}_P(f) + n_P \geq 0 \text{ for all } P \in C.$$

Thus asking for $f \in \mathcal{L}(D)$ is asking for f to have high order zeros whenever $n_P < 0$, and asking for f to have not-too-high order poles whenever $n_P > 0$. Even though $K(C)^\times$ is an infinite dimensional vector space, it turns out that $\mathcal{L}(D)$ is finite dimensional for each D.

Theorem 1.4.2 (Riemann-Roch)**.** *Let C be a nice curve over a perfect field K. There is an integer $g \geq 0$, called* genus *of C, such that if $D \in \operatorname{Div}_K(C)$ with $\deg D > 2g - 2$, then*

$$\dim_K \mathcal{L}(D) = \deg D - g + 1.$$

(There's a fancier version for all degrees that involves a correction term which is interesting in its own right. We'll be applying this theorem for elliptic curves, which has genus 1.)

The result follows from the case $K = \overline{K}$, since one can verify that

$$\mathcal{L}_{\overline{K}}(D) \overset{\text{def}}{=} \{f \in \overline{K}(C)^\times \colon \operatorname{div}(f) + D \geq 0\} \cup \{0\}$$

is acted on by Gal_K; by Galois descent of vector spaces we obtain

$$\mathcal{L}_{\overline{K}}(D)^{\operatorname{Gal}_K} \otimes_K \overline{K} \xrightarrow{\sim} \mathcal{L}_{\overline{K}}(D)$$

and one can check $\mathcal{L}_{\overline{K}}(D)^{\operatorname{Gal}_K} = \mathcal{L}(D)$.

Definition 1.4.3. An *elliptic curve* over K is a nice curve E over K of genus 1 with a distinguished point $\mathcal{O} \in E(K)$. $\triangle$

(Warning: there are genus 1 curves C/K with $C(K) = \emptyset$.)

Let's apply Riemann-Roch (Theorem 1.4.2) to E/K and $D = n \cdot \mathcal{O}$ for $n \geq 1$. Then

$$\dim_K \mathcal{L}(D) = n - 1 + 1 = n.$$

Note, of course, that $\mathcal{L}(\mathcal{O})$ consists of functions which are regular everywhere except with at worst a simple pole at $\mathcal{O}$. Since $\mathcal{L}(\mathcal{O})$ is one-dimensional, and $K \subseteq \mathcal{L}(\mathcal{O})$, it follows that $\mathcal{L}(\mathcal{O}) = K$.

Since $\mathcal{L}(2 \cdot \mathcal{O})$ is 2-dimensional and contains $\mathcal{L}(\mathcal{O}) = K$, we obtain

$$\mathcal{L}(2 \cdot \mathcal{O}) = K \oplus Kx$$

for some $x \in K(C)^\times$ with $\operatorname{ord}_{\mathcal{O}} x = -2$. (We know its order is exactly 2 because if it was 1 it would've shown up in $\mathcal{L}(\mathcal{O})$.) Observe also that

$$\mathcal{L}(3 \cdot \mathcal{O}) = K \oplus Kx \oplus Ky$$

for some $y \in K(C)^\times$ with $\operatorname{ord}_{\mathcal{O}} y = -3$. It now follows that

$$\mathcal{L}(4 \cdot \mathcal{O}) = K \oplus Kx \oplus Ky \oplus Kx^2,$$

since x^2 has $\operatorname{ord}_{\mathcal{O}} x^2 = -4$. Similarly,

$$\mathcal{L}(5 \cdot \mathcal{O}) = K \oplus Kx \oplus Ky \oplus Kx^2 \oplus Kxy$$

and

$$\mathcal{L}(6 \cdot \mathcal{O}) = K \oplus Kx \oplus Ky \oplus Kx^2 \oplus Kxy \oplus Kv,$$

where $v = x^3$ (since $\operatorname{ord}_{\mathcal{O}} x^3 = -6$), or $v = y^2$ (since $\operatorname{ord}_{\mathcal{O}} y^2 = -6$). In particular, if we pick $v = x^3$, then $y^2 \in \mathcal{L}(6 \cdot \mathcal{O})$ gives a linear dependence

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

with $a_i \in K$ and $c \in K^\times$. We can replace x by cx and y by c^2y to obtain

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

This is the *Weierstrass model* (cf. Definition 1.1.1)

Remark 1.4.4. Where is a_5? We should think of the equation as a degree 6 homogenous, where $\deg x = 2$ and $\deg y = 3$, and $\deg a_i = i$. △

Lemma 1.4.5. *We have $K(E) = K(x, y)$.*

Proof. By definition (Fact 1.3.5), we have $[K(E) : K(x)] = \deg(x \colon E \to \mathbb{P}^1_K)$. Our claim is that this degree is equal to 2. This is because given a point in $\mathbb{P}^1_K$ then there are two preimages. More rigorously, $\deg(x \colon E \to \mathbb{P}^1_K = \operatorname{ord}_{\mathcal{O}}(\frac{1}{x}) = 2$, because the only pole of x is at $\mathcal{O}$. Similarly, $[K(E) : K(y)] = 3$. Then $[K(E) : K(x, y)]$ is a number dividing both 2 and 3, hence is equal to 1. □

Let $C \subseteq \mathbb{P}^2_K$ be the curve defined by (♡). We have a morphism

$$\begin{aligned} \varphi \colon E &\to C \subseteq \mathbb{P}^2_K \\ P &\mapsto [x(P), y(P), 1] \quad \text{if } P \neq \mathcal{O} \\ \mathcal{O} &\mapsto \left[\left(\frac{x}{y}\right)(\mathcal{O}), 1, \left(\frac{1}{y}\right)(\mathcal{O})\right] = [0, 1, 0], \end{aligned}$$

since $\operatorname{ord}_{\mathcal{O}}(\frac{x}{y}) = 1$ and $\operatorname{ord}_{\mathcal{O}}(\frac{1}{y}) = 3$.

Note that $\deg \varphi = [K(E) : K(x, y)] = 1$. If we can prove C is nice, then φ is automatically an isomorphism (since it is on function fields); the hard part is showing C is smooth.

Assume $C \subseteq \mathbb{P}^2_K$ given by (♡) is not smooth.

Exercise 3: Show that C is smooth at $[0, 1, 0]$.

Suppose C is singular at some $P \in C \setminus \{[0,1,0]\}$. Without loss of generality, we my assume $P = (0,0)$ after a linear change of coordinates of x and y. Set

$$f \stackrel{\text{def}}{=} y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0.$$

and observe that

$$\frac{\partial f}{\partial x} = a_1y - 3x^2 - 2a_2x - a_4 \quad \text{and} \quad \frac{\partial f}{\partial y} = 2y + a_1x + a_3.$$

So if C is singular then C is given by the equation $C : y^2 + a_1xy = x^3 + a_2x$.

This gives a rational map

$$\begin{aligned} \psi \colon C &\dashrightarrow \mathbb{P}^1_K \\ (x,y) &\longmapsto [x,y]. \end{aligned}$$

(Note that C is singular so this rational map doesn't necessarily become a morphism.)

The map ψ has degree 1. The morphism is *birational*, with inverse given by

$$\begin{aligned} \mathbb{P}^1 &\dashrightarrow C \\ [1,t] &\longmapsto (t^2 + a_1 - a_2, t^3 + a_1t^2 - a_2t) \end{aligned}$$

(*This* is automatically a morphism, since $\mathbb{P}^1$ is a nice curve!) We obtain the composition

$$E \xrightarrow{\varphi} C \xrightarrow{\psi} \mathbb{P}^1_K$$

giving a morphism $\psi \circ \varphi \colon E \to \mathbb{P}^1_K$ with degree 1. Thus $E \xrightarrow{\sim} \mathbb{P}^1_K$ since they are nice It follows that the genus of E is equal to the genus of $\mathbb{P}^1_K$. But the latter is zero, so that's a contradiction.

This means that $\varphi \colon E \xrightarrow{\sim} C \subseteq \mathbb{P}^2_K$.

Last remark: the model (♡) is not unique. Any two such models for E (that map $\mathcal{O} \mapsto [0,1,0]$) are related by

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + su^2x' + t \end{aligned}$$

for $r, s, t \in K$ and $u \in K^\times$.

In conclusion, an elliptic curve is a genus 1 curve with a distinguished point (Definition 1.4.3). Riemann-Roch (Theorem 1.4.2) gives Equation (♡). Any two such equations are related by a change of variables as above.

1.5 Feb 4, 2020

[There will be usual OH on Thursdays, from 1–2:30pm. Today, there will be OH 2:30–4pm.]

Recall that an elliptic curve over K is a nice curve E over K of genus 1 with a distinguished point $\mathcal{O} \in E(K)$. (Recall that *nice* means smooth, projective, and geometrically irreducible.)

Using Riemann-Roch (Theorem 1.4.2) we showed that there is an embedding

$$\varphi\colon E \hookrightarrow \mathbb{P}^2_K$$

so that the image is cut out by a *Weierstrass equation*

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

and $\varphi(\mathcal{O}) = [0,1,0]$. We've been calling this equation (♡). (The idea is to choose $x \in \mathcal{L}(2\mathcal{O}) \setminus \mathcal{L}(\mathcal{O})$, so $\operatorname{ord}_{\mathcal{O}} x = -2$, and $y \in \mathcal{L}(3\mathcal{O}) \setminus \mathcal{L}(2)$, so $\operatorname{ord}_{\mathcal{O}} y = -3$.)

Other such embeddings are related by a change of basis, specifically by

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + su^2x' + t \end{aligned}$$

with $u \in K^\times$ and $r, s, t \in K$.

One would need to show that any smooth model given by (♡) is an elliptic curve. (The hard part is showing curves defined by (♡) has genus 1. We'll do that later, once we understand the genus better.)

Suppose char $K \neq 2$. By completing the square in y, we may assume $a_1 = a_3 = 0$. If further char $K \neq 2, 3$, we may also take $a_2 = 0$, since we may "complete the cube" (replace $x \mapsto x - a_2/3$). We arrive at the short Weierstrass equation

$$y^2 = x^3 + ax + b$$

with $a, b \in K$ and $\Delta \overset{\text{def}}{=} -16(4a^3 + 27b^2) \neq 0$.

With the short form, the model is unique up to change of basis:

$$\begin{aligned} x &= u^2x', \\ y &= u^3y' \end{aligned}$$

with $u \in K^\times$. In this basis, $(y')^2 = (x')^3 + ax' + b$ turns into

$$y^2 = x^3 + au^4x + bu^6, \quad (u \in K^\times)$$

We may define

$$j(E) \overset{\text{def}}{=} \frac{1728(4a)^3}{\Delta} \in K,$$

called the *j-invariant* of E. Note that $j(E)$ does not depend on the model.

Proposition 1.5.1. *For elliptic curves E and E' over $\overline{K}$, E and E' are isomorphic if and only if $j(E) = j(E')$.*

The backwards direction can fail for K non-algebraically closed. For example, $y^2 = x^3+1$ and $y^2 = x^3+2$ are isomorphic over $\overline{\mathbb{Q}}$ but not over $\mathbb{Q}$. This is because we need $1 = u^6 \cdot 2$, and $u \in \overline{\mathbb{Q}}$ but $u \notin \mathbb{Q}$. (We say elliptic curves are *isomorphic* if there is an isomorphism of curves that matches distinguished points.)

Proof of Proposition 1.5.1. Let's prove the backwards direction. If $j = 0$, then $y^2 = x^3 + b$ is isomorphic to $y^2 = x^3 + 1$, because there is $u \in \overline{K}^\times$ such that $u^6b = 1$.

If $j \neq 0$, then $a \neq 0$ and a change of coordinates allows us to assume $a = 1$ (i.e., we may find $u \in \overline{K}^\times$ such that $u^4a = 1$). Our Weierstrass equation becomes

$$y^2 = x^3 + x + b.$$

This form is unique up to a sign in b (since $u^4 = 1$ implies $u^6 = \pm 1$). But

$$j(E) = \frac{1728(4 \cdot 1)^3}{-16(4 \cdot 1^2 + 27b^2)}$$

determines b up to a sign as well. □

Given $j \in K$ with $\operatorname{char} K \neq 2, 3$, there is an elliptic curve E/K with $j(E) = j$. Indeed, for $j = 0$ we have $y^2 = x^3 + 1$, and for $j = 1728$ we have $y^2 = x^3 + x$. For $j \neq 0, 1728$, the curve

$$y^2 = x^3 + \frac{27}{4}\frac{j}{j-1728}x - \frac{27}{4}\frac{j}{j-1728} \tag{1}$$

suffices. (This curve has $\Delta = 2^6 3^{12} j^2/(j-1728)^3 \neq 0$.)

The automorphisms of the elliptic curve in Equation (1) are $\mathbb{Z}/2\mathbb{Z}$, generated by $(x, y) \mapsto (x, -y)$, whereas the automorphisms of $y^2 = x^3 + 1$ are $\mathbb{Z}/6\mathbb{Z}$, generated by $(x, y) \mapsto (\zeta_3 x, -y)$ and the automorphisms of $y^2 = x^3 + x$ are $\mathbb{Z}/4\mathbb{Z}$, generated by $(x, y) \mapsto (-x, iy)$. (These are, of course, automorphisms over $\overline{K}$.)

We also have a definition of $j(E)$ when $\operatorname{char} K$ is arbitrary. See the book for details.

Now let's assume $\operatorname{char} K \neq 2$ (so possibly $\operatorname{char} K = 3$), and suppose

$$E : y^2 = f(x) \in K[x]$$

with f monic, cubic, and separable, so that E is an elliptic curve. Assume that f splits over K. Then a linear change in x will give a *Legendre form*

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

with $\lambda \in K \setminus \{0, 1\}$. Then

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

For $j \in \overline{K} \setminus \{0, 1728\}$, then there are exactly six $\lambda \in \overline{K}$ such that $j(E_\lambda) = j$.

Let's think about divisors. Take a nice curve C over a perfect field K. We defined the group of divisors $\operatorname{Div}(C)$ of C, as well as the subgroup $\operatorname{Div}^0(C) \subseteq \operatorname{Div}(C)$ consisting of degree zero divisors, and the subgroup $\operatorname{div}(\overline{K}(C)^\times) \subseteq \operatorname{Div}^0(C)$ consisting of "divisors coming from functions", i.e.

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

(We claimed without proof that $\operatorname{div}(\overline{K}(C)^\times) \subseteq \operatorname{Div}^0(C)$.)

From these groups we can define the *Picard group*, or *divisor class group*

$$\operatorname{Pic}(C) \stackrel{\text{def}}{=} \operatorname{Div}(C)/\operatorname{div}(\overline{K}(C)^\times) \quad \text{and} \quad \operatorname{Pic}^0(C) \stackrel{\text{def}}{=} \operatorname{Div}^0(C)/\operatorname{div}(\overline{K}(C)^\times).$$

Alternatively, the degree map $\operatorname{Div}(C) \xrightarrow{\deg} \mathbb{Z}$ descends to a map on $\operatorname{Pic}(C)$, and $\operatorname{Pic}^0(C)$ is the kernel. As usual we may define

$$\operatorname{Pic}_K(C) \stackrel{\text{def}}{=} \operatorname{Pic}(C)^{\operatorname{Gal}_K}.$$

Note that in general, $\operatorname{Pic}(C)^{\operatorname{Gal}_K}$ is not equal to $\operatorname{Div}_K(C)/\operatorname{div}(K(C)^\times)$ (it turns out equality will hold for elliptic curves).

We have

$$\operatorname{Pic}^0_K(C) = \operatorname{Pic}^0(C)^{\operatorname{Gal}_K} = \operatorname{Pic}_K(C) \cap \operatorname{Pic}^0(C).$$

Then:

- A divisor $D \in \operatorname{Div}(C)$ gives rise to an equivalence class $[D] \in \operatorname{Pic}(C)$.
- Given two divisors $D, D' \in \operatorname{Div}(C)$ we say D and D' are *linearly equivalent* if $[D] = [D']$, and we write $D \sim D'$. (This means $D = D' + \operatorname{div}(f)$.)

Example 1.5.2. Consider $\mathbb{P}^1 = \mathbb{A}^1 \cup \{[1, 0]\} = \overline{K} \cup \{\infty\}$. Then $\operatorname{Div}^0(\mathbb{P}^1)$ is generated by $D = (a) - (\infty)$ with $a \in \overline{K}$. Note that D is principal, i.e. $D = \operatorname{div}(f)$ for some $f \in \overline{K}(\mathbb{P}^1)^\times$, namely, if t is a coordinate for $\mathbb{P}^1$, $\operatorname{div}(t - a) = (a) - (\infty)$. It follows that $\operatorname{Pic}^0(\mathbb{P}^1) = 0$. △

Lemma 1.5.3. *Let E be an elliptic curve over K. For any divisor $D \in \operatorname{Div}^0(E)$, there is a unique point $P \in E$ such that $D \sim (P) - (\mathcal{O})$.*

Proof. Existence follows from Riemann-Roch (Theorem 1.4.2). Namely, Riemann-Roch says

$$\dim_{\overline{K}} \mathcal{L}(D + (\mathcal{O})) = \deg(D + (\mathcal{O})) + 1 - g = 1.$$

where $\mathcal{L}(D + (\mathcal{O})) = \{f \in \overline{K}(E)^\times : D + (\mathcal{O}) + \operatorname{div}(f) \geq 0\} \cup \{0\}$.

In particular we may take $f \in \mathcal{L}(D + (\mathcal{O})) \setminus \{0\}$. By definition, $D + (\mathcal{O}) + \operatorname{div}(f) \geq 0$ has degree 1. Thus this divisor is just a point, i.e. $D + (\mathcal{O}) + \operatorname{div}(f) = (P)$ for some $P \in E$. It follows that $D = (P) - (\mathcal{O}) - \operatorname{div}(f)$, and $D \sim (P) - (\mathcal{O})$.

Let's prove uniqueness of P. Suppose $(P) - (\mathcal{O}) \sim (P') - (\mathcal{O})$ for $P, P' \in E$. Then $(P) - (P') \sim 0$, so $\operatorname{div}(f) = (P) - (P')$ for some $f \in \overline{K}(E)^\times$. It follows that $f + (P') \geq 0$, and $f \in \mathcal{L}((P'))$, which is a vector space of dimension 1 by Riemann-Roch. Since the constants are contained in $\mathcal{L}((P'))$, it follows that f is constant. So $\operatorname{div}(f) = 0$ implies $(P) = (P')$. □

Lemma 1.5.3 gives a bijection

$$\begin{aligned} \varphi \colon E &\xrightarrow{\sim} \operatorname{Pic}^0(E) \\ P &\mapsto [(P) - (\mathcal{O})]. \end{aligned}$$

Thus we may give E a group law by stealing it from $\operatorname{Pic}^0(E)$. (One can verify that this group law agrees with the geometric definition from the first lecture. We'll do this next time.)

Note that the identity element of the group E is necessarily $\mathcal{O}$, since $\varphi(\mathcal{O}) = [(\mathcal{O}) - (\mathcal{O})] = 0$.

Remark 1.5.4. The bijection φ gives a way to check if a divisor on E is principal, i.e. is $\operatorname{div}(f)$ for some $f \in \overline{K}(E)^\times$. If

$$D = \sum_{P \in E} n_P (P) \in \operatorname{Div}(E),$$

then D is principal if and only if $\sum_{P \in E} n_P = 0$ and $\sum_{P \in E} n_P \cdot P = \mathcal{O}$, where the second sum is the group law in E. △

1.6 Feb 6, 2020

Let E be an elliptic curve over K, with distinguished point $\mathcal{O} \in E(K)$. We have a bijection

$$\begin{aligned} \varphi\colon E &\xrightarrow{\sim} \mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{div}(\overline{K}(E)^\times) \\ P &\mapsto [(P) - (\mathcal{O})] \end{aligned}$$

We give E the (abelian!) group law from $\mathrm{Pic}^0(E)$ using φ.

Observe that φ is compatible with the Gal_K-action: for $\sigma \in \mathrm{Gal}_K$, we have

$$\sigma(\varphi(P)) = \sigma([(P) - (\mathcal{O})]) = [(\sigma(P)) - (\sigma(\mathcal{O}))] = [(\sigma(P)) - (\mathcal{O})] = \varphi(\sigma(P)),$$

where in particular we used that $\mathcal{O} \in E(K)$ is fixed by σ. Thus φ descends to an isomorphism $\varphi\colon E(K) \xrightarrow{\sim} \mathrm{Pic}^0_K(E)$. Note also that $\varphi(\mathcal{O}) = [(\mathcal{O}) - (\mathcal{O})] = 0$, so $\mathcal{O}$ is the identity of E. Let's show that this group law on E is compatible with the geometric group law we saw in the first lecture.

Let's assume $E \subseteq \mathbb{P}^2_K$ is defined by

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

with $a_i \in K$ and $\mathcal{O} = [0, 1, 0]$.

Take any $P, Q \in E$. Let's describe $P + Q$; assume P and Q are not $\mathcal{O}$. Let L be the line through P and Q (or the tangent line if $P = Q$). Then L intersects E at three points $P, Q, R \in E$ (with multiplicity). We may write

$$L : ax + by = 1$$

with $a, b \in K$ not both zero. Then $ax + by - 1 \in \overline{K}(E)$ gives rise to a divisor

$$\begin{aligned} \mathrm{div}(ax + by - 1) &= (P) + (Q) + (R) - 3 \cdot (\mathcal{O}) \\ &= (P) - (\mathcal{O}) + (Q) - (\mathcal{O}) + (R) - (\mathcal{O}) \end{aligned}$$

so in $\mathrm{Pic}^0(E)$ we obtain

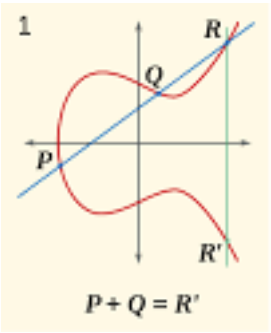
$$0 = \varphi(P) + \varphi(Q) + \varphi(R).$$

In particular, in E we have

$$P + Q + R = \mathcal{O},$$

or in other words $P + Q = -R$. So giving a geometric description of $P + Q$ reduces to giving a geometric description of $-R$ from R.

Assume $R \neq \mathcal{O}$. Consider the line through R and $\mathcal{O}$. This intersects E at three points, and we saw that they add to $\mathcal{O}$. Thus the third point is $-R = P + Q$.



We have operations $-\colon E \to E$ and $+\colon E \times E \to E$, as well as a distinguished point $\mathcal{O} \in E(K)$.

Claim 1.6.1. *The operations $-$ and $+$ are morphisms of varieties.*

Proof. We have a rational map

$$\begin{aligned} -\colon E &\dashrightarrow E \\ (x,y) &\mapsto (x, -y - a_1 x - a_3) \end{aligned}$$

that extends to a morphism $\mathcal{O} \mapsto \mathcal{O}$.

To make the notion of $E \times E$ precise in Silverman conventions (i.e., giving an embedding into projective space), we observe that the *Segre embedding* sends

$$\begin{aligned} \mathbb{P}^m \times \mathbb{P}^n &\hookrightarrow \mathbb{P}^{(m+1)(n+1)-1} \\ ([x_0, \dots, x_m], [y_0, \dots, y_n]) &\mapsto [x_0 y_0, \dots, x_i y_j, \dots, x_m y_n]. \end{aligned}$$

Then $E \times E$ lives in $\mathbb{P}^2 \times \mathbb{P}^2 \hookrightarrow \mathbb{P}^8$.

Now $+\colon E \times E \to E$ is a rational map: on the open subset

$$U \stackrel{\text{def}}{=} \{(P,Q) \in E \times E \colon P \neq \mathcal{O}, Q \neq \mathcal{O}, P \neq \pm Q\}$$

we have a morphism

$$+\colon U \to E;$$

explicit equations for this morphism are given in Silverman, Ch 3. (Warning: The rational map $+$ does not automatically extend to a morphism, because $E \times E$ is not a curve!)

To extend $+$ to a morphism, one could play with the explicit equations and make it defined on $E \times E \setminus U$. Alternatively, we may translate U around by the group structure:

Take any $Q \in E$. The *translation by* Q map $\tau_Q \colon E \to E$ is given by $P \mapsto P+Q$. Note that τ_Q is a morphism, because it's a morphism on $E \setminus \{\mathcal{O}, -Q\}$: now τ_Q extends to a morphism on all of E because it's a curve. In fact, τ_Q is an isomorphism, since it has inverse given by τ_{-Q}.

Given two points P and Q, $\tau_P \times \tau_Q$ is an automorphism of $E \times E$. Then we may consider

$$V \stackrel{\text{def}}{=} (\tau_P \times \tau_Q)(U) \subseteq E \times E.$$

The claim is that the V's cover $E \times E$ as $P, Q \in E$ vary. We are done because to define $+$ on each V we may use the commutative diagram

$$\begin{array}{ccc} V & \longrightarrow & E \\ {\scriptstyle \tau_{-P} \times \tau_{-Q}} \downarrow & & \uparrow {\scriptstyle \tau_{P+Q}} \\ U & \xrightarrow{+} & E \end{array}$$

so $+\colon V \to E$, and gluing these morphisms together we get that $E \times E \xrightarrow{+} E$ is a morphism. □

We say that E is a *group variety*.

Aside 1.6.2. We focus on Weierstrass models since they are simple and every E/K has such a model. One should keep in mind how much we are using these models. There are higher dimensional generalizations of elliptic curves called *abelian varieties*, and proofs that don't use the model often generalize to abelian varieties. △

Example 1.6.3 (Edward's curve)**.** Suppose char $K \neq 2$. Fix a $d \in K^\times$ that's not a square. Then

$$E/K : x^2 + y^2 = 1 + dx^2y^2,$$

with $\mathcal{O} = (0,1)$, is a smooth affine model for E. The projective model is singular, and you need to blow up. The blowup is an elliptic curve over K.

Then $E(K) = \{(x,y) \in K^\times \colon x^2 + y^2 = 1 + dx^2y^2\}$. (The points at infinity are defined over $K(\sqrt{d})$.)

For $(x_1, y_1), (x_2, y_2) \in E(K)$, we have

$$(x_1,y_1) + (x_2,y_2) = \Big(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \Big).$$

Nice properties of Edward's curve is that the group law is given by just one equation and that there is symmetry. Computing the group law is also more efficient. There are applications to cryptography. Unfortunately, not all elliptic curves are of this form; for example, the point $(1,0) \in E(K)$ has order 4 – the existence of such a point is a pretty special condition to impose on an elliptic curve. △

Definition 1.6.4. A homomorphism $\varphi\colon E \to E'$ of elliptic curves is a morphism of curves where $\varphi(\mathcal{O}) = \mathcal{O}$. △

Proposition 1.6.5. *The map φ is a homomorphism of groups.*

Some more background will be useful: Consider a morphism $\varphi\colon C \to C'$ of nice curves over K. This induces a morphism

$$\begin{aligned} \varphi_*\colon \operatorname{Div}(C) &\to \operatorname{Div}(C') \\ \sum_{P\in C} n_P(P) &\mapsto \sum_{P\in C} n_P(\varphi(P)) \end{aligned}$$

that preserves degrees, i.e. $\deg \varphi_* D = \deg D$ for each D. Thus this induces an isomorphism

$$\varphi_*\colon \operatorname{Pic}^0(C) \to \operatorname{Pic}^0(C').$$

This is because φ_* sends principal divisors to principal divisors, i.e. $\varphi_*(\operatorname{div} f) = \operatorname{div}(\varphi_* f)$, where $\varphi_* f$ is defined as follows: Note that φ defines an inclusion

$$\varphi^*\colon \overline{K}(C') \hookrightarrow \overline{K}(C)$$

given by $g \mapsto g \circ \varphi$, and now $\varphi_* f = N_{\overline{K}(C)/\overline{K}(C')}(f)$.

Proof of Proposition 1.6.5. Consider the diagram

$$\begin{array}{ccc} E & \xrightarrow[P\mapsto[P-\mathcal{O}]]{\sim} & \operatorname{Pic}^0(E) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ E' & \xrightarrow[P\mapsto[P-\mathcal{O}]]{\sim} & \operatorname{Pic}^0(E') \end{array}$$

It commutes because

$$\psi([P-\mathcal{O}]) = [\varphi(P) - \mathcal{O}] = [\varphi(P) - \varphi(\mathcal{O})],$$

so $\psi = \varphi_*$, of which the latter is a group homomorphism. □

2 The Geometry of Elliptic Curves

2.7 Feb 11, 2020

Let E/K be an elliptic curve over a perfect field K, with distinguished point $\mathcal{O} \in E(K)$. (We have made a choice of $\overline{K}$.)

Then E is an abelian group with an isomorphism

$$\begin{aligned} E &\xrightarrow{\sim} \mathrm{Pic}^0(E) \\ P &\longmapsto [(P) - (\mathcal{O})] \\ \sum_{P \in E} n_p P &\longmapsto \Big[\sum_{P \in E} n_p (P) \Big] \end{aligned}$$

where the sum $\sum n_P P$ uses the group law in E.

We said a homomorphism $\varphi\colon E \to E'$ of elliptic curves is a morphism of curves such that $\varphi(\mathcal{O}) = \mathcal{O}$. We saw that such a φ is a group homomorphism (Proposition 1.6.5).

Definition 2.7.1. We say φ is *defined over* K if it's defined over K as a morphism (or if it's stable under Gal_K). △

Example 2.7.2. For $m \in \mathbb{Z}$, we have a homomorphism $[m]\colon E \to E$ where

$$[m](P) = \underbrace{P + \cdots + P}_{m \text{ times}} \quad (\text{if } m \geq 0)$$

and

$$[m](P) = \underbrace{-P - \cdots - P}_{-m \text{ times}} \quad (\text{if } m < 0). \qquad \triangle$$

Non-Example 2.7.3. Fix $Q \in E \setminus \{\mathcal{O}\}$. Then $\tau_Q\colon E \to E$ given by $P \mapsto P + Q$ is not a homomorphism, since $\tau_Q(\mathcal{O}) \neq \mathcal{O}$.

However, take any $\mathcal{O}' \in E(K)$, and let E' be the elliptic curve E with distinguished point $\mathcal{O}'$. Then the translation $\tau_{\mathcal{O}'}\colon E \to E'$ with respect to E is an isomorphism of elliptic curves. △

More generally, for any morphism $\psi\colon E \to E'$ of curves,

$$\tau_{-\psi(\mathcal{O})} \circ \psi\colon E \to E'$$

is a homomorphism of elliptic curves!

Definition 2.7.4. We say a homomorphism $\varphi\colon E \to E'$ is an *isogeny* if it is nonconstant, i.e. $\varphi \neq 0$. △

Warning: what we call a homomorphism, Silverman calls an isogeny. (The only difference is whether we call the zero map an isogeny or not.)

Let $\varphi\colon E \to E'$ be an isogeny, and define $\ker \varphi \subseteq E$; it's stable under Gal_K if φ is defined over K. Take any $Q \in E'$, and choose $P \in \varphi^{-1}(Q)$ (the fiber is nonempty since φ is nonconstant, hence surjective). It follows that $\varphi^{-1}(Q) = \{P + R\colon R \in \ker \varphi\}$, since on the level of groups φ induces an isomorphism

$$E/\ker \varphi \xrightarrow{\sim} E'.$$

So all the fibers have the same size:

$$\#\varphi^{-1}(Q) = \#\ker \varphi \quad \text{for all } Q \in E'.$$

One can show that $\#\ker \varphi = \deg_s \varphi$ is the separable degree of φ (cf. Fact 1.3.5).

Suppose now that φ is separable. For any $Q \in E'$,

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi = \#\ker \varphi = \#\varphi^{-1}(Q),$$

where $e_\varphi(P)$ is the ramification index of φ at P. Since each $e_\varphi(P)$ is a positive integer, we conclude that $e_\varphi(P) = 1$ for all $P \in E$, i.e., φ is *unramified*.

The Frobenius isogeny. Let us assume $p = \operatorname{char} K > 0$ and take $q = p^r$ for some $r \geq 1$. We have an automorphism of fields

$$\begin{aligned} K &\to K \\ x &\mapsto x^q, \end{aligned}$$

(here surjectivity is the assumption that K is perfect).

Let's consider a general nice curve $C \subseteq \mathbb{P}^n_K$. Let $C^{(q)} \subseteq \mathbb{P}^n_K$ be the nice curve over K with homogeneous ideal

$$I(C^{(q)}) = \{f^{(q)} \colon f \in I(C)\},$$

where $f^{(q)}$ is the polynomial obtained by raising the coefficients of f to the q-th power. Then the q-th power *Frobenius morphism* of C is a map

$$\begin{aligned} \varphi_q \colon C &\to C^{(q)} \\ [x_0, \ldots, x_n] &\mapsto [x_0^q, \ldots, x_n^q]. \end{aligned}$$

Indeed, if $P = [x_0, \ldots, x_n] \in C$ and $f \in I(C)$ is homogeneous, then $f(P) = 0$ and taking q-th powers

$$0 = f(P)^q = f^{(q)}(\underbrace{[x_0^q, \ldots, x_n^q]}_{=\varphi_q(P)})$$

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

Fact 2.7.5 (Silverman Ch II, §2). *The morphism φ_q is purely inseparable of degree q. Furthermore, $\varphi_q^*(K(C^{(q)})) = \{f^q \colon f \in K(C)\}$.*

Fact 2.7.6. *Let $\psi \colon C \to C'$ be a nonconstant morphism of nice curves over K with* char $K > 0$. *Then ψ factors as*

$$\psi \colon C \xrightarrow{\varphi_q} C^{(q)} \xrightarrow{\lambda} C'$$

where φ_q is the q-th Frobenius morphism, with $q = \deg_i \psi$, and λ is separable.

This fact was that the decomposition

$$\begin{array}{c} K(C) \\ | \\ L \\ | \\ \psi^* K(C') \end{array}$$

where $K(C)/L$ is purely inseparable and $L/\psi^*K(C')$ is separable, and satisfies $L = \{f^q \colon f \in K(C)\}$.

If E is an elliptic curve, and $q = p^r$ where $p = \operatorname{char} K > 0$, then $\varphi_q \colon E \to E^{(q)}$ is an isogeny. If E is given by $E : y^2 = x^3 + ax + b$, then $E^{(q)}$ is given by $E^{(q)} : y^2 = x^3 + a^q x + b^q$. Here, $\varphi_q(x, y) = (x^q, y^q)$.

In this case, $\ker \varphi_q = \{0\}$. Then $\varphi_q \colon E \to E^{(q)}$ is an isomorphism of groups. However, it is not an isomorphism of elliptic curves, since $\deg \varphi_q = q > 1$.

For an isogeny $\varphi \colon E \to E'$, we get a factorization

$$\varphi \colon E \xrightarrow{\varphi_q} E^{(q)} \xrightarrow{\lambda} E'$$

where φ_q is Frobenius, and λ is a separable isogeny.

For $m \in \mathbb{Z}$, define $E[m] = \ker[m]$ to be the m-torsion subgroup of E.

Example 2.7.7. Let's compute $E[2]$. When char $K \neq 2$, then

$$E/K : y^2 = f(x)$$

for some cubic and separable f. Since $[-1](x, y) = (x, -y)$, the 2-torsion has a nice description:

$$E[2] = \{P \in E \colon [-1]P = P\} = \{(x, 0) \colon x \in \overline{K} \text{ a root of } f\} \cup \{0\}.$$

Since $E[2]$ is a group of order 4, killed by $[2]$, we see $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

When char $K = 2$, then

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

and

$$[-1](x, y) = (x, -y - a_1x - a_3) = (x, y + a_1x + a_3)$$

Then $(x, y) \in E[2]$ if and only if $[-1](x, y) = (x, y)$, if and only if $a_1x + a_3 = 0$. Then:

- If $a_1 \neq 0$, there is a unique x and $E[2] \cong \mathbb{Z}/2\mathbb{Z}$.
- If $a_1 = 0$, then $a_3 \neq 0$ (otherwise our model is singular). Then $E[2] = \{0\}$, and in fact $E[2^n] = \{0\}$. $\triangle$

The story here is that for $m \neq 0$, the map $[m] \colon E \to E$ has degree m^2. Then:

- If m is not divisible by char K, then $[m]$ is separable.
- If m is divisible by $p = \text{char } K$, then $[m]$ is not separable. Consider $[p] \colon E \to E$, which has degree p^2. Then either $[p] \colon E \to E$ factors as

$$[p] \colon E \xrightarrow{\varphi_p} E^{(p)} \xrightarrow{\lambda} E$$

where φ_p is the p-th power Frobenius and λ is a separable isogeny of degree p, and $E[p] \cong \mathbb{Z}/p\mathbb{Z}$, or $[p] \colon E \to E$ factors as

$$[p] \colon E \xrightarrow{\varphi_{p^2}} E^{(p^2)} \xrightarrow{\lambda} E$$

where $\lambda \colon E^{(p^2)} \xrightarrow{\sim} E$ is degree 1. In this case, $E[p] = \{0\}$.

Proposition 2.7.8. *For $m \in \mathbb{Z} \setminus \{0\}$, $[m]$ is an isogeny.*

Proof. In the case char $K \neq 2$, suppose $[m] = 0$. We can assume $m = p$ is a prime, since $[m] \circ [n] = [mn]$. In particular, $[p]P = 0$ for all $P \in E[2]$. Since $E[2]$ is nontrivial, p cannot be odd. It follows that $p = 2$. But $[2] \neq 0$, since $E[2] = \ker[2]$ has order 4.

In the case char $K = 2$, the proof uses the same idea, but we first show that $E[3]$ is finite and nontrivial. $\square$

Example 2.7.9. Consider

$$E/\mathbb{F}_2 : y^2 + xy + y = x^3 + 1.$$

In this case $E[2] \cong \mathbb{Z}/2\mathbb{Z}$. Then

$$E \xrightarrow{\varphi_2} E \xrightarrow{\lambda} E$$

for some degree 2 isogeny λ. One can explicitly compute

$$\lambda(x, y) = \Big(\frac{x^2 + x + 1}{x + 1}, \frac{x^2y + x + 1}{x^2 + 1}\Big).$$

$\triangle$

2.8 Feb 13, 2020

Consider a separable isogeny $\varphi\colon E \to E'$. (Recall that this means the field extension $\overline{K}(E)/\varphi^*\overline{K}(E')$ is separable; the degree of this extension is denoted $\deg\varphi$.)

We saw that for any $Q \in E'$, the fiber has size $\#\varphi^{-1}(Q) = \deg\varphi$. In particular, $\ker\varphi$ is an abelian group of order $\deg\varphi$. Also, φ is unramified.

For $Q \in \ker\varphi$, we have a translation map $\tau_Q\colon E \to E$ given by translation by Q; it an isomorphism of curves, since

$$\varphi \circ \tau_Q = \varphi.$$

(In the language of algebraic topology, the map φ is a covering map, and τ_Q is a deck transformation.)

In other words, we have defined a map

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

This is an injective homomorphism. (Injectivity follows from the fact that the induced map on function fields determines the morphism.)

Since $\#\ker\varphi = \deg\varphi$ and $\#\mathrm{Aut}(\overline{K}(E)/\varphi^*\overline{K}(E')) \le \deg\varphi$, it follows that the extension $\overline{K}(E)/\varphi^*\overline{K}(E')$ is Galois, and the that map

$$\begin{aligned} \ker\varphi &\xrightarrow{\sim} \mathrm{Gal}(\overline{K}(E)/\varphi^*\overline{K}(E')) \\ Q &\mapsto \tau_Q^* \end{aligned}$$

is an isomorphism; note that the Galois group is an abelian group.

Remark 2.8.1. If φ is defined over K, then $\mathrm{Gal}_K \circlearrowright \ker\varphi$. △

Now take a finite abelian subgroup $A \subseteq E$. Our goal is to construct a separable isogeny φ with $\ker\varphi = A$. (We will succeed, and we'll see that φ is essentially unique.)

We have an injective homomorphism

$$\begin{aligned} A &\hookrightarrow \mathrm{Aut}(\overline{K}(E)/\overline{K}) \\ Q &\mapsto \tau_Q^* \end{aligned}$$

Galois theory says the field extension $\overline{K}(E)/\overline{K}(E)^A$ is Galois with Galois group A. The curve-to-function-field correspondence (Fact 1.3.5) implies $\overline{K}(E)^A = \varphi^*\overline{K}(C)$ where C is a nice curve and $\varphi\colon E \to C$ is a nonconstant morphism. (We want to show that the genus of C is 1.)

The morphism φ is unramified. For any $Q \in C$, choose $P \in \varphi^{-1}(Q)$. Then

$$\varphi^{-1}(Q) = \{P + R\colon R \in A\}$$

has cardinality $|A|$. We apply a black box:

Theorem 2.8.2 (Hurwitz formula; Silverman Ch II, §5)**.** *Let $\varphi\colon C \to C'$ be a nonconstant morphism of nice curves of genus g and g' respectively. Then*

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

if

a) $\mathrm{char}\, K = 0$, *or*

b) $\mathrm{char}\, K = p > 0$ *and* $p \nmid e_\varphi(P)$ *for all* $P \in C$.

In general, we always have "$\ge$".

In our setting, $e_\varphi(P) = 1$ for all $P \in E$, so Theorem 2.8.2 says

$$2 \cdot 1 - 2 = \deg \varphi \cdot (2 \cdot \text{genus}(C) - 2)$$

implies that the genus of C is 1. Let $E' = C$ with distinguished point $\varphi(\mathcal{O})$. Then E' is an elliptic curves, and $\varphi\colon E \to E'$ is an isogeny. It is separable and $\ker \varphi = A$.

Fix an elliptic curve $E/\overline{K}$. We get

$$\left\{ \begin{array}{c} \text{separable isogenies } \varphi\colon E \to E' \\ \text{up to an isomorphism of } E' \end{array} \right\} \longleftrightarrow \left\{ \text{finite subgroups of } E \right\}$$
$$\varphi \longmapsto \ker \varphi$$

Remark 2.8.3. For E/K, if $A \subseteq E$ is Gal_K-stable, then there is a separable isogeny $\varphi\colon E \to E'$ over K with kernel A. Since $\mathrm{Gal}_K \circlearrowright \overline{K}(E)^A \subseteq \overline{K}(E)$, one can play the same game with $(\overline{K}(E)^A)^{\mathrm{Gal}_K} = \varphi^* K(E')$. △

For $A \subseteq E$ finite, the isogeny φ whose kernel is A is denoted by

$$\varphi\colon E \to E/A.$$

This is the usual quotient as a group, and the content is that E/A has a curve structure.

Example 2.8.4. Let $\mathrm{char}\, K \neq 2$. Let's take E/K with a point of order 2. Up to a translation,

$$E/K : y^2 = x(x^2 + ax + b)$$

for $(a^2 - 4b)b \neq 0$; the point of order 2 is $P = (0,0) \in E(K)$. What is $E/\langle P \rangle$?

Let's do some [high school] algebra. Note that

$$\begin{aligned} x(x^2 + b) &= y^2 - ax^2 \\ x^2(x^2 + b)^2 - 4bx^4 &= (y^2 - ax^2)^2 - 4bx^4 \\ x^2(x^2 - b)^2 &= y^4 - 2ax^2y^2 + (a^2 - 4b)x^4 \\ \left(\frac{y(x^2 - b)}{x^2}\right)^2 &= \frac{y^6}{x^6} - 2a\frac{y^4}{x^4} + (a^2 - 4b)\frac{y^2}{x^2} \qquad \text{(away from } (0,0)) \end{aligned}$$

so we have an elliptic curve

$$E'/K : Y^2 = X^3 - 2aX + (a^2 - 4b)X$$

with a morphism

$$\begin{aligned} &\varphi\colon E \to E' \\ &(x,y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right). \end{aligned}$$

The map φ is an isogeny. (The only thing one needs to check is the point at infinity is mapped to the point at infinity.) In fact φ is separable, and $\ker \varphi = \{\mathcal{O}, (0,0)\}$. △

Proposition 2.8.5. *Let $\varphi\colon E_1 \to E_2$ be a separable isogeny. Let $\psi\colon E_1 \to E_3$ be an isogeny. Assume $\ker \varphi \subseteq \ker \psi$. Then $\psi = \lambda \circ \varphi$ for a unique isgeony $\lambda\colon E_2 \to E_3$.*

Proof idea. Since $\ker \varphi \subseteq \ker \psi$, we have $\ker \varphi \hookrightarrow \mathrm{Aut}(K(E_1)/\psi^*\overline{K}(E_3))$ given by $Q \mapsto \tau_Q^*$. We get a tower of extensions

$$\begin{array}{c} \overline{K}(E_1) \\ | \\ \overline{K}(E_1)^{\ker \varphi} = \varphi^* \overline{K}(E_2) \\ | \\ \psi^*(\overline{K}(E_3)) \end{array}$$

The extension $\varphi^*\overline{K}(E_2)/\psi^*(\overline{K}(E_3))$ gives λ. □

Example 2.8.6. Consider a separable isogeny $\varphi\colon E \to E'$ of degree n. Then $\ker\varphi$ is an abelian group of order n, and

$$\ker\varphi \subseteq E[n] = \ker[n].$$

This gives a factorization

$$[n]\colon E \xrightarrow{\varphi} E' \xrightarrow{\hat{\varphi}} E$$

for a unique $\hat{\varphi}$. The map $\hat{\varphi}$ is called the *dual isogeny* of φ. It satisfies $\hat{\varphi}\circ\varphi = [n]$. We'll see later that $\hat{\varphi}$ exists for all isogenies. We say E and E' are *isogenous* if there is an isogeny; the dual isogeny will show that isogenousness is an equivalence relation. △

Let $\mathrm{Hom}(E,E')$ be the group of homomorphisms $E \to E'$ (It has $+$ using the group law of E', i.e. $\varphi+\psi$ is the map sending P to $\varphi(P)+\psi(P)$.)

Let $\mathrm{End}(E) = \mathrm{Hom}(E,E)$ be the ring of endomorphisms of E, with $+$ as above and multiplication being composition of functions.

We define $\mathrm{Hom}_K(E,E')$ and $\mathrm{End}_K(E)$ in the same way, except everything needs to be defined over K.

Observation 2.8.7.

- $\mathrm{Hom}(E,E')$ is torsion-free. Indeed, take $\varphi \in \mathrm{Hom}(E,E')$ and $m \geq 1$ and suppose $m\cdot\varphi = 0$. That means $[m]\circ\varphi = 0$. Since $[m]$ is an isogeny (Proposition 2.7.8), it follows that $\varphi = 0$.
- Similarly, $\mathbb{Z} \to \mathrm{End}(E)$ given by $m \mapsto [m]$ is an injective homomorphism of rings.
- $\mathrm{End}(E)$ has no zerodivisors. △

Fact 2.8.8.

- *We'll see later that the group* $\mathrm{Hom}(E,E')$ *is finitely generated abelian group [hence, a free* $\mathbb{Z}$*-module].*
- *In fact,* $\mathrm{rank}_{\mathbb{Z}}\mathrm{Hom}(E,E') \leq 4$*, and* $\mathrm{rank}_{\mathbb{Z}}\mathrm{Hom}(E,E') \leq 2$ *when* $\mathrm{char}\, K = 1$*.*
- *When* $\mathrm{char}\, K = 0$*, we "usually" have* $\mathrm{End}(E) = \mathbb{Z}$ *[so* $\mathrm{End}(E)$ *consists of multiplication maps* $[m]$*].*
- *We will describe the possible rings* $\mathrm{End}(E)$*.*

2.9 Feb 18, 2020

We're going to talk about differentials today. (This is covered in Silverman, [Ch II, §4].)
Let C be a nice curve over $\overline{K}$.

Definition 2.9.1. The space of *(meromorphic) differential forms* on C, denoted by Ω_C, is the $\overline{K}(C)$-vector space generated by symbols dx (for $x \in \overline{K}(C)$) subject to the relations

- $d(x+y) = dx + dy$
- $d(xy) = x\,dy + y\,dx$
- $d(a) = 0$ for $a \in \overline{K}$. △

Let $\varphi\colon C \to C'$ be a nonconstant morphism. We have $\varphi^*\colon \Omega_{C'} \to \Omega_C$: from the map

$$\begin{aligned} \varphi^*\colon \overline{K}(C') &\to \overline{K}(C) \\ f &\mapsto f \circ \varphi, \end{aligned}$$

we get the map

$$\begin{aligned} \varphi^*\colon \Omega_{C'} &\to \Omega_C \\ \sum_i f_i\,dx_i &\mapsto \sum_i \varphi^*(f_i)\,d(\varphi^* x_i). \end{aligned}$$

Fact 2.9.2. *We have:*

- $\dim_{\overline{K}(C)} \Omega_C = 1$.
- *φ is separable if and only if $\varphi^*\colon \Omega_{C'} \to \Omega_C$ is injective (equivalently, nonzero).*

Now take any $P \in C$. Let $t \in \overline{K}(C)$ be a uniformizer at P (so $\operatorname{ord}_P(t) = 1$). We have $dt \neq 0$ (because $\overline{K}(C)/\overline{K}(t)$ is separable; see Silverman §1). For $\omega \in \Omega_C$, we have $\omega = g\,dt$ for a unique $g \in \overline{K}(C)$. We use the notation

$$\frac{\omega}{dt} \stackrel{\text{def}}{=} g.$$

Exercise 4: Take $x \in \overline{K}(C)$ with $dx \neq 0$ and take $y = f(x)$ with $f(x) \in \overline{K}(x)$ (so f is a rational function). Show that

$$\frac{dy}{dx} = f'(x),$$

where $f'(x)$ is the usual derivative. (The exercise shows that the relations in Definition 2.9.1 encode enough calculus.)

Fact 2.9.3. *We have*

- *For $\omega \neq 0$, the number $\operatorname{ord}_P(\omega) \stackrel{\text{def}}{=} \operatorname{ord}_P(\frac{\omega}{dt}) \in \mathbb{Z}$ is independent of t.*
- *$\operatorname{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.*
- *For $x, f \in \overline{K}(C)$ with $x(P) = 0$, then*

$$\operatorname{ord}_P(f\,dx) = \operatorname{ord}_P(f) + \operatorname{ord}_P(x) - 1$$

if $\operatorname{char} K = 0$ *or* $\operatorname{char} K \nmid \operatorname{ord}_P(x)$.

Define, for $\omega \neq 0$,

$$\operatorname{div}(\omega) = \sum_{P \in C} \operatorname{ord}_P(\omega) \cdot (P) \in \operatorname{Div}(C).$$

This is called **a** *canonical divisor*. For $f \in \overline{K}(C)^\times$, we have

$$\operatorname{div}(f\omega) = \operatorname{div}(\omega) + \operatorname{div}(f).$$

Thus there is a unique equivalence class

$$[\mathrm{div}(\omega)] \in \mathrm{Pic}(C),$$

called **the** *canonical divisor class of* C. In particular, $\deg(\mathrm{div}(\omega)) \in \mathbb{Z}$ is well-defined.

Example 2.9.4. Let $C = \mathbb{P}^1$ and let t be the coordinate function, sending $t([x,1]) = x$. Let's compute $\mathrm{div}(dt)$.

Note that $\mathbb{P}^1 = \overline{K} \cup \{\infty\}$. For $\alpha \in \overline{K}$, note that $\mathrm{ord}_\alpha(t-\alpha) = 1$, so serves as a uniformizer at α. Thus $\mathrm{ord}_\alpha(dt) = \mathrm{ord}_\alpha(d(t-\alpha)) = \mathrm{ord}_\alpha(1) = 0$. At ∞, note that $\mathrm{ord}_\infty(\frac{1}{t}) = 1$, so this serves as a uniformizer at ∞. Then $d(\frac{1}{t}) = -\frac{1}{t^2}dt$, and

$$\mathrm{ord}_\infty(dt) = \mathrm{ord}_\infty\Big(-t^2 d\Big(\frac{1}{t}\Big)\Big) = \mathrm{ord}_\infty(t^2) = -2,$$

so $\mathrm{div}(dt) = -2\cdot(\infty)$ △

Example 2.9.5. Let $E \subseteq \mathbb{P}^2 : y^2 = (x-e_1)(x-e_2)(x-e_3)$ for distinct $e_i \in \overline{K}$, where $\mathrm{char}\,\overline{K} \neq 2$. As usual, denote by $\mathcal{O} = [0,1,0]$. Let $\omega \stackrel{\mathrm{def}}{=} \frac{1}{y}\,dx \in \Omega_E$. Let's compute $\mathrm{div}(\omega)$.

Denote by $P = (\alpha,\beta) \in E$ and $P' = (\alpha,-\beta) \in E$.

Observe that $\mathrm{ord}_\mathcal{O} x = -2$, and $\mathrm{div}(x) + 2\mathcal{O} \geq 0$ with no other poles. It follows that

$$\mathrm{div}(x-\alpha) = (P) + (P') - 2\cdot(\mathcal{O}).$$

Then

$$\mathrm{ord}_P(x-\alpha) = \begin{cases} 1 & \text{if } \alpha \notin \{e_1,e_2,e_3\} \\ 2 & \text{otherwise} \end{cases}$$

Now

$$2\mathrm{div}(y) = \mathrm{div}(y^2) = \mathrm{div}((x-e_1)(x-e_2)(x-e_3)) = \sum_{i=1}^{3}(2((e_i,0)) - 2(\mathcal{O})),$$

and it follows that

$$\mathrm{div}(y) = \Big(\sum_{i=1}^{3}((e_i,0))\Big) - 3(\mathcal{O}),$$

and

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P\Big(\frac{1}{y}d(x-\alpha)\Big) = \mathrm{ord}_P\Big(\frac{1}{y}\Big) + \mathrm{ord}_P(x-\alpha) - 1.$$

We have two cases:

$$\mathrm{ord}_P(\omega) = \begin{cases} 0+1-1 & \text{if } \alpha \notin \{e_1,e_2,e_3\} \\ -1+2-1 & \text{if } \alpha \in \{e_1,e_2,e_3\} \end{cases},$$

so $\mathrm{ord}_P(\omega) = 0$ always. Finally, let's compute $\mathrm{ord}_\mathcal{O}\,\omega$. Since $d(\frac{1}{x}) = -\frac{1}{x^2}\,dx$, we have

$$\mathrm{ord}_\mathcal{O}(\omega) = \mathrm{ord}_\mathcal{O}\Big(\frac{1}{y}\,dx\Big) = \mathrm{ord}_\mathcal{O}\Big(-\frac{x^2}{y}\,d\Big(\frac{1}{x}\Big)\Big) = \mathrm{ord}_\mathcal{O}\Big(\frac{x^2}{y}\Big) + \mathrm{ord}_\mathcal{O}\Big(\frac{1}{x}\Big) - 1 = 0.$$

In other words,

$$\mathrm{div}\Big(\frac{dx}{y}\Big) = 0,$$

and in particular it has degree zero. △

Definition 2.9.6. We'll say $\omega \in \Omega_C$ is *holomorphic* if $\mathrm{ord}_P(\omega) \geq 0$ for all $P \in C$, i.e., $\mathrm{div}(\omega) \geq 0$. △

Fix $\omega_0 \in \Omega_C$, with $\omega_0 \neq 0$. Define $K_C \stackrel{\text{def}}{=} \operatorname{div}(\omega_0)$. We have

$$\begin{aligned} \{\omega \in \Omega_C : \omega \text{ holomorphic}\} &\xleftarrow{\sim} \{f \in \overline{K}(C)^\times : \operatorname{div}(\omega_0) + \operatorname{div}(f) \geq 0\} \cup \{0\} \\ f\omega_0 &\longleftarrow\!\shortmid f. \end{aligned} \tag{$*$}$$

(Recall that we had defined for $D \in \operatorname{Div}(C)$,

$$\mathcal{L}(D) \stackrel{\text{def}}{=} \{f \in \overline{K}(C)^\times : D + \operatorname{div}(f) \geq 0\} \cup \{0\}.$$

So the right hand side in $(*)$ is $\mathcal{L}(K_C)$.)

Theorem 2.9.7 (Riemann-Roch, full version)**.** *For $D \in \operatorname{Div}(C)$,*

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

where g is the genus of C.

[This theorem is a big black box. ■.] Let's consider the case $D = 0$ of Theorem 2.9.7. Then

$$\underbrace{\ell(0)}_{=1} - \ell(K_C) = \underbrace{\deg 0}_{=0} - g + 1.$$

In other words, $\ell(K_C) = g$. Explicitly,

$$\dim_{\overline{K}}\{\omega \in \Omega_C : \omega \text{ holomorphic}\} = g.$$

This is a good definition of the (geometric) genus of C.

When $D = K_C$, Theorem 2.9.7 says

$$\underbrace{\ell(K_C)}_{=g} - \underbrace{\ell(0)}_{=1} = \deg K_C - g + 1,$$

and this gives $\deg K_C = 2g - 2$.

Example 2.9.8. For $\mathbb{P}^1$, we computed $\deg(\operatorname{div}(dt)) = -2$, so $g = 0$. △

Example 2.9.9. For $E : y^2 = f(x)$, where f is cubic and separable, and char $K \neq 2$, we computed $\deg(\operatorname{div}(\frac{dx}{y})) = 0$, so $g = 1$. △

Finally, when $\deg D > 2g-2$, we recover the old Riemann-Roch (Theorem 1.4.2), because $\ell(K_C - D) = 0$, as we now show. Indeed, suppose there exists $f \in \mathcal{L}(K_C - D) \setminus \{0\}$. Then $K_C - D + \operatorname{div} f \geq 0$. Taking degrees,

$$(2g - 2) - \deg D + 0 \geq 0,$$

and $\deg D \leq 2g - 2$. Since $\ell(K_C - D) = 0$, the full version of Riemann-Roch (Theorem 2.9.7) says exactly that

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

as the old Riemann-Roch (Theorem 1.4.2) asserts.

Example 2.9.10. Consider $E \subseteq \mathbb{P}^2$ defined by a smooth model Equation (♡)

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

for $a_i \in K$. The claim is that E has genus 1, so that E is an elliptic curve with $\mathcal{O} = [0, 1, 0]$. Indeed, let us differentiate (♡) to obtain

$$2y\,dy + a_1x\,dy + a_1y\,dx + a_3\,dy = 3x^2\,dx + 2a_2x\,dx + a_4\,dx.$$

Collecting like terms,

$$(2x + a_1x + a_3)\,dy = (3x^2 + 2a_2x + a_4 - a_1y)\,dx$$

Define

$$\omega \stackrel{\text{def}}{=} \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} = \frac{dx}{2y + a_1x + a_3} \in \Omega_E.$$

We have $\operatorname{div}(\omega) = 0$, and $2g - 2 = \deg(\operatorname{div}(\omega)) = 0$ implies $g = 1$. We say ω is the *invariant differential of E*. It is a basis over $\overline{K}$ of $\{\omega \in \Omega_E : \omega \text{ holomorphic}\}$. △

2.10 Feb 20, 2020

[I was out of town. This is essentially copied from Arthur Tanjaya's pristinely latexed notes.]

Consider an elliptic curve E/K, $E \subseteq \mathbb{P}^2$ defined by

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

for $a_i \in K$. We defined the *invariant differential* of E as

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2 + a_4 - a_1y} \in \Omega_E.$$

Recall that Ω_E is a 1-dimensional $\overline{K}(E)$-vector space generated by dx, $x \in \overline{K}(E)$, with "usual" rules (linearity, product rule, and constants should have derivative zero). The invariant differential ω is holomorphic, i.e. $\operatorname{ord}_P(\omega) \geq 0$ for all $P \in E$. (We write $\operatorname{div}(\omega) \geq 0$ for this.)

Also recall that $\dim_{\overline{K}}\{\omega_0 \in \Omega_E : \omega_0 \text{ is holomorphic}\} = 1$. So ω is unique up to a scalar factor. As always, Gal_K acts on Ω_E by $\sigma(f\,dx) = \sigma(f)\,d(\sigma(x))$.

Given $Q \in E$, we have defined $\tau_Q : E \to E$, which is translation by Q. The pullback was defined as follows: given $\varphi : C \to C'$, and $f, x \in \overline{K}(C')$, we have $\varphi^*(f\,dx) = \varphi^*(f)\,d(\varphi^*x) = f \circ \varphi\, d(x \circ \varphi)$.

Proposition 2.10.1. *For any $Q \in E$, we have $\tau_Q^*(\omega) = \omega$.*

[Hence the name *invariant*.]

Proof. Note that $\tau_Q^*\omega \in \Omega_E$ is also holomorphic (τ_Q is an isomorphism, and being an isomorphism guarantees that the valuations will match up when you pull back). So $\tau_Q^*\omega = a_Q\omega$ for some $a_Q \in \overline{K}^\times$. (The constant a_Q is nonzero because you can go in reverse).

Now consider $a : E \to \overline{K}^\times \subseteq \mathbb{A}^1$ given by $Q \mapsto a_Q$. This is a morphism. (If you don't believe this, keep doing computations until you do.) Since this is a morphism from an elliptic curve to $\mathbb{A}^1$, but it's not surjective (missing 0), it must be constant. [This is from a big black box of Chapter 2. You can think of it as "bounded holomorphic function is constant" from complex analysis.]

So now consider $Q = \mathcal{O}$; note that $\tau_{\mathcal{O}}^*\omega = \omega$, so $a_Q = 1$ for all $Q \in E$. □

As an aside, the *additive group* $\mathbb{G}_a = \overline{K}$ has invariant differential dx, since $d(x + c) = dx$, and the *multiplicative group* $\mathbb{G}_m = \overline{K}^\times$ has invariant differential $\frac{dx}{x}$, because $\frac{d(cx)}{cx} = \frac{dx}{x}$.

Later we'll see that $[m]^*\omega = m\omega$, which implies $[m] : E \to E$ is separable if and only if $\operatorname{char} K \nmid m$.

Proposition 2.10.2. *Take $\varphi, \psi \in \operatorname{Hom}(E', E)$. Let ω be the invariant differential of E. Then*

$$(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega.$$

(Note that these are two different additions; the left hand side uses $+$ in E and the right hand side uses $+$ in $\Omega_{E'}$.)

Proof. For an "elementary" proof see AEC III §5. [The proof is really about the surface $E \times E$, but all of Silverman's algebraic geometry is about curves so he's stuck.] Here is the framework:

Consider

$$\begin{aligned} \mu : E \times E &\to E \\ (P, Q) &\mapsto P + Q \end{aligned}$$

and let $p_1, p_2 : E \times E \to E$ be the respective projection maps. We want to show that

$$\mu^*\omega = p_1^*\omega + p_2^*\omega \in \Omega_{E\times E}.$$

We will use crucially that ω is the invariant differential. The first step is to show that

$$\mu^*\omega = f_1p_1^*\omega + f_2p_2^*\omega \qquad \text{("ugly expression")}$$

with $f_1, f_2 \in \overline{K}(E \times E)$. (Moreover, $\{p_1^*\omega, p_2^*\omega\}$ generate $\Omega_{E\times E}$ over $\overline{K}(E \times E)$.) (Silverman takes the formula for addition and differentiates it to show this.) Intuitively, this is because the two copies of E are independent of each other.

After that, take any $Q \in E$. Consider

$$\begin{aligned} \iota_Q \colon E &\to E \times E \\ P &\mapsto (P, Q), \end{aligned}$$

and apply ι_Q^* to "ugly expression" giving

$$\underbrace{\iota_Q^*\mu^*\omega}_{(\mu\circ\iota_Q)^*\omega} = \iota_Q^*(f_1)\ \underbrace{\iota_Q^*p_1^*\omega}_{(p_1\circ\iota_Q)^*\omega} + \iota_Q^*(f_2)\ \underbrace{\iota_Q^*p_2^*\omega}_{(p_2\circ\iota_Q)^*\omega}.$$

Since $\mu \circ \iota_Q = \tau_Q$ and ω is the invariant differential, the left hand side of the above equation is just ω. On the other hand, $p_1 \circ \iota_Q$ is the identity map whereas $p_2 \circ \iota_Q$ is the constant map sending everything to Q. So the right hand side is equal to $\iota_Q^*(f_1)\omega = (f_1 \circ \iota_Q)\omega$. In total, we've verified that

$$\omega = (f_1 \circ \iota_Q)\omega \qquad \text{for all } Q \in E.$$

Thus we obtain $f_1 = 1$, and a similar argument shows that $f_2 = 1$ as well.

Now we can prove the proposition. Define

$$\begin{aligned} g \colon E' &\xrightarrow{\Delta} E' \times E' \xrightarrow{\varphi\times\psi} E \times E \\ P &\longmapsto (P, P) \end{aligned}$$

Then we have

$$\begin{aligned} \varphi + \psi = \mu \circ g &\colon E' \to E \\ \varphi = p_1 \circ g &\colon E' \to E \\ \psi = p_2 \circ g &\colon E' \to E, \end{aligned}$$

and so

$$\begin{aligned} (\varphi + \psi)^*\omega &= g^*\mu^*\omega \\ &= g^*(p_1^*\omega + p_2^*\omega) \\ &= g^*p_1^*\omega + g^*p_2^*\omega \\ &= \varphi^*\omega + \psi^*\omega \end{aligned}$$

since $\varphi, \psi \in \mathrm{Hom}(E', E)$. □

We will study the ring $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ over the next few classes. The addition is pointwise and the multiplication is composition of functions. Take $\varphi \in \mathrm{End}(E)$ and consider $\varphi^*\omega$, which is equal to $a_\varphi\omega$ for some $a_\varphi \in \overline{K}(E)$ (since Ω_E is 1-dimensional over $\overline{K}(E)$).

Claim 2.10.3. *We have $a_\varphi \in \overline{K}$, i.e. a_φ is constant.*

Proof. Take $Q \in E$ and consider $\tau_Q^*(\varphi^*\omega)$. The idea is to expand this two ways and show that they're both the same. On one hand,

$$\begin{aligned} \tau_Q^*(\varphi^*\omega) &= \tau_Q^*(a_\varphi\omega) \\ &= a_\varphi \circ \tau_Q\tau_Q^*\omega \\ &= a_\varphi \circ \tau_Q\omega. \end{aligned}$$

On the other hand,

$$\begin{aligned}(\varphi \circ \tau_Q)^*\omega &= (\tau_{\varphi(Q)} \circ \varphi)^*\omega \\ &= \varphi^* \tau_{\varphi(Q)}^* \omega \\ &= \varphi^* \omega \\ &= a_\varphi \omega.\end{aligned}$$

So $a_\varphi \circ \tau_Q = a_\varphi$ for all $Q \in E$, which implies that $a_\varphi \in \overline{K}$ (take $Q = -P$ in the equation $a_\varphi(P+Q) = a_\varphi(P)$). □

Proposition 2.10.4. *The map*

$$\begin{aligned}(*)\colon \operatorname{End}(E) &\to \overline{K} \\ \varphi &\mapsto a_\varphi\end{aligned}$$

is a homomorphism of rings.

Proof. The map $(*)$ respects addition by Proposition 2.10.2. The map $(*)$ also respects multiplication:

$$\begin{aligned}(\varphi \circ \psi)^*\omega &= \psi^*\varphi^*\omega \\ &= \psi^*(a_\varphi \omega) \\ &= a_\varphi \psi^* \omega \\ &= a_\varphi a_\psi \omega.\end{aligned}$$

(Note that if a_φ was not constant then you have to compose with ψ and you get mixed terms; we can pull the a_φ across because it's constant.)

This map also respects the identities. □

For $\varphi \neq 0 \in \operatorname{End}(E)$, φ is in the kernel of $(*)$ if and only if $\varphi^*\omega = 0$, or equivalently if φ is inseparable. In theory, this gives us a way to compute whether something is separable or not without having to compute function fields.

Corollary 2.10.5. *If* $\operatorname{char} K = 0$, *then* $\operatorname{End}(E)$ *is commutative*

Proof. Isogenies are always separable in characteristic 0, so $\operatorname{End}(E) \to \overline{K}$ is an injective homomorphism. □

Corollary 2.10.6. *For any $m \in \mathbb{Z}$, $[m]^*\omega = m\omega$ (because the map is a ring homomorphism). Also, $[m]\colon E \to E$ (with $m \neq 0$) is separable if and only if* $\operatorname{char} K \nmid m$.

Here's an example where $\operatorname{End}(E)$ is non-commutative:

Example 2.10.7. Take $p \equiv 3 \pmod 4$. Consider $E/\overline{\mathbb{F}}_p$ defined by $y^2 = x^3 - x$. Choose $i \in \overline{\mathbb{F}}_p$ such that $i^2 = -1$. We have two homomorphisms

$$\begin{aligned}\psi\colon E &\to E & \qquad \varphi\colon E &\to E \\ (x,y) &\mapsto (x^p, y^p) & \qquad (x,y) &\mapsto (-x, iy).\end{aligned}$$

We claim these two don't commute. We find:

$$\begin{aligned}(\psi \circ \varphi)(x,y) &= (-x^p, iy^p) \\ (\varphi \circ \psi)(x,y) &= (-x^p, i^p y^p) = (-x^p, -iy^p)\end{aligned}$$

because $p \equiv 3 \pmod 4$. Thus $\varphi \circ \psi \neq \psi \circ \varphi$.

Later we'll see $\mathbb{Z}[\varphi, \psi] \subseteq \operatorname{End}(E)$ is of finite index. Moreover, $\operatorname{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$ (i.e., it has basis over $\mathbb{Q}$ consisting of $1, i, j, ij$ with $i^2 = -1$, $j^2 = -p$, and $ij = -ji$). △

2.11 Feb 27, 2020

Let E/K be an elliptic curve and let $\omega \in \Omega_E$ be its invariant differential. (Thus, ω is holomorphic and $\tau_Q^* \omega = \omega_Q$ for $Q \in E$.) For $m \in \mathbb{Z}$, we have $[m]^* \omega = m\omega$. Thus, $[m]$ is separable if and only if $m \neq 0 \in K$, or equivalently $\operatorname{char} K \nmid m$.

The short term goal is to describe the torsion group $E[m]$ and to show that the torsion group $\operatorname{Hom}(E, E')$ is finitely generated as a group.

Proposition 2.11.1. *For any isogeny $\varphi\colon E \to E'$, there is a unique isogeny $\hat{\varphi}\colon E' \to E$ such that $\hat{\varphi} \circ \varphi = [\deg \varphi]$.*

We call $\hat{\varphi}$ the *dual* of φ.

Proof. Uniqueness is the easy part: if

$$\psi \circ \varphi = [\deg \varphi] = \psi' \circ \varphi,$$

then $(\psi - \psi') \circ \varphi = 0$. Because φ is surjective, it follows that $\psi = \psi'$.

Existence is harder. We proved this already for φ separable (Example 2.8.6), where we used that $\ker \varphi \subseteq E[\deg \varphi] = \ker[\deg \varphi]$. Note that if $\varphi \circ E \to E'$ and $\psi\colon E' \to E''$ have duals, then so does $\psi \circ \varphi$:

$$\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}.$$

This is because

$$(\psi \circ \varphi) \circ (\hat{\varphi} \circ \hat{\psi}) = \psi \circ \underbrace{(\varphi \circ \hat{\varphi})}_{=[\deg \varphi]} \circ \hat{\psi} = [\deg \varphi] \circ \underbrace{(\psi \circ \hat{\psi})}_{=[\deg \psi]} = [\deg \varphi \cdot \deg \psi] = [\deg(\psi \circ \varphi)].$$

We saw that any isogeny is the composition of a separable isogeny and a Frobenius. Thus it suffices to show that the p-th power Frobenius φ has a dual. Recall that $\deg \varphi = p$ and that $[p]$ is not separable. Thus $[p] = \lambda \circ \varphi$ for some isogeny λ. Then $\lambda = \hat{\varphi}$. □

We say E and E' are *isogenous* if there exists an isogeny between them. This forms an equivalence relation on elliptic curves; it's weaker than isomorphism. There's also a notion of *isogenous over K*, defined in the natural way.

If $\varphi = 0$ then we decree $\hat{\varphi} = 0$ and $\deg \varphi = 0$.

Theorem 2.11.2 (Properties of duals)**.** *Let $\varphi\colon E \to E'$ be a homomorphism.*

a) With $m = \deg \varphi$, then $\hat{\varphi} \circ \varphi = [m]$ on E, and $\varphi \circ \hat{\varphi} = [m]$ on E'.

b) For another $\psi = E' \to E''$, we have $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$.

c) For any $\psi\colon E \to E'$, we have $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.

d) For $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$, and $\deg[m] = m^2$.

e) $\deg \hat{\varphi} = \deg \varphi$.

f) $\hat{\hat{\varphi}} = \varphi$.

Proof. Let's assume all homomorphisms are nonzero.

To prove item a) we need to show $\varphi \circ \hat{\varphi} = [m]$ on E'. Then note that

$$(\varphi \circ \hat{\varphi}) \circ \varphi = \varphi \circ (\hat{\varphi} \circ \varphi) = \varphi \circ [m] = [m] \circ \varphi.$$

Because φ is surjective, $\varphi \circ \hat{\varphi} = [m]$.

We've done item b).

Item c) is legitimately hard. See Silverman for a proof in characteristic 0. We'll give an idea later.

To prove item d), first observe $\widehat{[0]} = [0]$ and $\widehat{[1]} = [1]$, and induction says

$$\widehat{[m+1]} = \widehat{[m] + [1]} = \widehat{[m]} + \widehat{[1]} = [m] + [1] = [m+1].$$

We now have $[\deg[m]] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2]$. It follows that $\deg[m] = m^2$.

Item e) follows from the fact that $\hat{\varphi} \circ \varphi = [\deg \varphi]$, since we may take degrees to get $\deg \hat{\varphi} \cdot \deg \varphi = (\deg \varphi)^2$, so $\deg \hat{\varphi} = \deg \varphi$.

Item f) follows from a) and e). □

Corollary 2.11.3. *Fix an elliptic curve E/K and an integer $m \geq 1$.*

a) If $\operatorname{char} K \nmid m$, *then* $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *as a group.*

b) If $p = \operatorname{char} K > 0$, *then either*

$$E[p^n] = \{0\} \text{ for all } n \geq 1$$

or

$$E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \text{ for all } n \geq 1.$$

Proof. For part a), we use that $[m]$ is separable. Then

$$\#E[m] = \#\ker[m] = \deg[m] = m^2.$$

We have good understanding of the subgroups $E[d] \subseteq E[m]$ for $d|n$; where $E[d]$ has order d^2. Without loss of generality, suppose $m = p^n$. Then $E[p^n] \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$ for $1 \leq a_i \leq n$ since everything is p^n-torsion. We know also that $a_1 + \cdots + a_r = 2n$, since $\#E[p^n] = p^{2n}$. It follows that $E[p] = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, hence $E[p^n] = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z}$ for $a_1, a_2 \leq n$ and $a_1 + a_2 = 2n$. It follows that $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$.

For part b), note that $[p]$ is inseparable of degree p^2. Then the separable degree

$$\deg_s[p] = 1 \text{ or } p.$$

If $\deg_s[p] = 1$, then $\deg_s[p^n] = (\deg_s[p])^n = 1$, so $E[p^n] = \{0\}$.

If $\deg_s[p] = p$, then $\deg_s[p^n] = p^n$, and similar to a), we have $E[p^n] = \mathbb{Z}/p^n\mathbb{Z}$. □

Aside 2.11.4. If $E/\mathbb{C}$ is an elliptic curve over $\mathbb{C}$, the Riemann surface $E(\mathbb{C})$ has homology

$$H_1(E(\mathbb{C}), \mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. \qquad \triangle$$

Let's study $\deg\colon \operatorname{Hom}(E, E') \to \mathbb{Z}$.

Corollary 2.11.5. *The map*

$$\deg\colon \operatorname{Hom}(E, E') \to \mathbb{Z}$$

is a positive definite quadratic form. We have

- $\deg([m] \circ \varphi) = m^2 \deg \varphi$
- $\deg \varphi \geq 0$, *and* $\deg \varphi = 0$ *if and only if* $\varphi = 0$.
- *The map*

$$\begin{aligned} \langle \cdot, \cdot \rangle\colon \operatorname{Hom}(E, E') \times \operatorname{Hom}(E, E') &\to \mathbb{Z} \\ (\psi, \varphi) &\mapsto \deg(\varphi + \psi) - \deg \varphi - \deg \psi \end{aligned}$$

  is bilinear.

Proof. For the last part, let us identify $\mathbb{Z} \subseteq \operatorname{End}(E)$. Then

$$\begin{aligned} \langle \varphi, \psi \rangle &= \deg(\varphi + \psi) - \deg \varphi - \deg \psi \\ &= \widehat{\varphi + \psi} \circ (\varphi + \psi) - \hat{\varphi} \circ \varphi - \hat{\psi} \circ \hat{\psi} \\ &= (\hat{\varphi} + \hat{\psi}) \circ (\varphi + \psi) - \hat{\varphi} \circ \varphi - \hat{\psi} \circ \hat{\psi} \\ &= \hat{\varphi} \circ \psi + \hat{\psi} \circ \varphi. \end{aligned}$$

□

Let's consider an elliptic curve $E/\mathbb{F}_q$.

Lemma 2.11.6. *We have $|E(\mathbb{F}_q)| = \deg(1-\varphi)$, where $\varphi\colon E \to E$ is the q-th power Frobenius isogeny.*

Proof. Note that $E^{(q)} = E$, so

$$E(\mathbb{F}_q) = \{P \in E\colon \varphi(P) = P\} = \ker(1-\varphi).$$

(This is because for $a \in \overline{\mathbb{F}}_q$, we have $a^q = a$ if and only if $a \in \mathbb{F}_q$.)

We need to show $1-\varphi$ is separable. This is follows from the computation

$$(1-\varphi)^*\omega = \omega + (-\varphi)^*\omega = \omega \neq 0.$$

(Note that $-\varphi$ is not separable, so $(-\varphi)^*\omega = 0$.)

Because $1-\varphi$ is separable, we have

$$\#E(\mathbb{F}_q) = \#\ker(1-\varphi) = \deg(1-\varphi). \qquad \square$$

We obtain

$$\#E(\mathbb{F}_q) = \deg(1-\varphi) = \deg 1 + \deg\varphi + \langle 1, -\varphi\rangle = q + 1 - \langle 1, \varphi\rangle.$$

Later, we'll prove

Theorem 2.11.7 (Hasse)**.** *For $E/\mathbb{F}_q$, we have*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

2.12 Mar 3, 2020

[I was out of town. This is once again essentially copied from Arthur Tanjaya's pristinely latexed notes. I'm sorry it's late!]

Last time, we gave properties of duals and described the group $E[m]$. Today, we are going to show that $\mathrm{Hom}(E, E')$ is a finitely generated group.

Before proceeding, let's sketch a proof for $K = \mathbb{C}$. We can view $E(\mathbb{C})$ as a connected, smooth, compact Riemann surface using the topology of $\mathbb{C}$. As a real manifold, $E(\mathbb{C})$ looks like a torus. Now define

$$\Lambda_E := H_1(E(\mathbb{C}), \mathbb{Z}),$$

the first (singular) homology group. By some algebraic topology, $\Lambda_E \cong \mathbb{Z}^2$.

Consider $\varphi \in \mathrm{Hom}(E, E')$. This gives a morphism of Riemann surfaces $\varphi\colon E(\mathbb{C}) \to E'(\mathbb{C})$ and therefore induces a map on homology $\varphi_*\colon \Lambda_E \to \Lambda_{E'}$. Thus we have a group homomorphism

$$\begin{aligned} \mathrm{Hom}(E, E') &\to \mathrm{Hom}_{\mathbb{Z}}(\Lambda_E, \Lambda_{E'}) \cong M_2(\mathbb{Z}) \cong \mathbb{Z}^4 \\ \varphi &\mapsto \varphi_*. \end{aligned}$$

It's not too hard to show that this homomorphism is injective. Note that since $\mathbb{Z}$ is a PID, $\mathrm{Hom}(E, E')$ is a free abelian group of rank ≤ 4.

Unfortunately, this argument does not work in general because the algebraic topology definitions don't work. It's not clear what H_1 should be, for example.

Aside 2.12.1. Suppose we had $\Lambda_E \cong \mathbb{Z}^2$ for any $E/\overline{K}$ with suitable functoriality (for example, $(\varphi \circ \psi)_* = \varphi_* \circ \psi_*$). Then we have a ring homomorphism

$$\begin{aligned} \mathrm{End}(E) &\to \mathrm{End}_{\mathbb{Z}}(\Lambda_E) \cong M_2(\mathbb{Z}) \\ \varphi &\mapsto \varphi_*. \end{aligned}$$

This gives us a homomorphism of $\mathbb{Q}$-algebras $\mathrm{End}(E) \otimes \mathbb{Q} \to M_2(\mathbb{Q})$. In characteristic p, $\mathrm{End}(E) \otimes \mathbb{Q}$ might be a division algebra of dimension 4 over $\mathbb{Q}$; the map is an isomorphism or $\mathbb{Q}$-algebras, but $M_2(\mathbb{Q})$ is not a division algebra. This is a contradiction. $\triangle$

From algebraic topology, we know $\Lambda_E = H_1(E(\mathbb{C}), \mathbb{Z}) = \pi_1(E(\mathbb{C}))^{\mathrm{ab}}$ (π_1 is actually abelian here, but we won't know that until later). Take $m \geq 1$, so $\Lambda_E/m\Lambda_E \cong (\mathbb{Z}/m\mathbb{Z})^2$, which implies that there exists an unramified cover $Y \to E(\mathbb{C})$ whose Galois group (group of deck transformations) is isomorphic to $\Lambda_E/m\Lambda_E$ (up to unique isomorphism of Y). This is a maximal unramified cover with Galois group abelian and exponent m.

We have a map $[m]\colon E \to E$ which is unramified and has degree $\deg[m] = m^2$. Note that $E[m]$ acts on E by translation, so this satisfies the UMP above and we conclude that

$$H_1(E(\mathbb{C}), \mathbb{Z}/m\mathbb{Z}) \cong \Lambda_E/m\Lambda_E \cong E[m].$$

The advantage here is that $E[m]$ has an algebrogeometric definition while H_1 involves simplices and loops and is difficult to study.

Let us go back to a general (perfect) field K. Let E, E' be elliptic curves over K and take $m \geq 1$. Then consider the map

$$\begin{aligned} \mathrm{Hom}(E, E') &\to \mathrm{Hom}(E[m], E'[m]) \\ \varphi &\mapsto \varphi|_{E[m]}. \end{aligned}$$

Unfortunately we have an issue: $\mathrm{Hom}(E[m], E'[m])$ is finite and so this map need not be injective. In order to fix this, the idea is to take m larger and larger. By doing that, we hope to recover injectivity.

Fix a prime ℓ and consider ℓ^n with $n \geq 1$. The map $[\ell]\colon E[\ell^{n+1}] \to E[\ell^n]$ is a surjective group homomorphism.

Definition 2.12.2. The *ℓ-adic Tate module* of E is

$$T_\ell(E) = \varprojlim_n E[\ell^n] = \{(P_1, P_2, \dots) \colon P_n \in E[\ell^n], [\ell]P_{n+1} = P_n \text{ for all } n \geq 1\}.$$

△

Assume $\ell \neq \operatorname{char} K$. Then $E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z})$, so $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2, where

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z} = \{(a_1, a_2, \dots) \colon a_n \in \mathbb{Z}/\ell^n\mathbb{Z}, \ell \cdot a_{n+1} \equiv a_n \pmod{\ell^n} \text{ for all } n \geq 1\}.$$

Now observe:

- $\mathbb{Z}_\ell$ is an integral domain of characteristic 0.
- $\mathbb{Z}_\ell$ is a discrete valuation ring, and the nonzero ideals are $\ell^n\mathbb{Z}_\ell$ for $n \geq 0$.

Definition 2.12.3. We define $\mathbb{Q}_\ell \stackrel{\text{def}}{=} \operatorname{Frac}(\mathbb{Z}_\ell)$ to be the quotient field of $\mathbb{Z}_\ell$. △

The valuation $v_\ell \colon \mathbb{Q}^\times \to \mathbb{Z}$ is defined by $v_\ell(\ell^n \frac{a}{b}) = n$, where $a, b \in \mathbb{Z}$ and $\ell \nmid a, b$. Likewise, the ℓ-adic absolute value is given by $|\cdot|_\ell \colon \mathbb{Q} \to \mathbb{R}$,

$$|a|_\ell = \begin{cases} \ell^{-v_\ell(a)} & \text{if } a \neq 0 \\ 0 & \text{if } a = 0 \end{cases}$$

Alternatively, $\mathbb{Q}_\ell$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\ell$. We can extend $|\cdot|_\ell$ to $\mathbb{Q}_\ell$ by continuity and then recover $\mathbb{Z}_\ell$ as

$$\mathbb{Z}_\ell = \{a \in \mathbb{Q}_\ell \colon |a|_\ell \leq 1\}.$$

Going back, we can view $T_\ell(E)$ as an algebraic version of $H_1(E, \mathbb{Z}_\ell)$. If $\ell = \operatorname{char} K$, then $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 0 or 1. Take any $\varphi \in \operatorname{Hom}(E, E')$. The restriction map $\varphi \colon E[\ell^n] \to E'[\ell^n]$ induces a homomorphism of $\mathbb{Z}_\ell$-modules $\varphi_\ell \colon T_\ell(E) \to T_\ell(E')$. This map is given by $(P_1, P_2, \dots) \mapsto (\varphi(P_1), \varphi(P_2), \dots)$.

Define

$$\begin{aligned} \operatorname{Hom}(E, E') &\to \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell(E), T_\ell(E')) \\ \varphi &\mapsto \varphi_\ell; \end{aligned}$$

this is a group homomorphism. Note that this group homomorphism is injective, since $\varphi_\ell = 0$ implies $\varphi(E[\ell^n]) = 0$ for all $n \geq 1$ and hence $\varphi = 0$. However, we don't know whether the groups are finitely generated, so we have to tensor up to get information:

Theorem 2.12.4. *For $\ell \neq \operatorname{char} K$, the homomorphism*

$$\operatorname{Hom}(E, E') \otimes \mathbb{Z}_\ell \to \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell(E), T_\ell(E'))$$

of $\mathbb{Z}_\ell$-modules is injective.

Corollary 2.12.5. $\operatorname{Hom}(E, E')$ *is a finitely generated abelian group of rank at most 4.*

Proof. We showed in Observation 2.8.7 that $\operatorname{Hom}(E, E')$ is torsion free and $\mathbb{Z}_\ell$ is a PID, so it suffices to show that $\operatorname{Hom}(E, E') \otimes \mathbb{Z}_\ell$ is free over $\mathbb{Z}_\ell$ of rank at most 4. Theorem 2.12.4 shows that $\operatorname{Hom}(E, E') \otimes \mathbb{Z}_\ell$ is isomorphic to a submodule of

$$\operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell(E), T_\ell(E')) \cong M_2(\mathbb{Z}_\ell) \cong \mathbb{Z}_\ell^4.$$

Thus, PIDness of $\mathbb{Z}_\ell$ implies that $\operatorname{Hom}(E, E') \otimes \mathbb{Z}_\ell$ is a free $\mathbb{Z}_\ell$-module of rank at most 4. □

Next time, we'll prove Theorem 2.12.4.

Note that $T_\ell(E)$ has a natural action of $\operatorname{Gal}_K = \operatorname{Gal}(\overline{K}/K)$. Since $\operatorname{Gal}_K \circlearrowright E[\ell^n]$ implies $\operatorname{Gal}_K \circlearrowright T_\ell(E)$ by $\sigma(P_1, P_2, \dots) = (\sigma P_1, \sigma P_2, \dots)$, if $\varphi \in \operatorname{Hom}_K(E, E')$, then φ_ℓ will be compatible with the Gal_K-actions:

$$\begin{aligned} \operatorname{Hom}_K(E, E') &\hookrightarrow \operatorname{Hom}_{\mathbb{Z}_\ell[\operatorname{Gal}_K]}(T_\ell(E), T_\ell(E')).\varphi \\ &\mapsto \varphi_\ell \end{aligned}$$

(Silverman uses the notation $\operatorname{Hom}_K(T_\ell(E), T_\ell(E'))$ for the group $\operatorname{Hom}_{\mathbb{Z}_\ell[\operatorname{Gal}_K]}(T_\ell(E), T_\ell(E'))$.)

Theorem 2.12.6. *The map $\operatorname{Hom}_K(E, E') \otimes \mathbb{Z}_\ell \hookrightarrow \operatorname{Hom}_K(T_\ell E, T_\ell E')$ is an isomorphism when K is finite (Tate, 1966) or when K is a number field (Faltings, 1983).*

2.13 Mar 5, 2020

Let E/K be an elliptic curve and choose a prime $\ell \neq \operatorname{char} K$. We have surjective group homomorphisms

$$\cdots \to E[\ell^n] \xrightarrow{[\ell]} \ldots \xrightarrow{[\ell]} E[\ell^3] \xrightarrow{[\ell]} E[\ell]^2 \xrightarrow{[\ell]} E[\ell].$$

The *ℓ-adic Tate module* is $T_\ell E \stackrel{\text{def}}{=} \varprojlim_n E[\ell^n]$; it is a free $\mathbb{Z}_\ell$-module of rank 2. (Recall that $\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$.)

Note that

- $\mathbb{Z}_\ell$ is a discrete valuation ring of characteristic zero.
- Every element is of the form $a_0 + a_1\ell + a_2\ell^2 + \ldots$ for unique $a_n \in \{0, 1, \ldots, \ell - 1\}$.

For each $\varphi \in \operatorname{Hom}(E, E')$, we have a $\mathbb{Z}_\ell$-module homomorphism

$$\varphi_\ell \colon T_\ell E \to T_\ell E'$$

and thus a homomorphism of $\mathbb{Z}_\ell$-modules

$$\begin{aligned} \operatorname{Hom}(E, E') \otimes \mathbb{Z}_\ell &\to \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell E, T_\ell E') \qquad (\diamondsuit) \\ \varphi &\mapsto \varphi_\ell \end{aligned}$$

Today we'll prove

Theorem 2.13.1 (cf. Theorem 2.12.4)**.** *The map ($\diamondsuit$) is injective.*

We used this last time to show that $\operatorname{Hom}(E, E')$ is a free abelian group of rank at most 4.

Proof of Theorem 2.13.1. Let M be a finitely generated subgroup of $\operatorname{Hom}(E, E')$. Define

$$M^{\text{div}} = \{\varphi \in \operatorname{Hom}(E, E') \colon [m]\varphi \in M \text{ for some } n \geq 1\}.$$

Claim 2.13.2. *The group M^{div} is finitely generated.*

Proof. To see this, note that $M \otimes \mathbb{R}$ is a finite dimensional vector space over $\mathbb{R}$; we can extend $\deg \colon M \to \mathbb{Z}$ to a continuous function $M \otimes \mathbb{R} \to \mathbb{R}$. This is because

$$\deg \varphi = 2\langle \varphi, \varphi \rangle,$$

where $\langle \varphi, \psi \rangle = \hat{\varphi} \circ \psi + \hat{\psi} \circ \varphi$ is the bilinear pairing from Corollary 2.11.5. Using the fact that $\langle \cdot, \cdot \rangle$ is bilinear, we may extend to a bilinear pairing on $M \otimes \mathbb{R}$.

Note that $M^{\text{div}} \subseteq M \otimes \mathbb{R}$, and for $\varphi \in M^{\text{div}} \setminus \{0\}$ we have $\deg \varphi \geq 1$. Thus

$$U = \{\varphi \in M \otimes \mathbb{R} \colon \deg \varphi < 1\}$$

is open and $U \cap M^{\text{div}} = \{0\}$. We find that M^{div} is a discrete subgroup of $M \otimes \mathbb{R}^d$. It follows that M^{div} is finitely generated. (This is because the image of M^{div} in $(M \otimes \mathbb{R})/M$ is discrete, and the quotient is compact; now M^{div} is finite index in M.) □

Let's continue proving Theorem 2.13.1. We have $\varphi \in M \otimes \mathbb{Z}_\ell$ with $M \subseteq \operatorname{Hom}(E, E')$ finitely generated. By Claim 2.13.2, we may assume that $M^{\text{div}} = M$.

Now let $\psi_1, \ldots, \psi_r$ be a basis of M as a $\mathbb{Z}$-module; this is also a basis of $M \otimes \mathbb{Z}_\ell$ over $\mathbb{Z}_\ell$. Pick φ, say with

$$\varphi = \sum_{i=1}^{r} \alpha_i \psi_i \quad (\alpha_i \in \mathbb{Z}_\ell)$$

so that

$$0 = \varphi_\ell = \sum_{i=1}^{r} \alpha_i (\psi_i)_\ell.$$

Choose $n \geq 1$ and take $a_i \in \mathbb{Z}$ with $\alpha_i \equiv a_i \pmod{\ell^n}$ for all $1 \leq i \leq r$ and define

$$\psi = \sum_{i=1}^{r} a_i \psi_i \in M.$$

Because

$$\psi_\ell = \psi_\ell - \varphi_\ell = \sum_{i=1}^{r} (a_i - \alpha_i)(\psi_i)_\ell,$$

where $a_i - \alpha_i \in \ell^n \mathbb{Z}_\ell$. Thus we have obtained $\psi \in M \subseteq \operatorname{Hom}(E, E')$ such that $\psi(E[\ell^n]) = 0$. It follows that $\ker[\ell^n] \subseteq \ker \psi$ and $[\ell^n]$ is separable (since $\ell \neq \operatorname{char} K$). It follows that

$$\psi = [\ell^n] \circ \lambda \quad \text{for some } \lambda \in \operatorname{Hom}(E, E').$$

In group theory notation we have $\psi = \ell^n \cdot \lambda$. They key observation is that since $M = M^{\text{div}}$ and $\psi \in M$, we have $\lambda \in M$ as well. It follows that $\ell^n | a_i$ for all i, and

$$\lambda = \sum_{i=1}^{r} \frac{a_i}{\ell^n} \psi_i,$$

and

$$\alpha_i \equiv 0 \pmod{\ell^n} \quad \text{for all } 1 \leq i \leq r,$$

i.e. $\alpha_i \in \ell^n \mathbb{Z}_\ell$. Since n is arbitrary, it follows that $\alpha_i = 0$ for every $1 \leq i \leq r$. □

Definition 2.13.3. Denote by

$$V_\ell E \stackrel{\text{def}}{=} T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

is a $\mathbb{Q}_\ell$ vector space of dimension 2. △

Note that we have actions $\operatorname{Gal}_K \circlearrowright E[\ell^n], T_\ell E, V_\ell E$ respecting the group structure. In particular, we obtain a representation

$$\rho_{E,\ell} \colon \operatorname{Gal}_K \to \operatorname{Aut}_{\mathbb{Q}_\ell}(V_\ell E) \cong \operatorname{GL}_2(\mathbb{Q}_\ell).$$

Theorem 2.13.4. *Suppose K is a number field or a finite field and fix a prime $\ell \neq \operatorname{char} K$. Then E and E' are K-isogenous if and only if $\rho_{E,\ell}$ and $\rho_{E',\ell}$ are isomorphic.*

Proof. The easier direction is the forwards one. Suppose there is a K-isogeny $\varphi \colon E \to E'$. We obtain a homomorphism of $\mathbb{Q}_\ell$ vector spaces $\varphi_\ell \colon V_\ell E \to V_\ell E'$ respecting the Gal_K actions. The map φ_ℓ has inverse $\frac{1}{\deg \varphi}(\hat{\varphi})_\ell$, so φ_ℓ is an isomorphism $V_\ell E \cong V_\ell E'$.

The harder direction is the backwards one. We have

$$\operatorname{Hom}_K(E, E') \otimes \mathbb{Q}_p \hookrightarrow \operatorname{Hom}_{\mathbb{Q}_\ell[\operatorname{Gal}_K]}(V_\ell E, V_\ell E')$$

and Faltings/Tate tells us it's surjective. Modulo this detail, the assumption $\operatorname{Hom}_{\mathbb{Q}_\ell[\operatorname{Gal}_K]}(V_\ell E, V_\ell E') \neq 0$ implies $\operatorname{Hom}_K(E, E') \neq 0$. □

Recall that our goal was to describe the ring $\operatorname{End}(E)$. We know:

- $\operatorname{End}(E)$ has no zerodivisors
- $\operatorname{End}(E)$ has characteristic 0. We can view $\mathbb{Z} \subseteq \operatorname{End}(E)$.

Thus given any $\varphi \in \operatorname{End}(E)$, we may consider the integral domain $\mathbb{Z}[\varphi]$ of characteristic zero. We can consider its fraction field $\mathbb{Q}(\varphi)$. Note that $\hat{\varphi} \in \mathbb{Q}(\varphi)$, beacuse $\hat{\varphi} \circ \varphi = \deg \varphi \in \mathbb{Z}[\varphi]$. We may define

$$P_\varphi(x) = (x - \varphi)(x - \hat{\varphi}) \in \mathbb{Q}(\varphi)[x].$$

Note that $P_\varphi(\varphi) = 0$. We claim that $P_\varphi(x) \in \mathbb{Z}[x]$ is monic of degree 2. This would implies that $[\mathbb{Q}(\varphi) : \mathbb{Q}] \leq 2$. To see this, note that

$$P_\varphi(x) = x^2 - (\varphi + \hat{\varphi})x + \varphi \cdot \hat{\varphi}.$$

Then $\varphi \cdot \hat{\varphi} = \deg \varphi \in \mathbb{Z}$, and $\varphi + \hat{\varphi} = \langle 1, \varphi \rangle = \deg(1 + \varphi) - \deg 1 - \deg \varphi \in \mathbb{Z}$.

Proposition 2.13.5. *We have* $\operatorname{disc} P_\varphi \leq 0$, *i.e.* $(\varphi + \hat{\varphi})^2 \leq 4 \deg \varphi$.

Proof. Take $m \in \mathbb{Z}$ and $n \geq 1$. Then

$$\deg(m - n\varphi) = (m - n\varphi)\widehat{(m - n\varphi)} = (m - n\varphi)(m - n\hat{\varphi}) = m^2 + (\varphi + \hat{\varphi})mn + n^2\varphi\hat{\varphi} = n^2 P_\varphi(m/n).$$

Because $0 \leq \deg(m - n\varphi)$, we obtain

$$P_\varphi(\alpha) \geq 0 \quad \text{for all } \alpha \in \mathbb{Q},$$

hence for all $\alpha \in \mathbb{R}$. It follows that $\operatorname{disc} P_\varphi \leq 0$. □

Corollary 2.13.6. *Either* $\mathbb{Q}(\varphi)$ *is* $\mathbb{Q}$ *or it is an imaginary quadratic extension of* $\mathbb{Q}$.

Theorem 2.13.7 (Hasse, cf. Theorem 2.11.7)**.** *For an elliptic curve* $E/\mathbb{F}_q$ *over a finite field,*

$$\big||E(\mathbb{F}_q)| - (q+1)\big| \leq 2\sqrt{q}.$$

Proof. Let $\varphi \in \operatorname{End}(E)$ be the q-th power Frobenius. We saw in Lemma 2.11.6 that

$$|E(\mathbb{F}_q)| = |\ker(1 - \varphi)| = \deg(1 - \varphi)$$

and in particular

$$|E(\mathbb{F}_q)| = \deg(1 - \varphi) = P_\varphi(1) = 1 - (\varphi + \hat{\varphi}) + \deg \varphi$$

so

$$\big||E(\mathbb{F}_q)| - (q+1)\big| = |\varphi + \hat{\varphi}| \leq 2\sqrt{\deg \varphi} = 2\sqrt{q},$$

with the inequality from Proposition 2.13.5. □

2.14 Mar 10, 2020

Last time, for $\varphi \in \mathrm{End}(E)$ we defined $P_\varphi(x) = (x-\varphi)(x-\hat{\varphi}) \in \mathbb{Q}(\varphi)[x]$ and observed that

$$P_\varphi(x) = x^2 - (\varphi + \hat{\varphi})x + \deg\varphi \in \mathbb{Z}[x]$$

with $P_\varphi(\varphi) = 0$. We showed that as a quadratic polynomial, $\mathrm{disc} P_\varphi \leq 0$.

Note that the ring $L = \mathrm{End}(E) \otimes \mathbb{Q}$ is a division algebra.

Proposition 2.14.1. *If $\mathrm{End}(E)$ is commutative, then L is either $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$.*

Note that in characteristic 0, we've shown that $\mathrm{End}(E)$ is commutative in Corollary 2.10.5.

Proof. Note that L is a field and is a finite extension of $\mathbb{Q}$. Also $\dim_{\mathbb{Q}} L = \mathrm{rank}_{\mathbb{Z}}\mathrm{End}(E) \leq 4$. The $L = \mathbb{Q}(\varphi)$ for some $\varphi \in \mathrm{End}(E)$ by the primitive element theorem. But then it satisfies the degree 2 polynomial relation $P_\varphi(\varphi) = 0$. Then either $L = \mathbb{Q}$ or $L/\mathbb{Q}$ is degree 2 and imaginary. □

The ring $\mathrm{End}(E)$ is an *order* in L, i.e. a subring that is a finitely generated $\mathbb{Z}$-module that spans L over $\mathbb{Q}$.

Example 2.14.2.

- Let L be a number field, i.e. a finite dimensional field extension of $\mathbb{Q}$. Let $\mathcal{O}_L$ be the integral closure of $\mathbb{Z}$ in L, called the *ring of integers* of L. That $\mathcal{O}_L$ is an order in L, in fact the maximal order in L (so every orders R of L are precisely the subrings of maximal index in $\mathcal{O}_L$), is an important theorem from a basic course in algebraic number theory. [See for example Lemma 2.38 in Mehrle's 6370 notes.]
- If $L = \mathbb{Q}$, then $\mathcal{O}_L = \mathbb{Z}$.
- If $L = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z} \setminus \{1\}$ squarefree, then the maximal order of L is

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

  The orders of L are $R = \mathbb{Z} + f \cdot \mathcal{O}_L$ where $f \geq 1$ is an integer. Moreover, $[\mathcal{O}_L : R] = f$. [See for example Example 2.48 in Mehrle's 6370 notes.] We'll show later that all such orders arise as $\mathrm{End}(E)$ for some E. △

Example 2.14.3. Let $E/\mathbb{Q} : y^2 = x^3 + 1$. We have an endomorphism

$$\begin{aligned} \varphi\colon E &\xrightarrow{\sim} E \\ (x,y) &\mapsto (\zeta x, y) \end{aligned}$$

for $\zeta \in \overline{\mathbb{Q}}$ a third root of unity. We have a ring homomorphism

$$\begin{aligned} \mathbb{Z}[\zeta] &\mapsto \mathrm{End}(E) \\ \zeta &\mapsto \varphi. \end{aligned}$$

In fact, $\mathbb{Z}[\zeta] \xrightarrow{\sim} \mathrm{End}(E)$. This is because $\mathbb{Z}[\zeta]$ is the ring of integers of $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$. △

Fact 2.14.4 (Random fact)**.** *Let K be a quadratic imaginary field. There is an elliptic curve $E/\mathbb{Q}$ with endomorphism ring $\mathrm{End}(E) \cong \mathcal{O}_K$ if and only if $\mathcal{O}_K$ is a PID. [Related: Stark-Heegner Theorem]*

For $\varphi \in \mathrm{End}(E)$ and a prime $\ell \neq \mathrm{char}\, K$, we defined $\varphi_\ell \in \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell E)$. This gives an injective ring homomorphism

$$\begin{aligned} \mathrm{End}(E) \otimes \mathbb{Z}_\ell &\hookrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell E) \cong M_2(\mathbb{Z}_\ell) \qquad (\star) \\ \varphi &\mapsto \varphi_\ell. \end{aligned}$$

Theorem 2.14.5. *For $\varphi \in \mathrm{End}(E)$ and $\ell \neq \mathrm{char}\, K$, then*

$$\det(xI - \varphi_\ell) = P_\varphi(x).$$

In particular, the coefficients of $\det(xI - \varphi_\ell)$ are in $\mathbb{Z}$ and independent of ℓ.

Proof. Let $f(x) = \deg(xI - \varphi_\ell) \in \mathbb{Q}_\ell[x]$. Cayley-Hamilton says that $f(\varphi_\ell) = 0$, so it has the same factors as the minimal polynomial of φ_ℓ. Note that $P_\varphi(\varphi_\ell) = 0$, by the ring homomorphism ($\star$). We have two cases:

- If $f(x)$ is the minimal polynomial, then $f = P_\varphi$.
- If the minimal polynomial is degree 1, then $\varphi_\ell \in \mathbb{Z}_\ell \cdot I$ is a scalar matrix. By the injectivity in ($\star$), the subgroup $\langle \varphi, 1 \rangle \subseteq \mathrm{End}(E)$ is free of rank 1, so $\varphi \in \mathbb{Z}$. It's easy to check that $P_\varphi(x) = (x - \varphi)(x - \hat{\varphi}) = (x - \varphi)^2$. □

Now suppose $\mathrm{End}(E)$ is non-commutative with E/K and $p = \mathrm{char}\, K > 0$. Recall that for $\ell \neq p$, we have

$$L \otimes \mathbb{Q}_\ell = \mathrm{End}(E) \otimes \mathbb{Q}_\ell \hookrightarrow M_2(\mathbb{Q}_\ell),$$

where $L = \mathrm{End}(E) \otimes \mathbb{Q}$.

Let's describe L. (See Silverman for a more elementary approach.) Let F be the center of L. Then F is a field. We have

Fact 2.14.6. *If L is a division algebra of finite dimension over its center F, then $L \otimes_F \overline{F} \cong M_d(\overline{F})$ for a unique $d \geq 1$. In particular, $\dim_F L = d^2$.*

In our case,

$$\dim_{\mathbb{Q}} L = [F : \mathbb{Q}] \dim_F L = [F : \mathbb{Q}] d^2.$$

On the other hand, $\dim_{\mathbb{Q}} L \leq 4$, and $d > 1$ since L is non-commutative by assumption. It follows that $F = \mathbb{Q}$ and $\dim_{\mathbb{Q}} L = 4$. In particular, for $\ell \neq p$ we get isomorphisms

$$L \otimes \mathbb{Q}_\ell \xrightarrow{\sim} M_2(\mathbb{Q}_\ell). \tag{2}$$

In particular, $\mathrm{rank}_{\mathbb{Z}} \mathrm{End}(E) = 4$.

Let v be a place of $\mathbb{Q}$ (i.e. $v = \infty$ or $v = \ell$ a prime). Define

$$\mathbb{Q}_v = \begin{cases} \mathbb{R} & \text{if } v = \infty \\ \mathbb{Q}_\ell & \text{if } v = \ell \end{cases}$$

We say L is *split* at v if

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_v \cong M_2(\mathbb{Q}_v).$$

Fact 2.14.7 (A little class field theory)**.** *Let L be a division algebra with center $\mathbb{Q}$ and $\dim_{\mathbb{Q}} L = 4$. Define the set*

$$\mathscr{S} \stackrel{\text{def}}{=} \{v \colon v \text{ a place of } \mathbb{Q} \text{ such that } L \text{ is not split}\}.$$

Then the set $\mathscr{S}$ is finite, nonempty, and has even cardinality, and $\mathscr{S}$ determines L up to isomorphism.

In our setting, $\mathscr{S} \subseteq \{\infty, p\}$, by Equation (2). Then $\mathscr{S} = \{\infty, p\}$ because it's nonempty and has even cardinality. It follows that L is uniquely determined, in particular L depends only on p. (It turns out that at ∞, we have $L \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$, the real quaternion ring.)

It follows that L has $\mathbb{Q}$-basis 1, i, j, and ij, where $i^2 = -1$, $j^2 = -p$, and $ij = -ji$. (One can check that this ring works, and uniqueness of L gives the desired claim.)

When $p = \mathrm{char}\, K > 0$, the ring $\mathrm{End}(E)$ could be commutative or not. Can we distinguish the cases?

Recall that either $E[p^n] = \mathbb{Z}/p^n\mathbb{Z}$ for all $n \geq 1$ (we say "E is *ordinary*"), or $E[p^n] = \{0\}$ for all $n \geq 1$ (we say "E is *supersingular*"). Next time we'll discuss:

Theorem 2.14.8.

(i) $\mathrm{End}(E)$ *is commutative if and only if E is ordinary*

(ii) If E is supersingular, then $j(E) \in \mathbb{F}_{p^2}$. In particular, there are only finitely many supersingular elliptic curves up to isomorphism over $\overline{K}$.

2.15 Mar 12, 2020

Let E/K be an elliptic curve. The ring $L = \mathrm{End}(E) \times \mathbb{Q}$ is a division algebra with order $\mathrm{End}(E)$. We've seen (Proposition 2.14.1) that if $\mathrm{End}(E)$ is commutative, then L is $\mathbb{Q}$ or an imaginary quadratic field. If $\mathrm{End}(E)$ is non-commutative, then $p = \mathrm{char}\, K > 0$ and L has $\mathbb{Q}$-basis $1, i, j, ij$ where $i^2 = -1$, $j^2 = -p$, and $ij = -ji$.

Recall that E is ordinary if and only if $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$ for all $n \geq 1$ and is supersingular if and only if $E[p^n] = \{0\}$ for all $n \geq 1$. Last time we stated

Theorem 2.15.1 (cf. Theorem 2.14.8)**.**

(i) $\mathrm{End}(E)$ *is commutative if and only if* E *is ordinary*

(ii) If E *is supersingular, then* $j(E) \in \mathbb{F}_{p^2}$.

Proof. First assume that E is ordinary. Then $T_pE \cong \mathbb{Z}_p$. As before we have a ring homomorphism

$$\begin{aligned} \mathrm{End}(E) &\to \mathrm{End}_{\mathbb{Z}_p}(T_pE) = \mathbb{Z}_p \\ \varphi &\mapsto \varphi_p. \end{aligned}$$

If φ_p then $\varphi(E[p^n]) = 0$ for all $n \geq 1$, so $\varphi = 0$. It follows that $\mathrm{End}(E)$ is isomorphic to a subring of $\mathbb{Z}_p$ and hence commutative.

Now assume E is supersingular. In this case, the multiplication-by-p map $[p]\colon E \to E$ is purely inseparable. Since K is perfect,

$$[p] = \lambda \circ \varphi$$

where $\varphi\colon E \to E^{(q)}$ is the q-th power Frobenius and $\lambda\colon E^{(q)} \to E$ is separable. Then

$$\begin{aligned} q = \deg \varphi = \deg_i [p] &= \deg [p] = p^2 \\ \deg \lambda = \deg_s [p] &= 1, \end{aligned}$$

so λ is an isomorphism. It follows that over $\overline{K}$

$$E \cong E^{(q)} \quad \text{hence} \quad j(E) = j(E^{(q)}) = j(E)^q.$$

It follows that $j(E) \in \mathbb{F}_q = \mathbb{F}_{p^2}$.

It's left to explain why $\mathrm{End}(E)$ is noncommutative.

Claim 2.15.2. *If* $E'/\overline{K}$ *is isogenous to* E*, then it is also supersingular and* $L \cong \mathrm{End}(E') \otimes \mathbb{Q}$.

Proof of Claim 2.15.2. Let $\varphi\colon E' \to E$ be an isogeny. Then

$$\begin{aligned} \mathrm{End}(E) \otimes \mathbb{Q} &\xrightarrow{\sim} \mathrm{End}(E') \otimes \mathbb{Q} \\ \psi &\mapsto \varphi^{-1} \circ \psi \circ \varphi, \end{aligned}$$

where $\varphi^{-1} = \frac{1}{\deg \varphi}\hat{\varphi}$. If E' is ordinary, then

$$\varphi(E'[p^n]) \subseteq E$$

gives a nontrivial p-group for large n. This is impossible, since $E[p^n] = 0$. □

Let's continue proving Theorem 2.15.1.

Suppose, for the sake of contradiction, that $\mathrm{End}(E)$ is commutative. From algebraic number theory, we have

Fact 2.15.3 (Chebotarev density; see Sec 6.5 in Mehrle's 6370 notes)**.** *There are infinitely many primes* ℓ *such that* $\ell\mathcal{O}_L$ *is a prime ideal in* $\mathcal{O}_L$.

(It's easy if $L = \mathbb{Q}$, and if $L = \mathbb{Q}(\sqrt{d})$, this is the same as saying that there are infinitely many ℓ such that d is not a square mod ℓ.)

Take $\ell \neq p$ so that $\ell\mathcal{O}_L$ is a prime ideal and $\ell \nmid [\mathcal{O}_L : \mathrm{End}(E')]$ when E' is isogenous to E. (There are only finitely many E' up to isomorphism, since $j(E') \in \mathbb{F}_{p^2}$.)

Since $\ell \neq p$, we have

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots \subseteq E$$

with $A_i \cong \mathbb{Z}/\ell^i\mathbb{Z}$. We have quotients $E_i = E/A_i$ (with homomorphisms $E \to E_i$ with kernel A_i).

Claim 2.15.4. *Among $E_1, E_2 E_3, \ldots$, there are only finitely curves up to isomorphism. (This follows from Claim 2.15.2 and part (ii) of the theorem.)*

So there are $m, n \geq 1$ so that $E_m \cong E_{m+n}$. By Claim 2.15.2, we may assume without loss of generality that $E \cong E_m \cong E_{m+n}$. So there is an isogeny $\varphi\colon E \to E$ with kernel $\mathbb{Z}/\ell^n\mathbb{Z}$. Note that $\ker\varphi \subseteq E[\ell^n]$, so

$$[\ell^n] = \lambda \circ \varphi \qquad \text{for some } \lambda \in \mathrm{End}(E).$$

In $\mathrm{End}(E)$, we have $\ell^n = \lambda\varphi$. Recall that $\ell\mathcal{O}_L$ is a prime ideal; since ℓ is prime in $\mathrm{End}(E)$, we have $\ell|\lambda$ or $\ell|\varphi$. But the latter doesn't happen since otherwise the cyclic group $\ker\varphi$ contains the non-cyclic group $E[\ell]$ as a subgroup.

So

$$\ell^{n-1} = \lambda' \circ \varphi$$

for some $\lambda' \in \mathrm{End}(E)$. Repeat the argument: we obtain $1 = \lambda'' \circ \varphi$ with $\lambda'' \in \mathrm{End}(E)$. So φ is an isomorphism; this contradicts the fact that φ has kernel $\mathbb{Z}/\ell^n\mathbb{Z}$. □

We can describe the supersingular elliptic curves over $\overline{\mathbb{F}}_p$:

- If $p = 2$, there is only one up to isomorphism: $y^2 + y = x^3$.
- For $p \geq 3$, define the polynomial

$$H_p(t) = \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \cdot t^i \in \mathbb{F}_p[t].$$

Then

Fact 2.15.5 (Silverman V, §4). *Take $E/\overline{\mathbb{F}}_p : y^2 = x(x-1)(x-\lambda)$ with $\lambda \in \overline{\mathbb{F}}_p \setminus \{0, 1\}$. Then E is supersingular if and only if $H_p(\lambda) = 0$.*

Moreover, H_p is separable, so the number of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ up to isomorphism is approximately $\frac{p-1}{12}$. (This is because $\deg H_p = \frac{p-1}{2}$ and usually E arises from 6 λ's.)

In fact, we have a "mass formula", which says

$$\sum_{\substack{E/\overline{\mathbb{F}}_p, \\ \text{s.s., up to iso}}} \frac{1}{|\mathrm{Aut}(E)|} = \frac{p-1}{24}.$$

Aside 2.15.6. Some final remarks on $\mathrm{End}(E)$:

- If $\mathrm{char}\, K = p > 0$, then
$$\mathrm{End}(E) = \mathbb{Z} \iff j(E) \notin \overline{\mathbb{F}}_p.$$
- If E is supersingular, then $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}(E) \otimes \mathbb{Q}$. △

3 Elliptic Curves over Fields of Interest

3.15 Mar 12, 2020 (Finite fields)

Let $E/\mathbb{F}_q$. We are interested in the points $E(\mathbb{F}_q)$.

Let φ be the q-th power Frobenius endomorphism of E, and define

$$P_\varphi(x) = (x-\varphi)(x-\hat{\varphi}) = x^2 - (\varphi+\hat{\varphi})x + \deg\varphi \in \mathbb{Z}[x].$$

Define $a = \varphi + \hat{\varphi}$, which we call the *trace of Frobenius*; it's the trace of the action of φ_ℓ on $T_\ell E$.

We showed that

$$|E(\mathbb{F}_q)| = \deg(1-\varphi) = P_\varphi(1) = 1 - a + q.$$

We had seen (Theorem 2.13.7) that $|a| \le 2\sqrt{q}$.

Aside 3.15.1. Suppose q is odd and $E/\mathbb{F}_q : y^2 = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ cubic and separable. We have a homomorphism

$$\chi\colon \mathbb{F}_q^\times \to \{\pm 1\}$$

with kernel $(\mathbb{F}_q^\times)^2$. We can extend $\chi(0) = 0$.

Then

$$|E(\mathbb{F}_q)| = 1 + \sum_{x\in\mathbb{F}_q} (\chi(f(x)) + 1),$$

because the first 1 is the point at infinity, and $\chi(f(x))+1$ is $\#\{y \in \mathbb{F}_q \text{ with } y^2 = f(x)\}$. So

$$|E(\mathbb{F}_q)| = q + 1 + \underbrace{\sum_{x\in\mathbb{F}_q} \chi(f(x))}_{-a},$$

so Hasse really says

$$\Big|\sum_{x\in\mathbb{F}_q} \chi(f(x))\Big| \le 2\sqrt{q}.$$

We're summing up q integers which are usually equally equal to ± 1, but the absolute value of the sum is small. So there's lots of cancellation!

For comparison, consider random variables (specifically, fair coin flips) $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$. Then

$$\mathbb{E}\Big(\Big|\sum_{i=1}^n \varepsilon_i\Big|\Big) \sim \sqrt{\frac{2}{\pi}} \cdot \sqrt{n}$$

as $n \to \infty$. So Hasse is telling us $\chi\colon \mathbb{F}_q^\times \to \{\pm 1\}$ acts "randomly".

These character sums show up a lot in number theory. △

Consider a nice variety V over $\mathbb{F}_q$. The *zeta function* of V is

$$Z(V,T) = \exp\Big(\sum_{n=1}^\infty |V(\mathbb{F}_{q^n})| \cdot \frac{T^n}{n}\Big) \in \mathbb{Q}[\![T]\!].$$

Fact 3.15.2 (One of the three Weil conjectures). *Actually, $Z(V,T) \in \mathbb{Q}(T)$. (So $Z(V,T)$ can be captured in a finite amount of information.)*

This is due to Weil for curves; Dwork (1960) first proved this with p-adic functional analysis and later Grothendieck proved this with étale cohomology.

Theorem 3.15.3. *For an elliptic curve $E/\mathbb{F}_q$,*

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

Thus if you know $|E(\mathbb{F}_q)|$, you can find a, and then compute any $|E(\mathbb{F}_{q^n})|$.

Proof. Let φ^n be the q^n-th power Frobenius of E. Then

$$|E(\mathbb{F}_{q^n})| = \deg(1-\varphi^n) = (1-\varphi^n)(\widehat{1-\varphi^n}) = 1-\varphi^n-\hat{\varphi}^n+q^n.$$

So

$$\begin{aligned}\sum_{n=1}^{\infty}|E(\mathbb{F}_{q^n})| &= \sum_{n=1}^{\infty}\frac{T^n}{n}-\sum_{n=1}^{\infty}\varphi^n\frac{T^n}{n}-\sum_{n=1}^{\infty}\hat{\varphi}^n\frac{T^n}{n}+\sum_{n=1}^{\infty}q^n\frac{T^n}{n}\\ &= -\log(1-T)+\log(1-\varphi T)+\log(1-\hat{\varphi}T)-\log(1-qT)\\ &= \log\Big(\frac{(1-\varphi T)(1-\hat{\varphi}T)}{(1-T)(1-qT)}\Big),\end{aligned}$$

and exponentiating both sides gives

$$\begin{aligned}Z(E,T) &= \frac{(1-\varphi T)(1-\hat{\varphi}T)}{(1-T)(1-qT)}\\ &= \frac{1-aT+qT^2}{(1-T)(1-qT)}.\end{aligned}$$

□

3.16 April 7, 2020 (Finite fields)

Today we'll continue talking about elliptic curves over finite fields. Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The group $E(\mathbb{F}_q)$ is finite with cardinality

$$\#E(\mathbb{F}_q) = q + 1 - a_E.$$

The integer a_E is the *trace of Frobenius* of E. Recall that

$$|a_E| \leq 2\sqrt{q}.$$

(This is Hasse's bound, see Theorem 2.13.7.) Fix a prime $\ell \neq p$. We have a free $\mathbb{Z}_\ell$-module of rank 2 defined by

$$T_\ell E := \varprojlim_n E[\ell^n]$$

and a vector space over $\mathbb{Q}_\ell$ of dimension 2 defined by

$$V_\ell := T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Note that $\mathrm{Gal}_{\mathbb{F}_q}$ and $\mathrm{End}(E)$ both act on $V_\ell E$. Denote by $\varphi \in \mathrm{End}(E)$ the q-th power Frobenius. We saw that the characteristic polynomial of φ is given by $x^2 - a_E x + q$, i.e.

$$\begin{aligned} \mathrm{tr}(\varphi_\ell | V_\ell E) &= a_E \\ \det(\varphi_\ell | V_\ell E) &= q. \end{aligned}$$

Note that $\varphi_\ell \in \mathrm{Aut}(V_\ell E) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$ is semisimple (i.e. diagonalizable over $\overline{\mathbb{Q}}_\ell$).

Observe that representation $\mathrm{Gal}_{\mathbb{F}_q} \circlearrowright V_\ell E$ is determined up to isomorphism by a_E (given ℓ and q): this is because $\mathrm{Gal}_{\mathbb{F}_q}$ is topologically generated by $\mathrm{Frob}_q \colon x \mapsto x^q$, and Frob_q acts on $V_\ell E$ as φ_ℓ, and φ_ℓ is determined up to conjugation by a_E (and q).

As an example of the power of this observation, we have:

Theorem 3.16.1. *For E, E' over $\mathbb{F}_q$, E and E' are isogenous over $\mathbb{F}_q$ if and only if $a_E = a_{E'}$ (or, equivalently, if and only if $\#E(\mathbb{F}_q) = \#E'(F_q)$).*

Proof. The forwards direction follows from the fact that an isogeny $f \colon E \to E'$ is an isogeny over $\mathbb{F}_q$ induces a homomorphism $f_\ell \colon V_\ell E \to V_\ell E'$ of $\mathbb{Q}_\ell[\mathrm{Gal}_{\mathbb{F}_q}]$-modules which is an isomorphism because $\ker f$ is finite. The isomorphism $V_\ell E \cong V_\ell E'$ implies

$$a_E = \mathrm{tr}(\mathrm{Frob}_q | V_\ell E) = \mathrm{tr}(\mathrm{Frob}_q | V_\ell E') = a_{E'}.$$

Let's now prove the backwards direction. Suppose $a_E = a_{E'}$, so $V_\ell E \cong V_\ell E'$ are isomorphic representations of $\mathrm{Gal}_{\mathbb{F}_q}$. In particular,

$$\mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_{\mathbb{F}_q}]}(V_\ell E, V_\ell E') \neq 0.$$

Tate (Theorem 2.12.6) says

$$\mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_{\mathbb{F}_q}]}(V_\ell E, V_\ell E') = \mathrm{Hom}_{\mathbb{F}_q}(E, E') \otimes \mathbb{Q}_\ell,$$

and this implies $\mathrm{Hom}_{\mathbb{F}_q}(E, E') \neq 0$. □

Recall that

$$E \text{ is } \begin{cases} \text{supersingular} & \text{if } E[p^n] = \{0\} \text{ for all } n \geq 1 \\ \text{ordinary} & \text{if } E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \text{ for all } n \geq 1 \end{cases}$$

We showed that E is ordinary if and only if $\mathrm{End}E$ is commutative (Theorem 2.15.1).

Proposition 3.16.2. *E is ordinary if and only if $p \nmid a_E$.*

Proof. Let $\varphi\colon E \to E$ be the q-th power Frobenius. We have $\hat{\varphi} \in \mathrm{End}E$, and $a_E = \varphi + \hat{\varphi} \in \mathrm{End}(E)$, and $q = \varphi \cdot \hat{\varphi} = \hat{\varphi} \cdot \varphi$. Also,

$$\#E[q] = \deg_s [q] = \deg_s \varphi \cdot \hat{\varphi} = \deg_s \hat{\varphi},$$

because $\deg_s \varphi = 1$. Since $\#E[q]$ is equal to 1 or q, $\deg_s \hat{\varphi}$ is also equal to 1 or q. Note that

$$\begin{aligned} E \text{ is ordinary} &\iff \hat{\varphi} \text{ is separable} \\ &\iff [a_e] \text{ is separable} \\ &\iff p \nmid a_E. \end{aligned}$$

(The second equivalence is due to the fact that for ω the invariant differential,

$$\begin{aligned} \hat{\varphi}^* \omega &= (a_E - \varphi)^* \omega \\ &= a_E^* \omega - \varphi^* \omega \\ &= a_E^* \omega, \end{aligned}$$

because φ is not separable. □

Which a_E occur? Well, there is an injective map

$$\{E/\mathbb{F}_q \text{ up to isogeny over } \mathbb{F}_q\} \hookrightarrow \{a \in \mathbb{Z} \colon |a_E| \leq 2\sqrt{q}\}$$

sending E to a_E. The image can be described; it's surjective if $q = p$. The image contains all a such that $p \nmid a$.

How does one compute a_E? One way is to count $E(\mathbb{F}_q)$. Unfortunately, this is not always practical; for example in cryptography $q \cong 2^{256}$ is typical.

In 1985, Schoof developed an algorithm to compute a_E that is polynomial time in $\log q$ (see [Silverman, XI.3]).

Let's sketch an algorithm. Assume $p \neq 2, 3$ and pick $E/\mathbb{F}_q : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{F}_q$. The idea is to compute $a_E \pmod{\ell}$ for many small primes ℓ.

If we know $a_e \pmod{\ell_i}$ with $1 \leq i \leq r$, the Chinese remainder theorem gives us $a_e \pmod{\prod \ell_i}$. Now if $\prod_{i=1}^r \ell_i > 4\sqrt{q}$, the number $a_E \mod \prod \ell_i$ determines a_E, because the Hasse bound says $|a_E| \leq 2\sqrt{q}$.

This is very efficient: for $q \leq 2^{256}$, we have $\prod_{\ell \leq 103} \ell > 4\sqrt{q}$.

So the question is how to compute $a_E \pmod{\ell}$. Let's assume $\ell \nmid 2p$. For $(x, y) \in E \setminus \{0\}$, note that

$$(x^{q^2}, y^{q^2}) - [a_E](x^q, y^q) + [q](x, y) = 0. \tag{3}$$

(This is because $\varphi^2 - a_E \varphi + q = 0$.)

To compute $a_E \pmod{\ell}$, we need only show that Equation (3) holds for all $P \in E[\ell] \setminus \{0\}$.

Fact 3.16.3. *There is a* division polynomial $\psi_\ell(x) \in \mathbb{F}_q[x]$ *of degree* $(\ell^2 - 1)/2$ *such that for any* $(x, y) \in E \setminus \{0\}$, *we have*

$$(x, y) \in E[\ell] \iff \psi_\ell(x) = 0.$$

The polynomial ψ_ℓ *can be computed recursively (see [Silverman, Ex. 3.7]).*

For example, $\psi_3(x) = 3x^4 + 6ax^2 + 12bx - a^2$.

Consider the ring

$$\mathcal{R} = \mathbb{F}_q[x, y]/\langle \psi_\ell(x), y^2 - (x^3 + ax + b) \rangle$$

and note that $\mathrm{Hom}_{\mathbb{F}_q}(\mathcal{R}, \overline{\mathbb{F}}_q) \leftrightarrow E[\ell] \setminus \{0\}$. (Actually, $\mathrm{Spec}\, \mathcal{R} = E[\ell] \setminus \{0\}$.)

Any element in $\mathcal{R}$ is of the form $f(x) + yg(x)$, where $f(x), g(x) \in \mathbb{F}_q(x)$ and $\deg f, \deg g < \frac{\ell^2 - 1}{2}$. It follows that $\dim_{\mathbb{F}_\ell} \mathcal{R} = \ell^2 - 1$.

We can compute (x^{q^2}, y^{q^2}) and (x^q, y^q) in $\mathcal{R}$, and we can compute $[q](x, y)$ in $\mathcal{R}$ even when q is large, because it depends only on $q \pmod{\ell}$. (We may use the group law of E; the denominators that arise will be units in $\mathcal{R}$.)

If $(x^{q^2}, y^{q^2}) = [-q](x, y)$ in $\mathcal{R}$, then $a_E \equiv 0 \pmod{\ell}$. Otherwise, $a_E \not\equiv 0 \pmod{\ell}$ and $[a_E](x^q, y^q) = (x^{q^2}, y^{q^2}) + [q](x, y)$. We can now find $a_E \pmod{\ell}$ by just checking the $\ell - 1$ possibilities.

More on Zeta functions

We begin with some topology. Let $f\colon M \to M$ be a continuous map with M a compact real manifold. Define the *Lefschetz number*

$$\Lambda_f := \sum_{i\geq 0}(-1)^i \operatorname{tr}(f^*|H^i(M,\mathbb{Q})).$$

The Lefschetz fixed point theorem says that if $\Lambda_f \neq 0$, then f has a fixed point. Moreover, if f has finitely many fixed points, then Λ_f is the number of fixed points of f, counted with a suitable multiplicity.

Now consider a nice variety $V/\mathbb{F}_q$ of dimension d, and let $\varphi\colon V \to V$ be the q-th power Frobenius. The fixed points are $V(\mathbb{F}_q)$.

Fix $\ell \nmid q$. Grothendieck and Artin showed that there are "étale cohomology groups" $H^i_{\text{ét}}(V,\mathbb{Q}_\ell)$ which are finite dimensional vector spaces over $\mathbb{Q}_\ell$, such that

$$\#V(\mathbb{F}_q) = \sum_{i=0}^{2d}(-1)^i \operatorname{tr}(\varphi^*|H^i_{\text{ét}}(V,\mathbb{Q}_\ell))$$

and

$$\#V(\mathbb{F}_{q^n}) = \sum_{i=0}^{2d}(-1)^i \operatorname{tr}((\varphi^*)^n|H^i_{\text{ét}}(V,\mathbb{Q}_\ell)).$$

Exercise : Denote by

$$Z(V,T) := \exp\Big(\sum_{n=1}^{\infty}\#V(\mathbb{F}_{q^n})\frac{T^n}{n}\Big) \in \mathbb{Q}[\![T]\!].$$

Then

$$Z(V,T) = \frac{P_1(T)P_3(T)\dots P_{2d-1}(T)}{P_0(T)P_2(T)\dots P_{2d}(T)},$$

where

$$P_i(T) = \det(I - T\cdot\varphi^*|H^i_{\text{ét}}(V,\mathbb{Q}_\ell)).$$

Deligne showed that the eigenvalues of $\varphi^* \circlearrowright H^i_{\text{ét}}(V,\mathbb{Q}_\ell)$ under any $\overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$ all have absolute value $q^{i/2}$. With this result,

Exercise : Show $P_i(T) \in \mathbb{Z}[T]$.

Let's consider the case of a nice curve $C/\mathbb{F}_q$ of genus g. We have

$H^0_{\text{ét}}(C,\mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$	φ^* acts trivially
$H^1_{\text{ét}}(C,\mathbb{Q}_\ell)$	$\dim_{\mathbb{Q}_\ell} = 2g$
$H^2_{\text{ét}}(C,\mathbb{Q}_\ell) \cong \mathbb{Q}_\ell$	φ^* acts by multiplication by q

It follows that

$$\#C(\mathbb{F}_q) = 1 - \operatorname{tr}(\varphi^*|H^1_{\text{ét}}(C,\mathbb{Q}_\ell)) + q,$$

where the middle term consists of $2g$ eigenvalues with absolute value $q^{1/2}$. It follows that

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

Exercise : If C has genus 1, then $C(\mathbb{F}_q) \neq \emptyset$.

It turns out that $H^1_{\text{ét}}(E,\mathbb{Q}_\ell)$ is "dual" in some sense to $V_\ell E$. (Specifically, $V_\ell E$ is a homological object.)

3.17 Apr 9, 2020 (Complex numbers)

Fix an ellptic curve E over $\mathbb{C}$. We already know a lot since $\mathbb{C}$ is algebraically closed. We also have topology and analysis:

$$E^{\text{an}} \stackrel{\text{def}}{=} E(\mathbb{C})$$

which is a connected compact Riemann surface (i.e. a complex manifold of dimension 1). Since E has an algebraic group law, E^{an} is a complex Lie group of dimension 1. (A complex Lie group is one where the group operations are holomorphic.)

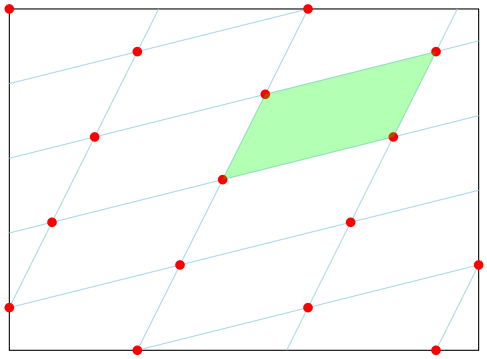
More generally, we have an equivalence of categories

$$\{\text{nice curves over } \mathbb{C} + \text{morphisms}\} \to \{\text{connected compact Riemann surfaces + holomorphic maps}\}$$
$$C \mapsto C^{\text{an}}.$$

Theorems of this flavour are often called "GAGA" (after a paper of Serre). As an example of a GAGA-type result, the morphisms $C \to \mathbb{P}^1_{\mathbb{C}}$ that are not constant equal to ∞ can be identified with the field of meromorphic functions on C^{an}. For $P \in C$ and $f \in \mathbb{C}(C)$, the number $\text{ord}_P(f)$ is also the order of vanishing of f at P in the sense of complex analysis.

We also have an agreement on differentials, and in particular C and C^{an} have the same genus.

Now consider a lattice $\Lambda \subseteq \mathbb{C}$, which is a discrete subgroup of rank 2, as below:



Now $\mathbb{C}/\Lambda$ is a connected compact Riemann surface of genus 1. It's also a Lie group, using addition from $\mathbb{C}$.

Consider lattices Λ, Λ' of $\mathbb{C}$. GIven $\alpha \in \mathbb{C}$ satisfying $\alpha\Lambda \subseteq \Lambda'$, multiplication by α gives a holomorphic map

$$\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$$
$$z + \Lambda \mapsto \alpha z + \Lambda'.$$

Conversely, we have

Lemma 3.17.1. *Let $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be holomorphic and $f(0) = 0$. Then f arises from α as above. In particular, f is a homomorphism of groups.*

Proof. We have covering maps $\mathbb{C} \twoheadrightarrow \mathbb{C}/\Lambda$ and $\mathbb{C} \twoheadrightarrow \mathbb{C}/\Lambda'$, and since $\mathbb{C}$ is simply connected there exists a lift, i.e. a unique map $F : \mathbb{C} \to \mathbb{C}$ such that $F(0) = 0$ and the diagram

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{F} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda' \end{array}$$

commutes. Note that F is holomorphic.

Thus for any $w \in \Lambda$, we have $F(z+w) - F(z) \in \Lambda'$, so $F(z+w) - F(z)$ is constant. Thus $F'(z+w) = F'(z)$ for all $w \in \Omega$. So $F' : \mathbb{C} \to \mathbb{C}$ is holomorphic and bounded, which means $F'(z) = \alpha \in \mathbb{C}$. It follows that $F(z) = \alpha z$, since $F(0) = 0$. □

Thus we see that

$$\mathrm{Hom}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') = \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subseteq \Lambda'\}.$$

(The left side consists of homomorphisms of complex Lie groups, or equivalently of holomorphic maps sending 0 to 0.)

In particular, $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ if and only if $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$.

Theorem 3.17.2. *For an elliptic curve $E/\mathbb{C}$, there is a lattice $\Lambda \subseteq \mathbb{C}$ such that $E^{\mathrm{an}} \cong \mathbb{C}/\Lambda$ as complex Lie groups.*

Proof ideas.

- Lie theory: consider the Lie group $G = E^{\mathrm{an}}$ and let $\mathfrak{g}$ be the Lie algebra of G. It's the tangent space of G at 0, with pairing. We have a holomorphic map $\exp \colon \mathfrak{g} \to G = E^{\mathrm{an}}$ (for $v \in \mathfrak{g}$, there exists a unique homomorphism of Lie groups $\gamma_v \colon \mathbb{C} \to G$ such that $\gamma_v(0) = 0$ and $(d\gamma_v)_0 \colon \mathbb{C} \to \mathfrak{g}$ is $t \mapsto tv$. Then $\exp(v) = \gamma_v(1)$.).

  The map $\exp$ satisfies many nice properties: $d(\exp)_0 = \mathrm{id}_{\mathfrak{g}}$, so $\exp$ is locally a homeomorphism near 0. Also, $\exp$ is a homomorphism of groups, so $\Lambda = \ker(\exp) \subseteq \mathfrak{g} \cong \mathbb{C}$ is discrete. Finally, $\exp$ is surjective, since the image is open and G is compact. It follows that $\exp$ gives an isomorphism $\mathfrak{g}/\Lambda \xrightarrow{\sim} E^{\mathrm{an}}$.

- Alternatively, let $V = \{\text{holomorphic differentials on } E\} \cong \mathbb{C}$. We get an injection

$$\begin{aligned} H_1(E^{\mathrm{an}}, \mathbb{Z}) &\hookrightarrow V^* \\ \gamma &\mapsto (\omega \mapsto \int_\gamma \omega). \end{aligned}$$

  Let Λ be the image of H_1 under this injection. We get a map

$$\begin{aligned} E^{\mathrm{an}} &\to V^*/\Lambda \\ P &\mapsto (\omega \mapsto \int_0^P \omega + \Lambda) \end{aligned}$$

  that turns out to be an isomorphism of Lie groups.

□

Remark 3.17.3. For a nice curve $C/\mathbb{C}$ of genus g, let $X \to C^{\mathrm{an}}$ be the universal cover (X is also a Riemann surface). The universal cover X depends on g according to the following table:

g	0	1	≥ 2
X	$\mathbb{P}^1(\mathbb{C})$	$\mathbb{C}$	$\mathbb{H}$,
$\chi = 2 - 2g$	> 0	0	< 0

where $\mathbb{H}$ is the complex upper half plane. △

Let's now explicitly construct an elliptic curve given a lattice Λ. By Riemann-Roch, we showed that there are $x, y \in \mathbb{C}(\Lambda)$ such that $\mathrm{div}(x) + 2(0) \geq 0$, $\mathrm{ord}_0\, x = -2$, $\mathrm{div}(y) + 3(0) \geq 0$, and $\mathrm{ord}_0\, y = -3$. Also, $\mathbb{C}(\Lambda) = \mathbb{C}(x, y)$, with x and y satisfying a Weierstrass relation.

We will explicitly construct x and y. The Weierstrass $\wp$-function (relative to Λ) is

$$\wp(z) = \wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \Big(\frac{1}{(z-w)^2} - \frac{1}{w^2} \Big).$$

Claim 3.17.4. *The function $\wp(z)$ is holomorphic on $\mathbb{C} \setminus \Lambda$.*

Proof idea. We need to check absolute and uniform convergence on compact subsets of $\mathbb{C} \setminus \Lambda$. The key is to observe

$$\Big| \frac{1}{(z-w)^2} - \frac{1}{w^2} \Big| \leq \frac{10}{|w|^3}|z| \quad \text{if } |w| > 2|z|,$$

noting that

$$\sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{|w|^k} \text{ converges for } k \geq 3.$$

□

More generally, define

$$G_{2k}(\Lambda) \stackrel{\text{def}}{=} \sum_{\substack{w\in\Lambda\\ w\neq 0}} \frac{1}{w^{2k}} \in \mathbb{C} \qquad \text{for } k \geq 2.$$

Exercise : Near 0, we have

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\Lambda) z^{2k}.$$

Lemma 3.17.5. *We have $\wp \in \mathbb{C}(\Lambda)$, i.e., $\wp(z+w) = \wp(z)$ for $w \in \Lambda$.*

Proof. We may differentiate term by term, so

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

Note also that $\wp'(z+w) = \wp'(z)$ for all $w \in \Lambda$. Then

$$\wp(z+w) = \wp(z) + C_w.$$

For $z = -w/2$, we have $\wp(w/2) = \wp(-w/2) + C_w$, but since $\wp$ is even we see that $C_w = 0$. □

We've found a function $\wp \in \mathbb{C}(\Lambda)$ that is holomorphic on $\mathbb{C}/\Lambda$ except at 0, where $\operatorname{ord}_0 \wp = -2$, as well as a function $\wp' \in \mathbb{C}(\Lambda)$ that is holomorphic except at 0, where $\operatorname{ord}_0 \wp' = -3$. It follows that $\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$.

The functions $\wp$ and $\wp'$ should satisfy a Weierstrass equation, ie. a linear relation in 1, x, y, x^2, xy, x^3, y^2. **Exercise :** Show that

$$\begin{aligned} y^2 = \wp'(z)^2 &= 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \dots \\ x^3 = \wp(z)^3 &= z^{-6} + 9G_4 z^{-2} + 15G_6 + \dots \\ x = \wp(z) &= z^{-2} + 3G_4 z^2 + \dots \end{aligned}$$

and hence

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

where $g_2(\Lambda) = 60G_4$ and $g_3(\Lambda) = 140G_6$. (The idea is to check that $y^2 - (4x^3 - g_2(\Lambda)x - g_3(\Lambda))$ is holomorphic on $\mathbb{C}/\Lambda$ and equals 0 at 0.)

Finally, we may define the map

$$\begin{aligned} \varphi\colon \mathbb{C}/\Lambda &\to E^{\text{an}} \\ z+\Lambda &\mapsto [\wp(z), \wp'(z), 1] \\ 0+\Lambda &\mapsto 0 = \mathcal{O} \end{aligned}$$

This is an isomorphism of complex Lie groups, and we obtain $\mathbb{C}/\Lambda \cong E^{\text{an}}$.

Summing everything up, we have equivalences between the category of elliptic curves over $\mathbb{C}$ with morphisms of varieties, the category of elliptic curves over $\mathbb{C}$ with homomorphisms of Lie groups, and the category of Lattices $\Lambda \subseteq \mathbb{C}$ with morphisms consisting of $\operatorname{Morp}(\Lambda, \Lambda') = \{\alpha \in \mathbb{C}\colon \alpha\Lambda \subseteq \Lambda'\}$. On the object level, the equivalence between the first two categories is given by $C \mapsto C^{\text{an}}$, whereas the equivalence between the latter two categories is given by $\mathbb{C}/\Lambda \leftarrow\!\shortmid \Lambda$.

Fix an imaginary quadratic field $K \subseteq \mathbb{C}$, and let R be an order of K, so $R \subseteq \mathcal{O}_K$ is a subring of finite index. Note that $R \subseteq \mathbb{C}$ is a lattice, and $\operatorname{Morp}(R, R) = \{\alpha \in \mathbb{C}\colon \alpha R \subseteq R\} = R$. It follows that $\operatorname{End}(\mathbb{C}/R) \cong R$, and hence there exists an elliptic curve $E/\mathbb{C}$ with $\operatorname{End}(E) \cong R$. Try proving this algebraically!

(Recall that the endomorphism rings of $E/\mathbb{C}$ are either $\mathbb{Z}$ or such an order.)

3.18 Apr 14, 2020 (Complex numbers)

Let $E/\mathbb{C}$ be an elliptic curve, and let $E^{\text{an}} = E(\mathbb{C})$. We saw last time that there is a lattice $\Lambda \subseteq \mathbb{C}$ such that $E^{\text{an}} \cong \mathbb{C}/\Lambda$ as Lie groups. The lattice is unique upt o scaling by an $\alpha \in \mathbb{C}^\times$.

Let $\Lambda \subseteq \mathbb{C}$ be a lattice. There is an elliptic curve $E/\mathbb{C}$ such that $E^{\text{an}} \cong \mathbb{C}/\Lambda$. Moreover,

$$E/\mathbb{C} : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

where

$$g_2(\Lambda) = 60 \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^4}, \qquad g_3(\Lambda) = 140 \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^6}.$$

For E, E' elliptic curves over $\mathbb{C}$, we have $E^{\text{an}} \cong \mathbb{C}/\Lambda$ and $(E')^{\text{an}} \cong \mathbb{C}/\Lambda'$ for some lattices Λ, Λ'. Then

$$\text{Hom}(E, E') \cong \text{Hom}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') \cong \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subseteq \Lambda'\}.$$

Altogether, we saw three equivalences of categories last time, between elliptic curves with morphisms of varieties, elliptic curves with morphisms of Lie groups, and lattices with morphisms given by $\{\alpha \in \mathbb{C} \colon \alpha\Lambda \subseteq \Lambda'\}$.

Fix an imaginary quadratic field $K/\mathbb{Q}$, so $K \subseteq \mathbb{C}$. We have the ring of integers $\mathcal{O}_K \subseteq \mathbb{C}$; it is a lattice and is the maximal order of K. Let's classify $E/\mathbb{C}$ with $\text{End}(E) \cong \mathcal{O}_K$.

Fix $\Lambda \subseteq \mathbb{C}$ with $\text{End}(\mathbb{C}/\Lambda) = \mathcal{O}_K$, i.e. $\alpha\Lambda \subseteq \Lambda$ for all $\alpha \in \mathcal{O}_K$. We say E has *complex multiplication* (CM) by $\mathcal{O}_K$. We can scale Λ so that $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. We have $\Lambda \subseteq \mathcal{O}_K$, since $\alpha \cdot 1 \in \Lambda$ for all $\alpha \in \mathcal{O}_K$. It follows that Λ is an ideal of $\mathcal{O}_K$.

Conversely, any nonzero ideal $I \subseteq \mathcal{O}_K$ is a lattice in $\mathbb{C}$ and $\text{End}(\mathbb{C}/I) = \mathcal{O}_K$. This motivates the following definition:

Definition 3.18.1. Let $\text{Cl}(\mathcal{O}_K)$ be the set of equivalence classes of non-zero ideals of $\mathcal{O}_K$, where $I_1 \sim I_2$ if $I_2 = \alpha I_1$ for some $\alpha \in K^\times$. This is called the *class group* of $\mathcal{O}_K$ (although as of now, this is a set). △

We let $\text{Ell}(\mathcal{O}_K)$ denote the set of elliptic curves $E/\mathbb{C}$ with $\text{End}(E) \cong \mathcal{O}_K$. Then

Theorem 3.18.2. *We have a bijection*

$$\begin{aligned} \text{Cl}(\mathcal{O}_K) &\leftrightarrow \text{Ell}(\mathcal{O}_K) \\ [I] &\mapsto \mathbb{C}/I. \end{aligned}$$

Fact 3.18.3.

- *We can* $\text{Cl}(\mathcal{O}_K)$ *into a group, by setting* $[I_1] \cdot [I_2] := [I_1 I_2]$.
- *Furthermore,* $\text{Cl}(\mathcal{O}_K)$ *is a finite group; it's size is computable. (See Corollary 4.20 in Mehrle's 6370 notes)*

Corollary 3.18.4. $\text{Ell}(\mathcal{O}_K)$ *is finite with cardinality* $\#\text{Cl}(\mathcal{O}_K)$.

Take any $[E] \in \text{Ell}(\mathcal{O}_K)$. For $\sigma \in \text{Aut}(\mathbb{C})$, we have $[E^\sigma] \in \text{Ell}(\mathcal{O}_K)$, as

$$E : y^2 = x^3 + ax + b \rightsquigarrow E^\sigma : y^2 = x^3 + \sigma(a)x + \sigma(b).$$

Thus we see $j(E^\sigma) = \sigma(j(E))$.

We can define the *Hilbert class polynomial*

$$H_{\mathcal{O}_K}(x) := \prod_{[E] \in \text{Ell}(\mathcal{O}_K)} (x - j(E)) \in \mathbb{C}[x].$$

Because the coefficients are fixed by all of $\text{Aut}(\mathbb{C})$, it follows that

$$H_{\mathcal{O}_K}(x) \in \mathbb{Q}[x].$$

In fact,

Fact 3.18.5. *We have* $H_{\mathcal{O}_K}(x) \in \mathbb{Z}[x]$.

Thus we can compute it by numerically approximating $H_{\mathcal{O}_K}$ and then rounding.

Example 3.18.6. Let $K = \mathbb{Q}(\sqrt{-7})$, so $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. We have $\#\mathrm{Cl}(\mathcal{O}_K) = 1$. It follows that

$$H_{\mathcal{O}_K}(x) = x - j(\mathbb{C}/\mathcal{O}_K) = x + 3^3 \cdot 5^3.$$

So up to isomorphism, there is only one $E/\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}_K$; it has j-invariant $j(E) = -3^3 \cdot 5^3$. △

Example 3.18.7. Let $K = \mathbb{Q}(\sqrt{-5})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Then $\mathrm{Cl}(\mathcal{O}_K) = \{[\mathcal{O}_K], [\mathbb{Z} \cdot 2 + \mathbb{Z}(1 + \sqrt{-5})]\}$. Then

$$\begin{aligned} H_{\mathcal{O}_K}(x) &= (x - 1264538.909...)(x + 538.909...) \\ &= x^2 - 1264000x - 68147200. \end{aligned}$$

So $E/\mathbb{C}$ has endomorphism ring $\mathcal{O}_K$ if and only if $j(E) \in \{63200 \pm 282880\sqrt{-5}\}$. △

Fact 3.18.8. *Let K be imaginary quadratic. The field $K^{(1)} := K(j(\mathbb{C}/\mathcal{O}_K))$ is an unramified extension of K that is Galois with Galois group $\mathrm{Cl}(\mathcal{O}_K)$. It is the maximal unramified abelian extension of K.*

Let's give some examples of the Lefschetz principle, which loosely says we can reduce results to those over $\mathbb{C}$:

Proposition 3.18.9 (Special case of Corollary 2.11.3)**.** *Let E/K be an elliptic curve with* $\operatorname{char} K = 0$*. Then $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ for all $m \geq 1$.*

Proof. We know $E[m] = \ker[m]$ is finite. So without loss of generality, we may replace K with a finitely generated field such that E is defined over K with $E[m] \subseteq E(K)$. Thus, there is an embedding $K \hookrightarrow \mathbb{C}$, so we can now assume $K = \mathbb{C}$. But now $E^{\mathrm{an}} \cong \mathbb{C}/\Lambda$ and the torsion points are just

$$E[m] \cong (\mathbb{C}/\Lambda)[m] = (\tfrac{1}{m}\Lambda)/\Lambda \cong \Lambda/m\Lambda \cong (\mathbb{Z}/m\mathbb{Z})^2.$$ □

Proposition 3.18.10. *Let $\varphi, \psi \colon E \to E'$ be homomorphisms of elliptic curves over K with* $\operatorname{char} K = 0$*. Then*

$$\varphi + \psi)^* = \varphi^* + \psi^*.$$

Proof sketch. Without loss of generality, we can set $K = \mathbb{C}$. Then $E^{\mathrm{an}} = \mathbb{C}/\Lambda$ and $(E')^{\mathrm{an}} \cong \mathbb{C}/\Lambda'$. Then

$$\varphi \colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$$

is given by multiplication by $\alpha \in \mathbb{C}^\times$ with $\alpha\Lambda \subseteq \Lambda'$. Then

$$\deg \varphi = \#\ker \varphi = \#(\alpha^{-1}\Lambda')/\Lambda = [\Lambda' : \alpha\Lambda].$$

It follows that $[\Lambda' : \alpha\Lambda] \cdot \Lambda' \subseteq \alpha\Lambda$, and

$$\deg \varphi \cdot \Lambda' \subseteq \alpha\Lambda, \quad \text{i.e.} \quad \frac{\deg \varphi}{\alpha} \cdot \lambda' \subseteq \Lambda.$$

Note that $\varphi^* \colon \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$ is multiplication by $\deg \varphi/\alpha$. We can now choose bases for Λ and Λ' with the same orientation in $\mathbb{C}$. Then φ gives rise to a map $\Lambda \to \Lambda'$ given by multiplication by α. This map is given by a matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z})$$

with respect to the chosen bases. We have $\det A = [\Lambda' : \alpha\Lambda] = \deg \varphi$, and so φ^* is given by the matrix

$$\mathrm{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Finally, $\mathrm{adj}(A + B) = \mathrm{adj}(A) + \mathrm{adj}(B)$ gives $(\varphi + \psi)^* = \varphi^* + \psi^*$. □

We remark that the observation $\mathrm{adj}(\mathrm{adj}(A)) = A$ and $\mathrm{adj}(AB) = \mathrm{adj}(B)\mathrm{adj}(A)$ gives other familiar properties of dual morphisms.

Let's talk briefly about modular curves. Recall that we had

$$\{E/\mathbb{C} \text{ up to isomorphism}\} \leftrightarrow \{\text{lattice } \Lambda \subseteq \mathbb{C} \text{ up to scaling}\}.$$

We can give the right side a geometric structure in the following way. Given Λ, we can scale so that $\Lambda = \mathbb{Z}+\mathbb{Z}\tau$ with $\tau \in \mathbb{H}$ in the upper half plane. Note that τ is not unique: take another basis of Λ given by $\{a\tau+b, c\tau+d\}$ with

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}).$$

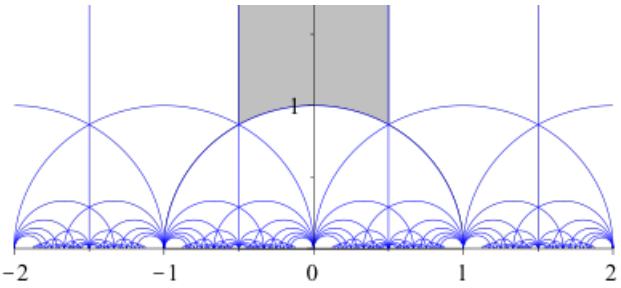
It follows that

$$\begin{aligned} \Lambda &= \mathbb{Z}(a\tau+b) + \mathbb{Z}(c\tau+d) \\ &= (c\tau+d)\cdot\left(\mathbb{Z} + \mathbb{Z}\cdot\frac{a\tau+b}{c\tau+d}\right). \end{aligned}$$

One can check that $\frac{a\tau+b}{c\tau+d} \in \mathbb{H}$ for $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Thus we have an action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ sending τ to $\frac{a\tau+b}{c\tau+d}$. In particular, we have

$$\{E/\mathbb{C} \text{ up to isomorphism}\} \leftrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash H$$

A fundamental domain for the orbits of $\mathrm{SL}_2(\mathbb{Z})\backslash H$ is given by



The portion of the boundary to the right of $i \in \mathbb{H}$ is identified to the portion of the boundary to the left of $i \in \mathbb{H}$, via the identification $a+bi \sim -a+bi$. For $F = \{z \in \mathbb{H} \colon |z| \geq 1, |\mathrm{Im}(z)| \leq 1/2\}$, the map $F \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ is surjective and injective away from the boundary. The points $\tau = e^{2\pi i/6} = \zeta_6$ and i are special: the elliptic curves $\mathbb{C}/\mathbb{Z}[\zeta_6]$ and $\mathbb{C}/\mathbb{Z}[i]$ have j-invariant 0 and 1728. Given any $E/\mathbb{C}$ with $\mathrm{Aut}(E) \ncong \mathbb{Z}/2\mathbb{Z}$, we have maps

$$\begin{array}{ccc} \mathbb{H} & & \\ \downarrow & \searrow^{j} & \\ \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} & \xrightarrow[\tau\mapsto j(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau))]{} & \mathbb{C} \end{array}$$

The map $j \colon \mathbb{H} \twoheadrightarrow \mathbb{C}$ is holomorphic with $j(A\tau) = j(\tau)$ for $A \in \mathrm{SL}_2(\mathbb{Z})$. In particular, for $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ we have $j(\tau+1) = j(\tau)$. We have

Fact 3.18.11. *We have $j(\tau) = J(e^{2\pi i\tau})$, where*

$$\begin{aligned} J(q) &= \frac{1}{q}\left(1 + 240\sum_{m=1}^{\infty} m^3 \frac{q^m}{1-q^m}\right)\prod_{n=1}^{\infty}(1-q^n)^{24} \\ &= \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots \in \mathbb{Z}((q)). \end{aligned}$$

Observation 3.18.12 (in memory of Conway)**.** McKay observed that $196884 = 196883 + 1$. It turns out that 196883 is the smallest degree of a nontrivial representation of the Monster simple group. To learn more, you can look up "Monstrous Moonshine". $\triangle$

Let $N \geq 1$. We define

$$\Gamma_0(N) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \colon A \cong \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\}.$$

Then $\Gamma_0(N)\backslash\mathbb{H}$ parametrizes elliptic curves over $\mathbb{C}$ with a cyclic subgroup $C \subseteq E$ of order N. The dictionary is given by sending

$$\tau \mapsto \left(\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)), \left\langle \frac{1}{N} + (\mathbb{Z} + \mathbb{Z}\tau \right\rangle \right).$$

This is interesting because if E and E', then they are isogenous by an isogeny with cyclic kernel.

You can find models over $\mathbb{Q}$ for $\Gamma_0(N)\backslash\mathbb{H}$.

Next time we'll talk about local fields and reducing equations modulo a maximal ideal.

3.19 Apr 16, 2020 (Local fields)

We first set some notation. Let R be a complete discrete valuation ring, i.e.R is a PID with a unique nonzero maximal ideal that is equal to its completion with respect to $\mathfrak{m}$. We set $\mathfrak{m}$ to be the maximal ideal of R, and π a uniformizer of R, so $\mathfrak{m} = R\pi$. We set $k = R/\mathfrak{m}$ to be the residue field, and K to be the quotient field of R. We call K a local field. (We are following Silverman, so we assume k and K are perfect.)

Associated to R is a *valuation* $v\colon K^\times \twoheadrightarrow \mathbb{Z}$ such that $a = \pi^{v(a)}u$ with $u \in R^\times$. We manually set $v(0) = +\infty$.

The completion of R (with respect to $\mathfrak{m}$) is

$$\hat{R} \stackrel{\text{def}}{=} \varprojlim_n R/\mathfrak{m}^n,$$

and completeness of R amounts to saying that $R \to \hat{R}$ is an isomorphism. We fix $c > 1$ and define $|\cdot|_v\colon K \to \mathbb{R}_{\geq 0}$ by $|a|_v = c^{-v(a)}$. This is an *absolute value*. The completeness of R is equivalent to the fact that every Cauchy sequence in K, using $|\cdot|_v$ is convergent.

Example 3.19.1. Let $R = \mathbb{Z}_p$; then $K = \mathbb{Q}_p$, $\mathfrak{m} = p\mathbb{Z}_p$, $k = \mathbb{F}_p$, and $\pi = p$. △

Example 3.19.2. Let $R = \mathbb{C}[\![x]\!]$; then $K = \mathbb{C}((x))$, $\pi = x$ and $k = \mathbb{C}$. △

Example 3.19.3. Let K'/K be a finite extension and let R' be the integral closure of R in K'. Then R' is also a complete DVR and K' is another local field. Then $k' = R'/\mathfrak{m}'$ is a finite extension of $k = R/\mathfrak{m}$. △

For today, finite extensions $K/\mathbb{Q}_p$ are the key example to think about.

Let us fix an elliptic curve E/K and choose a model

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

with $a_i \in R$, thus $E \subseteq \mathbb{P}^2_K$. The *reduction* of E is denoted $\widetilde{E} \subseteq \mathbb{P}^2_k$ and is the projective curve defined by

$$y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x + \overline{a_4}x + \overline{a_6}$$

where $\overline{a_i}$ is the iamge of a_i in $k = R/\mathfrak{m}$.

Note that $\widetilde{E}$ depends on the choice of a_i:

Example 3.19.4. Let $p \neq 2$; note that $y^2 = x^3 + x$ and $y^2 = x^3 + p^4x$ gives isomorphic curves over $\mathbb{Q}_p$. Their reductions mod p are $y^2 = x^3 + x$ and $y^2 = x^3$ respectively; the first defines an elliptic curve $\widetilde{E} \subseteq \mathbb{P}^1_{\mathbb{F}_p}$, whereas the second defines a singular curve $\widetilde{E} \subseteq \mathbb{P}^1_{\mathbb{F}_p}$ of genus 0.

The feeling is that $y^2 = x^3 + x$, with discriminant $\Delta = 64$, should be a "better" model than $y^2 = x^3 + p^4x$, with discriminant $\Delta = 64p^{12}$. △

Let's recall the discriminant $\Delta \in R$, $\Delta \neq 0$ of an elliptic curve. The model with $a_i \in R$ is a *minimal (Weierstrass) model* if $v(\Delta) \geq 0$ is minimal amongst all models for E/K. There's an algorithm to compute this Δ.

Suppose (x, y) and (x', y') are coordinates of two minimal models of E/K. We have

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned} \tag{$*$}$$

for $u \in K^\times$ and $r, s, t \in K$. Then $\Delta = u^{12}\Delta'$, hence $v(\Delta) = 12v(u) + v(\Delta')$ and $v(u) = 0$ means that $u \in R^\times$.

Exercise : Show furthermore that $r, s, t \in R$.

It follows that the reduction $\widetilde{E} \subseteq \mathbb{P}^2_k$ of a minimal model is unique up to a coordinate change $(*)$ with $u \in k^\times$ and $r, s, t \in k$.

Let $\widetilde{E}$ be *the* reduction of E modulo $\mathfrak{m}$.

Aside 3.19.5. If $\operatorname{char} k \neq 2, 3$, the equation $y^2 = x^3 + ax + b$ is minimal if and only if $v(\Delta) < 12$ or $v(a) < 4$. *Tate's algorithm* computes minimal models in general, plus a whole lot more. △

There's no reason to believe that $\widetilde{E}$ should be an elliptic curve. Let $\widetilde{E}_{ns}$ be the nonsingular points of E.

Fact 3.19.6. *One can check (via lots of casework) that $\widetilde{E}_{ns}$ is an abelian group under the "usual" geometric group law.*

(Note that defining "$P + P'$" in the geometric group law, we need to use the tangent line of E at P.)

There is an action $\mathrm{Gal}_k \circlearrowright \widetilde{E}_{ns}$.

We say E has *good reduction* if $v(\Delta) = 0$, i.e. $\widetilde{E}/k$ is an elliptic curve, so $\widetilde{E}_{ns} = \widetilde{E}$; otherwise E has *bad reduction*.

Suppose we have bad reduction; we may without loss of generality assume $\widetilde{E}$ is singular at $P = (0, 0)$. Then $\widetilde{E}_{ns} = E \backslash \{P\}$. The singularity at $(0, 0) \in \widetilde{E}$ imposes three conditions on the coefficients of the equation defining $\widetilde{E}$, and it turns out that

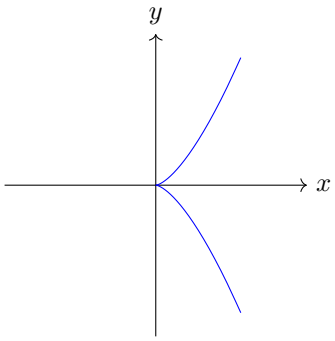
$$\widetilde{E} : y^2 + \overline{a_1}xy = x^3 + \overline{a_2}x^2,$$

or in other words

$$\underbrace{y^2 + \overline{a_1}xy - \overline{a_2}x^2}_{\substack{\text{homogeneous quadratic;} \\ \text{discriminant } \overline{a_1}^2 + 4\overline{a_2}}} - x^3 = 0.$$

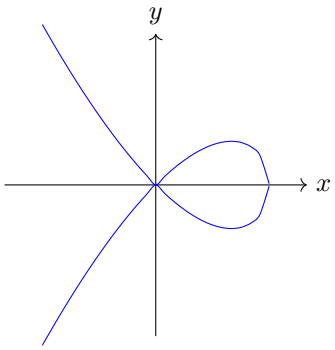
Then:

- We say E has a cusp at $(0, 0)$ if $\overline{a_1}^2 + 4\overline{a_2} = 0$. When char $k \neq 2$, up to a change in coordinates we have the curve $y^2 = \overline{x^3}$:



  The nonsingular points are $\widetilde{E}_{ns} \cong \mathbb{G}_a$ over k; it is a group scheme with $\mathbb{G}_a(\overline{k}) = (\overline{k}, +)$. We say E has *additive reduction*.

- We say E has a *node* at $(0, 0)$ if $\overline{a_1}^2 + 4\overline{a_2} \neq 0$. When char $k \neq 0$, up to a change in coordinates we have the curve $y^2 = x^3 + \overline{a_2}x^2$:



  [The curve is supposed to be connected/smooth with a single nodal singularity, and "any other singularities are due to the author" - Jake]

  The nonsingular points are $\widetilde{E}_{ns} \cong \mathbb{G}_m$ over k; it is a group scheme with $\mathbb{G}_m(\overline{k}) = (\overline{k}^\times, \times)$. We say E has *multiplicative reduction*. Note that $y^2 - \overline{a_2}x^2 = (y - \sqrt{\overline{a_2}}x)(y + \sqrt{\overline{a_2}}x)$ factors. Thus, we say it has *split multiplicative reduction* if $\overline{a_2} \in (k^\times)^2$, and it has *non-split mulitplicative reduction* otherwise.

(Note that a connected linear algebraic group over an algebraically closed field is either $\mathbb{G}_a$ or $\mathbb{G}_m$; it's not hard to decide which one $\widetilde{E}_{ns}$ is isomorphic to.)

We have a *reduction modulo* $\mathfrak{m}$ map

$$\begin{aligned}\mathbb{P}^n(K) &\to \mathbb{P}^n(k)\\ [a_0, \dots, a_n] &\mapsto [\overline{a_0}, \dots, \overline{a_n}],\end{aligned}$$

where $\overline{a_i}$ is the image of a_i in $R/\mathfrak{m}$, after scaling all coordinates so that all $a_i \in R$ and at least one $a_i \in R^\times$. This is well-defined. This gives a reduction map

$$\begin{aligned}E(K) &\to \widetilde{E}(k)\\ P &\mapsto \overline{P}.\end{aligned}$$

Thus for example, the reduction map sends $E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)$.

Define $E_0(K) = \{P \in E(K) \colon \overline{P} \in \widetilde{E}_{ns}(k)\}$. We have

Fact 3.19.7. *The map*

$$\begin{aligned}E_0(K) &\to \widetilde{E}_{ns}(k)\\ P &\mapsto \overline{P}\end{aligned}$$

is a group homomorphism, and $E_0(K)$ is a subgroup of $E(K)$.

(See [Silverman, VII §2]; it's straightforward.)

Fact 3.19.8. *The group $E(K)/E_0(K)$ is finite, i.e. $E_0(K)$ is finite index in $E(K)$.*

When $K/\mathbb{Q}_p$ is a finite extension, there is a topological proof. The idea is to use the fact that R is compact, hence $E_0(K)$ is an open subgroup of the compact $E(K)$. Thus the cosets are a disjoint open cover, and the compactness of $E(K)$ means that $[E(K) : E_0(K)]$ is finite. In general, it follows from Tate's algorithm and a Néron model.

One can even say more:

- If E is split multiplicative, $[E(K) : E_0(K)] = v(\Delta)$
- Otherwise, $[E(K) : E_0(K)] \leq 4$.

Fact 3.19.9. *The reduction map*

$$\begin{aligned}E_0(K) &\to \widetilde{E}_{ns}(k)\\ P &\mapsto \overline{P}\end{aligned}$$

is surjective.

This follows from Hensel's lemma.

We have a short exact sequence of groups

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow{P \mapsto 0} \widetilde{E}_{ns}(k) \longrightarrow 0$$

, where $E_1(K) = \{P \in E(K) \colon \overline{P} = \overline{O}\}$. Also $E(K)/E_0(K)$ is finite.

A key idea is that to study $E(K)$, it might be easier to break it into pieces $E(K)/E_0(K)$, $\widetilde{E}_{ns}(k)$, and $E_1(K)$. Later, we'll see

THEOREM 3.19.10. *The torsion subgroup of $E_1(K)$ is a p-group when $p = \operatorname{char} k$.*

This uses formal groups in Chapter IV of Silverman.

Corollary 3.19.11. *Suppose $K/\mathbb{Q}_p$ is finite. Consider E/K with good reduction. Then for $m \geq 1$ with $p \nmid m$, the map*

$$\begin{aligned} E(K)[m] &\mapsto \widetilde{E}(k) \\ P &\mapsto \overline{P} \end{aligned}$$

is an injective group homomorphism.

(The corollary follows because E has good reduction, we see that $E_0(K) = E(K)$, hence the kernel is in $E_1(K)$, which has no nontrivial m-torsion because $p \nmid m$.)

Corollary 3.19.12. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\text{tors}}$ is finite.*

Proof. Take p large enough so that E has good reduction over $\mathbb{Q}_p$. Then

$$E(\mathbb{Q})_{\text{tors}} \subseteq E(\mathbb{Q}_p)_{\text{tors}} \to \widetilde{E}(\mathbb{F}_p)$$

which is finite; its kernel is a p-group. It follows that $E(\mathbb{Q})_{\text{tors}}/\{\text{maximal } p\text{-subgroup}\}$ is a finite group. To finish, choose a second prime p. □

Example 3.19.13. Let $E/\mathbb{Q} : y^2 = x^3+3x+4$; it has discriminant $\Delta = -2^6 \cdot 3^3 \cdot 5$. It has good reduction at $p > 5$. One cna compute $\#\widetilde{E}(\mathbb{F}_{11}) = 14$ and $\#\widetilde{E}(\mathbb{F}_{17}) = 20$. It follows that $\#E(\mathbb{Q})_{\text{tors}} | 2$. But $(-1, 0) \in E(\mathbb{Q})$, so $E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-1, 0)\}$. Note that $(0, 2) \in E(\mathbb{Q})$. So $(0, 2)$ has infinite order, and hence $E(\mathbb{Q})$ is infinite. △

3.20 Apr 21, 2020 (Local fields)

Let K be a local field, which for our purposes has a definition that is more general than the "usual" one: it is a field with a discrete vlauation $v\colon K \to \mathbb{Z} \cup \{+\infty\}$ satisfying:

- $v(xy) = v(x) + v(y)$
- $v(x+y) \geq \min\{v(x), v(y)\}$
- $v(x) = +\infty$ if and only if $x = 0$.

Also K is complete with respect to the absolute value

$$|\cdot|_v \colon K \to \mathbb{R}_{\geq 0}, \qquad |x|_v = c^{-v(x)}$$

for a fixed $c > 1$. We assume $v(x) \neq 0$ for some $x \in K^\times$, so that the topology from $|\cdot|_v$ is non-trivial. Without loss of generality, v will be surjective.

This gives rise to the *valuation ring* $R = \{x \in K\colon v(x) \geq 0\}$, which is a complete DVR (discrete valuation ring). It has a maximal ideal $\mathfrak{m}$ and hence a residue field $R/\mathfrak{m}$.

We further assume that K and k are perfect, because we're following Silverman. The key example is a finite extension $K/\mathbb{Q}_p$. When $K = \mathbb{Q}_p$, we have $R = \mathbb{Z}_p$ and $k = \mathbb{F}_p$.

Now consider an elliptic curve E/K. Fix a minimal model for E given by

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

i.e. $a_i \in R$ with $v(\Delta)$ minimal. The (!) reduction modulo $\mathfrak{m}$ of E is the the curve $\widetilde{E} \subseteq \mathbb{P}^2_k$ defined by $(*)$.

Let $\widetilde{E}_{ns}$ be the nonsingular points of E; it is an algebraic group under the "usual" geometric group law. When E has good reduction (i.e. $v(\Delta) = 0$), $\widetilde{E}_{ns} = \widetilde{E}$ is an elliptic curve over k. When E has *bad reduction*, the group $\widetilde{E}_{ns}(\overline{k})$ is isomorphic to $(\overline{k}, +)$ or $(\overline{k}^\times, \times)$, in which case we say it is additive or multiplicative respectively.

We also have a reduction modulo $\mathfrak{m}$ map

$$E(K) \to \widetilde{E}(k), \qquad P \mapsto \overline{P}$$

We get subgroups of $E(K)$

$$E_0(K) \stackrel{\text{def}}{=} \{P \in E(K)\colon \overline{P} \in \widetilde{E}_{ns}(k)\}$$
$$E_1(K) \stackrel{\text{def}}{=} \{P \in E(K)\colon \overline{P} = \overline{0}\}.$$

They have important properties:

- $E(K)/E_0(K)$ is finite
- We have an exact sequence

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow{P \mapsto \overline{P}} \widetilde{E}_{ns}(k) \longrightarrow 0$$

- Any nonidentity element of $E_1(K)$ of finite order has order a power of p where $p = \operatorname{char} k > 0$. (This will be explained later with formal groups.)

Now let K' be a finite extension of K and let R' be the integral closure of R in K'; it is a complete discrete valuation ring with maximal ideal $\mathfrak{m}'$, hence K' is a local field. It follows that:

- $\mathfrak{m}R' = (\mathfrak{m}')^e R'$ for a unique $e \geq 1$, which we call the *ramification index*. The valuation $v'\colon K' \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ is linked to the valuation $v\colon K \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ in the following way: For $x \in K$, we have $v'(x) = ev(x)$.

- The injection $k \hookrightarrow k' = R'/\mathfrak{m}'$ is a finite extension, so this gives a number $f = [k' : k]$ called the *residue degree*
- We have $[K' : K] = ef$. (This uses that k and K are separable.)

For related topics, you might be interested in the theory of Dedekind domains.

We say K'/K is *unramified* if $e = 1$, and *totally ramified* if $e = [K' : K]$.

Fact 3.20.1. *There is a unique field L such that K'/L is totally ramified of degree e, and L/K is unramified of degree f. (Prove this using Hensel's lemma!)*

Let's study Gal_K. Assume K'/K is Galois. Note that $\mathrm{Gal}(K'/K)$ acts on R' and $\mathfrak{m}'$, hence on k'. It fixes R and $\mathfrak{m}$, and hence k. Thus we get a map $\mathrm{Gal}(K'/K) \to \mathrm{Gal}(k'/k)$.

Fact 3.20.2. *The map $\mathrm{Gal}(K'/K) \to \mathrm{Gal}(k'/k)$ is surjective. (Prove this using Hensel's lemma!)*

We obtain an exact sequence

$$1 \longrightarrow \mathrm{Gal}(K'/L) \longrightarrow \mathrm{Gal}(K'/K) \longrightarrow \mathrm{Gal}(k'/k) \longrightarrow 1$$

We increase K' to obtain

$$1 \longrightarrow \mathrm{Gal}(\overline{K}/K^{un}) \longrightarrow \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Gal}(\overline{k}/k) \longrightarrow 1$$

where K^{un} is the maximal unramified extension of K. The (possibly infinite) extension K^{un}/K is a local field.

We denote by $I_K \stackrel{\text{def}}{=} \mathrm{Gal}(\overline{K}/K^{un})$, which we call the *inertia subgroup* of Gal_K.

Now suppose there is a Gal_K action on a set Σ. We say the action is *unramified* if I_K acts trivially. In this case, we get actions of $\mathrm{Gal}(K^{un}/K) \circlearrowright \Sigma$ and $\mathrm{Gal}_k \circlearrowright \Sigma$.

Theorem 3.20.3. *Suppose E/K has good reduction. Then:*

(a) For any $m \geq 1$ not divisible by $\mathrm{char}\, k$*, the action $\mathrm{Gal}_K \circlearrowright E[m]$ is unramified.*

(b) For a prime $\ell \neq \mathrm{char}\, k$, the action $\mathrm{Gal}_K \circlearrowright T_\ell E$ is unramified.

Proof. Part (a) clearly implies part (b), so let's prove (a). Fix a finite K'/K such that $E[m] \subseteq E(K')$. Then we have a homomorphism

$$E[m] = E(K')[m] \xrightarrow{\text{reduction}} \widetilde{E}(k')[m] \subseteq \widetilde{E}[m],$$

where $\widetilde{E}$ is an elliptic curve because E has good reduction. Note that both $E[m]$ and $\widetilde{E}[m]$ both have order m^2, and the kernel is contained in the kernel of $E_1(K')[m]$ (since E_1 is the kernel of the reduction map). But $E_1(K')[m]$ is trivial, because the nontrivial torsion in $E_1(K')$ has order a power of $\mathrm{char}\, k' \nmid m$ (this will be explained later with formal groups). Thus we have an isomorphism

$$E[m] \xrightarrow{\sim} \widetilde{E}[m];$$

the actions of $\mathrm{Gal}_K \circlearrowright E[m]$ and $\mathrm{Gal}_k \circlearrowright \widetilde{E}[m]$ are compatible with $\mathrm{Gal}_K \to \mathrm{Gal}_k$. □

Theorem 3.20.4 (Criterion of Néron-Ogg-Shafarevich)**.** *Let E/K be a elliptic curve and fix $\ell \neq \mathrm{char}\, k$. The action of $\mathrm{Gal}_K \circlearrowright T_\ell E$ is unramified if and only if E has good reduction.*

(In the bad reduction case, one can actually check whether it's additive or multiplicative.)

Proof. The backwards direction is Theorem 3.20.3.

For the forwards direction, we suppose that $\mathrm{Gal}_K \circlearrowright T_\ell E$ is unramified. Equivalently, $I_K = \mathrm{Gal}(\overline{K}/K^{un})$ acts trivially on $T_\ell E$, and so $E[\ell^n] \subseteq E(K^{un})$ for all $n \geq 1$. We use the fact that E has good reduction over K if and only if it has good reduction over K^{un} (see [Silverman, VII 5.4]). Because $[E(K^{un}) : E_0(K^{un})]$ is finite, we have $E[\ell] \subseteq E_0(K^{un})$, so we get an exact sequence

$$1 \longrightarrow E_1(K^{un}) \longrightarrow E_0(K^{un}) \longrightarrow \widetilde{E}_{ns}(\overline{k}) \longrightarrow 1$$

where $E_1(K^{un})$ has no nontrivial ℓ-torsion (since $\ell \neq \operatorname{char} k$). Thus $\widetilde{E}_{ns}(\overline{k})$ contains a subgroup isomorphic to $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. If E has bad reduction, then $\widetilde{E}_{ns}(\overline{k})$ is isomorphic to $\overline{k}$ or $\overline{k}^\times$, which have no nontrivial ℓ-torsion or an ℓ-torsion subgroup of order ℓ, respectively. This is a contradiction. Therefore, E has good reduction! □

Aside 3.20.5. Let V be a nice variety over a local field K with valuation ring R. We say that V has *good reduction* if there is a smooth proper scheme $\mathcal{V} \to \operatorname{Spec} R$ whose generic fiber is V.

For V an elliptic curve, this agrees with our earlier definition. (To show this, use Néron-Ogg-Shafarevich (Theorem 3.20.4).) △

We say that E/K has *potentially good reduction* if there is a finite extension K'/K such that E has good reduction over K'.

Theorem 3.20.6. *The following are equivalent for E/K:*

(a) *E/K has potentially good reduction*

(b) *E has good or additive reduction*

(c) *For $\ell \neq \operatorname{char} k$, I_K acts on $T_\ell E$ through a finite group*

(d) *$j(E) \in R$.*

3.21 Apr 23, 2020 (Local fields)

We'll talk about formal groups today. The motivation for studying formal groups is as follows. Let E be an elliptic curve over a local field K and fix a Weierstrass model with $a_i \in R$, where R is the valuation ring of K with maximal ideal $\mathfrak{m}$. We defined

$$E_1(K) = \{P \in E(K) \colon P \equiv \mathcal{O} \pmod{\mathfrak{m}}\} \le E(K).$$

The claim is that $E_1(K)_{\text{tors}}$ is either trivial or a p-group, where $p = \operatorname{char} R/\mathfrak{m}$. To do this, we need to understand E "near" $\mathcal{O}$.

Let E be an elliptic curve over a general (perfect) field K. Let's study E "near" $\mathcal{O}$. There are many ways to interpret this, for example:

- We could study the Lie algebra, but this turns out to be a 1-dimensional K-vector space with trivial pairing. Thus we lose too much information.
- We could study the local ring $K[E]_{\mathcal{O}} \subseteq K(E)$, i.e. the ring of $f \in K(E)$ with $\operatorname{ord}_{\mathcal{O}}(f) \ge 0$. This ring has too much information, since from $K[E]_{\mathcal{O}}$ we can recover $K(E)$ and hence E/K up to isomorphism as a curve; we can also recover $\mathcal{O} \in E(K)$ from $K[E]_{\mathcal{O}}$.

We could also consider the completion:

$$\widehat{K[E]_{\mathcal{O}}} \stackrel{\text{def}}{=} \varprojlim_n K[E]_{\mathcal{O}}/\mathfrak{m}^n,$$

where $\mathfrak{m}$ is the maximal ideal of the local ring $K[E]_{\mathcal{O}}$. The completion turns out to be a complete discrete valuation ring.

Consider a model for E/K:

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

with $a_i \in K$. Because y is nonzero near the identity, we may divide by y^3 to obtain

$$\frac{1}{y} + a_1\frac{x}{y}\frac{1}{y} + a_3\left(\frac{1}{y}\right)^2 = \left(\frac{x}{y}\right)^3 + a_2\left(\frac{x}{y}\right)^2\frac{1}{y} + a_4\frac{x}{y}\left(\frac{1}{y}\right)^2 + a_6\left(\frac{1}{y}\right)^3. \tag{4}$$

Set $w \stackrel{\text{def}}{=} -\frac{1}{y}$ and $z \stackrel{\text{def}}{=} -\frac{x}{y}$. Then Equation (4) becomes

$$w = \underbrace{z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3}_{\text{call this } f(z,w)}. \tag{5}$$

Note that $\mathcal{O}$ is now $(z, w) = (0, 0)$ in this model.

We have $\operatorname{ord}_{\mathcal{O}} x = -2$ and $\operatorname{ord}_{\mathcal{O}} y = -3$, so $\operatorname{ord}_{\mathcal{O}} w = 3$ and $\operatorname{ord}_{\mathcal{O}} z = -2 + 3 = 1$. It follows that z is a uniformizer of $\widehat{K[E]_{\mathcal{O}}}$.

Exercise : We have $\widehat{K[E]_{\mathcal{O}}} = K[\![z]\!]$.

Thus $w \in \widehat{K[E]_{\mathcal{O}}} = K[\![z]\!]$ means that $w = w(z)$ can be expressed in terms of z, sort of like an "implicit function theorem".

Indeed, to compute $w(z)$, we observe that $w = O(z^3)$, i.e. $w \in z^3K[\![z]\!]$. Now recall (Equation (5)) that $z = f(z, w)$. Thus:

$$\begin{aligned}
w &= f(z,w) = z^3 + O(z^4) \\
w &= f(z,w) = z^3 + a_1z^4 + O(z^5) \\
w &= f(z,w) = z^3 + a_1x^4 + (a_1^2 + a_2)z^5 + O(z^6) \\
&\vdots
\end{aligned}$$

(We obtained better information at each step by considering $f(z,w) = f(z, z^3 + O(z^4))$ and $f(z,w) = f(z, z^3 + a_1 z^4 + O(z^5))$ respectively.)

We may repeat this to obtain

$$w = w(z) = z^3(1 + A_1 z_1 + A_2 z^2 + \dots)$$

with $A_n \in \mathbb{Z}[a_1, \dots, a_6]$ a degree n polynomial in the a_i, where $\deg a_i = i$. For example,

$$A_1 = a_1, \qquad A_2 = a_1^2 + a_2, \qquad a_1^3 + 2a_1 a_2 + a_3,$$
$$A_4 = a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^4 + a_4$$

Remark 3.21.1. In particular, $w = f(z,w)$ has a unique solution $w \in K[\![z]\!]$. △

We have Laurent series

$$x(z) = \frac{-z}{w(z)} = \frac{1}{z^2} - a_1 \frac{1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^3 + \dots \in \mathbb{Z}[a_1, \dots, a_6]((z)) \subseteq K((z)),$$

and

$$y(z) = -\frac{1}{w(z)} = \frac{-1}{z^3} + \frac{a_1}{z} + \dots \in \mathbb{Z}[a_1, \dots, a_6]((z)) \subseteq K((z)).$$

Observe that

$$[z, -1, w(z)] = [x(z), y(z), 1] \in E(K((z))),$$

where $w(z)$ is an explicit series in $\mathbb{Z}[a_1, \dots, a_6][\![z]\!]$. We call this a "formal solution".

Now suppose K is a local field with valuation ring $R \supseteq \mathfrak{m}$. Assume $a_i \in R$. As above $w(z) \in R[\![z]\!]$. The key observation is that we can plug in values $z_0 \in \mathfrak{m}$ into $w(z)$, so $w(z_0) \in R$. (This is because $w(z_0) = z_0^3(1 + A_1 z_0 + a_2 z_0^2 + \dots)$, where $A_i \in R$; thus $A_i z^i \to 0$ in K, and in the world of local rings one can prove that a series converges if and only if its summands converge to 0.)

We have an evaluation map

$$\mathfrak{m} \to E(K)$$
$$z_0 \mapsto [z_0, -1, w(z_0)],$$

i.e. we have exhibited many points of $E(K)$. In fact, $[z_0, -1, w(z_0)] \equiv [0, -1, 0] = \mathcal{O} \pmod{\mathfrak{m}}$, so our evaluation map lands inside $E_1(K)$.

Proposition 3.21.2. *We have a bijection*

$$\mathfrak{m} \xrightarrow{\sim} E_1(K)$$
$$z_0 \mapsto [z_0, -1, w(z_0)].$$

Proof. It's easy to see that the map is well-defined and injective. Let's verify surjectivity: take any $P \in E_1(K)$; without loss of generality $P = \mathcal{O}$. Write $P = [x, y, 1] = [-x/y, -1, -1/y]$. Since $P \equiv \mathcal{O} \pmod{\mathfrak{m}}$, we see that $z_0 := -x/y \in \mathfrak{m}$ and $w_0 := -1/y \in \mathfrak{m}$. We need to check that $w(z_0) = w_0$. But we have

$$\begin{aligned} w_0 &= f(z_0, w_0) \\ &= f(z_0, f(z_0, w_0)) \\ &= f(z_0, f(z_0, f(z_0, w_0))) \\ &= \dots . \end{aligned}$$

As before, we find that $w_0 = w(z_0)$. □

Note that the bijection of sets in Proposition 3.21.2 is not a homomorphism of groups. Thus we can use the bijection to give $\mathfrak{m}$ a new group law (steal it from $E_1(K)$).

Claim 3.21.3. *There is a unique power series $F(x,y) \in R[\![x,y]\!]$ such that $a \oplus b := F(a,b)$ defines the above group law on $\mathfrak{m}$.*

We will now construct an $F(x,y) \in K[\![x,y]\!]$ for a general K; in the local case it will satisfy the above claim.

We work with the field $K((z_1,z_2))$ in two independent variables. We have

$$[-z_1, 1, w(z_1)] + [-z_2, 1, -w(z_2)] \in E(K((z_1,z_2))), \tag{6}$$

where addition above uses the group law in E. The claim is that there exists $F(x,y) \in K[\![x,y]\!]$ such that Equation (6) is equal to $[-F(z_1,z_2), 1, -w(F(z_1,z_2))]$.

Indeed, in the (z,w)-coordinates there the points $[-z_1,1,w(z_1)]$ and $[-z_2,1,-w(z_2)]$ are connected by a line L of slope

$$\lambda = \frac{w(z_2)-w(z_1)}{z_2-z_1} = \sum_{n=0}^{\infty} A_n \frac{z_2^{n+3}-z_1^{n+3}}{z_2-z_1} \in \mathbb{Z}[a_1,\dots,a_6][\![z_1,z_2]\!].$$

So write $L : \lambda z + v$ with $v = w(z_1) - \lambda(z_1) \in \mathbb{Z}[a_1,\dots,a_6][\![z_1,z_2]\!]$. Plug in $w = \lambda z + v$ into equation to get a cubic in z with three roots, two of which are z_1 and z_2. Thus the third root is

$$z_3 = -z_1 - z_2 + \frac{a_3\lambda + a_3\lambda^2 - a_2 y - 2a_4\lambda v}{1 + a_2\lambda + a_6\lambda^2 + a_3\lambda^3} \in \mathbb{Z}[a_1,\dots,a_6][\![z_1,z_2]\!].$$

After some more steps, it follows that the point in Equation (6) has z-coordinate $F(z_1,z_2)$, where

$$F(x,y) = x + y - a_1xy - a_1(x^2y + xy^2) + (-2a_3x^3y + (a_1a_2 - 3a_3)x^2y^2 - 2a_3xy^3) + \cdots \in \mathbb{Z}[a_1,\dots,a_6][\![x,y]\!].$$

This gives a "formal group" $\hat{E}$ over any ring $R \supseteq \mathbb{Z}[a_1,\dots,a_6]$.

Definition 3.21.4. Let R be a ring. A *(one-parameter commutative) formal group $\mathscr{F}$ over R* is a power series $F(x,y) \in R[\![x,y]\!]$ such that:

(a) $F(x,y) = x + y +$ terms of degree ≥ 2

(b) $F(x,F(y,z)) = F(F(x,y),z)$

(c) $F(x,y) = F(y,x)$

(d) There exists a unique $i(T) \in R[\![T]\!]$ such that $F(T,i(T)) = 0$

(e) We have $F(x,0) = x$ and $F(0,y) = y$.

(It turns out that part (d) and (e) follow from part (a) and (b).)

We say $F(x,y)$ is the *formal group law* of $\mathscr{F}$. △

Is a formal group a group? No, because there is no underlying set.

3.22 Apr 28, 2020 (Local fields)

We'll finish up formal groups today; see [Silverman, Ch IV] for more. (There is a lot more out there than what's in Silverman, as well!)

Let R be a commutative ring. A formal group $\mathscr{F}$ over R is a power series $F(x,y) \in R[\![x,y]\!]$ satisfying:

(a) $F(x,y) = x + y + (\text{terms of degree } \geq 2)$

(b) $F(x, F(y,z)) = F(F(x,y), z)$

(c) $F(x,y) = F(y,x)$

(d) There is a unique $i(T) \in R[\![T]\!]$ such that $F(T, i(T)) = 0$.

(e) $F(x,0) = x$ and $F(0,y) = y$.

Exercise : Show that (a), (b), and (c) imply (d) and (e).

We say that F is the formal group law of $\mathscr{F}$.

Example 3.22.1. The *formal additive group* is denoted $\widehat{\mathbb{G}_a}$ over R and is defined by

$$F(x,y) = x + y \qquad \text{and} \qquad i(T) = -T.$$

△

Example 3.22.2. Te *formal multiplicative group* is denoted $\widehat{\mathbb{G}_m}$ over R and is defined by

$$F(x,y) = x + y + xy = (1+x)(1+y) - 1 \qquad \text{and} \qquad i(T) = \frac{1}{1+T} - 1 = \sum_{n=1}^{\infty} T^n.$$

(The 1's appear above because we want 0 to be the "identity"; one can readily check that $F(x,0) = x$ and $F(0,y) = y$.) △

Example 3.22.3. Let E/K be an elliptic curve with explicit model in x and y. Last time we constructed an $F(x,y) \in \mathbb{Z}[a_1, \dots, a_6][\![x,y]\!]$ satisfying the following. By setting $z = -x/y$, there is a unique $w(z) \in K[\![z]\!]$ such that $[z, -1, w(z)] \in E(K((z)))$. For z_1, z_2 independent variables, the addition law on E is such that

$$[z_1, -1, w(z_1)] + [z_2, -1, w(z_2)] = [F(z_1, z_2), -1, w(F(z_1, z_2))] \in E(K((z_1, z_2)))$$

Using that E is a group law, one can show that F is a formal group law. This gives a formal group $\widehat{E}$ over $\mathbb{Z}[a_1, \dots, a_6]$. △

Now suppose that R is a complete discrete valuation ring with quotient field K, and let $\mathfrak{m} \subseteq R$ be its maximal ideal and $k = R/\mathfrak{m}$. Let $(\mathscr{F}, F)$ be a formal group over R.

We can give $\mathfrak{m}$ a new (abelian) group law by setting $a \oplus b = F(a,b)$: note that $F(a,b)$ converges to an element in $\mathfrak{m}$ for all $a, b \in \mathfrak{m}$. The group axioms for $\mathfrak{m}$ follow from properties of F. The set $\mathfrak{m}^r$ is a subgroup of $\mathfrak{m}$.

We fix the notation $\mathscr{F}(\mathfrak{m}^r)$ to denote the set $\mathfrak{m}^r$ with group law from F.

Example 3.22.4. The group $\widehat{\mathbb{G}_a}(\mathfrak{m})$ is just $\mathfrak{m}$ with the usual $+$. △

Example 3.22.5. Consider $\widehat{\mathbb{G}_m}(\mathfrak{m})$. Observe that there is a group isomorphism

$$\begin{aligned} \widehat{\mathbb{G}_m}(\mathfrak{m}) &\xrightarrow{\sim} 1 + \mathfrak{m} \subseteq R^\times \\ x &\mapsto 1 + x. \end{aligned}$$

(This is because $F(x,y) = (1+x)(1+y) - 1$.) △

Example 3.22.6. Consider $\widehat{E}(\mathfrak{m})$. Last time we showed (Proposition 3.21.2, Claim 3.21.3) that there is a group isomorphism

$$\widehat{E}(\mathfrak{m}) \xrightarrow{\sim} E_1(K) = \{P \in E(K) \text{ such that } P \equiv 0 \pmod{\mathfrak{m}}\}.$$

△

Theorem 3.22.7. *Take any non-zero $P \in \mathscr{F}(\mathfrak{m})$ of finite order. Then the order of P is a power of $p = \operatorname{char} k > 0$.*

This gives the long-promised Theorem 3.19.10

Corollary 3.22.8. *The torsion subgroup of $E_1(K)$ is a p-group when $p = \operatorname{char} k$.*

Proof of Theorem 3.22.7. Without loss of generality, suppose $P \in \mathcal{F}(\mathfrak{m})$ has prime order ℓ. We need to show that $\ell = \operatorname{char} k$.

There is a minimal $r \geq 1$ such that $P \in \mathfrak{m}^r = \mathscr{F}(\mathfrak{m}^r)$. We have $\ell P = 0 \in \mathfrak{m}^{r+1} = \mathscr{F}(\mathfrak{m}^{r+1})$. Now observe that

$$\begin{aligned} \mathscr{F}(\mathfrak{m}^r)/\mathscr{F}(\mathfrak{m}^{r+1}) &\xrightarrow{\sim} \mathfrak{m}^r/\mathfrak{m}^{r+1} \cong k \\ a &\mapsto a \end{aligned}$$

is an isomorphism; this is because $F(x, y) = x + y +$ higher order terms. Thus $(k, +)$ has a point of order ℓ, and it follows that $\ell = \operatorname{char} k$. □

Notice that in the proof of Theorem 3.22.7 we saw that although $\mathscr{F}(\mathfrak{m})$ may be a complicated group, it comes with a filtration $\mathscr{F}(\mathfrak{m}) \supset \mathscr{F}(\mathfrak{m}^2) \supset \dots$ whose quotients are just $(k, +)$.

In fact, we can prove a stronger version of Theorem 3.22.7. Assume that $\operatorname{char} K = 0$ and $p = \operatorname{char} k > 0$, e.g. a finite extension $K/\mathbb{Q}_p$. We have a valuation $v \colon K \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$.

THEOREM 3.22.9. *Let $\mathscr{F}$ be a formal group over R. For any integer $r > \frac{v(p)}{p-1}$, we have an isomorphism of groups*

$$\mathscr{F}(\mathfrak{m}^r) \simeq (R, +).$$

In particular, $\mathscr{F}(\mathfrak{m}^r)$ is torsion-free.

Example 3.22.10. Take $p > 2$. Observe that there is a short exact sequence

$$1 \longrightarrow 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times \xrightarrow{(\bmod p)} \mathbb{F}_p^\times \longrightarrow 1$$

Since $1 + p\mathbb{Z}_p = \widehat{\mathbb{G}_m}(p\mathbb{Z}_p)$, Theorem 3.22.9 for $\mathfrak{m} = p\mathbb{Z}_p$ and $r = 1 > \frac{v(p)}{p-1} = \frac{1}{p-1}$ implies $\widehat{\mathbb{G}_m}(p\mathbb{Z}_p) \simeq \mathbb{Z}_p$. It follows that

$$\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

For $p = 2$, the theorem doesn't apply, and furthermore the result is false since

$$\mathbb{Z}_2^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2.$$

△

Example 3.22.11. Consider $E/\mathbb{Q}_p$ with good reduction, and $p \neq 2$. We have an exact sequence

$$0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E(\mathbb{Q}_p) \xrightarrow{\bmod p} \widetilde{E}(\mathbb{F}_p) \longrightarrow 0$$

Since by Theorem 3.22.9 we have that $E_1(\mathbb{Q}_p) \simeq \widehat{E}(p\mathbb{Z}) \cong \mathbb{Z}_p$ is torsion free, we see that the homomorphism

$$E(\mathbb{Q}_p)_{\text{tors}} \xhookrightarrow{\bmod p} \widetilde{E}(\mathbb{F}_p)$$

is actually injective! △

To prove Theorem 3.22.9, we need to relate $\mathscr{F}$ and $\widehat{\mathbb{G}_a}$. To do this, we define the *formal logarithm* of $\mathscr{F}$, which shall be

$$\log_{\mathscr{F}}(T) = \int_0^T \frac{1}{F_2(t,0)}\,dt \in K[\![T]\!],$$

where: $F \in R[\![x,y]\!]$ is the formal law of $\mathscr{F}$, $F_2 = \frac{\partial}{\partial y}F(x,y)$, so $F_2(x,y) = 1 + \text{terms of degree } \geq 1$. It follows that $F_2(t,0) \in 1 + tR[\![t]\!]$ is invertible, with $F_2(t,0)^{-1} \in 1 + tR[\![t]\!]$. Writing

$$F_2(t,0)^{-1} = 1 + \sum_{n=2}^{\infty} a_n t^{n-1},$$

we see that

$$\int_0^T F_2(t,0)^{-1}\,dt = T + \sum_{n=2}^{\infty} \frac{a_n}{n} T^n.$$

Note that $\log_{\mathscr{F}}(T) = \sum_{n=1}^{\infty} \frac{a_n}{n} T^n$ with $a_N \in R$ and $a_1 = 1$.

Example 3.22.12. Let $\mathscr{F} = \widehat{\mathbb{G}_m}$. Then $F(x,y) = x + y + xy$ so $F_2(x,y) = 1 + x$. It follows that

$$\log_{\widehat{\mathbb{G}_m}}(T) = \int_0^T \frac{1}{1+t}\,dt = \log(1+T),$$

where the $\log$ on the right side is the usual logarithm. △

Lemma 3.22.13. *We have*

$$\log_{\mathscr{F}}(F(x,y)) = \log_{\mathscr{F}} x + \log_{\mathscr{F}} y.$$

In other words, $\log_{\mathscr{F}}$ *is a* homomorphism *from* $\mathscr{F}$ *to* $\widehat{\mathbb{G}_a}$.

Proof. Define

$$h(x,y) = \log_{\mathscr{F}} F(x,y) - \log_{\mathscr{F}} x - \log_{\mathscr{F}} y.$$

We need to show $h = 0$. Since $h(0,0) = 0$, we need only show that $\frac{\partial h}{\partial x} = 0$ and $\frac{\partial h}{\partial y} = 0$; and by symmetry we'll just show $\frac{\partial h}{\partial y} = 0$.

Observe that

$$\frac{d}{dt}\log_{\mathscr{F}}(T) = \frac{1}{F_2(t,0)}.$$

So by the chain rule, we need to show

$$\frac{\partial h}{\partial y} = \frac{1}{F_2(F(x,y),0)}F_2(x,y) - 0 - \frac{1}{F_2(y,0)} \stackrel{?}{=} 0.$$

Well, observe that by associativity we have

$$\frac{\partial}{\partial z}F(F(x,y),z) = \frac{\partial}{\partial z}F(x,F(y,z)),$$

which by chain rule says

$$F_2(F(x,y),z) = F_2(x,F(y,z))F_2(y,z) \stackrel{z=0}{\Longrightarrow} F_2(F(x,y),0) = F_2(x,F(y,0)) \cdot F_2(y,0).$$

It follows that

$$\frac{1}{F_2(F(x,y),0)}F_2(x,y) = \frac{1}{F_2(y,0)},$$

which is exactly what we wanted to show. □

Exercise : For $x \in \mathfrak{m}^r$ (with $r \geq 1$), then $\frac{x^n}{n} \in \mathfrak{m}^r$ and $v(\frac{x^n}{n}) \to +\infty$. It follows that $\log_{\mathscr{F}} x$ converges and is in $\mathfrak{m}^r$ for all $x \in \mathfrak{m}^r$. (Again, this uses that $\log_{\mathscr{F}}(x) = \sum_{n=1}^{\infty} \frac{a_n}{n} x^n$ for $a_n \in R$ and $a_1 = 1$.)

For any $r \geq 1$, we have a group homomorphism

$$\begin{aligned} \mathscr{F}(\mathfrak{m}^r) &\to \widehat{\mathbb{G}_a}(\mathfrak{m}^r) \\ x &\mapsto \log_{\mathscr{F}}(x). \end{aligned}$$

This is not always an isomorphism, as we saw with

$$\widehat{\mathbb{G}_m}(2\mathbb{Z}_2) \to \widehat{\mathbb{G}_a}(2\mathbb{Z}_2)$$

in Example 3.22.10, where the left side has torsion and the right side does not.

Exercise : There is a unique $\exp_{\mathscr{F}}(T) \in K[\![T]\!]$ such that $\log_{\mathscr{F}} \exp_{\mathscr{F}}(T) = T = \exp_{\mathscr{F}} \log_{\mathscr{F}}(T)$. Moreover,

$$\exp_{\mathscr{F}}(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!} T^n \qquad \text{with } b_n \in R \text{ and } b_1 = 1.$$

Take $x \in \mathfrak{m}^r$. Does $\exp_{\mathscr{F}}(x)$ converge, and if so, is it in $\mathfrak{m}^r$? The answer turns out to be yes if $r > v(p)/(p-1)$, so we would obtain an isomorphism

$$\mathscr{F}(\mathfrak{m}^r) \xrightarrow{\log_{\mathscr{F}}} \widehat{\mathbb{G}_a}(\mathfrak{m}^r).$$

The idea is to estimate $v(n!) \leq (n-1)\frac{v(p)}{p-1}$ [see e.g. Legendre], and then for $x \in \mathfrak{m}^r$ we have

$$v\Big(\frac{x^n}{n!}\Big) = nv(x) - v(n!) \geq nr - (n-1)\frac{v(p)}{p-1} = r + (n-1)\underbrace{\Big(r - \frac{v(p)}{p-1}\Big)}_{>0}.$$

Example 3.22.14. Take $E/\mathbb{Q}$ given by $y^2 + y = x^3 - x^2 - 10x - 20$. We have $\Delta = -11^5$. Take $p \nmid 2 \cdot 11$ and observe that

$$E(\mathbb{Q})_{\text{tors}} \subseteq E(\mathbb{Q}_p)_{\text{tors}} \xrightarrow{(\text{mod } p)} \widetilde{E}(\mathbb{F}_p).$$

Note that $\#E(\mathbb{F}_3) = 5$. Moreover, $5 | \#E(\mathbb{F}_p)$ for all $p \nmid 2 \cdot 11$. It follows that $E(\mathbb{Q})_{\text{tors}}$ is either trivial or cyclic of order 5. But $(5,5) \in E(\mathbb{Q})$ has order 5, so

$$E(\mathbb{Q})_{\text{tors}} = \langle (5,5) \rangle = \{\mathcal{O}, (5, \pm 5), (16, \pm 60)\}.$$

Next time, we'll take $E/\mathbb{Q}$ and consider the structure of $E(\mathbb{Q})$. $\triangle$

3.23 Apr 30, 2020 (Number fields)

Let K be a number field, i.e. a finite field extension of $\mathbb{Q}$. Over the next few classes, we will prove

Theorem 3.23.1 (Mordell-Weil). *For an elliptic curve E/K, the abelian group $E(K)$ is finitely generated.*

This implies that $E(K) \cong A \times \mathbb{Z}^r$ for some $r \geq 0$, where $A = E(K)_{\text{tors}}$. The integer r is called the *rank* of E.

Note that $E(K)_{\text{tors}}$ is computable, since passing to the completions gives bounds on the size of the torsion and then we can brute force check the remaining possibilities. Even more, we have:

Theorem 3.23.2 (Mazur, 1977). *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphism to one of the following:*

- *$\mathbb{Z}/N\mathbb{Z}$ with $1 \leq N \leq 12, N \neq 11$, or*
- *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ with $1 \leq N \leq 4$.*

Moreover, all of these groups occur.

(This theorem is quite hard; the proof involves constructing some modular curves and understanding their points.)

The rank of an elliptic curve is more mysterious; for example, an open question is whether or not the rank of $E/\mathbb{Q}$ can be arbitrarily large. The expected answer changes over time, and at the moment there's no consensus. The record is due to Elkies, who found an elliptic curve $E/\mathbb{Q}$ with $r \geq 28$.

The strategy of a proof is as follows. There are two ingredients:

- Show that $E(K)/mE(K)$ is finite for some/all $m \geq 2$. (This is called "weak Mordell-Weil")
- There is a *height* function $h\colon E(K) \to \mathbb{R}_{\geq 0}$ satisfying:
  - For any $c > 0$, the set $\{P \in E(K)\colon h(P) \leq c\}$ is finite
  - Fix $Q \in E(K)$. There is C_1 (depending on E and Q) such that $h(P+Q) \leq 2h(P) + C_1$ for all $P \in E(K)$.
  - For $m \geq 2$ there is a constant C_2 depending on m and E such that
    $$h(mP) \geq m^2 h(P) - C_2$$
    for all $P \in E(K)$.

Using these ingredients, let's prove Mordell-Weil (Theorem 3.23.1).

By the weak Mordell-Weil, there exists a *finite* set $S \subseteq E(K)$ that represents all cosets in the finite set $E(K)/mE(K)$. Take any point $P_0 \in E(K)$. Then:

- There is $Q_0 \in S$ such that $P_0 = Q_0 + mP_1$, for $P_1 \in E(K)$,
- There is $Q_1 \in S$ such that $P_1 = Q_1 + mP_2$, for $P_2 \in E(K)$,
- There is $Q_2 \in S$ such that $P_2 = Q_2 + mP_3$, for $P_3 \in E(K)$,

and so on.

Since S is finite, there is $C_1 > 0$ such that $h(P-Q) \leq 2h(P) + C_1$ for all $P \in E(K)$ and $Q \in S$. Then we see that $h(mP_{n+1}) = h(P_n - Q_n)$. Furthermore, the properties of the height function say

$$m^2 h(P_{n+1}) - C_2 \leq h(mP_{n+1}) = h(P_n - Q_n) \leq 2h(P_n) + C_1,$$

so in particular (since $m \geq 2$)

$$h(P_{n+1}) \leq \frac{1}{2} h(P_n) + C.$$

By induction, it follows that $h(P_n) \leq \frac{1}{2^n} h(P_0) + 2C$. Then we observe that $E(K)$ is generated by the set

$$A := S \cup \{P \in E(K)\colon h(P) \leq 2C + 1\}.$$

(Note that $P_n \in A$ for n large enough, and since $P_n = Q_n + mP_{n+1}$ note also that P_0 is in the subgroup generated by A; furthermore, A does not depend on the initial choice of P_0.)

Remark 3.23.3. Our h will be explicit and the sets $\{P \in E(K)\colon h(P) \leq C\}$ are computable. The proof shows if we find a set of generators for $E(K)/mE(K)$, then we can compute a set of generators of $E(K)$. $\triangle$

Unfortunately, we don't know how to find generators of $E(K)/mE(K)$ in general.

Let's fix $m \geq 2$. Our goal is to show that $E(K)/mE(K)$ is finite. Note that we have an exact sequence of groups

$$0 \longrightarrow E[m] \longrightarrow E \xrightarrow{P \mapsto mP} E \longrightarrow 0$$

with compatible $\mathrm{Gal}_K = \mathrm{Gal}(\overline{K}/K)$ actions. Taking Gal_K invariants, we get an exact sequence

$$0 \longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{P \mapsto mP} E(K)$$

We remark that multiplication by m need not be surjective.

Take a point $P \in E(K)$. There is $Q \in E(\overline{K}) = E$ such that $P = mQ$. Now take any $\sigma \in \mathrm{Gal}_K$ and note that

$$P = \sigma(P) = \sigma(mQ) = m\sigma(Q),$$

so $m(\sigma(Q) - Q) = P - P = \mathcal{O}$. We obtain an element

$$\xi_\sigma \stackrel{\mathrm{def}}{=} \sigma(Q) - Q \in E[m].$$

In other words, we get maps

$$\begin{aligned} \xi\colon \mathrm{Gal}_K &\to E[m] \\ \sigma &\mapsto \xi_\sigma \end{aligned}$$

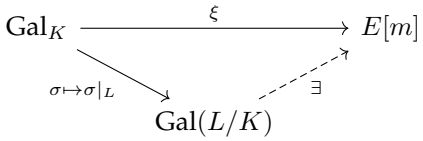
Let's discuss properties of these maps.

- For $\sigma, \tau \in \mathrm{Gal}_K$, we have

  $$\xi_{\sigma\tau} = \sigma\tau(Q) - Q = \sigma(Q) - Q + \sigma(\tau(Q) - Q),$$

  so $\xi_{\sigma\tau} = \xi_\sigma + \sigma\xi_\tau$.

- There exists a finite Galois extension L/K such that ξ factors through

  (We can take L so that $Q \in E(L)$ and $E[m] \subseteq E(L)$.)

- What if we chose another $Q' \in E(\overline{K})$ such that $mQ' = P$? Well, $m(Q' - Q) = P - P = 0$. So $Q' = Q + a$ for some $a \in E[m]$. It follows that

  $$\xi'_\sigma \stackrel{\mathrm{def}}{=} \sigma(Q') - Q' = \sigma(Q + a) - (Q + a) = \xi_\sigma + (\sigma(a) - a). \tag{7}$$

Let K be a (perfect) field; the case where K is a number field or local field suffices for us.

Let A be an abelian group with a Gal_K action that respects the group law and for each $a \in A$ there exists a finite Galois extension L/K such that $\mathrm{Gal}(\overline{K}/L)$ fixes a. (We say that A is a *(discrete)* Gal_K*-module*.)

A map $\xi\colon \mathrm{Gal}_K \to A$ is a *(continuous) 1-cocycle* if:

- $\xi_{\sigma\tau} = \xi_\sigma + \sigma\xi_\tau$ for all $\sigma, \tau \in \mathrm{Gal}_K$, and
- ξ factors through $\mathrm{Gal}(L/K)$ for some finite Galois extension L/K.

For example, a $P \in E(K)$ gives rise to a 1-cocycle $\xi\colon \mathrm{Gal}_K \to E[m]$.

A *1-coboundary* is a $\xi\colon \mathrm{Gal}_K \to A$ of the form $\sigma \mapsto \sigma(a) - a$ for some $a \in A$.

The *first cohomology group* of the Gal_K-module A is

$$H^1(K, A) = H^1(\mathrm{Gal}_K, A) = \frac{\{\text{1-cocycles } \mathrm{Gal}_K \to A\}}{\{\text{1-coboundaries } \mathrm{Gal}_K \to A\}}.$$

For example, given $P \in E(K)$, we get some 1-cocycles ξ which depend on a choice of Q; the cocycle ξ gives rise to a well defined cohomology class $[\xi] \in H^1(K, E[m])$ (see Equation (7)).

Group cohomology has many desirable properties:

- (Functoriality) given a homomorphism $\varphi\colon A \to B$ of Gal_K-modules, we obtain a homomorphism

  $$\varphi\colon H^1(K, A) \to H^1(K, B)$$

  sending $[\xi] \mapsto [\varphi \circ \xi]$.

- If we have an exact sequence

  $$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$$

  of Gal_K-modules then we obtain an exact sequence

  $$0 \longrightarrow A^{\mathrm{Gal}_K} \xrightarrow{\varphi} B^{\mathrm{Gal}_K} \xrightarrow{\psi} C^{\mathrm{Gal}_K} \xrightarrow{\delta} H^1(K, A) \xrightarrow{\varphi} H^1(K, B) \xrightarrow{\psi} H^1(K, C)$$

  The map δ is called the *connecting homomorphism*: for $c \in C^{\mathrm{Gal}_K}$, choose $b \in B$ so that $\psi(b) = c$; then for any $\sigma \in \mathrm{Gal}_K$, we have $c = \sigma(c) = \psi(\sigma(b))$, so $\psi(\sigma(b) - b) = 0$; it follows that $\sigma(b) - b = \varphi(\xi_\sigma)$ for a unique $\xi_\sigma \in A$. This gives a 1-cocycle $\xi\colon \mathrm{Gal}_K \to A$, and $\delta(c) = [\xi]$.

Remark 3.23.4. This is a special case of group cohomology for profinite groups. (As with other cohomology theories, there are higher cohomology groups, and so on.) △

For E/K, the exact sequence

$$0 \longrightarrow E[m] \longrightarrow E \xrightarrow{P \mapsto mP} E \longrightarrow 0$$

gives rise to the exact sequence

$$0 \longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{P \mapsto mP} E(K) \xrightarrow{\delta} H^1(K, E[m]) \longrightarrow H^1(K, E) \xrightarrow{P \mapsto mP} H^1(K, E)$$

and hence an exact sequence

$$0 \longrightarrow E(K)/mE(K) \hookrightarrow H^1(K, E[m]) \longrightarrow H^1(K, E)[m] \longrightarrow 0$$

The hope is to show that $H^1(K, E[m])$ is finite, because then we'd automatically conclude that $E(K)/mE(K)$ is finite. The problem is that it's infinite. So next time, we'll construct a *finite* group $\mathrm{Sel}^m(E/K) \subseteq H^1(K, E[m])$ that contains the image of $E(K)/mE(K)$.

This smaller group is obtained by considering local conditions, i.e. looking at K_v will force strong conditions on the cocycles that can occur, and cut out the group $\mathrm{Sel}^m(E/K)$.

3.24 May 5, 2020 (Number fields)

Last time we considered E/K with K a number field. For $m \geq 2$, we found an exact sequence of groups

$$0 \longrightarrow E(K)/mE(K) \hookrightarrow H^1(K, E[m]) \longrightarrow H^1(K, E)[m] \longrightarrow 0$$

We want to show $E(K)/mE(K)$ is finite; the idea is to construct a finite group $H^1(K, E[m])$ containing the image.

Definition 3.24.1. A *place* of K is an equivalence class of absolute values on K that do not induce the discrete topology. △

(An absolute value is a map $|\cdot|\colon K \to \mathbb{R}$ satisfying $|x| \geq 0$, with $|x| = 0$ if and only if $x = 0$, as well as $|xy| = |x||y|$ and $|x + y| \leq |x| + |y|$. Absolute values are equivalent if they induce the same topology on K.)

Let v be a place. We denote by K_v the completion of K with respect to the absolute value.

There are two kinds of places, namely:

- *Archimedean*: those coming from an embedding $\sigma\colon K \hookrightarrow \mathbb{C}$ given by $|x|_v \stackrel{\text{def}}{=} |\sigma(x)|$, i.e. stealing it from $\mathbb{C}$,
- *Non-Archimedean*: those coming from a nonzero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. The localization $\mathcal{O}_K$ at $\mathfrak{p}$ is a discrete valuation ring, hence comes with a valuation $\operatorname{ord}_P\colon K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ with $|x|_{\mathfrak{p}} \stackrel{\text{def}}{=} (\#\mathcal{O}_K/N(\mathfrak{p}))^{-\operatorname{ord}_P(x)}$. Non-Archimedean absolute values come with a *strong triangle inequality*, which says $|x+y|_{\mathfrak{p}} \leq \max\{|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}\}$.

For $K = \mathbb{Q}$, the completions are $\mathbb{Q}_p$ and $\mathbb{Q}_\infty = \mathbb{R}$. [This is Ostrowski.]

So let v be a place with an absolute value $|\cdot|_v$ and let K_v be the completion with respect to $|\cdot|_v$. Choose $\overline{K_v}$ and an embedding $\overline{K} \hookrightarrow \overline{K_v}$. We have a map

$$\begin{aligned} \operatorname{Gal}_{K_v} = \operatorname{Gal}(\overline{K_v}/K_v) &\hookrightarrow \operatorname{Gal}(\overline{K}/K) = \operatorname{Gal}_K \\ \sigma &\mapsto \sigma|_{\overline{K}}. \end{aligned}$$

Thus we can view $\operatorname{Gal}_{K_v} \subseteq \operatorname{Gal}_K$ that is well defined up to conjugacy. We have an inertia subgroup $I_v \subseteq \operatorname{Gal}_{K_v}$.

For any place v, we have a commuting diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(K, E[m]) & \longrightarrow & H^1(K, E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(K_v)/mE(K_v) & \longrightarrow & H^1(K_v, E[m]) & \longrightarrow & H^1(K_v, E)[m] & \longrightarrow & 0 \end{array}$$

where the horizontal rows are the exact sequences discussed last time. The first vertical map comes from the standard inclusion $K \hookrightarrow K_v$ and the third vertical map is given by restricting a 1-cocycle $\xi\colon \operatorname{Gal}_K \to E(\overline{K})$ to $\operatorname{Gal}_{K_v} \to E(\overline{K}) \subseteq E(\overline{K}_v)$.

We can combine these commuting diagrams to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(K, E[m]) & \longrightarrow & H^1(K, E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(K_v)/mE(K_v) & \longrightarrow & \prod_v H^1(K_v, E[m]) & \longrightarrow & \prod_v H^1(K_v, E)[m] & \longrightarrow & 0 \end{array}$$

where the product runs over all places.

We have a map

$$H^1(K, E[m]) \to \prod_v H^1(K_v, E)[m]$$

given by composing $H^1(K, E[m]) \to H^1(K, E)[m] \to \prod_v H^1(K_v, E)[m]$.

Definition 3.24.2. The *m-Selmer group* of $E(K)$ is

$$\mathrm{Sel}^m(E/K) = \ker(H^1(K, E[m]) \to \prod_v H^1(K_v, E)). \qquad \triangle$$

Observe that $E(K)/mE(K)$ sits inside m-Selmer group. The claim is $\mathrm{Sel}^m(E/K)$ is finite; this would imply the weak Mordell-Weil theorem.

Definition 3.24.3. The *Tate-Shafarevich group* of E/K is

$$Ш(E/K) \stackrel{\text{def}}{=} \ker(H^1(K, E) \to \prod_v H^1(K_v, E)). \qquad \triangle$$

Exercise : There is a short exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow \mathrm{Sel}^m(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0$$

The following conjecture is very important (and very hard):

Conjecture 3.24.4. *The Tate-Shafarevich group $Ш(E/K)$ is finite.*

This would imply, for p large enough, that $\mathrm{Sel}^p(E/K) \cong E(K)/pE(K)$.

Let S be the (finite!) set of places v of K such that v is Archimedean, or $v|m$, or E has bad reduction at v.

Lemma 3.24.5. *Let $v \notin S$. Consider a 1-cocycle $\xi\colon \mathrm{Gal}_{K_v} \to E[m]$ such that $[\xi] = 0$ in $H^1(K_v, E)$. Then $\xi(I_v) = 0$.*

Proof. There is $Q \in E(\overline{K_v})$ such that $\xi_\sigma = \sigma Q - Q$ for all $\sigma \in \mathrm{Gal}_{K_v}$ (This is the definition of $[\xi] = 0 \in H^1(K_v, E)$). Take $\sigma \in I_v$, and consider the reduction map

$$E(\overline{K_v}) \to \widetilde{E}(\overline{k_v}),$$

where k_v is the residue field of K_v, and $\widetilde{E}$ is the reduction of E at v (which is necessarily good).

The left side $E(\overline{K_v})$ has a Gal_{K_v} action and the right side $\widetilde{E}(\overline{k_v})$ has a Gal_{k_v} action and these actions are compatible with the reduction map.

Note that σQ and Q have the same reduction since $\sigma \in I_v$. Thus, $\xi_\sigma = \sigma Q - Q$ and $\mathcal{O}$ have the same reduction. But $\xi_\sigma \in E[m]$ and we have an isomorphism $E[m] \xrightarrow{\sim} \widetilde{E}[m]$ given by reduction (this uses that v is good and $v \nmid m$). It follows that $\xi_\sigma = \mathcal{O}$. □

Theorem 3.24.6. *The m-Selmer group $\mathrm{Sel}^m(E/K)$ is finite.*

Proof. For any $[\xi] \in \mathrm{Sel}^m(E/K)$, we have $\xi\colon \mathrm{Gal}_K \to E[m]$ and $\xi(I_v) = 0$ for all $v \notin S$ by Lemma 3.24.5. Let $K' := K(E[m])$ and observe that $E[m] \subseteq E(K')$. We have a homomorphism of groups

$$\xi' := \mathrm{Gal}_{K'} \to E[m]$$

because $\xi'_{\sigma\tau} = \xi'_\sigma + \sigma(\xi'_\tau) = \xi'_\sigma + \xi'_\tau$. Let L be the subfield of $\overline{K}$ fixed by $\ker(\xi)$; note that L/K' is a Galois extension with a homomorphism $\mathrm{Gal}(L/K) \hookrightarrow E[m]$.

For any $v \notin S$, the action $I_v \circlearrowright E[m]$ is trivial, because E has good reduction at v and $v \nmid m$. It follows that $I_v \subseteq \mathrm{Gal}_{K'}$. Thus, $\xi'(I_v) = \xi(I_v) = 0$, and hence $I_v \subseteq \mathrm{Gal}_L$ for all $v \notin S$. Thus L/K is unramified at $v \in S$ and $[L : K] = [L : K'][K' : K] \leq m^2[K' : K]$. Now, we apply

Theorem 3.24.7 (Hermite-Minkowski; Proposition 4.27 in Mehrle's 6370 notes)**.** *Given $n \geq 1$ and a finite set of places S of K, there are only finitely many L/K of degree n that are unramified at $v \notin S$.*

In our case, there are only finitely many L/K, so there are only finitely many $\xi'\colon \mathrm{Gal}_{K'} \to E[m]$, so there are only finitely many $\xi\colon \mathrm{Gal}_K \to E[m]$. Therefore, $\mathrm{Sel}^m(E/K)$ is finite. □

Let us end by remarking that in the short exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow \mathrm{Sel}^m(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0$$

the middle group $\mathrm{Sel}^m(E/K)$ is computable. On the other hand, there is no known algorithm to compute either of the other two groups.

Next time, we'll give a geometric description of $Ш(E/K)$ and talk about heights.

3.25 May 7, 2020 (Number fields)

Last time, we studied elliptic curves E over number fields K. For $m \geq 2$, we have an exact sequence

$$0 \longrightarrow E(K)/mE(K) \hookrightarrow \text{Sel}^m(K, E[m]) \longrightarrow Ш(E/K)[m] \longrightarrow 0$$

Here, $Ш(E/K)$ is the *Tate-Shafarevich group* defined by $Ш(E/K) = \ker(H^1(K, E) \to \prod_v H^1(K_v, E))$. Let's give a geometric description.

Definition 3.25.1. A *principal homogeneous space* or *torsor* for E/K is a nice curve C/K with a morphism $\mu\colon C \times E \to C$ defined over K that gives a simply transitive action of E on C, i.e.

- $\mu(x, 0) = x$ for all $x \in C$
- $\mu(\mu(x, P), Q) = \mu(x, P + Q)$ for $x \in C$ and $P, Q \in E$
- For all $x, y \in C$ there is a unique $P \in E$ such that $\mu(x + P) = y$.

△

Remark 3.25.2. Let C be a torsor for E/K. Then C and E are isomorphic over $\overline{K}$, hence C is nice and has genus 1. (The isomorphism $E \xrightarrow{\sim} C$ is given by $P \mapsto x + P$.) △

We say two torsors C_1 and C_2 of E are *equivalent* if there exists an isomorphism $\varphi\colon C_1 \xrightarrow{\sim} C_2$ satisfying $\varphi(x + P) = \varphi(x) + P$.

Now fix a point $x_0 \in C$, and let $\varphi\colon E \xrightarrow{\sim} C$ given by $P \mapsto x_0 + P$. For $\sigma \in \text{Gal}_K$ we get another isomorphism

$$\begin{aligned} \sigma(\varphi)\colon E &\xrightarrow{\sim} C \\ P &\mapsto \sigma(x_0) + P. \end{aligned}$$

We have

$$\begin{aligned} \xi_\sigma := \varphi^{-1} \circ \sigma(\varphi)\colon E &\xrightarrow{\sim} E \\ P &\mapsto (\sigma(x_0) - x_0) + P. \end{aligned}$$

Note that $\sigma(x_0) - x_0$ is the unique point $Q \in E$ such that $x_0 + Q = \sigma(x_0)$.

Exercise : The map $\xi\colon \text{Gal}_K \to E$ is a 1-cocycle.

Fact 3.25.3. *The map*

$$\begin{aligned} \{\text{torsors of } E/K \text{ up to equivalence}\} &\to H^1(K, E) \\ C &\mapsto [\xi] \end{aligned}$$

is a bijection.

(The *Weil-Châtelat group* for E is the left hand side with an explicit group operation; these were studied before group cohomology.)

Lemma 3.25.4. *Let C be a torsor of E. Then C corresponds to $0 \in H^1(K, E)$ in the bijection above if and only if $C(K) \neq \emptyset$.*

Proof. The forward direction proceeds as follows. The identity corresponds to $E \times E \to E$ given by $(P, Q) \mapsto P + Q$. If C is equivalent to E, then $C \cong E$ over K, and $C(K) \neq \emptyset$.

To prove the backwards direction, we fix $x \in C(K)$. Then we get an isomorphism

$$\begin{aligned} \varphi\colon E &\xrightarrow{\sim} C \\ P &\mapsto x + P \end{aligned}$$

is a morphism defined over K, and this is an equivalence. □

Issue in computations with $H^1(K, E)$.

Let C/K be a nice curve of genus 1. There is no known algorithm to determine if $C(K) \neq \emptyset$ or not. (There are conjectured ways to do this.) In particular, it's difficult to prove that $C(K)$ has no points. (One way to do this is as follows: if v is a place of K and $C(K_v) \neq \emptyset$, then $C(K) = \emptyset$.)

In light of the bijection from torsors to H^1, we see that

$$Ш(E/K) = \ker(H^1(K, E) \to \prod_v H^1(K_v, E))$$

corresponds to torsors C of E/K, up to equivalence, such that $C(K_v) \neq \emptyset$ for all places v of K. Thus Ш can be thought of those torsors for which there are local points but not global points.

Aside 3.25.5. Given C one can check if $C(K_v) \neq \emptyset$ for all v. For most v, reduction gives a smooth model with points that will lift to $C(K_v)$, by Hensel's lemma. △

Let $[\xi] \in H^1(K, E[m])$. This gives rise to an element in $H^1(K, E)$ and hence a torsor C. Then $[\xi] \in \text{Sel}^m(E/K)$ if and only if $C(K_v) \neq \emptyset$ for all v, and $[\xi] \in \text{img} E(K)/mE(K)$ if and only if $C(K) \neq \emptyset$.

Let's give an overview of 2-descent via an explicit example:

Example 3.25.6 (Explicit 2-descent, i.e. m=2)**.** Let $E/\mathbb{Q}$ be an elliptic curve with $E[2] \subseteq E(\mathbb{Q})$. Thus

$$E/\mathbb{Q} : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

for $e_i \in K$. We have $E[2] = \{\mathcal{O}, \underbrace{(e_1, 0)}_{=P_1}, \underbrace{(e_2, 0)}_{=P_2}, (e_3, 0)\}$, so $E[2] = \langle P_1 \rangle \oplus \langle P_2 \rangle$. We have

$$\begin{aligned} H^1(\mathbb{Q}, E[2]) &\simeq H^1(\mathbb{Q}, \langle P_1 \rangle) \times H^1(\mathbb{Q}, \langle P_2 \rangle) \\ &\simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2. \end{aligned}$$

The cocyles in $H^1(\mathbb{Q}, E[2])$ are homomorphisms since $E[2] \subseteq E(\mathbb{Q})$.

We have

$$\begin{aligned} E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, E[2]) &\simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ (x, y) &\longmapsto (x - e_1, x - e_2) \end{aligned}$$

(If $x = e_1$ or $x = e_2$, there's a different description.)

Now let $S = \{-1, 2\} \cup \{p : \ E \text{ has bad reduction at } p\}$; this is a finite set. We have

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \langle S \rangle \times \langle S \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

For $(a \cdot (\mathbb{Q}^\times)^2, b \cdot (\mathbb{Q}^\times)^2)$, the corresponding torsor of $E/\mathbb{Q}$ is

$$C_{a,b}/\mathbb{Q} : \begin{cases} x - e_1 = az_1^2 \\ x - e_2 = bz_2^2 \\ x - e_3 = abz_3^2 \end{cases}$$

whose projective closure defines a nice genus 1 curve in $\mathbb{P}^4_{\mathbb{Q}}$.

For example, if $y^2 = x^3 - x = (x+1)(x-0)(x-1)$, we have $e_1 = -1$ and $e_2 = 0$. Furthermore, $S = \{-1, 2\}$ and $\langle S \rangle = \{\pm 1, \pm 2\} \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. We get

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \langle S \rangle \times \langle S \rangle;$$

where $\langle S \rangle \times \langle S \rangle$ has 16 elements. Furthermore, $E[2] \subseteq E(\mathbb{Q})/2E(\mathbb{Q})$ embeds into $\{(1, 1), (2, -1), (2, 1), (1, -1)\}$, which has order 4.

Now we look at $C_{a,b}/\mathbb{Q}$ as defined above with $a, b \in \{\pm 1, \pm 2\}$. One can check:

Exercise : Show $E(\mathbb{Q})/2E(\mathbb{Q})$ has order 4 by checking when $C_{a,b}(\mathbb{R}) \neq \emptyset$ and $C_{a,b}(\mathbb{Q}_2) \neq \emptyset$.

Since $E(\mathbb{Q})_{\text{tors}} = E[2]$, we see that the rank is zero. △

Let's talk a little about heights. Take a point $P \in \mathbb{P}^n(\mathbb{Q})$, say with $P = [x_0, \dots, x_n]$. Since $\mathbb{Z}$ is a UFD, we can assume $x_i \in \mathbb{Z}$ and $\gcd(x_0, \dots, x_n) = 1$. (This uses $\mathbb{Z}^\times = \{\pm 1\}$.) We define the height

$$H(P) \stackrel{\text{def}}{=} \max\{|x_0, \dots, |x_n|\}.$$

For a number field K, this doesn't work, because $\mathcal{O}_K$ need not be a UFD, and $\mathcal{O}_K^\times$ can be infinite. So we give an alternate description:

Take any place v of K. Choose an absolute value $|\cdot|_v \colon K \to \mathbb{R}$: if the absolute value is non-archimedean and v corresponds to the prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, we set

$$|x|_v := (\#\mathcal{O}_K/\mathfrak{p})^{-\operatorname{ord}_\mathfrak{p}(x)},$$

and if the absolute value is archimedean and v corresponds to an embedding $\sigma \colon K \hookrightarrow \mathbb{C}$, we set

$$\begin{aligned} |x|_v &= |\sigma(x)| && \text{if } K_v = \mathbb{R} \\ &= |\sigma(x)|^2 && \text{if } K_v = \mathbb{C}. \end{aligned}$$

(This is technically not an absolute value, but that's fine.)

We choose these absolute values because we have the *product formula*, which says for any $x \in K^\times$,

$$\prod_v |x|_v = 1.$$

Exercise : Check this for $K = \mathbb{Q}$. (If you know number theory, you can prove the general case by using the $K = \mathbb{Q}$ case and $N_{K/\mathbb{Q}}(x)$.)

In this generality, the *height function*

$$H_K([x_0, \dots, x_n]) = \prod_v \max\{|x_0|_v, \dots, |x_n|_v\},$$

which is well defined! (The formula above assigns to $[\lambda x_0, \dots, \lambda x_n]$ the number

$$\underbrace{\prod_v \max\{|x_0|_v, \dots, |x_n|_v\}}_{=x} \cdot \underbrace{\prod_v |\lambda|_v\}}_{=1},$$

where we have used the product formula.)

Fact 3.25.7. *Let L be a finite extension of K. Then*

$$H_L(P)^{\frac{1}{[L:\mathbb{Q}]}} = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}.$$

This gives rise to a notion of *absolute height* $H \colon \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 1}$ given by $H(P) = H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$, where $P \in \mathbb{P}^n(K)$.

Theorem 3.25.8. *For any $C > 0$ and $d > 0$, the set*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \colon H(P) \leq C \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

is finite. In particular, $\{P \in \mathbb{P}^n(K) \colon H(P) \leq C\}$ is finite.

The (absolute logarithmic) height is $h = \log \circ H \colon \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$.

Let E/K be an elliptic curve and fix a nonconstant $f \in K(E)$ that is even, so $f(-P) = f(P)$. (For example, take the x-coordinate of a model $y^2 = x^3 + ax + b$.)

The *height* of E relative to $f \colon E \to \mathbb{P}^1_K$ is given by

$$\begin{aligned} h_f \colon E(\overline{K}) &\to \mathbb{R}_{\geq 0} \\ P &\mapsto h(f(P)). \end{aligned}$$

The map h_f satisfies the following properties:

- The set $\{P \in E(K) \colon h_f(P) \le C\}$ is finite for all C.
- There is $C_1 > 0$ such that

$$|h_f(P+Q) - h_f(P-Q) - 2h_f(P) - 2h_f(Q)| \le C_1$$

  for all $P, Q \in E(\overline{K})$. (This means h_f acts kind of like a quadratic form.)
- Fix $Q \in E(\overline{K})$. There exists $C_2 > 0$ such that

$$h_f(P+Q) \le 2h_f(P) + C_2.$$

- For $m \ge 2$, there is $C_3 > 0$ such that

$$|h_f(mP) - m^2 h_f(P)| \le C.$$

The second property uses crucially that f is even; the third and fourth properties are easy consequences of the second.

There is a related notion of the *Néron-Tate height* $\hat{h} \colon E(\overline{K}) \to \mathbb{R}_{\ge 0}$ given by

$$\hat{h}(P) = \frac{1}{\deg f} \lim_{m \to \infty} \frac{1}{m^2} h_f(mP).$$

A miraculous fact is that the limit exists and is independent of f. Furthermore, we have the properties

- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$
- $\hat{h}(mP) = m^2 \hat{h}(P)$
- $\hat{h}(P) = 0$ if and only if P is torsion.

We obtain a bilinear pairing $\langle \cdot, \cdot \rangle \colon E(\overline{K}) \times E(\overline{K}) \to \mathbb{R}$ given by

$$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

which gives an inner product on

$$E(K)/E(K)_{\text{tors}},$$

which is a free abelian group in the lattice $\mathbb{R} \otimes E(K)$. We may take the covolume of this lattice (i.e. the volume of the fundamental domain), which is called the *elliptic regulator*, denoted $R_{E/K}$.

Next time, we'll have a computer showcase, and see the full version of the Birch and Swinnerton-Dyer conjecture.

3.26 May 12, 2020 ($\mathbb{Q}$)

Let E be an elliptic curve over $\mathbb{Q}$. We know that the group $E(\mathbb{Q})$ is finitely generated! The torsion part $E(\mathbb{Q})_{\text{tors}}$ is computable, and the *rank* r of $E(\mathbb{Q})$ is mysterious.

Let p be a prime for which E has *good reduction* (i.e. good reduction over $\mathbb{Q}_p$). We have a finite group $E(\mathbb{F}_p)$, and a number $a_p(E)$ defined by

$$\#E(\mathbb{F}_p) = p - a_p(E) + 1.$$

Then Hasse proved $|a_p(E)| \le 2\sqrt{p}$ (Theorem 2.13.7).

In the early 1960's, Swinnerton-Dyer used a computer to calculate some values of

$$\prod_{\substack{p \le x \\ p \text{ good}}} \frac{|E(\mathbb{F}_p)|}{p}.$$

His initial conjecture, with Birch, was that

$$\prod_{\substack{p \le x \\ p \text{ good}}} \frac{|E(\mathbb{F}_p)|}{p} \sim C(\log x)^r,$$

so we would be able to compute ranks of elliptic curves by just looking $\mathbb{F}_p$-points.

Note that

$$\frac{|E(\mathbb{F}_p)|}{p} = 1 - a_p(E) \cdot p^{-1} + p \cdot (p^{-1})^2,$$

which can be obtained by evaluating the familiar polynomial $1 - a_p(E)x + px^2$ at $x = \frac{1}{p}$.

The L-function of E

Given an elliptic curve E, we may define the L-function associated to E as a product

$$L(E, s) \stackrel{\text{def}}{=} \prod_{p \text{ prime}} \frac{1}{P_p(p^{-s})}$$

where $P_p(x) \in \mathbb{Z}[x]$ is defined in the following way: Take $\ell \neq p$, and observe that $\text{Gal}_{\mathbb{Q}_p} \circlearrowright V_\ell(E)$. We have a subgroup $I_p \subseteq \text{Gal}_{\mathbb{Q}_p}$, and hence an action $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \text{Gal}_{\mathbb{Q}_p}/I_p \circlearrowright V_\ell(E)^{I_p}$. In particular, there is $\text{Frob}_p \in \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$; then

$$P_p(x) \stackrel{\text{def}}{=} \det(I - x \cdot \text{Frob}_p | V_\ell(E)^{I_p}).$$

Explicitly:

- If E has good reduction at p, then $P_p = 1 - a_p(E)x + px^2$
- If E has split multiplicative reduction at p, then $P_p(x) = 1 - x$
- If E has nonsplit multiplicative reduction at p, then $P_p(x) = 1 + x$
- If E has additive reduction at p, then $P_p(x) = 1$.

Exercise : Use the Hasse bound to show $L(E, s)$ is holomorphic for $s \in \mathbb{C}$ with $\text{Re}(s) > 3/2$.

Theorem 3.26.1 (Modularity). *[Due to Wiles,Taylor, Breuil, Conrad, Diamond] The function $L(E, s)$ extends to a holomorphic function on $\mathbb{C}$. In particular, the quantity $\text{ord}_{s=1} L(E, s)$ is defined.*

Conjecture 3.26.2 (Birch & Sinnerton-Dyer)**.**

i) We have

$$\text{ord}_{s=1} L(E, s) = r,$$

where r is the rank of E.

ii) We have

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}=\frac{|Ш|\cdot\Omega\cdot R\cdot\prod_p c_p}{|E(\mathbb{Q})_{\text{tors}}|^2},$$

where:

- $Ш = Ш(E/\mathbb{Q})$ *is the Tate-Shafarevich group (conjecturally finite),*
- Ω *is the* real period*, obtained from a minimal model* $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ *via the formula*

$$\Omega=\#(\text{connected components of } E(\mathbb{R}))\times\int_{E(\mathbb{R})^0}\frac{dx}{2y+a_1x+a_3}\in\mathbb{R},$$

- R *is* 2^r *times the elliptic regulator from last class, and*
- c_p *is the Tamagawa number, given by* $c_p=[E(\mathbb{Q}_p):E_0(\mathbb{Q}_p)]$

Note how BSD relates many constants together into an equation; it bears striking resemblance to the *class number formula* from algebraic number theory (Theorem 7.13 in Mehrle's 6370 notes), with Ш playing the role of the class number.

Thus the conjecture says that the numbers $a_p(E)$ know the value of r and give a way to compute it.

You can actually compute $L(E,1)$: we have

$$L(E,s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}\qquad(a_n\in\mathbb{Z}),$$

so

$$L(E,1)=(1+\varepsilon)\sum_{n=1}^{\infty}\frac{a_n}{n}e^{-2\pi n/\sqrt{N}},$$

where N is the *conductor* (some positive integer) and $\varepsilon\in\{\pm1\}$ is the root number. (Both N and ε are computable.)

If $\varepsilon=-1$, then $L(E,1)=0$. Then BSD predicts that $E(\mathbb{Q})$ is infinite.

Example 3.26.3. Let $E/\mathbb{Q}$ be given by $y^2+y=x^3-x^2$. We have $\Delta=11$ and $r=0$. Furthermore, $E(\mathbb{Q})_{\text{tors}}=\{\mathcal{O},(0,0),(0,-1),(1,0),(1,-1)\}\cong\mathbb{Z}/5\mathbb{Z}$. It turns out that $R=1$, $\Omega=6.34604\ldots$, $\prod_p c_p=1$, and $L(E,1)=0.25384\ldots$. Thus

$$|Ш|\overset{\text{BSD}}{=}\frac{L(E,1)\cdot|E(\mathbb{Q})_{\text{tors}}|^2}{\Omega\cdot R\cdot\prod_p c_p}\approx 1.$$

Thus we expect $Ш=0$. △

Theorem 3.26.4 (Kolyvagin, 1989)**.** *If* $\text{ord}_{s=1}L(E,s)\le 1$*, then BSD holds and* Ш *is finite.*

Theorem 3.26.5 (Gross-Zagier, 1986)**.** *Suppose* $\text{ord}_{s=1}L(E,s)=1$*. They give a way to construct a point in* $E(\mathbb{Q})$ *of infinite order. See Heegner points.*

Example 3.26.6. Question. Are there any right angle triangles with rational side lengths and area 101?

In other words (after projectivizing), we are searching for rational solutions to the set of equations

$$\begin{cases}a^2+b^2=c^2\\ \frac{1}{2}ab=101d^2\end{cases}$$

which defines a curve $C\subseteq\mathbb{P}^3_{\mathbb{Q}}$ that is nice of genus 1. Observe that

$$C(\mathbb{Q})\supseteq\{[0,1,\pm1,0],[1,0,\pm1,0]\}.$$

Now let $E/\mathbb{Q}$ be the elliptic curve given by C with $\mathcal{O}=[0,1,1,0]$. It turns out that E is isomorphic to the curve given by $E'/\mathbb{Q}:y^2=x^3-101^2x$. It turns out that $E'(\mathbb{Q})_{\text{tors}}=E[2]$.

Thus, there is such a triangle if and only if the rank of $E'(\mathbb{Q})$ is nonzero. (In this case, $\varepsilon = -1$ so BSD predicts that the rank is at least 1.)

We saw [live(!!!)] that the Mordell-Weil group $E(\mathbb{Q})$ of E is $\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2$; the "simplest" (lowest height) point of infinite rank is

$$[a, b, c] = \Big[\frac{267980280100}{44538033219}, \frac{44538033219}{1326635050}, \frac{2015242462949760001961}{59085715923689725950}\Big]. \qquad \triangle$$

More generally, the congruent number problem says the following. Fix $n \geq 1$ a squarefree integer. There is a right angle triangle with rational sides and area n if and only if E has rank at least 1, where

$$E/\mathbb{Q} : y^2 = x^3 - n^2 x.$$

This implies $L(E, 1) = 0$ by Theorem 3.26.4; the converse is BSD. Theorems of Tunnell, Shimura, and Waldspurger say that $L(E, 1) = 0$ if and only if the n-th term of a certain q-expansion vanishes:

Theorem 3.26.7 (Tunnell, 1983)**.** *Suppose n is an odd squarefree integer. If n is the area of a right angle triangle with rational side lengths, then*

$$\#\{(x, y, z) \in \mathbb{Z}^3 \colon n = 2x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{(x, y, z) \in \mathbb{Z}^3 \colon n = 2x^2 + y^2 + 8z^2\}.$$

The converse is true conditional on BSD.

(The point is that the condition $\#\{(x, y, z) \in \mathbb{Z}^3 \colon n = 2x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{(x, y, z) \in \mathbb{Z}^3 \colon n = 2x^2 + y^2 + 8z^2\}$ is checkable.)

While the two concepts linked by Tunnell's theorem are very elementary, the math used to link them together is very modern.