Math 99r - Arithmetic of Elliptic Curves

Taught by Zijian Yao
Notes by Dongryul Kim

Fall 2017

This course was taught by Zijian Yao. The lectures were usually on Tuesdays and Thursdays, but were irregular. There was no textbook, and 8 students were enrolled.

Contents

1 September 5, 2017

I am going to give you an actual overview of the class. Let me start with a polynomial $F(x, y) \in \mathbb{Q}[x, y]$. The question is, what are the $\mathbb{Q}$-points of $F(x, y) = 0$? The projective version of this is, that for a homogeneous polynomial $F(x, y, z) \in \mathbb{Q}[x, y, z]$, what are equivalence classes of $\mathbb{Q}$-solutions here?

We can ask, for instance, what the solutions to $ax + by + c = 0$, or $aX + bY + cZ = 0$? These are easy because they are linear. So let's complicate the problem and ask for quadratic solutions. For instance, are there rational solutions to $x^2 + y^2 = 05$ or $x^2 + 4y^2 = 27$? In the quadratic case, there is the Hasse principle, which says that the equation has rational solutions if it has solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$.

Now let's move to cubic equations, like

$$f(X, Y, Z) = X^3 + Y^3 + Z^3 + ?X^?Y^?Z^? + \cdots .$$

It is easy to find the $\mathbb{Q}$-points if the curve is singular; it reduces to the previous cases. So we only consider the smooth case.

Let E be this curve, and $E(\mathbb{Q})$ be the set of $\mathbb{Q}$-points.

Theorem 1.1. *$E(Q)$ is actually naturally an abelian group, and it is finitely generated.*

So what is the rank of this group? This is, by definition, the **algebraic rank** of E.

Conjecture 1.2 (Birch–Swinnerton-Dyer)**.** *The rank r can be computed by a certain L-function.*

Theorem 1.3 (Nikolav)**.** *The torsion can be computed. If $f(x, y) \in E_{\mathrm{affine}}(\mathbb{Q})_{\mathrm{tor}}$, then either $y = 0$ or $y \mid \Delta_E$. This also works for number fields.*

Theorem 1.4 (Mazur)**.** *$E(\mathbb{Q})_{\mathrm{tor}}$ is either of $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, \dots, 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4$.*

Given $E/\mathbb{Q}$, there are Tate modules we can construct,

$$\varprojlim_n E[\ell^n] = T_\ell E,$$

which has an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This $T_\ell(E)$ is a rank 2 $\mathbb{Z}_\ell$-module, and an these are the source of only Galois representations. What are the traces and determinants of this representation? It turns out that the trace of the Frobenius is going to be related to the size of $E(\mathbb{F}_\ell)$.

1.1 Elliptic curves

Let K be any field.

Definition 1.5. An **elliptic curve** $E/\overline{K}$ is a smooth projective curve $E \subseteq \mathbb{P}^2_{\overline{K}}$ of genus 1, together with an origin $O \in E(\overline{K})$.

We will later prove that $E(\overline{K})$ is naturally an abelian group with $O \in E(\overline{K})$ its origin. Another remark is that if $C/\mathbb{Q}$ is of genus $g \geq 2$, then $|C(\mathbb{Q})| < \infty$. Also, if $E/\overline{K}$ is an elliptic curve over $\overline{K}$ where $\operatorname{char} K \neq 2, 3$, then E can be cut out by $y^2 = x^3 + Ax + B$.

If we are over $\mathbb{C}$, a smooth curve is a Riemann surface, and they are classified by their genus. For instance, a genus 1 curve is a torus, and a genus 2 curve is a double torus, etc. Note that the torus can be made into an abelian group. But I will also give a definition of a genus that works over all fields, and it won't be obvious that these two notions of genus agree.

1.2 Varieties

Given an algebraically closed field $\overline{K}$, we define **affine space** to be

$$\mathbb{A}^n_{\overline{K}} = \overline{K}^n$$

as a set, and topologize $\mathbb{A}^n_{\overline{K}}$ by declaring that closed subsets are

$$V(f_1, \ldots, f_r) = \text{common solutions of } f_i$$

for $f_i \in \overline{K}[x_1, \ldots, x_n]$. This is sometimes called the **Zariski topology**. You can verify that this is a topology. But this is too coarse to actually make cohomology well-behaved. Instead you should look at the étale cohomology, $H_{\text{ét}}$. In fact,

$$H^1_{\text{ét}}(E, \mathbb{Z}_\ell)^\vee = T_\ell(E),$$

and this was one of the first examples of étale cohomology.

If $V \subseteq \mathbb{A}^n$ is an irreducible affine variety, then we define

$$I(V) = \{f \in \overline{K}[x_1, \ldots, x_n] : f(V) = 0\}.$$

When we take $V = V(\mathfrak{a})$ for an ideal $\mathfrak{a}$, we get

Lemma 1.6. *$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \{f : f^n \in \mathfrak{a}$ for some $n\}$.*

So we don't have a way to distinguish between $x = 0$ or $x^2 = 0$. We want to distinguish them, so we make a modified definition.

Definition 1.7. An **affine variety** consists of the pair $(V(\mathfrak{a}), \overline{K}[x_1, \ldots, x_n]/\mathfrak{a})$.

This ring $\overline{K}[x_1, \ldots, x_n]/\mathfrak{a}$ is the ring of functions defined over the variety. This is because we look at all possible functions and quotient out be all stuff that restricts to zero.

2 September 7, 2017

Usually I will not prove the technical parts in class, or it will take an absurd amount of time or I will have to go absurdly fast. The goal today is to do more algebraic geometry and then define elliptic curves.

I'm going to work with $\mathbb{C}$ or $\overline{K}$ for simplicity. An affine variety is a pair $(X, \mathscr{O}_X)$, where $\mathscr{O}_X$ is a sheaf that associates to each open subset the functions defined on it. What we are interested in this class is projective varieties. These are zero loci of homogeneous polynomials, inside $\mathbb{P}^n$. This projective space is

$$\mathbb{P}^n = \{(x_0, \dots, x_n) \in \overline{K}^{n+1} \setminus \{0\}\}/\sim,$$

quotiented out by nonzero scalar multiplication. But then it is more difficult to specify the functions on this space.

What are functions on $\mathbb{P}^1$? Not all homogeneous polynomials work. For instance, the function

$$f(x_0, x_1) = x_0^2 + x_1^2$$

is not well-defined. But it makes sense to ask about the vanishing locus of f.

So how are we going to study projective varieties? Each projective variety can be covered by affine varieties. The projective space $\mathbb{P}^1$ can be covered by

$$\mathbb{A}^1 = \{(x_0 : x_1) : x_0 \neq 0\} = \{(1 : x_1/x_0) : x_0 \neq 0\},$$
$$\mathbb{A}^1 = \{(x_0 : x_1) : x_0 \neq 0\} = \{(x_0/x_1 : 1) : x_1 \neq 0\}.$$

Given an affine variety like $V(y^2 - x^3 - x) \subseteq \mathbb{A}^2$, you can add some points to make it a projective variety in $\mathbb{P}^2$. Because this is a degree 3 equation, you can introduce a third variable and make it projective:

$$V(Y^2Z - X^3 - XZ^2) \subseteq \mathbb{P}^2.$$

2.1 Rational functions and dimension

Given an affine variety, the regular functions on that variety is the ring of regular functions on it. If $X = V(\mathfrak{a})$ is irreducible, or $\mathfrak{a}$ is prime, then the ring $\overline{K}[V]$ is an integral domain. So we can define the **rational functions** as

$$\overline{K}(V) = \operatorname{Frac}(\overline{K}[V]) = \Big\{\frac{\varphi}{\phi} : \varphi, \phi \in \overline{K}[V], \phi \neq 0\Big\}.$$

This is the analogue of meromorphic functions.

What if X is projective? In this case, the rational functions on X is

$$\Big\{\frac{\varphi}{\phi} : \varphi, \phi \text{ are homogeneous polynomials of same degree in } \overline{K}[x_0, \dots, x_n]/\mathfrak{a}\Big\}.$$

The dimension of a variety is a really difficult concept in algebraic geometry. But we more or less know the dimension once we see it. In the notes I gave the laziest definition of dimension.

There is a topological dimension, which is the length of the longest chain of irreducible closed subsets. You can also define it as the transcendental degree of the field of rational functions. It is the theorem that these two notions agree.

2.2 Curves

A **curve** is an irreducible 1-dimensional non-singular projective variety. From now on, I want you to think of it as a discrete valuation ring.

Definition 2.1. A **discrete valuation ring** or a **DVR** is a ring with a discrete valuation

$$v : R - \{0\} \to \mathbb{Z}_{\geq 0}$$

that looks like a logarithm of a norm.

Example 2.2. The ring $\mathbb{C}[[x]]$ is a DVR with the valuation

$$\mathbb{C}[[x]] - \{0\} \to \mathbb{Z}_{\geq 0}; \quad \sum_{n \geq 0} a_n x^n \mapsto \min\{n : a_n \neq 0\}.$$

This is the order of the function at 0.

Theorem 2.3. *Being nonsingular and dimension* 1 *at a point is equivalent to* $\mathscr{O}_{X,p}$ *being a DVR, which is also equivalent to being able to talk about the order of zeros of functions.*

For instance, in the variety $V(xy) \subseteq \mathbb{A}^2$, the order of $x^3 + xy = x^3$ at $(0, 0)$ is not very well defined.

Lemma 2.4. *Every rational map from a curve to another curve is actually regular.*

Lemma 2.5. *Any morphism* $\varphi : C_1 \to C_2$ *is either* 0 *or surjective.*

Theorem 2.6. *The following descriptions are equivalent over any* $\overline{K}$ *with* char $\neq 2, 3$*:*

(1) A curve given by $y^2 = x^3 + ax + b$ *such that* $\Delta \neq 0$

(2) A non-singular cubic curve in $\mathbb{P}^2$ *with a point* O

(3) A non-singular curve in $\mathbb{P}^2$ *of genus* 1 *together with a point* O*, i.e., and elliptic curve.*

It is quite clear that (1) implies (2), with O being the point at infinity. (2) implies (3) is the degree-genus formula, and (3) implies (1) is Riemann–Roch.

2.3 Degree

Theorem 2.7. *(1) A non-singular cubic curve* $E \subseteq \mathbb{P}^2$ *with a point* $O \in E$ *has a canonical abelian group structure.*
(2) A non-singlar curve $E \subseteq \mathbb{P}^2$ *of genus* 1 *with a point* O *has a canonical group structure.*

We are going give these group structures differently, and these two structures coincide.

Definition 2.8. A **degree** of a map $\varphi : C_1 \to C_2$ is the cardinality of a generic fiber.

Note that because φ is not injective, it induces a pullback map

$$\varphi^* : \overline{K}(C_2) \to \overline{K}(C_1); \quad f \mapsto f \circ \varphi.$$

Since φ is non-constant, this is going to be nonzero. That is, it is a field extension.

Lemma 2.9. *The degree* $[\overline{K}(C_1) : \overline{K}(C_2)]$ *is equal to* $\deg \varphi$*.*

Now because $\overline{K}(C_2) \to \overline{K}(C_1)$ is a finite field extension, there is a norm map $\overline{K}(C_1) \to \overline{K}(C_2)$.

3 September 12, 2017

Last time we defined a curve, which is a dimension 1 non-singular projective (irreducible) variety. We also talked about the degree of a map between curves. I was planning to talk about the genus and Riemann–Roch, but we will postpone this.

Theorem 3.1. *Let $K = \overline{K}$ be a field of characteristic not equal to 2 or 3. Then the following are equivalent descriptions:*

(a) curves defined by
$$y^2 = x^3 + Ax + B$$
that is non-singular,

(b) A non-singular cubic in $\mathbb{P}^2_K$ together with a point O,

(c) A non-singular curve in $\mathbb{P}^2_K$ of genus 1 with a point O.

Let's take this as a black box now.

3.1 Group structure on an elliptic curve

We declare that three points that lie on a line add up to 0. In other words, we add two points P and Q by taking the third intersection of the curve and PQ, and reflecting it.

Why is this well-defined? By Bezout's theorem, a degree m curve and a degree n curve intersect "generically" at mn points. This means that the intersection of the curve and the line PQ is, generically, three points.

So write the third intersection point as $\#(P, Q)$. We are going to now define

$$+ : E \times E \to E; \quad P + Q = \#(O, \#(P, Q)).$$

We need check that this is a group. We also want to check that + is a morphism.

Well it is clear that O is a group identity, and there is the inverse $-P = \#(O, P)$. For associativity, you need the following lemma.

Lemma 3.2. *If $\ell = \ell_1 \amalg \ell_2 \amalg \ell_3 \in \mathbb{P}^2$ and $h = h_1 \amalg h_2 \amalg h_3 \in \mathbb{P}^2$ be three lines, so that $\ell \cap h = \{P_1, \dots, P_9\}$. If a (non-singular) cubic in $\mathbb{P}^2$ goes through 8 of these, then it goes through them all.*

If you think hard, you will see that this proves associativity. So we almost have a canonical abelian group structure on the curve E.

3.2 Divisors

I'm going to give you an incorrect definition.

Definition 3.3. A **divisor** D on a curve C is a (finite) formal sum $D = \sum_{P \in C} n_P[P]$ for $n_P \in \mathbb{Z}$.

This has nothing to do with the “group structure on elliptic curve”; it is just a formal sum. For a divisor D, we define

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

and denote the set of divisors on C by $\mathrm{Div}(C)$. We also call $\mathrm{Div}^0(C)$ the subgroup of divisors with degree 0. This fits into the short exact sequence

$$0 \to \mathrm{Div}^0(C) \to \mathrm{Div}(C) \xrightarrow{\deg} \mathbb{Z} \to 0.$$

Definition 3.4. For a rational function $\varphi \in \overline{K}(C)^*$, define

$$\mathrm{div}(\varphi) = \sum_{P \in \mathrm{Zero}(\varphi)} n_P[P] - \sum_{Q \in \mathrm{Pole}(\varphi)} n_Q[Q].$$

Lemma 3.5. *The degree* $\deg(\mathrm{div}(\varphi)) = 0$.

Proof. A rational function is $\varphi : C \to \mathbb{P}^1$. Then $\mathrm{div} = \varphi^{-1}(0) - \varphi^{-1}(\infty)$ and so it has degree 0. □

Definition 3.6. A **principal divisor** is a divisor of the form $D = \mathrm{div}(\varphi)$ for some $\varphi \in \overline{K}(C)^*$.

Denote this subgroup by $\mathrm{PDiv}(C) \subseteq \mathrm{Div}^0(C)$. Now we can complete the picture as the following.

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathrm{PDiv}(C) \arrow[r, hook] \arrow[d, equal] & \mathrm{Div}^0(C) \arrow[r, two heads] \arrow[d, hook] & \mathrm{Pic}^0(C) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \mathrm{PDiv}(C) \arrow[r, hook] & \mathrm{Div}(C) \arrow[r, two heads] \arrow[d, two heads, "\deg"] & \mathrm{Pic}(C) \arrow[r] \arrow[d, two heads] & 0 \\
 & & \mathbb{Z} \arrow[r, equal] \arrow[d] & \mathbb{Z} \arrow[d] & \\
 & & 0 & 0 &
\end{tikzcd}$$

We will define a map

$$h : E \to \mathrm{Pic}^0(E); \quad P \mapsto [P] - [O].$$

Proposition 3.7. *h is a isomorphism of groups.*

4 September 14, 2017

Last time there was an exercise, claiming that if C_1 and C_2 are two generic cubic curves intersecting at 9 points, and another C goes through 8 of the points, then it passes through all 9 of them.

Proof. Let V be the vector space of homogeneous cubic polynomials in $\overline{K}[X_0, X_1, X_2]$. This has dimension 10. If this passes through 8 given points, then this condition cuts down the dimension to 2. Now C_1 and C_2 are linearly independent vectors in this space, so C is a linear combination of these two. □

Our ultimate goal is to show that the following are equivalent:

- $E : y^2 = x^3 + ax + b$ and $\Delta_E \neq 0$,
- cubic curve in $\mathbb{P}^2_{\overline{K}}$ with a point,
- curve of genus 1 in $\mathbb{P}^2_{\overline{K}}$ with genus 1.

We also had this map

$$h : E \to \mathrm{Pic}^0(E); \quad P \mapsto [P] - [O].$$

4.1 Discrete valuation ring

Now let $C/\overline{K}$ be any curve. We have the sequence

$$0 \to \mathrm{Div}^0(C) \to \mathrm{Div}(C) \twoheadrightarrow \mathbb{Z} \to 0.$$

There is also a partial order on $\mathrm{Div}(C)$, given by

$$\sum_P n_P[P] \geq \sum_P m_P[P] \quad \Leftrightarrow \quad n_P \geq m_P \text{ for all } P.$$

Given a rational function φ, we can define its divisor as

$$\mathrm{div}(\varphi) = \sum_{P \in \mathrm{zero}(\varphi)} e_P[P] - \sum_{Q \in \mathrm{pole}(\varphi)} e_Q[Q].$$

But how do we know the order of something? I owe you an explanation of DVRs.

Definition 4.1. The following description are equivalent, and we call this a **discrete valuation ring** or **DVR**:

(1) a local PID which is not a field.

(2) $R = \mathcal{O}_K$ for a discrete valuation field with $v : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ satisfying $v(xy) = v(x) + v(y)$, $v(x + y) \geq \min(v(x), v(y))$, and $v(x) = \infty$ if and only if $x = 0$.

Example 4.2. Consider the field $\mathbb{Q}_p$ with the p-adic valuation. The ring of integers here, $\mathbb{Z}_p$, is a DVR. Another example is the field $\mathbb{C}((x))$ with the valuation of taking the minimal n with $a_n \neq 0$. Then the ring of integers $\mathbb{C}[[x]]$ is a DVR.

Now consider $\mathbb{A}^1$, with the affine coordinate ring $\mathbb{C}[x]$. The local ring at the origin is going to be something like

$$\mathscr{O}_{\mathbb{A}^1,\{0\}} = \left\{\frac{f}{g} : g(0) \neq 0\right\},$$

which has a natural valuation. On the other hand, if you look at $V(xy) \subseteq \mathbb{A}^2$ and look at the local ring at $(0,0)$, then

$$\mathscr{O}_{Z,\{0\}} = \left\{\frac{f}{g} : g(0) \neq 0\right\}$$

is not even an integral domain. This means that being a nonsingular curve is closely related to locally being a DVR.

Definition 4.3. A **uniformizer** of a DVR R is some $\varpi \in R$ such that $v(\varpi) = 1$.

Then any $z \in R$ is uniquely expressed as $z = u\varpi^{v(z)}$, where $u \in R^\times$.

If $\varphi : C_1 \to C_2$ is a map between curves, and $\varphi(P) = Q$, then we have a pullback map

$$\varphi^* : \mathscr{O}_{C_2,Q} \to \mathscr{O}_{C_1,P}.$$

Now consider a uniformizer in $\mathscr{O}_{C_2,Q}$ and $\mathscr{O}_{C_1,P}$ and call them t_Q and t_P. We define the **ramification index** at P as

$$e_P = \operatorname{ord}_P(\varphi^* t_Q),$$

so that $\varphi^* t_Q = u t_P^{e_P}$.

There is an analogous picture in algebraic number theory. If $\operatorname{Spec} \mathcal{O}_K$ lies over $\operatorname{Spec} \mathbb{Z}$, then we can look at the splitting

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r}.$$

This e_j is the analogue and this analogy can be made precise.

4.2 Differential forms

Definition 4.4. For $C/\overline{K}$ a curve, the space $\Omega^1_{C/\overline{K}}$ is (the global sections of meromorphic differentials) the vector space over $\overline{K}(C)$ generated by symbols $\{df : f \in \overline{K}(C)\}$ subject to the following relations:

(1) $da = 0$ if $a \in \overline{K}$,

(2) $d(f+g) = df + dg$,

(3) $d(fg) = f dg + g df$.

Example 4.5. Consider a curve $C : y^2 = x^3 + x$. Let $\omega = dx/2y$ be a differential. Then we have

$$\frac{dx}{2y} = \frac{dy}{3x^2 + 1}$$

and so

$$\omega = \Big(-\frac{9}{4}xy\Big)dx + \Big(\frac{3}{2}x^2 + 1\Big)dy \in \Omega_C^1.$$

5 September 19, 2017

I defined differential forms and gave some examples. For C a curve over $\overline{K}$, the meromorphic differential forms Ω^1_C is a $\overline{K}(C)$-vector space of dimension 1. If $f \in \overline{K}(C)$, $df \in \Omega^1_C$ is a basis if and only if $\overline{K}(C)/\overline{K}(f)$ is a finite separable extension.

Example 5.1. Consider the curve $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$. Take the function $x - e_1$. Let $P_j = (e_j, 0)$ be the intersection with the y-axis. (These are the points of order 2.) The divisor of this is

$$\operatorname{div}(x - e_1) = 2[P_1] - 2[\infty].$$

Why is this? For simplicity assume $e_1 = 0$. To find the order of zero at P_1, we need to look at the local ring and compute what power of the uniformizer it is. The local ring is

$$(\mathbb{C}[x, y]/y^2 - x(x - e_2)(x - e_3))_{(0,0)}.$$

In this ring, $x - e_2$ and $x - e_3$ are units. So this ring is

$$\mathbb{C}[x, y]_{(0,0)}/(y^2 - ux) \cong \mathbb{C}[y]_{(0)}.$$

with the identification $x = y^2/u$. Then y can be taken the be the uniformizer and so x has valuation 2. As an exercise, show that

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

5.1 Divisor of a meromorphic form

Recall that a map $\varphi : C_1 \to C_2$ gives a field extension $\overline{K}(C_1)/\overline{K}(C_2)$. We can also pullback differential forms. We can define

$$\varphi^* : \Omega^1_{C_2} \to \Omega^1_{C_1}; \quad \varphi(df) = d(\varphi^* f).$$

Lemma 5.2. *The map φ^* is injective if and only if φ is separable.*

If $\omega \in \Omega^1_C$ is a differential, its divisor is defined to be

$$\operatorname{div}(\omega) = \sum_{P \in \mathrm{zero}(\omega)} e_P[P] - \sum_{Q \in \mathrm{pole}(\omega)} e_Q[Q].$$

Here e_P is defined as the order of the rational function $\omega/dt_P = \varphi_P$ locally at P. This gives the notion of zeros and poles.

Lemma 5.3. *Both* zero(ω) *and* pole(ω) *consists of finitely many points.*

Example 5.4. Let's take the curve $C : y^2 = x(x - 1)(x + 1)$. What is $\operatorname{div}(dx)$? You can show that the zeros are precisely $\{(0, 0), (1, 0), (-1, 0)\}$ and the pole is at ∞. If you work hard, you can show that

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

So as a coincidence, we have

$$\operatorname{div}\Big(\frac{dx}{y}\Big) = 0.$$

5.2 Canonical divisor and genus

Given a curve, there is a canonical way of getting a divisor. Look at any differential form, and consider its divisor. This gives a divisor, and the class does not depend on the choice of the differential form. This is called **canonical divisor**.

Actually, there is a better way of looking at this. A divisor is actually an isomorphism class of line bundles. In this interpretation, we're just looking at the cotangent line bundle.

If $D \in \operatorname{Div}(C)$ is a divisor, we may consider

$$\mathscr{L}(D) = \{\varphi : \operatorname{div}(\varphi) + D \geq 0\} \cup \{0\}$$

which is a vector space over $\overline{K}$ of finite dimension. For example, $\mathscr{L}(0) = \overline{K}$ and $\mathscr{L}(D) = 0$ if $\deg D < 0$.

Define

$$\ell(D) = \dim_{\overline{K}}(\mathscr{L}(D)).$$

If $D = D' + \operatorname{div}(\varphi)$ for some φ, then $\ell(D) = \ell(D')$.

Definition 5.5. The **genus** of C is defined as $g_C = \ell(K_C)$, where K_C is the canonical divisor.

Consider an curve $C : y^2 = x^3 + ax + b$. Then the form $\omega = dx/y$ has $\operatorname{div}(dx/y) = 0$. So the canonical divisor is 0 and $\ell(K_C) = 1 = g_C$.

5.3 Degree-genus formula and Riemann–Roch

I am going to black box two theorems.

Theorem 5.6 (Degree-genus formula). *Consider a curve C in $\mathbb{P}^2$ of degree d. The genus of this curve is given by*

$$g = \frac{(d-1)(d-2)}{2}.$$

Theorem 5.7 (Riemann–Roch). *Let C be a smooth projective curve. For any divisor D,*

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

Implicitly, there is a Serre duality here that interchanges a certain H^0 and H^2. The dualizing sheaf K_C plays a role in this.

For example, plug in $D = 0$. Then we get that this is correct. Next, if we put $D = K_C$, we get

$$g - 1 = \deg(K_C) - g + 1$$

and so $\deg(K_C) = 2g - 2$.

Consider a curve of genus 1 in $\mathbb{P}^2$. I claim that it looks like

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

i.e., there is an isomorphism $\varphi \to C$ such that $O \mapsto \infty$. I'll give a sketch. Consider the divisor $n[O]$ with $n \geq 1$. By Riemann–Roch, we have

$$\ell(n[O]) = n + \ell(K_C - n[O]) = n.$$

Since $\ell([O]) = 2$, there is a non-constant element $x \in \mathscr{L}(2[O])$. Then there is another basis $y \in \mathscr{L}(3[O])$. Then $1, x, x^2, x^3, y, xy, y^2$ are in $\mathscr{L}(6[O])$. This shows that they are linearly dependent.

6 September 21, 2017

For the curve $y^2 = (x-e_1)(x-e_2)(x-e_3)$, we have

$$\operatorname{div}(x-e_i) = 2[P_i] - [\infty], \quad \operatorname{div}(y) = [P_1] + [P_2] + [P_3] - 3[\infty].$$

Also $\operatorname{div}(dx) = \operatorname{div}(y)$.

We have

$$\overline{K}(C) = \operatorname{Frac}\bigl(\overline{K}[x,y]/(y^2 - \textstyle\prod_i (x-e_i))\bigr).$$

The extension $\overline{K}(C)/\overline{K}(x)$ is comes from the map $x : C \to \mathbb{P}^1$ and the degree of this morphism is 2. This is because $\operatorname{div}(x-e_1)$ has two points over 0 and ∞. Likewise, $y : C \to \mathbb{P}^1$ has degree 3 and so $\overline{K}(C)/\overline{K}(y)$ has degree 3.

Our first goal is to show that a genus 1 curve in $\mathbb{P}^2$ looks like $y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$. Our second goal is to prove that $E \cong \operatorname{Pic}^0(E)$ is an isomorphism of groups.

6.1 Identifying the genus 1 curve

The tool we are going to use is Riemann–Roch: for $D \in \operatorname{Div}(C)$,

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

An application is that $\deg K_C = 2g - 2$.

Corollary 6.1. *Suppose $g = 1$. If $[P] = [Q] \in \operatorname{Pic}(C)$ for $P, Q \in C$, then $P = Q$.*

Proof. Suppose $\operatorname{div}(\varphi) = P - Q$. Then $\varphi \in \mathscr{L}([Q])$ but on the other hand,

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

This implies that φ is a constant function and so $P = Q$. □

Another observation to make is that if $P \in C$ and $g_C = 1$, then $\mathscr{L}([P]) = \overline{K}$.

Proposition 6.2. *Suppose C is a genus 1 curve and let O be a point. Then there exist $E \subseteq \mathbb{P}^2$ and an isomorphism $\alpha : C \xrightarrow{\sim} E \subseteq \mathbb{P}^2$ with $\alpha : O \mapsto \infty$, where E is given by*

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

Proof. Consider $\ell(n[O])$ for $n \geq 1$. This is

$$\ell(n[O]) = \ell(K_c - n[O]) + n - 1 + 1 = n.$$

We have $\ell([O]) = 1$ and $\ell(2[O]) = 2$. So there is a non-constant function x, such that x has a pole of order 2 at O. Next, $\ell(3[O]) = 3$ and so there is a function y that has a unique pole of order 3 at y.

On the other hand, $\ell(6[O]) = 6$ but

$$1, x, x^2, x^3, y, xy, y^2 \in \mathscr{L}(6[O]).$$

This implies that these are linearly dependent. This gives a relation between $x, y \in \overline{K}(C)$ satisfying

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

This gives a map $\alpha : C \to E$ where $E \subseteq \mathbb{P}^2$ is defined by the equation $(*)$.

We now want to show that $\deg \alpha = 1$. This will imply that α is an isomorphism. Note that x has a unique pole of order 2. This shows that $\overline{K}(C)/\overline{K}(x)$ is of degree 2. Likewise $\overline{K}(C)/\overline{K}(y)$ is of degree 3.

$$\begin{tikzcd}
 & \overline{K}(C) \arrow[ddl, dash, "2"'] \arrow[d, dash] \arrow[ddr, dash, "3"] & \\
 & \overline{K}(E) \arrow[dl, dash] \arrow[dr, dash] & \\
\overline{K}(x) & & \overline{K}(y)
\end{tikzcd}$$

This shows that $\overline{K}(C)/\overline{K}(E)$ has degree 1. □

6.2 Picard group of an elliptic curve

Theorem 6.3. *The map*

$$h : E \to \operatorname{Pic}^0(E); \quad P \mapsto [P] - [O]$$

is an isomorphism of groups.

Proof. We first show that it is a bijection of sets. Let us first prove surjectivity. For any $D \in \operatorname{Div}^0(E)$, we want to find a $P \in E$ and φ such that $D - ([P] - [O]) = \operatorname{div}(\varphi)$. We have

$$\ell(D + [O]) = 0 + 1 - 1 + 1 = 1$$

by Riemann–Roch. So there exists a $\varphi \neq 0$ such that $\operatorname{div} \varphi + D + [O] \geq 0$. Because this is of degree 1, there exists some $P \in E$ such that $\operatorname{div} \varphi + D + [O] = [P]$.

For injectivity, we need to prove that $[P] - [O] = [Q] - [O]$ then $P = Q$. This is by the first corollary today.

Now it suffices to show that $h(P + Q) = h(P) + h(Q)$. This can be seen from the geometric construction we used. If P, Q, R lie on the same line, then $[P] + [Q] + [R] - 3[O]$ is the divisor of the equation that cuts out that line. □

Lemma 6.4. *The group* $+ : E \times E \to E$ *is a morphism of varieties.*

6.3 Review of number theory

The big goal is to prove Mordell–Weil theorem, i.e., if E is defined over a number field K, $E(K)$ is finitely generated. Next, we are going to study, for a $F/\mathbb{Q}_p$, an elliptic curve E over F or $\mathbb{Q}_p$. From this we get a Galois representation. In some sense, number theory is studying the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, with class field theory concerned with only 1-dimensional representations. But the interesting thing is that elliptic curves produce a large number of 2-dimensional Galois representations of $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$. We want to understand the characters of this representation and when it is unramified.

Let us talk about extensions of number fields. You should look up $\mathbb{Q}_p$. Inside $\mathbb{Q}$ there is the ring of integers $\mathbb{Z}$. For $K/\mathbb{Q}$, I have the ring of integers $\mathcal{O}_K \subseteq K$. This is

$$\mathcal{O}_K = \{\alpha \in K : \alpha \text{ is a root of a monic integral polynomial}\}.$$

These are not PIDs, e.g., $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}) \in \mathbb{Q}[\sqrt{-5}]$. But they are Dedekind domains and have unique factorization of prime ideals. Then $(\mathcal{O}_K)_\mathfrak{p}$ are DVRs. So they can be though of as curves. So for this extension $\mathbb{Z} \hookrightarrow \mathcal{O}_K$, we can similarly define ramification.

If p is a prime, we can write

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Definition 6.5. The e_i is the **ramification index** of $\mathfrak{p}_i/\mathfrak{p}$ in $K/\mathbb{Q}$.

If $K/\mathbb{Q}$ is Galois, then $e(\mathfrak{p}_i/\mathfrak{p}) = e(\mathfrak{p}_j/\mathfrak{p})$.

7 September 29, 2017

I have defined elliptic curves over algebraically closed fields. But this is not very satisfactory, because we want to talk about rational solutions. In general, a variety X is defined over K if it the vanishing locus of functions with coefficients in K. That is, when its ideal can be generated by polynomials with rational coefficients. For instance, $(\pi y - \pi x^2) \subseteq \mathbb{C}[x, y]$ is defined over $\mathbb{Q}$.

Let $L/\mathbb{Q}$ be finite. If E/L is an elliptic curve, its rational points are rational solutions. We could also thing of this as

$$E(\overline{L})^{G_L} = E(L),$$

where G_L is the absolute Galois group.

7.1 Isogeny

Definition 7.1. Let E_1, E_2 be two elliptic curves (over k). An **isogeny** is a morphism $\varphi : E_1 \to E_2$ such that $\varphi(O_{E_1}) = O_{E_2}$.

We are also going to write

$$\mathrm{Hom}(E_1, E_2) = \mathrm{Isog}(E_1, E_2).$$

This is actually an abelian group, because if $\varphi_1, \varphi_2 \in \mathrm{Hom}(E_1, E_2)$, then we can define.

$$(\varphi_1 + \varphi_2)(x) = \varphi_1(x) +_2 \varphi_2(x).$$

Lemma 7.2. *Every isogeny $\varphi : E_1 \to E_2$ is a group homomorphism, i.e., $\varphi(x + y) = \varphi(x) + \varphi(y)$.*

Proof. We have the group isomorphism $E \to \mathrm{Pic}^0(E)$ given by $P \mapsto [P] - [O]$. So we have

$$\begin{tikzcd} E_1 \arrow[r, "\cong"] \arrow[d, "\varphi"] & \mathrm{Pic}^0(E_1) \arrow[d, "\varphi_*"] \\ E_x \arrow[r, "\cong"] & \mathrm{Pic}^0(E_2). \end{tikzcd}$$

Because φ_* is a group homomorphism, we also have that φ is a group homomorphism. □

If $\varphi : E_1 \to E_2$ is non-constant, it is surjective and we can look at it.

$$0 \to \ker(\varphi) \to E_1 \xrightarrow{\varphi} E_2 \to 0.$$

If there is no ramification, the kernel is going to be have size $\deg \varphi$.

Lemma 7.3. *φ is separable if and only if $\varphi^* : \Omega_{E_2} \to \Omega_{E_1}$ is nonzero.*

If φ is separable, then $|\ker(\varphi)| = \deg \varphi$.

For $m \neq 0 \in k$, there is the multiplication map

$$[m] : E \to E; \quad P \mapsto mP.$$

Lemma 7.4. *(1)* $[m] \neq 0$ *if* m *is an integer that is nonzero in* k.
(2) $[m]$ *is separable of degree* m^2.

Corollary 7.5. *Then* $\ker([m])$ *is isomorphic to* $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *(as a group scheme, or over an algebraically closed field).*

Proof. We know that $\ker([m])$ is an m-torsion abelian group of order m^2. Also, for $n \mid m$, there are n^2 elements of order dividing n. This implies that the group is actually $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. □

7.2 Invariant differential

To prove separability of $[m]$, we need to find a differential form that does not pull back to zero.

Theorem 7.6. *Let* T_a *be the translation by* $a \in E$. *There exists a differential* ω *such that* $T_a^*\omega = \omega$ *for all* a.

The proof of this goes by giving an explicit differential in coordinates.

Corollary 7.7. *Let* $\varphi \in \operatorname{Hom}(E_1, E_2)$. *Then* $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$.

Using this, we get $[m]^*\omega = m\omega$. This shows the first part of (2) in the lemma, that $[m]$ is separable.

8 October 3, 2017

Our goal is to show that for E/K, that $E(K)$ is finitely generated. This means that $E(K)$ has finite rank and torsion.

Definition 8.1. The rank of $E(K)$ is called the **algebraic rank** of E/K.

To show that $E(K)$ is finitely generated, we will show that $E(K)/mE(K)$ is finite and use height to show that $E(K)$ is finitely generated.

8.1 Group cohomology

We have the short exact sequence

$$0 \to E(\overline{K})[m] \to E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \to 0,$$

and we are going to take the Galois invariant. Taking invariants is left exact. So it continues as

$$0 \to E(K)[m] \to E(K) \xrightarrow{m} E(K) \to H^1(G_K, E(\overline{K})[m]) \to \cdots .$$

Our first job is to identify what H^i are.

Let M be an abelian group with an action of G. Then there are abelian groups $H^i(G,M)$. This is created in a way such that whenever

$$0 \to M' \xrightarrow{\varphi} M \to M'' \to 0$$

is an short exact sequence of abelian groups with equivariant maps, (i.e. a short exact sequence of G-module) then you get a long exact sequence

$$0 \to (M')^G \to M^G \to (M'')^G \to H^1(G,M') \to H^1(G,M) \to H^1(G,M'') \to \cdots .$$

Here, $H^0(G,M) = M^G$, and we are going to have

$$H^1(G,M) = \frac{Z^1(G,M)}{B^1(G,M)} = \frac{\{(\varphi : G \to M) : \varphi(g_1g_2) = g_1\varphi(g_2) + \varphi(g_1)\}}{\{(\varphi : G \to M) : \varphi_m(g) = gm - m \text{ for some } m\}}.$$

Here are some properties:

(1) Suppose M receives a trivial G action. Then $Z^1(G,M) = \mathrm{Hom}_{\mathsf{Grp}}(G,M)$ and $B^1(G,M) = 0$. So we have

$$H^1(G,M) = \mathrm{Hom}_{\mathsf{Grp}}(G,M).$$

(2) There is something called inflation-restriction. Suppose G acts on M and H is a normal subgroup of M. Then G/H acts on M^H. Then we have an exact sequence

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{inf}} H^1(G,M) \xrightarrow{\text{res}} H^1(H,M).$$

We have, by group cohomology,

$$\begin{aligned}&0 \to E(K)[m] \to E(K) \xrightarrow{m} E(K)\\ &\quad \to H^1(G_K, E(\overline{K})[m]) \to H^1(G_K, E(\overline{K})) \xrightarrow{m} H^1(G_K, E(\overline{K})) \to \cdots .\end{aligned}$$

So we have an injection

$$0 \to E(K)/mE(K) \hookrightarrow H^1(G_K, E(\overline{K})[m]) \twoheadrightarrow H^1(G_K, E(\overline{K}))[m] \to 0.$$

Lemma 8.2. *Suppose L/K is finite Galois. If $E(L)/mE(L)$ is finite, then $E(K)/mE(K)$ is finite.*

Proof. Let us consider the map $E(K) \to E(L)$. Let us take the quotient to get

$$\begin{tikzcd}
0 \arrow[r] & \ker(i) \arrow[r, hook] \arrow[d, hook] & E(K)/mE(K) \arrow[r, "i"] \arrow[d, hook] & E(L)/mE(L) \arrow[d, hook] \\
0 \arrow[r] & H^1(\mathrm{Gal}(L/K), E(\overline{K})[m]^{G_L}) \arrow[r] & H^1(G_K, E(\overline{K})[m]) \arrow[r] & H^1(G_L, E(\overline{K})[m]).
\end{tikzcd}$$

But we have that $\mathrm{Gal}(L/K)$ is finite and $E(\overline{K})[m]$ is finite. So this H^1 is finite and so $\ker(i)$ is finite. Because $E(L)/mE(L)$ is finite, $E(K)/mE(K)$ is finite. □

Let us first replace K by $K([m]^{-1}(O))$. This is adjoining all the coordinates of points in $[m]^{-1}E(O)$ to K. This only extends K in finite dimension. The result is that G_K acts trivially on $E(\overline{K})[m]$. Then we get an inclusion

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}_{\mathsf{Grp}}(G_K, E(\overline{K})[m]).$$

In other words, we have a pairing

$$E(K)/mE(K) \times G_K \to E(\overline{K})[m]$$

that is nondegenerate on the left side. What is the kernel of the right?

Proposition 8.3. *The kernel on the right is G_L, where $L = K([m]^{-1}E(K))$.*

9 October 5, 2017

Let E/K be an elliptic curve, and let $m \geq 2$.

Theorem 9.1. *$L = K([m]^{-1}E(K))$ is a finite extension over K.*

Theorem 9.2 (Weak Mordell–Weil)**.** *The group $E(K)/mE(K)$ is finite.*

Theorem 9.3 (Mordell–Weil)**.** *The group $E(K)$ is finitely generated.*

Today, we are going to show that Theorem 9.1 implies Theorem 9.2, and that this implies Theorem 9.3.

9.1 Weak Mordell–Weil theorem

Firstly, we may assume without loss of generality, that $E[m]$ is defined over K, after taking a finite extension. This is because of the statement that K'/K is finite Galois then $E(K')/mE(K')$ finite implies $E(K)/mE(K)$ finite. The proof of this fact went by looking at the inflation-restriction sequence

$$\begin{tikzcd}
0 \arrow[r] & \ker(i) \arrow[r, hook] \arrow[d, hook] & E(K)/mE(K) \arrow[r, "i"] \arrow[d, hook] & E(L)/mE(L) \arrow[d, hook] \\
0 \arrow[r] & H^1(\mathrm{Gal}(L/K), E(\overline{K})[m]^{G_L}) \arrow[r] & H^1(G_K, E(\overline{K})[m]) \arrow[r] & H^1(G_L, E(\overline{K})[m]).
\end{tikzcd}$$

The upshot of this is that G_K acts trivially on $E(\overline{K})[m]$, and so we get

$$E(K)/mE(K) \hookrightarrow H^1(G_K, E[m]) = \mathrm{Hom}(G_K < E[m]).$$

So there is a **Kummer pairing**

$$E(K)/mE(K) \times G_K \to E[m].$$

What is the kernel on the right? We need to figure out what this map is.

We had applied the Galois invariants of the sequence

$$0 \to E[m] \to E(\overline{K}) \xrightarrow{\times m} E(\overline{K}) \to 0$$

to get

$$0 \to E(K)[m] \to E(K) \xrightarrow{\times m} E(K) \xrightarrow{\phi} H^1(G_K, E[m]) \to \cdots .$$

In general, the boundary map ϕ can be described. A short exact sequence $0 \to M' \to M \to M'' \to 0$ gives rise to a boundary map $M'' \to H^1(G, M')$. This is described as, for each $m \in M''$ look at any preimage $n \in M$ and then looking at the cocycle

$$\varphi_m : G \to M'; \quad g \mapsto gn - n.$$

So let's apply this. For $P \in E(K)$, pick a $Q \in E(\overline{K})$ such that $mQ = P$. So the above recipe shows that this pairing is given by

$$(P, \sigma) \mapsto \sigma Q - Q.$$

So the kernel of the Kummer pairing on the right is going to be elements $\sigma \in G_K$ such that $\sigma Q = Q$ for all $Q \in [m]^{-1}E(K)$. That is, it is precisely

$$L = K([m]^{-1}E(K)).$$

In other words, the pairing actually is defined on

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G_K/G_L, E[m]) = \mathrm{Hom}(\mathrm{Gal}(L/K), E[m]).$$

If we know that $\mathrm{Gal}(L/K)$ is finite, then we deduce the $E(K)/mE(K)$ is finite.

9.2 Mordell–Weil theorem

For simplicity, let's do this over $K = \mathbb{Q}$. We can't say that that weak Mordell–Weil immediately implies Mordell–Weil. Take for instance $\mathbb{Q}$. The idea is that we do have something like the Euclidean algorithm on $\mathbb{Z}$ but not on $\mathbb{Q}$. Because $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite, we can label representatives as $P_1, \dots, P_r$. Then for all P, we can write $P = mQ_1 + P_{i_1}$ for some P_{i_1}, then $Q_1 = mQ_2 + P_{i_2}$ and so on. If we eventually hit a fixed finite set $\{R_1, \dots, R_s\}$ that we understand well, we are in good shape.

Lemma 9.4. *Suppose A is an abelian group such that there exists an $m \geq 2$ such that A/mA is finite. Suppose there exists a* ***height function*** *$h : A \to \mathbb{R}$ in the following sense:*

(1) there exists a constant β such that $h(mx) \geq m^2 h(x) - \beta$,

(2) for each $y \in A$, there exists a constant γ_y such that $h(x + y) \leq 2h(x) + \gamma_y$ for all $x \in A$,

(3) for every δ, the set $\{z \in A : h(z) < \delta\}$ is finite.

Then A is finitely generated.

Proof. Take a representative $\{P_1, \dots, P_r\} \subseteq A$ of A/mA. Write

$$P = mQ_1 + P_{i_1}, \quad Q_1 = mQ_2 + P_{i_2}, \quad Q_2 = mQ_3 + P_{i_3}, \dots.$$

Then the condition (1) implies

$$h(Q_{n+1}) \leq \frac{1}{m^2}(\beta + h(mQ_n)) = \frac{1}{m^2}(\beta + h(Q_n - P_{i_{n+1}})).$$

Let $\gamma = \max\{\gamma_{(-P_1)}, \dots, \gamma_{(-P_r)}\}$. Then we can continue

$$h(Q_{n+1}) \leq \frac{1}{m^2}(\beta + h(Q_n - P_{i_{n+1}})) \leq \frac{1}{m^2}(\beta + \gamma + 2h(Q_n)) \leq \frac{2}{m^2}h(Q_n) + c.$$

So if we iterate this process, we are going to get $h(Q_n)$ bounded for n sufficiently large. Then (3) shows that there can be only finitely many such possible Q_n. Now A is generated by P_i and the finitely many possible such Q_n. □

Theorem 9.5. *Consider an elliptic curve $E/\mathbb{Q}$ given by $y^2 = x^3 + Ax + B$. Define the function*

$$h : E(\mathbb{Q}) \to \mathbb{R}; \quad \Big(\frac{a_x}{b_x}, y\Big) \mapsto \log(\max\{|a_x|, |b_x|\}).$$

This is a height function.

Proof. I will only prove (2) and (3). You know how to compute the group law in coordinates, and here it is. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, then

$$x(P_1 + P_2) = \Big(\frac{y_1 - y_2}{x_1 - x_2}\Big)^2 - (x_1 + x_2).$$

Now let $P_0 = (x_0, y_0) = (\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3})$, and let $P = (\frac{a}{d^2}, \frac{b}{d^3})$. Plug it in, and you get

$$x(P_0 + P) = \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}.$$

Then

$$h(x(P_0 + P)) \le C_{x_0,y_0} + \log\max\{|a|^2, |d|^4, |bd|\}.$$

So we are almost done. P is a point on the elliptic curve, so

$$d^2b^2 = d^2a^3 + Aad^6 + Bd^8 \le C_{A,B}\max\{|a|^4, |d|^8\}.$$

This shows that

$$h(x(P_0 + P)) \le C_{x_0,y_0,A,B} + \log\max\{|a|, |d|^2\}.$$

You can check (1) similarly.

The third condition is clear, because there are just finitely many rationals with bounded height. □

Corollary 9.6. *$E(\mathbb{Q})$ is finitely generated.*

Next time we will start looking at Tate modules.

10 October 10, 2017

Today we are going to talk about Tate modules. We will first define p-adic numbers.

10.1 p-adic numbers

If p is a prime, we can consider

$$\cdots \to \mathbb{Z}/p^3\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}.$$

Then we can define $\mathbb{Z}_p$ to be its limit, $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. This consists of elements

$$(x_1, x_2, \dots) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \cdots, \quad x_n \bmod p^{n-1} = x_{n-1}.$$

The ring $\mathbb{Z}_p$ has characteristic zero, because if $N < p^k$, then $N \neq 0 \in \mathbb{Z}/p^k\mathbb{Z}$ and hence $N \neq 0 \in \mathbb{Z}_p$.

Every $\mathbb{Z}/p^k\mathbb{Z}$ has a discrete topology, and we can use this to give $\mathbb{Z}_p$ a profinite topology. The topology on $\mathbb{Z}_p$ is totally disconnected, i.e., for any $x \neq y$, they are in different connected components.

Algebraically, $\mathbb{Z}_p$ is a discrete valuation ring with maximal ideal $p\mathbb{Z}_p$ and residue field $\mathbb{F}_p$. We also write $\mathbb{Q}_p$ for the fractional field of $\mathbb{Z}_p$. Because $\mathbb{Q}_p$ is a local field, there is a short exact sequence

$$0 \to I_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p} \to 0,$$

where I is the inertia group. Here, we know $G_{\mathbb{F}_p} \cong \hat{\mathbb{Z}}$.

10.2 Tate modules

Let E/k be an elliptic curve, and $\ell \neq \operatorname{char} k$ be a prime. We have

$$E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}.$$

We can take the inverse limit, and define the **Tate module** as

$$T_\ell E = \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Now the Galois group G_k acts on $E[\ell^n]$, and so we get a continuous action of G_k on $T_\ell E$, with respect to the profinite topologies on each side. Then we get a group homomorphism

$$\rho_E : G_k \to \operatorname{Aut}_{\mathbb{Z}_\ell} T_\ell E = \mathrm{GL}_2(\mathbb{Z}_\ell).$$

That is, there is a ℓ-adic representation attached to E. This is also related to étale cohomology with $\mathbb{Z}_\ell$ and $\mathbb{Z}_\ell$ coefficients. More precisely, $H^1_{\text{ét}}(E, \mathbb{Z}_\ell)^\vee \cong T_\ell E$.

We can use Tate modules to study isogenies between elliptic curves. Suppose we have some isogeny $\varphi{:}E_1 \to E_2$. Clearly this induces a map $E_1[\ell^n] \to E_2[\ell^n]$, and if we take the inverse limit, we get

$$\varphi_\ell : T_\ell E_1 \to T_\ell E_2.$$

That is, we get a map

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell E_1, T_\ell E_2).$$

Proposition 10.1. *This map is injective.*

Proof. Suppose $\varphi : E_1 \to E_2$ such that $\varphi_\ell = 0$. Then $\varphi : E_1[\ell^n] \to E_2[\ell^n]$ is zero for all n, so $\ker \varphi$ has infinite cardinality. This is impossible unless $\varphi = 0$. □

Proposition 10.2. *Actually,* $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell E_1, T_\ell E_2)$ *is an injection.*

Here, note that $\mathrm{Hom}(E_1, E_2)$ is torsion-free.

Proof. Let $\varphi \in \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$ such that $\varphi_\ell = 0$. We can write

$$\varphi = \alpha\psi_1 + \cdots + \alpha_s\psi_s,$$

where $\alpha_i \in \mathbb{Z}_\ell$.

Fix $n \geq 1$ and choose integers $a_1, \dots, a_n$ such that $a_i \equiv \alpha_i \pmod{\ell^n}$. Now

$$\psi = a_1\psi_1 + \cdots + a_s\psi_s$$

is a true isogeny, and we have $\psi(E_1[\ell^n]) = 0$. Then we can write $\psi = [\ell^n] \circ \lambda$ for some $\lambda \in \mathrm{Hom}(E_1, E_2)$. But we can't yet conclude that $\alpha_i \equiv 0 \pmod{\ell^n}$, which is what we need.

So let us go back to representing φ. Let

$$M = \mathbb{Z}\psi_1 + \mathbb{Z}\psi_2 + \cdots + \mathbb{Z}\psi_s \subseteq \mathrm{Hom}(E_1, E_2)$$

be a $\mathbb{Z}$-submodule. Then let

$$M^{\mathrm{div}} = \{\psi' \in \mathrm{Hom}(E_1, E_2) : [m] \circ \psi' \in M \text{ for some } m\}.$$

Note that $M \subseteq M^{\mathrm{div}} \subseteq \frac{1}{d}M$, where $d = \mathrm{lcm}_i \deg \psi_i$. This shows that M^{div} is still a free abelian group of finite rank. (Everything is torsion-free because $\mathrm{Hom}(E_1, E_2)$ is torsion-free.)

Now replace $\psi_1, \dots, \psi_s$ by a basis of M^{div}. We had $\psi = [\ell^n] \circ \lambda$ for some λ, and by divisibility, we also have $\lambda \in M^{\mathrm{div}}$. So we can write

$$\lambda = b_1\psi_1 + \cdots + b_s\psi_s,$$

and by linear independence of ψ_i, we get $a_i = \ell^n b_i$. That is, $\alpha_i \equiv 0 \pmod{\ell^n}$. □

Corollary 10.3. $\operatorname{rank}_{\mathbb{Z}} \operatorname{Hom}(E_1, E_2) \leq 4$.

Theorem 10.4 (Isogeny theorem)**.** *We have an isomorphism* $\operatorname{Hom}_k(E_1, E_2) \otimes \mathbb{Z}_\ell \xrightarrow{\cong} \operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell E_1, T_\ell E_2)^{G_k}$*, when*

(1) k is a finite field (Tate 1966, Endomorphisms of abelian varieties over finite fields)

(2) k is a number field (Faltings 1983, Finiteness theorems for abelian varieties over number fields).

10.3 Endomorphism ring of an elliptic curve

Let $\varphi : E_1 \to E_2$ be an isogeny. This map induces a map

$$\varphi^* : \operatorname{Pic}^0 E_2 \to \operatorname{Pic}^0 E_1; \quad \sum m_i P_i \mapsto \sum m_i \varphi^{-1}(P_i).$$

Recall that we also have a map $\lambda_E : E \xrightarrow{\cong} \operatorname{Pic}^0(E)$. So we can define the dual

$$\varphi^\vee : E_2 \xrightarrow{\lambda_{E_2}} \operatorname{Pic}^0(E_2) \xrightarrow{\varphi^*} \operatorname{Pic}^0(E_1) \xrightarrow{\lambda_{E_1}^{-1}} E_1.$$

This is called the **dual isogeny**.

Proposition 10.5. *Let* $\varphi : E_1 \to E_2$ *be a degree* m *isogeny.*

(1) $\varphi^\vee \circ \varphi = [m]$ *on* E_1 *and* $\varphi \circ \varphi^\vee = [m]$ *on* E_2*.*

(2) $(\varphi + \psi)^\vee = \varphi^\vee + \psi^\vee$*.*

(3) $(\varphi \circ \psi)^\vee = \psi^\vee \circ \varphi^\vee$*.*

(4) $(\varphi^\vee)^\vee = \varphi$*.*

(5) $[m]^\vee = [m]$*.*

This is what we will use the understand $\operatorname{End}(E)$. We have already noted that $\operatorname{rank}_{\mathbb{Z}} \operatorname{End}(E) \leq 4$, and we also have this anti-involution $\vee$ satisfying (3) and (4).

Proposition 10.6. *Suppose* R *is a ring and* $\iota : R \to R$ *is a anti-involution satisfying* $\operatorname{rk}_{\mathbb{Z}} R \leq 4$*. Also assume* ι *satisfies*

- $\iota(\varphi + \psi) = \iota(\varphi) + \iota(\psi)$,
- $\iota(\varphi\psi) = \iota(\psi)\iota(\varphi)$,
- $\iota(m) = m$,
- $\varphi\iota(\varphi) \in \mathbb{Z}_{\geq 0}$.

Then R *is one of the following:*

(1) $\mathbb{R} = \mathbb{Z}$

(2) R is a subring of an imaginary quadratic field of finite $\mathbb{Z}$-rank,

(3) R is a subring of the quaternion algebra of finite $\mathbb{Z}$-rank.

Definition 10.7. If E/k is an elliptic curve of $\operatorname{End}(E) \supsetneq \mathbb{Z}$, then we say that E has **complex multiplication**.

If k has characteristic zero, only (1) and (2) can happen. If k has characteristic p, then only (2) and (3) can happen. This is because there is the Frobenius that acts on k.

10.4 Weil pairing

Suppose E/k is an elliptic curve.

Proposition 10.8. *For a positive integer $n > 0$, relatively prime to* $\operatorname{char} k$*, there exists a non-degenerate, Galois equivariant, bilinear pairing*

$$e_n : E[n] \times E[n] \to \mu_n \subseteq \overline{k}$$

*that is alternating, i.e., $e_n(x, x) = 1$, and is compatible with different n. This is called the **Weil pairing**.*

Hence this induces

$$e_\ell : T_\ell E \times T_\ell E \to \mu_{\ell^\infty} = \mathbb{Z}_\ell(1).$$

Another way to think about this is that we have the cup product on H^1, which takes them to H^2, and then some Poincaré duality gives the map.

Here is another way to think about it. Note that $\bigwedge^2 T_\ell E \cong \mathbb{Z}_\ell(1)$. This corresponds to the determinant map

$$\det \rho_E : G_k \to \mathbb{Z}_\ell^\times$$

of the character.

11 October 12, 2017

For an elliptic curve, we can look at its rational points $E(\mathbb{Q})$, which is finitely generated. On the other hand, we now have a way of looking at torsion points $E[m]$ or $T_\ell(E)$, which also receives an action from $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Here, we can also look at local models, like $E/\mathbb{Q}_p$, and consider $T_\ell(\mathbb{Q}_p)$ having an action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

11.1 Reduction

Recall the proof of weak Mordell–Weil. WE had the embedding

$$E(K)/mE(K) \hookrightarrow H^1(G_{\overline{K}/K}, E(\overline{K})[m]),$$

and then we had an embedding

$$\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Hom}(E(K)/mE(K), E(\overline{K})[m]).$$

This shows that L/K is an abelian, and all elements are killed after multiplying m.

Now there is a theorem that says that if L/K is abelian and there is some N such that $\sigma^N = 1$ for all $\sigma \in \mathrm{Gal}(L/K)$, and L/K is unramified over all but finitely many primes, then it is finite.

Here is the philosophy. We have two ways of mapping $\mathbb{Z}_p$ to a field:

$$\mathbb{F}_p \twoheadleftarrow \mathbb{Z}_p \hookrightarrow \mathbb{Q}_p.$$

Now the curve $xy = p$ in $\mathbb{A}^2$ is nonsingular if we change to $\mathbb{Q}_p$ but it is singular if we change to $\mathbb{F}_p$.

Now $\mathbb{Z}_p$ can be considered as a line, and the two fibers are going to be the one defined over $\mathbb{Q}_p$ and the one over $\mathbb{F}_p$. We can ask, for a curve E defined over $\mathbb{Q}_p$, whether there is a curve $\mathcal{E}$ such that it has good reduction over $\mathbb{F}_p$.

This is our strategy for studying $E(K)[m]$, for $K/\mathbb{Q}_p$. There is some mysterious "Neron model" $\mathcal{E}$ so that we have $E(K) \cong \mathcal{E}(\mathcal{O}_K$. Then we can actually reduce

$$\begin{tikzcd}
& E(K)[m] \arrow[d, hook] & \\
\ker = \hat{E} \arrow[r] & E(K) \arrow[r, two heads, "\text{reduction}"] \arrow[d, "\cong"] & E_s(k_s) \\
& \mathcal{E}(\mathcal{O}_K) \arrow[ur, "\text{reduction}"'] &
\end{tikzcd}$$

The key theorem is now that $E(K)[m] \to E_s(k_s)$ is a injective map. If you change the diagram, this is equivalent to that $\times m : \hat{E} \to \hat{E}$ is injective.

Let us try to think what $\hat{E}$ looks like. We have

$$p\mathbb{Z}_p \to \mathbb{Z}_p \to \mathbb{F}_p, \quad 1 + p\mathbb{Z}_p \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times.$$

Here, $\hat{E}$ really is going to be a formal group.

11.2 Formal group

The group law for $p\mathbb{Z}$ can be written as $(x, y) \mapsto x + y$, and the group law for $1 + pF$ can be written as $(x, y) \mapsto x + y + xy$.

Definition 11.1. A **commutative formal group law** is a power series $F(x, y) \in K[[x, y]]$ such that

(1) $F(x, y) = x + y +$ (higher order terms),

(2) $F(F(x, y), z)) = F(x, F(y, z))$,

(3) $F(x, y) = F(y, x)$.

Example 11.2. There are $F(x, y) = x + y$, $F(x, y) = x + y + xy$, and there are $F(x, y)$ for elliptic curves.

Lemma 11.3. *(1) $F(x, 0) = x$ and $F(y, 0) = y$.*

(2) There exists a unique $i(x)$ such that $F(x, i(x)) = F(i(x), x) = 0$.

Proof. (1) is an exercise. (2) follows from Hensel's lemma. □

A **morphism** between two formal group laws from $F(x, y)$ to $G(x, y)$ is an $f \in K[[t]]$ such that

$$f(F(x, y)) = G(f(x), f(y)).$$

Definition 11.4. Let me give a naïve definition. Let $K/\mathbb{Q}_p$. A **formal group** over K is (m_K, F) where F is a formal group law and $m_K \subseteq \mathcal{O}_K$ is the maximal ideal.

Here, if $x, y \in m_K$, then $F(x, y)$ actually converges to an element in m_K, and it turns out that this forms a commutative group on m_K.

Proposition 11.5. *Let (m_K, F) be a formal group.*

(1) $[m]T = mT +$ higher order terms.

(2) If $a \in \mathcal{O}_K$ is invertible and $f(T) = aT +$ higher order terms, then there exists a g such that $f(g(T)) = f(g(T)) = T$.

Proof. (1) We can do this by induction.

(2) This is by Hensel's lemma. I claim that there exist $g_n(T) \in \mathcal{O}_K[[T]]$ for all n such that $f(g_n(T)) \equiv T \pmod{T^{n+1}}$ and $g_{n+1}(T) \equiv g_n(T) \pmod{T^n}$. Take $g_1(T) = a^{-1}T$. Now take $g_{n+1} = g_n + \lambda T^n$. Then we will have

$$f(g_{n+1}(T)) \equiv f(g_n(T)) + a\lambda T^n = T + a\lambda T^n + bT^n \pmod{T^{n+1}}.$$

Then set $\lambda = -b/a$. □

12 October 17, 2017

We were talking about formal groups. This is a power series $F(x, y) \in R[[x, y]]$ satisfying

(1) $F(x, y) = x + y + \text{higher order terms}$,

(2) $F(x, F(y, z)) = F(F(x, y), z)$,

(3) $F(x, y) = F(y, x)$,

(4) there exists a $i(x)$ such that $F(x, i(x)) = F(i(x), x) = 0$,

(5) $F(x, 0) = x$, $F(0, y) = y$.

Here, (4) and (5) are implied by (1), (2), (3).

12.1 Formal group associated to an elliptic curve

If I can associate a power series to each group, you get a better feeling of what the group looks like. Let us consider the elliptic curve that looks like

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

and choose $z = -\frac{x}{y}$ and $w = -\frac{1}{y}$. Then we get

$$w = z^3 + a_1zw + a_2z^2w + \cdots = f(z, w),$$

and we can regard $w = w(z)$ as a function of z to parametrize. We would then have

$$\begin{aligned} w(z) &= f(z, w) = f(z, f(z, w)) = f(z, f(z, f(z, w))) = \cdots \\ &= z^3(1 + A_1z + A_2z^2 + \cdots) \end{aligned}$$

which is a power series in z. Then we get a parametrization

$$x(z) = \frac{1}{z^2(1 + A_1z + \cdots)}, \quad y(z) = -\frac{1}{z^3(1 + A_1z + \cdots)}.$$

This is how you get the formal group. If you have $z_1, z_2 \in E$, you have a group law $z_3 = z_3(z_1, z_2)$ on the elliptic curve, and you can check that

$$F(z_1, z_2) = z_1 + z_2 + \cdots$$

and it is a formal group law because addition on an elliptic curve is commutative and associative.

Definition 12.1. A morphism $f : F \to G$ is a power series $f \in R[[T]]$ such that $f(0) = 0$ and $f(F(x, y)) = G(f(x), f(y))$.

Proposition 12.2. *Let $f = aT + \text{higher terms}$ with $a \in R^\times$. Then there exists a unique g such that $f(g(T)) = g(f(T)) = T$.*

Corollary 12.3. *If $m \in R^\times$, then $[m] : F \to F$ is an isomorphism.*

13 October 19, 2017

13.1 Weierstrass minimal model

Recall that the curve $E : y^2 = x^3 + Ax + B$ is nonsingular if and only if $\Delta_E = 4A^3 + 27B^2 \neq 0$. Let E/K_v be a curve over a local field. (For this lecture, take $K_v = \mathbb{Q}_p$.) If the coefficients are $A, B \in \mathbb{Q}_p$, then you can change variables to get

$$Y^2 = X^3 + (Au^4)X + (Bu^6).$$

Now we want to choose the minimal u such that $Au^4, Bu^6 \in \mathbb{Z}_p$.

Definition 13.1. The **Weierstrass minimal model** for $E/\mathbb{Q}_p$ is the $Y^2 = X^3 + A'X + B'$ such that $A', B' \in \mathbb{Z}_p$ and $v(\Delta')$ is minimal among all possible choices. (This is unique up to units.)

Let E be a minimal model. Define the special fiber E_s as

$$E_s = E \otimes_{\mathbb{Z}_p} \mathbb{F}_p : y^2 = x^3 + \overline{A}x + \overline{B}.$$

Then this is a curve over $\mathbb{F}_p$. This has no reason to be an elliptic curve. For instance, when

$$y^2 = x^3 + \frac{1}{p^5},$$

we would get $E_s : y^2 = x^3 + p = x^3$, so it is singular. This is a particular case of Néron models.

Let E be an elliptic curve over $\mathbb{Q}$, and let $E_{\min}$ be its minimal model. Let us assume that E_s is an elliptic curve.

Lemma 13.2. *$E(\overline{\mathbb{Q}_p}) = E_{\min}(\overline{\mathbb{Z}_p})$.*

Lemma 13.3. *Consider*

$$0 \to \ker(r) \to E_{\min}(\overline{\mathbb{Z}_p}) \xrightarrow{r} E_s(\overline{\mathbb{F}_p}) \to 0$$

and $M(E)$ the formal group $(m = (p), F_E)$. There is an isomorphism $M(E) \to \ker(r)$.

Corollary 13.4. *The map $[m] : E(\overline{\mathbb{Q}_p}) \to E(\overline{\mathbb{Q}_p})$ with $p \nmid m$ induces an isomorphism on $\ker(r)$.*

Proof. Because $m \in \overline{\mathbb{Z}_p}^\times$, the map $[m]$ on the formal group is invertible. □

So we get a diagram, and applying the snake lemma gives the following corollary.

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & 0 \arrow[r] \arrow[d] & E(\overline{\mathbb{Q}_p})[m] \arrow[r, hook] \arrow[d] \arrow[dr] & E_s(\overline{\mathbb{F}_p})[m] \arrow[d, hook] & \\
0 \arrow[r] & \ker(r) \arrow[r] \arrow[d, "{[m]}", "\cong"'] & E(\overline{\mathbb{Q}_p}) \arrow[r] \arrow[d, "{[m]}"] & E_s(\overline{\mathbb{F}_p}) \arrow[r] \arrow[d, "{[m]}"] & 0 \\
0 \arrow[r] & \ker(r) \arrow[r] & E(\overline{\mathbb{Q}_p}) \arrow[r] & E_s(\overline{\mathbb{F}_p}) \arrow[r] & 0
\end{tikzcd}$$

Corollary 13.5. *If E_s is nonsingular, i.e., E has good reduction, then*

$$\psi : E(\overline{\mathbb{Q}_p})[m] \hookrightarrow E_s(\overline{\mathbb{F}_p})$$

is injective for $p \nmid m$.

Then consider $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ acting on $E[m] = E(\overline{\mathbb{Q}_p})[m]$. Also note that there is

$$0 \to I_p \to \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \to 0.$$

Lemma 13.6. *The map ψ is $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$-equivariant.*

This shows that I_p trivially on $E[m]$. That is $E[m]$ is unramified. Take $\ell \neq p$. Then I_p acta trivially on $E[\ell^n]$ for all n, so I_p acts trivially on the Tate module $T_\ell E = \varprojlim_n E[\ell^n]$.

14 October 25, 2017

We had the minimal model $\mathcal{E}/\mathbb{Z}_p$. We need to show that $E(\overline{\mathbb{Q}}_p) \cong \mathcal{E}(\overline{\mathbb{Z}}_p)$ and $0 \to M(E) \to \mathcal{E}(\overline{\mathbb{Z}}_p) \to E_s(\mathbb{F}_p) \to 0$.

Corollary 14.1. *If E has good reduction, then $G_{\mathbb{Q}_p}$ acting on $E[m]$ is unramified.*

14.1 Inertia actions

Take $\mathbb{Q}_p$ as an example. Consider the absolute Galois group $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. There is a map

$$G_{\mathbb{Q}_p} \twoheadrightarrow \hat{\mathbb{Z}} \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to 0.$$

How is this defined? We can look at $\overline{\mathbb{Z}}_p$ sitting inside $\overline{\mathbb{Q}}_p$. Another strategy is to find a subextension $L/\mathbb{Q}_p$ so that $\mathrm{Gal}(L/\mathbb{Q}_p)$ is $\hat{\mathbb{Z}}$.

We use

$$L = \mathbb{Q}_p^{\mathrm{unr}} = \text{maximal unramified subextension } L \subseteq \overline{\mathbb{Q}}_p \text{ of } \mathbb{Q}_p.$$

Lemma 14.2. *There exists a short exact sequence*

$$0 \to I_K \to G_K \to \mathrm{Gal}(K^{\mathrm{unr}}/K) \to 0,$$

where I_K is defined as

$$I_{L/K} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(x) \equiv x \bmod \mathfrak{P} \textit{ for all } x \in \mathcal{O}_L\}, \quad I_K = \varinjlim_{L} I_{L/K}.$$

15 October 26, 2017

15.1 Unramified and tamely ramified extensions of local fields

We have the short exact sequence

$$0 \to I(K/\mathbb{Q}_p) \to \mathrm{Gal}(K/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(k/\mathbb{F}_p) \to 0.$$

Here, $I(K/\mathbb{Q}_p) = \{\sigma \in \mathrm{Gal} : \sigma x \equiv x \pmod{\varpi}\}$. As an aside, there also is a wild inertia

$$P(K/\mathbb{Q}_p) = \{\sigma : \sigma x \equiv x \pmod{\varpi^2}\}.$$

Then P is the unique p-Sylow subgroup of I.

Definition 15.1. Let G act on a set S. This is **unramified** of I acts trivially. It is also called **tamely ramified** if P acts trivially.

Definition 15.2. An extension of local fields L/K is **unramified** if $e = 1$. It is **tamely ramified** if $p \nmid e$ and **wildly ramified** if $p \mid e$.

What this all means is that we have a tower

$$\begin{tikzcd}
L \arrow[d, dash, "{p^{v_p(e)}, \text{ wild}}"] \\
L^1 = L^P \arrow[d, dash, "{e/p^{v_p(e)}, \text{ tame}}"] \\
L^0 = L^I \arrow[d, dash, "{f, \text{ unramified}}"] \\
K
\end{tikzcd}$$

You can also do this for infinite extensions. The field L^P is the maximal tamely ramified subextension. So we will have

$$\begin{tikzcd}
\overline{\mathbb{Q}}_p \arrow[d, dash] \\
\mathbb{Q}_p^{\mathrm{tam}} = \overline{\mathbb{Q}}_p^{P_{\mathbb{Q}_p}} \arrow[d, dash] \\
\mathbb{Q}_p^{\mathrm{unr}} = \overline{\mathbb{Q}}_p^{I_{\mathbb{Q}_p}} \arrow[d, dash] \\
\mathbb{Q}_p
\end{tikzcd}$$

Lemma 15.3. *Let $p \nmid m$ and consider a root of unity ζ_m. Then $K = \mathbb{Q}_p(\zeta_m)$ is unramified over $\mathbb{Q}_p$.*

Proof. Compute the discriminant. Or show that the surjection $G(K/\mathbb{Q}_p) \to G(\mathbb{F}_p(\zeta_m)/\mathbb{F}_p)$ bijective by counting elements. □

Proposition 15.4. *We have $\mathbb{Q}_p^{\mathrm{unr}} = \bigcup_{p \nmid m} \mathbb{Q}_p(\zeta_m)$ and $\mathbb{Q}_p^{\mathrm{tam}} = \bigcup_{p \nmid n} \mathbb{Q}(p^{1/n})$.*

Then $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_P) \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ and we get

$$0 \to I_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p} \to \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \to 0.$$

Here, the tame part of the inertia group is

$$I_{\mathbb{Q}_p}/P_{\mathbb{Q}_p} \cong \prod_{r \neq p} \mathbb{Z}_r.$$

15.2 Good reduction and unramified Tate modules

Let us go back to elliptic curves. Fix any $\ell \neq p$ and $E/\mathbb{Q}_p$. We have the action

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \text{ over } T_\ell(E).$$

Theorem 15.5. *(1) The Tate module is unramified if and only if E has good reduction.*
(2) The Tate module is tamely unramified if and only if E has semistable reduction.

Recall that if E/K with $K/\mathbb{Q}_p$ finite, a minimal Weierstrass model for E is given by

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

where $a, b \in \mathcal{O}_K$ and Δ is minimal as possible. Also recall that E is defined to have **good reduction** if and only if $\Delta_{\min} \in \mathcal{O}_K^\times$. This is equivalent to $\Delta(E_s) \neq 0$. What can go wrong with elliptic curves? If it is singular, then it either has a node or a cusp.

Definition 15.6. A bad reduction can be either **semistable**, which means that there is a node, or **additive**, which means that there is a cusp.

In the case when E has a good reduction, there is a map

$$E(K) \to E_s(k) \to 0; \quad (x : y : z) \mapsto (x : y : z).$$

Here we need to scale so that $x, y, z \in \mathcal{O}_K$ and one of them is a unit. This map is surjective because we have Hensel's lemma.

Lemma 15.7. *We have a map*

$$\widehat{M}_E \xrightarrow{\cong} \ker(r : E(K) \to E_s(k)).$$

Let us recall $\widehat{M}_E = (\mathfrak{m}_K, F_E)$. Here, we have used $z = -\frac{x}{y}$ and $w = -\frac{1}{y}$. Then there is a map

$$z \mapsto \Big(\frac{z}{w(z)}, -\frac{1}{w(z)}\Big) \in E(K).$$

This maps to the origin, i.e., infinity point, because

$$v_K\Big(\frac{z}{w(z)}\Big) = v_K\Big(\frac{z}{z^3(1+\cdots)}\Big) = -2v_K(z) \leq -2$$

and likewise $v_K(-1/w(z)) < 0$.

It is clear that it is a group homomorphism because the formal group law came from addition. To show that this is a bijection, we create an inverse map

$$\ker(r) \to \widehat{M}_E; \quad (x, y) \mapsto -\frac{x}{y} \in \mathfrak{m}_K.$$

This really lies in $\mathfrak{m}_k$ because $y^2 = x^3+ax+b$ with $a, b \in \mathcal{O}_K$ implies $v_K(y) = 3v$ and $v_K(x) = 2v$ for some $v < 0$.

Corollary 15.8. *If E has good reduction and $p \nmid m$, then $E(K)[m] \hookrightarrow E_s(k)$.*

Corollary 15.9. *If E has good reduction then $T_\ell(E)$ is unramified.*

Proof. We need to show that $I_K = I(\overline{K}/K)$ acts on $E[\ell^n]$ trivially. Take K'/K such that $E[\ell^n] \subset E(K')$. So

$$E(K')[\ell^n] \hookrightarrow E_s(K')$$

is Galois-equivariant and so I_K fixes $E[\ell^n]$. □

16 October 31, 2017

We have seen that E/K_v has good reduction if and only if for all $\ell \neq p$, $T_\ell(E)$ is unramified. I will show you that if $T_\ell(E)$ is unramified for some $\ell \neq p$ then E has good reduction.

16.1 Global review

So far we've been looking at $E(K)$ and $E[m]$, but a priori there aren't any relations between them. Now to prove Mordell–Weil, we need to show that $K([m]^{-1}(E(K)))$ is finite over K. This is because we have

$$E(K)/mE(K) \hookrightarrow H^1(G_K, E[m]).$$

We may assume without loss of generality that $E(K)$ contains $E[m]$, so then G_K acts trivially on $E[m]$. Then

$$E(K)/mE(K) \hookrightarrow \operatorname{Hom}(G_K, E[m]).$$

The G_K part kernel is going to be G_L where $K([m]^{-1}(E(K)))$. So if we get that this is finite, then $E(K)/mE(K)$ embeds into $\operatorname{Hom}(\operatorname{Gal}(L/K), E[m])$, which is finite.

But let me use some facts about $\operatorname{Gal}(L/K)$. The Weil pairing gives that

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

This shows that L/K is an abelian extension, and also it is Galois group is m-torsion. Now it is a fact in number theory that an abelian extension that is unramified at almost all primes and has finite exponent is finite.

Proposition 16.1. *If L/K is abelian of exponent m, and it is unramified over almost all primes, then it is finite.*

If p is not infinite, not a divisor of m, and has good reduction, then we will show that L/K is unramified at p.

Theorem 16.2. *Let E/K and $L = K([m]^{-1}E(K))$, and let S be the primes with bad reduction, or divisors of m, or ∞. Then L/K is unramified at every p not in S.*

Now L/K being unramified at p means that L_P/K_p for all P dividing p. To prove this theorem, it suffices to show that for all $Q \in [m]^{-1}E(K)$,

$$K(Q) = K'/K$$

is unramified at all p not in S.

But recall that E/K_p has good reduction if and only if $E[\ell^k]$ is unramified for all k and ℓ not dividing p. Then $E[m]$ is unramified at p, because m is made out of primes not dividing p. We want to show that for any $\sigma \in I_P$, $\sigma Q - Q = 0$. But

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

Also because p has good reduction, we can look at the image under reduction $E(K'_P) \to E_s(k')$. But because σ is inertial, it is sent to 0 in $E_s(k')$. So

$$0 \to \ker \to E(K'_P) \twoheadrightarrow E_s(k') \to 0$$

shows that $\sigma Q - Q$ is in the kernel. But $[m]$ acts isomorphically on the kernel. This shows that $\sigma Q - Q = 0$.

17 November 1, 2017

We want to prove the following:

Proposition 17.1. *If L/K is abelian of exponent m and L/K is unramified at almost all primes, then L/K is finite.*

Proposition 17.2. *Let E/K be an elliptic curve and let $L = K([m]^{-1}E(K))$. If p is a finite prime with good reduction, such that E has good reduction, then L/K is unramified at p.*

Proof. We did this last time. We want to show that for any $Q \in [m]^{-1}(K)$, $K' = K(Q)/K$ is unramified at p. That is, for any P over p, we want to show that $K(Q)_P = K'_P/K_p$ is unramified.

We need to show that for all $\sigma \in I_P$, $\sigma Q - Q = 0$. To show this, recall that

$$0 \to \ker \to E(K'_P) \to E_s(k'_P) \to 0$$

is exact. But $\sigma Q - Q \in E(K'_P)$ maps to 0 so lies in the kernel. On the other hand, the kernel is the associated formal group. Also $[m](\sigma Q - Q) = \sigma([m]Q) - [m]Q = 0$. But m is not divisible by p and so $\sigma Q = Q$. □

17.1 Kummer theory

To prove Proposition 17.1, we can assume that $\zeta_m \in K$ without loss of generality. This is because we can apply the theorem to $L(\zeta_m)/K(\zeta_m)$.

What I claim is that every abelian extension of exponent m is contained in a compositum of fields $K(\sqrt[n]{a})/K$. If you think about it, finding an finite abelian extension E/K of exponent m is finding a quotient

$$G_K \to \mathrm{Gal}(E/K).$$

This maps to $\mathbb{Z}/m\mathbb{Z}$, so this is sort of looking at $H^1(G_K, \mathbb{Z}/m\mathbb{Z})$.

So consider the sequence

$$0 \to \mu_m \to K^\times \xrightarrow{m} K^\times \to H^1(G_K, \mu_m) \to H^1(G_K, \overline{K}^\times) \to \cdots .$$

But Hilbert 90 gives $H^1(G_K, \overline{K}^\times) = 0$. So we get the isomorphism

$$K^\times/(K^\times)^m \cong \mathrm{Hom}(G_K, \mu_m)$$

because $\mu_m \subseteq K^\times$.

18 November 2, 2017

We need to prove the following:

Proposition 18.1. *Let L/K be an abelian extension of exponent m and unramified outside a finite set. Then L/K is finite.*

This follows from the following two facts:

Theorem 18.2. *(a) (Class number theorem) If $K/\mathbb{Q}$ is finite, then Cl_K is finite.*

(b) (Unit theorem) $\mathcal{O}_K^\times$ is finitely generated.

Note that the Picard group of $\operatorname{Spec}\mathcal{O}_K$ is just the class group. This is because the divisors are just fractional ideals and principal divisors are principal fractional ideals.

18.1 Class number theorem

I am going to define the **adele** as

$$\mathbb{A}_{\mathbb{Q}}^{\infty} = \prod\nolimits'_p \mathbb{Q}_p = \Big\{(x_p) \in \prod_p \mathbb{Q}_p : x_p \in \mathbb{Z}_p \text{ for almost every } p\Big\}, \quad \mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \mathbb{A}_{\mathbb{Q}}^{\infty}.$$

Then $\mathbb{Q}$ naturally includes in $\mathbb{A}_{\mathbb{Q}}$. I am going to give this a topology such that the open sets are $\prod_p U_p$ with $U_p = \mathbb{Z}_p$ for almost all p and U_p open in $\mathbb{Q}_p$. It is a fact that $\mathbb{A}_{\mathbb{Q}}$ becomes a topological ring with this structure.

Now we want to give a topology on $\mathbb{A}_{\mathbb{Q}}^\times$ so that it is a topological group. But if I just give the subspace topology, it might be that the inversion on $\mathbb{A}_{\mathbb{Q}}^\times$ is not continuous. So we embed

$$\mathbb{A}_{\mathbb{Q}}^\times \hookrightarrow \mathbb{A}_{\mathbb{Q}} \times \mathbb{A}_{\mathbb{Q}}; \quad x \mapsto (x, x^{-1})$$

and give a subspace topology here. So we get a embedding $\mathbb{Q}^\times \hookrightarrow \mathbb{A}_{\mathbb{Q}}^\times$.

We can similarly define

$$\mathbb{A}_K = \prod\nolimits'_{v \text{ finite}} K_v \times \prod_{v \mid \infty} K_v.$$

Then

$$K^\times \hookrightarrow \mathbb{A}_K^\times \twoheadrightarrow C_K = \mathbb{A}_K^\times / K^\times.$$

This idelic class group C_K actually surjects onto $\mathrm{Cl}(K)$. The map is given by $(x_p) \mapsto (p)^{v_p(x)}$.

Because $C_K \twoheadrightarrow \mathrm{Cl}_K$, it would be nice if C_K is finite. But this is not true because we have infinite stuff. So we define

$$\mathbb{A}'_K = \Big\{x = (x_v) : \prod_v |x|_v = 1\Big\} \subseteq \mathbb{A}_K^\times.$$

It is a fact that $K^\times \subseteq \mathbb{A}_K^1$. Also, $\mathbb{A}'_K / K^\times \twoheadrightarrow \mathrm{Cl}_K$.

Now, $\mathbb{A}'_K$ is compact. Also, $K^\times$ is an open subgroup. This shows that $\mathbb{A}'_K / K^\times$ is finite and discrete. Thus it is finite, and it follows that Cl_K is finite.

18.2 Concluding Mordell–Weil

For a finite set of prime S containing all infinite primes, we consider

$$\mathcal{O}_{K,S} = \{x \in K : v(x) \geq 0 \text{ for all } v \notin S\}.$$

Then $\mathcal{O}_{K,S}^\times$ is finitely generated. This is because it is finitely generated over $\mathcal{O}_K^\times$, and $\mathcal{O}_K^\times$ is finitely generated by the unit theorem.

Now let us go back to the proposition. We know that

$$L \subseteq K(\{\sqrt[m]{a} : a \in K^\times/(K^\times)^m\}).$$

But when is $K(\sqrt[m]{a})/K$ unramified outside S? We can compute the discriminant and it is going to be

$$a^{m-1} \cdot \operatorname{Disc}(K(\zeta_n)/K) = \pm a^{m-1} m^m.$$

So if it is going to be unramified at $v \notin S$, we would need $v(a) \equiv 0 \pmod{m}$.

On the other hand, we note that

$$\mathcal{O}_{K,S}^\times \twoheadrightarrow \Sigma = \{a \in K^\times/(K^\times)^n : m \mid v(a) \text{ for all } v \notin S\}.$$

This is because we have elements $x_i \in K$ such that $v_j(x_i) = \delta_{ij}$ for all $v_j \in S$. Also $L \subseteq K(\{\sqrt[m]{a} : a \in \Sigma\})$. Then we get $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^m \twoheadrightarrow \Sigma$ and $\mathcal{O}_{K,S}^\times$ is finitely generated so $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^m$ is finite. Then Σ is finite, and then the extension L/K is finite.

19 November 14, 2017

There is a modular form

$$\begin{aligned} f(q) &= q\prod_n (1-q^n)^2(1-q^{11n})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + \cdots \end{aligned}$$

of weight 2.

19.1 Hasse's theorem

We are now going to consider elliptic curves over a finite field. To get a feeling, consider an elliptic curve

$$E : y^2 + y = x^3 - x^2$$

over $\mathbb{F}_p$ for all p such that $p \nmid \Delta$.

Question. *What is the size of $E(\mathbb{F}_p)$?*

Over $\mathbb{Q}$, we've been showing that this is finitely generated. Over $\mathbb{F}_p$, it is going to finite anyways. Actually there is a trivial bound

$$\#E(\mathbb{F}_p) \leq 2p + 1.$$

This is because for each x there is at most 2 solutions y and there is also the infinity point. But heuristically, half of the time you will be able to solve for x and half of the time you will not be able to solve it. So you expect $\#E(\mathbb{F}_p) \sim p + 1$.

Theorem 19.1 (Hasse)**.** *$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}$.*

I would like to also consider $\alpha_p = (p+1) - \#E(\mathbb{F}_p)$ and see what this means. Let us compute this number.

p	2	3	5	7	13	17
$\#E(\mathbb{F}_p)$	5	5	5	10	10	20
α_p	-2	-1	1	-2	4	-2

Table 1: Number of rational points of E over $\mathbb{F}_p$

Note that this is exactly the coefficients of the weight 2 modular form I have written above.

Definition 19.2. An elliptic curve is **modular** if there exists a modular form f such that its q-expansion

$$f(q) = \sum a_n q^n$$

satisfies $a_p = \alpha_p$.

It is a big theorem of Wiles and other people such that a lot of elliptic curves are modular.

Let me give another heuristic for Hasse's theorem. What is going to happen is there are going to be two complex numbers x_1, x_2 of absolute value $\sqrt{p}$ such that $\alpha_p = x_1 + x_2$. Or maybe we can find a linear map T so that α_p is the trace of T and p is the determinant.

Suppose p is a good prime, so that $E/\mathbb{Q}$ gives $E/\mathbb{F}_p$. Now there is a Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \text{ on } T_\ell(E)$$

and because it is unramified, this gives an action of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on $T_\ell(E)$. Now there is a Frobenius σ_p that generates $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. The claim that the action of σ_p has trace α_p and determinant p. Then you need to show that the eigenvalues have absolute value $\sqrt{p}$.

Now I am going to give you a cheat proof that doesn't work in general, but works for elliptic curves.

Proof. Recall a bunch of things from before. If $\phi : E_1 \to E_2$ is an isogeny, we can define its dual isogeny $\hat{\phi} : E_2 \to E_1$ such that

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

Also recall that $\phi : E_1 \to E_2$ is separable if and only if $\phi^* : \Omega^1_{E_2} \to \Omega^1_{E_1}$ is nonzero. For example, the map

$$\varphi : E \to E; \quad (x, y) \mapsto (x^p, y^p)$$

is not separable. This is because

$$\varphi^*\Big(\frac{dx}{2y + a_1 x + a_3}\Big) = \frac{d(x^p)}{\cdots} = \frac{px^{p-1}dx}{\cdots} = 0.$$

Because $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$, we have $(1 - \varphi)^*\omega = \omega$ and so $1 - \varphi$ is separable. This implies that the size of the fiber of $1 - \varphi$ is the degree of $1 - \varphi$.

What is $E(\mathbb{F}_p)$? It is the fixed points of $E(\overline{\mathbb{F}}_p)$ under the Frobenius. So it is the kernel of $1 - \varphi$, which has size the degree of $1 - \varphi$. Then we need to show

$$2\sqrt{p} \geq |\deg(1 - \varphi) - p - 1| = |\deg(1 - \varphi) - \deg(1) - \deg(\varphi)|.$$

Because $2\sqrt{\deg(1)\deg(\varphi)} = 2\sqrt{p}$, it suffices to show that $\deg : \mathrm{End}(E) \to \mathbb{Z}$ is a quadratic form. But recall that $[\deg(\varphi)] = \varphi \circ \hat{\varphi}$. Then

$$\langle f, g \rangle = \deg(f + g) - \deg(f) - \deg(g)$$

is a bilinear form. □

20 November 29, 2017

We've been proving the Weil conjectures for elliptic curves.

Theorem 20.1 (Weil conjectures)**.** *For smooth and proper $V/\mathbb{F}_p$ of dimension d, we define*

$$Z(V,t) = \exp\biggl(\sum_{n\geq 0} \frac{\#(V(\mathbb{F}_{p^n}))}{n} t^n\biggr).$$

Then

(i) $Z(V,t) \in \mathbb{Q}(t)$,

(ii) it satisfies a functional equation,

(iii) the Riemann Hypothesis holds. That is, if

$$Z(V,t) = \frac{P_1(t)\cdots P_{2d-1}(t)}{P_0(t)P_2(t)\cdots P_{2d}(t)}$$

with

$$P_i = \prod_{j=1}^{\deg P_i} (1-\beta_{ij}(t)) \in \mathbb{Z}[t],$$

each β_{ij} is "pure of weight j", i.e., $|i(\alpha)| = p^{j/2}$ for all $i : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

If we define

$$\zeta(V,s) = Z(V, p^{-s}),$$

this means that all the zeros of $\zeta(V,s)$ have imaginary parts half-integers, and poles have imaginary parts integers.

Last time we showed that

$$Z(E,t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-pt)}.$$

So what we need to show that α and β have pure weight of 1.

20.1 Modular forms

From my point of view, the motivation is to construct Galois representations. Basically given a modular form, you get a geometric object. This is going to be what we are going to do shortly. As I have said, getting a module form from a geometric object is the modularity conjecture. From a geometric object, we get a Galois representation of $G_{\mathbb{Q}}$. The converse direction is called the Fontaine–Mazur conjecture and is also hard. The Langlands is between modular forms and Galois representations.

Consider the upper half plane $\mathcal{H} = \{\Im(z) > 0\}$ and look at the $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathcal{H}$, given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}.$$

In $\mathrm{SL}_2(\mathbb{Z})$, given N there exist subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}, \qquad \Gamma_1(N) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$
$$\Gamma(N) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}.$$

These all acts properly discontinuously, so we can define $\Gamma \backslash \mathcal{H} = Y_\Gamma$ as a Riemann surface.

Here is the philosophy. The moduli space of elliptic curves is $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$. Then $\Gamma \setminus \mathcal{H}$ is going to parametrize elliptic curves with some level structure.

Definition 20.2. Note that $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, with the identification given by the entry d. Consider $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$. A **modular form** of weight k and level Γ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

(1) for any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$,
$$f(\gamma\tau) = (c\tau + d)^k f(\tau),$$
(2) it "grows mildly" at ∞.

This is an odd definition. A more natural definition can be made in terms of sections of line bundles. The first condition means that f is a section ω^k on $Y_\Gamma = \mathcal{H}/\Gamma$. If ω^k is the differentials, we get

$$d(\gamma z) = \frac{1}{(cz+d)^2} dz$$

and so weight is -2.

The reason I want Γ_1 in Γ is that $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$. Then $f(\tau + 1) = f(\tau)$. So we have a Fourier expansion

$$f(\tau) = \sum a_n e^{2\pi i \tau n}.$$

The mild growth condition is then going to mean that this is holomorphic at 0, so that we are adding over $n \geq 0$.

Definition 20.3. We say that f is a **cusp form** if $a_0 = 0$. $M_k(\Gamma)$ are the modular forms, and $S_k(\Gamma) \subseteq M_k(\Gamma)$ are the cusp forms.

Next time we are going to define a diamond operator $\langle d \rangle$ and also I am going to define the Hecke operator. For every $p \nmid N$, we can define operators T_p on $S_2(\Gamma)$. Let $\mathbb{T}$ be the algebra generated by T_p. Also, they commute with each other, so we can simultaneously diagonalize. A simultaneous eigenvector is called an eigenform. Let us write

$$T_p f = a_p f.$$

It turns out that $a_p = a_p(f)$ is the p-th coefficient.

There is a concrete formula for T_p. It is given by

$$T_p(f) = \frac{1}{p}\sum_{i=0}^{p-1} f\Big(\frac{\tau + i}{p}\Big) + p\langle d\rangle f(p\tau).$$

If $p \mid N$, there are operators U_p on $S_2(\Gamma)$ and then we can consider $\mathbb{T}^+$ the algebra generated by U_p.

21 November 30, 2017

The Langlands conjecture is roughly trying to establish

$$\left\{\begin{matrix}\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p) \\ \text{“geometric”}\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}\text{automorphic representations} \\ \text{of } \mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})\end{matrix}\right\}.$$

Class field theory is the $n = 1$ trivial case of Langlands. Thef left side is something like 1-dimensional representations of $G_{\mathbb{Q}}^{\mathrm{ab}}$ and the right hand side is characters $\mathbb{Q}^\times \setminus \mathbb{A}_{\mathbb{Q}}^\times \to \mathbb{C}^\times$.

But this is hard, and people look at the local version instead. Let $\ell \neq p$. Then

$$\left\{\begin{matrix}\rho_\ell : G_{\mathbb{Q}_\ell} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p) \\ \varphi\text{-s.s.}\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}\text{automorphic representations} \\ \text{of } \mathrm{GL}_n(\mathbb{Q}_\ell)\end{matrix}\right\}.$$

But we should have something for $\ell = \infty$. But there is no Galois group whose representation corresponds to automorphic representations of $\mathrm{GL}_n(\mathbb{R})$.

Grothendieck actually looked at something that might work. Recall that $\mathbb{Z}$ lies in $G_{\mathbb{F}_p}$ and so we can look at the inverse image.

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] & G_{\mathbb{Q}_\ell} \arrow[r, two heads] & G_{\mathbb{F}_\ell} \arrow[r] & 0 \\
0 \arrow[r] & I \arrow[r] \arrow[u, equal] & W_\ell \arrow[r, two heads] \arrow[u, hook] & \mathbb{Z} \arrow[r] \arrow[u, hook] & 0
\end{tikzcd}$$

Here W_ℓ is topologized so that I is open. Then the left hand side would correspond to representations $W_\ell \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$. In the $\ell = \infty$ case, we have $W_\infty = \mathbb{C}^\times \rtimes \{\pm 1\}$ that behaves well.

Lemma 21.1. *Let α, β be the eigenvalues of the map ϕ acting on $T_\ell(E)$. Then $|\alpha| = |\beta| = p^{1/2}$.*

Proof. The characteristic polynomial is $f(X) = X^2 - \mathrm{tr}(\phi)X + \det(\phi) = (X - \alpha)(X - \beta)$. Our goal is to show that $f(X) = (X-\alpha)(X-\beta) \geq 0$ for all $X \in \mathbb{R}$, or maybe $X \in \mathbb{Q}$. But note that

$$0 \leq \det(n - m\phi) \cdot m^2 = \det(n - m\phi|_{T_\ell(E)}) = \det(\tfrac{n}{m} - \phi_{T_\ell(E)})m^2 = f(\tfrac{n}{m})m^2.$$

So we are done. □

21.1 Modular curves

We were trying to get an elliptic curve over $\mathbb{Q}$ form a modular form of weight 2, with $\mathbb{Q}$ coefficients. The reason we are working over $\mathbb{Q}$ is that if we work with a number field we would get an abelian variety.

What was an elliptic curve? We defined it as a genus 1 curve with a marked point. But over $\mathbb{C}$, this just looks like $\mathbb{C}/\Lambda$ where Λ is a lattice. Because we can scale Λ, we can fix one point to be 1. Then we can determine an elliptic curve by this one complex number. But there are different ways of writing down the same lattice, so the moduli space of elliptic curves is

$$\mathcal{E}ll = \mathrm{GL}_2(\mathbb{Z}) \setminus \mathcal{H}^{\pm 1} = \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}.$$

So if $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$, then there is a map $Y_\Gamma \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$. Because $\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H}$ is the moduli space of elliptic curves, Y_Γ should be the moduli space of elliptic curves with some "level Γ" structure. You should think about what this structure really means. It is related to the p-torsion points.

We can define

$$\Gamma_0(N) \setminus \mathcal{H} = Y_0(N), \quad \Gamma_1(N) \setminus \mathcal{H} = Y_1(N).$$

These are not necessarily compact spaces, but you make a one-point compactification and make it into a curve $X_0(N)$ and $X_1(N)$. These are called **modular curves**. It can be proved that they have nice integral models. Generally, Y_Γ can be compactified to X_Γ.

22 December 6, 2017

We had a moduli interpretation of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ as elliptic curves. The exercise was to figure out what $\Gamma_0(p)\backslash\mathcal{H}$ corresponds to. Then answer is that it corresponds to a pair of lattices $\Lambda \subseteq \Lambda'$ of index p, and this corresponds to an elliptic curve with a order p subgroup. The reason is that in $\Gamma_0(p)$ you are only allowed to send e_1 to $xe_1 + (py)e_2$ and so you have to fix the sublattice generated by e_1 and pe_2. To see how this is an elliptic curve with a order p subgroup, you look at $\frac{1}{p}\Lambda'$ inside Λ.

What does $\Gamma_1(p)\backslash\mathcal{H}$ classify? These are elliptic curves with a point of order p. Again, this sends e_1 to something that is e_1 modulo p. So the choice of e_1 modulo p determines everything. So looking at $\frac{1}{p}e_1$ gives a order p point. Then the map

$$\Gamma_1(p) \setminus \mathcal{H} \to \Gamma_0(p) \setminus \mathcal{H}$$

is given by mapping (E, Q) to $(E, \langle Q\rangle)$.

Likewise, $\Gamma(p)\backslash\mathcal{H}$ corresponds to elliptic curves E with a choice of p-torsion points α, β that are linearly independent over $\mathbb{F}_p$.

22.1 Hecke operators

Recall that $M_k(\Gamma)$ are the modular forms, and $S_k(\Gamma)$ are the cusp forms. Suppose that $p \nmid N$. These are maps

$$T_p : M_k(\Gamma) \to M_k(\Gamma).$$

Here is a description. Suppose $f : \mathcal{H} \to \mathbb{C}$ satisfies $f(\gamma z) = j(\gamma z)^{-k} f(z)$, where $j(z) = \frac{1}{cz+d}$.

Now consider the two maps

$$\begin{tikzcd}
& \Gamma_0(pN) \setminus \mathcal{H} \arrow[dl, "f_1"'] \arrow[dr, "f_2"] & \\
\Gamma_0(N) \setminus \mathcal{H} \arrow[rr, dashed] & & \Gamma_0(N) \setminus \mathcal{H}
\end{tikzcd}$$

where the left map is given by $(E, H \times H') \mapsto (E, H)$ and the right map is given by $(E, H \times H') \mapsto (E/H', H)$, where H and H' are subgroups of order N and p. Now we get a map from $\Gamma_0(N) \setminus \mathcal{H}$ to $\Gamma_0(N) \setminus \mathcal{H}$ on divisors, given by pull-back and push-forward, i.e., looking at the preimages on the left map and then projecting down on the right map.

Now in algebraic geometry, you can also pull back and push forward a section and then get another section. Here, what you're doing is looking at what a point is mapped to, and then add them up.

Let me summarize the properties of Hecke operators.

- T_p acts on $S_k(\Gamma)$.
- T_p commute with each other.

- Each T_p is self-adjoint with respect to an inner product on $S_k(\Gamma)$. So we have a simultaneous diagaonalization

  $$S_k(\Gamma) = \bigoplus_v \mathbb{C}\langle v\rangle.$$

  So if $\mathbb{T}$ is the $\mathbb{C}$-algebras generated by Hecke operators, then each v corresponds to a character $\theta : \mathbb{T} \to \mathbb{C}$. Such is called a Hecke eigensystem.
- If $f = \sum a_n q^n$ and $a_1 = 1$, then $\theta_f(T_p) = a_p$.

So the crucial thing is to study the space of modular forms, rather than individual modular forms. This was a big shift of the theory, due to Hecke.

23 December 7, 2017

Last time we were talking about the modular curve $Y_0(N) = \Gamma_0(N) \setminus \mathcal{H}$ and $Y_1(N) = \Gamma_1(N) \setminus \mathcal{H}$ with compactifications $Y_0(N) \hookrightarrow X_0(N)$ and $Y_1(N) \hookrightarrow X_1(N)$. For $N \geq 5$, the curves $X_1(N)$ are going to be smooth schemes over $\mathbb{Z}[N^{-1}]$. Then $X_0(N)$ is a smooth Deligne–Mumford stack over $\mathbb{Z}[N^{-1}]$.

Last time we described the Hecke correspondence. Fix N and a prime ℓ. For $p \nmid N\ell$, we have two projections

$$\begin{tikzcd}
 & X_0(pN) \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
X_0(N) \arrow[rr, dashed] & & X_0(N)
\end{tikzcd}$$

and then we can pull-back push-forward. The map is actually

$$J_0(N) = \mathrm{Pic}^0(X_0(N)) \to J_0(N).$$

In general, Pic^0 is going to be represented by a scheme. So the Jacobian $J_0(N)$ is also going to be a scheme and the Hecke correspondence is a map on schemes.

Let me tell you a bit more about abelian varieties. These are projective group schemes, and over $\mathbb{C}$ they are always going to look like $\mathbb{C}^g/\Lambda$ where Λ is a rank $2g$ lattice. Here, you need to specify more data, namely polarization, to make this into a scheme. We can also look at Tate modules. If you have an abelian variety $A/\mathbb{Q}$, then

$$T_\ell(A) = \varprojlim A[\ell^n]$$

has a $G_\mathbb{Q}$-action, and so gives a Galois representation

$$\rho_{A,\ell} : G_\mathbb{Q} \to \mathrm{GL}_{2g}(\overline{\mathbb{Z}}_\ell).$$

23.1 Eichler–Shimura construction

Let f be a cusp eigenform of level $\Gamma_0(N)$, normalized so that $a_1 = 1$. This means that it gives a character $\theta : \mathbb{T} \to \mathbb{C}$ given by $T_p \mapsto a_p$. It turns out that a_p all lie in some number field, so let $K = \mathbb{Q}(a_p)$. Let $[K : \mathbb{Q}] = g$. Consider the ideal

$$\mathfrak{a} = \ker(\theta) \subseteq \mathbb{T}$$

acting on $J_0(N)$. (This is defined over $\mathbb{Z}[N^{-1}]$.) The Jacobian $J_0(N)$ has good reduction away from N, and we can define

$$A_f = J_0(N)/\mathfrak{a}J_0(N).$$

Lemma 23.1. *A_f is an abelian variety of dimension g.*

There is a general construction in algebraic geometry, and this gives you n elliptic curve. Or for simplicity assume that $g = 1$. Then we get a Tate module $V = T_\ell(A_f)$. Here we want to show that

$$a_p = \mathrm{tr}(\varphi_p|_V).$$

We first look at a integral model $J_0(N)_{\mathbb{Z}_p}$, with the Hecke operators T_p acting on it. We want to show that this action is integral. This is done by base changing to $\mathbb{F}_p$, i.e., looking at the special fiber.

$$\begin{tikzcd}
J_0(N)_{\mathbb{Z}_p} \arrow[d] & J_0(N)_{\mathbb{F}_p} \arrow[l, hook'] \arrow[d] \\
\operatorname{Spec} \mathbb{Z}_p & \operatorname{Spec} \mathbb{F}_p \arrow[l, hook']
\end{tikzcd}$$

Theorem 23.2 (Eichler–Shimura)**.** *On $J_0(N)_{\mathbb{F}_p}$, we have $T_p = F + V$.*

Here, F is the Frobenius, and V is the Vershiebung, the dual of the Frobenius map. But because we have good reduction, the trace of T_p can be computed as the sum of the traces of F and V.

Corollary 23.3. *a_p is indeed $\operatorname{tr}(\varphi_p|_V)$.*

This is a complicated construction, but it is the start of everything.

23.2 Two stories

We have studied elliptic curves along with Riemann–Roch, and we studied the Picard group and the group law. We looked at the Tate module, and proved Mordell–Weil. Then we studied elliptic curves over finite fields, we can actually count points here. This led to the more general study of Weil conjectures and modular forms.

Fermat's last theorem says that there is no solution to $x^p + y^p = z^p$. If there is such a solution, we can consider the elliptic curve

$$E : y^2 = x(x - \alpha^p)(x - \beta^p)$$

where α and β are some solutions. This is called the **Frey curve**. Suppose E comes from a modular form f. Then by the Eichler–Shimura construction, we get a Galois representation ρ_f of level N. (Here f is of weight 2 and level N.) Ribet made this conjecture that to this we can associate an f of weight 2 and level 2. Then $f \in S_2(\Gamma_0(2))$. But the dimension is the genus of $S_2(\Gamma_0(2))$, which is 0. This gives a contradiction, and so there cannot be a solution. So all you need to prove Fermat's last theorem is the modularity conjecture.

Theorem 23.4 (Taylor–Weils, modularity lifting)**.** *Consider the representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{F}_p)$. If $\overline{\rho}$ is "modular" and ρ satisfies some nice conditions, then ρ is modular.*

Here "modular" means that it is a reduction of some modular form. This is called the "$R = \mathbb{T}$" theorem. Here is how you use this. It can be shown that every $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_2)$ that is "nice" is going to be modular. So if ρ_E has "nice" reduction $\overline{\rho}_E$, then we can use modularity lifting to conclude that ρ_E is modular. But what if it is not nice? You can show that there exists a E' such that $E'[3]$ is nice and $E'[5] \cong E[5]$. But $E'[3]$ nice implies that $\rho_{E'}$ modular, and so $E'[5]$ is nice. Then you can use modularity lifting again to get that ρ_E is modular.

Conjecture 23.5 (Birch–Swinnerton-Dyer)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then we can define the algebraic rank $r_{\text{alg}} = \operatorname{rk} E(\mathbb{Q})$. This is equal to the analytic rank r_{an}, defined as the order of zero of $L(E,s)$.*

Here, $L(E,s)$ was not even defined meromorphically on the complex plane before the modularity conjecture. How they did analytic continuation was by using the fact that $L(f,s)$ is equal to $L(E,s)$.

Index